GUIDE D'AUDIT DES DISPOSITIFS « LANCEURS D'ALERTE »

AGUERA Charline
M2 Audit Interne des Organisations
2018

« J'ai compris qu'il ne suffisait pas de dénoncer l'injustice, il fallait donner sa vie pour la combattre. »

Albert Camus

Remerciements

J'adresse mes remerciements à l'ensemble des personnes qui m'ont aidé dans la réalisation de ce mémoire.

En premier lieu je souhaite adresser mes remerciements les plus sincères à l'ensemble des auditeurs du service Contrôle Périodique du Crédit Agricole Alpes Provence pour leurs conseils et leur transmission de savoir.

Je tiens à remercier particulièrement Amélie BRIES et Matthieu CHIRON pour le temps qu'ils ont accordé à répondre à mes questions.

Je remercie également toute l'équipe pédagogique de ma formation et en particulier Jacques VERA pour m'avoir accompagnée dans le choix de ce sujet.

Je désir aussi remercier Audrey ADDE et Philippe MAS pour m'avoir fourni des informations sur leur entreprise, leur contribution est essentielle à ce projet.

Je souhaite également remercier l'ensemble des personnes qui ont accepté de répondre à mon questionnaire d'enquête sans qui je n'aurais pas pu mener ce projet là où je le souhaitais.

Enfin, je remercie Michel BLANC, Responsable du service Contrôle Périodique du Crédit Agricole Alpes Provence pour son aide, le temps qu'il m'a accordé et son avis critique. Il m'a guidé dans mon travail et m'a aidé à trouver des solutions pour avancer.

Sommaire

Remerciements ***3***

Table des matières ***5***

Table des annexes ***6***

Introduction ***7***

PARTIE 1 : LE CONCEPT DE « LANCEURS D'ALERTE » : DE L'ORIGINE AUX ETATS-UNIS A LA MISE EN PLACE EN FRANCE DEPUIS LA LOI SAPIN II ***9***

PARTIE 2 : LES RISQUES ASSOCIES AUX DISPOSITIFS ***27***

PARTIE 3 : GUIDE D'AUDIT DES DISPOSITIFS D'ALERTE INTERNE ET DE RECUEIL DES SIGNALEMENTS ***37***

Conclusion ***81***

Bibliographie ***83***

Annexes ***88***

Table des matières

Remerciements ***3***

Sommaire ***4***

Table des matières ***5***

Table des annexes ***6***

Introduction ***7***

PARTIE 1 : LE CONCEPT DE « LANCEURS D'ALERTE » : DE L'ORIGINE AUX ETATS-UNIS A LA MISE EN PLACE EN FRANCE DEPUIS LA LOI SAPIN II ***9***

I- Évolution du concept : du Whistleblowing aux lanceurs d'alerte **10**

A. Naissance du concept aux États-Unis 10

B. L'introduction récente en France 11

Fig. 1 : Focus UKBA **13**

II- Loi Sapin II : apports et mise en conformité **13**

A. Le contenu de la loi 13

B. La mise en place des dispositifs de recueil des alertes 22

C. État des lieux : où en sont les entreprises dans leur mise en conformité ? 25

PARTIE 2 : LES RISQUES ASSOCIES AUX DISPOSITIFS ***27***

I- Les risques liés à la règlementation et aux dispositifs **28**

A. Les risques lors de la mise en place du dispositif 28

B. Les risques techniques liés aux dispositifs 29

II- Le risque de rejet des utilisateurs potentiels **33**

PARTIE 3 : GUIDE D'AUDIT DES DISPOSITIFS D'ALERTE INTERNE ET DE RECUEIL DES SIGNALEMENTS ***37***

I- Objet de l'étude et champ d'investigation : **38**

II- Sommaire du Guide d'audit **40**

III- Guide d'audit **40**

IV- GRILLES D'ANALYSE **63**

A. Notice explicative des grilles d'analyse **63**

B. Grilles d'analyse 68

Consultation du CHSCT Comité d'Hygiène, de Sécurité et des Conditions de Travail 70

Conclusion ***80***

Bibliographie ***82***

ANNEXES ***87***

Table des annexes

Annexe 1 : Informations autorisées par la CNIL.....88

Annexe 2 : Contextualisation de l'enquête.....89

Annexe 3 : Résultats de l'enquête..... 92

Introduction

« Sentinelles de veille et éveilleurs de conscience, whistleblowers et lanceurs d'alerte appartiennent définitivement à la même famille. Ni guetteurs de l'apocalypse, ni prophètes de malheur, ils proposent une alternative au silence, font émerger une nouvelle forme de citoyenneté. » (Florence Hartmann dans *Lanceurs d'alerte : les mauvaises consciences de nos démocraties*).

La loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite aussi Loi Sapin II, a créé un statut général et protecteur des lanceurs d'alerte. Il est ainsi pertinent de s'intéresser aux apports de cette loi et aux risques associés.

La loi Sapin II, et notamment les lanceurs d'alerte, est un thème traité en Master 2 Audit Interne des Organisations à l'IAE d'Aix-en-Provence. L'intervention de Mme Tuloup en avril 2018 lors d'une conférence sur la fraude, a soulevé des questionnements qui m'ont interpellés et ont piqué mon intérêt face aux différentes polémiques en France sur ce sujet : Panama Papers, LuxLeaks ou plus récemment les abattoirs en France.

La loi Sapin II définit le lanceur d'alerte comme « une personne physique qui révèle ou signale, de manière désintéressée et de bonne foi, un crime ou un délit, une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice graves pour l'intérêt général, dont elle a eu personnellement connaissance, [...], les signalement relatifs aux manquements au code de conduite anti-corruption et anti-trafic d'influence.»

Aux États-Unis, on parle de Whistleblower, il est défini comme une personne, généralement un employé d'une agence gouvernementale ou d'une entreprise privée, qui divulgue, au public ou à des personnes en situation d'autorité, des situations de mauvaise gestion, de corruption, d'illégalité ou de tout autre acte répréhensible.

Ces deux définitions sont proches pourtant il y a une différence dans la perception du concept. Le Whistleblower en Amérique répond à une tradition politique ancrée dans le « noyau

dur » de la démocratie américaine alors qu'en France l'introduction du concept est plus récente et suscite de nombreux débats.

La frontière entre d'une part, l'éthique et la transparence et, d'autre part, la dénonciation mensongère, médisante ou imprudente, peut parfois être très mince. Compte tenu de son positionnement et de la transversalité de ses missions, la fonction d'audit interne a un rôle important dans le contrôle des dispositifs de recueil des signalements et de la conformité de l'entité à la loi Sapin 2.

Comment a évolué le concept de lanceurs d'alerte en France et quels sont les risques liés aux dispositifs de recueil des signalements ?

Afin de traiter le sujet et de répondre aux questionnements émis, un plan de recherche a été établi. Il consiste tout d'abord en un questionnaire posté en ligne et disponible pendant deux semaines puis à un benchmark réalisé auprès de six entreprises. Cette recherche empirique a été complétée par de nombreuses lectures sur le sujet.

L'objectif de ce mémoire est d'une part de comprendre comment le concept de lanceurs d'alerte est apparu et s'est développé en France et quels sont les risques associés, et d'autre part de mettre à disposition un guide d'audit des dispositifs de recueil d'alertes.

Nous verrons dans un premier temps les différences entre Whistleblower et lanceurs d'alerte, le contenu de la loi Sapin II ainsi qu'un état des lieux sur les dispositions mises en place par les entreprises aujourd'hui (Partie 1). Nous verrons dans un second temps que les dispositifs permettant le recueil des alertes ne sont pas sans risques (Partie 2), avant de terminer par un guide d'audit des dispositifs d'alerte interne et de recueil des signalements (Partie 3).

PARTIE 1 : LE CONCEPT DE « LANCEURS D'ALERTE » : DE L'ORIGINE AUX ETATS-UNIS A LA MISE EN PLACE EN FRANCE DEPUIS LA LOI SAPIN II

I- Évolution du concept : du Whistleblowing aux lanceurs d'alerte

A. Naissance du concept aux États-Unis

C'est aux États-Unis que le concept apparaît pour la première fois. Les lanceurs d'alerte existent dès la guerre de Sécession : ce sont ceux qui dénoncent alors la corruption. Le 2 mars 1863, émerge la première loi protectrice des lanceurs d'alerte par le « False Claims Act » (FCA). Le congrès des États-Unis avait promulgué cette loi pour lutter contre la corruption militaire et la fraude. Ce texte se proposait de permettre à chaque citoyen d'engager une action contre une entreprise ou un sous-traitant de l'armée américaine, au nom de l'État, en étant ainsi récompensé par un pourcentage du montant de l'amende perçue[1].

C'est en 1972 que le terme « Whistleblower » est employé pour la première fois. Cette expression désignait à l'origine les policiers soufflant (« blow ») dans leur sifflet (« whistle ») pour, à la fois, alerter les citoyens d'un danger et appeler les forces de l'ordre. C'est Ralph Nader[2], dans son livre « Whistle Blowing », qui utilise pour la première fois l'expression « Whistleblower » pour désigner le lanceur d'alerte. Il le définit comme celui qui reporte un crime réel ou supposé de son employeur, l'expression devient dès lors populaire, tout comme les whistleblowers eux-mêmes. Ce succès est dû en partie à l'encouragement de certaines associations comme *Governement Accountability Project*[3] (GAP) créé en 1977.

Suite à de nombreuses affaires, relayées par de nombreux débats médiatiques, un arsenal législatif s'est développé. Le FCA est codifié en 1986 puis modifié en 2009 par le *Fraud Enforcement and Recovery Act* et par le *Patient Protection and Affordable Care Act* de 2010. Son but est de contribuer à la réduction de la criminalité financière en encourageant les actions des lanceurs d'alerte en particulier dans le domaine de la fraude. D'autres textes se distinguent, notamment le *Whistle Protection Act* datant de 1989, renforcé en 2000 par le *No-fear Act*, puis en 2012 par le *Whistleblower Protection Enhancement Act*. Cette loi, qui concerne les salariés

[1] Mécanisme du « Quitam », littéralement « qui tam pro domino rege quam pro se ipso in hac parte sequitu », apparu en Angleterre au XVe siècle, permet à des personnes physiques d'engager une action contre un tiers au nom de l'État en étant récompensé par une partie du montant de l'amende perçue.
[2] Ralph Nader, né en 1934, est un avocat et politicien américain, célèbre par ses campagnes en faveur des droits des consommateurs dès les années 1960 avec l'association Public Citizen.
[3] Le *Government Accountability Project* est un organisme de protection et de défense des dénonciateurs aux États-Unis.

du secteur public, a pour objectif de défendre toute personne apportant la preuve d'« une infraction à une loi, à une règle ou à un règlement » ou encore d' « une mauvaise gestion évidente, d'un flagrant gaspillage de fonds, d'un abus de pouvoir ou d'un danger significatif et spécifique en ce qui a trait à la santé et à la sécurité du public ».

Dans le domaine de la corruption, c'est le *Foreign Corrupt Practices Act* (FCPA), datant de 1977, qui est le texte de référence aux États-Unis. C'est une loi fédérale américaine qui a pour but de lutter contre la corruption d'agents publics à l'étranger. Elle a un impact international, on parle d'extraterritorialité. Cette loi touche toutes les entreprises de n'importe quel secteur et de n'importe quelle nationalité.

En 2002, après l'éclatement de la bulle spéculative et des scandales qui s'en sont suivis (Enron ou WorldCom), le Parlement américain a adopté la loi « Sarbanes-Oxley », dite aussi loi SOX, pour intensifier la répression contre les fraudes comptables. Elle est guidée par trois grands principes : l'exactitude et l'accessibilité de l'information, la responsabilité des gestionnaires et l'indépendance des organes vérificateurs. Cette loi contraint les sociétés françaises cotées aux États-Unis, ainsi que les filiales en France de sociétés cotées aux États-Unis, de mettre en place un dispositif d'alerte professionnelle. C'est la première apparition en France du concept de Whistleblowing.

B. L'introduction récente en France

En France, l'introduction récente du concept, s'est faite de manière plus laborieuse, suscitant de nombreuses controverses.

La question des lanceurs d'alerte scientifiques, en lien avec les crises sanitaires des vingt dernières années, a constitué la « porte d'entrée » de la réflexion sur les lanceurs d'alerte en France. C'est Francis Chateauraynaud et Didier Torny, deux sociologues, en 1999, qui utilisent pour la première fois le terme de « lanceur d'alerte », dans leur livre *Les sombres précurseurs : une sociologie pragmatique de l'alerte et du risque*. Nonobstant, les porteurs d'alerte ne sont pas directement liés au monde des affaires ou aux sciences de gestion mais le concept est plus large et constitue une réflexion critique sur les risques technologiques, sanitaires ou encore environnementaux et sur leur prévention. A cette époque-là, la maladie de la vache folle, les dangers de l'amiante, les fuites de gaz toxiques à Bhopal, l'explosion du réacteur de Tchernobyl, l'apparition brutale du sida ou encore l'affaire du sang contaminé, entrainent le

développement d'organismes de vigilance comme Greenpeace qui multiplie les alarmes. Des chercheurs mais aussi de simples citoyens dénoncent l'aveuglement des administrations et les conflits d'intérêts. C'est ici que naît l'idée de les nommer les « lanceurs d'alerte ».

En 2007, à l'occasion du Grenelle de l'environnement, différentes associations proposent un statut juridique pour les lanceurs d'alerte. Une loi est actée sur ce sujet. Un an plus tard, la mission Corinne Lepage, chargée de traduire juridiquement les axes prévus par le Grenelle de l'environnement dans le domaine de la gouvernance écologique, intègre la réflexion sur la protection juridique des lanceurs d'alerte.

Le lanceur d'alerte traîne avant de se détacher du champ social et sanitaire pour arriver progressivement sur le terrain de l'entreprise et de la gestion. La situation est identique pour le cadre légal en France qui tarde à se libérer de cet aspect sanitaire jusqu'en 2013. Pendant quinze ans l'essentiel des alertes concerne des enjeux scientifiques.

Au fil des années, les lanceurs d'alerte ont gagné d'autres domaines et ont émergé dans la sphère de l'éthique politique jusqu'à l'anti-corruption. En 2006, le lancement d'alerte voit sa définition mise à jour dans le dictionnaire terminologique québécois. Celle-ci devient : « la communication par un salarié ou un contractuel de l'entité à des autorités, internes ou externes, de ses soupçons concernant un cas de fraude, d'irrégularité ou de mauvaise gestion délibérée de la part d'une personne ou d'un groupe dans l'entité ». La notion de mauvaise gestion comme acte délibéré fait ainsi passer le concept dans les sciences de gestion en français.

Au-delà de la question des lanceurs d'alerte scientifiques la relation entretenue par la France avec ses lanceurs d'alerte est restée pendant longtemps conflictuelle. Ces derniers étant vus comme de simples délateurs. De fait, les débuts de l'introduction du concept en France, notamment par la modification des chartes d'entreprises, ont suscité d'importantes polémiques.

L'expression « lanceurs d'alerte » n'est pas la traduction de Whistleblower, ce dernier étant traditionnellement plus lié à la dénonciation d'illégalités ou d'injustices. Le lanceur d'alerte a d'abord été « conçu comme celui ou celle qui se donne pour but de signaler un danger ou un risque, afin de l'éviter en interpellant les pouvoirs en place et en suscitant la prise de conscience de ses contemporains »[4]. D'autres éléments montrent la distinction entre les concepts français et américain. Notamment, l'aspect « récompense » à laquelle les lanceurs d'alerte ont droit aux États-Unis. En effet, en 2007, le Whistleblower Office a été créé afin de

[4] F. Chateauraynaud & D. Torny, Les Sombres précurseurs, op. cit. p. 32-37de l'édition de 2013.

récompenser les dénonciateurs de fraudes fiscales en leur garantissant 30% des montants récupérés grâce à leurs informations.

En France, les réticences semblent être en partie surmontées depuis et la divergence entre « lanceur d'alerte » et « Whistleblower » se réduit. En démontre le vote de sept lois depuis 2008 en faveur des lanceurs d'alerte.

Et ailleurs ?

Au Royaume Uni, c'est l'UK Bribery Act qui est relatif à la prévention de la corruption. Cette loi britannique, adoptée le 8 avril 2010 et entrée en vigueur le 1er juillet 2011, est considérée comme la plus sévère au monde en matière de lutte contre la corruption en entreprise. Elle vise la corruption active, la corruption passive, la corruption active d'agent public étranger et le défaut de prévention de la corruption par les entreprises. C'est la première loi qui pénalise l'éventuel absence d'efforts de prévention par les entreprises, de plus, par une sanction « illimitée ».

Ainsi, elle se différencie de la FCA en condamnant la corruption passive et en ayant une portée extraterritoriale plus large puisqu'elle vise les entités commerciales étrangères ayant une filiale au Royaume-Uni ou y entretenant des liens commerciaux.

Fig. 1 : Focus UKBA

II- Loi Sapin II : apports et mise en conformité

A. Le contenu de la loi

L'accessibilité des informations et des données, la diversification des sources d'information, le développement des réseaux sociaux, cumulés à l'avènement des exigences de sincérité, ont conduit à la multiplication des lanceurs d'alerte. Les internautes dévoilent de plus en plus d'informations confidentielles et sensibles sur les réseaux dans une volonté de démarche citoyenne. Les secrets, mêmes les plus protégés ne sont plus à l'abri d'une divulgation. Le Législateur a donc d'abord essayé d'encadrer les actions de ces lanceurs d'alerte par quelques éléments dans différents textes.

Dans la sphère financière, le sujet des alertes n'est pas méconnu. Déjà, l'arrêté du 3 novembre 2014 relatif au contrôle interne[5], prévoit la faculté d'alerte « pour tout dirigeant ou

[5] Arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution.

préposé de faire part d'interrogations sur d'éventuels dysfonctionnements, au responsable de la conformité […] ». D'autres textes existent, parmi lesquels il est possible de citer le règlement relatif aux abus de marché (MAR) qui lui inclut le dispositif de signalement sur un périmètre plus restreint : l'intégrité des marchés. Ce règlement MAR indique qu'il convient « d'établir des systèmes et des procédures efficaces de détection et de notification des transactions suspectes » et permet déjà aux informateurs de porter des informations à l'attention des autorités compétentes dans le but d'infliger des sanctions. Malgré son existence, le dispositif de signalement ne fonctionne pas de manière optimale, d'où l'utilité d'une loi qui en renforce certains aspects et qui décline le dispositif sur l'ensemble des secteurs d'activité, ne se limitant plus au secteur financier.

Pour faire face à la multiplication des scandales comme celui du Médiator, des Panama Papers, du LuxLeaks, ou plus récemment des abattoirs en France, dont les révélations sont à l'origine de lanceurs d'alerte, la Loi Sapin 2 renforce leur protection. Cette loi constitue un véritable progrès en matière de lancement d'alerte, elle définit le lanceur d'alerte, institue une procédure de signalement et accorde un régime de protection commun.

La loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, est aussi dite loi Sapin 2. Elle compte 169 articles et a nécessité 43 ordonnances et 20 décrets d'application. Elle couvre un champ très vaste allant du droit bancaire au droit des sociétés en passant par des sujets plus transversaux ou institutionnels.

Elle est composée de 3 volets qui sont ses trois objectifs principaux : renforcer la transparence, mieux lutter contre la corruption et moderniser la vie économique. A chaque volet sont associées des mesures phares (voir figure ci-dessous).

Renforcer la transparence	Lutter contre la corruption	Moderniser la vie économique
• Création d'un répertoire numérique public des représentants d'intérêts auprès des personnes publiques ; • **Création d'un statut plus protecteur pour les lanceurs d'alerte**.	• **Création d'une agence française anticorruption ;** • **Mise en place d'un dispositif de prévention de la corruption pour les grandes entreprises ;** • **Création d'une peine complémentaire de mise en conformité des procédures de prévention et de détection de la corruption pour les entreprises ;** • Instauration d'une convention judiciaire d'intérêt public ; • Faciliter la poursuite des faits de corruption d'un agent public étranger.	• Interdiction de la publicité pour les sites de trading sur instruments risqués ; • Faciliter l'accès à de nouvelles sources de financement pour les entreprises et les projets d'infrastructure ; • Mobiliser davantage l'épargne des français vers le financement d'entreprises sociales et solidaires ; • Permettre aux épargnants modestes de débloquer leur plan d'épargne retraite complémentaire (PERP) ; • Mieux encadrer la rémunération des dirigeants d'entreprise.

Fig. 2 : Mesures phares des trois volets qui composent la loi dite « Sapin 2 »[6]

Pour être en conformité avec les grandes lignes de la loi et répondre à leurs obligations de vigilance, les entreprises devront mettre en place huit mesures opérationnelles, appelées les huit « piliers » :

1. Un code de conduite

- Il définit et illustre les différents types de comportements à proscrire comme étant susceptibles de désigner des situations de trafic d'influence ou de corruption.

2. Un dispositif d'alerte interne

- Il doit permettre de recueillir des signalements d'employés relatifs à l'existence de conduites ou de situations contraires au code de bonne conduite de l'entreprise.

3. Une cartographie des risques

- Elle identifie, analyse et hiérarchise les risques de corruption.

4. Des procédures d'évaluation

- De la situation des clients, fournisseurs de premier rang et intermédiaires au regard de la cartographie des risques

[6] Fait à partir du site www.economie.gouv.fr, le portail de l'Économie, des Finances, de l'Action et des Comptes publics.

5. Des procédures de contrôles comptables, internes ou externes

- Pour s'assurer que les livres, registres et comptes ne sont pas utilisés pour masquer des faits de corruption ou de trafic d'influence.

6. Un dispositif de formation

- A l'attention des cadres et des personnes les plus exposées aux risques de corruption et de trafic d'influence.

7. Un régime disciplinaire

- Qui prévoit des sanctions pour les salariés de la société en cas de violation du code de conduite (avertissement, blâme, suspension, etc.)

8. Un dispositif de contrôle et d'évaluatoin interne des mesures mises en oeuvre

- Pour vérifier régulièrement que les procédures internes sont effectivement appliquées. Cette fonction pouvant être exercée en interne comme être externalisée.

