



**GUIDE**  
**DISPOSITIF**  
**D'ALERTE INTERNE**

# SOMMAIRE

<b>PROPOS LIMINAIRES</b> .....	<b>3</b>
<b>FICHE 1 : RÉGIME JURIDIQUE</b> .....	<b>5</b>
1. Pourquoi mettre en place une procédure interne de recueil et de traitement des signalements ?.....	5
2. Comment mettre en place une procédure interne de recueil et de traitement des signalements ?.....	8
3. Le rôle du Défenseur des droits.....	13
<b>FICHE 2 : RECUEIL ET TRAITEMENT DE LA RECEVABILITÉ DU SIGNALEMENT</b> .....	<b>14</b>
1. Les modalités de recueil des signalements.....	14
2. Les modalités de traitement de la recevabilité des signalements recueillis.....	15
3. La personne en charge de la procédure de recueil et de traitement.....	15
4. Les délais d'information de l'auteur du signalement et des personnes visées par le signalement.....	16
5. La recevabilité du signalement.....	17
<b>FICHE 3 : EXAMEN DU SIGNALEMENT</b> .....	<b>18</b>
1. Analyse et vérification des allégations et enquête interne.....	18
2. Principes à respecter.....	19
<b>FICHE 4 : CLÔTURE DE LA PROCÉDURE</b> .....	<b>21</b>
<b>FICHE 5 : SUITES À DONNER À L'ALERTE</b> .....	<b>22</b>
1. Clôture sans suite.....	22
2. Clôture avec suite.....	22
<b>FICHE 6 : LES SOLUTIONS D'EXTERNALISATION DES DISPOSITIFS DE RECUEIL ET DE TRAITEMENT DES ALERTES</b> .....	<b>24</b>
<b>FICHE 7 : POUR ALLER PLUS LOIN</b> .....	<b>26</b>

---

## CONTRIBUTEURS :

Carmen BRICENO  
Jean-Yves TROCHON  
Iohann LE FRAPPER  
Nathalie KALESKI  
Wafa AYED

Copyright couverture :  
© Shivendu Jauhari  
istockphoto.com

---

**ÉDITION** : Mars 2025

# I PROPOS LIMINAIRES

La réglementation visant à protéger les lanceurs d'alerte en France et en Europe est relativement récente.

Parmi les instruments juridiques internationaux fondateurs se trouvent la Convention civile sur la corruption du Conseil de l'Europe de 1999<sup>1</sup> et la Convention des Nations Unies contre la corruption de 2003<sup>2</sup>. Ces Conventions imposent aux États Parties l'obligation d'établir dans leur droit interne des mesures appropriées permettant d'assurer une protection adéquate aux « *personnes qui communiquent des informations* » de bonne foi et sur la base de soupçons raisonnables.

Une prise de conscience du besoin d'harmonisation et de renforcement de la protection des lanceurs d'alerte a pris forme à la suite du rapport publié en 2009 par la commission des questions juridiques et des droits de l'homme de l'Assemblée parlementaire du Conseil de l'Europe. Ce rapport soulignait des divergences significatives de traitement de la question entre les différents États membres principalement attribuées à l'absence d'une culture de signalement positive<sup>3</sup>. En réponse, en 2010, l'Assemblée a adopté la Résolution 1729<sup>4</sup>, invitant les États membres à revoir leur législation en matière de protection des « *donneurs d'alerte* », en gardant à l'esprit les principes directeurs stipulés dans cet instrument ainsi que dans la Recommandation 1916<sup>5</sup> demandant au Comité des Ministres de créer des lignes directrices pour la protection des donneurs d'alerte.

Les travaux du Groupe d'États contre la corruption (GRECO) ont permis également de maintenir la protection des lanceurs d'alerte parmi les priorités européennes.

En avril 2014, le Conseil de l'Europe a publié une recommandation concernant la protection des « *lanceurs d'alerte* »<sup>6</sup>. Cette recommandation reconnaît l'alerte comme un élément essentiel du respect de la vie privée, de la liberté d'expression et de la liberté de conscience. Elle souligne également le rôle important que jouent les lanceurs d'alerte dans les secteurs public et privé pour dissuader et prévenir les actes répréhensibles, ainsi que pour renforcer la responsabilité et la transparence démocratiques.

La Directive 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 concernant la protection des personnes qui signalent des violations du droit de l'Union (« Directive lanceurs d'alerte ») s'est inspirée largement des principes établis par la recommandation du Conseil de l'Europe. La jurisprudence de la Cour européenne des droits de l'homme (CEDH) relative au droit à la liberté d'expression a également influencé cette directive.

En France, la notion de « lanceur d'alerte » a été introduite à la fin des années 1990 par les sociologues Francis Châteauraynaud et Didier Torny<sup>7</sup>. En 2007, une loi<sup>8</sup> relative à la lutte contre la corruption a introduit dans le droit du travail (article L1161-1 du Code du Travail) une disposition protectrice des salariés qui témoignent de bonne foi de faits de corruption : première introduction de la notion de lanceur d'alerte dans le droit français mais sans toutefois mentionner le terme de « lanceur d'alerte ».

<sup>1</sup> Convention civile sur la corruption, Strasbourg, 4.XI.1999.

<sup>2</sup> Résolution 58/4 de l'Assemblée générale du 31 octobre 2003, Article 33.

<sup>3</sup> Commission des questions juridiques et des droits de l'homme, Doc. 12006 du 4 septembre 2009 : <https://pace.coe.int/fr/files/12302/html>

<sup>4</sup> Assemblée Parlementaire Résolution 1729 (2010) : <https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-FR.asp?fileid=17851&lang=FR>

<sup>5</sup> Assemblée Parlementaire du Conseil de l'Europe, Recommandation 1916/2010 : <https://pace.coe.int/fr/files/17852/html>

<sup>6</sup> Conseil de l'Europe, Recommandation CM/Rec (2014) <https://rm.coe.int/16807096c8>

<sup>7</sup> « *Les sombres précurseurs. Une sociologie pragmatique de l'alerte et du risque* », Éditions EHESS, Paris 1999.

<sup>8</sup> Loi n° 2007-1598 du 13 novembre 2007 relative à la lutte contre la corruption (article 9).

En 2013, la loi dite « Blandin »<sup>9</sup> a défini le terme de lanceur d'alerte, mais cette définition était limitée à la santé publique et à l'environnement.

C'est en 2016 que la France, par l'adoption de la Loi Sapin II<sup>10</sup>, a consacré un cadre général de protection des lanceurs d'alerte, remplaçant une partie des dispositifs spécifiques ou sectoriels qui avaient été auparavant instaurés notamment dans le secteur public.

Enfin, la loi Wasserman<sup>11</sup> et son décret d'application<sup>12</sup> de mars et octobre 2022 respectivement, transposant en droit français la Directive lanceurs d'alerte, ont renforcé le cadre de protection.

La Directive et sa loi de transposition française placent les lanceurs d'alerte au cœur de la défense de l'intérêt général. Grâce à leur position privilégiée, ils sont essentiels pour détecter les menaces ou violations dans les organismes avec lesquels ils travaillent. Ils jouent un rôle crucial dans la protection des libertés fondamentales, le bon fonctionnement du marché et des institutions de l'Union, ainsi que dans le respect de la réglementation.

Ce guide, rédigé par le Groupe d'experts de la Commission Compliance de l'AFJE et du Cercle d'Éthique des Affaires, prétend exposer l'état actuel du cadre légal du dispositif d'alerte interne en France ainsi que les différentes étapes de cette procédure. Il comprend également des recommandations et les bons réflexes identifiés par les auteurs dans leur pratique professionnelle afin d'orienter les responsables de conformité et les juristes d'entreprise dans la compréhension et le déploiement du dispositif.

## **Bonne lecture.**

---

<sup>9</sup> Loi n° 2013-316 du 16 avril 2013 relative à l'indépendance de l'expertise en matière de santé et d'environnement et à la protection des lanceurs d'alerte.

<sup>10</sup> 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.

<sup>11</sup> Loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte.

<sup>12</sup> Décret n° 2022-1284 du 3 octobre 2022 relatif aux procédures de recueil et de traitement des signalements émis par les lanceurs d'alerte et fixant la liste des autorités externes instituées par la loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte.

# FICHE 1 : RÉGIME JURIDIQUE

La loi Sapin II de 2016<sup>13</sup> a établi les premiers contours de l'environnement réglementaire du lanceur d'alertes en droit français. Ses dispositions ont été renforcées par la loi de transposition de la directive « *Lanceurs d'alerte* » entrée en vigueur le 1er septembre 2022. Cette loi, dite Wasserman<sup>14</sup>, qui modifie la loi Sapin II, a été précisée par le décret d'application n° 2022-1284 en date du 3 octobre 2022<sup>15</sup>.

