



ONUDC

Office des Nations Unies
contre la drogue et le crime

LANCEZ L'ALERTE, DÉFENDEZ LA SANTÉ !

**LIGNES DIRECTRICES SUR
LA PROTECTION DES LANCEURS
D'ALERTE DANS LE SECTEUR
DES SOINS DE SANTÉ**



LANCEZ L'ALERTE, DÉFENDEZ LA SANTÉ !

LIGNES DIRECTRICES SUR
LA PROTECTION DES LANCEURS
D'ALERTE DANS LE SECTEUR
DES SOINS DE SANTÉ



© Nations Unies, 2021.

Les appellations employées dans cette publication et la présentation des données qui y figurent n'impliquent de la part de l'Office des Nations Unies de lutte contre la drogue et le crime (ONUDC) aucune prise de position quant au statut juridique des pays, territoires, villes ou zones, ou de leurs autorités, ni quant au tracé de leurs frontières ou limites.

Le contenu de la présente publication ne reflète pas nécessairement les vues ou la politique de l'ONUDC ou des organismes qui y ont contribué, pas plus qu'il n'en vaut approbation.

L'ONUDC encourage l'utilisation, la reproduction et la diffusion des données contenues dans cette publication. Sauf mention contraire, ces données peuvent être copiées, téléchargées et imprimées à des fins d'études personnelles, de recherche et d'enseignement, ou pour être utilisées dans des produits ou services non commerciaux, à condition que l'ONUDC soit dûment mentionné comme source et titulaire des droits d'auteur et que rien ne laisse supposer que l'Office approuve les opinions, les produits ou les services des utilisateurs.

Toutes photographies : stock.adobe.com ; couverture © Adi ; p. vi, p. viii © fovito ; p. 4 © Patrizio Martorana ; p. 8 © Denis Yarkovoy ; p. 16 © Evgeny Chernyshov ; p. 26 © Patrick Daxenbichler ; p. 32 © Grispb ; p. 36 © Robert Demeter ; p. 40 © Alexandra Giese ; p. 52 © K. Ozawa ; p. 56 © outdoorsman.

Production éditoriale : Section des publications, de la bibliothèque et des services en anglais, Office des Nations Unies à Vienne.

TABLE DES MATIÈRES

Remerciements	v
Glossaire	vii
Résumé	ix
INTRODUCTION	1
PREMIÈRE PARTIE.	
MISE EN PLACE D'UNE POLITIQUE DE PROTECTION DES LANCEURS D'ALERTE	3
1. QUI EST UN LANCEUR D'ALERTE ?	5
1.1 Un membre de l'organisation	6
1.2 Des individus extérieurs à l'organisation.....	7
2. QU'EST-CE QUI PEUT ÊTRE SIGNALÉ ?.....	9
2.1 Déterminer les types d'actes répréhensibles qui peuvent être signalés	10
2.2 Déterminer ce qu'est exactement un acte répréhensible grave dans l'organisation	13
2.3 Définir et mettre en œuvre l'élément de « bonne foi »	14
3. OÙ FAIRE UN SIGNALEMENT ET COMMENT ?	17
3.1 Mettre en place des voies de communication internes, ouvertes et inclusives	17
3.2 Créer des interfaces de signalement accessibles et conviviales.....	20
3.3 Garantir la confidentialité tout au long du processus de signalement.....	21
DEUXIÈME PARTIE.	
TRAITER LES INFORMATIONS REÇUES ET ASSURER UNE PROTECTION	25
4. TRAITER UN SIGNALEMENT : ÉVALUATION INITIALE	27
4.1 Accusé de réception	27
4.2 Évaluation du signalement	28
5. MENER DES ENQUÊTES ET DES EXAMENS : ÉTABLIR LES FAITS	33
5.1 Conduite d'une enquête	33
5.2 Choix de la personne « idéale » pour mener des enquêtes ou des examens	35

6. TRAITER L'ACTE RÉPRÉHENSIBLE ET CLORE L'AFFAIRE.....	37
6.1 Traitement de l'acte répréhensible.....	38
6.2 Clôture de l'affaire.....	39
7. ASSURER LA PROTECTION DES LANCEURS D'ALERTE	41
7.1 Protection contre les traitements injustifiés.....	42
7.2 Mécanismes de protection permettant de prévenir les représailles ou d'y mettre fin...	43
7.3 Sanctionner les représailles.....	45
7.4 Fournir un soutien et un retour d'information au lanceur d'alerte	48

TROISIÈME PARTIE.

FORMATION ET SENSIBILISATION

51

8. FORMATION DES PREMIERS DESTINATAIRES DES SIGNALEMENTS, DES ENQUÊTEURS ET DU PERSONNEL.....	53
8.1 Formation des premiers destinataires des signalements	53
8.2 Formation des enquêteurs.....	54
8.3 Formation de tout le personnel	54
9. SENSIBILISER	57
10. TIRER LES ENSEIGNEMENTS DU PROCESSUS : ÉVALUATION DES RISQUES.....	59

REMERCIEMENTS

Ces lignes directrices ont été élaborées par l'Office des Nations Unies contre la drogue et le crime (ONUDC) grâce au généreux financement du Foreign, Commonwealth and Development Office du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord et du Bureau of International Narcotics and Law Enforcement Affairs des États-Unis d'Amérique.

L'ONUDC exprime sa profonde gratitude aux personnes qui ont mis leurs connaissances et leur expérience au service de l'élaboration de ces lignes directrices.

L'ONUDC tient à remercier tout particulièrement les personnes qui ont participé aux travaux du groupe d'experts, lequel a tenu une réunion virtuelle le 25 janvier 2021, et celles qui ont formulé des commentaires écrits et oraux : Juha Keränen, Conseiller ministériel, Ministère des finances de la Finlande ; Martin Fletcher, Directeur général de l'Australian Health Practitioner Regulation Agency et Professeur adjoint au Royal Melbourne Institute of Technology (RMIT University) ; May Giuliani, Conseillère juridique, Australian Health Practitioner Regulation Agency ; Aled Jones, Professeur de sécurité des patients et de qualité des soins de santé, School of Healthcare Sciences, Université de Cardiff ; Brian Mdlalose, Avocat de l'État, National Prosecuting Agency de l'Afrique du Sud ; Cherese Thakur, Coordinatrice du plaidoyer, amaBhungane Centre for Investigative Journalism, Afrique du Sud ; Georgia Georgiadou, Chef d'unité adjointe, Commission européenne ; Maria Mollica, Chargée de mission, Commission européenne ; Khadija Sharife, journaliste d'investigation, Coordinatrice de la Platform to Protect Whistleblowers in Africa, Afrique du Sud ; Gabriella Razzano, Directrice, OpenUp, Afrique du Sud ; Helené Donnelly OBE, Ambassadrice du changement culturel et Principale gardienne de la liberté d'expression, Staffordshire and Stoke on Trent Partnership National Health Service (NHS) Trust ; Leonie Raby, Conseillère principale pour le renseignement, National Guardian's Office, Royaume-Uni ; et Sam Bereket, Responsable du renseignement et de l'examen des affaires, National Guardian's Office, Royaume-Uni.

L'ONUDC souhaite également remercier les experts Sheryl Goodman, Présidente de Procurement Integrity Consulting Services, et Ashley Savage, spécialiste des signalements, des droits à l'information et de la gouvernance, ainsi que les consultants de l'ONUDC Suhaas Ema et Alberto Martinez Garcia, pour leur contribution substantielle à la rédaction de ces lignes directrices.

Les lignes directrices ont bénéficié de la précieuse contribution des membres du personnel de l'ONUDC qui ont revu et commenté diverses sections de ce guide : Giovanni Gallo, Julia Pilgrim, Louise Portas, Kari Rotkin, Jennifer Sarvary-Bradford, Tim Steele et Brigitte Strobel-Shaw du Service de la lutte contre la corruption et la criminalité économique.



GLOSSAIRE

Acte répréhensible à signaler : dans le cadre professionnel, manquement ou acte répréhensible, y compris omission, d'un niveau de gravité correspondant à celui qui est visé dans la politique de protection des lanceurs d'alerte de l'organisation.

Enquête interne : examen de signalements mené au sein d'une organisation, dans le but d'établir des faits.

Enquêteur ou agent chargé d'établir les faits : personne chargée de mener une enquête interne sur un acte répréhensible ou des représailles signalés dans l'organisation. Elle est également chargée de rédiger le rapport final et de formuler des recommandations sur les mesures à prendre à l'issue de l'enquête.

Interface de signalement : moyen par lequel une personne communique des informations grâce à un mécanisme de signalement. Exemples d'interfaces de signalement : face à face, téléphone, courriel, applications en ligne et numériques, entre autres.

Lanceur d'alerte : personne qui entre dans la définition de celles pouvant signaler des abus conformément à la politique de protection des lanceurs d'alerte de l'organisation et qui dénonce de bonne foi et/ou sur la base de soupçons raisonnables, en utilisant les voies de signalement établies, un acte répréhensible à signaler.

Organisation du secteur des soins de santé : toute entité, publique ou privée, qui fournit des biens et services médicaux ou connexes ou en coordonne la fourniture. Ce terme peut également désigner un établissement du secteur des soins de santé, défini comme tout établissement, public ou privé, qui fournit des biens et services médicaux ou connexes, notamment les hôpitaux militaires, les unités de santé mentale et les services médicaux des prisons.

Personne qui communique des informations : personne qui dénonce dans le cadre professionnel un acte répréhensible à signaler.

Premier destinataire du signalement : personne chargée de recevoir tout signalement fait par une personne qui communique des informations et, dans la plupart des cas, de procéder à son évaluation initiale.

Représailles : traitement injuste ou injustifié subi par un lanceur d'alerte en raison d'un signalement qu'il a fait.

Secteur des soins de santé : ensemble des personnes morales ou physiques intervenant dans la fourniture de biens et services médicaux et connexes et sa coordination.

Signalement : dénonciation d'une irrégularité qui s'est produite, se produit ou est susceptible de se produire au sein d'une organisation.

Voie de signalement : système permettant de dénoncer des actes répréhensibles et des irrégularités présumés de manière sûre, avec un risque de représailles aussi réduit que possible.



RÉSUMÉ

LA CORRUPTION : UN PROBLÈME ENDÉMIQUE DANS LE SECTEUR DES SOINS DE SANTÉ

Le secteur des soins de santé est vaste, complexe et exposé à la corruption¹. Ses vulnérabilités tiennent notamment à la complexité des systèmes nationaux de soins de santé, au large éventail d'activités que comprend la filière médicale et au grand nombre d'acteurs concernés, souvent issus des secteurs tant public que privé. En outre, compte tenu des quantités considérables d'avoirs qui sont en jeu, le secteur est particulièrement sensible à la corruption². Ces vulnérabilités peuvent également affaiblir les systèmes de soins, favoriser un gaspillage des ressources et fragiliser la résilience des pays – et leur agilité – face aux urgences sanitaires, compromettant ainsi la couverture des services de soins de santé essentiels et l'accès à ces services³. En l'absence de garanties et de contrôles dans la chaîne d'approvisionnement en produits médicaux, l'achat et la distribution de produits et de médicaments de mauvaise qualité, périmés voire falsifiés deviennent possibles⁴. La corruption permet la production, l'achat et l'utilisation de produits médicaux falsifiés⁵. Au mieux, ces produits sont inefficaces ; au pire, ils nuisent aux consommateurs. Dans les deux cas, ils mettent en danger la vie des personnes qui en ont le plus besoin.

Le coût estimé de la corruption dans le secteur des soins de santé est déjà très élevé en temps normal. Ainsi, d'après l'Organisation mondiale de la Santé (OMS), sur les 5 700 milliards de dollars dépensés dans le monde pour la santé en 2008, les fraudes et abus ont engendré des pertes d'un montant de 415 milliards (environ 7,3 %) ⁶.

En période de crise sanitaire, le risque de corruption dans le secteur des soins de santé est encore plus grand et ses effets dévastateurs deviennent encore plus évidents.

DÉNONCER LA CORRUPTION DANS LE SECTEUR DES SOINS DE SANTÉ : UNE ÉTAPE ESSENTIELLE POUR LUTTER CONTRE LES INFRACTIONS ET SAUVER DES VIES

Il est crucial de prévenir la corruption dans le secteur des soins de santé en raison du risque excessif qu'elle représente pour les vies humaines. Il est donc essentiel que les États et les organisations du secteur mettent en place pour ce faire des garanties et des mécanismes de contrôle⁷.

¹ Tim K. Mackey, Taryn Vian et Jillian Kohler, « The sustainable development goals as a framework to combat health-sector corruption », *Bulletin de l'Organisation mondiale de la Santé*, vol. 96, n° 9 (septembre 2018), p. 634 à 643.

² Voir, par exemple, la déclaration d'Oslo sur la corruption portant sur des quantités considérables d'avoirs, en particulier la recommandation 8, dans Office des Nations Unies contre la drogue et le crime (ONUDC), « Preventing and combating corruption involving vast quantities of assets: expert recommendations » (Vienne, 2019).

³ Mackey, Vian et Kohler, « The sustainable development goals as a framework to combat health-sector corruption », *Bulletin de l'Organisation mondiale de la Santé*, vol. 96, n° 9 (septembre 2018), p. 589 à 664.

⁴ ONUDC, Service de la recherche et de l'analyse des tendances, « Report on the COVID-19-related trafficking of medical products as a threat to public health », note de recherche (Vienne, 2020).

⁵ ONUDC, *Lutte contre la criminalité liée aux produits médicaux falsifiés : Guide de bonnes pratiques législatives* (Vienne, 2019).

⁶ Ben Jones et Amy Jing, « Prevention not cure in tackling health-care fraud », *Bulletin de l'Organisation mondiale de la Santé*, vol. 89, n° 12 (décembre 2011), p. 858 et 859.

⁷ ONUDC, « Accountability and the prevention of corruption in the allocation and distribution of emergency economic rescue packages in the context and aftermath of the COVID-19 pandemic », document d'orientation (Vienne, 2020).

Or, malgré toutes les mesures préventives qui peuvent être prises, la corruption ou d'autres actes répréhensibles graves peuvent toujours se produire. Il est donc indispensable que les organisations du secteur des soins de santé mettent en place des mécanismes permettant de détecter les actes répréhensibles et d'y remédier le plus tôt possible.

L'un de ces mécanismes consiste à encourager le personnel des organisations de soins de santé à signaler tout soupçon d'acte répréhensible et à protéger ce personnel contre toute forme de représailles.

À cet égard, en vertu de l'article 33 de la Convention des Nations Unies contre la corruption, les États parties sont tenus d'envisager d'incorporer dans leur système juridique interne des mesures appropriées pour assurer la protection contre tout traitement injustifié de toute personne qui signale aux autorités compétentes, de bonne foi et sur la base de soupçons raisonnables, tous faits concernant les infractions créées conformément à la Convention. Les États parties sont également tenus, en vertu du paragraphe 4 de l'article 8, d'envisager de mettre en place des mesures et des systèmes de nature à faciliter le signalement par les agents publics aux autorités compétentes des actes de corruption dont ils ont connaissance dans l'exercice de leurs fonctions.

La mise en place d'un système de signalement efficace et d'un mécanisme connexe de protection des lanceurs d'alerte est donc reconnue comme l'une des mesures les plus utiles pour détecter les actes répréhensibles à un stade précoce⁸ et permettre la prise rapide de mesures d'atténuation susceptibles d'empêcher que l'acte répréhensible signalé ne devienne un fait de corruption à grande échelle ou ne cause un préjudice aux patients. Dans le secteur des soins de santé, la mise en place d'un tel mécanisme de signalement peut donc prévenir des dommages et sauver des vies.

Les présentes lignes directrices proposent un processus en plusieurs étapes visant à aider les organisations à établir des politiques et procédures internes qui facilitent le signalement d'actes répréhensibles présumés et protègent les personnes qui communiquent des informations. Les lignes directrices comprennent les informations nécessaires à l'instauration d'une culture d'information ouverte et équitable, qui encourage les personnes à faire rapidement part de leurs préoccupations. Les étapes proposées sont les suivantes :

- *Définir* qui peut faire un signalement et ce qui peut être signalé ;
- *Instaurer* une culture positive du signalement ;
- *Identifier* les voies de signalement internes et les interfaces connexes ;
- *Établir* des mécanismes de confidentialité efficaces et des moyens de signalement anonyme ;
- *Mettre en place* des mécanismes permettant d'évaluer les signalements, d'enquêter en interne et de prendre les mesures correctives nécessaires ;
- *Protéger* efficacement les lanceurs d'alerte :
 - *en prévenant* les représailles, ou
 - *en mettant fin* aux représailles s'il y en a déjà eu ;
- *Établir* des mécanismes de lutte contre les représailles ;
- *Fournir* des conseils, un soutien et un retour d'information aux lanceurs d'alerte ;
- *Assurer* la formation et la sensibilisation aux processus de signalement nouvellement établis ;
- *Réfléchir* à des moyens durables et innovants de faire évoluer les politiques de protection des lanceurs d'alerte dans l'organisation.

Il est important de souligner qu'il n'existe pas de solution unique. Les décideurs doivent prendre en considération divers facteurs, qui tiennent compte à la fois du contexte spécifique dans lequel l'organisation rédige la politique relative à la protection des lanceurs d'alerte et des normes culturelles et sociétales propres à chaque pays.

Ces politiques peuvent être élaborées et appliquées par une organisation même si le pays où elle se trouve n'a pas adopté de législation sur la protection des lanceurs d'alerte. Lorsque de telles lois existent, la politique doit explicitement s'y référer afin que les lanceurs d'alerte potentiels soient correctement informés.

⁸ ONUDC, *Guide de ressources sur les bonnes pratiques en matière de protection des personnes qui communiquent des informations* (Vienne, 2015).

INTRODUCTION

Le 11 mars 2020, l'Organisation mondiale de la Santé (OMS) a déclaré que l'épidémie de maladie à coronavirus (COVID-19), maladie respiratoire causée par le coronavirus 2 du syndrome respiratoire aigu sévère (SARS-CoV-2), avait atteint le stade de pandémie¹. La crise sanitaire mondiale qui en a résulté a contraint les États à prendre des mesures d'urgence pour contenir et atténuer la propagation du virus. Le risque de corruption dans le secteur des soins de santé se trouvant ainsi augmenté, l'Office des Nations Unies contre la drogue et le crime (ONUDD) a averti qu'en prenant de telles mesures d'urgence, les États Membres avaient nécessairement relâché les garanties et fait passer la rapidité de la riposte et de l'effet avant la conformité, la surveillance et la responsabilité, ce qui ouvrait des possibilités de corruption non négligeables².

Le secteur des soins de santé est déjà considéré comme vulnérable à la corruption en temps normal³ ; cette vulnérabilité est amplifiée en période de crise sanitaire. La corruption peut même exacerber une épidémie ou la propagation d'un virus et saper les efforts visant à contenir une pandémie⁴.

Les présentes lignes directrices mettent l'accent sur l'importance d'établir une politique interne relative à la protection des lanceurs d'alerte dans le secteur des soins de santé afin de détecter les cas graves d'actes répréhensibles, y compris la corruption, qui peuvent se produire, se produisent ou se produiront au sein d'une organisation, de les traiter le plus tôt possible et de prendre des mesures pour en atténuer les conséquences néfastes, notamment sur la sécurité des patients et sur la réputation et les finances de l'organisation.

Ces lignes directrices sont destinées à toutes les organisations du secteur de la santé, publiques ou privées⁵, qui souhaitent adopter une politique efficace de protection des lanceurs d'alerte. Si elles peuvent servir de guide pour la rédaction d'une telle politique, elles n'ont pas vocation à être un modèle de politique. Elles s'adressent à la direction des organisations, aux décideurs, aux responsables de la conformité et à toute autre personne chargée de fixer, de rédiger et d'adopter des politiques internes et de veiller à leur mise en œuvre effective.

Les lecteurs sont guidés tout au long du processus d'adoption d'une politique de protection des lanceurs d'alerte, qu'il s'agisse de déterminer qui peut communiquer des informations ou ce qui peut être communiqué et comment, de mettre en œuvre des mesures de protection efficaces, de fournir des conseils et un retour d'information au lanceur d'alerte, de mener une enquête interne ou de prendre des mesures correctives. Les lignes directrices informent également les lecteurs sur la manière de dispenser la formation nécessaire, de sensibiliser l'ensemble du personnel d'une organisation et d'instaurer une culture positive du signalement.

Comme le montrent les lignes directrices, une organisation peut mettre en place un mécanisme de signalement et des mesures de protection connexes même s'il n'existe pas de cadre législatif dans les pays où elle est implantée. Axées sur le secteur des soins de santé, ces lignes directrices peuvent également être utiles aux organisations d'autres secteurs.

¹ ONUDD, « Accountability and the prevention of corruption in the allocation and distribution of emergency economic rescue packages ».

² Ibid.