Fig. 3 : Les huit piliers de la Loi Sapin 2[7]

La mise en œuvre de ces huit obligations est contrôlée. La loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, a créé l'AFA, Agence Française Anticorruption. C'est un service à compétence nationale placé auprès du ministre de la Justice et du ministre chargé du Budget. La mission principale de l'AFA est d'aider les autorités compétentes et les personnes qui y sont confrontées à prévenir et à détecter les faits de corruption, trafic d'influence, concussion, prise illégale d'intérêt et détournement de fonds publics et favoritisme. Au-delà de cette mission de conseil et d'assistance, l'AFA a aussi une mission de contrôle qui porte sur le respect des huit obligations imposées par l'article 17 de la loi (les 8 piliers de la Loi Sapin II). Elle contrôle la qualité des procédures mises en œuvre pour lutter contre les atteintes à la probité et l'exécution des mesures judiciaires. En cas de défaillance dans la mise en œuvre de ces huit obligations, le directeur de l'AFA communique le rapport de son contrôle à la personne et la met en demeure de présenter ses observations écrites dans un délai de deux mois. Après ce délai, il peut décider de délivrer un avertissement ou de saisir la commission des sanctions[8]. La commission des sanctions peut donner un délai inférieur à trois ans à l'organisation pour adapter ses procédures

[7] Réalisé à partir des données disponibles sur www.portail.arca.fr, cabinet de conseil en gestion des risques.
[8] La commission des sanctions fait partie de l'AFA, elle est composée de six membres : deux conseillers d'État désignés par le vice-président du Conseil d'État, deux conseillers à la Cour de cassation désignés par le premier président de la Cour de cassation et deux conseillers maîtres à la Cour des comptes désignés par le premier président de la Cour des comptes.

ou prononcer une sanction pécuniaire d'un montant inférieur ou égal à 200 000 euros pour les personnes physiques et inférieur ou égal à un million d'euros pour les personnes morales.

Focus sur les dispositifs de recueil des alertes

La loi Sapin II impose aux entreprises concernées de mettre en place des dispositifs d'alerte professionnelle. A travers les articles 8 et 17 elle instaure deux types de dispositifs : un dit « général » et le second spécifique à la lutte anti-corruption.

L'article 8 impose la mise en place d'une procédure de recueil des signalements qui vise tous « les crimes, les délits, les violations graves et manifestes d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice grave pour l'intérêt général ». Cela concerne « les personnes morales de droit public ou de droit privé employant au moins cinquante salariés, les administrations de l'État, les communes de plus de 10 000 habitants ainsi que les établissements publics de coopération intercommunale à fiscalité propre dont elles sont membres, départements et les régions, dans des conditions fixées par décret en Conseil d'État ». Ce dispositif de recueil des signalements est obligatoire depuis le 1er janvier 2018.

L'article 17, impose, depuis le 1er juin 2017, la mise en place d'un dispositif d'alerte interne, plus spécifique, il doit permettre le recueil des signalements émanant des salariés relatifs aux manquements au code de conduite anti-corruption et anti-trafic d'influence. Il concerne les sociétés qui emploient au moins cinq cents salariés ou qui appartiennent à un groupe dont la société mère a un chiffre d'affaires supérieur à cent millions d'euros et un siège social en France.

La corruption est définie comme « un comportement pénalement répréhensible par lequel une personne (le corrompu) sollicite, agrée ou accepte un don, une offre ou une promesse, des présents ou des avantages quelconques en vue d'accomplir, de retarder ou d'omettre d'accomplir un acte entrant d'une façon directe ou indirecte dans le cadre de ses fonctions.[9] ».

[9] Définition donnée par le site Droit-finances.

Le trafic d'influence « désigne le fait pour une personne de recevoir ou de solliciter des dons dans le but d'abuser de son influence, réelle ou supposée, sur un tiers afin qu'il prenne une décision favorable. [10]»

La loi donne la possibilité aux entreprises de mettre en place un seul et unique dispositif technique de recueil des deux types de signalement présentés par les articles 8 et 17. Ce dispositif pourra aussi porter sur toute autre violation des principes et règles éthiques, RSE et déontologiques de l'entreprise.

Ainsi, la mise en place de ce dispositif, relatif au pilier 2 de la loi Sapin 2 doit entretenir une forte relation avec le pilier 1 : la rédaction du code de conduite, notamment pour le recueil des signalements faits par les employés relatifs aux violations du code de conduite.

Le code de conduite : point de départ de la mise en conformité

Depuis le 1er juin 2017, les entreprises doivent mettre en œuvre *"Un code de conduite définissant et illustrant les différents types de comportements à proscrire comme étant susceptibles de caractériser des faits de corruption ou de trafic d'influence. Ce code de conduite devra être intégré au règlement intérieur de l'entreprise et faire l'objet, à ce titre, de la procédure de consultation des représentants du personnel prévue à l'article L. 1321-4 du Code du travail."* Il doit permettre de prévenir, de détecter et de sanctionner les faits de corruption et de trafic d'influence. Il doit définir toutes les formes de corruption et de trafic d'influence et notamment distinguer les délits passifs et actifs. Il doit établir les pratiques interdites et autorisées.

Fig. 4 : Le code de conduite

Après avoir élargi le domaine des alertes pouvant être remontées par les dispositifs, la loi, et plus particulièrement l'article 8, élargi aussi le périmètre des lanceurs d'alerte potentiels. Avant cette loi, seuls les salariés des établissements étaient concernés, l'objectif était d'alerter son employeur contre les dérives présentent au sein de son entreprise. Puis, devant la multiplication des fuites, le Conseil des Ministres du Conseil de l'Europe adopte une recommandation qui vise à protéger le lanceur d'alerte et à élargir le concept. De fait, à partir du 1er janvier 2018 les salariés mais aussi les collaborateurs externes et occasionnels pourront émettre une alerte ; il s'agit des intérimaires, des alternants, des stagiaires, et des prestataires / fournisseurs de premier rang.

[10] Définition donnée par le site Transparency International France.

La loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique permet de caractériser le lanceur d'alerte avec cinq particularités additionnelles :

Fig. 5 : Les caractéristiques du lanceur d'alertes

Le lanceur d'alerte est une personne physique. De fait, les personnes morales (association, syndicat professionnel, etc.) sont exclues du champ d'application de la loi Sapin II et ne sont pas considérées comme lanceurs d'alerte potentiels. La personne qui lance une alerte a personnellement constaté les informations qu'elle signale, elle ne remonte pas des éléments découverts par une autre personne. Le lanceur d'alerte agit de bonne foi et de manière désintéressée. C'est-à-dire, qu'il ne doit pas chercher à nuire à autrui et qu'à l'inverse de la loi américaine, il n'est pas rémunéré et ne bénéficie d'aucun avantage pour avoir effectué un signalement. Ce qui écarte la possibilité d'émettre une alerte dans son propre intérêt. Enfin, le lanceur d'alerte révèle des faits qualifiés de graves.

L'apport majeur de la loi Sapin 2 est la création d'un statut juridique unique applicable aux lanceurs d'alerte qui bénéficient désormais d'un socle commun de protection alors que cohabitaient jusqu'à présent des dispositions différentes dispersées dans divers textes. De manière générale, le lanceur d'alerte ne pourra pas faire l'objet de mesures disciplinaires ou discriminatoires dans la mesure où il agit de bonne foi et même si les faits se révèlent être infondés. Ainsi, il ne pourra pas : être sanctionné, licencié, ou faire l'objet d'une mesure discriminatoire directe ou indirecte touchant sa rémunération, sa qualification ou encore la promotion professionnelle. Il ne peut pas non plus être écarté d'une procédure de recrutement

ou d'une formation professionnelle. La loi n°2016-1691 du 9 décembre 2016, dite loi Sapin 2 ajoute que les lanceurs d'alerte sont exonérés de la responsabilité pénale lorsqu'ils portent atteinte à un secret protégé par la loi.

En outre, la loi n°2016-1690 du 9 décembre 2016 concernant les dispositions relatives aux compétences et à la saisine du Défenseur des droits, qui modifie la version en vigueur au 11 décembre 2011, définit les rôles du Défenseur des droits, notamment ceux liés aux lanceurs d'alerte. De fait, il est chargé « d'orienter vers les autorités compétentes toute personne signalant une alerte dans les conditions fixées par la loi » et « de veiller aux droits et libertés de cette personne ».

Pour pouvoir bénéficier de la protection mise en place par la loi et afin de préserver ses intérêts et ceux de l'entreprise, le lanceur d'alerte devra respecter une certaine gradation dans l'émission de son alerte. La procédure de signalement se décompose en trois paliers. Dans un premier temps, l'alerte doit être portée à la connaissance d'un supérieur hiérarchique, de l'employeur ou du référent désigné par ce dernier. Si, dans un délai raisonnable, le lanceur d'alerte ne perçoit aucune suite donnée à son signalement, il peut saisir l'autorité judiciaire, l'autorité administrative ou l'ordre professionnel concerné. Si, dans un délai de trois mois, le signalement n'est toujours pas traité, il peut, en dernier recours, avertir l'opinion publique. Néanmoins, « en cas de danger grave et imminent ou en présence d'un risque de dommages irréversibles » le signalement pourra directement être adressé au deuxième palier, c'est-à-dire à l'autorité judiciaire, l'autorité administrative ou aux ordres professionnels. Il peut aussi être rendu public. C'est ce que la loi appelle « procédure d'urgence de signalement d'alertes ». Il est aussi admis que l'alerte soit portée directement au deuxième palier si c'est la direction que le lanceur d'alerte met en cause.

Le passage d'un niveau à l'autre doit respecter la stricte confidentialité de l'identité du lanceur d'alerte, des faits signalés ainsi que de l'identité de la personne visée par l'alerte. Il faudra être vigilant lorsque les vérifications ou lorsque le traitement nécessite la communication avec des tiers, notamment lors de réunion de documents ou de preuves. Il est important de mettre en place des dispositifs sécurisés et opérationnels pour protéger la confidentialité, élément majeur attendu par les dispositions de la loi Sapin II. Les entreprises devront s'assurer que les canaux de signalement mis en place comprennent des garanties de confidentialité absolue. En cas de divulgation de l'identité du lanceur d'alerte la sanction encourue est deux ans d'emprisonnement et 30 000€ d'amende.

La confidentialité imposée par le texte est à distinguer de l'anonymat de l'alerte. La loi Sapin II n'impose pas le recueil d'alertes anonymes mais elles peuvent difficilement être évitées, il convient donc que le dispositif permette leur collecte.

Le texte de loi prévoit aussi des sanctions pénales en cas d'agissement contraire aux règles prévues. Si l'employeur fait volontairement obstacle à la transmission d'un signalement au référent ou autre personne et organisme visé par la loi, il risque un an d'emprisonnement et 15 000€ d'amende. En cas de plainte en diffamation contre un lanceur d'alerte et constitution de partie civile abusive ou dilatoire l'amende civile peut être portée à 30 000€.

Suite aux dispositions émises par la loi du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, la Commission Nationale de l'Informatique et des Libertés (CNIL) a modifié son autorisation unique n°AU-004, le 22 juin 2017[11]. Avant la loi Sapin 2, l'autorisation unique n°AU-004 - nécessaire pour mettre en place un dispositif d'alerte professionnel - était complexe à obtenir. Sans fondement légal de droit français, la CNIL considérait ces dispositifs comme des systèmes de délation organisée et était particulièrement vigilante à l'égard de leur mise en place. C'est pour cela qu'en 2005, elle adopta l'Autorisation Unique n°AU-004, afin de fixer les conditions dans lesquelles ces dispositifs étaient autorisés du point de vue de la protection des données personnelles. Initialement, l'AU-004 était limitée à des secteurs particuliers : la finance, la comptabilité, la banque, la lutte contre la corruption, puis a été étendue aux pratiques anticoncurrentielles et enfin aux faits de discrimination et de harcèlement sur le lieu de travail, à la santé, l'hygiène, la sécurité au travail et aux problématiques environnementales. Avec la loi Sapin II, texte de droit français considéré comme fondement légal, la CNIL modifie le 22 juin 2017 son autorisation unique. Elle étend son champ d'application pour couvrir tous les dispositifs visant à recueillir les signalements ou révélations cités dans les articles 8 et 17 de la loi Sapin 2.

L'AU-004 du 22 juin 2017 définit les secteurs d'activité exclus du champ (il s'agit des informations qui relèvent du secret médical, du secret défense nationale ou du secret des relations entre un avocat et son client), les responsables de traitement concernés, les objectifs poursuivis par le traitement, les données personnelles concernées (voir Annexe 1), la durée de conservation des données, les destinataires des données, l'information des personnes, et les

[11] La délibération n°2017-191 du 22 juin 2017 portant sur l'autorisation unique de traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle, modifie la délibération n°2005-305 du 8 décembre 2005.

précautions à prendre en matière de sécurité. En cas d'infraction à la loi informatique et libertés, les organismes qui seront considérés comme non conformes à l'AU-004 seront soumis à des sanctions de la CNIL. Le responsable de traitement encours des peines pouvant aller jusqu'à cinq ans d'emprisonnement et 3 000 000 d'euros d'amende pour la personne morale.

B. La mise en place des dispositifs de recueil des alertes

Pour l'application de la règlementation, l'entreprise pourra décider d'externaliser la procédure de recueillement d'alerte ou de procéder à sa mise en œuvre en interne.

Si l'entreprise décide d'externaliser le dispositif, elle fera appel à un prestataire qui pourra mettre à sa disposition une plateforme de traitement des alertes et être en charge du filtrage de premier niveau. Il pourra même accompagner l'adoption du dispositif d'un point de vue social et mener des investigations nécessaires au traitement des cas les plus complexes. Il conviendra d'être particulièrement vigilant lors de la remontée des alertes du prestataire qui effectue le premier filtrage vers l'entreprise qui en assure le traitement, ce transfert devra être encadré pour assurer la confidentialité des données. Des clauses contractuelles devront être rédigées auprès de ces prestataires quant aux aspects relatifs aux données à caractère personnel. Les cabinets de conseil proposent désormais cette assistance en alliance avec leur société d'avocats. Leur multitude de compétences notamment en risk management, conformité ou encore droit social ainsi que leur présence dans le monde entier font d'eux des acteurs majeurs dans l'externalisation du dispositif. Le principal bénéfice d'une externalisation est que les collaborateurs s'adressent à un interlocuteur extérieur à leur société et cela diminue leurs craintes notamment en termes de confidentialité et de représailles.

Les établissements peuvent aussi faire le choix d'internaliser le système de recueil des signalements. Ils devront commencer par désigner un référent qui sera chargé de recueillir les alertes. Sa désignation doit être faite par la direction de l'entreprise et il doit avoir les compétences, l'autorité et les moyens suffisants pour traiter l'alerte. Dans les structures de grandes tailles il pourra s'agir du déontologue, du secrétaire général, du directeur éthique ou du directeur juridique.

Dans un second temps, les organisations devront mettre en place des canaux de remontées adéquats. Plusieurs options sont envisageables, il pourra s'agir d'une plate-forme web, d'une

adresse mail spécifique, d'une hotline, d'une adresse courrier ou d'un fax. Cette mise en place doit se faire en étroite concertation avec les instances représentatives du personnel pour qu'elles comprennent et soutiennent le contenu et les modalités du dispositif. Si l'entreprise décide de mettre en place un système de traitement automatisé de données à caractère personnel, elle devra solliciter la CNIL afin d'obtenir l'autorisation. Pour ce faire, une fois que l'entreprise respecte en tout point le cadre défini dans l'autorisation unique 004, elle adresse à la CNIL une déclaration de conformité disponible sur le site de la CNIL. Lorsque le dispositif d'alerte professionnelle envisagé sort du cadre fixé par l'AU-004, notamment au regard du fondement juridique et du champ d'application, l'entreprise adresse à la CNIL un dossier complet de demande d'autorisation individuelle.

Concernant le traitement des alertes, l'analyse et l'enquête seront effectuées de manière à déterminer la réalité et la matérialité des faits rapportés. Les investigations sont menées en interne, avec, éventuellement, l'appui d'un support externe soumis aux mêmes règles de confidentialité.

Il est important d'informer clairement sur le dispositif l'ensemble des utilisateurs potentiels. Ils devront être sensibilisés sur les objectifs poursuivis, les domaines concernés par les signalements, le référent, le caractère facultatif du dispositif, l'absence de conséquence à l'égard des employés de la non utilisation du dispositif, etc. L'information peut être diffusée par tout moyen : communications écrites destinées à tous les collaborateurs, communications orales au cours de réunions à l'échelle de toute l'organisation, messages sur l'intranet et sur la page web du site de l'organisation, etc. Ces informations doivent être accessibles à tout moment à l'ensemble des collaborateurs, même extérieurs et occasionnels. Un véritable plan d'animation et de sensibilisation doit être déployé. Un plan de formation spécifique au dispositif devra être étendu à l'ensemble du personnel, dans l'idéal il prévoira des formations en présentiel pour les cadres et les personnes les plus exposées. Cette sensibilisation passe aussi par l'introduction dans les contrats avec les prestataires / fournisseurs d'une clause afin qu'ils puissent informer leurs propres collaborateurs de l'existence du dispositif chez leur client.

En matière d'information le référent a aussi un rôle important. Il doit informer dans les meilleurs délais le lanceur d'alerte : de la réception de son alerte et des suites données à son signalement ; ainsi que la personne visée par l'alerte : de données la concernant afin de lui permettre de

s'opposer à leur traitement[12]. Il doit aussi mettre en place un suivi qu'il reportera de manière régulière à la direction. Ce reporting présentera les faits signalés, le traitement des remontées, les suites des alertes, le suivi des actions de traitement et les pertes éventuelles. Les alertes remontées devront être exploitées et utilisées pour actualiser la cartographie des risques de corruption et ainsi éviter la réitération de ces comportements.

La cartographie des risques de corruption : autre pilier de la loi Sapin II

Depuis le 1er juin 2017, les entreprises doivent mettre en œuvre « *une cartographie des risques prenant la forme d'une documentation régulièrement actualisée et destinée à identifier, analyser et hiérarchiser les risques d'exposition de la société à des sollicitations externes aux fins de corruption, en fonction notamment des secteurs d'activité et des zones géographiques dans lesquels la société exerce son activité.* »

Fig. 6 : La cartographie des risques de corruption

Le règlement intérieur et les procédures internes de l'établissement devront être mis à jour afin d'intégrer les spécificités du nouveau dispositif. La loi Sapin II demande un enrichissement important et précis des procédures (cf. Guide d'audit - Partie 3).

Un des éléments majeurs sur lequel l'organisation doit s'attarder est la sécurité du dispositif, fondamentale pour garantir la confidentialité des données et ainsi répondre aux exigences de la CNIL. L'outil de remontée et de traitement des alertes doit être suffisamment sécurisé pour garantir l'accès seulement aux personnes autorisées. L'accès peut donc se faire via un identifiant et un mot de passe individuel, régulièrement renouvelé. Il faudra veiller à ce que les administrateurs "systèmes" qui ont accès à l'outil de traitement pour assurer sa maintenance n'aient pas accès aux alertes elles-mêmes. Pour assurer cette sécurité, il conviendra de protéger le S.I. du risque d'intrusions qu'elles soient internes ou externes.

D'une manière générale, les organisations assujetties à cette réforme devront intégrer l'ensemble des exigences issues de la loi Sapin 2 mais aussi les articuler avec les règlementations étrangères (Foreign Corrupt Practices Act, Sarbanes-Oxley, UK Bribery Act) et les autres textes spécifiques (exemple : règlement abus de marchés).

[12] Conformément aux articles 6 et 32 de la loi du 6 janvier 1978, la personne visée par l'alerte doit être informée des faits qui lui sont reprochés afin de pouvoir faire usage de ses droits, dont ses droits de la défense et le respect du principe contradictoire.

C. État des lieux : où en sont les entreprises dans leur mise en conformité ?

D'après une étude réalisée sur 60 personnes, dont 92% travaillant dans une entreprise de plus de 50 employés, voire 500 employés dans 78% des cas (voir Annexe 2), 65% des personnes interrogées n'ont pas connaissance de l'existence d'un dispositif d'alerte interne ou d'une procédure de recueil des signalements au sein de leur l'entreprise (voir Annexe 3). Ce pourcentage peut être la conséquence de deux tendances : deux entreprises sur trois n'ont pas encore mis à la disposition de leurs employés un dispositif de remontées ou l'entreprise n'a pas communiqué sur le dispositif.

Après avoir interrogé les directions conformité de trois banques, d'une entreprise d'habitat social, d'une entreprise de BTP et d'une entreprise de négoce dans l'outillage et le matériel pour professionnel, la tendance est claire : deux entreprises sur six ont aujourd'hui déployé le dispositif demandé par la loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique. Sur les quatre autres, trois sont en train de déployer le dispositif et ont déjà nommé un référent et une n'a pas commencé sa démarche de mise en conformité. Toutes les entreprises interrogées comptent plus de 500 salariés et sont donc, depuis le 1er juin 2017, dans l'obligation de mettre en place le dispositif d'alerte interne de lutte anti-corruption imposé par l'article 17[13] et depuis le 1er janvier 2018, la procédure de recueil des signalements imposée par l'article 8[14]. Ce retard dans la mise en conformité des entreprises peut s'expliquer par le fait que la loi n'a pas encore prévu de sanctions en cas de défaut de mise en œuvre de la procédure de recueil de signalement. Cependant, en n'instaurant pas de procédure d'alerte appropriée, les entreprises s'exposent au risque que les salariés dénoncent des faits via le troisième palier, à savoir en avertissant directement l'opinion publique.

[13] Pour rappel l'article 17 impose la mise en place d'un dispositif d'alerte interne permettant le recueil des signalements émanant des salariés relatifs aux manquements au code de conduite anti-corruption et anti-trafic d'influence.

[14] Pour rappel l'article 8 impose, aux entreprises de plus de 50 salariés, depuis le 1er janvier 2018, la mise en place une procédure de recueil des signalements qui vise tous « les crimes, les délits, les violations graves et manifestes d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice grave pour l'intérêt général » et celui ça doit être à la disposition des salariés mais aussi des collaborateurs externes et occasionnels.

Entreprise	**Nomination d'un référent**	**Mise en place d'un dispositif**	**Quel canal a été ou va être mis en place**	**Communication du dispositif à l'ensemble de l'entreprise**	**Conformité de l'entreprise avec la Loi Sapin II**
Banque 1	OUI	EN COURS	Mail + adresse postale + messagerie vocale + formulaire sur intranet	NA	NON
Banque 2	OUI	EN COURS	Mail	NA	NON
Banque 3	OUI	OUI	Mail + application smartphone	NON[15]	NON
Habitat social	OUI	EN COURS	Mail	NA	NON
BTP	NON	NON	Mail	NON	NON
Entreprise de négoce	OUI	OUI	Ligne téléphonique	OUI	OUI

Fig., 7 : Tableau de benchmark

Cependant, dans une société où la transparence prend de plus en plus d'importance, la recherche d'éthique est aussi une opportunité pour les organisations. Combattre des comportements de corruption – objectif de la loi Sapin II – permet aux entreprises de communiquer sur leurs valeurs. Au-delà d'une question d'image, les alertes permettent de prévenir et de lutter contre les abus au sein des entreprises (40% des fraudes sont révélées par des lanceurs d'alerte[16]) et, par la procédure de signalement en trois paliers, ces dispositifs empêchent que certaines informations ne soient rendues publiques et ne portent ainsi atteinte à l'image et à la réputation de l'entreprise.