Ce décret apporte des précisions concrètes aux dispositions de la loi Sapin II ainsi modifiée en ce qui concerne la procédure de recueil et de traitement des signalements.

## 1. POURQUOI METTRE EN PLACE UNE PROCÉDURE INTERNE DE RECUEIL ET DE TRAITEMENT DES SIGNALEMENTS ?

### ► Une obligation légale

Les personnes morales de droit privé et les entreprises exploitées en leur nom propre par une ou plusieurs personnes physiques employant au moins 50 salariés sont tenues de prévoir un dispositif de recueil et de traitement des signalements.

Pour mémoire, la loi prévoit des obligations similaires au sein des administrations de l'Etat, les personnes morales de droit public employant au moins 50 agents (sauf exceptions), et des collectivités locales d'au moins 10.000 habitants.

De même, les autorités externes (administratives, judiciaires, personnes morales habilitées, ordres professionnels ou défenseurs des droits) figurant sur la liste annexée au décret sont également tenues de mettre en place une telle procédure, notamment si les lanceurs d'alertes n'ont pas confiance dans les dispositifs mis en place au sein des entreprises.

A côté du dispositif général prévu par l'article 6 de la loi Sapin II modifiée, les entités concernées par l'article 17 de la loi, tenues de mettre en place un dispositif de lutte contre la corruption, doivent établir un dispositif d'alerte interne destiné à permettre le recueil des signalements relatifs à l'existence de conduites ou de situations contraires au code de conduite de la société.

Par ailleurs, le dispositif d'alerte est également requis, conformément à l'article L. 225-102-4 du Code de commerce, issu de la loi dite de « devoir de vigilance », pour le recueil des signalements relatifs à l'existence ou à la réalisation des risques d'atteintes graves envers les droits humains et les libertés fondamentales, la santé et la sécurité des personnes ainsi que l'environnement, résultant des activités de la société et de celles des sociétés qu'elle contrôle directement ou indirectement, ainsi que des activités de ses sous-traitants ou fournisseurs.

En complément du cadre général de protection établi par la loi Sapin II, il existe des dispositifs spécifiques, notamment ceux applicables à la fonction publique.<sup>16</sup>

<sup>13</sup> cf. note 9

<sup>14</sup> cf. note 10

<sup>15</sup> cf. note 11

<sup>16</sup> Pour plus d'information sur ces dispositifs consultez la *circulaire du 26 juin 2024 relative à la procédure de signalement des alertes émises par les agents publics et aux garanties et protections qui leur sont accordées dans la fonction publique dans le cadre des articles 6 à 15 de 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 modifiée par la loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte du Ministère de la transformation et de la fonction publiques.*

En principe, ces dispositifs ne relèvent pas du régime général de la loi Sapin II, sauf en ce qui concerne les mesures d'accompagnement et de protection des lanceurs d'alerte qui seraient plus favorables à ce dernier que celles prévues dans le dispositif spécifique<sup>17</sup>.

En outre, les organismes n'entrant pas dans le périmètre de la loi, peuvent également choisir d'instaurer un dispositif d'alerte interne pour répondre à ses engagements éthiques.

## BONNE PRATIQUE N° 1

Face aux différents dispositifs d'alerte existants, l'entité peut décider de les regrouper dans une procédure unique pour faire connaître le dispositif et faciliter son accès aux salariés et parties prenantes de l'entreprise. Dans ce contexte, le dispositif « *devrait explicitement viser l'ensemble des finalités correspondantes, en distinguant celles qui résultent d'une disposition obligatoire spécifique de celles qui sont adoptées volontairement par l'organisme.* »<sup>18</sup>

### ► Quid des groupes des sociétés ?

En ce qui concerne les groupes de sociétés, un système mutualisé est possible pour les filiales employant moins de 250 salariés. Au-delà, elles doivent disposer d'un dispositif propre distinct de celui du groupe, même si le traitement des signalements devra le plus souvent être organisé en coordination avec ce dernier. Le dispositif mis en place en France sera alors élaboré en cohérence avec le dispositif groupe.

A noter que la loi française instituant le régime de protection le plus avancé en Europe, un dispositif groupe mis en place par une société-mère étrangère devra nécessairement prendre en compte les particularités de la loi française.

## BONNE PRATIQUE N° 2

Plusieurs grandes entreprises ont opté pour la mise en place d'une procédure « groupe » reposant sur un mandat donné par les filiales à la holding de recevoir et/ou gérer des signalements pour leur compte. Cette pratique est reflétée dans le guide AFA sur les enquêtes internes anti-corruption<sup>19</sup> : « *Pour les autres entités (d'au moins 250 salariés), il est possible d'externaliser le canal de réception des alertes auprès d'un tiers, sans préjudice du traitement de l'alerte à son niveau. La loi n'exclut pas que ce tiers puisse être une autre société du groupe.* ».

<sup>17</sup> Défenseur des droits - *La protection des lanceurs d'alerte en France*, Rapport bisannuel (2022-2023)

<sup>18</sup> CNIL - *Référentiel relatif aux traitements de données à caractère personnel destinés à la mise en œuvre d'un dispositif d'alerte du 6 juillet 2023*, n° 13. [https://www.cnil.fr/sites/cnil/files/2024-01/referentiel\\_alertes\\_professionnelles.pdf](https://www.cnil.fr/sites/cnil/files/2024-01/referentiel_alertes_professionnelles.pdf). Voir également les recommandations de l'AFA du 12 janvier 2021, n° 253.

<sup>19</sup> Agence Française Anticorruption (AFA) - *Guide Pratique Les Enquêtes Internes anticorruption*, p. 17, paragraphe 2.2.1

## ► L'importance de la mise en œuvre d'un dispositif interne efficace

Avant la loi Waserman, la personne souhaitant bénéficier du statut de lanceur d'alerte devait, sauf exceptions, suivre la voie du canal interne avant de saisir une autorité (canal externe) ou de rendre public son signalement. Désormais, un lanceur d'alerte peut librement choisir d'adresser son signalement au travers du canal interne ou directement à une autorité administrative ou judiciaire, un ordre professionnel, une personne morale habilitée ou le défenseur des droits, sans que le choix de ces canaux ne soit hiérarchisé. Concernant le canal externe, le choix de l'autorité administrative dépendra de la nature des faits remontés.

Pour mémoire, le lanceur d'alerte peut également procéder à une divulgation publique sans même saisir une autorité externe dans certaines circonstances exceptionnelles (notamment en cas de danger grave ou imminent ou s'il considère que l'autorité externe est en conflit d'intérêts).

### JURISPRUDENCE. L'AFFAIRE LUXLEAKS<sup>20</sup>

L'auteur d'une divulgation aux médias portant sur des informations confidentielles obtenues dans le cadre d'une relation professionnelle (dans l'espèce un salarié de PwC au Luxembourg) peut bénéficier de la protection de l'article 10 de la Convention européenne de sauvegarde des droits de l'homme (*Arrêt Halet c. Luxembourg (Grande chambre)*, 14 février 2023, requête n° 21884/18).

Ainsi, la Cour européenne des droits de l'Homme (CEDH) construit un régime protecteur du lanceur d'alerte au-delà des limites des dispositions légales internes de certains États Membres.

Le recours au canal externe (voire une divulgation publique), présente évidemment des risques substantiels pour l'entreprise, si toutefois l'alerte présente de sérieux indices de gravité. L'un des enjeux les plus importants est l'exposition éventuelle de l'entreprise à une enquête par une autorité administrative ou judiciaire déclenchée sur la base d'une alerte anonyme. Il est évident que l'exposition médiatique d'une alerte peut entraîner des conséquences réputationnelles, voire commerciales et financières, immédiates pour l'entreprise mise en cause avant même le résultat d'éventuelles enquêtes (a fortiori quand l'entreprise est cotée en Bourse).

C'est pourquoi, l'entreprise de toute taille a tout intérêt à mettre en place un dispositif de signalement interne présentant de solides garanties pour les éventuels lanceurs d'alerte, afin de les inciter à utiliser en priorité ce canal plutôt que de s'adresser à une autorité externe ou procéder à une divulgation publique.

