ONUDC
Office des Nations Unies
contre la drogue et le crime

La Convention des Nations Unies contre la corruption

Guide de ressources sur

les bonnes pratiques en matière de protection des personnes qui communiquent des informations

OFFICE DES NATIONS UNIES CONTRE LA DROGUE ET LE CRIME
Vienne

La Convention des Nations Unies
contre la corruption

Guide de ressources sur les bonnes pratiques en matière de protection des personnes qui communiquent des informations

NATIONS UNIES
New York, 2016

La version originale du présent document n'a pas été revue par les services d'édition.

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

Préface

La corruption est un crime lourd de conséquences. Pourtant, la plupart des cas de corruption ne sont pas signalés ni détectés. Si les personnes hésitent à signaler des cas de corruption, c'est principalement parce qu'elles ont le sentiment que les autorités ne prendront pas leur signalement au sérieux et que rien ne sera fait. D'autres facteurs expliquent cette réticence, notamment la méconnaissance des mécanismes de signalement disponibles et la crainte de représailles.

De nombreuses enquêtes montrent que moins de 10 % des cas de corruption sont signalés*. Aussi les États parties doivent-ils de toute urgence surmonter ces obstacles, renforcer l'efficacité du suivi des signalements et protéger les personnes qui se manifestent.

La Convention des Nations Unies contre la corruption contient les dispositions nécessaires pour jeter les bases de telles initiatives. Ces dispositions sont exposées et expliquées en détail tout au long du présent Guide.

Le Guide explique pourquoi il est essentiel, afin de lutter contre la corruption, d'encourager et de protéger les personnes qui communiquent des informations concernant des allégations de corruption. Il devrait servir de ressource à l'usage des États parties pour qu'ils s'acquittent des obligations qui leur incombent au titre de la Convention en matière d'assistance et de protection à l'égard de ces personnes, qu'il s'agisse de membres du public ou de "lanceurs d'alerte" — terme par lequel on désigne habituellement les personnes qui travaillent au sein d'une organisation (publique ou privée) ou d'un secteur d'activité en proie à des irrégularités. L'adoption de mesures énergiques pour s'attaquer au problème, sur le plan juridique et politique, ainsi que pour protéger l'intérêt général, permettra aux États, aux autorités et aux organisations de tous les secteurs d'identifier et de poursuivre les auteurs d'actes illicites, et contribuera avant tout à éviter que la corruption ne prenne racine.

L'objectif du présent Guide est d'aider les États parties et d'autres acteurs nationaux à définir les réformes juridiques et institutionnelles qui pourraient être nécessaires pour répondre aux exigences internationales; de recenser les ressources et les mécanismes de soutien auxquels ils peuvent recourir à cette fin; et de mettre en évidence les questions qui devront être continuellement réexaminées à la lumière des nouveaux défis auxquels ils pourraient être confrontés.

* Voir, par exemple, les travaux de recherche de l'ONUDC sur la corruption dans les Balkans occidentaux, disponibles à l'adresse: http://www.unodc.org/unodc/en/data-and-analysis/statistics/corruption.html.

Les exemples de lois et de pratiques nationales donnés dans le présent Guide visent à aider les États parties et autres à reconnaître les différentes caractéristiques de leur propre cadre législatif et institutionnel pouvant servir de base à la protection des personnes qui communiquent des informations, ainsi que les éléments susceptibles d'entraver cette protection. La protection des personnes qui communiquent des informations est un domaine qui évolue rapidement; le présent Guide renvoie également le lecteur à un certain nombre de ressources qui peuvent constituer des sources constantes d'informations actualisées.

Remerciements

Le présent Guide est l'aboutissement du travail réalisé par le Service de la lutte contre la corruption et la criminalité économique de l'Office des Nations Unies contre la drogue et le crime (ONUDC) conformément au programme thématique intitulé "Action contre la corruption, la fraude économique et la criminalité liée à l'identité" (2012-2015).

L'ONUDC tient à remercier sa consultante, Anna Myers, pour sa contribution essentielle à la rédaction du Guide.

L'ONUDC exprime également sa profonde gratitude à ceux qui ont contribué, grâce à leurs connaissances et à leur expérience, à différentes étapes de l'élaboration du présent Guide, et aux experts qui ont participé à la réunion du Groupe international d'experts, tenue à Vienne les 22 et 23 mai 2014: Julio Bacioterracino, OCDE (France); Christian Bauer, Europol (Pays-Bas); Izani Bin Wan Ishak, Malaysian Anti-Corruption Commission (Malaisie); Jovana Blagotic, OCDE (France); A. J. Brown, Griffith University (Australie); Han Chee Rull, Malaysian Anti-Corruption Commission (Malaisie); Franz Chevarria Montesinos, spécialiste des lanceurs d'alerte (États-Unis); Tom Devine, Government Accountability Project (États-Unis); J. K. Devitt, Transparency International (Irlande); Paul Farley, Police de la ville de Londres (Royaume-Uni); Alexandra Habershon, Banque mondiale (États-Unis); Cathy James, Public Concern at Work (Royaume-Uni); Wolfgang Job, Ministère de l'intérieur (Autriche); Karen Kramer, ONUDC (Vienne); Hendrik Mauyoma, Ministère de la justice (Namibie); Sean McKessy, Securities and Exchange Commission (États-Unis); Sechang Oh, AntiCorruption and Civil Rights Commission (République de Corée); Fernandon Ortega Cadillo, Département de la prévention de la corruption (Pérou); Guido Strack, Whistleblower-Netzwerk (Allemagne); Slagana Taseva, Transparency International (Ex-République yougoslave de Macédoine); Alison Tilley, ODAC (Afrique du Sud); Mark Worth, Blueprint for Speech (Allemagne); Free Zenda, Ministère de la justice (Namibie); Wan Zulkifli Mohamed, Malaysian Anti-Corruption Commission (Malaisie).