Pour autant, ce type de dispositif ne correspond pas à la culture française, qui associe spontanément ces pratiques à de la délation et garde les stigmates d'une Histoire encore récente.

[15] L'entreprise a mis la procédure à disposition de l'ensemble des collaborateurs sur le site internet et l'intranet mais elle n'a pas communiqué dessus. Les collaborateurs interrogés ne sont pas au courant de son existence.
[16] Selon Transparency France.

PARTIE 2 : LES RISQUES ASSOCIES AUX DISPOSITIFS

I- Les risques liés à la règlementation et aux dispositifs

Depuis sa mise en place, la loi Sapin II n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique fait débat. Les opinions divergent et certains y associent de nombreux risques.

A. Les risques lors de la mise en place du dispositif

Premièrement, la mise en place de ces dispositifs peut s'avérer contraignante et couteuse pour l'entreprise. Elle nécessite une déclaration auprès de la CNIL, la consultation des instances représentatives du personnel, la modification du règlement intérieur ainsi qu'un plan de communication interne. Tant d'actions astreignantes, quand seulement pour modifier le règlement intérieur il faut consulter le Comité d'Hygiène, de Sécurité et des Conditions de Travail, consulter le Comité d'Entreprise, transmettre la nouvelle version en double exemplaire à l'Inspection du travail pour contrôle de légalité, le déposer au greffe du Conseil de prud'hommes et le communiquer à l'ensemble des salariés. En plus de la contrainte, c'est un réel coût financier pour les entreprises, particulièrement lorsqu'elles décident de faire intervenir un prestataire pour externaliser le dispositif. Ces prestataires se vantent d'utiliser des technologies de pointe pour assurer la sécurité et la confidentialité des informations, en moyenne leurs prestations s'élèvent à 4 500 euros par an pour une structure de 1 000 salariés. Au-delà du coût financier, l'externalisation de la procédure peut présenter d'autres inconvénients, notamment un mécanisme inadapté à la réalité de l'entreprise. L'externalisation peut aussi envoyer un mauvais signal aux salariés : la direction n'est pas impliquée et choisit la politique de l'autruche, d'autant plus si l'organisme extérieur n'a pas été choisi avec les instances représentatives du personnel. Toutefois, l'avantage d'un tel dispositif est sa neutralité qui peut diminuer les craintes des utilisateurs notamment celles relatives au respect de la confidentialité. Le traitement en interne peut aussi représenter un coût élevé, particulièrement pour les petites entreprises d'à peine plus de cinquante salariés qui manquent de moyens pratiques.

Une autre difficulté s'impose aux entreprises, qu'elles aient fait le choix d'internaliser ou d'externaliser le dispositif, elles devront nommer un référent. Même si elle ne semble pas l'être, cette tâche risque d'être délicate, car si la loi offre un cadre protecteur au lanceur d'alerte, la responsabilité pénale du référent peut être, au contraire, fortement engagée. En effet l'article 9

de la loi Sapin II prévoit des sanctions pénales lourdes si le référent ne respecte pas son obligation de stricte confidentialité, il encourt jusqu'à deux ans d'emprisonnement et 30 000 euros d'amende. Sa responsabilité pénale peut aussi être engagée s'il est considéré qu'il a fait obstacle à la transmission d'un signalement, il risque dans ce cas un an d'emprisonnement et 15 000 euros d'amende. Pour permettre au référent de prouver qu'il n'a pas fait obstacle à la transmission d'une alerte, la CNIL autorise l'archivage des données alors que le décret avait imposé leur destruction. Le risque de blocage dans la remontée de l'alerte peut aussi être à l'origine d'un référent malveillant. Voici toute la difficulté à nommer un référent qui dispose de la compétence, de l'autorité, de l'éthique et des moyens suffisants à l'exercice de ses missions.

B. Les risques techniques liés aux dispositifs

En fonction du canal de remontées choisit par l'entreprise des risques techniques y sont associés. Dans tous les cas il faudra être vigilant face au risque d'usurpation d'identité et de modification voire suppression des alertes, et ce, sur n'importe quel canal.

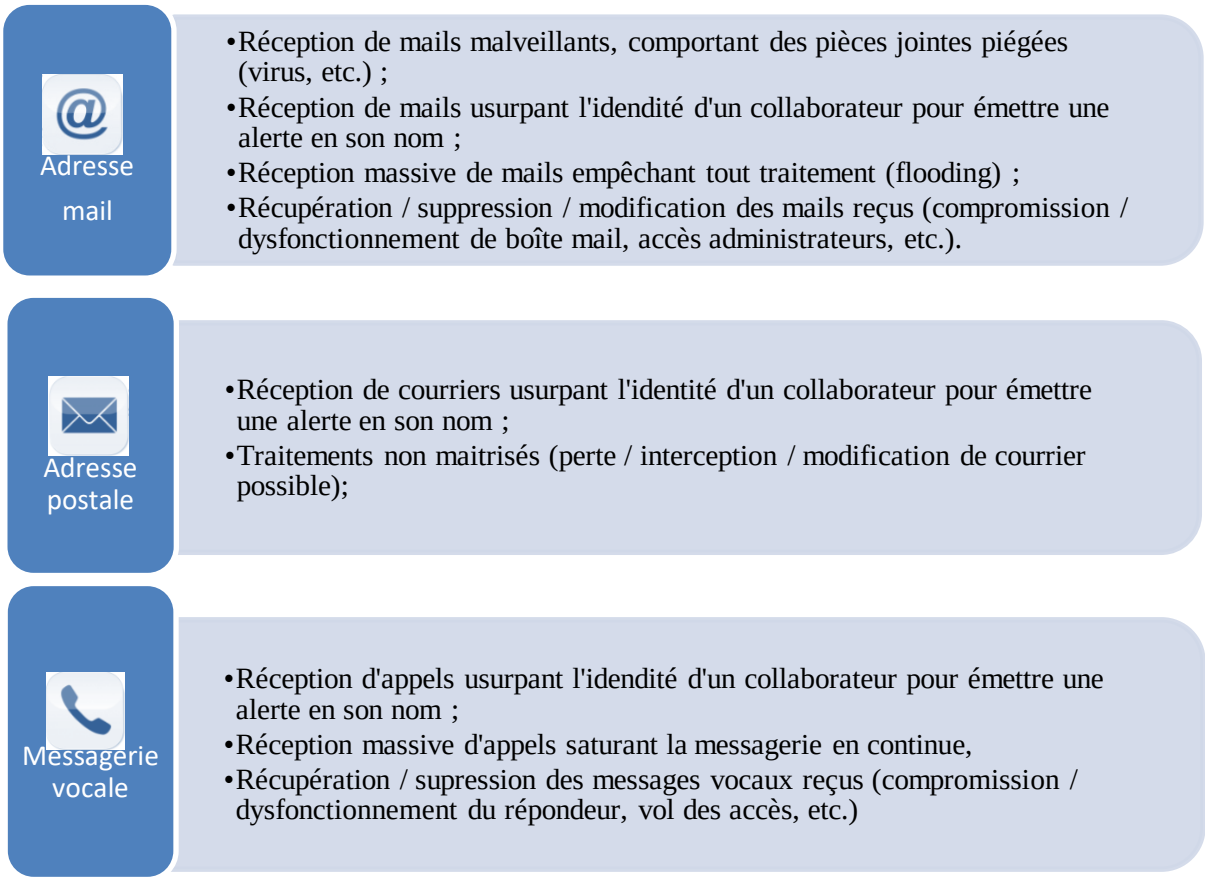


Fig. 8 : Risques associés aux canaux de remontées[17]

[17] Figure réalisée avec les informations récoltées par entretien avec le DSI du Crédit Agricole Alpes Provence.

L'organisation, et plus particulièrement le CISO[18] pourra prendre des mesures pour prévenir ces évènements redoutés. Si l'entreprise fait le choix d'une adresse mail, il conviendra d'utiliser une messagerie à accès très restreint qui dispose de mécanismes de filtrage et de nettoyage en amont[19]. Elle pourra aussi communiquer un alias et non l'adresse réelle de la messagerie. Un alias est un « mail de façade » qui redirige les mails reçus sur une boîte de messagerie. En cas d'attaque ou de ciblage malveillant, il suffira simplement de remplacer l'alias sans changer la messagerie. Fréquemment il faudra retirer les mails reçus et les déposer dans un environnement sécurisé par exemple en les exportant mensuellement dans un dossier ZIP chiffré et déposé sur un espace bureautique à accès restreint. Malgré ces mesures de précaution, deux risques resteront à assumer : la réception de mails comportant des pièces jointes piégées (car difficile à filtrer) et l'imputabilité des mails reçus (le mail n'étant pas signé il ne peut pas être totalement associé à l'expéditeur qui apparaît).

Si l'organisation décide de mettre en place une boite postale celle-ci devra être dédiée au dispositif avec un circuit de distribution « court ». C'est-à-dire qu'il y aura au maximum un intermédiaire entre le lanceur d'alerte et le référent. De la même manière, même si le courrier est signé, rien ne garantit qu'il soit associé à l'expéditeur, sauf si une copie d'une pièce d'identité est jointe à l'envoi.

Enfin, la messagerie vocale est un canal qui peut aussi être envisagé. Il faudra veiller à utiliser une messagerie vocale externe disposant d'une possibilité d'export des enregistrements afin de pouvoir les extraire fréquemment du répondeur et de les déposer dans un emplacement sécurisé (export mensuel dans un dossier zip chiffré et déposé sur un espace bureautique à accès restreint). Une fois de plus l'imputabilité des messages reçus n'est que partiellement garantie, une ligne téléphonique est un identifiant complexe à exploiter.

Le référent devra disposer d'un environnement sécurisé dans lequel seront conservés les codes d'accès et de paramétrage de la boîte mail et du répondeur. Il pourra s'agir d'un dossier zip chiffré ou d'un logiciel gestionnaire de mots de passe labellisé ANSSI[20].

---

[18] CISO en anglais : Chief information security officer, en français on parle de RSSI : Responsable de la sécurité des systèmes d'information. Il s'agit de l'expert qui garantit la sécurité, la disponibilité et l'intégrité du système d'information et des données.

[19] Le filtrage et le nettoyage de boîte mail sont des techniques qui permettent de réduire les courriers indésirables (spams).

[20] L'ANSSI est l'agence nationale de la sécurité des systèmes d'information, elle délivre des Visas de sécurité permettant d'identifier facilement les solutions de cybersécurité les plus fiables et reconnues comme telles à l'issue d'une évaluation réalisée par des laboratoires agréés selon une méthodologie rigoureuse (d'après le site officiel de l'ANSSI).

Ces dispositifs peuvent être à l'origine de dérives, notamment une utilisation abusive. En effet, un des risques majeurs serait l'émergence d'un système de délation, ce qui est redouté par 20% des collaborateurs interrogés. Des utilisateurs pourraient essayer de l'utiliser pour servir leurs propres intérêts notamment en signalant des informations calomnieuses. C'est pour limiter ces abus que l'article 9 de la loi Sapin II prévoit des sanctions et des poursuites judiciaires contre l'utilisation abusive ou malveillante du dispositif. Ainsi l'émission de faux signalements est punie de deux ans de prison et 30 000 euros d'amende. A savoir que si la réalité des faits signalés n'est pas avérée, le lanceur d'alerte n'est pas forcément considéré comme étant de mauvaise foi, il faudra prouver qu'il avait connaissance de la fausseté des faits dénoncés. La CNIL recommande fortement aux entreprises d'inciter ses collaborateurs à ne pas émettre d'alerte de manière anonyme afin de limiter le risque d'alerte abusive[21]. A l'inverse, une personne totalement désintéressée et de bonne foi pourra facilement être attaquée par la partie adverse. En effet la partie adverse aura tout loisir de mettre en avant des éléments prouvant que le lanceur d'alerte n'était ni désintéressé ni de bonne foi. Il pourra, par exemple, ressortir un ancien désaccord avec des collaborateurs. En Angleterre, où une règlementation sur le sujet existe depuis 1998, la notion de bonne foi a été supprimée en 2013, mettant en avant que le plus important était de savoir si les allégations étaient vraies ou fausses.

De plus, la loi Sapin II donne une nouvelle définition plus large du lanceur d'alerte et peut manquer de clarté. Notamment lorsqu'elle impose la mise en place d'une procédure de recueil des signalements pour viser une « menace ou un préjudice grave pour l'intérêt général ». Il revient au lanceur d'alerte d'apprécier de manière subjective si le fait dont il a été témoin est suffisamment grave pour être divulgué. C'est une appréciation personnelle et individuelle de l'intérêt général qui peut aboutir à des abus. Une somme d'intérêts particuliers risque de ne pas constituer un intérêt général. De fait, un salarié qui dénoncerait la façon illégale dont sont calculés les bonus dans son entreprise ne se verrait pas accorder la protection du lanceur d'alerte.

La difficulté d'obtenir le statut de lanceur d'alerte est un risque relevé par de nombreux avocats[22]. Après la notion de « désintéressé » vue précédemment, le fait que le lanceur d'alerte doive avoir eu « personnellement connaissance » des faits est une notion vague. La partie adverse pourra aisément trouver des arguments visant à refuser le statut. Autre notion vague

[21] Recommandation de la CNIL dans son avis du 22 juin 2017.
[22] Dont Patrick Thiébart, avocat en droit social et Tewfik Bouzenoune avocat en droit pénal général, de la presse, de la concurrence, des marchés publics, du travail.

dans la loi Sapin II : la situation de « danger grave et imminent » ou de « risque de dommages irréversibles ». Pour rappel, la loi prévoit une « procédure d'urgence de signalement d'alerte » dans les deux situations citées précédemment, le signalement pourra directement être adressé au deuxième palier c'est-à-dire à l'autorité judiciaire, l'autorité administrative ou aux ordres professionnels. Il peut aussi être rendu public. Il revient une fois de plus au lanceur d'alerte de juger personnellement de l'importance du fait qu'il signale. Cette notion pourra facilement être attaquée par l'avocat de la partie adversaire, comme ce fut le cas dans l'affaire ArcelorMittal. Le 29 juin un ancien sous-traitant du groupe révèle à la presse un scandale sanitaire et environnemental : le déversement d'acide à décaper l'acier usagé, dans une décharge à ciel ouvert, en pleine nature, proche des habitations. Après cette dénonciation, son contrat d'intérim arrive à son terme, il n'est pas renouvelé, sans explication, et plus aucune mission ne lui sera proposée. La loi Sapin II protège les lanceurs d'alerte seulement s'ils ont suivi le processus de signalement gradué en trois paliers (cf. Partie 1), ils peuvent être réembauchés suite à un licenciement ou autre mesure discriminante. Dans le cas précédent il faudra réussir à prouver la situation de « danger grave et imminent » ou de « risque de dommages irréversibles ». Très souvent, la Cour de cassation jouera un rôle crucial dans son interprétation.

D'autres éléments sont reprochés à la règlementation, notamment la prolifération des textes organisant les alertes professionnelles. Il existait et existe toujours d'autres lois qui protègent les personnes qui émettent des alertes d'harcèlement sexuel[23], de corruption[24] ou relatives à la sécurité sanitaire des médicaments[25], à un risque pour la santé publique ou l'environnement[26]. La loi Sapin II site qu'elle s'applique également « à d'autres procédures d'alerte instaurées par le législateur », cette juxtaposition de mécanismes concurrents ne favorise pas leur lisibilité et leur efficacité.

[23] D'après l'article L1153-3 du code du travail : « *Aucun salarié […] ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire pour avoir témoigné de faits de harcèlement sexuel ou pour les avoir relatés.* ».

[24] D'après l'article L1161-1 du code du travail : « *Aucune personne […] ne peut être sanctionné […] pour avoir relaté ou témoigné, de bonne foi, soit à son employeur, soit aux autorités judiciaires ou administratives, soit, en de faits de corruption dont il aurait eu connaissance dans l'exercice de ses fonctions.* ».

[25] D'après l'article L5312-4-2 du code de la santé publique : « *Aucune personne […] ne peut être sanctionné […] pour avoir relaté ou témoigné, de bonne foi, soit à son employeur, soit aux autorités judiciaires ou administratives, de faits relatifs à la sécurité sanitaire des produits mentionnés à l'article L. 5311-1 dont elle aurait eu connaissance dans l'exercice de ses fonctions.* ».

[26] D'après l'article L1351-1 du code de la santé publique : « *Aucune personne […] ne peut être sanctionné […] pour avoir relaté ou témoigné, de bonne foi, soit à son employeur, soit aux autorités judiciaires ou administratives, soit, en dernier ressort, à un journaliste, au sens de l'article 2 de la loi du 29 juillet 1881 sur la liberté de la presse de faits relatifs à un risque grave pour la santé publique ou l'environnement dont elle aurait eu connaissance dans l'exercice de ses fonctions.* ».

Cette prolifération de textes peut faire naitre une certaine ambiguïté autour du concept. En août 2017, le terme « lanceur d'alerte » recherché sur un célèbre moteur de recherche donnait 1 270 000 pages de résultats en 0,31 secondes. Le terme est employé de façon très large et certaine fois de manière abusive. Sur ce même moteur de recherche nous retrouvons des exemples de cette confusion sémantique : le blog passeurdalertes.org classe parmi les lanceurs d'alerte une association pour la protection animale ; Europe 1 désigne André Delepierre comme le « lanceur d'alerte sur la pollution atmosphérique » ; la Ligue des droits de l'Homme désigne Cédric Herrou, l'agriculteur qui recueille les migrants près de la frontière entre l'Italie et la France, comme le « lanceur d'alerte de la démocratie en France », etc. Le terme « lanceur d'alerte » recouvre des situations tout à fait différentes et pas forcément celles entendues par la Loi Sapin II. Le terme est souvent utilisé pour qualifier ce qu'il conviendrait de nommer : militant, politique, citoyen engagé, informateur ou encore vigilant.

II- Le risque de rejet des utilisateurs potentiels

Un des principaux risques est la non utilisation du dispositif liée à l'éventuel rejet de la part des utilisateurs potentiels.

En France, le concept de lanceur d'alerte est un sujet « tabou » pour des raisons culturelles. Dans la mémoire collective, le signalement renvoie à des pratiques de dénonciation, de délation, souvent anonymes, durant la Seconde Guerre Mondiale pendant la période d'occupation du pays.

Toutefois, à la question : « *Seriez-vous prêts à utiliser le dispositif en cas de connaissance d'un fait de corruption, de trafic d'influence, d'un crime, d'un délit ou autre au sein de votre entreprise ? (Votre confidentialité étant assurée)* », 91,67% des personnes interrogées répondent « Oui ». Cependant, à la question « Pour quelles raisons ne seriez-vous pas prêts à émettre une alerte ? », 73% des sondés y expriment une crainte.

Parmi l'ensemble des personnes interrogées,

27% ont des craintes quant à leur sécurité personnelle, elles ont peur de subir des représailles sous forme de menaces, pression ou harcèlement.

Certains d'entre eux ont peur pour leur sécurité physique. Les représailles ou le harcèlement peuvent entraîner des conséquences sur la santé. La victime de ces harcèlements peut ressentir des symptômes proches du stress, de l'anxiété, de la dépression voire même des troubles psychosomatiques (amaigrissements, troubles digestifs, hypertension, malaises, etc.). Ces craintes de représailles ne sont pas infondées. Ce fût la réalité de Céline Boussiée lorsqu'elle a dénoncé en 2013 des mauvais traitements sur des enfants polyhandicapés au sein de l'institut médico-éducatif dans lequel elle travaillait, elle a subi de nombreuses menaces, harcelée elle a dû déménager à plusieurs reprises.

Outre ces conséquences sur la santé, on peut se demande si les menaces et la pression ne pourraient pas amener à la corruption. En effet, la personne ciblée par l'alerte pourrait essayer de corrompre le lanceur d'alerte pour le faire taire et ainsi, le dispositif anti-corruption deviendrait source de corruption.

20% redoutent une protection insuffisante qui se traduirait par la perte de leur emploi ou des sanctions cachées (non promotion ou bonus diminué par exemple).

Les lanceurs d'alerte bénéficient de la protection annoncée par la loi si et seulement s'ils obtiennent le statut de « lanceur d'alerte ». Comme expliqué précédemment, obtenir ce statut peut être compliqué, il faut pouvoir prouver de son honnêteté, de sa bonne foi et avoir suivi la procédure en trois paliers de signalement. En matière de protection, la loi dit qu'un salarié ne peut pas être sanctionné, licencié ou faire l'objet d'une discrimination pour avoir alerté sur un délit, un crime ou un fait de corruption dont il aurait été informé dans l'exercice de ses fonctions. Tout acte discriminatoire à son égard serait nul. Par exemple, si un salarié se retrouve licencié pour avoir relaté des faits évoqués dans la loi Sapin II, ce licenciement est nul et le salarié a le droit d'être réintégré dans sa société et à son poste. Pour un lanceur d'alerte, est-ce vraiment une protection que de voir son licenciement pour faute annulé ? En effet, il est difficile d'imaginer une réintégration dans l'entreprise après un tel évènement. Il pourrait être compliqué pour le salarié de supporter le jugement et le regard des autres.

Après une telle démarche de dénonciation il peut aussi être difficile de retrouver un emploi dans une autre entreprise. A compétences égales, les cadres dirigeants préfèrent recruter une personne agissant avec équité, écoute, éthique et respect. De fait, si les cadres dirigeants jugent le lancement d'alerte juste ils devraient le recruter alors que s'ils considèrent cette action

injuste, ils devraient le rejeter. En réalité, la décision n'est pas si binaire. Une étude[27] a mis en évidence plusieurs réalités sur le recrutement des lanceurs d'alerte. Tout d'abord il ressort de cette étude que les cadres dirigeants réagissent différemment selon la gravité du manquement éthique de l'entreprise. S'ils estiment l'alerte sans gravité et injuste ils auront tendance à ne pas recruter le lanceur d'alerte. Cependant ils acceptent de le recruter s'il a dénoncé des faits graves et qu'il a suivi une procédure de signalement juste. Aujourd'hui de nombreux exemples sont la preuve que les lanceurs d'alerte ont peu de chance d'être recrutés par une autre entreprise. C'est le cas de Karim Ben Eli après le scandale d'Arcelor Mittal en juin 2017, de Céline Boussiée qui a dénoncé en 2013 la maltraitance sur des enfants polyhandicapés au sein d'un IME ou encore Stéphanie Gibaud qui dénonçait les pratiques d'évasion fiscale d'UBS en 2008. Chacune de ces trois personnes déclare ne pas avoir retrouvé de travail depuis et vivre dans une situation précaire en touchant le RSA. Ces trois victimes mais aussi l'ensemble des lanceurs d'alerte se sont retrouvés face à un dilemme : Parler au risque de perdre son emploi, de mettre en péril la prospérité de l'entreprise voire l'emploi de ses collègues de travail ? Ou se taire pour ne pas avoir d'ennui, pour ne pas trahir la collectivité ?