³ Mackey, Vian et Kohler, « The sustainable development goals as a framework to combat health-sector corruption ».

⁴ Voir, par exemple, le rôle que la corruption aurait joué pendant l'épidémie d'Ebola, U4 Anti-Corruption Resource Centre, « Ebola and corruption overcoming critical governance challenges in a crisis situation », *U4 Brief*, n° 4 (mars 2015).

⁵ Les entreprises doivent également promouvoir la détection et le signalement des violations de leurs programmes de lutte contre la corruption. Pour plus d'informations, voir ONUDD, *Un programme de déontologie et de conformité contre la corruption pour les entreprises : guide pratique* (Vienne, 2013), p. 93.

PREMIÈRE PARTIE.

MISE EN PLACE D'UNE
POLITIQUE DE PROTECTION
DES LANCEURS D'ALERTE



Chapitre 1.

QUI EST UN LANCEUR D'ALERTE ?

Avant d'élaborer une politique, les responsables de la mise en œuvre doivent s'assurer qu'elle est conforme à la législation nationale. Ils doivent procéder à un examen du droit national dans les domaines suivants :

- Législation spécifique sur les lanceurs d'alerte et/ou les signalements protégés ;
- Législation anticorruption, y compris la législation relative aux services financiers ;
- Législation sur l'administration des services publics ;
- Toute autre législation relative à l'accès à l'information et à la protection des données qui pourrait s'appliquer à l'organisation.

Sous réserve d'un tel examen, toute organisation qui souhaite adopter une politique visant à établir des voies de signalement des actes répréhensibles juridiques et administratifs, ainsi qu'à assurer la protection des personnes qui dénoncent des actes répréhensibles à signaler, doit d'abord déterminer qui peut faire un signalement.

Si on limite de manière excessive la définition d'un lanceur d'alerte, les mesures de protection pourraient s'avérer inefficaces.

Dans l'article 33 de la Convention des Nations Unies contre la corruption, le terme « lanceur d'alerte » est délibérément écarté, au profit du terme plus large « personnes qui communiquent des informations ». Le Conseil de l'Europe définit le « lanceur d'alerte » comme « toute personne qui signale ou divulgue des informations sur une menace ou un préjudice pour l'intérêt public dans le cadre de sa relation de travail, que ce soit dans le secteur public ou privé »⁶. La Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union (également appelée directive européenne sur les lanceurs d'alerte) prévoit que le terme « lanceur d'alerte » s'applique aux « auteurs de signalement travaillant dans le secteur privé ou public qui ont obtenu des informations sur des violations dans un contexte professionnel »⁷. De nombreux pays n'utilisent pas le terme

⁶ Conseil de l'Europe, recommandation CM/Rec (2014)7 du Comité des ministres aux États membres sur la protection des lanceurs d'alerte, adoptée par le Comité le 30 avril 2014.

⁷ Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, *Journal officiel de l'Union européenne*, L. 305 (26 novembre 2019), art. 4. Cette directive s'applique à un large éventail de domaines d'intervention clés de l'Union européenne dans lesquels les violations des règles de l'Union européenne peuvent causer un préjudice à l'intérêt public, y compris le domaine de la santé publique.

« lanceur d’alerte ». Par exemple, ce terme n’apparaît pas dans le *Public Interest Disclosure Act* de 1998 du Royaume-Uni de Grande-Bretagne et d’Irlande du Nord, qui évoque plutôt les salariés ou travailleurs qui communiquent des informations dans l’intérêt public⁸. Selon l’une des définitions académiques les plus fréquemment citées, les « lanceurs d’alerte » sont « des membres d’organisations (anciens ou actuels) [qui dénoncent] des pratiques illicites, immorales ou illégitimes sous le contrôle de leurs employeurs à des personnes ou des organisations qui [...] prennent des mesures »⁹.

1.1 UN MEMBRE DE L'ORGANISATION

Dans la pratique, un lanceur d’alerte est souvent un membre d’une organisation qui prend connaissance d’actes répréhensibles dans des contextes liés au travail et décide de les signaler.

Il convient d’inclure les catégories suivantes de professionnels de la santé travaillant dans le secteur privé¹⁰ ou public, au moins, dans la définition de « personne qui communique des informations » :

- Le personnel du ministère de la santé, y compris les fonctionnaires, le personnel permanent et temporaire, le personnel administratif, les assistants, les secrétaires, le personnel de gestion des installations, les stagiaires et les bénévoles ;
- Le personnel des organismes de réglementation de la santé et/ou des autorités des soins de santé ;
- Le personnel des entreprises pharmaceutiques publiques et privées ;
- Le personnel des compagnies d’assurance maladie publiques et privées ;
- Le personnel des laboratoires publics et privés ;
- Les travailleurs et praticiens de la santé et des services sociaux ;
- Le personnel des hôpitaux et autres établissements de santé ;
- Les membres des conseils d’administration sanitaires locaux et nationaux ;
- Le personnel des services d’urgence et de transport (conducteurs ambulanciers, personnel paramédical, etc.) ;
- Le personnel des fournisseurs et distributeurs de médicaments et de fournitures médicales ;
- Le personnel des entreprises et des organisations intervenant dans la production, le commerce, la vente et la distribution de produits liés à la santé ;
- Le personnel d’organisations de la société civile liées au secteur des soins de santé (Médecins sans frontières, Fédération internationale des Sociétés de la Croix-Rouge et du Croissant-Rouge, etc.)¹¹.

La politique doit se concentrer sur les « membres de l’organisation », mais elle doit inclure toutes les catégories de personnel, sans limitation. À ce titre, les catégories de personnel suivantes devraient pouvoir signaler des actes répréhensibles potentiels : employés permanents et temporaires, consultants, vacataires, experts, stagiaires, travailleurs de la gestion des installations et bénévoles.

En d’autres termes, tous les individus internes à l’organisation devraient avoir le droit de signaler les cas d’irrégularités juridiques et disciplinaires dont ils pourraient avoir connaissance.

⁸ ONUDC, *Guide de ressources sur les bonnes pratiques en matière de protection des personnes qui communiquent des informations*.

⁹ Cette définition a été donnée par Maria P. Miceli et Janet P. Near en 1985 et demeure, à ce jour, la définition académique la plus largement utilisée. Voir Maria P. Miceli et Janet P. Near, « Organizational dissidence: The case of whistle-blowing », *Journal of Business Ethics*, vol. 4, n° 1 (février 1985).

¹⁰ ONUDC, *Un programme de déontologie et de conformité contre la corruption pour les entreprises*, p. 93.

¹¹ Les termes de cette liste doivent être lus conjointement aux définitions données dans le glossaire des présentes lignes directrices.

Par exemple, le National Health Service (NHS) du Royaume-Uni définit un lanceur d'alerte comme « un individu qui travaille pour une organisation du NHS ». La définition inclut également « les travailleurs intérimaires, les travailleurs temporaires, les étudiants et les bénévoles »^a.

La politique de l'ONU sur la protection contre les représailles des personnes qui signalent des manquements et qui collaborent à des audits ou à des enquêtes dûment autorisés s'applique à « tout fonctionnaire (quels que soient le type et la durée de son engagement), stagiaire, Volontaire des Nations Unies, vacataire ou consultant »^b.

^a Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, National Health Service (NHS) England, « External Whistle-blowing Policy », (février 2017).

^b Bulletin du Secrétaire général sur la protection contre les représailles des personnes qui signalent des manquements et qui collaborent à des audits ou à des enquêtes dûment autorisés, ST/SGB/2017/2/Rev.1, sect. 2.1.

En outre, la politique doit s'appliquer aux membres actuels et anciens de l'organisation, ainsi qu'aux candidats à l'emploi qui pourraient observer des actes répréhensibles ou des fraudes au cours du processus de recrutement ou d'autres négociations précontractuelles¹².

Il est important que les organisations soient claires lorsqu'elles définissent le terme « lanceur d'alerte », afin que les personnes susceptibles de communiquer des informations puissent facilement déterminer la portée et le champ d'application de la politique.

1.2 DES INDIVIDUS EXTÉRIEURS À L'ORGANISATION

La politique peut également élargir le champ des « personnes qui communiquent des informations » aux personnes extérieures qui ne sont pas employées par l'organisation, mais qui peuvent avoir connaissance de cas d'actes répréhensibles dans un contexte commercial ou contractuel. Cette catégorie peut inclure, par exemple, les intermédiaires, les partenaires commerciaux, les prestataires de services et les fournisseurs, les candidats à un marché public, les patients d'un hôpital ou leurs proches et les clients d'une société pharmaceutique. Il est important que les personnes chargées de rédiger la politique sur la protection des lanceurs d'alerte de l'organisation tiennent compte de la manière dont la politique sera diffusée aux personnes extérieures, de la façon dont les signalements émanant de personnes extérieures peuvent être reçus et traités et des éventuels moyens de recours disponibles.

Pendant la crise de la maladie à coronavirus (COVID-19), de nouveaux acteurs se sont fait connaître et jouent un rôle clef dans l'achat et la distribution de fournitures médicales essentielles (par exemple, des masques et des gants). En raison de l'urgence de la situation, les gouvernements et les entreprises privées ont désigné des intermédiaires pour contacter les entreprises étrangères et réaliser des achats sur le marché international en leur nom. En limitant le champ des personnes qui peuvent faire un signalement, ces opérations vulnérables pourraient sortir du champ d'application du mécanisme de signalement. Une politique solide doit être élaborée de sorte qu'elle puisse s'appliquer dans des circonstances exceptionnelles.

Qu'il existe ou non une loi sur la protection des lanceurs d'alerte, chaque organisation ou entité énumérée ci-dessus devra disposer d'une politique autonome pour son propre personnel. En outre, une politique sectorielle plus large, applicable à de multiples organisations travaillant au même échelon de la chaîne d'approvisionnement médicale, pourrait être envisagée. Toutefois, les organisations qui décident de mettre en œuvre de telles politiques peuvent se heurter à des difficultés, car elles devront peut-être harmoniser ou unifier leurs procédures afin de garantir la cohérence des signalements et de leur traitement.

¹² Voir, par exemple, Union européenne, Directive du Parlement européen et du Conseil sur la protection des personnes qui signalent des violations du droit de l'Union, art. 4, par. 3.



Chapitre 2.

QU'EST-CE QUI PEUT ÊTRE SIGNALÉ ?

Une politique sur la protection des lanceurs d'alerte doit énumérer les types d'actes répréhensibles qui peuvent être signalés. Même si une organisation est basée dans un pays qui a adopté une législation sur la protection des lanceurs d'alerte, il se peut que cette législation ne soit pas suffisamment spécifique. Par exemple, certaines lois prévoient la possibilité de signaler une question de « santé et de sécurité publiques », mais la plupart renvoient à des questions d'« intérêt public » ou d'« intérêt général »¹³.

Certaines lois sur la protection des lanceurs d'alerte couvrent les types suivants d'actes répréhensibles potentiels :

- Créer et présenter un danger pour la santé, la sécurité ou le bien-être publics ;
- Commettre un acte de mauvaise gestion, de gaspillage flagrant de fonds publics ou de manquement flagrant au devoir.

Par conséquent, il peut être difficile de mettre directement en œuvre une loi ou un règlement au niveau institutionnel. Le rôle d'une politique est également de fournir des informations supplémentaires et des détails sur les types d'actes répréhensibles qui peuvent être signalés en interne, en fonction des préoccupations et des spécificités de l'organisation.

Le terme « acte répréhensible » est défini dans les présentes lignes directrices comme un manquement à signaler qui comprend des actes, mais peut également inclure des omissions (ne pas faire quelque chose).

Par exemple, dans la politique sur les dénonciations faites dans l'intérêt public (lanceurs d'alerte) de l'Australian Health Practitioner Regulation Agency (AHPRA), une « dénonciation faite dans l'intérêt public » est définie comme la communication d'informations sur une personne, un agent public ou un organisme public qui montre, ou tend à montrer, l'existence d'une conduite inappropriée ou un acte de corruption. La politique fournit des exemples de conduite inappropriée pouvant donner lieu à une dénonciation faite dans l'intérêt public, notamment une conduite qui :

¹³ Voir, par exemple, France, 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, art. 6.

- Est illégale ;
- Constitue une mauvaise utilisation ou un gaspillage substantiel de l'argent ou des ressources de l'AHPRA ou du Conseil d'administration ;
- Constitue un manquement grave dans l'exercice d'une fonction de droit national ;
- Constitue une mauvaise administration qui porte atteinte à l'intérêt d'une personne de manière substantielle ou spécifique ;
- Représente un danger substantiel et spécifique pour la santé ou la sécurité du public ;
- Présente un danger substantiel et spécifique pour l'environnement^a.

^a Australie, Australian Health Practitioner Regulation Agency (AHPRA), « Public Interest Disclosure (Whistleblower) Policy » (mai 2020).

2.1 DÉTERMINER LES TYPES D'ACTES RÉPRÉHENSIBLES QUI PEUVENT ÊTRE SIGNALÉS

Définir l'étendue des actes répréhensibles à inclure dans la politique

Détecter et combattre la corruption dans une organisation est l'un des principaux objectifs d'une politique sur la protection des lanceurs d'alerte. Toutefois, cette politique ne doit pas limiter les actes répréhensibles à signaler aux activités de corruption.

Premièrement, un acte répréhensible peut être très grave sans être un acte de corruption.

Par exemple, le fait pour un employé d'un centre de soins de santé de ne pas stériliser les instruments chirurgicaux n'est probablement pas un acte de corruption, mais il constitue un danger pour la santé et la sécurité des autres membres du personnel de santé et des patients.

Deuxièmement, un acte répréhensible peut sembler être une violation administrative ou procédurale au départ, mais peut s'avérer faire partie d'un système de corruption plus vaste après enquête.

Par exemple, entre 1976 et 2009, la France a commercialisé un médicament « amaigrissant » appelé Mediator. Conçu à l'origine pour les personnes diabétiques en surpoids, cet agent anorexigène (coupe-faim) et hypolipidémique était un médicament sur ordonnance particulièrement intéressant pour les personnes qui souhaitaient simplement perdre un peu de poids. En 2007, le Dr Irène Frachon, pneumologue dans un hôpital public de Brest, a observé un nombre croissant de cas de maladies cardiaques dans sa patientèle et s'est rendu compte que tous les patients concernés avaient été traités au Mediator. Après une longue étude épidémiologique qui a confirmé ses inquiétudes, elle a signalé l'affaire à ses supérieurs et à l'Agence nationale de sécurité du médicament et des produits de santé (ANSM). À la suite de ce signalement et du retrait du médicament du marché en 2009, des investigations complémentaires menées par les services d'enquête et de poursuite ont révélé des soupçons de fraude de la part des Laboratoires Servier, qui commercialisaient le médicament. Le procès a débuté en 2019.

Par ailleurs, le scandale dit « du sang contaminé » en France a débuté en avril 1991, à la suite de la publication d'un article de la médecin et journaliste Anne-Marie Casteret dans l'hebdomadaire *L'Événement du jeudi* prouvant que le Centre national de transfusion sanguine (CNTS) avait sciemment distribué des produits sanguins contaminés par le VIH à des hémophiles en 1984 et 1985. Les procédures judiciaires ont mis à jour des actes de corruption et des infractions liées à la fraude à grande échelle, y compris des actes commis hors de France. Par exemple, certains gouvernements avaient retardé la mise sur le marché d'un test sanguin utilisé aux États-Unis d'Amérique au profit d'un test développé en France. En 1999, Laurent Fabius, alors Premier Ministre issu du Parti socialiste, Georgina Dufoix, alors Ministre des affaires sociales, et Edmond Hervé, alors Ministre de la santé, ont été inculpés d'homicide involontaire.

En outre, le fait de limiter les actes répréhensibles à signaler à la corruption peut obliger les personnes qui les détectent à vérifier s'ils constituent un acte de corruption avant de les signaler. Une telle situation peut exposer ces personnes, leurs collègues et même leurs proches à des risques.

Il est donc essentiel pour l'organisation de déterminer quelles catégories d'actes répréhensibles, au-delà de la fraude, de la corruption et des abus, peuvent être signalées par ses membres.

Lorsqu'elle définit les catégories d'actes répréhensibles à inclure dans la politique sur la protection des lanceurs d'alerte, l'organisation doit tenir compte des trois points suivants :

1. Les griefs personnels n'entrent généralement pas dans le champ des actes répréhensibles à signaler dans le cadre des lois et politiques sur la protection des lanceurs d'alerte. Néanmoins, il devrait également être possible de faire part de ces problèmes. Il convient d'élaborer une politique de signalement distincte à cet égard.

Par exemple, dans la politique sur la dénonciation faite dans l'intérêt public (lanceurs d'alerte) de l'AHPR, si des personnes ont un grief personnel concernant l'AHPR ou un conseil d'administration sans qu'il existe un manquement grave, elles sont fortement encouragées à utiliser les voies de recours prévues pour traiter de tels griefs. Par exemple, si leur préoccupation porte sur une décision particulière prise en vertu du droit national, elles sont invitées à déposer une plainte ou à communiquer des informations en utilisant les procédures définies sur la page « Plaintes et communication d'information » du site Web de l'AHPR^a.

^a Australie, Australian Health Practitioner Regulation Agency (AHPR), « Public Interest Disclosure (Whistleblower) Policy » (mai 2020).

Toutefois, le signalement de questions relatives au personnel, telles que des conflits entre la personne concernée et un autre membre du personnel¹⁴, des griefs liés aux performances et d'autres questions relatives aux ressources humaines, pourrait constituer une alerte si ces questions sont considérées comme dangereuses pour la santé et le bien-être du personnel et des utilisateurs des services de soins de santé. Les cas d'intimidation et de harcèlement doivent également être visés en raison de leur incidence sur le bien-être du personnel et des patients. L'intimidation et le harcèlement peuvent également être utilisés comme une forme de représailles contre des personnes qui ont fait part de leurs préoccupations. Dans tous les cas, ces actes sont suffisamment graves pour entrer dans le champ des actes répréhensibles à signaler.

2. La politique doit permettre de signaler les cas d'actes répréhensibles qui se sont produits, se produisent ou sont susceptibles de se produire, ainsi que les tentatives de dissimulation de tels actes¹⁵.
3. La politique doit préciser que toute clause de confidentialité ou de non-divulgence qui peut se trouver dans le contrat liant ces individus à l'organisation ne s'appliquera pas aux catégories d'actes répréhensibles à signaler visées dans la politique.

Définir un seuil de gravité

Le coût de la protection d'un lanceur d'alerte peut être élevé. D'importantes ressources financières et humaines doivent être allouées pour prévenir les représailles et y mettre fin de manière efficace. De nombreux pays ont ainsi été amenés à définir un seuil de gravité de l'information communiquée. Alors que certains pays ont choisi d'inclure le concept d'intérêt public dans leurs lois, d'autres ont utilisé des termes tels que « grave » ou « sérieux » pour définir les catégories d'actes répréhensibles à signaler.

¹⁴ Voir, par exemple, Union européenne, Directive du Parlement européen et du Conseil sur la protection des personnes qui signalent des violations du droit de l'Union, art. 22.

¹⁵ Ibid, art. 5, par. 2.

Quelle que soit l'approche retenue, seules les personnes qui signalent certains types de comportements devraient être protégées. Il est donc important de préciser un seuil de gravité dans la classification des comportements qui constituent des actes répréhensibles à signaler.

Par exemple, un membre du personnel qui signale qu'un collègue a emporté chez lui un stylo provenant du stock de fournitures de bureau ne bénéficie pas de la protection réservée aux lanceurs d'alerte.

Néanmoins, les lois et les politiques ne doivent pas limiter excessivement les informations qui peuvent être communiquées, sous peine de les rendre inefficaces.

En ce qui concerne les infractions liées à la corruption, certains pays n'incriminent pas les cas de corruption *de minimis*. Cependant, on encourage fortement à inclure ces cas dans le champ des actes répréhensibles à signaler dans le contexte de la protection des lanceurs d'alerte. En outre, la corruption généralisée et systématique, quelle que soit son ampleur, peut avoir une incidence négative sur la prestation des services de soins de santé¹⁶ et doit être considérée comme atteignant le seuil de gravité requis pour constituer un acte répréhensible à signaler.

L'organisation doit définir ce qu'elle considère comme un acte répréhensible « grave » ou « sérieux »

Plus les exigences relatives à l'évaluation de la qualité et de la gravité des informations avant leur communication sont rigoureuses, plus il est probable que les personnes garderont le silence – en particulier si elles ne sont pas sûres d'être protégées¹⁷ – ou prendront des risques inutiles en évaluant ou en enquêtant sur les informations par elles-mêmes. L'incertitude quant à la gravité des allégations peut décourager le signalement. Les personnes qui communiquent des informations ne devraient pas être tenues de fournir des preuves positives ; il devrait suffire de soulever des préoccupations ou des soupçons raisonnables. En outre, le personnel doit être encouragé à faire part de ses préoccupations à un stade précoce au lieu d'attendre de disposer de preuves.