En outre, un bon dispositif d'alerte interne est un outil efficace de détection et de gestion des risques opérationnels pour les entreprises. Il permet d'identifier en amont les possibles violations de réglementations ou des politiques internes dans tous les domaines (social, fraude,

<sup>20</sup> Entre 2012 et 2014, des déclarations fiscales établies par PwC et publiées dans des médias révélèrent que des accords très avantageux avaient été conclus avec l'administration fiscale luxembourgeoise pour certaines multinationales. Des enquêtes internes montrèrent qu'un auditeur vola des données en 2010, qu'il transmit à un journaliste en 2011, tandis qu'un employé remit seize documents entre octobre et décembre 2012, qui furent publiés. Le journaliste fut acquitté, l'auditeur reconnu lanceur d'alerte, mais l'employé fut condamné pénalement au paiement d'une amende. Il saisit la CEDH pour violation de la liberté d'expression, mais sa demande fut rejetée. En 2021, il demanda le renvoi de l'affaire devant la Grande Chambre, aboutissant à l'arrêt du 14 février 2023.

et corruption, pratiques commerciales, fiscal, vigilance environnementale et droits humains-santé et sécurité, etc.)<sup>21</sup>. Il est également un indicateur pertinent pour mesurer la maturité de la culture éthique au sein d'une organisation et la confiance dans la gouvernance afférente.

## 2. COMMENT METTRE EN PLACE UNE PROCÉDURE INTERNE DE RECUEIL ET DE TRAITEMENT DES SIGNALEMENTS ?

Tout d'abord, le dispositif d'alerte interne doit être adapté au profil de risque de l'entreprise. Il doit préciser le rôle du supérieur hiérarchique, qui doit pouvoir orienter et conseiller ses collaborateurs, sauf dans l'hypothèse où il est lui-même l'auteur du comportement incriminé.<sup>22</sup>

La procédure détaille la démarche de recueil et de traitement de signalements mise en place par l'entreprise. Elle doit avoir préalablement fait l'objet d'une consultation des instances de dialogue social et respecter la législation relative à la protection des données personnelles (Règlement général sur la protection des données (RGPD) et de la loi du 6 janvier 1978 « informatique et libertés » modifiée), ainsi que l'ensemble d'autres règles de droit applicables en vertu des législations spécifiques ou générales (droit du travail).<sup>23</sup>

Le décret d'application de la loi Wasserman requiert que la procédure fasse l'objet d'une publicité suffisante (affichage, notification, site internet et intranet) et qu'elle soit facilement accessible. Cette exigence de publicité s'explique par la variété de personnes pouvant recourir au signalement interne. Il convient de noter que l'AFA vérifie les modalités de communication du dispositif aux bénéficiaires<sup>24</sup>. Par ailleurs, le règlement intérieur de l'entreprise doit mentionner l'existence du dispositif de protection des lanceurs d'alerte.<sup>25</sup>

### ► Quelles informations doivent être incluses dans une procédure d'alerte interne ?

Le dispositif d'alerte interne doit préciser notamment les conditions pour bénéficier du statut de lanceur d'alerte, la typologie de faits pouvant être signalés, les étapes de la procédure, les modalités de traitement, les droits des personnes concernées et les mesures de sécurité et de conservation de données personnelles<sup>26</sup>.

Par ailleurs, la procédure doit intégrer au moins les informations suivantes :

- a. **Modalités d'accès et d'échange** : Précision des canaux pour effectuer une alerte (adresse électronique dédiée, logiciel de gestion, plateforme éthique, voie hiérarchique, par exemple) et des modalités d'échange d'informations avec l'auteur de l'alerte et de transmission par ce dernier des preuves à l'appui de son signalement.
- b. **Anonymat** : Indication de la possibilité d'adresser des alertes de manière anonyme et de poursuivre les échanges tout en conservant l'anonymat.

<sup>21</sup> C'est même le moyen de détection le plus efficace des fraudes (42% des fraudes sont détectées par des "tips" notamment de la part des employés, soit trois fois plus que par la voie de l'audit interne. Cf. ACFE Report to the nations 2022, page 22. <https://if.pf.s3.eu-west-3.amazonaws.com/427/RTTN-2022-FR-V6-BD.pdf>

<sup>22</sup> AFA- Avis relatif aux recommandations de l'Agence française anticorruption destinées à aider les personnes morales de droit public et de droit privé à prévenir et à détecter les faits de corruption, de trafic d'influence, de concussion, de prise illégale d'intérêts, de détournement de fonds publics et de favoritisme, JORF numéro 0010 du 12 janvier 2021 n° 256 et 257, page 34 (« Recommandations de l'AFA »)

<sup>23</sup> Cf. CNIL. Référentiel relatif aux traitements de données à caractère personnel destinés à la mise en œuvre d'un dispositif d'alerte.

<sup>24</sup> Cf. Agence Française Anticorruption. Contrôles des entités assujetties à l'article 17 de la loi n° 2016-1691 du 9 décembre 2016 questionnaire et pièces à fournir, Question E15

<sup>25</sup> Cf. article L.1321-2 du Code du travail

<sup>26</sup> Recommandations de l'AFA. n° 262 et ss. Voir supra note n° 21

- c. **Traitement des alertes** : Informations sur les délais pour accuser réception du signalement, communiquer sur sa recevabilité ou non, sur les suites à donner aux signalement et retour sur la clôture de la procédure à l'auteur de l'alerte et aux personnes visées.
- d. **Désignation des référents** : Identification du (des) référent(s) désigné(s) pour recueillir les signalements et, si différent, celui en charge de leur traitement.
- e. **Garanties de la procédure** : Indication des mesures qui seront mises en place pour garantir la sécurité et la confidentialité des informations traitées, notamment, de l'identité de l'auteur de l'alerte, des faits signalés et des personnes visées, y compris lors de communications avec des tiers. La violation de cette confidentialité peut entraîner des sanctions pénales et disciplinaires.

### ► Qui peut bénéficier du statut protecteur de lanceur d'alerte ?

Les personnes indiquées ci-après répondant aux critères de la définition de « lanceurs d'alertes » (cf. infra), peuvent bénéficier du statut de « lanceur d'alerte » :

- a. Les membres du personnel, les personnes dont la relation de travail s'est terminée, lorsque les informations ont été obtenues dans le cadre de cette relation, et les personnes qui se sont portées candidates à un emploi au sein de l'entité concernée, lorsque les informations ont été obtenues dans le cadre de cette candidature ;
- b. Les actionnaires, les associés et les titulaires de droits de vote au sein de l'assemblée générale de l'entité ;
- c. Les membres de l'organe d'administration, de direction ou de surveillance ;
- d. Les collaborateurs extérieurs et occasionnels ;
- e. Les cocontractants de l'entité concernée, leurs sous-traitants ou, lorsqu'il s'agit de personnes morales, les membres de l'organe d'administration, de direction ou de surveillance de ces cocontractants et sous-traitants ainsi que les membres de leur personnel.

### ► Quelles sont les conditions pour bénéficier du statut de lanceur d'alerte ?

Tout auteur souhaitant bénéficier du statut de lanceur d'alerte à la suite d'un signalement doit remplir les conditions cumulatives suivantes :

- a. Être une **personne physique** ;
- b. Signaler sans volonté d'obtenir une **contrepartie financière directe** ;

À la différence de la pratique aux Etats-Unis où les lanceurs d'alerte peuvent bénéficier de rétributions importantes, le droit français n'admet que les signalements sans contrepartie financière directe.<sup>27</sup> La loi exclut donc que l'intérêt financier puisse être au cœur des motivations d'un lanceur d'alerte.

En revanche, la contrepartie financière indirecte n'est pas exclue (le critère du désintéressement prévu en 2016 n'est plus applicable) et ne fait pas obstacle à la reconnaissance du statut de lanceur d'alerte. La notion de « contrepartie financière directe » apparaît encore relativement floue à ce jour. La jurisprudence en définira sans doute les contours.

<sup>27</sup> A l'exception de l'aviseur fiscal qui peut être rémunéré par l'administration fiscale en échange d'une récompense ou d'une indemnisation. Article L. 10-0 AC du livre de procédures fiscales.

- c. Agir **de bonne foi** en alertant sur des faits qu'il estime raisonnablement être exacts et honnêtes au moment du dépôt du signalement ;

La bonne foi est un critère déterminant pour l'obtention du statut de lanceur d'alerte.

Une personne est considérée de bonne foi si elle a des raisons valables de croire que les faits signalés sont vrais et méritent une alerte, en se basant sur les informations dont elle dispose.

A savoir que, même si la mention de l'action en dénonciation calomnieuse à l'encontre d'un lanceur d'alerte de mauvaise foi n'a pas été retenue dans la loi Wasserman, rien n'empêche l'entreprise de rappeler explicitement cette possibilité dans sa procédure. La bonne foi est présumée par le législateur, l'entreprise ne pouvant déduire que le lanceur d'alerte est de mauvaise foi du seul fait que les allégations sont infondées à l'issue d'une enquête interne.