En plus de perdre leur emploi, les lanceurs d'alerte se retrouve embarqués dans une procédure rigide et extrêmement coûteuse. Certains réclament une aide financière au nom de l'intérêt général. Cette aide fait partie du rôle du Défenseur des droits qui pourrait accorder aux lanceurs d'alerte une aide financière. Cependant cette aide n'aurait rien d'automatique, elle pourrait lui être refusé s'il n'a pas respecté le système de signalement par paliers et elle pourrait être diminuée de la fraction des frais de procédure pris en charge au titre d'un contrat d'assurance de protection juridique. Pour certains la loi mettrait en place une course d'obstacles pour peu de garanties.

D'autres questions peuvent se poser autour de la protection des lanceurs d'alerte. En effet, la loi Sapin II précise que les lanceurs d'alerte ne sont pas pénalement responsables lorsqu'ils portent « atteinte à un secret protégé par la loi, dès lors que cette divulgation est nécessaire et proportionnée à la sauvegarde des intérêts en cause […] ». Le lanceur d'alerte bénéficie donc d'une irresponsabilité pénale limitée à certains cas : l'atteinte à un secret légal. De plus, la loi

27 D'après une étude réalisée en 2016 par Thierry Nadisic, docteur en comportement organisationnel et Tessa Melkonian, professeur en management et comportement organisationnel. *Prix de la meilleure recherche francophone de l'année 2016* décerné par l'Association francophone des chercheurs en Gestion de Ressources Humaines.

ne protège pas les lanceurs d'alerte actuellement en jugement comme ceux de l'affaire LuxLeaks.

17% des personnes interrogées craignent que leur confidentialité ne soit pas conservée.

Cette statistique met en évidence un manque de confiance de la part des utilisateurs potentiels vis à vis de la loi Sapin II en général et des dispositifs mis en place par leur entreprise en particulier. C'est pourquoi il faudra particulièrement veiller à la sécurité des canaux de remontées. L'accès à l'outil de recueil et de traitement des signalements doit être sécurisé. L'outil devra être protégé contre les risques d'intrusions externes et internes. L'entreprise devra mettre en œuvre des modalités d'évaluation du SI de gestion des alertes en vérifiant régulièrement son fonctionnement en procédant au back testing de sa robustesse.

15% des sondés expriment d'autres raisons qui constitueraient des freins à l'émission d'une alerte.

D'autres raisons, de manière plus marginale, ont été citées comme constituant un frein au lancement d'une alerte : crainte de se tromper (7%), faits non graves (5%), crainte sur le traitement de l'alerte (<2%) et souhait de protéger l'entreprise et ses collaborateurs (<2%).

L'ensemble de ces craintes avouées amène à se demander si les utilisateurs potentiels arriveront à les surpasser et à utiliser le dispositif. Certains sont toujours réticents, il s'agit des syndicats. Ces dispositifs d'alerte remettent en cause le rôle historique des syndicats, à savoir, leur rôle de canal d'intermédiation entre les salariés et les dirigeants de la société. Aujourd'hui ils se demandent si leur légitimité à représenter les intérêts individuels des salariés et à faire valoir leurs réclamations sera impactée par la loi Sapin II. D'où l'intérêt de consulter les partenaires sociaux tout au long de la mise en place du dispositif par la conformité.

PARTIE 3 : GUIDE D'AUDIT DES DISPOSITIFS D'ALERTE INTERNE ET DE RECUEIL DES SIGNALEMENTS

I- Objet de l'étude et champ d'investigation :

Dans le cadre du plan annuel d'audit, l'entreprise a diligenté une mission d'audit sur les dispositifs de recueil d'alertes prévus par la loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite loi Sapin II. Cette mission veut s'assurer que l'entreprise a mis en place des dispositifs de recueil des signalements et que leur exploitation est optimale et conforme aux règlementations.

La mission d'audit a pour objectif de s'assurer que le dispositif est correctement encadré et sécurisé au travers de l'analyse des rôles liés au pilotage et au contrôle. Ainsi, l'audit s'attachera à évaluer :

1. L'encadrement, le cadre procédural, la gouvernance et les reportings
2. Le fonctionnement du dispositif
3. Le dispositif de contrôle interne

<u>Utilisation du guide :</u>

Pour réaliser les contrôles prévus par le guide il conviendra de rajouter à celui-ci quatre colonnes (après la colonne Mode opératoire)[28] :

- Avis de l'audit interne : à laquelle l'audit répondra pour chaque thème du guide par « Satisfaisant », « Convenable », « Insuffisant » ou « Dégradé » en sélectionnant la cotation qu'il convient dans la liste déroulante ;
- Commentaire de l'audit interne : dans laquelle l'audit inscrira pour chaque ligne les conclusions de ses contrôles et investigations ;
- Référence fiche de constat : dans laquelle l'auditeur remplira, si besoin, la référence de la fiche de constat liée à la question d'audit ;
- Statut des travaux : afin d'évaluer l'avancement de la mission l'auditeur répondra grâce à la liste déroulante par « Fait », « En cours » ou « A Faire ».

Les cotations de chaque thème permettront de coter les sous-parties qui elles-mêmes permettront de coter les trois grands domaines du guide cités précédemment. Les cotations des domaines permettront de donner un avis final sur la cotation de la mission dans sa globalité.

[28] Ces quatre colonnes ne sont pas retranscrites dans le guide de ce mémoire par soucis de place et de lisibilité.

Le guide d'audit se présente sous la forme suivante :

1. Domaines
   1.1. Thématiques
      1.1.1. Sous-parties -> Grilles de dépouillement (GDD)

II- Sommaire du Guide d'audit

Guide d'audit "Lanceurs d'alerte"

DOMAINE A
L'ENCADREMENT, LE CADRE PROCÉDURAL, LA GOUVERNANCE ET LES REPORTINGS

Thématiques
ENCADREMENT
CADRE PROCEDURAL
GOUVERNANCE ET REPORTINGS

- GDD 1 Corps procédural
- GDD 2 Règlement intérieur
- GDD 3 Pilotage et reportings

DOMAINE B
LE FONCTIONNEMENT DU DISPOSITIF

Thématiques
CONFORMITE
SENSIBILISATION DES COLLABORATEURS
CONFIDENTIALITE ET PROTECTION DES LANCEURS D'ALERTE
ARCHIVAGE
SECURITE DU SI

- GDD 4 Respect des délais
- GDD 5 Traitement des alertes
- GDD 6 Qualité des informations
- GDD 7 Formations
- GDD 8 Archivage
- GDD 9 Dossiers

DOMAINE C
LE DISPOSITIF DE CONTRÔLE INTERNE

Thématiques
EXHAUSTIVITE DU PLAN DE CONTRÔLE
EFFICIENCE DU DISPOSITIF DE CONTRÔLE
PLANS D'ACTION

- GDD 10 Exhaustivité contrôles
- GDD 11 Efficience contrôles

Sous-partie	Question	Finalité (objectifs de CI)	Référence normative	Risques			Ex. de bonnes pratiques	Mode opératoire
				Facteurs (scénarios d' empêchement)	Points de contrôle	Impacts		
1. Encadrement, cadre procédural, gouvernance et reporting								
1.1. Encadrement								
1.1.1. Désignation d'un référent	-La désignation du référent est-elle actée en comité par un PV ?	-S'assurer qu'une personne est chargée du recueil des alertes et que la décision a été validée par la direction.	-Décret n° 2017-564 du 19 avril 2017 relatif aux procédures de recueil des signalements émis par les lanceurs d'alerte.	-Absence de désignation d'une personne référente en la matière ; -Absence d'arbitrage objectif lors des définitions de fonctions ; -Absence de validation par la direction.	-Organigram ; -PV	-Risque de non-conformité ; -Méconnaissance des collaborateurs sur la personne à solliciter ; -Non utilisation du dispositif ; -Risque opérationnel.	-Désignation, par la gouvernance, d'un responsable de la conformité chargé de piloter le dispositif en étroite coopération avec les dirigeants.	-Entretiens ; -Analyse de documents : contrôler la nomination du référent dans un PV de comité.
	-Une fiche de poste a-t-elle été définie ?	-S'assurer que les responsabilités et pouvoirs sont formalisés, communiqués, et attribués à des personnes appropriées ; -S'assurer que le référent connaît ses missions.	-Décret n° 2017-564 du 19 avril 2017.	-Absence de répartition des tâches et des responsabilités ; -Fiche de poste non mise à jour ; -La fiche de poste n'est pas à la disposition du référent.	-Fiche de poste.	-Perte de temps (méconnaissance des tâches à effectuer, tâches incompatibles) ; -Divulgation involontaire des informations confidentielles ; -Sanctions en cas de divulgation : 2 ans de prison et 30 000€ d'amende.	-Définir des fiches de poste ; -Procédure de diffusion des fiches de poste ; -Mise à jour régulière de ces documents ; -Prévoir les habilitations aux fichiers/données en conséquence.	-Entretien : s'assurer que le référent connaît ses missions ; -Analyse de documents : contrôler que le référent a à sa disposition une fiche de poste à jour.

Sous-partie	Question	Finalité (objectifs de CI)	Référence normative	Risques			Ex. de bonnes pratiques	Mode opératoire
				Facteurs (scénarios d' empêchement)	Points de contrôle	Impacts		
1.1.1. Désignation d'un référent (suite)	-Un back up et des subdélégations ont-t-ils été définis ?	-S'assurer de la continuité d'activité ; -Être sûr que les responsabilités et pouvoirs sont formalisés, communiqués, et attribués à des personnes appropriées.	-Code du travail.	-Absence de répartition des tâches et des responsabilités ; -Pas de liste de personnes habilitées, pas de fiche de poste ; -Relation informelle.	-Délégations de pouvoirs ; -Liste des pouvoirs ; -Fiches de poste.	-Risque opérationnel ; -Perte de temps (méconnaissance des personnes habilitées, tâches incompatibles); -Discontinuité d'activité ; -Absence de traitement des alertes.	-Définir une liste de personnes habilitées et des délégations de pouvoirs avec la signature des personnes concernées ; -Mise en place d'un back up et de subdélégations ; -Prévoir les accès aux fichiers/données en conséquence ; -Procédure de diffusion de ces documents à l'ensemble des personnes concernées.	-Analyse de documents : s'assurer que les fiches de poste prévoient un backup et des subdélégations en cas d'absence ponctuelle et périodique du référent.
1.2. Cadre procédural								
1.2.1. Procédures, modes opératoires, outils et pratiques	-Une note d'information sur les obligations règlementaires a-t-elle été définie ?	-S'assurer que l'organisation dispose d'une connaissance suffisante des obligations qui s'imposent à elle.	-Loi Sapin 2, chapitre II, art. 8. III17)	-Défaut / manque de mise à jour des connaissances ; -Défaut / manque de diffusion des informations ; -Diversité et densité des informations ; -Les documents attestant de la conformité ne sont pas conservés ou sont égarés.	-Corps procédural ; -Manuel des procédures ; -Procédure de mise à jour des connaissances ; -Procédure de veille sur les règlementations.	-Non-conforme aux obligations légales.	-Sensibiliser le personnel aux aspects règlementaires du dispositif ; -Procédure de veille sur les règlementations et de diffusion des informations.	-Revue de procédures ; -Grille 1 (cf. Notice explicative des grilles d'analyse).

Sous-partie	Question	Finalité (objectifs de CI)	Référence normative	Risques			Ex. de bonnes pratiques	Mode opératoire
				Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts		
1.2.1. Procédures, modes opératoires, outils et pratiques (suite)	-Existe-t-il un manuel d'utilisation du dispositif ?	-S'assurer que les lanceurs d'alerte potentiels ont à leur disposition un manuel leur expliquant comment lancer une alerte.	-AU 004 de la CNIL ; -Décret d'application 2017-564 du 19/04/2017, relatif aux procédures de recueil des signalements émis par les lanceurs d'alerte.	-Absence de référentiel de procédures ; -Procédure incomplète et inefficace ; -Procédure non mise à jour ; -Absence d'encadrement du dispositif.	-Corps procédural relatif au dispositif ; -Manuel des procédures ; -Cohérence globale des procédures.	-Risque de non-conformité ; -Mauvaise exécution des tâches ; -Opérations non sécurisées : perte d'informations et de savoirs ; -Allongement des délais de traitement ; -Divulgation d'alertes à l'opinion publique ; -Atteinte à l'image et à la réputation de l'entreprise ; -Découragement des salariés.	-Définir et formaliser les procédures, modes opératoires et outils nécessaires aux collaborateurs ; -L'information doit être claire.	-Revue de procédures ; -Grille 1 (cf. Notice explicative des grilles d'analyse).
	-Une procédure de traitement des alertes a-t-elle été définie ?	-S'assurer que le référent sait comment exécuter ses missions.	-AU 004 de la CNIL ; -Décret d'application 2017-564 du 19/04/2017, relatif aux procédures de recueil des signalements émis.	-Absence de référentiel de procédures ; -Procédure incomplète et inefficace ; -Procédure non mise à jour ; -Absence d'encadrement du dispositif.	-Corps procédural relatif au dispositif ; -Manuel des procédures ; -Cohérence globale des procédures.	-Non-conformité ; -Mauvaise exécution des tâches, non optimisation des pratiques ; -Opérations non sécurisées : perte d'informations et de savoirs ; -Perte de productivité : allongement des délais.	-Définir et formaliser les procédures, modes opératoires et outils nécessaires au référent (et au subdélégué) ; -L'information doit être claire.	-Revue de procédures ; -Grille 1 (cf. Notice explicative des grilles d'analyse).

Sous-partie	Question	Finalité (objectifs de CI)	Référence normative	Risques			Ex. de bonnes pratiques	Mode opératoire
				Facteurs (scénarios d' empêchement)	Points de contrôle	Impacts		
1.2.1. Procédures, modes opératoires, outils et pratiques (suite)	-Une procédure de garantie de confidentialité a-t-elle été définie ?	-Vérifier qu'une procédure mentionne les aspects relatifs à la confidentialité.	-Décret n° 2017-564 du 19 avril 2017 relatif aux procédures de recueil des signalements.	-Absence de référentiel de procédures ; -Procédure incomplète et inefficace ; -Procédure non mise à jour ; -Absence d'encadrement du dispositif.	-Corps procédural relatif au dispositif ; -Manuel des procédures ; -Cohérence globale des procédures.	-Opérations non sécurisées : perte d'informations et de savoirs ; -Le référent ou tout destinataire de l'alerte, est passible de 2 ans de prison et de 30 000€ d'amende en cas de divulgation des informations recueillies par les procédures de signalement ; -Méfiance et découragement des salariés.	-Existence d'une procédure qui précise comment l'organisme employeur garantit la stricte confidentialité de l'identité du lanceur d'alerte et des personnes visées, ainsi que des faits signalés.	-Revue de procédures ; -Grille 1 (cf. Notice explicative des grilles d'analyse).
	-Ce corps procédural est-il à jour ?	-Vérifier que l'ensemble du corps procédural est à jour vis-à-vis des dernières règlementations .	-Loi Sapin 2, chapitre II, art. 8. III17).	-Procédures non mises à jour.	-Fréquence des mises à jour.	-Risque de non-conformité ; -Non-fiabilité des informations.	-Mise en place d'une veille pour les nouvelles règlementations en vigueurs ; -Mettre à jour les procédures dès la connaissance d'une nouvelle règlementation en la matière.	-Revue de procédures ; -Grille 1 (cf. Notice explicative des grilles d'analyse).

Sous-partie	Question	Finalité (objectifs de CI)	Référence normative	Risques			Ex. de bonnes pratiques	Mode opératoire
				Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts		
1.2.2. Mise à jour du règlement intérieur	-Le règlement intérieur a-t-il été mis à jour ?	-S'assurer que le règlement intérieur intègre les spécificités du dispositif.	-Loi Sapin 2 ; -Code du travail.	-Absence de formalisation des informations relatives au dispositif dans le règlement intérieur.	-Règlement intérieur.	-Non-conformité aux obligations légales.	-La procédure de signalements est intégrée au règlement intérieur ; -Lors de la modification du règlement intérieur, l'organisation a suivi toutes les étapes imposées par le Code du travail.	-Analyse de documents : vérifier que le règlement intérieur intègre le dispositif ; -Entretiens ; -Grille 2 (cf. Notice explicative des grilles d'analyse).
1.2.3. Rédaction de scénarios de traitement	-Des scénarios de correction ont-ils été définis et validés par la direction ?	-S'assurer que des actions de traitement types ont été prévues pour les alertes les plus significatives.	-Recommandations du MEDEF Mouvement des Entreprises De France.	-Absence de scénarios ; -Scénarios inadaptés / impertinents ; -Absence de validation par la direction ; -Scénarios non mis à la disposition du référent.	-Scénarios de correction.	-Traitement des alertes inadapté ; -Perte de temps (méconnaissance des tâches à effectuer) ; -Non-optimisation du traitement ; -Opérations non sécurisées : perte d'informations et de savoirs ; -Non-respect de la confidentialité ; -Sanctions : 2 ans de prison et 30 000€ d'amende.	-Rédaction de scénarios de correction pour les alertes majeures ; -Ces scénarios prévoient toutes les étapes devant être réalisées pour traiter une alerte ; -Ces scénarios prévoient des actions précises avec une définition des rôles.	-Analyse de documents : vérifier que des scénarios de correction existent et qu'ils ont été approuvés par la direction (signature, accord, mail, PV de réunion, etc.).

Sous-partie	Question	Finalité (objectifs de CI)	Référence normative	Risques			Ex. de bonnes pratiques	Mode opératoire
				Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts		
1.2.4. Consultation des IRP (Institutions Représentatives du Personnel)	-Les instances représentatives du personnel ont-elles été consultées lors de la mise en place du dispositif ?	-S'assurer que l'instance dirigeante a informé-consulté le comité d'entreprise.	-Recommandations du MEDEF Mouvement des Entreprises De France.	-Absence de consultation des instances représentatives du personnel ; -L'avis des IRP n'a pas été formalisé ; -L'avis des IRP n'a pas été pris en compte.	-Comptes rendus de réunion ; -Fiches de présence aux réunions ; -Avis formalisé ; -Support de réunion.	-Rejet du dispositif de la part des instances représentatives du personnel et du personnel ; -Méfiance et découragement des salariés à l'égard du dispositif.	-La procédure d'alerte fait l'objet d'une consultation des IRP compétentes dans un délai raisonnable ; -L'information communiquée est claire et complète.	-Entretiens ; -Analyse de documents : vérifier que les IRP ont été consultées et retrouver une trace de leur avis concernant le dispositif.
1.2.5. L'autorisation de la CNIL	-Dans le cas d'un dispositif automatisé, a-t-il été soumis à l'autorisation préalable de la Commission nationale de l'informatique et des libertés (CNIL) ?	-S'assurer que l'entreprise est en conformité avec la CNIL.	-Délibération n° 2017-191 du 22 juin 2017 ; -Autorisation Unique AU-004 ; -Journal Officiel du 26 août 2017.	-Absence d'autorisation fournie par la CNIL ; -Exploitation d'un dispositif automatisé de traitement de données personnelles sans accord de la CNIL.	-Déclaration comportant un engagement de conformité à l'autorisation unique n° AU-004.	-Sanctions de la CNIL : sanctions financières pouvant s'élever jusqu'à 3 millions d'euros, retrait de l'autorisation et sanctions pénales.	-Adresser une déclaration de conformité à la CNIL ; ou un dossier complet de demande d'autorisation individuelle (lorsque le dispositif d'alerte professionnelle envisagé sort du cadre fixé par l'AU-004).	-Analyse de documents ; -Entretiens : s'assurer que l'entreprise respectait en tout point le cadre défini lors de sa demande d'autorisation ; sinon retrouver le dossier de demande d'autorisation.

Sous-partie	Question	Finalité (objectifs de CI)	Référence normative	Risques			Ex. de bonnes pratiques	Mode opératoire
				Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts		
1.3. Gouvernance et reporting								
1.3.1. Pilotage	-Le pilotage des alertes est-il adapté ?	-S'assurer que l'entreprise pilote le dispositif de lanceurs d'alerte.	- Recommandation de l'AFA.	-Absence de suivi ; -Absence d'analyse et d'exploitation des alertes ; -Absence d'indicateurs de mesures définis ; -Outil de suivi inexistant.	-Tableaux de bord ; - Indicateurs ; -Comptes rendus de réunion.	-Réitération des comportements à risque.	-Suivi statistique mensuel (nombre d'alertes reçues, de dossiers clos, de dossiers ayant donné lieu à une enquête, nombre et type de mesures prises pendant et à l'issue de l'enquête.)	-Entretiens ; -Grille 3 (cf. Notice explicative des grilles d'analyse).
	-Les faits remontés par ces signalements sont-ils utilisés pour actualiser la cartographie des risques de corruption ?	-Être sûr que les principaux risques, pouvant avoir un impact sur l'organisation, sont identifiés et recensés de façon exhaustive ; -Être sûr que les risques sont évalués de façon pertinente selon leur niveau d'impact et leur probabilité d'occurrence.	- Recommandation de l'AFA.	-Mauvaise appréhension des risques selon leur nature et leur impact ; -Manque de moyen pour identifier et évaluer les risques ; -Non-fiabilité de la cartographie ; -Cartographie non mise à jour.	- Cartographie des risques de corruption ; -Procédure de mise à jour de la cartographie ; -Moyens alloués au recensement des risques.	-Mauvaise maitrise des risques ; -Réitération des comportements à proscrire ; -Performance revue à la baisse (malversation, perte financière, fraude…) ; -Des risques ne sont pas identifiés pouvant mettre en péril l'organisation ; -Mauvaise identification et évaluation des risques.	-Mise en place d'un processus de recensement continu ; -Mise à jour de la cartographie des risques à minima annuellement en respectant la confidentialité ; - Hiérarchisation des risques ; - Statistiques d'occurrence et de la gravité des incidents rencontrés.	-Entretiens ; -Analyse de documents : vérifier que la cartographie des risques de corruption a régulièrement été mise à jour suite aux alertes remontées.