L'ONUDC salue également la contribution des membres de son personnel qui étaient chargés de la mise au point du Guide, à savoir Constanze von Söhnen et Shannon Bullock, et de ceux qui ont fait part de leur expérience et de leurs commentaires, Candice Welsch et Constantine Palikarski.

L'ONUDC tient également à exprimer toute sa reconnaissance au Gouvernement australien, qui a généreusement financé la production du présent Guide.

Table des matières

Introduction

La corruption n'est pas l'apanage d'une région, d'une culture ou d'un système juridique particuliers. Lorsque rien n'est fait pour la juguler, elle prive des services publics, comme la santé, la protection sociale, la justice et l'éducation, de ressources considérables. La corruption dans la fonction publique constitue une grave atteinte à la confiance des usagers et à l'obligation pour l'agent public de rendre compte de son action, atteinte qui alimente la méfiance à l'égard des pouvoirs publics. Elle crée également un terrain propice à la criminalité organisée, entraîne des violations des droits de l'homme et menace la sécurité et le bien-être des communautés.

Dans le secteur privé, les actes de corruption produisent les mêmes conséquences néfastes, surtout lorsqu'il s'agit d'opérations frauduleuses conclues avec des acteurs étatiques, par exemple lors de la passation de marchés de biens et de services publics. Dans le domaine du commerce international, la corruption peut avoir des conséquences défavorables pour les populations au-delà des frontières. La corruption dans le secteur privé fausse la concurrence et peut augmenter les coûts; elle engendre une dépendance malsaine entre la demande et l'offre de corruption, aboutit à des opportunités commerciales ratées et viole les intérêts des investisseurs et des actionnaires. Les mêmes conséquences peuvent découler d'affaires de corruption entre deux acteurs du secteur privé. Les irrégularités dans la conduite transnationale des affaires et la privatisation de certaines fonctions publiques ont fait prendre davantage conscience des effets négatifs causés à la société par la corruption dans le secteur privé.

Par conséquent, pour être efficace, la lutte contre la corruption exige l'engagement de la société dans son ensemble. Le 31 octobre 2003, l'Assemblée générale des Nations Unies a adopté la Convention des Nations Unies contre la corruption (ci-après dénommée "la Convention contre la corruption"). Cette Convention a été largement ratifiée[1] et il s'agit du seul instrument universel et juridiquement contraignant qui offre un cadre complet pour prévenir et combattre la corruption.

La Convention contre la corruption exige des États qu'ils érigent en infraction les actes de corruption et qu'ils renforcent les enquêtes et les poursuites concernant ces infractions. Elle reconnaît également qu'une approche globale est nécessaire pour lutter contre ce

[1] Pour l'état des signatures et des ratifications, voir l'adresse: http://www.unodc.org/unodc/en/treaties/CAC/signatories.html.

fléau. La protection des personnes qui communiquent des informations présente un intérêt pour les trois objectifs de la Convention, à savoir: *a)* promouvoir et renforcer les mesures visant à prévenir et combattre la corruption de manière plus efficace; *b)* promouvoir, faciliter et appuyer la coopération internationale et l'assistance technique aux fins de la prévention de la corruption et de la lutte contre celle-ci, y compris le recouvrement d'avoirs; *c)* promouvoir l'intégrité, la responsabilité et la bonne gestion des affaires publiques et des biens publics. Les gouvernements accordent une importance croissante à la protection des personnes qui communiquent des informations. Non seulement cette protection permet de détecter plus facilement la corruption, mais elle constitue également une arme de dissuasion précieuse, dans la mesure où les auteurs de faits illicites peuvent moins facilement tabler sur le silence de ceux qui les entourent. Cette dimension préventive est soulignée dans la Convention contre la corruption, qui encourage les États à favoriser la participation active des personnes — en veillant notamment à ce qu'elles puissent communiquer en toute sécurité avec les autorités — et du public en général au signalement et à la prévention de la corruption.

Les infractions de corruption se révèlent difficiles à détecter, et ce pour diverses raisons. Dans certains cas, les personnes directement impliquées dans l'acte délictueux tirent toutes un avantage de la situation et, par conséquent, aucun signalement n'est effectué auprès de la police. Dans d'autres cas, par exemple lorsqu'un agent public exige un pot-de-vin en recourant à des moyens de contrainte, le corrupteur peut craindre de subir les représailles de cet agent ou de voir sa responsabilité pénale engagée car le fait de verser un pot-de-vin, comme le fait de le recevoir, constituent des infractions. Lorsque les personnes impliquées dans la corruption coopèrent avec les autorités, leur motivation est souvent liée au fait qu'elles pourront négocier la sanction ou obtenir un allègement de la peine dont elles sont passibles.