### JURISPRUDENCE. NOTION DE BONNE FOI

Dans l'affaire *Guja c. Moldova*, la CEDH a affirmé qu'un « acte motivé par un grief ou une animosité personnels ou encore par la perspective d'un avantage personnel, notamment un gain pécuniaire, ne justifie pas un niveau de protection particulièrement élevé »<sup>28</sup>

Dans un arrêt du 8 juillet 2020, la Cour de cassation a considéré que la mauvaise foi ne pouvait résulter « que de la connaissance par le salarié de la fausseté des faits qu'il dénonce et non de la seule circonstance que les faits dénoncés ne sont pas établis ».<sup>29</sup>

- d. signaler des **informations** portant sur un **crime**, un **délit**, une **menace** ou un **préjudice pour l'intérêt général**, une **violation ou une tentative de dissimulation d'une violation** 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, du droit de l'Union européenne, de la loi ou du règlement ou encore la violation de référentiels éthique de l'entreprise (ex : charte éthique, code de conduite).

Seules les informations relatives à des situations contraires à la loi ou portant atteinte à l'intérêt général peuvent être signalées ou divulguées. Ainsi, par exemple, les dysfonctionnements mineurs au sein de la direction d'entreprise, qui ne menacent pas l'intérêt général et n'enfreignent aucune réglementation, ne peuvent donc pas justifier une alerte bénéficiant de la protection prévue par la loi Sapin II.

« Le lanceur d'alerte ne doit pas être affecté par le trouble qu'il dénonce, auquel cas il lui appartient de déposer plainte. »<sup>30</sup> « Au regard de ces considérations, lorsqu'il [le Défenseur des droits] est saisi par une personne victime des faits dénoncés qui n'a signalé que son propre cas, ou qui ne dispose d'aucun élément permettant d'établir que les faits excéderaient sa situation personnelle, le Défenseur des droits ne retient pas la qualification de lanceur d'alerte. »<sup>31</sup>

<sup>28</sup> CEDH 12 févr. 2008, *Guja c/ Moldova* [GC], n° 14277/04

<sup>29</sup> 8 juillet 2020, Cour de cassation, Pourvoi n° 18-13.593

<sup>30</sup> Rapporteur au Sénat n° 712 [2015-2016], 22 juin 2016, cité par le Rapport bisannuel du Défenseur des droits, voir *supra* note n° 16

<sup>31</sup> Défenseur des droits, Rapport bisannuel 2022-2023, voir *supra* note n° 16

Le nouveau texte a étendu le champ de protection des lanceurs d'alertes. La loi Sapin II de 2016 comportait des filtres exigeants pour délimiter la violation susceptible d'être à l'origine de l'alerte.

La loi Wasserman a introduit une ouverture à deux niveaux. D'une part, elle a supprimé les notions de gravité et de caractère manifeste des violations, incluant ainsi des sujets en apparence « bénins ». D'autre part, le législateur a depuis accepté qu'en plus des faits proprement dits, de simples « informations » sur ceux-ci peuvent faire l'objet du signalement ou de la divulgation. Il reste à préciser par la pratique dans quelle mesure un renseignement donné revêt une importance suffisante pour motiver une alerte.

Enfin, le décret d'application de la loi précise que les faits couverts peuvent être « hypothétiques » mais « très susceptible de se produire ».

e. Les informations sont **rapportées ou connues par le lanceur d'alerte**

Depuis la loi Wasserman, il est possible pour un lanceur d'alertes de signaler des faits lui ayant été rapportés mais dont il n'a pas eu directement connaissance. La condition de connaissance personnelle est maintenue uniquement pour les faits signalés hors du cadre professionnel.

Néanmoins, cette connaissance doit être licite. Une personne ayant obtenu une information appartenant à l'entreprise par des moyens illicites (ex : vol de documents) ne saurait se prévaloir de la qualité de lanceur d'alerte.

Par ailleurs, la loi Wasserman intègre une inopposabilité des secrets d'affaires au lanceur d'alerte (à l'exception toutefois des informations couvertes par certains secrets comme le secret de défense nationale, secret médical, secret professionnel d'avocat). Cela signifie que dans le cadre de l'alerte émise par un salarié, celui-ci ne peut se voir opposer la notion de secret d'affaires pour l'empêcher d'alerter dès lors que celui-ci est de bonne foi et que l'information a été obtenue de manière licite. La question de la mise en place d'un dispositif spécifique aux secrets d'affaires peut se poser à cette occasion.

Enfin, il convient de préciser que si les informations n'ont pas été recueillies dans le cadre professionnel, une condition supplémentaire doit être satisfaite : la personne doit avoir eu une connaissance personnelle des faits rapportés.

### **JURISPRUDENCE. GRILLE D'ANALYSE DES ATTEINTES POTENTIELLES À LA LIBERTÉ D'EXPRESSION DES LANCEURS D'ALERTE.**

Dans l'arrêt *Guja C. Moldova* la CEDH a dégagé une grille d'examen reposant sur 6 critères permettant d'apprécier la proportionnalité de l'atteinte portée à la liberté d'expression de l'auteur de la divulgation que sont les moyens utilisés pour procéder à la divulgation, l'authenticité de l'information divulguée, la bonne foi, l'intérêt public que présente l'information divulguée, le préjudice causé et la sévérité de la sanction.

Cette jurisprudence a été confirmée par la décision de la Grande Chambre *Halet c. Luxembourg* dit des « Luxleaks ». <sup>32</sup>

<sup>32</sup> Jurisprudence citée par le Rapport bisannuel du Défenseur des droits. Voir supra notes n° s 19, 27 et 29

## ▶ Quelles garanties pour le lanceur d'alerte ?

- a. Garantie de confidentialité.** La procédure doit fournir des garanties de confidentialité, d'impartialité et de diligence dans le traitement de l'alerte. Ces garanties doivent concerner aussi bien l'auteur du signalement que les personnes interrogées dans le cadre des vérifications ou enquêtes et les personnes mises en cause et le contenu des allégations de l'alerte (confidentialité).

En cas de violation de la confidentialité de l'identité des auteurs du signalement, des personnes visées par celui-ci ou des informations recueillies, l'auteur de l'infraction encourt des sanctions pénales (peine d'emprisonnement, amende) et civiles (octroi de dommages et intérêts). En outre, la décision peut faire l'objet d'une mesure de publicité.

- b. Protection des données personnelles.** La mise en place d'une procédure d'alerte implique la collecte et le traitement des données personnelles. Ainsi, l'entité doit s'assurer de la protection des données des personnes concernées tout au long de la procédure en conformité avec le règlement général de protection des données personnelles (RGPD)<sup>33</sup>, la loi LIL<sup>34</sup> et le Référentiel CNIL.<sup>35</sup>

Il convient d'inclure dans la procédure d'alerte et/ou dans la politique de confidentialité de l'entité les informations relatives aux opérations de traitement effectuées, les finalités poursuivies, les types de données susceptibles d'être collectées, les personnes potentiellement concernées, les principales étapes de la procédure, la durée de conservation des données, les règles applicables -le cas échéant- au transfert des données en dehors de l'Union Européenne et enfin, les droits de personnes concernées (droit d'accès, de rectification, d'opposition de limitation et d'effacement).

- c. Protection contre des représailles.** La loi Wasserman a établi une liste élargie de 15 mesures prises à l'encontre des lanceurs d'alertes susceptibles de constituer des représailles. Ces mesures concernent notamment le licenciement, la mise à pied, le non-renouvellement ou la résiliation anticipée d'un contrat de travail temporaire, la discrimination ou encore le harcèlement. Elles sont frappées de nullité, sauf si l'entreprise démontre que le lanceur d'alerte n'était pas de bonne foi ou cherchait à obtenir un avantage financier direct. La loi punit également l'obstruction à la transmission d'un signalement (risque de sanctions pénales et civiles à savoir peine d'emprisonnement et amendes en cas de « procédures-bâillon »)<sup>36</sup>.

- d. Irresponsabilité civile et pénale.** Conformément au I de l'article 10-1 de la loi Sapin II, un lanceur d'alerte qui signale ou divulgue publiquement des informations n'est pas civilement responsable des dommages résultant de ce signalement ou de cette divulgation, à condition que deux critères soient remplis :

i) Le signalement doit respecter les conditions prévues par la réglementation (notamment les articles 6 et 8 de la loi du 9 décembre 2016 ainsi que le décret du 3 octobre 2022) ;

ii) L'auteur doit avoir des raisons fondées de croire que le signalement ou la divulgation publique des informations était nécessaire pour protéger les intérêts en cause.

<sup>33</sup> Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

<sup>34</sup> Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

<sup>35</sup> Voir *supra*, note n° 4.