Il est donc important de définir clairement ce qui est considéré comme un acte répréhensible « grave » ou « sérieux » dans une organisation. À cette fin, certaines organisations donnent dans leurs politiques une liste non exhaustive des types d'actes répréhensibles à signaler qui répondent à ces critères.

Dans le secteur des soins de santé en particulier, les lois et règlements en vigueur définissent souvent les actes répréhensibles « graves » ou « sérieux » comme des comportements qui présentent un risque pour la santé et la sécurité publiques¹⁸. Aux États-Unis, les infractions à signaler sont définies comme des « pratiques qui menacent la santé et la sécurité publiques »¹⁹.

Ainsi, pour reprendre l'exemple précédent, dans un contexte hospitalier, le terme « fournitures de bureau » peut également inclure le stock de médicaments ou de substances utilisés pour traiter les patients. Ces substances peuvent être extrêmement dangereuses et doivent être utilisées avec prudence. Si un membre du personnel, tel qu'un travailleur de la santé, voit un collègue prendre de telles substances sans justification apparente, un tel comportement pourrait être signalé, car il constitue une menace potentielle pour la santé et la sécurité.

¹⁶ Sarah Briery et Elif Ozdemir, « Petty corruption in the provision of public services in Ghana », Washington University in St. Louis, pour Strengthening Action against Corruption (STAAC)-Ghana. Disponible sur demande auprès de STAAC-Ghana [Foreign, Commonwealth and Development Office (anciennement Department for International Development)].

¹⁷ ONUDC, *Guide de ressources sur les bonnes pratiques en matière de protection des personnes qui communiquent des informations*.

¹⁸ Voir, par exemple, Conseil de l'Europe, recommandation CM/Rec (2014)7 du Comité des ministres aux États membres sur la protection des lanceurs d'alerte, adoptée par le Comité en avril 2014. On trouvera de plus amples détails dans ONUDC, *Guide de ressources sur les bonnes pratiques en matière de protection des personnes qui communiquent des informations*.

¹⁹ États-Unis d'Amérique, National Nurses United, « Whistleblower Protection Laws for Health-care Workers ».

Il est important de garder à l'esprit que les références à la « santé » et à la « sécurité », entre autres termes, sont plus facilement compréhensibles pour les profanes, et les organisations devraient s'efforcer d'utiliser ce langage simple lorsqu'elles définissent les actes répréhensibles « graves » ou « sérieux ».

2.2 DÉTERMINER CE QU'EST EXACTEMENT UN ACTE RÉPRÉHENSIBLE GRAVE DANS L'ORGANISATION

Une fois que l'organisation a décidé que les actes répréhensibles à signaler doivent, premièrement, ne pas se limiter aux activités de corruption et, deuxièmement, atteindre un certain seuil de gravité, il est important de déterminer les types d'actes répréhensibles qui figureront dans la politique.

Par conséquent, avant d'adopter une politique sur la protection des lanceurs d'alerte, l'organisation peut devoir procéder à une évaluation interne des risques afin de déterminer les types d'actes répréhensibles qui peuvent se produire en son sein et qui peuvent soit conduire à la corruption, soit présenter un risque grave pour la santé et la sécurité publiques.

Selon l'organisation et sa position spécifique dans la chaîne d'approvisionnement des soins de santé, ces violations peuvent inclure :

- Des violations des règles de santé et de sécurité ;
- Le non-respect des procédures de passation de marchés pour les soins de santé et les fournitures médicales ;
- Le versement de pots-de-vin directs par les patients au personnel de santé ;
- La falsification et la manipulation des factures et des relevés de compte afin qu'ils indiquent des montants incroyablement bas ou élevés ;
- L'achat de fournitures qui ne semblent pas correspondre à celles dont l'acquisition est prévue ou à l'usage auquel elles sont destinées ;
- La réception ou la distribution de médicaments périmés, faux ou falsifiés ;
- Les traitements médicaux inutiles ;
- Un traitement préférentiel indu accordé aux fournisseurs médicaux privés ;
- Des soins dangereux prodigués aux patients ;
- Une mauvaise pratique clinique ou autre faute professionnelle pouvant nuire aux patients ;
- Un manquement à la protection des patients ;
- La mauvaise administration de médicaments ;
- L'absence de formation du personnel ;
- Des conditions de travail dangereuses ;
- Une culture de harcèlement, de discrimination, d'abus et d'exploitation (notamment fondée sur le sexe et la race).

Par exemple, un membre du personnel du ministère de la santé participant à la procédure de passation de marchés pour des fournitures médicales se rend compte que le comité désigné pour sélectionner le lauréat ne dispose d'aucune expertise médicale qui pourrait lui permettre de vérifier le caractère approprié des fournitures proposées par les candidats. Une telle situation doit être considérée comme devant être signalée, car il existe un risque que les fournitures médicales achetées ne correspondent pas aux normes prescrites, ou qu'elles soient périmées ou falsifiées.

Selon la politique de l'Organisation mondiale de la Santé (OMS) sur le signalement des actes répréhensibles et la protection contre les représailles, les actes répréhensibles à signaler sont définis comme des « irrégularités [qui] entraînent un risque significatif pour l'Organisation (c'est-à-dire nuisant aux intérêts, à la

réputation, aux activités ou à la gouvernance de l'OMS) ». Par conséquent, la politique s'applique notamment au signalement de chacun des actes suivants :

- La fraude (c'est-à-dire un acte délibéré et trompeur visant à obtenir un avantage indu – argent, biens ou services – par tromperie ou par un autre moyen contraire à l'éthique) ;
- La corruption ;
- Le gaspillage des ressources ;
- Le sabotage ;
- Tout acte représentant un danger important et précis pour la santé ou la sécurité publiques ;
- L'exploitation et les abus sexuels²⁰.

Il convient de mentionner que certaines organisations prévoient également la possibilité de faire part de préoccupations concernant des mesures spécifiques de santé et de sécurité prises ou appliquées pendant la pandémie de COVID-19²¹.

2.3 DÉFINIR ET METTRE EN ŒUVRE L'ÉLÉMENT DE « BONNE FOI »

Le concept de bonne foi figure parfois dans la législation nationale ou dans les politiques des organisations afin que les individus ne signalent pas sciemment des informations qui sont fausses et qui pourraient avoir pour but de nuire à une personne ou de la discréditer par le biais d'allégations intentionnellement fausses, et des dispositions visent alors à prévenir et/ou à punir de tels signalements. Ce type de comportement, probablement rare, ne doit pas être accepté, et la politique établie par l'organisation doit également prévoir des processus, y compris des processus disciplinaires, pour empêcher les personnes de communiquer de telles informations.

L'exigence de bonne foi dans le contexte de la protection des lanceurs d'alerte doit être considérée comme satisfaite lorsqu'une personne a des motifs raisonnables de croire que l'information communiquée est vraie²². À cet égard, c'est une bonne pratique de veiller à ce que le concept de bonne foi soit lié à l'information et non au motif du signalement.

La Convention des Nations Unies contre la corruption prévoit, dans son article 33, que les signalements doivent être faits « de bonne foi et sur la base de soupçons raisonnables ».

La loi type visant à faciliter et à encourager le signalement des actes de corruption et à protéger les lanceurs d'alerte et les témoins de l'Organisation des États américains (OEA) va plus loin et prévoit une présomption de bonne foi des lanceurs d'alerte. Cette pratique législative déplace la charge de la preuve sur l'accusé en lui demandant de démontrer qu'aucune violation n'a eu lieu, et protège le lanceur d'alerte.

Dans les textes les plus récents, comme la Directive du Parlement européen et du Conseil sur la protection des personnes qui signalent des violations du droit de l'Union, la notion de bonne foi a été remplacée par des références à des « motifs raisonnables ». Le concept de motifs raisonnables peut réduire le risque d'interprétation erronée et de focalisation excessive sur le motif de la personne qui communique des informations. En application de la Directive, les pays de l'Union européenne adoptent le concept de motifs raisonnables, en remplaçant le terme « bonne foi » par des renvois à ce concept partout où il apparaît dans le droit actuel.

²⁰ Organisation mondiale de la Santé (OMS), « Signalement des actes répréhensibles et protection contre les représailles à l'OMS : politique et procédures » (2015). Voir également Nieves Zúñiga, « Gender sensitivity in corruption reporting and whistleblowing », *U4 Helpdesk Answer*, n° 10 (juin 2020).

²¹ L'une de ces organisations est l'Occupational Safety and Health Administration (OSHA) du Ministère du travail des États Unis. Voir OSHA, « Whistleblower laws enforced by OSHA », disponible à l'adresse : www.whistleblowers.gov/.

²² ONUDC, *Guide de ressources sur les bonnes pratiques en matière de protection des personnes qui communiquent des informations*. Voir également « Frequently asked questions: "Does the intention behind the disclosure matter?" » (Questions fréquemment posées : l'intention à l'origine du signalement est-elle importante ?), disponible à l'adresse : <https://whistleblower-protection.eu/>.

Que se passe-t-il si l'information se révèle finalement être fausse ?

Si, à l'issue de l'enquête (ou du processus d'établissement des faits), il s'avère que l'information communiquée ne constitue pas une violation, aucune mesure ne doit être prise à l'encontre du lanceur d'alerte ou de la personne qui a communiqué des informations.

La bonne foi ou les motifs raisonnables sont évalués au moment du signalement des faits ; ce qui compte, c'est que les lanceurs d'alerte croient que l'information est vraie au moment où ils la communiquent.

Pour reprendre l'exemple du personnel de santé qui prend des fournitures médicales dans le stock de l'hôpital sans justification apparente, cette action peut finalement être considérée comme parfaitement justifiée. Aucune mesure ne doit être prise à l'encontre de la personne qui a communiqué l'information, puisqu'elle l'a fait en croyant qu'elle était vraie, ou à l'encontre de la personne visée par cette information.

Que se passe-t-il si le signalement est fait de mauvaise foi ?

Lorsqu'il est prévu dans la législation nationale ou dans la politique d'une organisation, le concept de bonne foi doit être lié à l'information, et non au lanceur d'alerte. Comme indiqué précédemment, le motif du signalement ne devrait pas être pertinent²³ si la personne qui communique des informations remplit les critères susmentionnés et croit que les informations sont vraies au moment du signalement.

Par conséquent, peu importe que la relation personnelle entre la personne qui communique des informations et la personne visée par le signalement soit bonne ou mauvaise ; ce qui compte, c'est que la personne qui communique l'information la croit vraie.

Par exemple, une personne peut signaler une violation commise par un supérieur hiérarchique même si l'on sait que ces deux personnes ne s'apprécient pas. La personne peut même chercher à faire licencier son supérieur hiérarchique dans l'espoir d'obtenir une promotion. Toutefois, cette motivation ne doit pas être prise en considération si la personne qui communique des informations croit réellement qu'elles sont vraies.

²³ Ibid.



Chapitre 3.

OÙ FAIRE UN SIGNALEMENT ET COMMENT ?

La plupart des législations nationales anticorruption prévoient la possibilité de signaler les actes de corruption aux services d'enquête et de poursuite (telles que la police, le ministère public ou les autorités chargées de la lutte contre la corruption) ou à un médiateur, selon le cas.

Toutefois, si une organisation souhaite mettre en place une politique sur la protection des lanceurs d'alerte, il est également important de créer des voies internes spécifiques pour traiter ces signalements. En fait, certaines législations nationales²⁴ évoquent la possibilité de faire un signalement à un employeur (qu'il s'agisse d'un superviseur, d'une commission ou d'une autorité spéciale, d'une société externe chargée de recevoir les signalements ou de toute autre personne dans l'organisation).

Une politique interne forte qui garantit cette possibilité et permet au personnel de signaler en toute sécurité d'éventuels actes répréhensibles au sein de leur organisation tout en les protégeant contre les mesures de rétorsion et les représailles est toujours nécessaire. En conséquence, les organisations sont invitées à mettre en place des voies de signalement internes, ouvertes et inclusives, accessibles par diverses interfaces de signalement conviviales garantissant un niveau élevé de confidentialité.

3.1 METTRE EN PLACE DES VOIES DE COMMUNICATION INTERNES, OUVERTES ET INCLUSIVES

En fonction du statut et de la situation de l'organisation, plusieurs voies peuvent être établies.

Dans certains cas, si l'organisation n'est pas en mesure de l'établir en interne, une voie de signalement pourrait être prévue au niveau d'un organe de contrôle indépendant.

Par exemple, dans le domaine des marchés publics, une voie de signalement peut être créée au niveau de l'autorité de régulation des marchés publics^a.

^a C'est le cas, par exemple, en Grèce, où une plateforme réservée aux signalements a été mise en place au sein de l'autorité unique des marchés publics hellénique. Pour plus d'informations, voir Autorité hellénique unique des marchés publics, « Whistle-blowing platform in public procurement », disponible à l'adresse : <https://www.eaadhsy.gr/>.

²⁴ Voir, par exemple, Ghana, *Whistleblower Act* (Act No. 270) (2006), sect. 3.

Toutefois, dans la mesure du possible et en fonction de son statut (public ou privé), il est toujours recommandé à l'organisation de mettre en place des voies de signalement internes pour les raisons exposées ci-dessous.

Tout d'abord, la mise en place de ces voies est considérée comme une bonne pratique internationale, car elle « fait partie des bonnes pratiques de gestion et de gouvernance transparentes »²⁵, en particulier dans le secteur public. Dans certains pays, certaines sociétés du secteur privé ont l'obligation de se doter de voies de signalement internes si elles souhaitent être cotées sur les marchés boursiers²⁶.

Deuxièmement, les voies de signalement internes permettent aux organisations d'être informées des actes répréhensibles à un stade précoce, ce qui leur permet de prendre des mesures d'atténuation en temps voulu afin d'éviter d'avoir à mener une enquête.

Troisièmement, lorsque des cas d'actes répréhensibles sont signalés dans des succursales de grandes sociétés multinationales situées dans différents pays, les voies de signalement internes permettent de réagir de manière plus rapide, mieux adaptée et plus efficace que les autorités nationales, dont la compétence peut être limitée aux cas d'actes répréhensibles qui ont lieu dans un lieu spécifique.

Toute politique établie par une organisation doit prévoir des mécanismes de signalement interne, mais les membres du personnel d'une organisation ne se sentent pas toujours à l'aise pour signaler certains actes répréhensibles directement à leur superviseur, ou en personne²⁷. Afin de résoudre ce problème, le terme « signalement interne » devrait être défini de manière large, et non se limiter à la communication d'informations, en personne, aux superviseurs directs.

Compte tenu de ce qui précède, il est recommandé de prendre les mesures ci-dessous :

Premièrement, la politique doit permettre de faire un signalement directement à la direction de l'organisation. Dans certains cas, la politique doit également prévoir la possibilité de signaler des actes répréhensibles à des responsables situés à un niveau hiérarchique plus élevé que le superviseur direct. Cette option doit toujours figurer parmi les voies de signalement possibles établies par la politique.

Deuxièmement, l'organisation pourrait également étudier la viabilité de la création d'une unité interne indépendante chargée de recevoir le signalement d'actes répréhensibles présumés. Par exemple, elle pourrait créer une unité dédiée à cet effet au sein du département de la conformité.

Troisièmement, l'organisation doit recenser les organes indépendants, le cas échéant, qui sont chargés de recevoir les signalements dans leur secteur, et les désigner comme des voies de signalement possibles. Il peut s'agir d'autorités réglementaires (par exemple, les autorités de réglementation de la santé), de bureaux d'inspecteurs généraux, de bureaux d'auditeurs généraux ou d'autres commissions. Dans le secteur privé en particulier, le rôle de la Chambre de commerce pourrait être envisagé. Dans certains pays, les bureaux des inspecteurs du travail sont en mesure de recevoir des signalements concernant certaines violations administratives et légales liées au travail²⁸. Par ailleurs, comme les salariés ne se sentent pas toujours à l'aise pour recourir à ces options, les entreprises peuvent désigner une personne de confiance comme médiateur²⁹.

Enfin, les politiques de protection des lanceurs d'alerte pourraient également prévoir « d'autres voies de signalement internes », telles que des prestataires de services externes qui gèrent des centres d'appel ou des lignes d'assistance téléphonique. Les organisations peuvent souhaiter confier ces services à des sociétés

²⁵ Conseil de l'Europe, Protection des lanceurs d'alerte, recommandation CM/Rec (2014)7 et exposé des motifs (2014).

²⁶ Aux États-Unis, la Securities and Exchange Commission, tenant compte de la section 406 de la loi Sarbanes Oxley (2002), a adopté des amendements au Code of Federal Regulations (CFR), notamment 17 CFR parties 228 et 229, qui imposent aux entreprises d'adopter des codes déontologiques prévoyant également des voies de signalement internes. Par exemple, à la suite de ces modifications, la National Association of Securities Dealers Automated Quotations (NASDAQ) (règle des marchés boursiers 5610) et le New York Stock Exchange (NYSE) (sect. 303.A10 du manuel des sociétés cotées) exigent des sociétés cotées qu'elles élaborent des procédures permettant aux employés de signaler les actes illicites.

²⁷ Voir, par exemple, en ce qui concerne le secteur privé, ONUDC, *Un programme de déontologie et de conformité contre la corruption pour les entreprises*, p. 93.

²⁸ C'est notamment le cas en France, en vertu de l'article L8113-5 du Code du travail.

²⁹ ONUDC, *Un programme de déontologie et de conformité contre la corruption pour les entreprises*.

extérieures indépendantes. On trouve souvent cette option dans le secteur privé, car elle offre un degré d'indépendance et de neutralité que d'autres voies de signalement purement internes ne garantiraient peut-être pas.

En résumé, l'organisation dispose de plusieurs options pour définir des voies de signalement :

- La possibilité de signaler directement les cas d'actes répréhensibles à la direction (c'est-à-dire aux supérieurs), qui ne doit pas être limitée aux supérieurs hiérarchiques directs du lanceur d'alerte ;
- La mise en place d'une unité indépendante dans l'organisation qui se consacre à la réception des signalements d'actes répréhensibles présumés, par exemple au sein du département de la conformité, le cas échéant ;
- La désignation d'un médiateur ou d'un autre organisme indépendant suscitant une grande confiance, y compris les autorités réglementaires, le cas échéant, pour recevoir les signalements ;
- Le recours aux services d'un prestataire externe indépendant.

Il est considéré comme une bonne pratique pour les organisations de prévoir plusieurs voies de signalement dans leur politique pour les personnes qui souhaitent signaler un acte répréhensible. Faire un signalement à la direction doit toujours apparaître comme l'une des options possibles. Par conséquent, la formation des cadres est une composante essentielle de toute politique sur la protection des lanceurs d'alerte. C'est pourquoi le personnel ayant des responsabilités de gestion devrait au moins recevoir des informations et une formation sur la manière de recevoir ces signalements et sur ce qu'il convient de faire des informations reçues³⁰. Le personnel est plus susceptible de faire confiance à un système dans lequel le destinataire de l'information a été correctement formé.

Il convient de noter que le manque de protection, la crainte de représailles et le degré de confidentialité peuvent, dans certains cas, avoir une plus grande incidence sur les femmes lorsqu'elles décident s'il convient ou non de signaler un acte répréhensible³¹.

C'est pourquoi, quelle que soit la taille de l'organisation ou la nature de ses activités, il est essentiel que les voies de signalement soient ouvertes à tous les membres et tiennent compte de la dimension de genre³². Par conséquent, les organisations doivent envisager des moyens de créer des voies efficaces pour le signalement des actes répréhensibles, tout en tenant compte des différents besoins et vulnérabilités des hommes, des femmes et des groupes minoritaires. Elles doivent également utiliser un langage et une communication inclusifs et développer des voies visibles qui tiennent compte de la dimension de genre pour le signalement des actes répréhensibles³³. Prévoir toute une série de voies de signalement contribuera à réduire les différences entre les sexes dans les préférences en matière d'information, et les destinataires des signalements devraient être formés à y apporter l'attention voulue³⁴.

Enfin, les organisations doivent garder à l'esprit que le destinataire de l'information peut également être autorisé à recevoir et à demander des informations concernant des actes répréhensibles potentiels et à enquêter à ce sujet. Ce pouvoir varie en fonction de la personne chargée de recevoir l'information et de ses responsabilités. Les supérieurs hiérarchiques et les services de conformité, par exemple, peuvent prendre des mesures de protection immédiates, tandis que les prestataires de services externes ne peuvent que conseiller à l'organisation de prendre de telles mesures. Par conséquent, la formation dispensée doit aborder non seulement la manière de recevoir les signalements d'actes répréhensibles présumés, mais aussi ce qu'il convient de faire de ces signalements (écrits et/ou verbaux). En outre, les supérieurs doivent être formés sur la manière de communiquer les informations et à qui (c'est-à-dire quelle entité/autorité est désignée par la politique comme responsable du traitement des signalements et de l'ouverture des enquêtes),

³⁰ Voir la troisième partie des présentes lignes directrices.