Par ailleurs, d'autres personnes peuvent être proches des individus impliqués dans des actes de corruption sans avoir elles-mêmes directement trempé dans de tels actes. Il peut s'agir de témoins de l'acte en question ou encore de personnes qui auront décelé les méthodes utilisées pour contourner le système et les procédures ou pour détourner des fonds de leur destination, ou qui sont susceptibles de voir le préjudice causé. Quand bien même ces personnes seraient en mesure de dire ce qu'elles savent, bien souvent elles n'en font rien.

Il est également important de rendre le signalement d'irrégularités plus facile et plus sûr afin de créer une culture organisationnelle plus résistante à la corruption. Il est plus difficile pour le secteur privé et le secteur public d'entretenir des liens frauduleux lorsque les organisations elles-mêmes indiquent clairement que le signalement de la corruption est encouragé et que les représailles à l'encontre des personnes qui signalent des irrégularités ne seront pas tolérées. Le fait d'encourager le personnel à contester les mauvaises pratiques et à signaler les irrégularités présumées renforce la capacité d'une organisation de résister aux pratiques malhonnêtes.

Malheureusement, sur de nombreux lieux de travail, les employés deviennent vulnérables s'ils signalent une irrégularité à une personne autre que leur employeur en raison des obligations implicites ou explicites de confidentialité, ou de leur sens de la loyauté. Les membres du public qui communiquent aux autorités des informations relatives à la corruption ne disposent pas nécessairement du statut légal leur permettant d'être protégés, et ce même s'ils sont victimes d'actes d'intimidation ou de menaces.

Le présent Guide adopte une approche holistique et étudie les mesures de protection disponibles pour les personnes qui communiquent des informations en général. Il explique pourquoi et comment les agents publics et autres employés sont protégés en droit et dans

la pratique à travers le monde lorsqu'ils signalent des irrégularités. Il examine également comment de telles mesures peuvent être mises en place pour protéger d'autres types de personnes qui communiquent des informations, comme les membres du public.

Le Guide explique en outre en quoi les mesures de protection des personnes qui communiquent des informations et les mesures de protection des témoins sont liées, et quels sont les éventuels éléments communs entre ces deux catégories de mesures. De plus, il décrit et explique certains des grands principes juridiques liés aux droits de l'homme, comme la liberté d'opinion et d'expression et le droit d'accès à l'information.

La protection des personnes qui communiquent des informations est déjà prévue dans plusieurs stratégies ou lois nationales de lutte contre la corruption, et l'adoption ou la révision de ce type de dispositions bénéficie d'une attention accrue des États et d'autres acteurs. Depuis 2010, des lois visant à protéger les lanceurs d'alerte ont été adoptées dans plus de 15 pays, parmi lesquels l'Australie, la Bosnie-Herzégovine, les États-Unis d'Amérique, l'Éthiopie, l'Inde, l'Irlande, la Jamaïque, la Malaisie, Malte, l'Ouganda, le Pérou, la République de Corée, la Serbie, la Slovaquie, le Viet Nam et la Zambie.

A. Leçons tirées des recherches sur le signalement

L'importance de la participation du public est évidente: de nombreuses recherches démontrent que les informations communiquées par des personnes constituent un des moyens les plus répandus — si ce n'est le moyen le plus répandu — de détecter des cas de fraude, de corruption et d'autres formes d'actes illicites.

Si les systèmes d'inspection sont importants, ils se sont avérés moins efficaces pour découvrir de tels actes. L'étude décrite ci-dessous confirme qu'un large éventail de personnes et d'institutions — allant des citoyens et des entreprises aux organisations non gouvernementales — sont en mesure de signaler des cas de corruption aux autorités compétentes, et qu'elles peuvent toutes être des sources d'informations importantes.

Exemple: L'Indonésie

Il ressort d'une étude de cas de corruption locale, menée dans les régions indonésiennes quelques années après l'entrée en vigueur du régime d'autonomie régionale, que toutes les enquêtes, sans exception, avaient été déclenchées sur la base d'informations communiquées par la population.

Aucun cas de corruption n'a été découvert grâce aux services de contrôle, aux organes de vérification des comptes ou aux institutions du secteur de la justice. Les cas de corruption ont été découverts puis signalés avant tout par des organisations non gouvernementales (ONG) ou des coalitions, de simples villageois, ainsi que par les personnes directement affectées par la corruption (par exemple des entreprises exclues de contrats lucratifs, des responsables politiques négligés lors d'un processus de présélection, etc.).

Les chercheurs ont découvert que, indépendamment de l'origine des premiers signalements, les ONG et les coalitions communautaires étaient le moteur de la divulgation et du règlement des affaires étudiées. Dans une affaire, un entrepreneur qui avait découvert des indices de corruption au sein du parlement local a préféré le signaler à une ONG locale plutôt qu'à la police ou aux procureurs du district.

Source: Rinaldi, T. *et al.*, *Fighting Corruption in Decentralised Indonesia — Case Studies on Handling Local Government Corruption*, Banque mondiale, Washington, D. C., mai 2007, p. 6.

Secteur public

D'après une importante étude australienne, les alertes lancées par les employés constituent le moyen le plus important de révéler les irrégularités dans les organisations du secteur public. Cette conclusion est fondée sur un sondage auquel ont répondu 828 responsables et titulaires de postes liés à la déontologie au sein de 14 organismes nationaux, provinciaux et locaux, sélectionnés parmi 118 organismes (et un échantillon total de 7 663 réponses)[2].