<sup>36</sup> Loi Sapin II, article 13.

Concernant l'irresponsabilité pénale, selon l'article 122-9 du code pénal, n'est pas pénalement responsable l'auteur d'un signalement qui porte atteinte à un secret protégé par la loi ou bien qui soustrait, détourne ou recèle des documents ou tout autre support contenant des informations dont il a eu connaissance de manière licite (donc sans vol ni effraction), sous réserve que les deux conditions suivantes soient remplies :

i) Le signalement doit être effectué conformément aux conditions prévues par la réglementation : il ne doit donc pas concerner des faits, informations ou documents couverts par un secret protégé exclu du régime de l'alerte (comme le secret de défense nationale, le secret médical, le secret des délibérations judiciaires, le secret de l'enquête ou de l'instruction judiciaires, ou le secret professionnel de l'avocat) ;

ii) La divulgation des informations doit être nécessaire et proportionnée à la protection des intérêts en cause.

Enfin, les facilitateurs (toutes personnes physiques ou toutes personnes morales de droit privé à but non lucratif) qui aident ou agissent en lien avec le lanceur d'alertes bénéficient des mêmes protections<sup>37</sup>. La notion de facilitateur méritera d'être éclaircie par la jurisprudence.

### ► Quelles limites aux garanties de protection ?

L'article 23 de la Directive lanceurs d'alerte exhorte les États à prévoir des sanctions effectives, proportionnées et dissuasives applicables aux auteurs de signalements frauduleux. Comme la loi Wasserman ne prévoit aucune disposition spécifique concernant la responsabilité pénale de l'auteur d'un signalement de mauvaise foi, c'est le droit commun qui s'applique.

Ainsi, une personne ayant effectué un signalement de mauvaise foi peut s'exposer à des poursuites pour dénonciation calomnieuse, diffamation ou injure, atteinte à la vie privée ou au droit à l'image, ou violation du secret professionnel. Elle peut par ailleurs se voir infliger une sanction disciplinaire.

## 3. LE RÔLE DU DÉFENSEUR DES DROITS

La loi organique n° 2016-1690 du 9 décembre 2016 relative à la compétence du Défenseur des droits pour l'orientation et la protection des lanceurs d'alerte, avait chargé le Défenseur des droits d'une mission d'accompagnement des lanceurs d'alertes. Conformément à la loi, le Défenseur des droits est compétent pour recevoir leurs signalements, les orienter vers les autorités compétentes et veiller à leurs droits. La loi Wasserman et la loi organique n° 2022-400 du 21 mars 2022<sup>38</sup> ont considérablement renforcé son périmètre d'intervention en précisant que le Défenseur des droits est compétent pour informer, conseiller et défendre les droits et libertés des lanceurs d'alerte (et les facilitateurs).

Parmi ses nouvelles missions, le Défenseur des droits est compétent pour rendre un avis sur la qualité de lanceur d'alerte d'une personne, quel que soit le régime de protection applicable. Les avis sont rendus par le Défenseur des droits dans un délai qui peut aller jusqu'à six mois à compter de la réception de la demande qui lui est adressée, laquelle ne peut être faite qu'après que le signalement a été effectué. Un tel avis du Défenseur des droits, appelé à tort « *certification* », ne lie pas toutefois les juridictions en cas de contentieux, par exemple prud'hommal.

<sup>37</sup> Article 6-1 loi Sapin II

<sup>38</sup> Loi organique n° 2022-400 du 21 mars 2022 visant à renforcer le rôle du Défenseur des droits en matière de signalement d'alerte

# FICHE 2 : RECUEIL ET TRAITEMENT DE LA RECEVABILITÉ DU SIGNALEMENT

## 1. LES MODALITÉS DE RECUEIL DES SIGNALEMENTS

Le canal de recueil doit prévoir les modalités de la réception des signalements selon un des trois moyens suivants :

- De manière écrite (adresse de courriel dédié, plateforme externe)
- De manière orale (par téléphone, messagerie vocale ou rencontre physique à la demande du lanceur d'alerte)
- Ou des deux manières<sup>39</sup>

Comme indiqué dans la *Fiche n° 1*, les modalités de recueil des signalements doivent être précisées dans la procédure d'alerte. Elle doit préciser également si le canal de réception de l'alerte est géré par un tiers.

Quel que soit le canal choisi, il faut s'assurer que celui-ci permette la transmission complète des éléments de signalement, quels que soient leur forme ou leur support.

### BONNE PRATIQUE N° 3

L'article 6 II du décret d'application<sup>40</sup> prévoit de strictes conditions de consignation du signalement oral. Au vu de la complexité particulière de ce canal de recueil, il nous semble très difficile de le mettre en place. Nous recommandons d'exclure en France le signalement oral de la procédure de réception des alertes par les entités de droit privé, ce qui est permis par le législateur français, à moins que l'entité n'alloue des ressources suffisantes pour leur recueil et traitement.

### BONNE PRATIQUE N° 4

Les personnes qui émettent un signalement doivent recevoir les informations relatives au traitement des données personnelles dès le début du process de recueil<sup>41</sup>. Il convient de rendre facilement accessible la politique de confidentialité relative au traitement des alertes (par exemple : site internet, intranet, sur la plateforme d'alerte, communication directe aux salariés, affichage).

<sup>39</sup> A noter que à différence du dispositif d'alerte interne, le recueil de signalements par les autorités publiques doit pouvoir se faire par écrit et par oral. cf. Article 10 du décret d'application, voir *supra* note 11.

<sup>40</sup> Voir *supra* note 11.

<sup>41</sup> Voir *supra* note 22, n° 80.

## 2. LES MODALITÉS DE TRAITEMENT DE LA RECEVABILITÉ DES SIGNALEMENTS RECUEILLIS

Un signalement doit être traité si les critères de validité de l'alerte sont réunis. (Cf. Fiche 1). A défaut, l'entreprise doit informer l'auteur des motifs du rejet du signalement. Elle reste libre de déterminer s'il y a lieu de procéder néanmoins au traitement du signalement ainsi recueilli.

En cas de signalement anonyme, l'étude de recevabilité du signalement sera réalisée si le caractère sérieux des faits mentionnés est établi et les éléments factuels sont suffisamment détaillés.

### BONNE PRATIQUE N° 5

Afin de faciliter et accélérer l'examen de la recevabilité de l'alerte puis son traitement ultérieur, il convient de prévoir dans le cadre de la procédure que l'auteur de l'alerte non anonyme transmet en même temps que son signalement tout élément justifiant qu'il appartient à l'une des catégories de personnes mentionnées à l'article 8 de la loi du 9 décembre 2016 (Article 4 du décret du 3 octobre 2022).

Si les faits objets du signalement ainsi que les documents transmis ne permettent pas d'établir le caractère fondé et sérieux de l'alerte, le gestionnaire du dispositif dresse un compte-rendu des opérations de vérification et conclut à l'irrecevabilité de l'alerte après motivation.

L'auteur du signalement est informé de cette décision ainsi que de sa possibilité de saisir un canal extérieur.

*A contrario*, si l'alerte est considérée comme sérieuse et fondée, le gestionnaire du dispositif procédera à l'instruction de l'alerte.

## 3. LA PERSONNE EN CHARGE DE LA PROCÉDURE DE RECUEIL ET DE TRAITEMENT

Le décret d'application prévoit que la procédure doit mentionner les personnes ou services désignés par l'entreprise pour le recueil et le traitement des signalements. Le canal de réception et le traitement des alertes peuvent être gérés par des personnes ou services différents. Les personnes ou services désignés doivent disposer, par leur positionnement, de la compétence, de l'autorité et des moyens suffisants à l'exercice de leurs missions et présenter des garanties d'impartialité.

La procédure prévoit les garanties permettant l'exercice impartial de ces missions<sup>42</sup>.

<sup>42</sup> Article 5 du décret du 3 octobre 2022.

## BONNE PRATIQUE N° 6

Afin de prévenir toute situation de conflit d'intérêt, il est essentiel d'inclure dans la procédure les modalités de gestion des signalements potentiels concernant le ou les gestionnaires du dispositif.

La réception des signalements peut être gérée par un tiers au nom et pour le compte de l'entreprise. De plus en plus de structures recourent à de telles solutions d'externalisation qui permettent de s'assurer d'un recueil et traitement efficace des alertes en protégeant l'entreprise contre les risques de violation des droits des lanceurs d'alertes et leurs conséquences.