³¹ Brierly et Ozdemir, « Petty corruption in the provision of public services in Ghana ».

³² Sir Robert Francis QC, *Freedom to Speak Up: An independent review into creating an open and honest reporting culture in the NHS*, février 2015, p. 21.

³³ Zúñiga, « Gender sensitivity in corruption reporting and whistleblowing ».

³⁴ Ibid.

tout en veillant, le cas échéant, à ce que la confidentialité du nom et de l'identité du lanceur d'alerte soit garantie et préservée. Les politiques devraient accorder le statut de lanceur d'alerte à ceux qui font un signalement par les voies voulues et devraient garantir l'anonymat de ces personnes.

3.2 CRÉER DES INTERFACES DE SIGNALEMENT ACCESSIBLES ET CONVIVIALES

Lorsque l'organisation a déterminé le meilleur type de voies de signalement, en tenant compte de son statut et de sa structure, elle doit ensuite établir différentes interfaces de signalement. Chaque membre du personnel d'une organisation peut se sentir plus à l'aise avec certaines interfaces, telles que les réunions en face à face, les appels téléphoniques, les messages enregistrés, les courriels, les plateformes en ligne ou même les applications pour smartphones³⁵.

Un bon mécanisme de signalement prévoit un large éventail d'interfaces, permettant aux individus de choisir d'utiliser celle avec laquelle ils se sentent le plus à l'aise. Si des réunions en face à face sont possibles, les organisations doivent envisager le lieu où elles se tiendront, en tenant compte des difficultés liées au transport et/ou des difficultés financières auxquelles les personnes peuvent être confrontées si elles sont situées en dehors des grandes villes³⁶. Si une interface téléphonique est proposée, il est important que le service soit disponible 24 heures sur 24 et 7 jours sur 7. Ces mesures sont particulièrement essentielles pour garantir un environnement inclusif, sensible au genre et à la dimension de genre, dans lequel toutes les personnes souhaitant signaler des cas d'actes répréhensibles peuvent se sentir à l'aise de le faire de la manière qui leur convient, indépendamment de leur sexe, de leur genre, de leur rang, de leur grade ou d'autres facteurs ou statuts sociaux ou culturels.

Les interfaces doivent être adaptées aux spécificités, à la culture et à l'environnement de travail de l'organisation, ainsi qu'au contexte social externe. Par exemple, le personnel soignant dans les hôpitaux travaille dans des environnements complexes où il subit une pression importante liée au temps ; il ne dispose pas non plus de beaucoup de temps où il peut s'isoler des autres. Si un hôpital souhaite mettre en place des voies de signalement efficaces, il devrait fournir aux travailleurs de la santé des interfaces de signalement qui peuvent être utilisées dans de telles conditions. Dans ce cas, il faut envisager la possibilité de faire un signalement par le biais d'une application pour smartphone ou par SMS.

Si le processus de signalement est long, compliqué ou doit se faire par téléphone ou en personne, les membres d'une organisation peuvent non seulement se sentir mal à l'aise et s'abstenir de signaler les cas, mais aussi ne pas avoir suffisamment de temps pour le faire.

Lors de crises de santé publique telles que la pandémie de COVID-19, il est également important de tenir compte des restrictions à la libre circulation des personnes. Si une politique ne prévoit pas d'interfaces de signalement à distance, toutes les voies de signalement pourraient être inutiles. Les politiques de signalement, en particulier dans le secteur des soins de santé, devraient prévoir la possibilité de signaler les cas par le biais de courriels, de sites Web, d'applications mobiles et de SMS voire, si aucune ressource à distance n'est disponible, par courrier postal.

Par exemple, l'Occupational Safety and Health Administration (OSHA) du Ministère du travail des États-Unis a créé une page Web dédiée pour permettre de signaler les problèmes de santé et de sécurité pendant la pandémie de COVID-19. Cette page Web propose plusieurs moyens de déposer une plainte : en ligne, par courrier, par télécopie, par courriel, par téléphone ou en personne^a.

^a États-Unis, OSHA, Ministère du travail, « Déposer une plainte », disponible à l'adresse : www.osha.gov/workers/file_complaint.html.

³⁵ ONUDC, *Reporting Mechanisms in Sport: A Practical Guide for Development and Implementation*, 2019.

³⁶ Zúñiga, « Gender sensitivity in corruption reporting and whistleblowing », 2020, disponible à l'adresse : <https://www.u4.no/publications/gender-sensitivity-in-corruption-reporting-and-whistleblowing.pdf>.

3.3 GARANTIR LA CONFIDENTIALITÉ TOUT AU LONG DU PROCESSUS DE SIGNALEMENT

Les organisations disposent d'un large éventail d'options lorsqu'il s'agit d'établir des voies de signalement. Les options décrites ci-dessus peuvent prendre de nombreuses formes en fonction du statut et de la structure de l'organisation, ainsi que de sa position dans la chaîne d'approvisionnement des soins de santé.

Lorsqu'elle décide de la voie de signalement la mieux adaptée à ses besoins, l'organisation doit tenir compte des éléments suivants :

1. Proposer plusieurs options au personnel afin qu'il puisse choisir celle qui lui convient le mieux ;
2. Veiller à ce que les voies de signalement soient établies et gérées d'une « manière sécurisée qui garantit la confidentialité »³⁷ et que les lanceurs d'alerte puissent signaler les actes répréhensibles « en toute confiance et sans crainte de représailles »³⁸.

Outre la mise en place de plusieurs voies et interfaces de signalement, une bonne politique de protection des lanceurs d'alerte doit également être soutenue, promue et pilotée par la direction et/ou l'encadrement, et doit prévoir les méthodes de signalement suivantes :

- *Le signalement ouvert*, lorsque des personnes signalent ou communiquent ouvertement des informations, ou déclarent qu'elles ne cherchent pas à faire en sorte ou n'exigent pas que leur identité soit gardée secrète ;
- *Le signalement confidentiel*, lorsque le nom et l'identité de la personne qui communique l'information sont connus du destinataire, mais ne seront pas divulgués sans le consentement de la personne, sauf si la loi l'exige ;
- *Le signalement anonyme*, qui consiste à recevoir un signalement ou une information sans que personne n'en connaisse la source³⁹.

Il est essentiel de garantir un niveau élevé de confidentialité pour que la politique sur la protection des lanceurs d'alerte soit efficace.

Souvent, le lanceur d'alerte continuera à travailler dans l'organisation après avoir signalé l'acte répréhensible présumé et sera confronté à des situations difficiles, en raison de facteurs tels que le sentiment de loyauté envers les collègues et les superviseurs, les obligations contractuelles de confidentialité et le risque de représailles. Il est donc primordial de garantir la confidentialité, non seulement sur l'identité du lanceur d'alerte, mais aussi sur le signalement lui-même.

Signalement confidentiel

Comme mentionné ci-dessus, dans le cas d'un signalement confidentiel, le nom et l'identité de la personne qui a communiqué l'information sont connus par le destinataire, mais ne seront pas divulgués sans le consentement de la personne, sauf si la loi l'exige.

Si l'organisation choisit de faire appel à un prestataire de services externe pour la réception des signalements d'actes répréhensibles présumés, elle doit s'assurer que ce prestataire peut offrir les garanties de confidentialité nécessaires⁴⁰.

³⁷ Directive du Parlement européen et du Conseil sur la protection des personnes qui signalent des violations du droit de l'Union, art. 9.

³⁸ Coopération économique Asie-Pacifique, « APEC Anti-Corruption Code of Conduct for Business », septembre 2007, art. 4 g, également inclus dans Organisation de coopération et de développement économiques (OCDE), ONUDC et Banque mondiale, *Anti-Corruption Ethics and Compliance Handbook for Business*, 2013.

³⁹ ONUDC, E4J University Modules Series: Anti-corruption, Module 6: Detecting and Investigating Corruption, « Whistle-blowing systems and protection », disponible à l'adresse : <https://www.unodc.org/e4j/en/anti-corruption/module-6/key-issues/whistle-blowing-systems-and-protections.html>.

⁴⁰ ONUDC, *Reporting Mechanisms in Sport*.

En cas de violation de ces obligations de confidentialité, la politique doit également prévoir des sanctions. En outre, des mesures correctives, y compris le licenciement, doivent être prévues afin de prévenir les représailles et/ou la divulgation d'informations protégées. Dans certains cas, les organisations peuvent souhaiter inclure des clauses de responsabilité civile et des motifs de résiliation dans les contrats signés avec les prestataires de services externes et, le cas échéant, peuvent transmettre les affaires à l'organisme gouvernemental compétent.

Il est important de se rappeler que les signalements seront examinés par des enquêteurs ou des unités indépendantes et que, par conséquent, toute information susceptible de compromettre la confidentialité des signalements doit être évitée. Ainsi, les noms des personnes concernées ne doivent apparaître dans aucun document relatif au signalement, et leurs informations personnelles doivent être conservées séparément dans un endroit sûr (physique ou électronique). Un soin particulier doit être apporté à la rédaction des signalements, qui doivent être rédigés de manière à éviter de dévoiler explicitement ou implicitement l'identité du lanceur d'alerte (par exemple, en indiquant l'emplacement de son bureau ou le nombre d'années pendant lesquelles il a travaillé dans l'organisation).

Une politique efficace sur la protection des lanceurs d'alerte garantit donc que l'identité de la personne qui signale les faits restera confidentielle à chaque étape du processus qui suit le signalement de l'acte répréhensible présumé. Les organisations doivent être conscientes que leurs politiques de sécurité et de cybersécurité ont une incidence directe sur la protection des lanceurs d'alerte et de leurs informations. Si la confidentialité est assurée, d'autres mesures peuvent ne pas être nécessaires (bien qu'elles doivent toujours être connues et disponibles).

Pour garantir la confidentialité, il est nécessaire de définir ce que signifie le terme « identité » dans le contexte de la protection des lanceurs d'alerte

Lorsqu'une organisation établit une politique sur la protection des lanceurs d'alerte, elle doit définir clairement le concept d'« identité » associé au principe de confidentialité ou l'adoption de mécanismes permettant aux lanceurs d'alerte de rester anonymes.

Stricto sensu, l'« identité » désigne le nom de la personne qui communique des informations, mais le concept doit également être élargi pour inclure d'autres renseignements qui peuvent conduire à l'identification de cette personne, y compris des détails tels que l'adresse, le numéro de téléphone (ou le numéro de poste du bureau), l'adresse électronique (y compris l'adresse électronique personnelle), ainsi que, dans certains cas, le département, l'unité ou l'organisation dans laquelle la personne travaille et ou le rôle/titre du poste. Si l'unité ou le service est relativement petit, ces renseignements peuvent facilement conduire à l'identification du lanceur d'alerte.

En outre, certaines organisations peuvent garder la trace des sites Web que le personnel visite lorsqu'il utilise son ordinateur de travail, y compris s'il accède au site Web réservé au signalement. Par conséquent, la définition de l'« identité » devrait également couvrir les adresses de protocole Internet (IP) des ordinateurs dans de tels cas.

Les informations fournies doivent également être traitées avec toute la prudence professionnelle requise, y compris pendant la phase d'enquête (ou d'établissement des faits)⁴¹, car parfois le type d'informations peut permettre d'identifier la personne qui les a communiquées. Il arrive qu'une seule personne ait accès aux informations communiquées ; dans ce cas, la manière dont l'information est traitée est d'une importance capitale. Par conséquent, étant donné que certains types d'informations peuvent toujours conduire à l'identification des lanceurs d'alerte même si la confidentialité est garantie, les premiers destinataires des signalements et les enquêteurs devraient préciser aux lanceurs d'alerte si et comment la confidentialité sera garantie d'après leur évaluation.

⁴¹ Voir la deuxième partie, chap. 5, des présentes lignes directrices.

En outre, une bonne politique ne doit pas garantir la confidentialité uniquement sur demande. Les premiers destinataires des signalements doivent donc être formés pour évaluer le niveau de risque que les individus peuvent prendre en signalant les cas d'actes répréhensibles dont ils ont connaissance. Par conséquent, même dans les cas où des personnes signalent ou communiquent ouvertement des informations sans demander que leur identité reste confidentielle, les destinataires de ces signalements devraient être en mesure de décider si l'identité de ces personnes doit être divulguée ou non, en fonction du niveau de risque qui pourrait peser sur le lanceur d'alerte. Ces décisions doivent être prises en consultation avec la personne concernée.

Signalement anonyme

Même si les garanties et les mesures de confiance nécessaires sont en place, certains membres du personnel craindront toujours d'être exposés et de subir des représailles. Dans certains cas, le personnel peut également penser que le mécanisme de signalement mis en place n'est pas là pour le protéger, mais pour tester sa loyauté envers l'organisation. Ainsi, même lorsque tous les efforts ont été déployés pour assurer la confidentialité, il peut être impossible de gagner la confiance de l'ensemble du personnel.

Dans les pays où elles sont légalement tenues de le faire, les organisations doivent permettre au personnel de signaler des problèmes de manière anonyme. Dans d'autres pays, les organisations devraient fortement envisager d'autoriser les signalements anonymes, à moins que ces signalements soient interdits par la loi.

Cette option pourrait encourager ceux qui n'ont pas confiance dans les mécanismes en place à se manifester et à signaler les actes répréhensibles. Toutefois, l'organisation doit également être consciente des inconvénients liés aux signalements anonymes et sensibiliser le personnel à ces risques potentiels, comme indiqué ci-dessous :

- Les informations communiquées sont limitées et ne seront peut-être pas suffisantes pour ouvrir une enquête ;
- Dans certains cas, l'interaction avec la personne qui communique des informations n'est pas possible ;
- Des ressources supplémentaires peuvent être nécessaires pour déterminer si des actes répréhensibles ont été commis ;
- L'organisation pourrait ne pas être en mesure de protéger la personne qui a communiqué des informations, étant donné que l'identité de cette personne a été dissimulée lorsqu'elle a fait un signalement anonyme.

Néanmoins, il existe certaines mesures que les organisations peuvent prendre pour éviter certains de ces écueils. Par exemple, des technologies telles que des plateformes de messagerie chiffrée, des plateformes de signalement en ligne sécurisées, des lignes d'assistance téléphonique anonymes ou des applications mobiles dotées de fonctions de signalement anonyme pourraient être utilisées pour permettre aux lanceurs d'alerte de rester anonymes, tout en proposant une voie de communication.

L'Organisation mondiale de la Santé autorise les particuliers à effectuer des signalements par le biais d'un portail en ligne, y compris de manière anonyme, auquel cas il est précisé qu'aucune tentative ne sera faite à aucun moment pour retrouver les coordonnées de la personne qui communique des informations. Toutefois, même si elles choisissent de rester anonymes, les personnes qui communiquent des informations peuvent se reconnecter au portail à l'aide du numéro de dossier fourni et du mot de passe choisi afin de recevoir un retour d'information et de fournir des informations complémentaires en réponse à toute question publiée sur le portail par les destinataires du signalement^a.

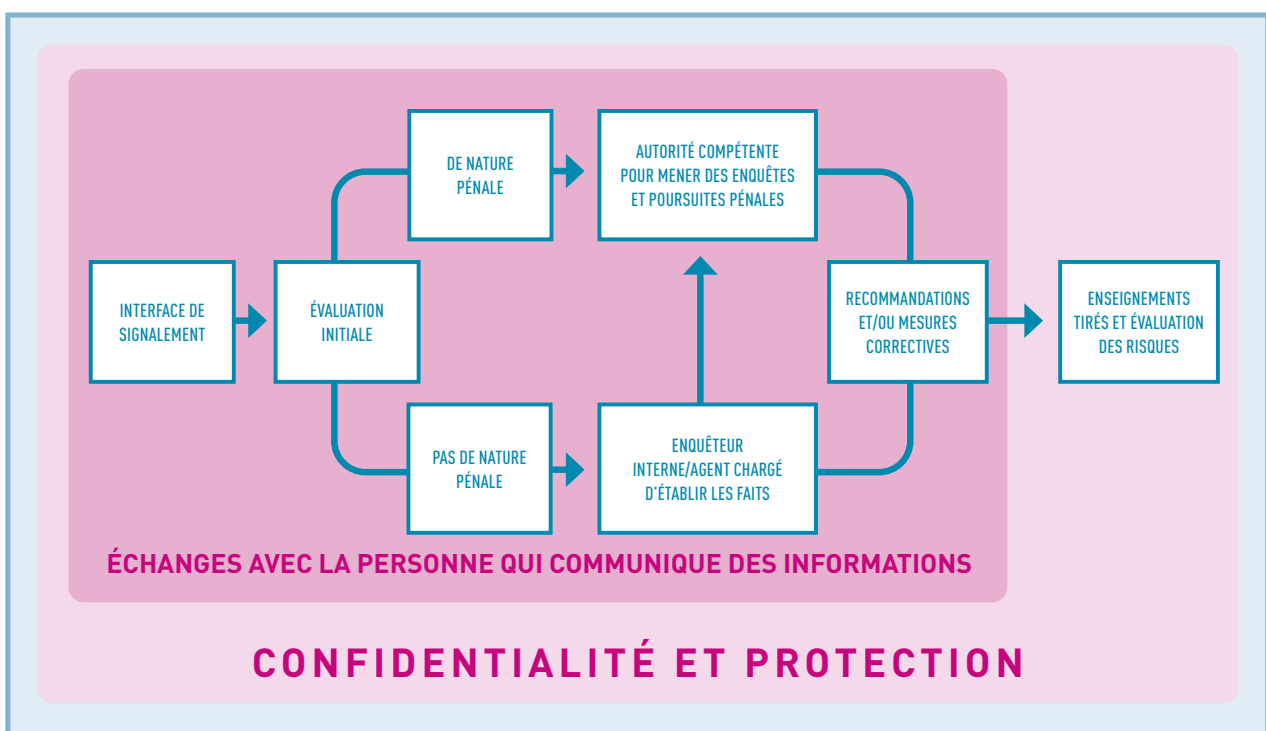
^a Pour plus d'informations, voir le portail en ligne Expolink créé par l'OMS, disponible à l'adresse : <https://wrs.expolink.co.uk/integrity>.

Les organisations peuvent également améliorer la qualité des informations reçues par le biais des signalements anonymes en sensibilisant le personnel aux détails qui sont nécessaires pour mener une enquête. Par exemple, ces renseignements pourraient être donnés aux personnes susceptibles de communiquer des informations sous la forme d'une liste récapitulative ou d'un arbre de décision, et pourraient être mises en avant lors des sessions de formation du personnel et diffusées via intranet et d'autres méthodes de publication. Les organisations peuvent également dresser une liste de questions sur le signalement par le biais de sites Web ou d'applications mobiles afin d'aider les personnes intéressées à trouver suffisamment de détails. Il est également important que les personnes qui traitent les appels aux lignes d'assistance anonymes reçoivent la formation voulue pour s'assurer qu'elles posent les bonnes questions et obtiennent des informations de manière systématique.

DEUXIÈME PARTIE.

TRAITER LES INFORMATIONS
REÇUES ET ASSURER
UNE PROTECTION

L'image ci-dessous illustre les différentes étapes d'un processus de signalement :



Chapitre 4.

TRAITER UN SIGNALEMENT : ÉVALUATION INITIALE

Les signalements faits par le personnel et les autres personnes répondant à la définition de « lanceur d’alerte » énoncée dans la première partie, au chapitre 1, peuvent sauver des vies, mais aussi réduire ou prévenir les pertes financières et de réputation pour l’organisation.

Les lanceurs d’alerte jouent un rôle essentiel pour préserver l’honnêteté, l’efficacité et la responsabilité des entités publiques et privées. Les lanceurs d’alerte étant une source essentielle pour la détection des gaspillages, des fraudes et des abus et la protection de la santé et de la sécurité publiques, il est important de mettre en place un processus sûr et inclusif pour encourager les signalements d’actes répréhensibles.

Pour instaurer la confiance au sein de l’organisation, il est essentiel que l’environnement soit conçu de manière à empêcher les tiers de découvrir qui est le lanceur d’alerte et d’exercer des représailles à son encontre, notamment en veillant à ce que les signalements soient traités en temps voulu⁴².

Il est important de veiller à ce que les informations communiquées fassent l’objet d’un suivi rapide et structuré et que toute mesure ultérieure soit communiquée à la personne qui a fait le signalement.