En 2010, le cabinet d'audit PricewaterhouseCoopers (PwC) a publié un rapport mondial sur la fraude dans le secteur public. Il a fondé ses conclusions sur les réponses communiquées par 170 représentants d'entreprises et d'organismes publics de 35 pays. Il a constaté que 31 % des cas de fraude avaient été détectés grâce à des dénonciations internes (adressées de façon informelle par des personnes travaillant au sein des organisations concernées)[3], 14 % grâce à des dénonciations externes (adressées de façon informelle par des personnes externes à l'organisme public) et 5 % grâce à des systèmes d'alerte formels et internes. Outre les 50 % de cas découverts grâce à des alertes (formelles et informelles), 14 % avaient été détectés par hasard[4]. Il a été constaté que la proportion de cas détectés grâce à un système d'alerte dans le secteur public était largement plus importante que dans le secteur privé. PwC a conclu que d'autres mesures permettant de détecter des cas de fraude ou de corruption, comme un audit interne ou un dispositif de gestion des risques, étaient a priori moins efficaces dans le secteur public que dans le secteur privé.

Secteur privé

PwC mène également, tous les deux ans, une enquête mondiale sur la criminalité économique[5]. En 2005, la première enquête a conclu que 31 % des cas de fraude en entreprise avaient été découverts grâce à des dénonciations et des alertes. L'enquête a conclu que les "contrôles" internes conçus pour détecter la fraude étaient "insuffisants" et que les lanceurs d'alerte devaient être encouragés à signaler les irrégularités et protégés contre les représailles. En 2011, l'enquête de PwC a conclu que 11 % des cas de fraude avaient été détectés grâce à des dénonciations internes, tandis que 7 % avaient été découverts grâce à des dénonciations externes. Cinq pour cent des cas avaient été détectés grâce à des systèmes d'alerte internes. Ainsi, la proportion totale de cas découlant d'alertes, sous une forme ou une autre, s'élevait à 23 %, ce qui était nettement inférieur à la proportion relevée en 2005, mais restait appréciable. Le rapport le plus récent, publié en 2014, a indiqué que ces chiffres restaient inchangés. Selon l'enquête de 2014, les cinq types de fraudes les plus communément signalés étaient le détournement d'avoirs, la fraude dans la passation des marchés, la corruption, la cybercriminalité et la fraude comptable.

L'Association of Certified Fraud Examiners (ACFE) (association des experts agréés en lutte antifraude) étudie régulièrement les alertes en milieu professionnel et fonde ses conclusions sur des rapports élaborés par des experts agréés en lutte antifraude dans les secteurs public et privé. Son dernier rapport sur la fraude en milieu professionnel adressé aux États (2014) comprenait des données relatives à 1 483 cas survenus dans plus de 100 pays. Le résumé du rapport souligne notamment les résultats suivants[6]:

[2] Brown, A. J. (dir. publ.), *Whistleblowing in the Australian Public Sector. Enhancing the Theory and Practice of Internal Witness Management in Public Sector Organizations*, Australian National University E Press, Australie, 2008.

[3] Les dénonciations sont considérées comme des alertes informelles en ce sens que le membre du personnel ne passe pas par un système formel d'alerte ou de signalement.

[4] PricewaterhouseCoopers, *Global Economic Crime Survey 2010*, 2011, p. 13, disponible à l'adresse: http://www.pwc.co.uk/forensic-services/publications/.

[5] Il s'agit d'une enquête menée auprès des présidents-directeurs généraux, des directeurs financiers et des responsables de la conformité de plus de 5 000 entreprises dans 40 pays.

[6] Association of Certified Fraud Examiners, Business Fraud, *Report to the nations on occupational fraud and abuse*, p. 4, disponible à l'adresse: http://www.acfe.com/rttn/docs/2014-report-to-nations.pdf.

- Les personnes sondées ont estimé que dans une organisation classique la fraude représentait une perte annuelle de 5 % des revenus. Les actes de corruption constituaient une forme intermédiaire de fraude en termes de fréquence (37 % des cas) et de perte moyenne (200 000 dollars des États-Unis).
- Les dénonciations restent, de loin, la méthode de détection la plus répandue. Plus de 40 % de tous les cas ont été détectés grâce à la dénonciation, soit plus du double du taux affiché par toute autre méthode de détection. Les employés étaient à l'origine de près de la moitié des dénonciations ayant abouti à la découverte de cas de fraude.
- Les organisations disposant d'une permanence téléphonique pour recueillir les signalements avaient beaucoup plus de chance de détecter les cas de fraude grâce aux dénonciations. Ces organisations ont également subi des fraudes dont le coût était de 41 % moins élevé et, dans 50 % des cas, elles les détectaient plus rapidement.
- Les plus petites organisations subissent généralement des pertes d'une importance excessive en raison de la fraude en milieu professionnel.

Le rapport a également conclu que "plus de la moitié de toutes les dénonciations émanaient de parties autres que des employés en tant que tels". Par conséquent, il convient de souligner à quel point il est important d'admettre des dénonciations provenant de diverses sources, et de sensibiliser les fournisseurs, les clients et les propriétaires/actionnaires aux moyens dont ils disposent pour signaler des soupçons de fraude[7].