### 4. LES DÉLAIS D'INFORMATION DE L'AUTEUR DU SIGNALEMENT ET DES PERSONNES VISÉES PAR LE SIGNALEMENT

Trois délais sont fixés par les textes :

▶ **7 jours ouvrés :**

L'auteur du signalement est informé par écrit de la réception de son signalement dans les sept jours ouvrés à compter de cette réception, que le signalement ait été effectué par écrit ou à l'oral.

▶ **1 mois :**

Pour informer la personne visée par une alerte (par exemple, en tant que témoin, victime ou auteur présumé des faits), sauf exception dûment justifiée, à la suite de l'émission d'une alerte, conformément à l'article 14 du RGPD.<sup>43</sup> Cette information peut être différée, selon l'article 14-5-b) lorsqu'elle est susceptible « *de compromettre gravement la réalisation des objectifs dudit traitement* ».

En pratique, il est fréquent que l'information du mis en cause soit reportée pour éviter la disparition de preuves ou une interférence avec le bon déroulement de l'enquête interne (ex : pressions sur des témoins ou lanceurs d'alerte). C'est pourquoi l'entretien avec le mis en cause intervient souvent en fin du cycle des entretiens.

▶ **3 mois :**

À compter de l'accusé de réception, ou à compter de l'expiration d'une période de 7 jours ouvrés suivant le signalement, l'entreprise communique par écrit à l'auteur du signalement « *des informations sur les mesures envisagées ou prises pour évaluer l'exactitude des allégations* » ; l'entreprise peut également, si cela lui est possible dans ce même délai, donner des informations sur les mesures de remédiation envisagées.<sup>44</sup>

A noter que l'entité n'a pas l'obligation d'informer le lanceur d'alerte des suites données à l'investigation, mais seulement des mesures destinées à évaluer l'exactitude des allégations. La procédure prévoit que l'entité communique par écrit à l'auteur du signalement, dans un délai raisonnable n'excédant pas trois mois à compter de l'accusé de réception du signalement ou, à défaut d'accusé de réception, trois mois à compter de l'expiration d'une période

<sup>43</sup> Référentiel CNIL, alinéa n° 91 et n° 92, voir *supra* note n° 22.

<sup>44</sup> Article 4 du décret du 3 octobre 2022.

de sept jours ouvrés suivant le signalement, des informations sur les mesures envisagées ou prises pour évaluer l'exactitude des allégations et, le cas échéant, remédier à l'objet du signalement ainsi que sur les motifs de ces dernières

## 5. LA RECEVABILITÉ DU SIGNALEMENT

La procédure doit prévoir les suites données aux signalements ne répondant pas aux conditions posées par les articles 6 et 8 de la loi du 9 décembre 2016 (pour rappel : les conditions relatives à la personne de l'auteur du signalement, aux faits signalés, aux circonstances dans lesquelles ils ont été connus par l'auteur du signalement *cf. Fiche n° 1*), et ce faisant rappeler les conditions de recevabilité de l'alerte.

Elle doit également prévoir les suites données aux signalements anonymes.

Le lanceur d'alerte doit être informé de la décision d'irrecevabilité de son alerte et des motifs du refus.

### BONNE PRATIQUE N° 7

Dans certains cas, il conviendra d'attendre la fin du traitement de l'alerte (mesures d'investigation, enquête interne) pour décider que l'alerte n'est pas recevable et prendre toute mesure, même si le cas d'irrecevabilité de l'alerte paraît manifeste, car :

- 1° Un salarié, en litige avec son employeur, peut en effet par le lancement d'une alerte interne, rechercher une protection qu'il espère analogue à celle d'un salarié protégé. Le traitement de l'alerte permettra de renforcer le dossier de l'employeur en cas de contentieux initié par le salarié qui pourrait prétendre faire l'objet de représailles. Même raisonnement applicable dans toute situation de conflit entre l'entité et l'une des personnes visées à l'article 8 de la loi du 9 décembre 2016.
- 2° Même irrecevable, l'alerte peut porter sur des faits avérés et l'entreprise avoir intérêt à procéder à une enquête sur les faits en question.

### BONNE PRATIQUE N° 8

Dans le cadre des alertes hors champ de la procédure ou encore irrecevables, une bonne pratique consiste à réorienter l'auteur du signalement non recevable vers la personne ou le service compétente de l'entité (RH, qualité, ...) pour rechercher une solution à la doléance, et ce afin de ne pas complètement fermer la porte aux attentes d'une personne qui exprime souvent un mal-être via son signalement.

# FICHE 3 : EXAMEN DU SIGNALEMENT

## POUR ALLER PLUS LOIN :

Consulter le guide « **ENQUÊTE INTERNE : Ouvrir, conduire et clôturer une enquête interne** », édité par l'AFJE et le Cercle d'Éthique des Affaires.

Une fois le signalement déclaré recevable, il convient de procéder à son traitement afin de vérifier le bien-fondé des allégations.

## 1. ANALYSE ET VÉRIFICATION DES ALLÉGATIONS ET ENQUÊTE INTERNE

Il convient de préciser que le traitement d'une alerte ne nécessite pas obligatoirement l'ouverture d'une enquête interne. Il peut s'agir d'une simple vérification des preuves apportées par le lanceur d'alerte.

Il est important de demander à l'auteur du signalement tout complément d'information nécessaire (qui, quoi, quand, où ?), notamment « afin d'évaluer l'exactitude des allégations qui sont formulées ». <sup>45</sup>

Dans le cadre des signalements relevant des problématiques de ressources humaines (plus de deux alertes sur trois dans plusieurs grandes entreprises consultées par le Cercle d'éthique des affaires)<sup>46</sup> le traitement de l'alerte peut consister en la résolution managériale d'un différend entre salariés, la mise en place d'une conciliation ou médiation, la mise en œuvre d'un processus disciplinaire (exemple : réalité des faits de manquement grave à la loi ou au référentiel d'entreprise établie par la documentation fournie par le lanceur d'alerte).

**Attention à éviter toute confusion avec le droit d'alerte du CSE en cas d'atteinte aux droits des personnes.**

Si une enquête interne s'avère nécessaire, il faut respecter un certain nombre de précautions, telles que celles mentionnées ci-après :

- Rédaction de lettres de mission désignant les enquêteurs et le périmètre de l'enquête ; l'enquête interne peut être menée par des collaborateurs de l'entreprise et/ou par des tiers agissant pour le compte de l'entreprise ;
- Des mesures conservatoires à envisager avec diligences pour préserver les données utiles à l'enquête (risque de destruction de preuves) ;

<sup>45</sup> Décret du 3 octobre 2022, article 4. III.

<sup>46</sup> Rajouter référence (enquête, autres).

- Des mesures de protection des victimes et des lanceurs d'alerte à mettre en place de façon immédiate et durable, compte tenu de la nature des allégations, de l'obligation de sécurité de l'employeur (ex. du harcèlement), du risque de représailles, des circonstances (ex : menaces) ;
- Pendant la phase des entretiens, avec une variété de pratiques d'entreprises constatées : le compte-rendu est soit un verbatim soit une synthèse, qui peut donner lieu ou non à communication, validation ou signature de la personne entretenue ;
- Attention à ne pas collecter des informations, dont la source est illicite pour l'employeur sur les terrains civil, commercial et prud'homal (à la différence du contexte d'une plainte pénale), par exemple des enregistrements audio ou vidéo à l'insu de la personne mise en cause ou visée par l'alerte. Toutefois, il convient de préciser que dans un arrêt du 22 décembre 2023<sup>47</sup>, l'Assemblée plénière de la Cour de cassation a opéré un revirement de jurisprudence. Elle accepte désormais que le juge civil puisse tenir compte, sous conditions, d'éléments de preuve obtenus de manière déloyale, et s'aligne ainsi sur la jurisprudence européenne.

Le rapport d'enquête comporte des constats factuels et une ou des recommandations sur les suites qu'il convient de donner à l'alerte.

**Pour en savoir plus, nous vous recommandons de consulter les travaux du groupe d'experts de l'AFJE et du Cercle éthique des affaires sur l'enquête interne.**

## 2. PRINCIPES À RESPECTER

Dans cette étape de la procédure, plusieurs principes directeurs doivent être respectés pour toute personne impliquée dans le traitement des alertes :

### ► Confidentialité :

- L'identité du lanceur d'alerte, des personnes visées ou mentionnées par l'alerte, et les faits signalés ne peuvent être divulgués qu'aux personnes ayant besoin de l'information pour analyser et traiter l'alerte.
- L'identité très sensible du lanceur d'alerte ne doit pas être divulguée, sauf accord préalable et écrit de ce dernier. C'est un cas fréquent lorsque l'alerte doit être transférée à une filiale (exemple : DRH) ou à une équipe chargée du traitement effectif de l'alerte (exemple : enquêteurs de la holding ou d'autres entités).
- Dans l'hypothèse où le lanceur d'alerte a déposé une alerte anonyme, le traitement effectif de l'alerte peut nécessiter, selon les circonstances, de demander la levée de l'anonymat.