4.1 ACCUSÉ DE RÉCEPTION

Une fois que le signalement d’un acte répréhensible présumé est reçu par l’une des interfaces établies par l’organisation, la première étape consiste à envoyer un accusé de réception écrit au lanceur d’alerte. Dans la Directive européenne sur les lanceurs d’alerte, par exemple, il est proposé que cet accusé de réception soit envoyé dans les sept jours⁴³. Les réponses automatiques, lorsqu’elles sont envisagées, doivent être soigneusement conçues. Dans certains cas, le message peut également inclure des informations préliminaires sur les prochaines étapes et donner une vue d’ensemble du processus au lanceur d’alerte. Si les réponses automatiques peuvent être un moyen efficace d’accélérer le processus, le lanceur d’alerte peut considérer que le message standardisé ne constitue pas une vraie réponse. Les lanceurs d’alerte ont souvent besoin d’être sûrs de quelqu’un s’occupe du dossier et que les informations ont été reçues correctement.

⁴² Pour des travaux de recherche sur les effets du traitement en temps voulu des signalements dans le secteur des soins de santé, voir Paul Rauwolf et Aled Jones, « Exploring the utility of internal whistleblowing in healthcare via agent-based models », *BMJ Open*, vol. 9, n° 1 (janvier 2019).

⁴³ Directive du Parlement européen et du Conseil sur la protection des personnes qui signalent des violations du droit de l’Union, art. 9.

Les accusés de réception peuvent prendre diverses formes, mais voici un exemple de réponse qui pourrait être envoyée lorsqu'un signalement est fait :

Je vous écris pour vous informer que j'ai bien reçu votre signalement concernant [insérer le texte du signalement].

Merci de m'avoir fait part de vos préoccupations. Je m'efforcerai de vous répondre sous dix jours.

Je pourrais avoir besoin de vous parler à l'avenir. En attendant, si vous avez quelque chose à ajouter ou si vous avez d'autres questions, n'hésitez pas à me contacter^a.

^a ONUDC, *Reporting Mechanisms in Sport*.

4.2 ÉVALUATION DU SIGNALEMENT

Une fois qu'une préoccupation a été reçue, elle doit être enregistrée de manière systématique. Les premiers destinataires des signalements et les enquêteurs doivent connaître et utiliser une terminologie cohérente dans l'ensemble de l'organisation, et il est préférable que tous les cas soient enregistrés dans un système sécurisé de gestion des affaires. Le problème doit être évalué pour déterminer : s'il correspond à la ou aux définitions d'un acte répréhensible à signaler ; quelle entité est la mieux placée pour traiter ou enquêter sur les allégations et mener l'enquête (s'il existe plusieurs entités), en fonction du type d'acte répréhensible (principalement dans le secteur public) ; et le degré d'urgence. Une fois que l'information a été considérée comme devant être signalée en vertu de la politique de protection des lanceurs d'alerte⁴⁴, il convient de répondre à quatre questions :

- Qui communiquera avec la personne qui a communiqué des informations ?
- Si la protection des lanceurs d'alerte est accordée, quelles sont les mesures nécessaires pour préserver la confidentialité et assurer la protection ?
- Quelle entité se chargera d'examiner les cas potentiels d'actes répréhensibles, si plusieurs entités ont ce pouvoir ?
- Dans quelle catégorie le signalement sera-t-il classé ?

Il est donc important que la personne qui reçoit en premier lieu les allégations soit très bien formée sur la manière de réagir et sur les questions qui peuvent ou doivent être posées au lanceur d'alerte⁴⁵.

Dans le secteur privé en particulier, les premiers destinataires des signalements doivent également être formés au domaine de compétence de l'organisation, à ses activités principales et à ses aspects techniques et, dans une certaine mesure, être familiarisés avec les termes techniques et le jargon, surtout si les premiers destinataires des signalements font partie du personnel d'un prestataire de services externe. Dans le cas des entreprises multinationales, les premiers destinataires des signalements doivent également être sensibilisés aux différentes pratiques de travail et normes culturelles des pays où l'organisation opère. En effet, si un lanceur d'alerte peut essayer d'utiliser des termes génériques, l'explication de l'acte répréhensible et des circonstances connexes peut nécessiter l'utilisation d'une terminologie technique ou la description de situations spécifiques qui pourraient être difficiles à comprendre pour une personne extérieure à l'organisation. C'est notamment le cas pour le secteur des soins de santé, où les informations techniques peuvent être très spécifiques. Les premiers destinataires des signalements doivent également établir une relation de confiance avec la personne qui communique des informations. Cette dernière doit se sentir à l'aise et en confiance, notamment lors des réunions en face à face ou des appels téléphoniques. À cet égard, les premiers destinataires des signalements doivent être en mesure d'expliquer en détail comment les informations communiquées vont être traitées et quelles protections sont accordées au lanceur d'alerte.

⁴⁴ Voir la première partie, chap. 2, des présentes lignes directrices.

⁴⁵ Voir la troisième partie des présentes lignes directrices.

Au cours de l'évaluation des allégations, les premiers destinataires des signalements doivent se poser certaines questions pour évaluer les informations reçues et déterminer comment procéder.

Par exemple, l'Office of Inspector General des États-Unis d'Amérique a créé un tableau pour informer les lanceurs d'alerte potentiels des types de violations qui peuvent être signalées, des personnes qui peuvent le faire et des institutions qui sont les destinataires autorisés⁴⁶. À cet égard, dès la réception des allégations, les premiers destinataires des signalements doivent déterminer la catégorie de lanceur d'alerte, le type d'information communiquée et si les institutions qui ont reçu le signalement sont autorisées à traiter les allégations, afin de décider de la suite à donner.

Par exemple, les employés civils du département de la santé et des services sociaux peuvent signaler les violations suivantes (exclusivement) :

- Violation de toute loi, règle ou règlement ;
- Mauvaise gestion flagrante ;
- Gaspillage de fonds flagrant ;
- Abus d'autorité ;
- Danger substantiel et spécifique pour la santé ou la sécurité publique ;
- Censure liée à la recherche ou à l'analyse scientifique (intégrité scientifique).

⁴⁶ Disponible à l'adresse : www.oig.hhs.gov/fraud/report-fraud/whistleblower.asp.

Le tableau suivant contient une liste de questions et de mesures que les destinataires des signalements doivent prendre en considération⁴⁶ :

QUESTIONS POUR L'ÉVALUATION INITIALE	MESURES POSSIBLES
<p>Quel est le degré d'urgence du signalement ?</p> <ul style="list-style-type: none"> • L'acte répréhensible présumé est-il un événement ponctuel, récurrent ou anticipé ? • Existe-t-il un préjudice pour les individus ? • Existe-t-il un danger potentiel pour une grande partie de la population (par exemple, la production de médicaments falsifiés) ? 	<p>Tous les signalements doivent être traités en temps voulu. Toutefois, certains signalements doivent être traités en priorité (par exemple, en cas de danger immédiat pour des personnes sous traitement médical).</p> <p>Dans le secteur des soins de santé, il est important d'évaluer dans quelle mesure les allégations pourraient nuire à la santé et au bien-être des personnes et dans quelle mesure ces risques sont concrets et imminents.</p>
<p>Le signalement contient-il suffisamment d'informations pour répondre aux autres questions de ce tableau ?</p>	<p>Dans le cas contraire, contacter le lanceur d'alerte et lui demander plus d'informations. Toutefois, on ne peut pas demander au lanceur d'alerte de mener un travail d'enquête.</p> <p>Il convient de toujours manifester la plus grande empathie lorsqu'on communique avec les lanceurs d'alerte. Par mesure de précaution, ces communications doivent être réalisées par une personne professionnellement formée à cette tâche spécifique.</p>

(suite page 30)

⁴⁶ Le tableau est basé sur le tableau contenu dans ONUDC, *Reporting Mechanisms in Sport*, et a été adapté aux fins de la présente publication.

QUESTIONS POUR L'ÉVALUATION INITIALE	MESURES POSSIBLES
<p>L'acte répréhensible signalé relève-t-il de la compétence de l'organisation ?</p> <ul style="list-style-type: none"> • L'acte répréhensible est-il couvert par le règlement de l'organisation ? • L'organisation a-t-elle une compétence sur l'entité ou l'individu visés dans le signalement ? 	<p>Si l'information communiquée relève du domaine pénal, vous êtes tenu d'alerter les autorités compétentes et de leur confier l'affaire. Si une évaluation supplémentaire est nécessaire à ces fins, le signalement doit être transmis à l'agent chargé d'établir les faits.</p> <p>S'il ne s'agit pas d'une violation d'une loi, d'une règle ou d'une politique, mais d'un mécontentement, et qu'il ne sera pas classé dans une autre procédure ou ne fera pas l'objet d'une enquête, il convient d'en informer le lanceur d'alerte, de préférence dans une conversation expliquant pourquoi aucune autre mesure ne peut être prise. Les motifs de la décision doivent être communiqués par écrit. À ce stade, le lanceur d'alerte peut avoir d'autres informations. Dans tous les cas, le signalement doit être enregistré dans le système.</p> <p>En fonction de la raison de l'insatisfaction exprimée par la personne qui a communiqué des informations, il peut exister d'autres procédures mieux adaptées dans l'organisation, telles qu'une procédure de doléance ou de recours auprès de la direction.</p>
<p>Des signalements similaires ont-ils été faits précédemment ?</p>	<p>Il se peut qu'un signalement ne contienne pas suffisamment d'informations à lui seul, mais lorsqu'il est examiné en parallèle avec les informations contenues dans d'autres signalements, un dossier plus viable peut apparaître. C'est pourquoi il est important d'enregistrer chaque signalement. Pour traiter avec soin les allégations reçues, vous devez les examiner et les suivre.</p>
<p>Quels sont les risques liés à la préservation de la confidentialité ?</p> <ul style="list-style-type: none"> • Le lanceur d'alerte est-il le seul à avoir accès à l'information en question ? • Le lanceur d'alerte travaille-t-il dans une petite équipe ? 	<p>Il se peut que le lanceur d'alerte ait déjà parlé de ses préoccupations à quelqu'un ou qu'il se trouve dans une position où il est facile pour les autres de deviner qui a fait le signalement.</p> <p>Les antécédents professionnels d'un lanceur d'alerte et sa relation de travail avec la ou les personnes accusées peuvent être utiles pour bien comprendre la situation et les risques potentiels.</p> <p>Les enquêteurs doivent être informés de ces risques.</p>
<p>Y a-t-il déjà eu des représailles contre le lanceur d'alerte ?</p>	<p>Dans ce cas, le signalement peut être influencé par l'anxiété et la frustration liées aux représailles. Il est nécessaire de communiquer avec le lanceur d'alerte pour distinguer les faits liés à l'acte répréhensible des faits liés aux représailles.</p>

Pour répondre à certaines des questions énumérées ci-dessus, il peut être utile que les premiers destinataires des signalements (et, par la suite, les enquêteurs ou les agents chargés d'établir les faits) disposent de certains documents et informations supplémentaires. Les lanceurs d'alerte doivent être encouragés à donner le plus d'informations possible mais, dans certaines circonstances, notamment en cas de signalement anonyme, les informations fournies sont limitées et incomplètes. La collecte d'informations supplémentaires peut parfois être essentielle pour évaluer l'acte répréhensible présumé et mener une enquête.

Voici des exemples des types de documents et d'informations qui peuvent être importants, dans certains cas, pour qu'un signalement soit évalué et déclenche une enquête^a :

- Documentation concernant des signalements supplémentaires, tels qu'un signalement concernant la sécurité ou la santé ou tout autre signalement protégé par la loi, soumis à tout autre organisme d'exécution ;
- Des copies de tous les documents pertinents obtenus légalement, tels que les courriels, les relevés téléphoniques, les textos, les journaux d'activité, les notes de réunion, les ordres de travail, les lettres ou les mémorandums, liés au signalement ;

- Des copies de toute lettre d'embauche et/ou de licenciement ;
- Une copie du manuel du personnel de l'employeur et/ou de la convention collective ;
- Des copies de toute(s) mesure(s) disciplinaire(s) prise(s) à l'encontre du lanceur d'alerte au cours de son emploi ;
- Une description du travail actuel du lanceur d'alerte ;
- Des copies des cinq derniers bulletins de salaire du lanceur d'alerte (si des représailles ont déjà eu lieu et que le salaire a été affecté).

^a On trouvera une liste analogue d'informations utiles lors du dépôt d'une plainte à l'adresse : www.whistleblowers.gov/complaint_page.

En plus des documents énumérés ci-dessus, il peut être important de dresser une liste contenant les noms et coordonnées de personnes qui peuvent vérifier les allégations. À cet égard, les lanceurs d'alerte doivent être encouragés à recenser les personnes suivantes :

- Les témoins potentiels qui peuvent confirmer les allégations, en incluant un bref résumé de ce que chaque témoin pourrait savoir ;
- Les responsables de la gestion qui ont pris la décision ayant conduit à l'acte répréhensible présumé ;
- Les personnes qui ont traité les documents relatifs à la décision en question (personnel administratif, de bureau ou des ressources humaines).

L'organisation peut être en possession de la plupart des documents et des coordonnées concernant ces personnes. Il est donc important de donner aux destinataires des signalements (ainsi qu'aux enquêteurs ou aux agents chargés d'établir les faits) accès à ces informations, afin que l'évaluation des allégations et l'enquête ultérieure puissent être menées efficacement. En outre, il convient d'utiliser des systèmes informatisés de gestion des documents permettant de maintenir et de préserver la sécurité des renseignements relatifs aux personnes, aux signalements et aux preuves. Ces documents doivent être conservés de la manière voulue s'ils sont susceptibles d'être utiles à des enquêtes pénales.



Chapitre 5.

MENER DES ENQUÊTES ET DES EXAMENS : ÉTABLIR LES FAITS

5.1 CONDUITE D'UNE ENQUÊTE

Lorsqu'une organisation met en place une politique sur la protection des lanceurs d'alerte, c'est non seulement pour instaurer une culture de la confiance, mais aussi pour promouvoir la responsabilité, la transparence et l'intégrité. Elle peut également souhaiter adopter une approche préventive et être informée des cas d'actes répréhensibles sur les plans juridique, administratif et disciplinaire qui sont commis en son sein, mener immédiatement une enquête interne et veiller à ce que les mesures correctives soient prises au sérieux et mises en œuvre rapidement.

À cet égard, il est donc essentiel de disposer d'une politique établissant la manière de traiter les enquêtes administratives internes. Le terme « enquête » étant souvent associé à une procédure pénale, il est possible de privilégier un autre terme, tel que « examen administratif », « examen de la gestion » ou « établissement des faits » dans la politique.

Un bureau ou une personne devraient être chargés de rassembler les informations pertinentes pour évaluer si les allégations répondent aux critères voulus. Certaines organisations ont créé une section dédiée. Les personnes en question doivent être dûment formées pour mener de telles enquêtes, jouir d'une grande confiance (si possible, être certifiées en tant qu'examineurs) et être suffisamment indépendantes pour établir les faits dans le cadre de chaque enquête ou examen, y compris lorsque les cadres supérieurs ou de haut niveau de l'organisation sont visés. Idéalement, les personnes exerçant ce rôle devraient se situer en dehors de la chaîne hiérarchique, de manière à réduire le risque d'ingérence dans le processus.

Dans certains cas, notamment dans le secteur public, des unités sont créées pour recevoir les signalements et mener des enquêtes. Dans certains cas, les enquêtes sont également externalisées. Dans ce cas, une attention particulière doit être accordée à la garantie et au maintien de la confidentialité des informations.

Par exemple, le bureau des enquêtes de l'Office of Inspector General des États-Unis est chargé de recevoir et d'examiner les allégations et, si cela se justifie, de les transmettre pour enquête. Parfois, les allégations ne constituent pas un signalement ou ne nécessitent pas d'enquête et sont donc transmises à la direction sous la forme d'une demande de réponse aux allégations^a.

^a Pour plus d'informations, voir le site Web de l'Office of Inspector General of the United States Department of State, à l'adresse : www.stateoig.gov/hotline/whistleblower.

Dans d'autres cas, notamment dans le secteur privé, l'unité destinataire peut être un prestataire de services externe, tandis que l'enquêteur se trouve au sein de l'entreprise, généralement dans le département de conformité, lorsqu'un tel département existe.

Dans certaines organisations, l'agent chargé d'établir les faits travaille au sein du service de conformité de l'organisation, tandis que les voies de signalement sont gérées par un prestataire externe. Dans ce cas, le prestataire externe transmettra les informations à l'agent chargé d'établir les faits après l'évaluation initiale. Lorsqu'on considère que l'information communiquée ne justifie pas l'ouverture d'une enquête, il est même possible que les premiers destinataires des signalements ne fournissent pas le nom du lanceur d'alerte à l'enquêteur. Ainsi, personne au sein de l'organisation n'a accès à l'identité du lanceur d'alerte^a.

^a L'organisation peut également confier l'enquête à un prestataire externe.

Les enquêteurs peuvent mener les activités suivantes :

- *Rassembler les preuves de l'acte répréhensible présumé.* Il est important que l'enquêteur ait un accès illimité à tous les documents et dossiers de l'organisation. La confidentialité des documents ne saurait constituer un obstacle à l'enquête et, par conséquent, la politique doit prévoir que l'enquêteur ait immédiatement accès à tous les documents, informations, témoins et personnes faisant l'objet d'une enquête (sujets). En outre, des sanctions peuvent être imposées aux individus qui refusent de donner accès à des preuves potentielles⁴⁷.
- *Demander, si nécessaire, des informations complémentaires à la personne qui a communiqué des informations.* L'enquêteur doit obtenir suffisamment d'informations pour mener une enquête efficace⁴⁸.
- *Mener des entretiens et recevoir des témoignages verbaux et des déclarations écrites.* L'enquêteur doit être formé pour comprendre la complexité des affaires et poser les bonnes questions. De nombreux enquêteurs sont tenus de faire prêter serment au témoin ou au sujet et d'enregistrer l'entretien.
- *Examiner la ou les allégations faites* et déterminer si elles font intervenir une fraude, un acte de corruption ou toute autre conduite illicite ou criminelle potentielle justifiant la saisine des autorités nationales, y compris les services d'enquête et de poursuite, le cas échéant. Certaines enquêtes exigent de démêler des mécanismes complexes et des plans élaborés conçus pour éviter la détection. Dans ces cas, les enquêteurs doivent être suffisamment formés pour les détecter et obtenir les preuves nécessaires pour prouver qu'une infraction a pu être commise.
- *Formuler des suggestions sur les mesures disciplinaires et correctives recommandées.* Une fois l'enquête terminée, l'enquêteur devra formuler une recommandation sur les mesures à prendre pour remédier aux actes répréhensibles qui ont fait l'objet d'une enquête et qui ont été corroborés.

⁴⁷ Voir la deuxième partie, chap. 5, sect. 2, des présentes lignes directrices.

⁴⁸ Voir, par exemple, la Directive du Parlement européen et du Conseil sur la protection des personnes qui signalent des violations du droit de l'Union, art. 9, par. 1 c.

5.2 CHOIX DE LA PERSONNE « IDÉALE » POUR MENER DES ENQUÊTES OU DES EXAMENS

L'indépendance et l'impartialité des enquêteurs sont essentielles, surtout lorsque l'enquête n'a pas été externalisée. Pour éviter toute ingérence, la personne chargée des enquêtes internes ne doit pas se voir confier d'autres rôles ou fonctions. Lorsqu'elle ne mène pas d'enquêtes, cette personne pourrait participer au développement continu du programme relatif aux lanceurs d'alerte, à la formation et à la sensibilisation. Lorsqu'il n'est pas possible d'affecter une personne à un poste à temps plein, celle-ci doit disposer de suffisamment de temps, en dehors de son rôle et de ses responsabilités de base, pour mener des enquêtes approfondies en temps voulu. L'enquêteur ne doit pas être mis dans une position qui favoriserait des enquêtes précipitées ou incomplètes. Il est nécessaire que l'organisation établisse un poste spécifique d'enquêteur ou d'agent chargé d'établir les faits et l'inscrive dans sa politique. Il devrait également être exigé que la personne retenue pour le poste soit familiarisée avec les activités principales de l'organisation et obtienne une qualification professionnelle reconnue concernant la conduite d'enquêtes pénales et/ou administratives, telle qu'une certification en tant qu'examineur de fraude, dans les deux ans suivant son entrée en fonction, si cette personne ne possède pas déjà une telle qualification⁴⁹.

Il est possible pour l'organisation de mener un processus de recrutement interne. Dans ce cas, elle devrait financer la certification.

Toutefois, l'organisation peut considérer qu'il est préférable d'engager une personne de l'extérieur. En effet, il est possible que son personnel ne soit pas qualifié, qu'il soit soumis à des conflits d'intérêts ou qu'il ne jouisse pas de l'indépendance voulu. L'enquêteur entreprendra des missions d'enquête concernant d'autres membres du personnel de l'organisation. Si les personnes sont recrutées en interne, elles peuvent ne pas être perçues comme indépendantes.

Il peut donc être préférable de recruter un candidat externe, afin de réduire le risque que les enquêtes ne soient pas menées de manière totalement neutre. En outre, en recrutant un candidat externe, l'organisation peut exiger les qualifications voulues comme condition préalable à l'embauche.