Des conclusions semblables ressortent d'une étude menée en 2011 par KPMG sur les enquêtes en matière de fraude en Europe, au Moyen-Orient, dans les Amériques, en Asie et dans le Pacifique, selon laquelle 10 % des dénonciations s'étaient faites dans le cadre de mécanismes d'alerte, 14 % provenaient de sources anonymes et 8 % de fournisseurs ou de clients[8].

En 2010, l'ACFE a mené une évaluation mondiale selon laquelle les rapports d'alerte des employés constituaient la source la plus fréquente d'informations concernant la fraude (40 %). De plus, il ressort clairement de l'évaluation que, dans bien des cas, les termes "fraude" et "corruption" sont utilisés indifféremment. L'ACFE a conclu que "dans le cadre d'un programme de lutte contre la fraude, il est essentiel d'offrir aux personnes les moyens de signaler toute activité suspecte. La direction devrait encourager activement les employés à signaler les activités suspectes, et adopter puis mettre en avant une politique de protection contre les représailles."

B. Cadre offert par la Convention des Nations Unies contre la corruption

Prévoir des voies de signalement

Les autorités compétentes obtiennent ou reçoivent de sources multiples des informations concernant la corruption. Il peut s'agir de personnes physiques ou de personnes morales, comme des sociétés ou d'autres types d'organisations. Parmi ces sources figurent:

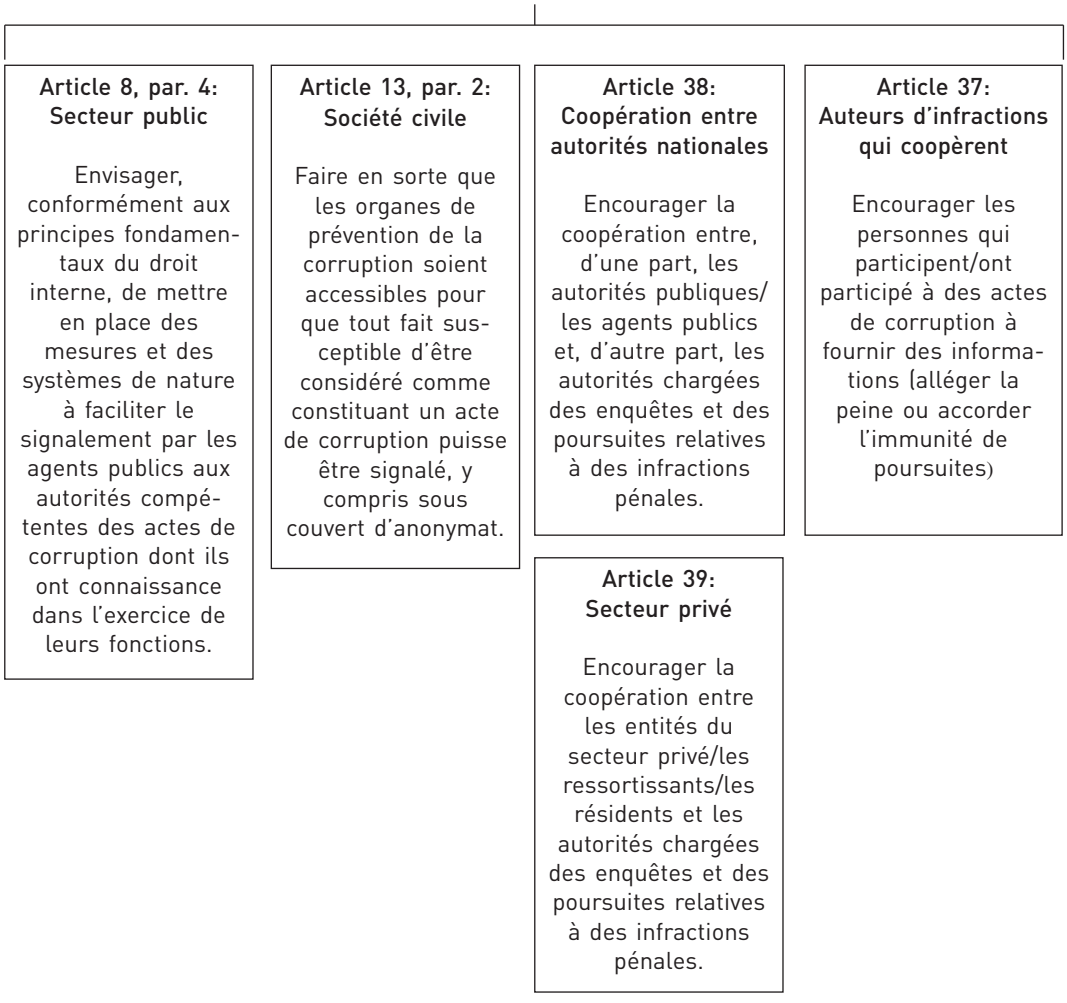
- Des agents publics au sein d'organismes publics — gouvernement central ou local, instances administratives, et entreprises d'État, etc. (y compris d'autres pays);

[7] Ibid., p.21.
[8] KPMG, *Who is the Typical Fraudster?*, 2011.