Sous-partie	Question	Finalité (objectifs de CI)	Référence normative	Risques			Ex. de bonnes pratiques	Mode opératoire
				Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts		
1.3.2. Implication de l'instance dirigeante	-Le dispositif a-t-il été validé par le Conseil d'Administration et communiqué à la direction ?	-S'assurer que l'instance dirigeante a validé le choix du canal de remontées ; -Être sûr que la direction générale rend compte au conseil des caractéristiques essentielles du dispositif.	-Recommandation de l'AFA.	-Absence de l'implication de l'instance dirigeante ; -Absence de validation par le Conseil d' Administration; -Validation non formalisée ; -Absence de communication à la direction ou remontées erronées ou incomplètes.	-Comptes rendus de réunion ; -Fiches de présence aux réunions ; -Formalisation de l'accord ; -Information au CA.	-Désengagement de la direction ; -Risque de défaut de pertinence de la démarche corrective ; -Inefficacité en termes de réduction du coût du risque opérationnel et ce malgré des actions engagées.	-Gouvernance du programme de conformité anticorruption au plus haut niveau de l'organisation ; -Approbation du dispositif de prévention et de détection de la corruption par l'instance dirigeante.	-Entretiens ; -Analyse de documents : vérifier la validation de la direction (email, PV, etc.) et l'information au CA.
	-Les faits signalés sont-ils portés à la connaissance des instances dirigeantes ?	-S'assurer que l'instance dirigeante est engagée dans la prévention et la détection des faits de corruption.	-Recommandation de l'AFA.	-Absence de dispositif de remontée de l'information vers l'instance dirigeante ; -Reportings incomplets ; -Défaut dans la qualité et la complétude de l'information remontée.	-Reporting ; -Comptes rendus de réunion ; -Fiches de présence aux réunions.	-Méconnaissance des risques par la direction ; -Risque de défaut de pertinence de la démarche corrective ; -Inefficacité en termes de réduction du coût du risque opérationnel et ce malgré des actions engagées.	-Reportings réguliers à destination des instances dirigeantes : présentation des faits remontés et du suivi (minimum trimestriellement) ; -Remontée des incidents au fil de l'eau, confirmation de l'absence de perte le cas échéant.	-Entretiens ; -Grille 3 (cf. Notice explicative des grilles d'analyse).

Sous-partie	Question	Finalité (objectifs de CI)	Référence normative	Risques			Ex. de bonnes pratiques	Mode opératoire
				Facteurs (scénarios d' empêchement)	Points de contrôle	Impacts		
2. Fonctionnement du dispositif								
2.1. Conformité								
2.1.1. Dispositif opérationnel	-Les canaux de signalement ont-ils été définis et sont-ils adéquats ?	-S'assurer de l'existence de canaux de remontées bien définis.	-Décret n° 2017-564 du 19 avril 2017 relatif aux procédures de recueil des signalements.	-La définition des canaux n'est pas claire ; -Ils ne garantissent pas la confidentialité de l'émetteur.	-Procédure lanceurs d'alertes ; -Dispositif de recueil.	-Non-conformité aux obligations légales ; -Divulgation d'alertes à l'opinion publique ; -Atteinte à l'image et à la réputation de l'entreprise.	-Plusieurs options sont possibles : mise en place d'une plate-forme web, courriel, hotline, courrier, fax, etc.	-Entretiens ; -Revue de procédures : vérifier que le ou les canaux de remontée des alertes ont été définis.
	-Les canaux de signalement sont-ils accessibles à l'ensemble des lanceurs d'alerte potentiels ?	-S'assurer que les collaborateurs externes ont accès au canal d'alerte (prestataires / fournisseurs de premier rang).	-Article 8 de la loi n°2016-1691 du 9 décembre 2016.	-Le dispositif n'intègre pas les collaborateurs externes (ex : accès par l'intranet) ; - Le système d'information ne permet pas l'accès aux collaborateurs externes.	-Accessibilité du dispositif.	-Non-conformité aux obligations légales ; -Divulgation d'alertes à l'opinion publique ; -Atteinte à l'image et à la réputation de l'entreprise.	-Mise en place d'un canal de remontée accessible aussi bien aux personnes internes qu'aux collaborateurs externes ; -Le canal n'est pas exclusivement disponible par l'intranet ; -Son existence est communiquée aux personnes concernées (prestataires, fournisseurs).	-Entretiens : demander la démonstration du lancement d'une alerte par une personne extérieure.

Sous-partie	Question	Finalité (objectifs de CI)	Référence normative	Risques			Ex. de bonnes pratiques	Mode opératoire
				Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts		
2.1.2. Respect des procédures	-Les signalements traités étaient-ils adressés aux personnes adéquates ?	-S'assurer que les alertes traitées avaient été adressées à une personne habilitée.	-AU 004 de la CNIL.	-L'alerte a été traitée par une personne non autorisée ; -Mauvaise formalisation des pouvoirs et responsabilités.	-Historiques des alertes ; -Dossiers de signalement.	-Traitement de l'alerte par une personne non habilitée, qui ne connaît pas les mesures de sécurité en matière de confidentialité ; -Opérations non sécurisées : perte d'informations et de savoirs ; -Non-respect de la confidentialité ; -Sanctions en cas de divulgation : 2 ans de prison et 30 000€ d'amende.	-Rédiger la liste des personnes habilitées à recevoir une alerte (supérieur hiérarchique direct ou indirect, employeur ou référent) ; -Sécuriser le système de recueil de signalements pour empêcher l'envoi d'alertes à d'autres personnes que celles autorisées.	-Échantillonnage ; -Grille 4 (cf. Notice explicative des grilles d'analyse).
	-Les alertes sont-elles attestées par des preuves et des témoignages ?	-S'assurer que les alertes sont basées sur des éléments factuels.	-Dispositions du 1° du II de l'article 5 du décret n° 2017-564 du 19 avril 2017 relatif aux procédures de recueil des signalements ; -AU 004 de la CNIL.	-Absence de preuves ou preuves non recevables.	-Dossiers de signalement ; -Outils de signalement.	-Non-respect des réglementations en vigueurs ; -Traitement d'alertes infondées ; -Utilisation abusive du système.	-Rédiger une liste des preuves recevables par exemple : écrits, courriels, rapports, documents comptables, témoignages, entretiens etc. ; -Joindre les preuves au dossier.	-Échantillonnage ; -Grille 5 (cf. Notice explicative des grilles d'analyse).

Sous-partie	Question	Finalité (objectifs de CI)	Référence normative	Risques			Ex. de bonnes pratiques	Mode opératoire
				Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts		
2.1.2. Respect des procédures (suite)	-Le référent respecte-t-il les différents délais imposés par la CNIL et la loi Sapin II ?	-S'assurer que le référent respecte les différents délais imposés par la règlementation en matière d'information des personnes concernées.	-Dispositions du 1° du II de l'article 5 du décret n° 2017-564 du 19 avril 2017 relatif aux procédures de recueil des signalements émis par les lanceurs d'alerte ; -AU 004 de la CNIL.	-Traitement tardive des alertes ; -Le référent n'informe pas le lanceur d'alerte et la personne concernée de la réception de l'alerte.	-Outil ; -Dossier de signalement ; -Envois ; -Historique des actions dans l'outil.	-Alerte traitée tardivement ; -Risque de fraude ; -Réitération des comportements à proscrire ; -Des risques ne sont pas identifiés pouvant mettre en péril l'organisation.	-Le référent informe le lanceur d'alerte "sans délai" de la réception de son alerte, il informe la personne visée par l'alerte dès l'enregistrement de données la concernant et il traite le signalement dans un délai inférieur à 3 mois.	-Échantillonnage ; - Grille 4 (cf. Notice explicative des grilles d'analyse).
	-Le référent respecte-t-il ses obligations d'information du lanceur d'alerte et de la personne visée par l'alerte ?	-S'assurer que le référent communique toutes les informations prévues par la règlementation au lanceur d'alerte et à la personne visée par l'alerte.	-Dispositions du 1° du II de l'article 5 du décret n° 2017-564 du 19 avril 2017 relatif aux procédures de recueil des signalements. AU 004 de la CNIL.	-Le référent ne communique pas tous les éléments nécessaires au lanceur d'alerte et à la personne visée.	-Envois.	-Non-conformité aux obligations légales ; -Le référent ne permet pas à la personne visée de s'opposer au traitement de ses données personnelles.	-Le référent communique au lanceur d'alerte et à la personne visée par l'alerte les informations dont ils ont besoin ; -Pour ce faire il effectue un envoi par accusé de réception écrit et daté.	-Échantillonnage, -Grille 6 (cf. Notice explicative des grilles d'analyse).

Sous-partie	Question	Finalité (objectifs de CI)	Référence normative	Risques			Ex. de bonnes pratiques	Mode opératoire
				Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts		
2.1.3. Respect des scénarios de correction	-Les actions de traitement entreprises correspondent-elles aux scénarios de correction validés par la direction ?	-S'assurer du respect des scénarios de correction des risques majeurs.	-Recommadations du MEDEF Mouvement des Entreprises De France.	-Risque non prévu par les scénarios ; -Prise de liberté dans le choix des actions menées ; -Scénarios non mis à la disposition du référent.	-Historique des traitements ; -Dossiers de signalement ; -Scénarios de traitement.	-Traitement des alertes inadapté ; -Opérations non sécurisées : perte d'informations et de savoirs ; -Non-respect de la confidentialité ; -Sanctions en cas de divulgation : 2 ans de prison et 30 000€ d'amende.	-Lors d'une alerte, identifier sa typologie et se référer aux scénarios de traitement pour appliquer à la lettre les actions qu'il préconise.	-Échantillonnage ; -Grille 5 (cf. Notice explicative des grilles d'analyse).
2.1.4 Respect des injonctions de la CNIL	-Les catégories de données pouvant être enregistrées sont-elles respectées ?	-S'assurer que l'entreprise ne détient pas des informations qui ne sont pas autorisées par la CNIL.	-Article 3 de la version révisée de l'AU-004 de la CNIL.	-Collecte d'informations hors catégories autorisées.	-Outil de traitement des signalements ; -Dossiers de signalement.	-Sanctions de la CNIL : sanctions financières pouvant s'élever jusqu'à 3 millions d'euros, retrait de l'autorisation, sanctions pénales.	-L'outil ne traite que des catégories de données autorisées ; -Existence d'un outil qui détecte par identification de mots clés, des informations interdites enregistrées dans le système.	-Échantillonnage ; -Analyse de documents : prendre 5 dossiers et vérifier que les informations présentes respectent les catégories autorisées par la CNIL (voir Annexe 1).

Sous-partie	Question	Finalité (objectifs de CI)	Référence normative	Risques			Ex. de bonnes pratiques	Mode opératoire
				Facteurs scénarios d'empêchement	Points de contrôle	Impacts		
2.2. Sensibilisation des collaborateurs								
2.2.1 Animation du dispositif	-Le dispositif de lancement d'alertes a-t-il été communiqué à l'ensemble des collaborateurs ?	-S'assurer que l'organisation a entrepris des actions de sensibilisation du personnel.	-Loi Sapin 2, chapitre II, art. 8.III17) ; -Décret n° 2017-564 du 19 avril 2017 ; -Code du travail ; -Loi "Informatique et Libertés".	-Pas de communication sur le sujet ; -Procédures non diffusées.	-Plan de communication / sensibilisation ; -Diffusion des informations ; -Mise à disposition des modes opératoires, guides, procédures aux collaborateurs.	-Désengagement des salariés ; -Mauvaise exécution des tâches ; -Opérations non sécurisées ; -Perte d'information et de savoirs ; -Divulgation d'alertes à l'opinion publique ; -Atteinte à l'image et à la réputation de l'entreprise.	-Diffusion : réunions, messages sur l'intranet et sur la page web ; -Donner des informations précises aux collaborateurs, tels que des exemples d'alertes qui ont été remontées ; -Communiquer lors de modifications des procédures ; -Veiller à ce que les modes opératoires et procédures soient connus de tous.	-Entretiens ; -Analyse de documents : vérifier que la mise en place du dispositif a fait l'objet d'une communication, s'assurer de la diffusion des procédures.
		-S'assurer que les circuits d'information sont adaptés à la nature des informations transmises.	-Loi Sapin 2, chapitre II, art. 8.III17) ; -Décret n° 2017-564 du 19 avril 2017 ; -Code du travail ; -Loi "Informatique et Libertés".	-Défaut d'information : données clés manquantes pour le bon fonctionnement du dispositif ; -Surplus d'information : infos non essentielles parasitant les circuits d'information.	-Circuits d'information formalisés ; -Supports de communication ; -Processus de diffusion.	-Informations transmises aux personnes inadéquates ; -Manque d'information.	-Transmettre les informations de manière détaillée ; -Formaliser un processus de diffusion avec liste des personnes concernées ; -Recenser les informations nécessaires au bon fonctionnement du dispositif.	-Analyse de documents : vérifier que les circuits de diffusion des informations sont adaptés au dispositif (diffusion à l'ensemble des collaborateurs, extérieurs et occasionnels).

Sous-partie	Question	Finalité (objectifs de CI)	Référence normative	Risques			Ex. de bonnes pratiques	Mode opératoire
				Facteurs (scénarios d' empêchement)	Points de contrôle	Impacts		
2.2.1 Animation du dispositif (suite)	-Les informations sur le dispositif de lancements d'alertes sont-elles accessibles ?	-S'assurer que l'entreprise permet aux salariés et extérieurs de prendre part à la lutte anticorruption du groupe.	-Décret n° 2017-564 du 19 avril 2017 ; -Recommandations de l'AFA Agence Française Anticorruption.	-Les procédures ne sont pas à la disposition de l'ensemble des personnes concernées ; -L'entreprise n'a pas indiqué l'emplacement de ces documents.	-Mise à disposition des modes opératoires, guides, procédures.	-Manque d'implication des salariés ; -Mauvaise ou non-utilisation du dispositif car manque d'information ; -Divulgation d'alertes à l'opinion publique ; -Atteinte à l'image et à la réputation de l'entreprise.	-La procédure de recueil des signalements est accessible par notification, affichage, publication, etc. -Les managers reçoivent régulièrement leur équipe pour donner du sens au dispositif en expliquant les conséquences de sa non utilisation par exemple.	-Entretiens : vérifier l'accès à tout moment aux corps procédural relatif au dispositif par l'ensemble des collaborateurs même extérieurs et occasionnels.
	-Les collaborateurs ont-ils reçu une formation de qualité sur le dispositif d'alerte à leur disposition ?	-S'assurer que l'entreprise a mis en œuvre un plan de formation spécifique aux remontées d'alertes ; -S'assurer que les formations sont correctement effectuées ; -S'assurer de l'efficacité des formations.	-Recommandations de l'AFA Agence Française Anticorruption.	-Absence de formation sur le sujet ; -Formation inadaptée à la nature des risques et aux fonctions exercées ; -Manque de compétence chez les formateurs ; -Pas d'évaluation.	-Plan de formation ; -Circuit de validation d'une formation ; -Documents relatifs aux formations (détails, planning, modalités, fiche de présence ; -Cursus antérieur à chaque formateur.	-Formations inefficaces ; -Manque d'implication des salariés.	-Formations en présentiel personnes les plus exposées ; -Formation spécifique consacrée au recueil des signalements ; -La formation permet aux participants de poser librement des questions ; -Les cadres s'assurent que les équipes ont suivi et compris les formations ; -E-learning réguliers.	-Entretiens ; -Analyse de documents : vérifier qu'une formation spécifique au dispositif existe ; -Échantillonnage ; -Grille 7 (cf. Notice explicative des grilles d'analyse).

Sous-partie	Question	Finalité (objectifs de CI)	Référence normative	Risques			Ex. de bonnes pratiques	Mode opératoire
				Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts		
2.2.2. Consultation des IRP	-Les instances représentatives du personnel sont-elles informées en cas d'alerte relative aux ressources humaines ?	-S'assurer que l'instance dirigeante a informé-consulté les IRP lorsqu'une alerte concerne les ressources humaines.	- Recommandations du MEDEF Mouvement des Entreprises De France.	-Absence de consultation des instances représentatives du personnel.	- Informations aux IRP.	-Manque d'implication des IRP ; -Mauvaise gestion RH de l'alerte ; -Mauvais traitement de l'alerte.	-Les alertes relatives aux ressources humaines font l'objet d'une consultation systématique des instances représentatives du personnel compétentes dans un délai raisonnable.	-Entretien ; -Grille 5 (cf. Notice explicative des grilles d'analyse).
2.3. Confidentialité et protection du lanceur d'alerte								
2.3.1. Respect de la confidentialité	-La confidentialité est-elle garantie ?	-S'assurer que l'entreprise garantie la stricte confidentialité de l'identité du lanceur d'alerte, des faits objets du signalement et des personnes visées par le signalement, notamment lors des transferts de déclarations entre les différents paliers de signalement.	-AU 004 de la CNIL.	-Manque de vigilance lors des transferts d'informations ; -Absence de procédure sur la confidentialité ; -Accès non sécurisé à l'outil.	-Dossiers de signalement.	-Le référent ou tout destinataire de l'alerte, est passible de 2 ans de prison et de 30 000€ d'amende en cas de divulgation des identités ou des informations recueillies par les procédures de signalement.	-Le responsable de traitement, avant chaque transmission de données, opère un tri parmi ces dernières pour s'assurer que le destinataire accède aux seules données strictement nécessaires et proportionnées au regard de la justification de la communication ; -Accès restreint sur un serveur sécurisé, coffre, etc.	-Entretiens : demander quelles sont les mesures de précaution prises pour garantir la confidentialité.

Sous-partie	Question	Finalité (objectifs de CI)	Référence normative	Risques			Ex. de bonnes pratiques	Mode opératoire
				Facteurs (scénarios d' empêchement)	Points de contrôle	Impacts		
2.3.1. Respect de la confidentialité (suite)	-Si l'identité des lanceurs d'alerte est divulguée, leur consentement est-il formalisé ?	-S'assurer que l'entreprise garantie la stricte confidentialité de l'identité du lanceur d'alerte, des faits objets du signalement et des personnes visées par le signalement.	-Décret n° 2017-564 du 19 avril 2017.	-Absence de formalisation du consentement du lanceur d'alerte ; -Absence de conservation du document.	-Consentement écris ; -Dossiers de signalement.	-Le référent ou tout destinataire de l'alerte, est passible de 2 ans de prison et de 30 000€ d'amende en cas de divulgation des identités ou des informations recueillies par les procédures de signalement.	-Si le lanceur d'alerte est d'accord pour que son identité soit divulguée, l'entreprise lui fait attester son consentement par document écrit ; - Le document prouvant le consentement est réalisé en double exemplaire : un pour le lanceur d'alerte et un pour l'entreprise qui sera conservé dans le dossier de signalement.	-Analyse de documents : récupérer cinq dossiers dont l'identité du lanceur d'alerte a été divulguée, s'assurer de l'existence dans le dossier d'un consentement écrit par le lanceur d'alerte.
2.3.2. Protection du lanceur d'alerte	-Les lanceurs d'alerte ont-ils fait l'objet d'une mesure discriminatoire directe ou indirecte à la suite de leur signalement ?	-S'assurer que les lanceurs d'alerte n'ont pas subi de discrimination après l'émission de leur alerte.	-Article L 1132-3-3 du code du travail ; -Article 6 ter A alinéa 2 de la loi n°83-634 du 13 juillet 1983 ; -Article L.4122-4 alinéa 2 du code de la défense.	-Écarter le lanceur d'alerte d'une procédure de recrutement ou de l'accès à un stage ou une formation professionnelle ; -Sanctionner, licencier ou appliquer une mesure discriminatoire, (rémunération, mutation, etc.).	-Dossiers collaborateurs.	-Saisie du Conseil de prud'hommes : versement d'indemnités au lanceur d'alerte pouvant s'élever à plusieurs centaines de milliers d'euros.	-Le lanceur d'alerte bénéficie d'une protection contre les représailles.	-Échantillonnage; -Analyse de documents : sélectionner 5 signalements, s'assurer que dans le dossier collaborateur du lanceur d'alerte son signalement n'est pas stocké, vérifier que sa rémunération n'a pas diminuée.

Sous-partie	Question	Finalité (objectifs de CI)	Référence normative	Risques			Ex. de bonnes pratiques	Mode opératoire
				Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts		
2.4. Archivage								
2.4.1. Conservation des données	-Les modalités de conservation et d'archivage des données prévues par la CNIL sont-elles respectées ?	-S'assurer que l'entreprise ne conserve pas les données collectées dans le cadre de la procédure de signalement au-delà des délais mentionnés par la CNIL.	-Dispositions du 3° du II de l'article 5 du décret n° 2017-564 du 19 avril 2017 ; -AU 004 de la CNIL.	-Absence d'une procédure d'archivage spécifique au dispositif.	-Procédure d'archivage ; -Historique d'archivage.	-Sanctions de la CNIL : sanctions financières pouvant s'élever jusqu'à 3 millions d'euros, retrait de l'autorisation d'exploitation des données, sanctions pénales.	-Le référent respecte les modalités d'archivage en fonction des suites possibles : classement hors champ, sans suite ou avec poursuites judiciaires ; -Pour cela il se réfère à la procédure rédigée à cet effet.	-Échantillonnage; -Grille 8 (cf. Notice explicative des grilles d'analyse).
2.4.2. S.I. Archivage	-Le système d'archivage fait-il l'objet d'un système d'information distinct à accès restreint ?	-S'assurer que seules les personnes autorisées ont accès aux données archivées relatives aux signalements.	-AU 004 de la CNIL.	-Absence d'un outil d'archivage spécifique au dispositif ; -L'outil d'archivage spécifique n'est pas sécurisé.	-Procédure d'archivage ; -Habilitations.	-Sanctions de la CNIL : sanctions financières pouvant s'élever jusqu'à 3 millions d'euros, retrait de l'autorisation d'exploitation des données, sanctions pénales.	-Les données relatives aux signalements et à leur traitement sont archivées dans un système d'information qui leur est propre. Cet outil est sécurisé par un code d'accès, une liste d'habilitation, etc.	-Entretiens ; -Analyse de document : à partir de la « notice » ou du descriptif de l'outil, vérifier qu'il est distinct de l'outil d'archivage usuel.