Quoi qu'il en soit, les enquêteurs ou les agents chargés d'établir les faits doivent garantir leur indépendance et ne doivent être influencés d'aucune manière. Ils devraient être obligés de déclarer tout conflit d'intérêts éventuel qui serait susceptible d'entacher leur impartialité. Lorsqu'un enquêteur ou un agent chargé d'établir les faits déclare un conflit d'intérêts, il est conseillé à l'organisation de désigner une autre personne dûment qualifiée pour traiter l'affaire.

En ce qui concerne le secteur des soins de santé, il pourrait être très souhaitable de faire intervenir des professionnels tels que des médecins pour aider à l'enquête ou à l'examen en tant qu'experts du programme. Comme ils n'auront pas besoin d'être formés aux termes et procédures spécifiques qu'ils pourraient rencontrer au cours de l'enquête, ils peuvent jouer un rôle de spécialistes pour aider à déterminer si un acte répréhensible a été commis. Les médecins ou autres praticiens de la santé, en particulier ceux qui ont déjà travaillé dans le secteur, peuvent être au courant de certaines pratiques de corruption et, dans certains cas, pourraient être utiles à l'entité ou à la personne chargée de mener l'enquête. Chaque fois que des experts sont associés à une enquête, il est recommandé qu'ils signent une déclaration d'indépendance ou de conflit d'intérêts comprenant des dispositions expresses de confidentialité.

⁴⁹ Par exemple, dans certaines entreprises privées, les candidats sélectionnés pour occuper le poste d'enquêteur au sein du département de conformité doivent être certifiés par l'Association of Certified Fraud Examiners (www.acfe.com).



Chapitre 6.

TRAITER L'ACTE RÉPRÉHENSIBLE ET CLORE L'AFFAIRE

Pour mettre en place une politique efficace sur la protection des lanceurs d'alerte, il ne suffit pas de recevoir des signalements d'actes répréhensibles présumés. Des mesures doivent être prises pour mettre fin à l'acte répréhensible, en atténuer les conséquences et sanctionner les personnes qui l'ont commis.

Il convient de noter que, dans certains cas, le processus mentionné dans la deuxième partie, chapitre 5, peut conduire à la conclusion que les allégations ne peuvent être étayées. La politique doit donc établir des mécanismes pour garantir que :

- La personne (le sujet) visée par les allégations ne subit aucune conséquence négative. Le principe de confidentialité est également fondamental à cette fin ;
- Si des dommages à la réputation ou à la carrière ont été causés, des mesures sont établies pour les réparer ou les limiter ;
- Le lanceur d'alerte ne fait pas l'objet de représailles ou de mesures disciplinaires, à condition que la personne ait fait un signalement de bonne foi et/ou pour des motifs raisonnables⁵⁰.

Dans certains cas, avant de prendre une décision finale (y compris une décision de ne pas donner suite), la personne chargée d'évaluer l'acte répréhensible présumé (premier destinataire du rapport ou enquêteur) peut également être invitée à consulter un supérieur ou un autre collègue. Dans de telles situations, une attention particulière doit être portée à la consultation de la personne, afin de ne pas compromettre l'indépendance et l'impartialité de la décision finale.

Par exemple, la politique sur les dénonciations faites dans l'intérêt public (lanceurs d'alerte) de l'Australian Health Practitioner Regulation Agency prévoit que lorsqu'un signalement est traité par une personne chargée du traitement de ces questions, celle-ci consulte le Responsable en chef des dénonciations faites dans l'intérêt public avant de prendre une décision finale sur le signalement (y compris la décision de ne pas donner suite)^a.

^a www.ahpra.gov.au/about-ahpra/complaints/whistleblower-policy.aspx.

⁵⁰ Voir la première partie, chap. 2, sect. 3, des présentes lignes directrices.

6.1 TRAITEMENT DE L'ACTE RÉPRÉHENSIBLE

Si l'enquête montre que l'allégation d'acte répréhensible est vraie, ou qu'il est très probable qu'elle le soit, les enquêteurs doivent établir la nature de l'acte répréhensible dans leur rapport.

Dans les cas où les actes répréhensibles ne sont pas de nature pénale, la politique doit prévoir un mécanisme de prise et de suivi des mesures correctives. Le rapport transmis par l'unité d'enquête au service de l'organisation chargé des mesures disciplinaires doit comprendre l'identification du type d'acte répréhensible et des recommandations en termes *a)* de renforcement des contrôles internes et *b)* de mesures disciplinaires. Dans certaines organisations, les procédures disciplinaires sont traitées par une organisation externe ou un organe de contrôle (tel que le conseil du personnel).

Il est très important de préserver la confidentialité de l'identité du lanceur d'alerte à chaque étape du processus, même si le sujet de l'enquête fait l'objet d'une procédure disciplinaire. Si une audience disciplinaire est finalement organisée et que le lanceur d'alerte est cité comme témoin, son identité doit figurer dans la liste de toutes les personnes qui ont fait des déclarations verbales pendant la phase d'enquête, sans distinction.

Le lanceur d'alerte peut encore subir des représailles de la part de ses collègues ou de ses supérieurs, même lorsque l'affaire est close et que la sanction a été infligée. Dans ce cas, une certaine forme de protection et/ou de compensation pourrait s'imposer si les représailles sont prouvées.

Dans les cas où l'acte répréhensible pourrait également constituer une infraction pénale – ce qui serait le cas s'il s'agissait d'un acte de corruption, par exemple – l'unité d'enquête doit transmettre l'affaire au procureur ou au service d'enquête et de poursuite compétent (si elle n'a pas elle-même la compétence ou l'autorité pour enquêter). La politique doit prévoir que, dans le cas où une enquête met au jour une infraction pénale, en particulier une infraction susceptible d'être liée à la criminalité organisée (comme un réseau de corruption au sein de l'organisation), l'enquêteur doit suspendre son enquête et transmettre le dossier aux autorités compétentes.

Il est donc essentiel que la politique contienne les instructions suivantes :

- Lorsque l'affaire est de nature pénale, ou susceptible de faire intervenir une infraction pénale, le dossier doit être transmis sans délai aux autorités compétentes ;
- L'enquêteur, ainsi que la direction de l'organisation, doivent rester à la disposition des autorités pour des enquêtes complémentaires (il est important que l'organisation coopère avec les autorités) ;
- Dans la mesure du possible, les enquêteurs ne doivent pas initialement communiquer l'identité du lanceur d'alerte aux autorités compétentes. Toutefois, dans certains cas, il pourrait être essentiel pour les services d'enquête et de poursuite de connaître le nom de la personne qui a signalé l'affaire, notamment par le biais d'ordonnances judiciaires. Néanmoins, certaines précautions doivent être prises, par exemple :
 - Le lanceur d'alerte doit être informé et donner son consentement exprès. La politique pourrait contenir un formulaire de renonciation à cette fin ;
 - L'identité du lanceur d'alerte doit être communiquée de manière confidentielle et la politique doit prévoir un mécanisme à cet effet.

Il est important de noter qu'à ce stade, si le pays où se trouve l'organisation ne dispose pas d'une législation sur la protection des lanceurs d'alerte, le fait de transmettre l'affaire à l'extérieur de l'organisation augmente le risque que l'identité du lanceur d'alerte soit divulguée, et que la personne puisse subir des représailles. Il est donc fortement recommandé que la politique établisse des mécanismes permettant d'éviter de devoir communiquer le nom du lanceur d'alerte (dans la mesure du possible). Une autre possibilité consiste à conclure un accord avec les services d'enquête et de poursuite pour autoriser, par exemple, l'enquêteur (ou une autre personne en contact avec le lanceur d'alerte) à jouer le rôle d'intermédiaire si des informations supplémentaires doivent être recueillies.

6.2 CLÔTURE DE L'AFFAIRE

D'autres aspects doivent être pris en compte lors de la clôture de l'affaire.

Tout d'abord, un rapport final comprenant toutes les violations légales ou administratives pertinentes, les faits et les preuves permettant de prouver ou de réfuter les allégations et les témoins doit être rédigé. Un processus de divulgation doit être appliqué, et le dossier doit être sécurisé après la clôture de l'affaire. Il est important de toujours se rappeler que le lanceur d'alerte peut faire l'objet de représailles même après la fin de la procédure. Cela vaut également dans les cas où il a été conclu qu'aucun acte répréhensible n'a été commis et qu'aucune mesure corrective n'a été prise.

À cet égard, il est important de disposer d'indications claires sur les étapes à suivre, par exemple :

- S'assurer que, à tous les stades de l'affaire, tous les processus ont été menés à bien conformément aux procédures prévues et documentées et dans le respect des exigences légales ;
- S'assurer que toutes les décisions et actions ont été consignées dans le dossier de l'affaire ;
- Vérifier les exigences nationales par rapport aux lois pertinentes sur la protection des données dans le pays d'opération. Les lois sur la protection des données peuvent exiger que les données personnelles figurant dans le dossier soient supprimées ou modifiées à ce stade. Cela est particulièrement important dans le secteur des soins de santé, car les dossiers peuvent contenir des informations médicales sur les patients et le personnel ;
- Assurer la stricte confidentialité des renseignements relatifs à l'enquête. Une attention particulière doit être accordée aux mesures techniques et institutionnelles nécessaires pour atténuer ces risques et garantir la sécurité des données ;
- Consigner la date de clôture et le nom de la personne qui a pris la décision de clôturer le dossier ;
- Enregistrer le dossier conformément aux politiques existantes en matière de protection des données et aux pratiques internes de gestion des dossiers (le cas échéant) ;
- Informer le lanceur d'alerte de la clôture de l'affaire⁵¹.

Deuxièmement, l'enquêteur pourrait également subir des représailles. Les enquêteurs internes restent, dans la plupart des cas, des employés de l'organisation, et il se peut qu'ils aient été en contact avec la personne dénoncée lorsqu'ils se sont renseignés sur l'affaire. Ils peuvent subir des pressions pour révéler l'identité de la personne qui fait le signalement, abandonner une enquête ou émettre des conclusions favorables à l'auteur présumé de l'acte répréhensible. À ce titre, les enquêteurs pourraient être en danger (selon la structure hiérarchique) s'ils résistent à l'ingérence de la direction ou de leurs collègues. Il est également possible qu'ils deviennent eux-mêmes des personnes qui communiquent des informations. Une bonne politique doit garantir l'indépendance et la sécurité dont les enquêteurs ont besoin pour mener à bien leur travail. Ils doivent toujours être protégés contre le licenciement, la rétrogradation ou la discrimination liés à leur participation au processus d'enquête.

⁵¹ Voir, par exemple, la Directive du Parlement européen et du Conseil sur la protection des personnes qui signalent des violations du droit de l'Union, art. 11, par. 2 e.



Chapitre 7.

ASSURER LA PROTECTION DES LANCEURS D'ALERTE

Les lanceurs d'alerte peuvent se mettre en situation de risque personnel et professionnel important⁵². En signalant des cas d'éventuels actes répréhensibles commis par leurs collègues, leurs pairs ou leurs supérieurs, ils s'exposent au risque de représailles dans leur environnement de travail, qui peuvent prendre des formes telles que la perte d'emploi, le harcèlement, la restriction des conditions et de l'accès au lieu de travail ou la réduction des responsabilités⁵³. L'absence de mesures de protection contre ces formes de représailles pourrait diminuer l'impact de voies de signalement solides. En d'autres termes, le personnel ne se manifesterait pas s'il n'est pas sûr que des mesures de protection seront mises en place pour limiter le plus possible le risque qu'il prend⁵⁴.

La protection contre les représailles dans le secteur des soins de santé est cruciale. Le secteur représente une part importante des dépenses du produit intérieur brut (PIB). L'Organisation de coopération et de développement économiques (OCDE) a indiqué qu'« en 2019, avant le début de la pandémie de coronavirus, la part moyenne des dépenses de santé dans le PIB de l'ensemble de l'OCDE était d'environ 8,8 %. Ce chiffre est resté largement stable depuis 2009, la croissance des dépenses de santé étant restée en phase avec la croissance économique globale depuis la dernière crise économique [2008] »⁵⁵. Ainsi, les organisations liées aux soins de santé sont puissantes, et les individus pourraient réfléchir à deux fois avant de signaler des actes répréhensibles.

En outre, il est important de noter qu'une solide politique sur la protection des lanceurs d'alerte ne profite pas exclusivement aux lanceurs d'alerte. Les organisations en tireront également un grand profit. Lorsqu'elles sont en place, des politiques efficaces encouragent les signalements d'actes répréhensibles susceptibles d'éviter des préjudices aux patients, des pertes financières importantes ou des sanctions judiciaires ou administratives coûteuses, sans parler de l'atteinte à la réputation de l'organisation. Par exemple, la détection précoce de la fraude au sein d'une organisation et la coopération avec les services d'enquête et de poursuite pourraient permettre d'éviter des poursuites pénales contre l'organisation lorsque cette fraude est signalée. Elle peut également réduire les dommages financiers causés par l'activité illicite. Après

⁵² ONUDC, *Guide de ressources sur les bonnes pratiques en matière de protection des personnes qui communiquent des informations*.

⁵³ ONUDC, *Un programme de déontologie et de conformité contre la corruption pour les entreprises*.

⁵⁴ Pour des travaux de recherche sur ce sujet, voir Aled Jones, Annette Lankshear et Daniel Kelley, « Giving voice to quality and safety matters at board level: a qualitative study of the experiences of executive nurses working in England and Wales », *International Journal of Nursing Studies*, vol. 59 (2016).

⁵⁵ Base de données en ligne, Statistiques de l'OCDE sur la santé 2020, disponible à l'adresse : <https://www.oecd.org/fr/els/systemes-sante/base-donnees-sante.htm>.

tout, tout acte répréhensible, quel qu'il soit, commis au sein d'une organisation ou à l'encontre de son personnel, aura des effets néfastes sur celle-ci. Un système solide de protection des lanceurs d'alerte contribuera à améliorer le bien-être et à retenir le personnel, ce qui permettra d'améliorer la prestation de services aux patients et au public. Le régime de protection doit également s'appliquer aux témoins de l'acte répréhensible, aux collègues du lanceur d'alerte (y compris ceux qui peuvent être identifiés à tort comme étant le lanceur d'alerte) et aux facilitateurs (y compris les premiers destinataires des signalements, les enquêteurs, les responsables et autres personnes chargées de traiter les signalements).

Il est donc important que l'organisation, lorsqu'elle établit sa politique relative aux lanceurs d'alerte, prévoie une protection contre tout traitement injustifié. À cet égard, la politique doit contenir :

- Une définition de ce qui est considéré comme un traitement injustifié dans l'organisation ;
- Des mesures pour prévenir les représailles ou y mettre fin ;
- Des mesures visant à sanctionner les représailles lorsqu'elles se produisent.

7.1 PROTECTION CONTRE LES TRAITEMENTS INJUSTIFIÉS

Lorsque l'organisation établit une politique sur la protection des lanceurs d'alerte, il est important qu'elle détermine les types de traitement injustifié dont le lanceur d'alerte doit être protégé.

À cet égard, dans la politique des Nations Unies sur la protection contre les représailles des personnes qui signalent des manquements et qui collaborent à des audits ou à des enquêtes dûment autorisés, le terme « représailles » est défini comme « toute mesure directement ou indirectement préjudiciable ayant une incidence négative sur l'emploi ou les conditions de travail d'une personne, lorsque cette mesure a été recommandée, prise ou menacée d'être prise dans le but de punir, d'intimider ou de léser une personne » qui a signalé un comportement répréhensible, comme indiqué dans la politique⁵⁶.

L'organisation doit donc définir les représailles et fournir une liste non exhaustive de scénarios de représailles dans le cadre de la politique de protection des lanceurs d'alerte. Les formes potentielles de traitement injuste ou de représailles peuvent inclure :

- Suspension, mise à pied, licenciement ou résiliation de contrat ;
- Coercition, intimidation, brimades ou harcèlement, y compris le harcèlement sexuel ;
- Rétrogradation ou perte d'une possibilité de promotion ;
- Transfert de fonctions ou changement de lieu de travail ;
- Réduction des salaires ou des heures de travail ;
- Imposition ou administration de toute mesure disciplinaire, réprimande ou autre sanction, y compris de nature financière ;
- Traitement discriminatoire, désavantageux ou injuste, y compris fondé sur le sexe ;
- Menace de violence, de dommages à la propriété ou toute autre action qui entraînerait des blessures ou constituerait une autre infraction ;
- Violence, dommages à la propriété ou toute autre action qui entraînerait des blessures ou constituerait une autre infraction ;
- Contre-allégations non fondées ou fausses ;
- Inscription sur une liste noire (un accord sectoriel ou industriel, formel ou informel, qui empêche une personne de trouver un autre emploi) ;
- Fourniture d'informations inexacts ou fausses dans une référence d'emploi pour empêcher une personne d'obtenir un emploi futur, ou le refus de fournir une référence lorsqu'on le lui demande ;
- Poursuites civiles ou pénales pour violation du secret, calomnie ou diffamation ;
- Tout autre traitement injuste ou représailles (menace ou réalité) non couvert par la présente liste.

⁵⁶ ST/SGB/2017/2/Rev.1, sect. 1.4.

Par exemple, la politique de l’OMS sur le signalement des actes répréhensibles et la protection contre les représailles définit les représailles comme « toute décision et/ou mesure administrative préjudiciable, directe ou indirecte, qui est brandie comme menace, préconisée ou prise à l’encontre d’un membre du personnel qui a signalé un cas d’irrégularité présumée entraînant un risque significatif pour l’OMS ; ou a collaboré à une vérification ou à une enquête dûment autorisée sur un cas d’irrégularité présumée ». La politique dresse une liste d’actions qui pourraient constituer des représailles contre les lanceurs d’alerte :

- Harcèlement ;
- Discrimination ;
- Évaluations négatives du travail du membre du personnel sans fondement ;
- Changements contractuels non justifiés : fin de contrat, rétrogradation, mutation ou transfert ;
- Modification non justifiée des attributions ;
- Refus non justifié des congés et autres types d’absence ;
- Retards abusifs dans l’autorisation des voyages ou l’octroi des prestations dont le membre du personnel bénéficie ;
- Menace à l’encontre de la personne qui signale un acte répréhensible, sa famille et/ou ses biens, y compris les menaces pouvant être extérieures à l’OMS^a.

^a OMS, « Signalement des actes répréhensibles et protection contre les représailles ».

La politique doit donc protéger les lanceurs d’alerte contre toute forme de représailles liées aux cas d’actes répréhensibles qu’ils signalent. La protection devrait également être accordée même lorsque les enquêtes établissent ultérieurement qu’aucun acte répréhensible n’a été commis, pour autant que la personne ait eu des motifs raisonnables de croire que l’information était vraie au moment du signalement.

Il convient de noter que les mesures prises à l’encontre des lanceurs d’alerte doivent être évaluées en tenant compte de la réalité du contexte et de la situation. Une action qui pourrait sembler normale vue de l’extérieur peut en effet être perçue comme un traitement injustifié, en fonction de divers facteurs tels que le sexe, la classe, la race et d’autres identités et/ou vulnérabilités de la personne dans son contexte social. Il est donc essentiel de ne pas dresser une liste exhaustive et de permettre une évaluation des situations au cas par cas⁵⁷.

Il est également important de noter que les politiques les plus efficaces en matière de protection des lanceurs d’alerte ne limitent pas la protection accordée au lanceur d’alerte *stricto sensu* (c’est-à-dire la première personne qui signale l’acte répréhensible), mais l’étendent à toutes les personnes qui coopèrent au processus, telles que les facilitateurs, les témoins, les collègues (y compris ceux qui ont été identifiés à tort comme étant les lanceurs d’alerte) et les membres de la famille qui travaillent dans l’organisation.

7.2 MÉCANISMES DE PROTECTION PERMETTANT DE PRÉVENIR LES REPRÉSAILLES OU D’Y METTRE FIN

Lorsqu’un pays adopte une loi sur la protection des lanceurs d’alerte, des mécanismes de protection sont également créés. La loi peut prévoir le principe de la confidentialité et de la non-divulgence du nom et de l’identité du lanceur d’alerte. Pour traiter les cas où l’identité du lanceur d’alerte est divulguée pour quelque raison que ce soit, et où des représailles sont exercées en conséquence, la loi peut également établir des mécanismes permettant soit de réparer les dommages causés (comme la possibilité pour le lanceur d’alerte de porter l’affaire devant le tribunal du travail ou de bénéficier d’un renversement de la charge de la preuve), soit de mettre fin aux représailles et de réintégrer la personne dans ses fonctions ou dans d’autres fonctions équivalentes.

⁵⁷ ONUDC, *The Time is Now: Addressing the Gender Dimensions of Corruption* (Vienne, 2020).

Lorsqu'une telle loi existe, l'organisation qui souhaite établir une politique spécifique doit être consciente des mécanismes juridiques existants et s'assurer que sa politique est conforme à ceux-ci.