- Des employés du secteur privé — au sein de sociétés privées cotées ou non en bourse, et dans tous les secteurs, réglementés ou non (par exemple les finances, les transports, l'alimentation, la santé, les services sociaux, l'éducation, l'énergie, la vente au détail et la construction);
- Des sociétés ou d'autres personnes morales privées (par exemple des entreprises concurrentes qui ont perdu un marché parce qu'elles ont refusé de verser un pot-de-vin ou de prendre part à toute autre forme de corruption);
- Des syndicats ou des associations commerciales et professionnelles;
- Des organisations non gouvernementales (ONG) et des associations locales;
- Des membres du public;
- Des médias, notamment les médias sociaux;
- Des auteurs d'infractions ou des personnes impliquées.

La Convention contre la corruption reconnaît pleinement cette diversité. Elle contient plusieurs dispositions qui recommandent aux États de mettre en place des mesures et des systèmes de nature à faciliter le signalement, et de faire en sorte que les organes de prévention de la corruption soient accessibles pour permettre le signalement des cas de corruption (voir figure I).

Figure I. Articles de la Convention contre la corruption prévoyant des voies de signalement et des possibilités de coopération



Mesures de protection

S'agissant des mesures de protection, le texte de la Convention contre la corruption opère une distinction entre, d'une part, les mesures visant à protéger les témoins, les experts, les victimes et les auteurs d'infractions qui coopèrent lorsqu'ils sont témoins dans le cadre d'une procédure pénale (art. 32 et 37) et, d'autre part, les mesures visant les personnes qui communiquent des informations de manière plus générale (art. 33).

L'article 33 de la Convention demande aux États parties d'envisager l'adoption de 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 établies conformément à la présente Convention".

L'article 33 s'applique aux personnes qui peuvent posséder des informations qui ne sont pas suffisamment détaillées pour constituer des éléments de preuve au sens juridique du terme. Les États sont donc tenus d'envisager une protection dans tous les cas et non pas uniquement si la personne dépose en tant que témoin ou expert dans le cadre de la procédure pénale et peut, à ce titre, bénéficier de la protection prévue pour les témoins (pour de plus amples informations sur l'interaction entre, d'une part, la protection des personnes qui communiquent des informations ou des lanceurs d'alerte et, d'autre part, la protection des témoins et des auteurs d'infractions qui coopèrent, voir chapitre II, sections A et C.9).

En outre, l'article 33 demande aux États parties d'envisager des mesures de protection pour toute personne, qu'il s'agisse d'un citoyen, d'un usager, d'un client ou d'un employé, etc. Les mesures de protection dont une personne a besoin peuvent dépendre de nombreux facteurs, comme le type d'informations communiquées, la position de la personne et le niveau de la menace à laquelle la personne est confrontée en raison du signalement. Les employés, par exemple, peuvent être en proie à un conflit et hésiter entre signaler l'irrégularité et respecter leur devoir de loyauté ou de confidentialité envers leur employeur. Ils sont en outre particulièrement exposés à des représailles en raison de leurs relations de travail suivies. De nombreux pays reconnaissent le besoin d'assurer une protection particulière à cette catégorie de personnes qui communiquent des informations du fait qu'elles peuvent être les premières à avoir connaissance d'un problème et seraient, par conséquent, les mieux placées pour le signaler avant qu'un grave préjudice ne soit causé ou qu'une infraction ne soit commise. Les personnes présentes sur le lieu de travail étant "bien placées", elles peuvent tomber sur des activités ou des informations témoignant d'actes de corruption que des personnes extérieures ne pourraient voir.

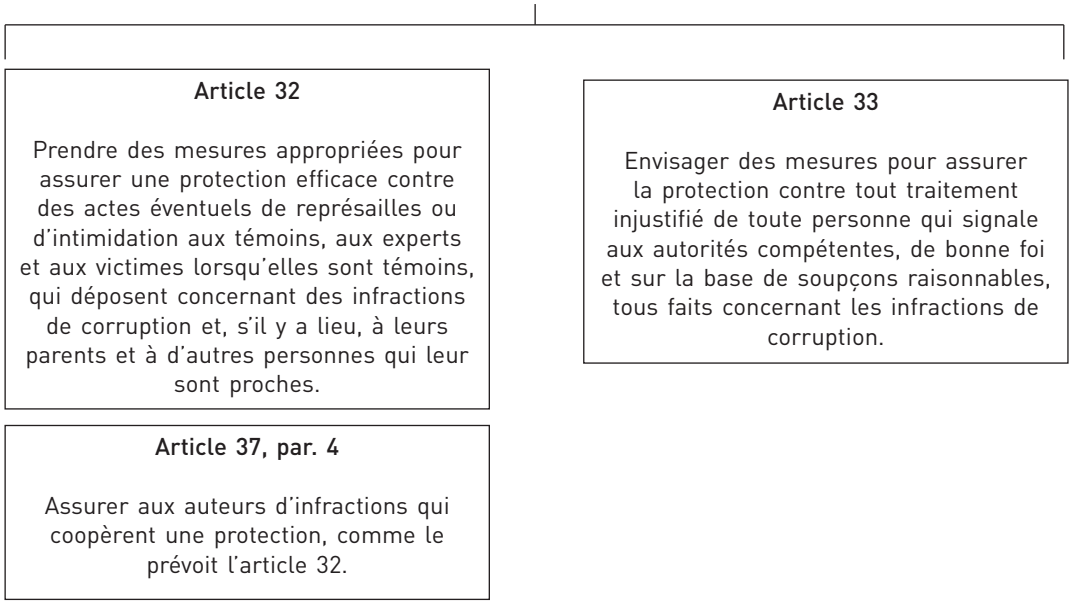
Dans certains pays, les employés peuvent intenter un recours ou demander réparation pour tout traitement injustifié qu'ils auraient subi au travail du fait qu'ils ont signalé des actes délictueux ou irréguliers ou communiqué des informations à ce sujet. De telles mesures de protection sur le lieu de travail revêtent une utilité accrue dans les cas qui ne sont habituellement pas couverts par les programmes de protection des témoins, et constituent une arme supplémentaire dans l'arsenal dont disposent les États parties pour lutter contre la corruption. Les mesures de protection peuvent également s'étendre aux situations dans lesquelles un employé qui communique des informations sur des irrégularités présumées en milieu professionnel est victime de représailles ou de harcèlement en dehors du lieu de travail.