Sous-partie	Question	Finalité (objectifs de CI)	Référence normative	Risques			Ex. de bonnes pratiques	Mode opératoire
				Facteurs (scénarios d' empêchement)	Points de contrôle	Impacts		
2.4.3. Dossiers de signalement	-Les dossiers de signalements comportent-ils les éléments minimums requis ?	-S'assurer que le dispositif de signalement permet la traçabilité des actions de traitement ; -S'assurer de l'accessibilité des autorités lors de leurs contrôles.	-Dispositions du 1° du II de l'article 5 du décret n° 2017-564 du 19 avril 2017 relatif aux procédures de recueil des signalements.	-Absence d'accès aux actions entreprises ; -Pas de visibilité sur la vie du dossier de signalement.	-Outil de signalement ; -Dossiers de signalement.	-Les contrôles ne peuvent pas être effectués, que ce soit par le contrôle interne, l'audit ou les autorités.	-L'outil de gestion des signalements conserve l'historique des actions menées par le référent ; -Le référent a constitué des dossiers pour chaque signalement. Ces dossiers sont constitués : des faits, des dates, des preuves, des différents envois d'information, courriers, actions mises en place etc.	-Échantillonnage ; -Grille 9 (cf. Notice explicative des grilles d'analyse).
2.5. Sécurité du SI								
2.5.1. Sécurité des accès	-Le dispositif de traitement des signalements est-il suffisamment sécurisé ?	-S'assurer que l'accès à l'outil de recueil et de traitement des signalements est sécurisé.	-AU 004 de la CNIL	-Accès au système d'information non contrôlé ; -Non mise à jour des listes de personnes autorisées ; -Absence de confidentialité au niveau de la connaissance des codes d'accès.	-Outil, guide utilisateur, liste de personnes habilitées ayant accès au S.I. ; -Procédure de mise à jour des logins et mots de passe.	-Perte de confidentialité ; -Perte de qualité/intégrité des informations ; -Absence de détection de modification de fichiers/données sensibles ; -Sanctions à l'encontre du référent.	-Accès via un identifiant et un mot de passe individuels, régulièrement renouvelés, ou par tout autre moyen d'authentification. Ces accès sont enregistrés et leur régularité est contrôlée ; -Établir la liste des autorisations d'accès à l'outil ; -Formaliser une procédure d'attribution (arrivée, mutation), de suppression et de mise à jour des mots de passe.	-Entretiens ; -Analyse de documents : vérifier que l'accès à l'outil est sécurisé, à partir du guide utilisateur ou d'une démonstration

Sous-partie	Question	Finalité (objectifs de CI)	Référence normative	Risques			Ex. de bonnes pratiques	Mode opératoire
				Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts		
2.5.1. Sécurité des accès (suite)	-Les administrateurs "systèmes" qui ont accès à l'outil de traitement pour assurer sa maintenance ont-ils accès aux alertes elles-mêmes ?	-S'assurer que seules les personnes autorisées ont accès à l'outil de recueil et de traitement des signalements.	-AU 004 de la CNIL.	-Accès au système d'information non contrôlé ; -Non mise à jour des listes de personnes autorisées ; -Absence de confidentialité au niveau des codes d'accès.	-Outil de traitement ; -Historique des connexions ; -Liste des personnes habilitées ayant accès au S.I.	-Perte de confidentialité ; -Perte de qualité/intégrité des informations ; -Absence de détection de modification de fichiers/données sensibles ; -Sanctions à l'égard du référent.	-Les administrateurs "systèmes" qui ont accès à l'outil de traitement pour assurer sa maintenance n'ont pas accès aux alertes elles-mêmes.	-Entretiens.
	-Si oui à la question précédente, ces administrateurs ou prestataires de service se sont-ils engagés par voie contractuelle à respecter la confidentialité des informations auxquelles ils ont accès ?	-S'assurer que seules les personnes autorisées ont accès à l'outil de recueil et de traitement des signalements.	-AU 004 de la CNIL.	-Clauses de contrats inadaptées avec les prestataires de service ; -Habilitations des personnes extérieures non mises à jour.	-Contrats ; -Clauses contractuelles	-Perte de confidentialité ; -Risque de fuite d'informations confidentielles ; -Sanctions à l'égard du référent.	-Existence de clauses de confidentialité qui précise que les administrateurs ou prestataires se sont engagés à ne pas utiliser les données à des fins détournées, à assurer leur confidentialité, à respecter la durée de conservation limitée des données et à procéder à la destruction ou à la restitution de tous les supports manuels ou informatisés de données à caractère personnel au terme de sa prestation.	-Analyse de documents : vérifier la présence d'une clause spécifique à la confidentialité dans le contrat signé avec les prestataires / administrateurs qui ont accès aux données.

Sous-partie	Question	Finalité (objectifs de CI)	Référence normative	Risques			Ex. de bonnes pratiques	Mode opératoire
				Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts		
2.5.1. Sécurité des accès (suite)	-L'outil de traitement est-il protégé contre les risques d'intrusions internes et externes ?	-Être sûr qu'il existe un système de sécurité adapté permettant de protéger les données informatiques contre les pirates, les virus, les pannes électriques, la foudre…	-AU 004 de la CNIL.	-Destruction ou altération du matériel et/ou des fichiers ; -Obsolescence des équipements ; -Non-sécurisation externe du SI.	-Outil de traitement ; -Liste des différents dispositifs de sécurité ; -Procédure de mise à jour des moyens de sécurité.	-Perte d'informations confidentielles ; -Sanctions financières et pénales.	-Existence de moyens de protection des installations ; -Existence d'une protection contre les virus.	-Entretiens.
2.5.2. Sécurité du S.I.	-L'entreprise a-t-elle mise en œuvre des modalités d'évaluation du SI de gestion des alertes ?	-S'assurer que l'entreprise vérifie régulièrement le fonctionnement de l'outil.	-Exigences des autorités de tutelle.	-L'entreprise n'évalue pas le dispositif.	-Guide utilisation outil ; -Procédure d'évaluation du dispositif.	-Problème technique touchant l'outil, inconnu par l'entreprise ; -Absence de remontée d'alertes émises ; -Impossibilité d'améliorer le dispositif.	-Procéder au back testing de la robustesse du dispositif de signalement dans les établissements.	-Entretiens ; -Analyse de documents : analyser les comptes rendus des évaluations du SI de gestion des alertes.

Sous-partie	Question	Finalité (objectifs de CI)	Référence normative	Risques			Ex. de bonnes pratiques	Mode opératoire
				Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts		
3. Dispositif de contrôle interne								
3.1. Exhaustivité du plan de contrôle	-Est-ce que le plan de contrôle couvre l'exhaustivité du dispositif de lancement d'alerte ?	-S'assurer qu'il existe des contrôles pour l'ensemble des points majeurs règlementaires.	-Arrêté du 03 Novembre 2014 Article 11.	-Le plan de contrôle ne couvre pas l'ensemble des risques liés au dispositif ; -Les points de vérification, la taille des échantillons et les périodicités définis ne sont pas pertinents ; -Le plan de contrôle n'est pas à jour.	-Plan de contrôle.	-Mauvaise maîtrise et efficience du dispositif de signalement dans sa globalité ; -Méconnaissance et impossibilité de gérer les risques significatifs pouvant l'affecter.	-Le plan de contrôle est exhaustif et régulièrement mis à jour ; -Les points de contrôle sont définis ainsi que les personnes exécutant ces contrôles.	-Grille 10 (cf. Notice explicative des grilles d'analyse).
3.2. Efficience du dispositif de contrôle	-La fréquence des contrôles est-elle respectée ?	-S'assurer que les contrôles mis en place sont effectués.	-Arrêté du 03 Novembre 2014 Article 11.	-Les contrôles ne respectent pas la périodicité fixée dans le plan de contrôle.	-Fiche de contrôle ; -Piste d'audit.	-Perte de maitrise des risques.	-Existence d'un planning de contrôle. Les contrôles sont effectués selon le calendrier prévu par le plan de contrôle.	-Grille 11 (cf. Notice explicative des grilles d'analyse).

Sous-partie	Question	Finalité (objectifs de CI)	Référence normative	Risques			Ex. de bonnes pratiques	Mode opératoire
				Facteurs (scénarios d' empêchement)	Points de contrôle	Impacts		
3.2. Efficience du dispositif de contrôle (suite)	-La traçabilité des contrôles est-elle réalisée ?	-S'assurer que ces contrôles sont formalisés.	-Arrêté du 03 Novembre 2014 Article 11	-Absence d'une piste d'audit pour chaque contrôle ; -Piste d'audit impertinente.	-Pistes d'audit.	-Impossibilité pour l'audit et les autorités de réaliser des contrôles.	-Chaque contrôle et ses résultats sont retranscris dans une piste d'audit.	-Grille 11 (cf. Notice explicative des grilles d'analyse).
	-La fiabilité des contrôles est-elle avérée ?	-S'assurer que les éléments prévus par le plan de contrôle sont réalisés (ensemble des vérifications)	-Arrêté du 03 Novembre 2014 Article 11	-Les contrôles ne respectent pas le plan de contrôle ; -L'ensemble des points de vérification n'est pas contrôlé ; -L'échantillon est trop petit.	-Fiche de contrôle, -piste d'audit.	-Contrôles inefficaces ; -Risques non détectés ; -Impossibilité d'optimiser le dispositif.	-Les contrôles sont réalisés conformément à ce qui est prévu par le plan de contrôle.	-Grille 11 (cf. Notice explicative des grilles d'analyse).
3.3. Plans d'action	-Des plans d'action sont-ils formalisés et suivis efficacement ?	-Vérifier, qu'en cas de contrôle faisant apparaître des dysfonctionnements, des plans d'actions ont été mis en place et suivis.	-Arrêté du 03 Novembre 2014 Article 11.	-L'entité n'a pas défini d'actions correctrices ; -Les actions ne sont pas explicites et n'ont pas d'échéance ; -Les actions correctrices échues ne sont pas mises en œuvre.	-Plans d'action ; -Tableaux de suivi des plans d'action.	-Réitération des incidents et pertes associées.	-L'entité a défini et formalisé des actions correctrices et plans d'actions, ces actions sont explicites, avec des échéances, pertinentes et de nature à réduire ou éliminer le risque détecté ; -En cas d'actions correctrices échues non mises en œuvre, les raisons du retard sont déterminées.	-Grille 11 (cf. Notice explicative des grilles d'analyse).

IV- GRILLES D'ANALYSE

A. Notice explicative des grilles d'analyse

Grille 1 : Corps procédural

Objectif : s'assurer que toutes les procédures sont complètes et présentent les éléments imposés par la loi Sapin II.

Permet de répondre à la question du guide suivante : 1.2.1.

Mode opératoire : récupérer le corps procédural relatif au dispositif de lancement d'alerte et l'analyser. Pour répondre à la cinquième colonne de cette grille il convient de se référer au tableau 1.2 de la page suivante qui présente les éléments minimums attendus dans les procédures par la règlementation.

Pour remplir les cases il convient d'ouvrir la liste déroulante et de répondre par « Oui », « Non » ou « Non Applicable ». Cette grille est automatisée, elle totalise le nombre d'anomalies (réponses « Non ») et donne un taux de conformité (Nombre de « oui » / Nombre total de réponse).

Grille 2 : Modification du règlement intérieur

Objectif : s'assurer que l'entreprise a suivi toutes les étapes obligatoires lors de la modification du règlement intérieur pour y insérer le dispositif de lancement d'alerte.

Permet de répondre à la question du guide suivante : 1.2.2.

Mode opératoire : récupérer les preuves d'une modification légale du règlement intérieur et répondre par « Oui », « Non » ou « Non Applicable » aux questions de la grille. Cette grille est automatisée, elle totalise le nombre d'anomalies (réponses « Non ») et donne un taux de conformité (Nombre de « oui » / Nombre total de réponse).

Grille 3 : Pilotage et reporting

Objectif : s'assurer que l'instance dirigeante est destinatrice de reportings réguliers, complets et de qualité.

Permet de répondre aux questions du guide suivantes : 1.3.1 et 1.3.2.

Mode opératoire : récupérer les éléments de pilotage (tableaux de bord, présentations PowerPoint, etc.) et de reportings (comptes rendus de réunion, présentations PowerPoint, mails, etc.) et vérifier leur fréquence et leur contenu.

Pour remplir les cases il convient d'ouvrir la liste déroulante et de répondre par « Oui » ou « Non ». Cette grille est automatisée, elle totalise le nombre d'anomalies (réponses « Non ») et donne un taux de conformité (Nombre de « oui » / Nombre total de réponse).

Grille 4 : Respect des délais

Objectif : s'assurer que les délais de traitement de l'alerte imposés par la règlementation sont respectés.

Permet de répondre à la question du guide suivante : 2.1.2.

Mode opératoire : sélectionner un échantillon de cinq dossiers de signalement, et compléter les colonnes 1 à 5 et 8. Les colonnes 6, 7, 9, 10 et 11 se complètent automatiquement. La grille totalise le nombre de dossiers conformes (réponses « OK ») colonne 11 et donne un taux de conformité (Nombre de « OK » / Nombre total de réponse).

Éléments de règlementation :
Le référent doit informer le lanceur d'alerte "sans délai" de la réception de son alerte, il informe la personne visée par l'alerte dès l'enregistrement de données la concernant (lorsque des mesures conservatoires sont nécessaires, l'information de cette personne intervient après l'adoption de ces mesures.) et il traite le signalement dans un délai inférieur à 3 mois.

Grille 5 : Traitement des alertes

Objectifs :

- S'assurer que le traitement des alertes respecte ce qui est prévu par le scénario de correction correspond au type d'alerte ;
- S'assurer que l'alerte traitée était accompagnée de preuves recevables ;
- S'assurer en cas d'alerte faisant référence au domaine des ressources humaines, les instances représentatives du personnel ont été consultées.

Permet de répondre aux questions du guide suivantes : 2.1.2., 2.1.3. et 2.2.2.

Mode opératoire : sélectionner un échantillon de 5 dossiers de signalement et récupérer les scénarios de correction correspondant au type d'alerte. Pour chacun des échantillons constituer un tableau de la grille 3. Pour remplir les cases munies d'une étoile, se référer au scénario de correction et recopier les actions prévues par celui-ci (voir exemple Tableau 3.1.).

Pour compléter le tableau il convient d'ouvrir la liste déroulante et de répondre par « Oui » ou « Non ». Cette grille est automatisée, quand un « Non » est entré, la case conformité colonne 13 est

automatiquement « KO ». La grille totalise le nombre de dossiers conformes (réponses « OK ») colonne 13 et donne un taux de conformité (Nombre de « OK » / Nombre total de réponse).

Grille 6 : Qualité des informations

Objectifs : vérifier que les informations à la destination du lanceur d'alerte et de la personne visée par l'alerte sont complètes

Permet de répondre à la question du guide suivante : 2.1.2

Mode opératoire : sélectionner un échantillon de cinq dossiers de signalement et analyser les envois (courriers/mail, etc.) au lanceur d'alerte et à la personne visée par l'alerte.

Pour compléter le tableau il convient d'ouvrir la liste déroulante et de répondre par « Oui » ou « Non ». Cette grille est automatisée, quand un « Non » est entré, la case conformité colonne 7 est automatiquement « KO ». La grille totalise le nombre de dossiers conformes (réponses « OK ») colonne 7 et donne un taux de conformité (Nombre de « OK » / Nombre total de réponse).

Grille 7 : Formations

Objectifs :

- S'assurer que les collaborateurs ont effectué la formation spécifique aux lanceurs d'alerte (e-learning ou présentiel) ;
- S'assurer que les collaborateurs qui ont effectué la formation l'ont assimilé.

Permet de répondre à la question du guide suivante : 2.2.1.

Mode opératoire : sélectionner un échantillon de 20 collaborateurs, vérifier de quand date leur dernière formation et s'ils ont réussi l'évaluation de la formation. En fonction des réponses entrées dans les quatre premières colonnes remplir la cinquième par « OK » ou « KO ». Le tableau est automatisé, il calcule le taux de conformité en fonction du nombre d'échantillons conformes.

Grille 8 : Archivage

Objectifs :

- S'assurer que les informations collectées ne sont pas conservées au-delà de la date limite imposée par la loi Sapin II,
- S'assurer que les informations ont été rendues anonymes avant leur archivage.

Permet de répondre à la question du guide suivante : 2.4.1.

Mode opératoire : sélectionner un échantillon de cinq numéros de signalement. Vérifier qu'il n'existe plus de dossier correspondant au numéro. Accéder au système d'archivage, rechercher les dossiers archivés et les informations demandées par la grille. Dans la colonne « Suites possibles » un seul « Oui » est possible en fonction du cas de signalement, les deux autres sous-colonnes seront « NA » pour Non Applicable.

Pour remplir les cases il convient d'ouvrir la liste déroulante et de répondre par « Oui », « Non » ou « Non Applicable ». Cette grille est automatisée, elle totalise le nombre de dossiers conformes (réponses « OK ») colonne 9 et donne un taux de conformité (Nombre de « OK » / Nombre total de réponse).

Éléments de règlementation :
En cas de classement hors champ, les données doivent être immédiatement supprimées ou archivées après anonymisation.
En cas de classement sans suite, l'ensemble des éléments constitutifs du dossier de signalement doivent être détruits après anonymisation dans un délai de deux mois après la clôture des vérifications.
En cas de procédure disciplinaire ou de poursuites judiciaires engagées, les données relatives à l'alerte doivent être conservées pour une durée n'excédant pas le terme de la procédure.

Grille 9 : Complétude des dossiers de signalement

Objectif : s'assurer que les dossiers de signalement, montés par le référent, sont complets et qu'ils permettent la traçabilité des actions de traitement.

Permet de répondre à la question du guide suivante : 2.4.3.

Mode opératoire : sélectionner un échantillon de cinq dossiers de signalement et vérifier qu'ils contiennent les éléments minimums attendus.

Pour remplir les cases il convient d'ouvrir la liste déroulante et de répondre par « Oui », « Non » ou « Non Applicable ». Cette grille est automatisée, quand un « Non » est entré, la case conformité colonne 10 est automatiquement « KO ». La grille totalise le nombre de dossiers conformes (réponses « OK ») colonne 10 et donne un taux de conformité (Nombre de « OK » / Nombre total de réponse).

Grille 10 : Exhaustivité des contrôles

Objectifs :

- S'assurer que les principaux risques font l'objet d'un contrôle adapté,
- S'assurer que le plan de contrôle est détaillé

Permet de répondre à la question du guide suivante : 3.1.

Mode opératoire : à partir du plan de contrôle annuel, vérifier les éléments demandés par la grille.

Pour compléter le tableau il convient d'ouvrir la liste déroulante et de répondre par « Oui », « Non » ou « NA ». Cette grille est automatisée, quand un « Non » est entré, la case conformité colonne 10 est automatiquement « KO ». La grille totalise le nombre de dossiers conformes (réponses « OK ») colonne 10 et donne un taux de conformité (Nombre de « OK » / Nombre total de réponse).

Grille 11 : Efficience des contrôles

Objectifs : s'assurer que les contrôles sont effectués selon la fréquence indiquée dans le plan de contrôle, qu'ils sont fiables et qu'en cas d'anomalie constatée un plan d'action a été formalisé.

Permet de répondre aux questions du guide suivantes : 3.2. et 3.3.

Mode opératoire : accéder à l'outil de contrôle interne, pour chacun des contrôles relatifs aux dispositifs de lancement d'alerte vérifier que la fréquence est respectée. Pour s'assurer de la fiabilité du contrôle il convient d'effectuer le même contrôle et de vérifier si l'on arrive aux mêmes conclusions que l'unité en charge du contrôle. Si l'unité constate une anomalie elle doit avoir défini et formalisé des actions correctrices explicites et pertinentes dans un plan d'action. Il faut vérifier si ce plan d'action existe et pour répondre à la colonne pilotage il faut vérifier que les actions correctrices sont suivies.

Pour répondre aux colonnes « Fréquence » et « plans d'action », il faut ouvrir la liste déroulante et choisir « Oui », « Non » ou « NA ». Pour répondre à la fiabilité, il convient de faire dérouler la liste et de choisir la cotation fixée par l'unité et par l'audit (« Satisfaisant », « Convenable », « Insuffisant » ou « Dégradé »). Les colonnes « Conformité » se remplissent automatiquement par « OK » ou « KO » en fonction des réponses dans les cases précédentes. La grille totalise le nombre de dossiers conformes (réponses « OK ») et donne un taux de conformité (Nombre de « OK » / Nombre total de réponse).

B. Grilles d'analyse

Grille 1 : Corps procédural

Thème	**Existence de la procédure** ***(Oui/Non/NA)***	**Mise à jour récente (dans les 12 derniers mois)** ***(Oui/Non/NA)***	**Diffusion aux collaborateurs concernés** ***(Oui/Non/NA)***	**La procédure contient-elle les éléments minimums attendus* ?** ***(Oui/Non/NA)*** **Cf. Tableau ci-après**	**Avis Audit Interne global** ***(Oui/Non/NA)***	**Commentaires Audit Interne**
Règlementation						
Manuel d'utilisation du dispositif						
Rôles du référent						
Protection du lanceur d'alerte						
Scénarios de correction						
Nombre de oui						
Nombre de non						
Taux de conformité						

Tableau 1.1.

Grille 1 : Corps procédural (suite)

Procédures	**Éléments minimums attendus***
Note d'information Règlementation	*Textes de loi *Objectifs *Caractère facultatif du dispositif *Absence de conséquence de la non-utilisation du dispositif *Les types d'alerte, qui peut lancer une alerte
Manuel d'utilisation du dispositif	*L'identité du référent *Les 3 étapes de recueil des signalements *Comment adresser l'alerte (canaux de remontée), comment adresser une alerte de manière anonyme *Comment joindre les preuves *Comment le lanceur d'alerte doit transmettre le moyen de communiquer avec lui *Comment agir en situation de « danger grave et imminent ou en présence d'un risque de dommages irréversibles »
Rôles du référent	*Le référent doit informer sans délai le lanceur d'alerte de la réception de son alerte, du délai estimé pour son examen et de la façon dont il sera tenu informé des suites *Consultation des IRP (Institutions Représentatives du Personnel) dans le cas d'une alerte touchant au domaine RH *Contenu minimum du dossier de signalement (numéro de signalement, identité, fonctions et coordonnées du lanceur d'alerte et des personnes faisant l'objet d'une alerte, faits signalés, preuves, éléments recueillis dans le cadre de la vérification des faits signalés, compte rendu des opérations de vérification, suites données à l'alerte). *Le référent doit se référer aux scénarios de correction prévus pour traiter les alertes *Transmission de l'information de pertes éventuelles à la comptabilité pour passage à perte *Le référent n'enregistre que les catégories de données autorisées : - identité, fonctions et coordonnées de l'émetteur de l'alerte professionnelle; - identité, fonctions et coordonnées des personnes faisant l'objet d'une alerte ; - identité, fonctions et coordonnées des personnes intervenant dans le recueil ou dans le traitement de l'alerte ; - faits signalés ; - éléments recueillis dans le cadre de la vérification des faits signalés ; - compte rendu des opérations de vérification ; - suites données à l'alerte. *Les modalités d'archivage sont précisées dans la procédure.
Protection du lanceur d'alerte	*Comment l'organisme employeur garantit la stricte confidentialité de l'identité du lanceur d'alerte, des personnes visées, ainsi que des faits signalés.
Scénarios de correction	*Scénarios de correction pour les alertes majeures *Étapes spécifiques devant être réalisées pour traiter l'alerte en question *Définition des rôles *Validation de la direction

Tableau 1.2.