Par exemple, la République de Corée a mis en place la Commission de lutte contre la corruption et des droits civils, qui a le pouvoir de proposer des mesures de secours provisoires aux lanceurs d'alerte, comme demander aux organisations de réintégrer les salariés dans leurs fonctions^a. Toute politique institutionnelle doit se conformer à l'autorité de la Commission lors de l'établissement de leurs mécanismes internes visant à empêcher le licenciement des lanceurs d'alerte.

^a République de Corée, Loi sur la prévention de la corruption et la création et la gestion de la Commission de lutte contre la corruption et des droits civils, art. 62-3.

Toutefois, lorsqu'il n'existe pas de loi ou que la loi n'offre pas une protection suffisante, l'organisation, lors de l'établissement de la politique, dispose toujours d'une certaine souplesse pour proposer un certain niveau de protection aux membres qui décident de signaler des actes répréhensibles en passant par les voies internes.

Assurer la confidentialité

Comme mentionné au chapitre 6 de la deuxième partie, il est essentiel que la politique prévoit des voies de signalement internes qui garantissent une confidentialité absolue et offrent la possibilité de signaler les cas de manière anonyme. La peur d'être découvert en tant que lanceur d'alerte peut aller au-delà de la crainte de perdre son emploi. Comme le montre l'exemple ci-dessous, les gens peuvent craindre pour leur vie et le bien-être de leur famille.

Dans une étude sur les lanceurs d'alerte dans le secteur des soins infirmiers, une infirmière interrogée sur ses premières impressions lorsqu'elle a décidé de donner l'alerte a déclaré : « Il y a probablement eu un mois ou deux où j'étais très inquiète pour mon bien-être ou celui de mes enfants. Je me suis dit que même s'il n'avait pas le courage de s'en prendre à moi, il s'en prendrait peut-être à mes enfants. [...] J'ai été un peu inquiète pendant un moment^a. »

^a Debra Jackson *et al.*, « Understanding whistleblowing: qualitative insights from nurse whistleblowers », *Journal of Advanced Nursing*, vol. 66, n° 10 (octobre 2010), p. 2198.

Prendre l'affaire au sérieux et la traiter rapidement

Il est essentiel de prendre l'affaire au sérieux et d'enquêter, non seulement pour détecter et traiter les actes répréhensibles, mais aussi pour assurer la protection du lanceur d'alerte et prévenir les actes potentiels de représailles. En fait, plus une affaire est traitée rapidement, moins il y a de risque que le lanceur d'alerte soit identifié ou, s'il est découvert, qu'il fasse l'objet de représailles, car il deviendrait évident que les représailles sont une conséquence du signalement.

En outre, si les lanceurs d'alerte ont l'impression que le signalement ne donne lieu à aucune mesure, ils peuvent être découragés d'en faire à l'avenir, perdre confiance dans l'organisation elle-même et envisager de faire un signalement à l'extérieur de l'organisation (par exemple, aux médias). Il s'agit d'une considération importante dans les affaires liées au secteur des soins de santé, car les lanceurs d'alerte qui se tournent vers les médias ou d'autres voies externes pourraient violer les droits de tiers en divulguant des informations ou des dossiers médicaux.

En outre, certains des actes répréhensibles commis représentent un réel danger pour la santé publique et la vie des personnes. Les lanceurs d'alerte peuvent donc ressentir le besoin de faire un signalement public étant donné l'urgence de la situation. En protégeant les lanceurs d'alerte, l'organisation se protège également contre des pertes économiques et de réputation potentiellement graves. La politique doit souligner l'importance de signaler les actes répréhensibles. Le signalement de violations et d'actes répréhensibles

peut être une question sensible pour des raisons culturelles, juridiques et politiques (par exemple, les lanceurs d'alerte peuvent être perçus comme des traîtres ou des informateurs)⁵⁸. Pour assurer la protection de ces personnes, il faut changer cette perception négative et encourager le signalement.

Réaffecter ou réintégrer le lanceur d'alerte si nécessaire

La réaffectation ou la réintégration du lanceur d'alerte est un mécanisme efficace qui pourrait être mis en place pour prévenir et atténuer les conséquences des représailles. Dans tous les cas, la personne concernée doit être consultée avant une éventuelle réaffectation ou réintégration, afin que celle-ci ne soit pas perçue comme un traitement préjudiciable.

La politique devra prévoir la possibilité de réaffecter le lanceur d'alerte à un nouveau poste, si celui-ci continue à travailler dans l'entreprise après avoir dénoncé les faits. La réaffectation ne doit pas réduire le rang ou le salaire du lanceur d'alerte.

Par exemple, si l'organisation est de grande taille, la politique pourrait proposer au lanceur d'alerte d'être déplacé de manière permanente ou temporaire vers un autre département ou une autre branche, afin d'éviter les représailles venant de son équipe d'origine ou d'y mettre fin.

Pour les cas où la réaffectation n'est pas possible, la politique peut également prévoir d'autres mesures d'allègement, telles que le placement en congé spécial à plein traitement ou toute autre mesure appropriée, y compris des mesures de sécurité, au cas par cas⁵⁹. Lorsque la réaffectation n'est pas possible, il convient de le préciser au lanceur d'alerte au plus tôt, afin de gérer ses attentes.

La possibilité de réintégrer le lanceur d'alerte dans son emploi, si la personne a été licenciée avant que toute mesure de protection ait pu être mise en place, doit également être envisagée dans la politique. Même lorsqu'il n'existe pas de norme nationale pour réintégrer le lanceur d'alerte ou réparer le préjudice causé par les représailles, l'organisation peut prévoir des mécanismes internes à cet égard, en fonction de sa taille.

Ces décisions doivent être prises après qu'une enquête appropriée sur les représailles présumées a été menée. Une personne ou une unité devrait être chargée de ces questions. Cette personne sera généralement issue du département des ressources humaines. L'organisation peut également envisager de proposer les services d'un médiateur pour rétablir les relations de travail entre les collègues et la personne accusée d'un acte répréhensible, dans des circonstances appropriées.

7.3 SANCTIONNER LES REPRÉSAILLES

Malheureusement, les mesures mises en place pour prévenir les représailles ne sont pas toujours suffisantes pour protéger efficacement le lanceur d'alerte. La politique doit donc prévoir d'autres mécanismes pour sanctionner les actes de représailles qui peuvent survenir dans l'organisation à la suite d'un signalement.

Mécanismes permettant de signaler les représailles et d'enquêter à leur sujet

La politique doit permettre aux personnes de signaler un traitement injustifié survenu à la suite d'une dénonciation. Par conséquent, l'organisation doit préciser dans la politique que toutes les voies établies pour le signalement d'actes répréhensibles doivent également être en mesure de recevoir des plaintes

⁵⁸ ONUDC, *Un programme de déontologie et de conformité contre la corruption pour les entreprises*.

⁵⁹ Voir, par exemple, OMS, « Signalement des actes répréhensibles et protection contre les représailles ». Dans la section 8.3 de la circulaire ST/SGB/2017/2/Rev.1, il est prévu que le Bureau de l'éthique peut recommander au Secrétaire général de « prendre toutes mesures utiles pour sauvegarder les intérêts du requérant, notamment : le sursis temporaire à l'exécution de la mesure regardée comme constituant des représailles ; avec le consentement de l'intéressé, la réaffectation provisoire ou le changement de rattachement hiérarchique ; pour les fonctionnaires, le placement en congé spécial à plein traitement ».

concernant les représailles ou le traitement injustifié que les lanceurs d'alerte peuvent subir après avoir fait un signalement.

Il faut garder à l'esprit que, en cas de représailles, les lanceurs d'alerte et les autres membres du personnel peuvent perdre confiance dans le système de signalement. C'est particulièrement vrai lorsque les représailles résultent de la divulgation de leur identité au cours du processus de signalement. Dans ces cas, les organisations gouvernementales peuvent également recevoir les allégations de représailles⁶⁰.

L'allégation de représailles (ou de traitement injustifié) doit faire l'objet d'une enquête selon les mêmes mécanismes que ceux prévus dans la politique d'enquête sur les actes répréhensibles. Il est toutefois recommandé que la personne chargée d'enquêter sur l'acte répréhensible présumé ne soit pas également chargée d'enquêter sur les représailles présumées. Bien que liés, ces deux processus doivent rester distincts et être traités indépendamment l'un de l'autre.

Par exemple, certaines entreprises de fournitures médicales prévoient différentes voies pour signaler les cas de représailles. Il peut s'agir, entre autres, du responsable de la conformité, du bureau d'éthique et du département des ressources humaines. En outre, comme indiqué dans les présentes lignes directrices, plusieurs voies devraient être mises en place pour le signalement des actes répréhensibles. Par conséquent, il est également possible pour le lanceur d'alerte d'utiliser une voie différente de celle par laquelle il a signalé l'acte répréhensible pour dénoncer des représailles présumées.

Comme mentionné ci-dessus, les représailles peuvent être définies comme une décision et/ou une action administrative défavorable, directe ou indirecte, qui est menacée, recommandée ou prise à l'encontre d'un individu⁶¹. À cet égard, elle peut prendre de nombreuses formes et dépend également du contexte social, culturel, juridique et politique de l'organisation ou du pays où elle est située, ainsi que de la situation socioéconomique particulière, du sexe et des vulnérabilités de la personne concernée. Par conséquent, une décision ou une action (telle qu'une promotion ou un transfert) qui peut être vécue ou considérée comme normale dans un pays, dans une organisation ou pour une personne, peut être perçue ou vécue comme un traitement injustifié dans un autre contexte. Il est donc nécessaire de relier l'acte de représailles présumé à un signalement existant et de le placer dans son contexte afin de déterminer s'il doit être considéré comme un traitement injustifié.

Ainsi, les représailles font intervenir une succession de trois éléments :

- Une dénonciation concernant un acte répréhensible suspecté ou présumé à signaler ;
- Une décision administrative défavorable directe ou indirecte et/ou une action ou une omission préjudiciable ;
- Une relation de cause à effet entre le signalement et la décision défavorable et/ou l'action ou l'omission préjudiciable.

Afin d'étayer une telle allégation, une enquête doit trouver des preuves de ces trois éléments.

Idéalement, la politique devrait prévoir le renversement de la charge de la preuve, au profit du lanceur d'alerte. En d'autres termes, si les deux premiers éléments susmentionnés sont établis par les enquêteurs, la relation de causalité sera présumée, à moins que la personne (ou l'administration) soupçonnée de représailles puisse démontrer par des preuves claires et convaincantes que l'acte qui est susceptible de constituer des représailles ne serait produit même si le lanceur d'alerte n'avait pas signalé une suspicion d'acte répréhensible⁶².

⁶⁰ Par exemple, l'Equal Employment Opportunity Commission des États-Unis est chargée de faire appliquer les lois fédérales contre la discrimination à l'égard des personnes qui ont signalé une situation de discrimination.

⁶¹ Voir, par exemple, ST/SGB/2017/2/Rev.1, sect. 1.4, et OMS, « Signalement des actes répréhensibles et protection contre les représailles ».

⁶² Voir, par exemple, ST/SGB/2017/2/Rev.1, sect. 7.1, et OMS, « Signalement des actes répréhensibles et protection contre les représailles ».

Mécanismes de sanction contre les représailles

Bien que les sanctions soient plus courantes dans les instruments juridiques que dans les politiques, les organisations pourraient bénéficier de l'effet dissuasif qu'elles pourraient avoir sur leur personnel. Pour ce faire, tous les membres du personnel devront être conscients des sanctions auxquelles ils sont potentiellement exposés, et ces sanctions devront être conformes aux codes et politiques disciplinaires existants.

Lorsque des représailles ont été exercées et qu'elles peuvent être liées au signalement d'actes répréhensibles, certaines sanctions peuvent être imposées à la personne qui exerce les représailles. Bien que certaines actions de représailles puissent être considérées comme une violation du code de déontologie de l'entreprise et que l'auteur puisse être sanctionné pour ces motifs, il est important de réglementer spécifiquement les conséquences des représailles faisant suite à un signalement. Cela permet à l'entreprise d'établir des sanctions proportionnées et d'éviter des définitions très larges qui pourraient entraîner le rejet de l'affaire.

Par exemple, les codes déontologiques peuvent obliger le personnel à se comporter de manière éthique sans préciser les comportements qui pourraient enfreindre cette disposition^a. Bien que les représailles puissent être considérées comme une violation de cette obligation, il appartient à l'organe chargé des procédures disciplinaires de prendre cette décision.

^a Par exemple, dans l'article 37, paragraphe 2 du Code de déontologie médicale du Conseil général des associations médicales officielles d'Espagne, il est indiqué que « les médecins doivent se traiter mutuellement avec la déférence, le respect et la loyauté qui leur sont dus, quelle que soit la relation hiérarchique entre eux ».

Les représailles sous toutes leurs formes doivent être prises en compte lors de la rédaction d'une liste de sanctions. Il est important de rappeler que les comportements de nature pénale doivent également être signalés aux autorités nationales compétentes en vue d'une enquête et, éventuellement, de poursuites. Néanmoins, même lorsque l'acte répréhensible est de nature criminelle, l'organisation peut imposer des sanctions disciplinaires au fautif. À cet égard, les politiques peuvent prévoir l'imposition des sanctions suivantes, en fonction de la gravité de l'acte répréhensible :

- Avertissement ou blâme écrit qui sera inscrit au dossier du membre du personnel ;
- Suspension sans traitement ;
- Réduction de salaire ou report, pour une période déterminée, de la possibilité de prétendre à une augmentation de salaire ;
- Rétrogradation ou report, pour une période déterminée, de la possibilité de prétendre à une promotion ;
- Réaffectation ;
- Licenciement (avec ou sans indemnité).

Les procédures disciplinaires n'étant pas exclusives des politiques de protection des lanceurs d'alerte, l'organe chargé de ces questions pourrait s'occuper des sanctions pour représailles. Dans la plupart des organisations, un département spécifique et indépendant des ressources humaines devrait être chargé d'analyser et de décider des sanctions.

7.4 FOURNIR UN SOUTIEN ET UN RETOUR D'INFORMATION AU LANCEUR D'ALERTE

Il est suggéré que la politique de protection des lanceurs d'alerte contienne également une procédure visant à fournir *a)* des conseils et un soutien aux personnes qui souhaitent signaler un acte répréhensible présumé et *b)* un suivi, sur une base régulière, avec le lanceur d'alerte sur l'évolution de l'affaire.

Orientation et soutien

Faire un signalement peut être très stressant, surtout pour le salarié d'une organisation qui souhaite dénoncer des actes répréhensibles commis par des collègues, des pairs ou des supérieurs. Plus une personne en sait sur la procédure, moins elle hésitera à signaler des cas d'actes répréhensibles et plus elle se sentira en confiance lorsqu'elle le fera.

Le premier destinataire du signalement doit être en mesure de fournir des conseils et un soutien au lanceur d'alerte. En tant que spécialistes du processus, les premiers destinataires peuvent également contribuer à faire en sorte que le personnel qui a connaissance de cas d'actes répréhensibles leur fasse suffisamment confiance pour les signaler. Étant donné que la déclaration peut parfois être compliquée, en raison de la quantité et du type d'informations nécessaires, des processus à suivre ou de la crainte d'être exposé, par exemple, ces experts devraient recevoir une formation sur la fourniture d'informations afin de dissiper les doutes des personnes qui sont susceptibles de communiquer des informations⁶³. Les lanceurs d'alerte devraient également avoir accès à une source indépendante de conseils, distincte des premiers destinataires des signalements. Il peut s'agir d'un service interne ou externe à l'organisation.

En outre, une personne ou un bureau spécifique, en dehors du mécanisme de signalement officiel, peut être désigné ou mis en place pour fournir des informations. Par exemple, un membre du personnel peut vouloir obtenir des informations sur les options disponibles avant de prendre la décision de faire un rapport. Des agents de conformité, un médiateur, un superviseur de confiance, des représentants syndicaux ou des représentants des employés peuvent jouer ce rôle. Les départements des ressources humaines sont aussi traditionnellement désignés pour aider le personnel, notamment en fournissant des conseils et un soutien à cet égard. Dans tous les cas, il est essentiel que les personnes désignées soient formées pour fournir des conseils et un soutien aux lanceurs d'alerte potentiels en ce qui concerne le partage des informations, et pour traiter ces affaires. Toute nouvelle disposition devrait être alignée sur les dispositions et politiques existantes visant à assurer le bien-être et le soutien du personnel.

Une attention particulière doit être accordée à l'importance de la confidentialité et de l'anonymat dans le processus de signalement. Les ressources informatiques et technologiques, telles que les webinaires, peuvent être utilisées pour réduire au minimum l'exposition et la stigmatisation potentielle des personnes qui assistent aux événements connexes. La politique devrait idéalement mettre en place un système permettant à toute personne qui envisage de faire un signalement d'obtenir un soutien et des conseils confidentiels.

Le soutien et les conseils peuvent être fournis sur une base non personnelle. Des sites Web et des brochures peuvent fournir les informations nécessaires⁶⁴. L'utilisation de courriels informatifs pourrait également être une option. Le General Medical Council du Royaume-Uni dispose d'une page Web dédiée expliquant le type d'informations qui peuvent lui être signalées et comment communiquer d'autres informations. En outre, elle fournit un guide intitulé « Raising and acting on concerns about

⁶³ Voir la troisième partie des présentes lignes directrices.

⁶⁴ Par exemple, l'OMS a élaboré une version simplifiée de sa politique relative au signalement des actes répréhensibles et à la protection contre les représailles, sous la forme d'une courte brochure qui fournit des informations clés sur les personnes qui peuvent faire un signalement, ce qui peut être dénoncé, comment faire un signalement et quelle protection peut être accordée aux personnes qui communiquent des informations. La brochure est disponible (en anglais) à l'adresse : www.who.int/about/ethics/whistleblowing-and-protection-against-retaliation.

patient safety » qui non seulement explique les étapes à suivre pour faire part d'une préoccupation, mais aussi donne les contacts utiles⁶⁵.

Dans les cas où l'impact du signalement oblige une personne à s'absenter du lieu de travail, les organisations doivent envisager toutes les options à leur disposition pour s'assurer que les lanceurs d'alerte se sentent capables de reprendre le travail (s'ils le souhaitent), par exemple en permettant au personnel de prendre des congés ou de travailler à distance. Si possible, ils devraient également donner accès à une ligne d'assistance ou de conseil financée par l'employeur.

Retour d'information

Une fois le signalement effectué, le lanceur d'alerte peut encore faire face à l'incertitude, à la peur des représailles ou même à la crainte que rien ne soit fait en réponse à son signalement⁶⁶. Il est essentiel qu'un suivi soit assuré pour rassurer le lanceur d'alerte sur le fait que les informations communiquées ont été prises au sérieux. Comme mentionné ci-dessus, la première étape de ce suivi doit être l'accusé de réception du signalement, s'il a été fait à distance, par exemple par courriel, par le biais d'une application mobile ou par Internet⁶⁷.

Fournir trop d'informations sur l'affaire au lanceur d'alerte pourrait compromettre l'enquête ou la procédure disciplinaire. Par conséquent, la politique doit préciser que le lanceur d'alerte sera tenu informé de l'évolution générale de l'affaire, sans préjudice des aspects confidentiels des enquêtes qui peuvent être menées. Dans la mesure du possible, des délais estimés doivent être donnés. La personne en charge de ce processus doit toujours agir de manière appropriée et conformément à la formation qui a dû être dispensée.

Si l'évaluation initiale ou l'enquête permet de conclure qu'il n'y a pas lieu de prendre d'autres mesures, le lanceur d'alerte doit être informé rapidement de cette décision. Il est conseillé de remercier la personne de s'être manifestée, même s'il n'est pas donné suite à ses préoccupations. Cela contribue à soutenir une culture ouverte du signalement.

La politique doit contenir un calendrier pour fournir un soutien et un retour d'information au lanceur d'alerte. Par exemple, la directive de l'Union européenne prévoit un délai ne dépassant pas trois mois⁶⁸. Le lanceur d'alerte doit également être informé de ce qu'il aura et n'aura pas le droit de savoir pendant la procédure et lorsque l'affaire sera close, afin de gérer les attentes. Cela est nécessaire pour instaurer une culture de confiance dans l'organisation. Si la personne ne se sent pas écoutée ou prise au sérieux, ou si elle estime que le rapport n'a donné lieu à aucune action, elle peut porter l'affaire en dehors de l'organisation et la rendre publique. Un tel manque de confiance dans le système pourrait également se propager, créant un environnement qui décourage le signalement des actes répréhensibles.

⁶⁵ Voir General Medical Council of the United Kingdom, « What concerns should you raise with us? » et « Raising and acting on concerns about patient safety », disponibles à l'adresse : www.gmc-uk.org.


⁶⁶ ONUDC, *Reporting Mechanisms in Sport*.

⁶⁷ Voir la deuxième partie, chap. 4, des présentes lignes directrices.