Dans la pratique, diverses approches ont été adoptées pour assurer la protection des personnes qui communiquent des informations. Certains États parties privilégient les mesures de protection pour les témoins et/ou les auteurs d'infractions qui coopèrent et mettent en place des systèmes de signalement des infractions de corruption, mais ils ne tiennent pas compte des problèmes particuliers auxquels sont confrontées les personnes

qui communiquent des informations dans un cadre professionnel; certains prévoient une protection liée au contexte professionnel pour les employés du secteur public, tandis que d'autres étendent également cette protection au secteur privé, ou adoptent des dispositions qui couvrent toute personne.

En principe, les États parties sont encouragés à combler les lacunes, dans la législation ou dans la pratique, qui pourraient dissuader inutilement des personnes de communiquer des informations aux autorités compétentes ou qui les excluraient d'un dispositif de protection.

Figure II. Articles de la Convention contre la corruption relatifs à la protection des personnes qui communiquent des informations



Autres instruments internationaux

Outre la Convention contre la corruption, il existe un certain nombre d'instruments internationaux auxquels de nombreux États sont parties et qui les encouragent ou les invitent également à assurer une protection renforcée pour les personnes qui communiquent des informations (les articles pertinents sont mentionnés dans l'annexe du présent Guide). Parmi ces instruments figurent notamment:

- La Convention civile sur la corruption (1999), la Convention pénale sur la corruption (1999)[9] et la Recommandation sur la protection des lanceurs d'alerte (2014)[10] du Conseil de l'Europe;
- La Convention interaméricaine contre la corruption (1996)[11] de l'Organisation des États américains (OEA);

[9] Le Conseil de l'Europe, qui compte 47 États membres, a mis en place un mécanisme d'évaluation contre la corruption — le Groupe d'États contre la corruption (GRECO) — en application d'un accord partiel et élargi permettant à des États qui ne sont pas membres du Conseil de l'Europe d'y adhérer. Fort de ses 49 États membres, le GRECO suit l'application de la Convention civile sur la corruption de 1999 (disponible à l'adresse: http://conventions.coe.int/Treaty/fr/Treaties/Html/174.htm) et de la Convention pénale sur la corruption de 1999 (disponible à l'adresse: http://conventions.coe.int/Treaty/fr/Treaties/Html/173.htm).

[10] Conseil de l'Europe, Recommandation CM/Rec(2014)7 du Comité des Ministres aux États membres sur la protection des lanceurs d'alerte, disponible à l'adresse: https://wcd.coe.int/ViewDoc.jsp?id=2188939&Site=CM.

[11] La Convention interaméricaine contre la corruption a été ratifiée par 29 pays d'Amérique latine et des Caraïbes, ainsi que par les États-Unis d'Amérique et le Canada. Elle est disponible à l'adresse: http://www.oas.org/juridico/français/b-58.htm.

- La Convention de l'Union africaine sur la prévention et la lutte contre la corruption (2003)[12]; le Protocole de la Communauté de développement de l'Afrique australe contre la corruption (2001)[13];
- La Convention sur la lutte contre la corruption, la Recommandation visant à renforcer la lutte contre la corruption dans les transactions commerciales internationales, la Recommandation IX-iii) (2009)[14] et la Recommandation sur l'amélioration du comportement éthique dans le service public (1998)[15] de l'Organisation de coopération et de développement économiques (OCDE).

Certains de ces instruments sont accompagnés de documents d'orientation utiles, par exemple les lois types de l'OEA visant à protéger la liberté d'expression contre la corruption, à faciliter le signalement et à protéger les lanceurs d'alerte et les témoins (2004 et 2013)[16]; l'Exposé des motifs joint à la recommandation du Conseil de l'Europe; et un document publié par l'OCDE en 2011, contenant une étude sur les cadres de protection des lanceurs d'alerte, un recueil des meilleures pratiques et des principes directeurs relatifs à la législation[17].

C. Définitions et application du présent Guide

Dans le cadre des débats en matière de politique et de recherche, il est généralement admis que les décideurs politiques et les législateurs doivent avoir une idée précise des types de personnes qui communiquent des informations (ou des sources d'informations) visés, et des difficultés spécifiques que ces personnes rencontrent dans différentes circonstances. Plusieurs articles de la Convention contre la corruption opèrent ces distinctions, comme le montrent les figures I et II cidessus.

La Convention contre la corruption n'utilise pas le terme "lanceur d'alerte", mais parle plus généralement des personnes qui communiquent des informations.