L'enjeu est de sensibiliser les acteurs sur la stricte confidentialité dont ils sont redevables tant en cours qu'à l'issue du traitement de l'alerte, qu'il y ait ou non une enquête. La violation de cette obligation de confidentialité de source légale est punie d'une peine pouvant aller jusqu'à 2 ans d'emprisonnement, et 30 000 euros d'amende.<sup>48</sup>

<sup>47</sup> Cour de cassation, Assemblée plénière, 22 décembre 2023, 20-20.648, Publié au bulletin

<sup>48</sup> Loi Sapin II, art. 9.

## BONNE PRATIQUE N° 9

Il est crucial de rappeler par écrit l'importance de la confidentialité à toutes les personnes impliquées dans le traitement d'un signalement ou dans une enquête interne. Les enquêteurs occasionnels ou les collaborateurs doivent signer un accord de confidentialité lorsqu'ils sont sollicités pour participer au processus. Par ailleurs, l'existence d'un risque pénal constitue un argument convaincant pour refuser toute demande, qu'elle émane de la direction ou d'un tiers, visant à révéler l'identité des lanceurs d'alerte ou la nature des allégations.

### ▶ **Indépendance et impartialité :**

Le traitement de l'alerte a pour objet de vérifier le bien-fondé d'allégations, leur nature et ampleur avec objectivité et en toute neutralité. Ce n'est pas le cas si les personnes traitant des alertes ou menant des enquêtes sont soumises à des conflits d'intérêts ou si leur indépendance est compromise par des influences externes ou internes (ex : répondre aux attentes d'une partie prenante). Ce n'est pas non plus le cas si les enquêteurs veulent défendre ou favoriser une partie (ex : manager) au détriment de l'autre partie (ex : collaborateur ou prestataire) ou encore une posture plutôt qu'une autre.

## BONNE PRATIQUE N° 10

Prévoir dans la procédure l'obligation de déport de toute personne ayant un risque de conflit d'intérêts. Garder à l'esprit la présomption d'innocence des personnes mises en cause comme la bonne foi présumée du lanceur d'alerte ou des victimes alléguées.

### ▶ **Absence de mesures de représailles contre le lanceur d'alerte :**

La protection du lanceur d'alerte de bonne foi est essentielle, non seulement pendant le temps du traitement de l'alerte, mais aussi après la clôture de l'alerte.

Toute mesure de représailles est interdite de la part de l'employeur, interdiction sanctionnée pénalement (délit pénal de discrimination, voir l'article 225-1 du Code pénal).

# FICHE 4 : CLÔTURE DE LA PROCÉDURE

## POUR ALLER PLUS LOIN :

Consulter le guide « **ENQUÊTE INTERNE : Ouvrir, conduire et clôturer une enquête interne** », édité par l'AFJE et le Cercle d'Éthique des Affaires.

### La procédure est clôturée :

- ▶ **Dans le cas où le signalement ne respecte pas les conditions** de l'article 6 et le A du I de l'article 8 de la Loi (cf. Fiche n° 1). L'auteur du signalement est informé des raisons pour lesquelles l'entité estime que son signalement ne respecte pas les conditions de recevabilité (cf. Fiche n° 2).
- ▶ **Après traitement d'un signalement recevable**, dès que l'analyse des allégations formulées et des preuves recueillies en support de l'alerte est finalisée (sans enquête ou à la suite de l'enquête interne, par exemple)

Pour formaliser la clôture du dossier, il convient de rédiger un rapport consignnant l'ensemble des allégations et des preuves recueillies, des actions menées pour traiter l'alerte et les recommandations sur les éventuelles suites identifiées à donner à l'alerte.

## CE RAPPORT PEUT CONTENIR<sup>49</sup> :

1. La description des faits à l'origine de l'alerte (Le rapport d'enquête doit exposer les faits avec la plus grande précision possible)
2. La méthodologie d'enquête suivie.
3. La description de l'ensemble des actes d'investigation réalisés, les faits établis et les éléments recueillis de nature à conforter ou à lever le soupçon ainsi que les éventuelles limites rencontrées pour obtenir les éléments recherchés (exemples : absence d'archives papiers ou numériques, obstacles juridiques, difficultés techniques, etc.). L'ensemble de ces éléments (documents, CR des interviews des témoins, lanceur d'alerte, entre autres) est annexé au rapport.
4. Les conclusions. En fonction des résultats de l'enquête (faits avérés, non conclusifs ou non avérés) le rapport contient les recommandations concernant les suites à donner au signalement.

<sup>49</sup> AFA- Guide Les Enquêtes internes anticorruption, paragraphe 2.3.4, pages 29 à 31

# FICHE 5 : SUITES<sup>50</sup> À DONNER À L'ALERTE

## POUR ALLER PLUS LOIN :

Consulter le guide « **ENQUÊTE INTERNE : Ouvrir, conduire et clôturer une enquête interne** », édité par l'AFJE et le Cercle d'Éthique des Affaires.

## 1. CLÔTURE SANS SUITE

La procédure est clôturée sans suite si :

- ▶ **Les faits signalés par le lanceur d'alerte ne sont pas avérés.** Les informations sont inexactes ou infondées (ou la responsabilité des personnes mises en cause n'est pas établie) ou le signalement est devenu sans objet ; et
- ▶ **Aucune mesure ou action n'est identifiée afin de tirer des conséquences de l'alerte.**

Les données personnelles sont détruites ou anonymisées. L'alerte est archivée, sauf décision d'archivage intermédiaire le temps de la prescription, comme précisé ci-après.

## 2. CLÔTURE AVEC SUITE

Le dossier peut être clôturé avec suite dans les cas suivants :

- ▶ **Les faits ne sont pas avérés et l'enquête a pu démontrer la mauvaise foi du lanceur d'alerte** (ex : intention de nuire à autrui). L'entité peut décider de prononcer une sanction disciplinaire<sup>51</sup> à l'encontre du lanceur d'alerte (si l'auteur du signalement est un salarié) et/ou des poursuites judiciaires (dénonciation calomnieuse [article 226-10 du code pénal]) ;
- ▶ **Les allégations sont suffisamment étayées ou le signalement est devenu sans objet** mais des actions correctives ont été identifiées.

Lorsque les allégations sont avérées, « l'entité met en œuvre les moyens à sa disposition pour remédier à l'objet du signalement » (article 4.II Décret). Les éventuelles suites à donner à un signalement sont adaptées à l'objet de l'alerte et la gravité des faits.

<sup>50</sup> L'expression "suites" désigne toute décision prise par l'organisme pour tirer des conséquences de l'alerte. cf. *Guide pratique* de la CNIL sur les durées de conservation cité par les Recommandations de l'AFA, page 37.

<sup>51</sup> Les sanctions disciplinaires sont décidées par l'instance dirigeante. Elles sont adaptées à la gravité des faits. L'employeur dispose de 2 mois à compter du moment où il a eu une connaissance exacte de la réalité de la nature ou des faits reprochés pour engager la procédure disciplinaire. La prescription peut être interrompue si des poursuites judiciaires sont engagées. La procédure disciplinaire peut être engagée par convocation à un entretien préalable, mise à pied conservatoire ou notification de la sanction ne nécessitant pas d'entretien préalable.

Ces suites peuvent porter sur <sup>52</sup>:

- Des actions disciplinaires prévues dans le règlement intérieur ou tout autre dispositif opposable au salarié ;
- La mise en œuvre des procédures judiciaires à l'encontre de(s) personne(s) mises en cause si les faits relèvent de telles procédures ;
- La modification des règles internes (règlement interne, charte éthique, etc.) de l'organisme,
- La mise à jour de la cartographie des risques de l'entité (dans le cadre de la mesure concernant le dispositif d'alerte de l'article 17 de la loi Sapin II) ;
- L'ouverture d'une enquête interne ou externe ;
- La réorganisation des opérations ou des services de la société (y compris celles adoptées dans le but de protéger le lanceur d'alerte des éventuelles représailles).

## BONNE PRATIQUE N° 11

Pour éviter tout risque de conflit d'intérêts, il convient de mettre en place un organe collégial de décision pour traiter les suites à donner à l'alerte.