Grille 2 : Modification du règlement intérieur

Actions obligatoires lors de la modification du règlement intérieur	**Les actions ont été réalisées *(Oui/Non/NA)***	**Commentaires audit interne**
Consultation du CHSCT Comité d'Hygiène, de Sécurité et des Conditions de Travail		
Consultation du Comité d'Entreprise		
Transmission de la nouvelle version en double exemplaire à l'Inspection du travail accompagnée de l'avis des représentants du personnel		
Dépôt de la nouvelle version au greffe du Conseil de prud'hommes		
Communication de la modification du règlement intérieur à l'ensemble des salariés		
Nombre de oui		
Nombre de non		
Taux de conformité		

Grille 3 : Pilotage et reportings

Éléments de pilotage	**Ces éléments sont-ils suivis mensuellement par le référent ?** ***(Oui/Non/NA)***	**Les dirigeants effectifs sont-ils informés, à minima trimestriellement (reporting)** ***(Oui/Non/NA)***	**Commentaires audit interne**
Les faits signalés			
Le traitement des remontées			
Les suites des alertes			
Le suivi des actions de traitement			
Les pertes éventuelles			
Des données statistiques (ex : nombre d'alertes reçues, de dossiers clos, de dossiers ayant donné ou donnant lieu à une enquête, le nombre et le type de mesures prises pendant et à l'issue de l'enquête, etc.)			
Nombre de oui			
Nombre de non			
Taux de conformité			

Grille 4 : Respect des délais

Numéro de signalements	Destinataire du signalement	Le destinataire est-il adéquat ? *(Oui/Non)*	Date de réception de l'alerte	Date d'information du lanceur d'alerte de la réception de son alerte	Nombre de jours entre réception et accusé de réception	Date de traitement du signalement	Nombre de jours entre réception et traitement de l'alerte	Respect du délai de traitement du signalement	Conformité *(OK/KO)*

Nombre de OK	
Nombre de KO	
Taux de conformité	

Grille 5 : Traitement des alertes

n° de signalement	Scénario de correction	Présence de preuves recevables *(Oui/Non/NA)*	Les actions prévues par le scénario sont-elles effectuées ? *(Oui/Non/NA)*							Consultation des IRP		Conformité *(OK/KO)*
			*Évaluation des faits	*Informer le manager	*Entretien individuel avec la victime	*Informer les ressources humaines	*Consultation des IRP	*Licenciement de l'auteur	*Le fait signalé a été remonté à la direction	L'alerte fait-elle référence aux ressources humaines ? *(Oui/Non)*	*Les IRP ont-elles été consultées ? *(Oui/Non/NA)*	
Échantillon 1	Harcèlement sexuel											

Tableau 3.1.

n° de signalement	Scénario de correction	Présence de preuves recevables *(Oui/Non/NA)*	Les actions prévues par le scénario sont-elles effectuées ? *(Oui/Non/NA)*							Consultation des IRP		Conformité *(OK/KO)*
			*	*	*	*	*	*	*	L'alerte fait-elle référence aux ressources humaines ? *(Oui/Non)*	*Les IRP ont-elles été consultées ? *(Oui/Non/NA)*	
Échantillon 2	Fraude interne											

Tableau 3.2.

Nombre de OK	
Nombre de KO	
Taux de conformité	

Grille 6 : Qualité des informations

Information de la personne visée

Numéro de signalement	Date d'information de la personne visée	Cette information précise-t-elle : *(Oui/Non/NA)*				L'envoi est-il conforme aux règlementations ? *(OK/KO)*
		L'entité responsable du dispositif	Les faits qui sont reprochés	Les services destinataires de l'alerte	Les modalités d'exercice de ses droits d'accès et de rectification	

Information du lanceur d'alerte

Numéro de signalement	Date d'information du lanceur d'alerte	Cette information précise-t-elle : *(Oui/Non/NA)*		L'envoi est-il conforme aux règlementations ? *(OK/KO)*
		Délai estimé pour l'examen de l'alerte	Façon dont il sera tenu informé des suites	

Nombre de OK	
Nombre de KO	
Taux de conformité	

Grille 7 : Formations

Prénom Nom du collaborateur	**Poste**	**Date de la dernière formation lanceurs d'alerte**	**Réussite de l'évaluation de la formation *(Oui/Non/NA)***	**Conformité *(OK/KO)***	**Commentaires Audit Interne**

Nombre de OK	
Nombre de KO	
Taux de conformité	

Grille 8 : Archivage

	Suites possibles			Conservation des données				
Numéro de signalement	**Classement hors champ** *(Oui/NA)*	**Classement sans suite** *(Oui/NA)*	**Procédure disciplinaire ou poursuites judiciaires** *(Oui/NA)*	**Date de clôture des vérifications**	**Date de fin de procédure judiciaire**	**Date d'archivage**	**Anonymisation des données** *(Oui/Non/NA)*	**Les modalités d'archivage sont-elles conformes ?** *(OK/KO)*

Nombre de OK	
Nombre de KO	
Taux de conformité	

Grille 9 : Complétude des dossiers de signalement

Numéro de signalement	Les éléments suivants sont présents dans le dossier de signalement monté par le référent *(Oui/Non/NA)*								Conformité *(OK/KO)*
	Identité, fonctions et coordonnées de l'émetteur de l'alerte	Identité, fonctions et coordonnées de la/les personne(s) faisant l'objet de l'alerte	Fait signalé	Preuves	Traces des correspondances (avec l'émetteur et la personne faisant l'objet de l'alerte, ex : Courrier AR, mails, etc.)	Éléments recueillis dans le cadre de la vérification des faits signalés	Comptes rendus des opérations de vérification	Suites données à l'alerte	

Nombre de OK	
Nombre de KO	
Taux de conformité	

Grille 10 : Exhaustivité des contrôles

				Informations précisées par le contrôle ***(Oui/Non/NA)***					
Domaines à couvrir	***Risques à couvrir***	**Existence d'un contrôle**	**Référence**	**Le niveau de contrôle requis (1er ou 2ème degré)**	**La périodicité d'exercice**	**Le mode de sélection de l'échantillon**	**Points de vérification**	**Responsabilité du contrôle**	**Conformité du contrôle *(OK/KO)***
Recevabilité de l'alerte	*Preuves*		2455821						
Rôle du référent	*Respect des délais*		3353553						
	Utilisation des scénarios de correction		3545353						
	Qualité des informations transmises		4545765						
	Consultation IRP		1345345						
	Transmission des passages à perte		1579685						
	Contenu dossier signalement		7534878						
Protection du lanceur d'alerte	*Respect confidentialité*		1569753						

Nombre de OK	
Nombre de KO	
Taux de conformité	

Grille 11 : Efficience des contrôles

				Fréquence *(OK/ANO/NA)*					Fiabilité			Plans d'action *(Oui/Non/NA)*			
Thème	***Fréquence***	***Libellé***	***Réf. contrôle***	**T1 2017**	**T2 2017**	**T3 2017**	**T4 2017**	**Conformité fréquence *(OK/KO)***	**Constat unité**	**Constat audit**	**Conformité fiabilité *(OK/KO)***	**Existence de plan d'action**	**Pilotage du plan d'action**	**Conformité des plans d'action *(OK/KO)***	**Conformité globale *(OK/KO)***
Recevabilité de l'alerte	*Mensuelle*	*Preuves*	*2455821*												
Rôle du référent	*Trimestrielle*	*Respect des délais*	*3353553*												
	Trimestrielle	*Utilisation des scénarios de correction*	*3545353*												
	Semestrielle	*Qualité des informations transmises*	*4545765*												
	Semestrielle	*Consultation IRP*	*1345345*												
	Semestrielle	*Transmission des passages à perte*	*1579685*												
	Annuelle	*Contenu dossier signalement*	*7534878*												
Protection du lanceur d'alerte	*Mensuelle*	*Respect confidentialité*	*1569753*												

Conclusion

Ce mémoire s'était fixé comme objectif de répondre à la problématique suivante : comment a évolué le concept de lanceurs d'alerte en France et quels sont les risques liés aux dispositifs de recueil des signalements ?

Le concept est apparu pour la première fois aux États-Unis sous le nom de Whistleblowing. Il apparait en France par la loi Sarbanes Oxley puis est renforcé grâce à la loi Sapin II en 2016. Il existe des différences fondamentales entre Whistleblowing et lanceurs d'alerte, notamment concernant la manière dont ils sont perçus et leur rémunération.

La loi Sapin II a renforcé le statut des lanceurs d'alerte et leur protection, en obligeant les entreprises visées, à mettre en place des dispositifs d'alerte interne et de recueil des signalements et en infligeant des sanctions aux personnes qui s'opposent au traitement des alertes ou qui exercent des représailles à l'encontre des lanceurs d'alerte.

Cette loi s'est fixé l'objectif de prévenir et réduire la corruption. Cette recherche d'éthique devrait être une opportunité pour les organisations. Cela leur permettrait de communiquer sur leurs valeurs mais aussi de lutter contre les abus. Le benchmark a démontré que seulement deux entreprises sur six sont aujourd'hui en conformité avec la Loi Sapin II. De plus le questionnaire fait ressortir que 65% des interrogés ne sont pas au courant de l'existence d'un tel dispositif. Aujourd'hui les bénéfices de cette loi ne sont pas pris en compte par les entreprises. Ce retard dans la mise en conformité des entreprises peut s'expliquer par le fait que la loi n'a pas encore prévu de sanctions en cas de défaut de mise en œuvre de la procédure de recueil de signalement. Ceci vient remettre en question l'intention première de cette loi.

Ce concept peut causer des risques, clairement exprimés par les utilisateurs potentiels. La question d'une non utilisation de ces dispositifs se pose. Même si 92% ont déclaré utiliser le dispositif en cas de connaissance d'un fait répréhensible cité par la loi Sapin II, 73% ont exprimé des craintes à l'égard de ces dispositifs. L'utilisation de ces dispositifs n'est donc pas si évidente. Les éléments les plus redoutés sont les représailles, une mauvaise protection et le non-respect de la confidentialité. A ces craintes s'ajoute des risques liés à la règlementation.

Pour que ces dispositifs soient utilisés à bon escient, il est important que l'entreprise mette en œuvre un plan d'animation du dispositif pour faire adhérer les utilisateurs potentiels à la démarche de signalement. L'audit interne aura un rôle clé, puisqu'il devra contrôler le dispositif et veiller à sa

conformité avec la loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

Le travail que j'ai réalisé pourrait être complété et poursuivi sous différents aspects. Il serait pertinent d'étendre la recherche sur le risque que le dispositif soit à l'origine d'une nouvelle forme de corruption : corrompre pour ne pas être dénoncé. Ceci relance le débat introduit par le sociologue Edward Gross, à savoir : « les organisations, par leur motivation au profit et leur gestion par objectifs, ne sont-elles pas criminogènes, c'est-à-dire qu'elles poussent au comportement criminel et notamment à la fraude ? »

Bibliographie

Sites web :

Alertes professionnelles et loi Sapin 2 : extension de l'autorisation unique AU-004 par la CNIL ; Ludovique Clavreul et Maxime Hanriot [en ligne]. Les Échos Executives, 2017, [Consulté le 11 juillet 2018]. Disponible sur : https://business.lesechos.fr/directions-ressources-humaines/partenaire/partenaire-1288-alertes-professionnelles-et-loi-sapin-2-extension-de-la-autorisation-unique-au-004-par-la-cnil-315799.php

Autorisation unique AU-004 [en ligne]. CNIL, 2017, [Consulté le 1 juillet 2018]. Disponible sur : https://www.cnil.fr/fr/declaration/au-004-dispositif-dalertes-professionnelles

D'Einstein aux Panama papers, une brève histoire du mot "lanceur d'alerte" ; Chloé Leprince [en ligne]. France Culture, 2016, [Consulté le 31 juillet 2018]. Disponible sur : https://www.franceculture.fr/histoire/d-einstein-aux-panama-papers-une-breve-histoire-du-mot-lanceur-d-alerte

Délibération n°2017-191 du 22 juin 2017 [en ligne]. Légifrance, 2017, [Consulté le 6 juillet 2018]. Disponible sur : https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000035459127&fastReqId=386645448&fastPos=1

Dispositif d'alerte interne ; Agence Française Anticorruption [en ligne]. Economie.gouv, 2017, [Consulté le 2 juillet 2018]. Disponible sur : https://www.economie.gouv.fr/files/files/directions_services/afa/2017-10-04_-_Dispositif_dalerte_interne_vd.pdf

Former et sensibiliser en interne ; Agence Française Anticorruption [en ligne]. Economie.gouv, 2017, [Consulté le 6 juillet 2018]. Disponible sur : https://www.economie.gouv.fr/files/files/directions_services/afa/2017_-_Recommandations_AFA.pdf

Guide pratique : le dispositif anticorruption de la loi Sapin II [en ligne]. MEDEF Mouvement des entreprises de France, 2017, [Consulté le 6 juillet 2018]. Disponible sur : http://www.medef.com/fr/content/guide-pratique-dispositif-anticorruption-de-la-loi-sapin-ii

La corruption : définition et sanctions [en ligne]. Droit-Finances, 2018, [Consulté le 14 août 2018]. Disponible sur : https://droit-finances.commentcamarche.com/contents/1320-la-corruption-definition-et-sanctions

La protection des lanceurs d'alerte : extension du domaine de la lutte contre les discriminations ; Clara Gandin et Xavier Sauvignet [en ligne]. Village de la justice, 2018, [Consulté le 11 juillet 2018]. Disponible sur : https://www.village-justice.com/articles/protection-des-lanceurs-alerte-extension-domaine-lutte-contre-les,28360.html

Lanceur d'alerte d'hier et d'aujourd'hui ; Patrice Cailleba [en ligne]. Les Échos, 2016, [Consulté le 31 juillet 2018]. Disponible sur : http://archives.lesechos.fr/archives/cercle/2016/07/22/cercle_159136.htm

Lanceur d'alerte et recueil des signalements : ce que dit la nouvelle loi ; Nicolas Lepetit [en ligne]. Les Échos, 2017, [Consulté le 1er août 2018]. Disponible sur : https://www.lesechos.fr/idees-debats/cercle/030845187344-lanceur-dalerte-et-recueil-des-signalements-ce-que-dit-la-nouvelle-loi-2128488.php

Lanceur d'alerte : mise en place du recueil des signalements des lanceurs d'alerte au 1er janvier 2018 ; Rédaction des Éditions Tissot [en ligne]. Éditions Tissot, 2017, [Consulté le 2 juillet 2018]. Disponible sur : https://www2.editions-tissot.fr/actualite/droit-du-travail/lanceur-d-alerte-mise-en-place-du-recueil-des-signalements-des-lanceurs-d-alerte-au-1er-janvier-2018

Lanceurs d'alerte : quelles nouvelles obligations pour l'entreprise ? ; Direction de l'information légale et administrative [en ligne]. Service Public Pro, 2017, [Consulté le 2 juillet 2018]. Disponible sur : https://www.service-public.fr/professionnels-entreprises/actualites/A12221

Lanceurs d'alerte : ce que prévoit la nouvelle loi ; Gilles Marchand [en ligne]. Focus RH, 2017, [Consulté le 9 juillet 2018]. Disponible sur : https://www.focusrh.com/strategie-rh/organisation-et-conseil/lanceurs-d-alerte-ce-que-prevoit-la-nouvelle-loi-30096.html

Lanceurs d'alerte : comment ils ont osé sacrifier leur carrière ; Bruno Askenazi [en ligne]. Capital avec management, 2017 [Consulté le 26 juin 2018]. Disponible sur : https://www.capital.fr/votre-carriere/lanceurs-dalertes-comment-ils-ont-ose-sacrifier-leur-carriere-1263149

Lanceurs d'alerte : concrètement, comment respecter l'obligation de recueil des signalements ? ; Pauline Chambost [en ligne]. Éditions législatives, 2018 [Consulté le 14 août 2018]. Disponible

sur : http://www.editions-legislatives.fr/content/lanceurs-d%E2%80%99alerte-concr%C3%A8tement-comment-respecter-l%E2%80%99obligation-de-recueil-des-signalements

Lanceurs d'alerte : les entreprises ont jusqu'au 1er janvier 2018 pour mettre en place le dispositif de signalement ; Eric A. CAPRIOLI [en ligne]. L'Usine Digitale, 2017, [Consulté le 2 juillet 2018]. Disponible sur : https://www.usine-digitale.fr/article/lanceurs-d-alerte-les-entreprises-ont-jusqu-au-1er-janvier-2018-pour-mettre-en-place-le-dispositif-de-signalement.N597483

Lanceurs d'alerte [en ligne]. France Diplomatie, 2018, [Consulté le 2 juillet 2018]. Disponible sur : https://www.diplomatie.gouv.fr/fr/le-ministere-et-son-reseau/lanceurs-d-alerte/

Lanceurs d'alerte [en ligne]. Grant Thornton, 2018, [Consulté le 10 août 2018]. Disponible sur : https://www.grantthornton.fr/fr/service/conseil-operationnel-et-outsourcing/sapin-2/lanceurs-dalerte/

Lanceurs d'alerte et handicap : poursuivre le combat ! ; Emmanuelle Dal'Secco [en ligne]. Handicap.fr, 2017 [Consulté le 24 juin 2018]. Disponible sur : https://informations.handicap.fr/art-lanceur-alerte-boussie-853-10386.php

Lanceurs d'alerte, histoire d'un concept ; Frédéric Joignot [en ligne]. Journalisme pensif, 2013, [Consulté le 31 juillet 2018]. Disponible sur : http://fredericjoignot.blog.lemonde.fr/2013/09/15/lanceurs-dalerte-whistleblower-histoire-dun-concept/

Le lanceur d'alerte et la loi Sapin II ; Brigitte Pereira [en ligne]. Les Échos, 2017, [Consulté le 3 août 2018]. Disponible sur : https://www.lesechos.fr/idees-debats/cercle/cercle-165291-le-lanceur-dalerte-et-la-loi-sapin-ii-2059339.php#formulaire_enrichi::bouton_linkedin_inscription_article

Les alertes professionnelles en question [en ligne]. CNIL, 2011, [Consulté le 9 juillet 2018]. Disponible sur : https://www.cnil.fr/fr/les-alertes-professionnelles-en-questions-0

Les solutions pour une ligne de lanceur d'alerte [en ligne]. iScope, 2017, [Consulté le 10 août 2018]. Disponible sur : http://www.ethiquedesorganisations.com/ligne-de-lanceur-d-alerte.html

Loi n°2016-1690 du 8 décembre 2016 – art. Unique, Titre II : dispositions relatives aux compétences et à la saisine du défenseur des droits [en ligne]. Légifrance, 2016, [Consulté le 6 juillet 2018]. Disponible sur : https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=8B1F58C8E30167E60FC225

67DA0F996C.tplgfr41s_3?cidTexte=JORFTEXT000033558526&idArticle=LEGIARTI000033562616&dateTexte=20180808&categorieLien=id#LEGIARTI000033562616

Loi Sapin 2 : un socle commun pour les lanceurs d'alerte ; Virginie Bensoussan-Brulé [en ligne]. Lexing Alain Bensoussan Avocats, 2017, [Consulté le 3 août 2018]. Disponible sur : https://www.alain-bensoussan.com/avocats/lanceurs-dalerte-avec-la-loi-sapin-2/2017/06/27/

Loi Sapin II : Les lanceurs d'alerte ; Matthieu Hénon [en ligne]. Seban & Associés, 2017, [Consulté le 1er août 2018]. Disponible sur : http://www.seban-associes.avocat.fr/loi-sapin-ii-lanceurs-dalerte/

Pourquoi le statut de lanceur d'alerte sera difficile à obtenir ; Marianne Rey [en ligne]. L'Express l'entreprise, 2016, [Consulté le 10 août 2018]. Disponible sur : https://lentreprise.lexpress.fr/rh-management/droit-travail/pourquoi-le-statut-de-lanceur-d-alerte-sera-difficile-a-obtenir_1838699.html

Pourquoi les entreprises ne recrutent-elles pas les lanceurs d'alerte ; Thierry Nadisic et Tessa Melkonian [en ligne]. EM Lyon Business School, 2016 [Consulté le 14 juin 2018]. Disponible sur : http://knowledge.em-lyon.com/pourquoi-les-entreprises-ne-recrutent-elles-pas-les-lanceurs-dalerte/

Retour sur l'obligation de modifier le règlement intérieur pour y intégrer un code de conduite anti-corruption (loi sapin 2) ; Sébastien Millet [en ligne]. Préventica, 2017 [Consulté le 14 août 2018]. Disponible sur : https://www.preventica.com/actu-chronique-obligation-modifier-code-travail-anti-corruption.php

Tout savoir sur la loi #Sapin2 [en ligne]. Economie.gouv.fr, 2017, [Consulté le 1er août 2018]. Disponible sur : https://www.economie.gouv.fr/transparence-lutte-contre-corruption-modernisation

Visa de sécurité [en ligne]. ANSSI, 2018, [Consulté le 14 août 2018]. Disponible sur : https://www.ssi.gouv.fr/entreprise/visa-de-securite/

Article de revue :

GEORGES, Thierry. « Lanceurs d'alerte », Revue Banque, Banque & Droit : Loi Sapin 2, décembre 2017, pages 21 à 23.

Livres :

SCHICK Pierre, VERA Jacques, BOURROUILH-PAREGE Olivier. Audit interne et référentiels de risques, 2e édition, Paris, Edition DUNOD, coll. « Fonctions de l'entreprise », 2014, 355 pages.

BOUCHET Jean Paul, AUBERGER Marie Noëlle. Oser l'alerte, Edition Atelier Ed De L', coll. Social Eco. H.c., 2018, 160 pages.

ANNEXES

Annexe 1 : Informations autorisées par la CNIL

L'autorisation unique AU-004, distribuée par la CNIL, oblige les référents à ne traiter que certaines catégories de données. Il s'agit des suivantes :

- Identité, fonctions et coordonnées de l'émetteur de l'alerte professionnelle ;
- Identité, fonctions et coordonnées des personnes faisant l'objet d'une alerte ;
- Identité, fonctions et coordonnées des personnes intervenant dans le recueil ou dans le traitement de l'alerte ;
- Faits signalés ;
- Éléments recueillis dans le cadre de la vérification des faits signalés ;
- Compte rendu des opérations de vérification ;
- Suites données à l'alerte.

Toutes autres informations ne doivent pas être conservées par le référent.

Annexe 2 : Contextualisation de l'enquête

Ce mémoire m'a mené à réaliser une enquête afin de récolter l'avis de l'opinion publique, lanceurs d'alerte potentiels, sur un tel dispositif. L'objectif principal est de savoir s'ils ont connaissance d'un tel dispositif au sein de leur entreprise, s'ils seraient prêts à l'utiliser et quels seraient leurs freins. Il s'agit d'un questionnaire de dix questions qui a été diffusé sur le réseau professionnel LinkedIn et sur le réseau social Facebook du 7 août 2018 au 20 août 2018.

Quand une personne clique sur le lien du questionnaire, ce message explicatif s'affiche en introduction :

Bonjour, vous allez répondre à un questionnaire sur les lanceurs d'alerte en entreprise. Il n'est composé que de dix questions et ne vous prendra que 4 minutes.

Pour vous éclairer sur le sujet, le dispositif de recueil des alertes est une obligation prévue par la loi Sapin 2. Il permet aux salariés d'une entreprise de remonter, à une personne désignée, des faits de corruption, un délit, un crime, une menace ou un préjudice grave pour l'intérêt général qui a lieu au sein de l'entreprise. La confidentialité de l'identité du lanceur d'alerte est assurée, il peut aussi remonter un fait de manière anonyme.

Merci pour votre aide.