⁶⁸ Voir la Directive du Parlement européen et du Conseil sur la protection des personnes qui signalent des violations du droit de l'Union, art. 9, par. 1 f.

TROISIÈME PARTIE.

FORMATION ET SENSIBILISATION

A vibrant green and blue lizard is perched on the edge of a large, textured purple flower petal. The lizard's head is in the upper right, with its body extending towards the center. The petal has a fine, ribbed texture and a rich purple hue. The background is a soft, out-of-focus purple and pink.

Une fois qu'une organisation a rédigé sa politique sur la protection des lanceurs d'alerte et l'a rendue opérationnelle, il est essentiel qu'elle investisse dans la formation⁶⁹ et la sensibilisation de son personnel et des membres de l'entité spécialisée chargée de recevoir et d'examiner les signalements.

⁶⁹ Sur l'importance de la formation, voir ONUDC, *Guide de ressources sur les bonnes pratiques en matière de protection des personnes qui communiquent des informations*, p. 87 et 88.

Chapitre 8.

FORMATION DES PREMIERS DESTINATAIRES DES SIGNALEMENTS, DES ENQUÊTEURS ET DU PERSONNEL

Comme indiqué plus haut, la mise en place d'une politique et d'une procédure de protection des lanceurs d'alerte exige de l'organisation qu'elle engage du personnel (ou qu'elle identifie le personnel existant) ayant les connaissances, les compétences et la capacité d'évaluer les allégations et de mener des enquêtes. En outre, toute personne intervenant dans le processus doit recevoir une formation appropriée afin de garantir que les signalements sont traités correctement, avec soin et conformément à la législation nationale.

8.1 FORMATION DES PREMIERS DESTINATAIRES DES SIGNALEMENTS

Il est important que les premiers destinataires des signalements soient formés au traitement des signalements et sachent qu'ils sont tenus d'accorder une protection aux lanceurs d'alerte⁷⁰. La confidentialité étant essentielle à la protection des lanceurs d'alerte, lorsqu'une personne dénonce un acte présumé répréhensible sur les plans juridique ou administratif, les premiers destinataires des signalements doivent traiter les informations communiquées avec soin. Dans certaines sociétés, les informations communiquées varient en fonction de l'apparence de la personne à qui l'acte répréhensible est signalé ; les normes culturelles et sociétales doivent également être prises en considération⁷¹. Les premiers destinataires des signalements doivent être formés et sensibilisés pour recevoir et traiter des rapports qui peuvent être délicats ou pénibles et pour comprendre les besoins et les vulnérabilités des femmes lanceuses d'alerte ou des lanceurs d'alerte issus de groupes minoritaires⁷². Le rôle des premiers destinataires des signalements suppose également un certain nombre d'actions de proximité pour établir la confiance et ainsi encourager tous les membres de l'organisation à faire un signalement. Dans le secteur des soins de santé, il est important qu'ils connaissent la terminologie et les procédures utilisées dans leurs organisations.

Compte tenu des produits, des services et des sommes d'argent en jeu dans le secteur des soins de santé, il n'est pas rare que les rapports constituent des preuves de crimes de corruption ou contre le bien-être public. Dans la mesure du possible, les premiers destinataires des signalements doivent avoir une certaine

⁷⁰ Sur l'importance de la formation de la personne chargée de recevoir les signalements et d'y donner suite, voir la Directive du Parlement européen et du Conseil sur la protection des personnes qui signalent des violations du droit de l'Union, art. 12.

⁷¹ Nicolas Hamelin, Mehdi el Boukhari et Sonny Nwankwo, « Micro-credit, gender and corruption: are women the future of development? », dans *Women and Social Change in North Africa: What Counts as Revolutionary?*, Doris H. Gray and Nadia Sonneveld, dir. publ. (Cambridge, Royaume-Uni, Cambridge University Press, 2018).

⁷² Zúñiga, « Gender sensitivity in corruption reporting and whistleblowing ».

forme de formation juridique. Au minimum, ils devraient être formés à identifier les cas où l'acte signalé pourrait constituer une infraction pénale. Ils gagneraient donc à être formés sur les infractions les plus courantes commises dans le secteur, telles que la fraude pharmaceutique ou la corruption dans le secteur des soins de santé, et les infractions courantes commises sur le lieu de travail, telles que le détournement de fonds. Lorsqu'une infraction potentielle est identifiée, ils doivent, avec l'approbation du superviseur, informer les services d'enquête et de poursuite compétents.

En outre, les premiers destinataires des signalements sont chargés d'informer les lanceurs d'alerte de la procédure de signalement, des garanties procédurales (à savoir, la confidentialité, l'interdiction des représailles et le droit d'être informé de l'état d'avancement du rapport, entre autres) et des mesures de protection.

Ils doivent également être formés à prendre en compte les réalités contextuelles et sociales des personnes concernées et faire preuve de sensibilité et de réactivité dans leur travail. Ils doivent prendre en compte des facteurs individuels, tels que l'appartenance de la personne concernée à un groupe social marginalisé ou vulnérable et l'intersectionnalité des différents aspects de l'identité de la personne, tels que la race, la classe sociale et le sexe. En conséquence, les premiers destinataires des signalements devraient recevoir une formation spécialisée sur les questions de genre et de diversité.

8.2 FORMATION DES ENQUÊTEURS

Une formation doit également être dispensée aux enquêteurs ou aux agents chargés d'établir les faits. Une partie de la formation dispensée aux premiers destinataires des signalements, comme la manière de traiter les signalements ou la terminologie et les procédures utilisées dans l'organisation, pourrait également être utile aux enquêteurs. Toutefois, la formation des enquêteurs doit être axée sur l'amélioration de leurs compétences en matière d'enquête⁷³. Dans ce contexte, et pour faciliter le développement professionnel des agents chargés d'établir les faits, l'organisation devrait investir dans des cours de formation formels et dans la certification pour mener des enquêtes internes, y compris financières. Des analyses historiques des cas dans le secteur et dans l'organisation pourraient les aider à comprendre où chercher les vulnérabilités, les signaux d'alarme, les lacunes potentielles et les sources de chaque cas d'acte répréhensible. L'organisation doit conserver les documents officiels sous forme d'archives sécurisées afin de faciliter le processus d'apprentissage.

Les enquêteurs doivent être formés aux procédures et aux sanctions prévues par la politique sur la protection des lanceurs d'alerte de l'organisation, car ils sont chargés de rédiger, à la fin de l'enquête, les recommandations énonçant les sanctions à imposer, le cas échéant, pour l'acte répréhensible ou les représailles présumés.

Enfin, à l'instar des premiers destinataires des signalements, les enquêteurs doivent faire preuve d'une grande sensibilité et réactivité dans leurs fonctions. Par conséquent, ils devraient recevoir une formation sur le genre et la diversité afin de leur permettre de prendre en compte la situation individuelle de chaque lanceur d'alerte dans leurs enquêtes sur les actes répréhensibles ou représailles présumés.

8.3 FORMATION DE TOUT LE PERSONNEL

L'organisation doit s'efforcer de fournir une formation appropriée et adéquate à l'ensemble du personnel concernant les politiques relatives à la protection des lanceurs d'alerte, les mécanismes, les recours et le soutien disponibles⁷⁴. Cette formation devrait être intégrée aux programmes d'accueil des nouvelles recrues. En outre, une formation doit être dispensée aux services concernés, tels que les ressources

⁷³ Exemple de programme de formation des enquêteurs : programme obligatoire destiné au personnel chargé d'enquêter sur les dénonciations du Département du travail des États-Unis, voir Occupational Safety and Health Administration (OSHA), « Mandatory training program for OSHA whistleblower investigators », directive n° TED-01-00-020, 8 octobre 2015.

⁷⁴ Voir ONUDC, *Un programme de déontologie et de conformité contre la corruption pour les entreprises*, p. 78 à 82, et Royaume-Uni, Department for Business Innovation and Skills, « Whistleblowing: guidance for employers and code of practice » (Londres, 2015), p. 5.

humaines, la conformité et le contrôle et le bureau du médiateur, sur la manière de traiter les allégations et de guider et soutenir les personnes qui ont signalé ou envisagent de signaler des actes répréhensibles. L'organisation doit également s'assurer que la direction, les cadres supérieurs et les superviseurs sont formés pour fournir des conseils appropriés au personnel, y compris sur la manière de traiter ou d'examiner les allégations et les signalements. Il est également recommandé que l'organisation envisage d'utiliser des outils électroniques et en ligne, tels que des plateformes électroniques et des ressources d'apprentissage en ligne, pour mener à bien cette formation. La formation doit être dispensée à intervalles réguliers afin de garantir un apprentissage continu et les supports de formation doivent être fréquemment mis à jour pour s'assurer qu'ils restent pertinents et reflètent les lois et les meilleures pratiques applicables. L'organisation doit s'efforcer d'évaluer les résultats de l'apprentissage afin de mesurer l'efficacité de la formation.

En résumé, l'organisation doit fournir les catégories de formation suivantes :

- Formation des premiers destinataires des signalements à la manière de réagir, les questions à poser, les conseils à donner, les mesures à prendre et la manière de préserver la confidentialité ;
- Formation des enquêteurs ou des agents chargés d'établir les faits sur la manière de mener les enquêtes ;
- Formation du personnel des départements concernés (par exemple, conformité, bureau du médiateur) afin qu'il puisse apporter son soutien aux lanceurs d'alerte et assurer le suivi de leur dossier ;
- Formation de la direction et des cadres supérieurs à la réception des signalements, à la fourniture de conseils au personnel et à la transmission du signalement à la personne ou à l'unité compétente chargée de l'établissement des faits ;
- Formation de l'ensemble du personnel sur les droits et les recours en matière de signalement, les orientations disponibles et les mécanismes existants.



Chapitre 9.

SENSIBILISER

Les organisations doivent combattre la culture du silence qui peut exister au sein de leur personnel en sensibilisant à l'intérêt du signalement. En l'absence de mécanisme approprié, les désagréments liés au signalement d'une faute peuvent être trop évidents pour le personnel et le dissuader de s'exprimer. Une politique efficace de protection des lanceurs d'alerte doit promouvoir un environnement qui soutient et accueille la critique ouverte, le dialogue et la discussion⁷⁵.

Le signalement peut être présenté comme une occasion de réfléchir à la qualité des soins et de l'améliorer, plutôt que comme un acte préjudiciable aux personnes⁷⁶. Les professionnels de la santé se sentent souvent appelés à aider les autres et l'organisation devrait les aider à percevoir les rapports comme une occasion d'améliorer le système de santé. L'objectif devrait être de changer la façon dont sont perçus ceux qui décident de signaler les mauvaises pratiques.

Cependant, il serait naïf de penser que tous les membres du personnel s'engageront à signaler des actes répréhensibles potentiels uniquement par sens du devoir. L'organisation doit donner le ton au sommet et intégrer les principes éthiques, l'intégrité et la tolérance zéro dans la culture institutionnelle.

Afin de sensibiliser l'ensemble du personnel, il est essentiel que chacun ait accès à l'information. L'organisation doit mettre la politique sur la protection des lanceurs d'alerte à la disposition de toutes les personnes susceptibles d'être en mesure de faire part de préoccupations, et pas seulement des salariés. L'ensemble du personnel doit être informé et se voir rappeler régulièrement, par des affiches dans les salles de réunion et des activités de communication et de formation adaptées, l'existence et le contenu de cette politique.

Il convient de répondre aux questions suivantes :

- Existe-t-il une politique interne sur la protection des lanceurs d'alerte ?
- Pourquoi devrais-je faire part de mes préoccupations ?
- Quels manquements puis-je signaler ?
- À qui dois-je faire part de mes préoccupations et comment ?

⁷⁵ Jackson *et al.*, « Understanding whistleblowing », citant Benisa Berry, « Organizational culture: a framework and strategies for facilitating employee whistleblowing », *Employee Responsibilities and Rights Journal*, vol. 16 (mars 2004), p. 1 à 11.

⁷⁶ Ibid.

- Mon nom, mon identité et mes informations resteront-ils confidentiels si je fais un signalement ?
- Quels sont les risques que je prends ?
- Si je décide de faire un signalement, quelles mesures de protection seront mises en place ?

Ces informations doivent être annoncées ou présentées à l'aide de divers moyens, tels que des dépliants, des brochures⁷⁷, des affiches et, selon la taille de l'organisation, des conférences, des formations par jeux de rôle et des séminaires peuvent être organisés pour informer le personnel des différents mécanismes, voies et mesures de protection disponibles. L'organisation peut également choisir de faire connaître ses politiques sur son intranet, par le biais d'un bulletin d'information régulier et demander l'aide des syndicats du personnel concernés pour assurer une plus grande diffusion.

⁷⁷ Voir, par exemple, OMS, « Signalement des actes répréhensibles et protection contre les représailles ».

Chapitre 10.

TIRER LES ENSEIGNEMENTS DU PROCESSUS : ÉVALUATION DES RISQUES

Les organisations peuvent améliorer les contrôles internes en suivant les conclusions, les recommandations et les mesures correctives des affaires closes. En conservant et en analysant les données, les organisations peuvent détecter des schémas récurrents, ce qui peut constituer un outil d'apprentissage important pour les organisations concernées, à l'intérieur et à l'extérieur du secteur des soins de santé. Le développement de bases de connaissances peut contribuer à orienter les futurs mécanismes de signalement et aider à l'élaboration de nouvelles stratégies d'atténuation de la corruption dans le secteur des soins de santé. Les bases de connaissances sont également un outil crucial pour sensibiliser et briser le tabou et les dilemmes liés au signalement. Les enseignements tirés des affaires classées peuvent aider à :

- Améliorer les interfaces de signalement ;
- Mener les évaluations initiales ;
- Réduire les risques institutionnels ;
- Classer les signalements en catégories ;
- Innover dans les processus d'enquête ;
- Améliorer la communication.

Garder la trace des affaires classées permet également de constituer une base de bonnes pratiques qui pourront être adaptées et mises en œuvre à l'avenir. Par exemple, le centre médical Virginia Mason de Seattle, aux États-Unis, utilise les données obtenues par un « système d'alerte sur la sécurité des patients » pour améliorer sa culture de la sécurité⁷⁸. Une autre pratique essentielle et efficace consiste à conserver les dossiers officiels de tous les signalements faits et enquêtes menées au niveau de l'organisation, quel qu'en soit le résultat ou l'issue.

Ces dossiers peuvent servir d'outil analytique pour cartographier les zones de risque potentiel et les schémas au sein de l'organisation, afin de les inclure et de s'y concentrer dans les évaluations régulières des risques. Cela facilite ensuite l'élaboration de mesures d'atténuation sur mesure pour des zones à risque

⁷⁸ Pour une analyse, voir Aled Jones, « The role of employee whistleblowing and raising concerns in an organizational learning culture: elusive and laudable? » Comment on « Cultures of silence and cultures of voice: the role of whistleblowing in healthcare organisations », *International Journal of Health Policy and Management*, vol. 5, n° 1 (janvier 2016).

particulières. L'organisation peut donc souhaiter adopter ou améliorer sa politique en matière de tenue et de gestion des affaires⁷⁹.

Une façon d'adopter et de renforcer les mesures d'atténuation pour un domaine de risque particulier est de s'engager dans un processus d'évaluation du risque de corruption.

L'objectif du processus d'évaluation des risques est d'identifier un ensemble réaliste de risques potentiels, de les classer par ordre de priorité et de développer et mettre en œuvre des mesures et des stratégies d'atténuation efficaces et rentables. Les conclusions, les recommandations et les mesures correctives issues d'affaires antérieures ouvertes à la suite de signalements internes peuvent constituer une source d'information précieuse à toutes les étapes du processus.

Une fois qu'une organisation s'est engagée à effectuer une évaluation du risque de corruption, la première étape consiste à réaliser une auto-évaluation interne. Une telle évaluation consiste à réfléchir aux facteurs externes et internes qui façonnent le comportement de l'organisation et de ses membres, aux pouvoirs dont dispose l'organisation sur ces facteurs et aux contraintes auxquelles elle est confrontée dans l'exercice de ces pouvoirs. Les lois et règlements existants ainsi que les politiques et procédures internes de protection des lanceurs d'alerte doivent être inclus dans l'auto-évaluation. L'intégrité personnelle et professionnelle du personnel, la philosophie et le style de la direction, la manière dont l'organisation réagit aux signalements et aux informations provenant d'affaires classées donneront un aperçu des facteurs externes ou internes pertinents et démontreront comment l'organisation a réagi lorsqu'elle s'est heurtée à un risque particulier de corruption.

La deuxième étape consiste à recenser les éventuels risques de corruption. Les pratiques de corruption ou les risques potentiels de corruption mis en évidence dans les affaires classées peuvent être inclus dans la liste des vulnérabilités de corruption identifiées afin d'informer le processus d'évaluation des risques. Une fois la liste établie, l'organisation doit l'analyser et s'en servir comme base pour mener des entretiens avec le personnel, examiner les documents internes, les conclusions et recommandations antérieures et revoir les contrôles de la corruption existants.

La troisième étape consiste à évaluer les risques potentiels de corruption en fonction de la probabilité qu'ils se produisent et de la gravité de leur impact. Deux des questions clés à poser pour estimer la probabilité d'un risque de corruption sont de savoir si des actes de corruption similaires se sont produits dans l'organisation ou dans des organisations similaires et si les procédures internes comportent des garanties suffisantes pour dissuader ceux qui voudraient commettre de tels actes. Les informations fournies par les personnes qui ont communiqué des informations et les informations figurant dans les affaires classées sont très pertinentes à cet égard.

Il a été démontré que lorsqu'on demande aux individus d'estimer les risques, ils ont tendance à surestimer ou à sous-estimer la probabilité de certains événements en fonction de leur familiarité avec ceux-ci. Les organisations peuvent contrer le biais de familiarité en demandant aux individus pourquoi ils pensent qu'un acte de corruption est plus susceptible de se produire qu'un autre, ou si des cas récents ont pu affecter leurs estimations. Les informations figurant dans les dossiers ou signalements clos peuvent ou non indiquer la probabilité qu'un risque soit à nouveau un facteur, selon le contexte et les faits d'un cas particulier.

Si la probabilité et l'impact d'un risque de corruption particulier sont élevés, le risque doit être classé par ordre de priorité et une stratégie d'atténuation pertinente doit être élaborée. Pour ce faire, l'organisation doit analyser les contrôles existants, y compris ses procédures, règles et mesures visant à prévenir et détecter la corruption. Une fois encore, les constatations, recommandations et actions correctives antérieures peuvent aider à identifier les contrôles existants qui ne sont peut-être pas efficaces, à déterminer pourquoi ils ne sont pas efficaces et quel type de nouveaux contrôles peut être nécessaire. Comme les organisations disposent de ressources limitées, les nouveaux contrôles doivent être réalisables et abordables pour être efficaces. Pour être réalistes, les nouveaux contrôles doivent être spécifiques, clairs et leur coût ne doit pas

⁷⁹ Voir ONUDC, *État d'intégrité : Guide pour l'appréciation du risque de corruption dans les organismes publics* (Vienne, 2021).

dépasser la perte potentielle associée à un risque de corruption particulier. Une fois que de nouvelles mesures d'atténuation ont été définies, elles doivent être intégrées dans les plans de travail opérationnels et stratégiques de l'organisation, mises en œuvre et régulièrement revues et évaluées.

Cependant, il est crucial que le principe de confidentialité soit soigneusement observé dans le contexte du processus d'évaluation du risque de corruption. En effet, si les données extraites des affaires classées représentent une source précieuse d'informations, les types et les genres de données extraites doivent être examinés de manière à ne pas révéler, faire allusion ou conduire par inadvertance à l'identité de la personne qui communique des informations (comme son numéro de bureau ou son département). Toutefois, ces renseignements peuvent déjà avoir été divulgués si cette exposition a été préalablement autorisée par la loi, par exemple, si le consentement explicite de la personne concernée a été obtenu. Même si l'affaire est close, le risque de représailles peut toujours exister. Il est donc essentiel que le groupe chargé de réaliser l'évaluation des risques travaille en étroite collaboration avec la personne ou l'unité chargée des enquêtes sur les signalements afin d'évaluer le niveau d'information auquel il peut avoir accès et quels renseignements peuvent être inscrits dans le tableau d'évaluation des risques. Dans tous les cas, les informations obtenues à partir de dossiers clos doivent être recoupées afin de vérifier le principe de confidentialité.

Le processus d'évaluation du risque de corruption est détaillé dans la publication de l'ONUDC intitulée *État d'intégrité : Guide pour l'appréciation du risque de corruption dans les organismes publics*, qui fournit des informations supplémentaires et peut constituer une référence utile pour les organisations qui souhaitent utiliser les enseignements tirés des affaires classées pour atténuer et prévenir les risques de corruption futurs.



ONU DC

Office des Nations Unies
contre la drogue et le crime