## QUID DES DURÉES DE CONSERVATION DES DONNÉES ?

Conformément au Référentiel CNIL<sup>53</sup> :

- ◆ Les données relatives à une alerte peuvent être conservées en base active jusqu'à la prise de la décision définitive sur les suites à réserver à celle-ci. Cette décision doit intervenir dans un délai raisonnable à compter de la réception du signalement.
- ◆ Après la prise de la décision définitive sur les suites à réserver à l'alerte, les données pourront être conservées sous forme d'archives intermédiaires, « le temps strictement proportionné à leur traitement et à la protection de leurs auteurs, des personnes qu'ils visent et des tiers qu'ils mentionnent, en tenant compte des délais d'éventuelles enquêtes complémentaires ».
- ◆ Lorsqu'une procédure disciplinaire ou contentieuse est engagée à l'encontre d'une personne mise en cause ou de l'auteur d'une alerte abusive, les données relatives à l'alerte peuvent être conservées par l'organisation chargée de la gestion des alertes jusqu'au terme de la procédure ou de la prescription des recours à l'encontre de la décision intervenue.
- ◆ Les données peuvent être conservées plus longtemps, en archivage intermédiaire, si le responsable du traitement en a l'obligation légale (par exemple, pour répondre à des obligations comptables, sociales ou fiscales), ou à des fins probatoires dans l'optique d'un contrôle ou d'un contentieux éventuel, ou encore à des fins de réalisation des audits de qualité des processus de traitement des signalements.
- ◆ Les données anonymisées, n'entrant pas dans le cadre du RGPD peuvent être conservés sans limitation de durée.

<sup>52</sup> Recommandations de l'AFA, voir *supra* note n° 21.

<sup>53</sup> Référentiel CNIL n° 64 et 65, voir *supra* n° 22

# FICHE 6 : LES SOLUTIONS D'EXTERNALISATION DES DISPOSITIFS DE RECUEIL ET DE TRAITEMENT DES ALERTES

Comme évoqué précédemment, la loi laisse ouverte la possibilité pour les entreprises d'internaliser ou d'externaliser le dispositif de recueil et/ou de traitement des signalements.

Une externalisation peut être effectuée auprès d'un prestataire mettant à disposition des collaborateurs de l'entreprise (et le cas échéant des tiers) un numéro d'appel gratuit et une adresse électronique type xxx@alerte.com ou une plateforme informatique à partir de laquelle le prestataire devra :

- ▶ **Recueillir les signalements** en s'assurant qu'il contient les éléments indispensables pour être transmis au référent alerte de l'entreprise ;
- ▶ **Assurer le respect de la communication** aux différents stades de la procédure (délais de 7 jours ouvrés et 3 mois) ;
- ▶ **Assurer le respect des obligations de confidentialité de l'entreprise**, en canalisant la diffusion des informations sensibles au seul « référent Alerte » de l'entreprise ;
- ▶ **Effectuer un reporting périodique à l'entreprise** sous forme de tableaux (ex. nombre d'alertes, nature des alertes, suites données, etc).

Les prestataires sont nécessairement tenus par des engagements extrêmement stricts en ce qui concerne le respect de toutes les obligations (confidentialité, délais de communication avec les lanceurs d'alertes et l'entreprise, RGPD, etc).

## Quel sont les avantages et inconvénients de chaque dispositif ?

	Solution interne	Ligne téléphonique /adresse mail externalisée	Plateforme numérique externalisée
AVANTAGES	<ul style="list-style-type: none"> <li>• Moindre coût.</li> <li>• Plus forte réactivité en cas d'alerte urgente.</li> </ul>	<ul style="list-style-type: none"> <li>• Confiance accrue dans le dispositif par les lanceurs d'alertes.</li> <li>• Meilleure canalisation de la diffusion des informations confidentielles au sein de l'entreprise.</li> <li>• Meilleure canalisation de communication avec le lanceur d'alerte.</li> <li>• Meilleure allocation des ressources nécessaires en cas d'alertes nombreuses.</li> <li>• Interlocuteurs « humains » formés à écouter le lanceur d'alerte et communiquer avec l'entreprise.</li> </ul>	<ul style="list-style-type: none"> <li>• Confiance accrue dans le dispositif par les lanceurs d'alertes.</li> <li>• Meilleure canalisation de la diffusion des informations confidentielles au sein de l'entreprise.</li> <li>• Meilleure canalisation de communication avec le lanceur d'alerte.</li> <li>• Meilleure allocation des ressources nécessaires en cas d'alertes nombreuses.</li> <li>• Communication anonyme facilitée.</li> </ul>

	Solution interne	Ligne téléphonique /adresse mail externalisée	Plateforme numérique externalisée
LIMITES	<ul style="list-style-type: none"> <li>Moindre confiance dans le dispositif interne.</li> <li>Risques de non-respect de la confidentialité de l'identité du lanceur d'alerte et/ou des personnes mises en cause.</li> <li>Risque de favoriser les alertes auprès des autorités externes et/ou de médias.</li> <li>En cas d'un nombre significatif d'alertes, risque de mobilisation excessive de la fonction éthique &amp; compliance.</li> </ul>	<ul style="list-style-type: none"> <li>Coût (modéré sauf si accès à de multiples langues)</li> <li>Moindre possibilité de communiquer de manière anonyme.</li> </ul>	<ul style="list-style-type: none"> <li>Coût (significatif) qui ne se justifie qu'en cas d'un nombre d'alertes significatif.</li> <li>Selon les plateformes, pas de possibilité de contacter un interlocuteur « humain » mais recueil de signalement seulement possible au travers de la plateforme.</li> </ul>

# FICHE 7 : POUR ALLER PLUS LOIN

Alerte - Le nouveau régime des dispositifs d'alerte en France : comment conjuguer conformité et efficacité - Dossier par William Feugère, Cahiers de droit de l'entreprise n° 1, Janvier-Février 2023, dossier 1.

Alerte en entreprise - Alertes : où en sont les entreprises ? - Les clés de la réussite - Etude par François Jambin et Alexandre Chimi, Cahiers de droit de l'entreprise n° 1, Janvier-Février 2023, dossier 3.

Dispositif d'alerte professionnelle - Mise en conformité du dispositif d'alerte professionnelle d'EDF avec la directive « lanceur d'alerte ». - Partage d'expérience sur le déploiement d'un dispositif d'alerte mutualisé - Fiche pratique par Valérie Audoubert, François Jambin et Alexandre Chimi, Revue Internationale de la Compliance et de l'Éthique des Affaires n° 04, 01 août 2022, 205.

Dispositifs d'alerte professionnelle - Regards croisés sur les dispositifs d'alerte professionnelle et la protection du lanceur d'alerte à l'aune de la nouvelle législation française issue de la transposition de la directive européenne - Table ronde par Marie-Laure DENIS, Claire HÉDON, Patrick LEFAS et Roxana FAMILY, Revue Internationale de la Compliance et de l'Éthique des Affaires n° 04, 01 août 2022, entretien 189.

L'alerte et le lanceur d'alerte - L'éthique du lanceur d'alerte professionnelle - Etude par Isabelle Bufflier, Revue Internationale de la Compliance et de l'Éthique des Affaires n° 04, 01 août 2022, dossier 194.

L'alerte et le lanceur d'alerte - Le dispositif d'alerte interne au service de la protection du lanceur d'alerte - Etude par Renaud Mousty et Sylvain Mansotte, Revue Internationale de la Compliance et de l'Éthique des Affaires n° 04, 01 août 2022, dossier 192.

L'alerte et le lanceur d'alerte - Les conséquences de la loi de transposition du 21 mars 2022 sur la gestion des signalements et le traitement des alertes par les entreprises - Etude par Sophie Scemla, Thierry Dor et Diane Paillot de Montabert, Revue Internationale de la Compliance et de l'Éthique des Affaires n° 04, 01 août 2022, dossier 191.

Lanceurs d'alerte : un décret d'application lacunaire ne répondant pas aux attentes des entreprises - Commentaire par William Feugère, Revue Internationale de la Compliance et de l'Éthique des Affaires n° 06, 12 décembre 2022, comm. 284.

Protection - La protection des lanceurs d'alerte - Entretien par Sylvain Wasserman, Dominique Dedieu, Cédric Duchatelle, William Feugère et Laurence Goutard-Chamoux, Cahiers de droit de l'entreprise n° 2, Mars-Avril 2022, entretien 2.

Nouveau rôle et responsabilité du lanceur d'alerte - par Carmen BRICENO - Dossier La Responsabilité pénale des sociétés - Actes Pratiques et Ingénierie Sociétaire n° 186, Novembre-Décembre 2022.

GUIDE  
**DISPOSITIF  
D'ALERTE INTERNE**



Edition : Mars 2025



[WWW.AFJE.ORG](http://WWW.AFJE.ORG)



[WWW.CERCLE-ETHIQUE.NET](http://WWW.CERCLE-ETHIQUE.NET)