OK

Ci-dessous questionnaire dans son intégralité (les questions précédées d'une étoile * signifient que leur réponse est obligatoire pour valider le questionnaire) :

* 1. Connaissez-vous le concept de lanceurs d'alerte en entreprise?

- ◯ Je connais très bien et je sais que c'est une obligation pour certaines entreprises de mettre en place un dispositif de remontée des signalements.
- ◯ J'en ai déja entendu parler mais j'ai peu de connaissance à ce sujet.
- ◯ Je n'en ai jamais entendu parler.

* 2. Avez-vous connaissance d'un dispositif de signalement d'alerte au sein de votre entreprise ?

- ◯ Oui
- ◯ Non

* 3. Si oui à la question 2, avez-vous déjà utilisé ce dispositif pour signaler un fait ?

- ◯ Oui
- ◯ Non
- ◯ Non concerné(e)

* 4. Si oui, à la question 3, quel type d'alerte avez-vous signalée ?

- ◯ Cas de corruption
- ◯ Délit
- ◯ Crime
- ◯ Violation d'un engagement international
- ◯ Trafic d'influence
- ◯ Non concerné(e)
- ◯ Autre (veuillez préciser)

5. Seriez-vous prêt à utiliser le dispositif en cas de connaissance d'un fait de corruption, de trafic d'influence, d'un crime, d'un délit ou autre au sein de votre entreprise ? (votre confidentialité étant assurée)

- ◯ Oui
- ◯ Non

* 6. Pour quelle(s) raison(s) ne seriez-vous pas prêt à émettre une alerte ?

7. Quel(s) risque(s) associez-vous à la mise en place d'un tel dispositif ?

* 8. Dans quel secteur travaillez-vous actuellement ou avez-vous travaillé lors de votre dernier emploi ?

- ◯ Automobile
- ◯ Agriculture
- ◯ Agroalimentaire
- ◯ Assurance et protection sociale
- ◯ BTP, habitat social et urbanisme
- ◯ Distribution
- ◯ Banque, finance et comptabilité
- ◯ Franchise
- ◯ Economie sociale et solidaire
- ◯ Education, formation et recherche
- ◯ Energie et ressources naturelles
- ◯ Industries chimique et pharmaceutique
- ◯ Luxe
- ◯ Médias
- ◯ Santé, sanitaire et social
- ◯ Secteur public
- ◯ Services aux collectivités
- ◯ Technologies
- ◯ Télécommunications
- ◯ Tourisme - hôtellerie et loisirs
- ◯ Transports
- ◯ Autre (veuillez spécifier)

* 9. Quelle est la taille de l'entreprise dans laquelle vous travaillez actuellement ou avez-vous travaillé lors de votre dernier emploi ?

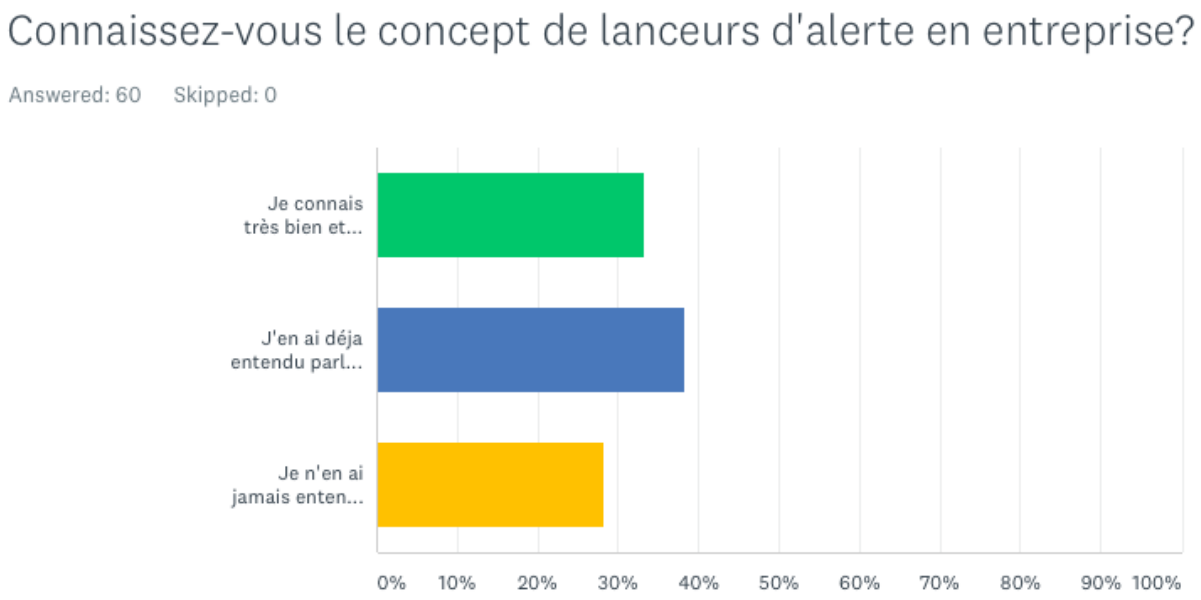
- ◯ Moins de 50 salariés
- ◯ Entre 50 et 500 salariés
- ◯ Plus de 500 salariés

* 10. Dans quelle tranche d'âge vous situez-vous?

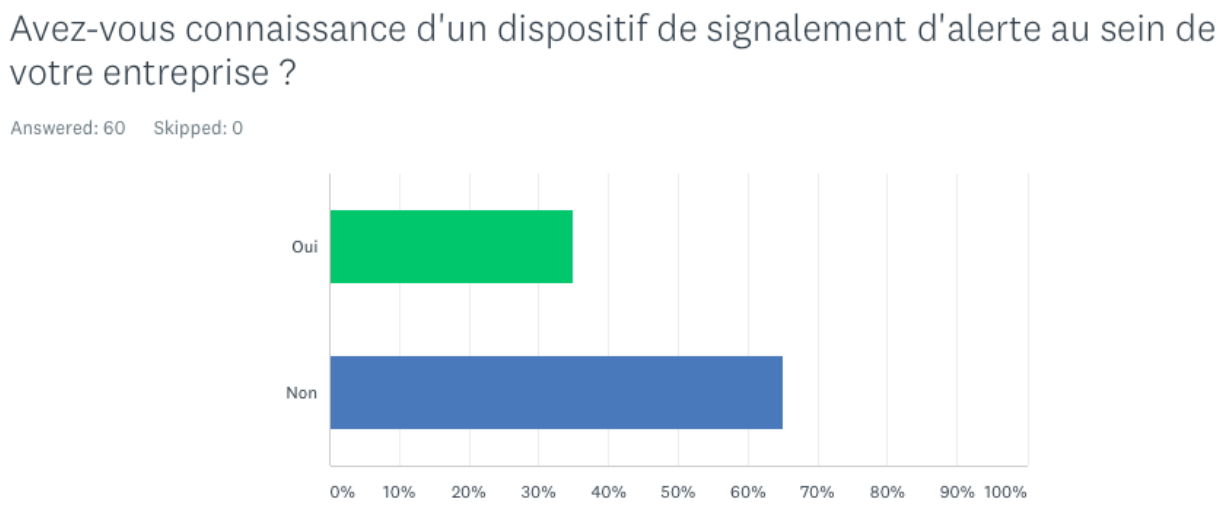
- ◯ Moins de 20 ans
- ◯ Entre 20 et 30
- ◯ Entre 31 et 50
- ◯ Entre 51 et 65
- ◯ 66 ans et plus

Annexe 3 : Résultats de l'enquête

Question 1 :



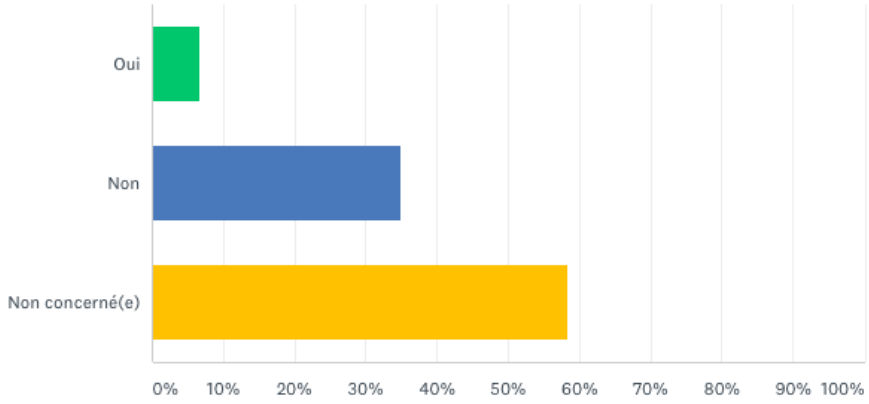
Question 2 :



Question 3 :

Si oui à la question 2, avez-vous déjà utilisé ce dispositif pour signaler un fait ?

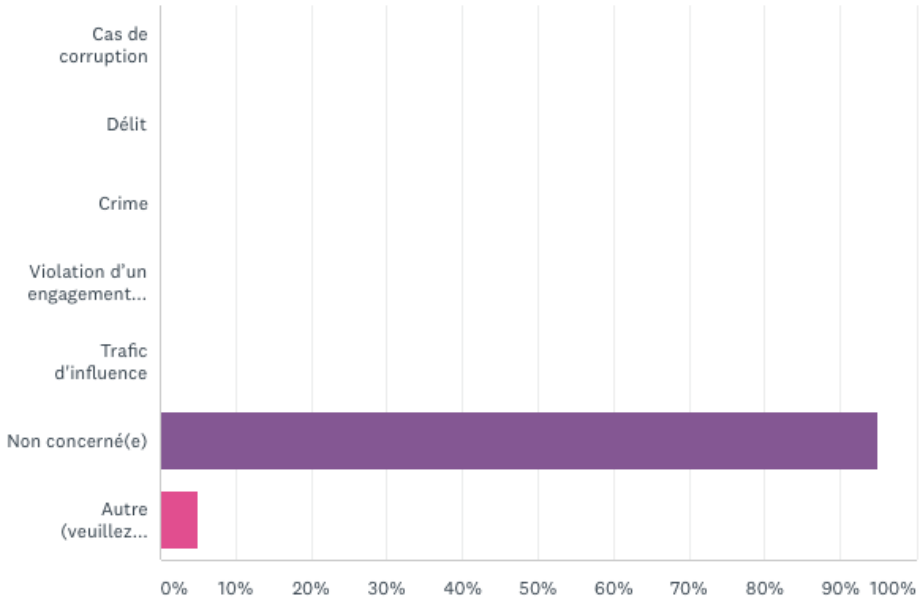
Answered: 60 Skipped: 0



Question 4 :

Si oui, à la question 3, quel type d'alerte avez-vous signalée ?

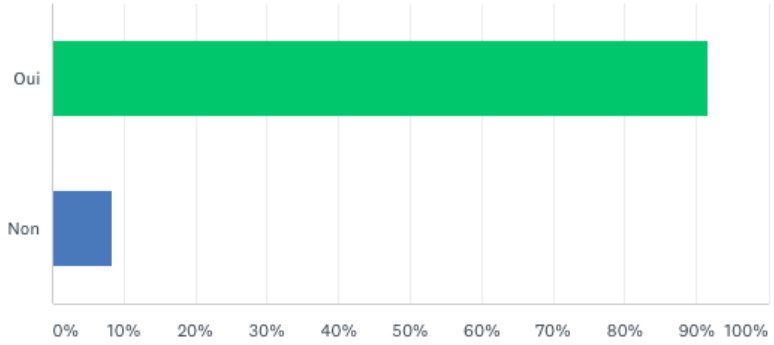
Answered: 60 Skipped: 0



Question 5 :

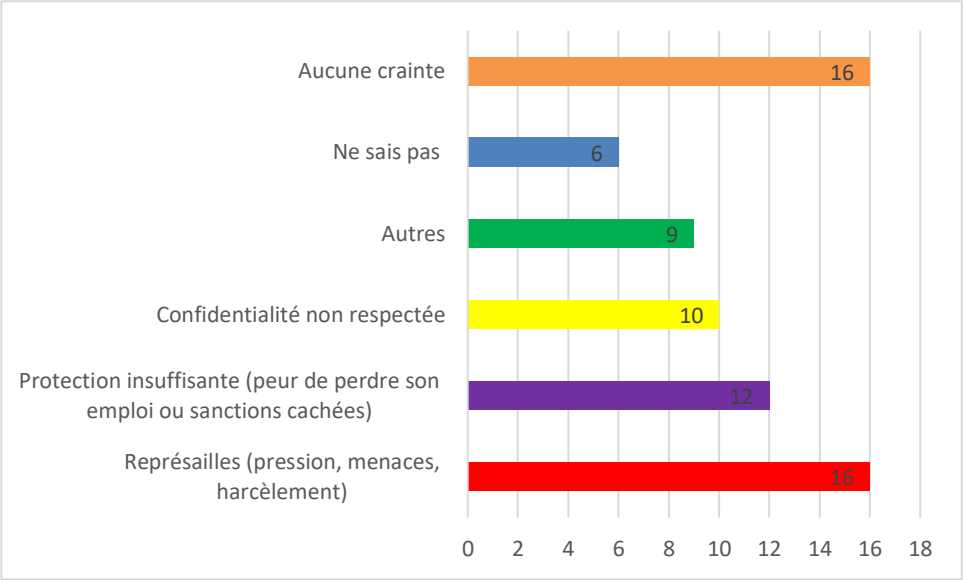
Seriez-vous prêt à utiliser le dispositif en cas de connaissance d'un fait de corruption, de trafic d'influence, d'un crime, d'un délit ou autre au sein de votre entreprise ? (votre confidentialité étant assurée)

Answered: 60 Skipped: 0



Question 6 :

Pour quelle(s) raison(s) ne seriez-vous pas prêt à émettre une alerte ?



Question 7 :

Quel(s) risque(s) associez-vous à la mise en place d'un tel dispositif ?

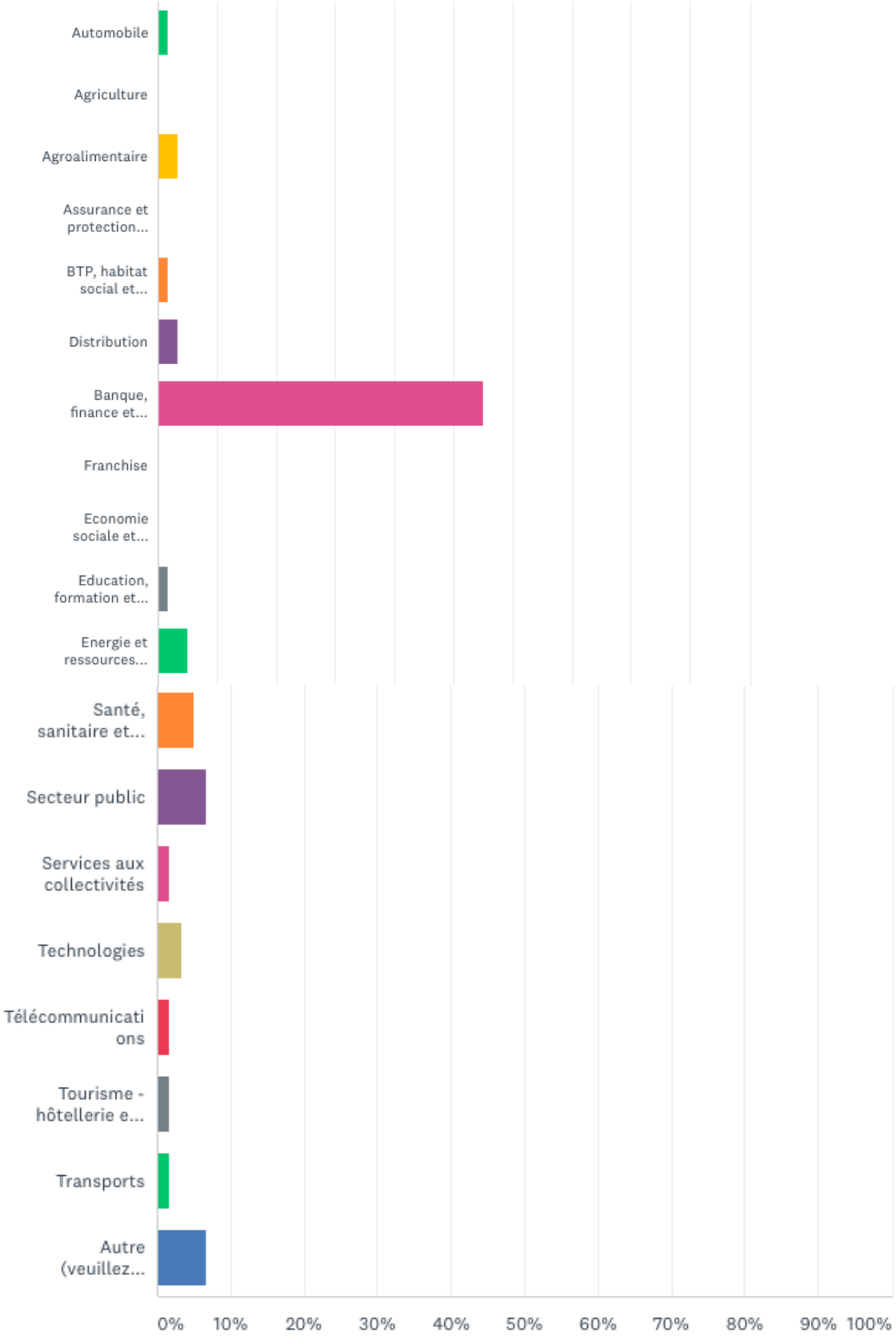
- Licenciement
- La division des équipes , collègues de boulot ...
- Harcèlement si anonymat non respecté
- Que la confidentialité ne soit pas respectée. Que le dispositif soit utilisé dans de mauvais cas

- Fausse accusation
- Risque de fuite du nom des dénonciateurs / perte anonymat
- Licenciement, abus de pouvoir...
- Mauvaise ambiance dans l'entreprise
- perte de confiance, méfiance...
- Un risque de blocage dans la remontée de l'alerte (non transmission) ou de non traitement par la personne désignée que ce soit par malveillance ou oubli
- abus du dispositif, déclenchement non justifié
- Le principal risque est l'abus qui peut en être fait notamment en dénonçant des personnes innocentes uniquement pour servir ses propres intérêts.
- fausses alertes
- Peur de représailles internes Regard des autres Risques de sanctions cachées (non promotion ou bonus diminué ou non versé, etc.)
- Dépression angoisse Perte de l'emploi
- Se faire virer
- Risque d'erreur d'interprétation ou une connaissance partielle des faits menant à une fausse alerte
- Anonymat non garanti
- Représailles
- Trafic d'influence et risques de corruption
- Fraude interne et externe notamment (impliquant la corruption). Aussi le non-respect de normes de conformité qui par mon jugement pourrait mettre vraiment en danger des personnes.
- Dégradation de l'image de la société et des collaborateurs. Liquidation de la société.
- délation
- perte d'emploi
- Le coût du dispositif
- protection insuffisante des lanceurs d'alerte
- Risque d'image, risque financier
- système de délation
- Risque d'image
- Délation
- Délation, alerte trop rapide
- harcèlement, influence, corruption
- Risque humain, perte financière et de dignité
- Risque d'erreur
- Dénonciations calomnieuses, voire infondées. Dénonciations jugées injuste, et parfois subjectives.
- Délation abusive
- utilisation abusive
- Des dénonciations calomnieuses

Question 8 :

Dans quel secteur travaillez-vous actuellement ou avez-vous travaillé lors de votre dernier emploi ?

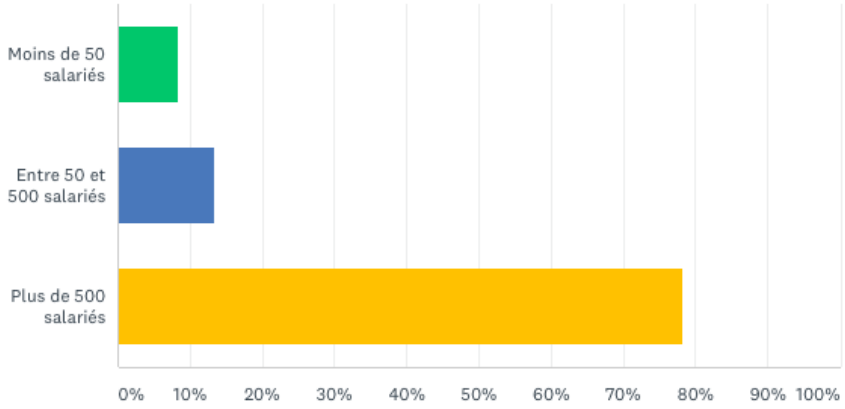
Answered: 60 Skipped: 0



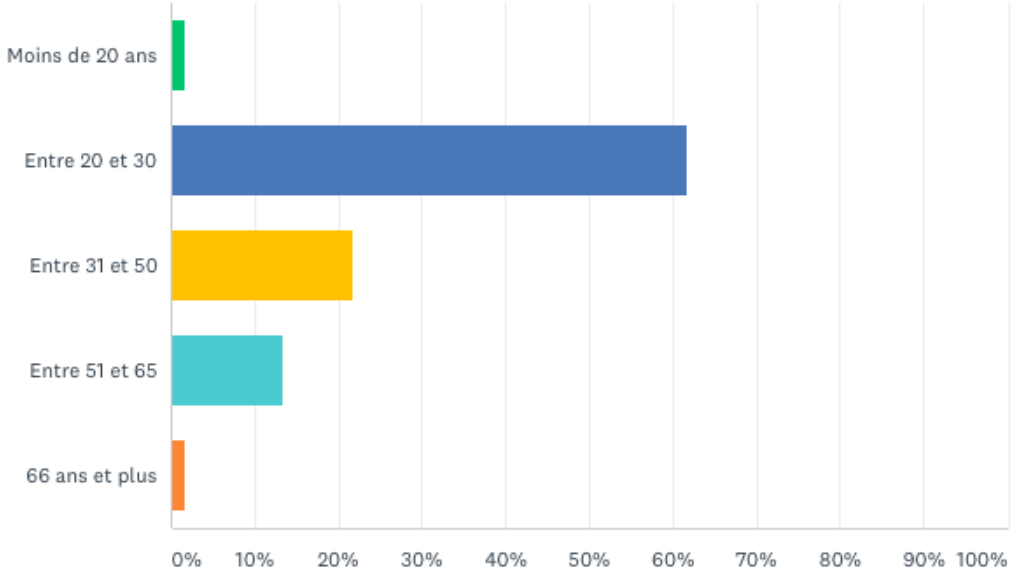
Question 9 :

Quelle est la taille de l'entreprise dans laquelle vous travaillez actuellement ou avez-vous travaillé lors de votre dernier emploi ?

Answered: 60 Skipped: 0



Question 10 :

Dans quelle tranche d'âge vous situez-vous?

Answered: 60 Skipped: 0