Dans de nombreux pays, comme le Royaume-Uni[18], le terme "lanceur d'alerte" (*whistle-blower)* désigne un employé ou un travailleur (une personne interne à l'organisation concernée) qui divulgue des informations d'intérêt général (par exemple sur des actes de corruption, des irrégularités, des risques en matière de santé et de sécurité). La définition arrêtée par le Conseil de l'Europe adopte le même point de vue: "toute personne qui fait des signalements ou révèle des informations concernant des menaces ou un préjudice pour l'intérêt général dans le contexte de sa relation de travail, qu'elle soit

[12]Cette Convention, qui a été ratifiée par 31 États africains, exige de ceux-ci qu'ils adoptent des mesures "afin de s'assurer que les citoyens signalent les cas de corruption, sans craindre éventuellement des représailles". Le texte de la Convention est disponible à l'adresse: http://www.peaceau.org/uploads/convention-combating-corruption-fr.pdf.

[13]En vertu de ce Protocole, 13 pays africains s'engagent à protéger les personnes qui signalent des actes de corruption. Son texte est disponible à l'adresse: http://www.afrimap.org/english/images/treaty/sadc_protocole_contre_la_corruption.pdf.

[14]Les 34 pays membres de l'OCDE et 7 pays non-membres (Afrique du Sud, Argentine, Brésil, Bulgarie, Colombie, Fédération de Russie et Lettonie) ont adopté cette Convention. Voir la Convention sur la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales, disponible à l'adresse: http://www.oecd.org/fr/corruption/conventionsurlaluttecontrelacorruptiondagentspublicsetrangersdanslestransactionscommercialesinternationales.htm.

[15]Voir notamment le principe 4. Les détenteurs d'une charge publique ont besoin de connaître leurs droits et leurs obligations lorsqu'ils révèlent des actes répréhensibles, disponible à l'adresse: http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=129&Lang=fr&Book=False.

[16]Model Law Protecting Freedom of Expression against Corruption, 2004, disponible à l'adresse: http://www.oas.org/juridico/english/model_law_whistle.htm; Model Law to Facilitate and Encourage the Reporting of Acts of Corruption and to Protect Whistleblowers and Witnesses, 2013, disponible à l'adresse: http://www.oas.org/juridico/english/law_reporting.htm.

[17]OCDE, Study on Whistleblower Protection Frameworks, *Compendium of Best Practices and Guiding Principles for Legislation*, disponible à l'adresse: http://www.oecd.org/daf/anti-bribery/48972967.pdf.

[18]*Public Interest Disclosure Act*, 1998.

dans le secteur public ou dans le secteur privé[19]". Les employés et autres personnes qui travaillent pour une organisation dans le secteur public ou privé sont souvent plus proches de la source du problème et, par conséquent, plus à même de communiquer des faits concernant des actes illicites ou irréguliers qui, s'il n'y est pas mis fin, peuvent entraîner un préjudice grave. Qu'il s'agisse d'une institution publique ou d'une entreprise privée, un organisme employeur doit faire preuve de diligence raisonnable et respecter les codes de conduite, les règlements intérieurs et le droit.

Dans les pays qui emploient le terme "lanceur d'alerte" en rapport avec le signalement et la protection sur le lieu de travail, les législateurs devraient prendre en considération les deux aspects suivants: premièrement, ils devraient envisager d'inclure un large éventail de personnes du secteur public et du secteur privé (par exemple des employés, des sous-traitants, des consultants, des stagiaires, des bénévoles, des travailleurs des secteurs informels de l'économie et d'autres personnes susceptibles d'avoir accès aux informations pertinentes); et, deuxièmement, ils devraient tenir compte de la nécessité d'assurer la protection d'autres personnes qui communiquent des informations et qui n'entreraient pas dans le champ d'application de la protection des lanceurs d'alerte en milieu professionnel ni dans celui de la protection des témoins. Il s'agit notamment des personnes qui communiquent des informations qui ne sont pas suffisamment détaillées pour constituer des éléments de preuve dans le cadre de procédures pénales, mais sont néanmoins liées à des actes de corruption présumés.

Dans d'autres pays, comme la Malaisie, la loi entend par lanceur d'alerte "toute personne qui dénonce un comportement répréhensible" à un service de détection et de répression[20]. Il importe peu de savoir qui est la source de l'information (un employé ou un membre du public par exemple), dans la mesure où le cadre applicable s'intéresse uniquement à la nature du problème ou du grief signalé. La loi assure la protection des informateurs ou "lanceurs d'alerte" en termes de confidentialité des informations et d'immunité de poursuites civiles et pénales[21].

Les membres du public sont plus enclins à signaler des préjudices ou des dommages qu'ils ont personnellement subis ou qui affectent leur communauté. Il peut s'agir, par exemple, d'une plainte concernant un retard injustifié dans la délivrance d'un permis, d'une route à moitié construite, d'un médecin absent ou peu formé, ou de produits alimentaires contaminés. De telles réclamations peuvent également aider à découvrir différentes formes de comportements délictueux. Si la personne à l'origine de la réclamation souhaite sans doute voir des poursuites engagées à l'encontre de l'individu responsable du préjudice causé, et peut soupçonner certains actes de corruption, les éléments de preuve établissant la faute ou la négligence devront probablement provenir d'autres sources. Toutefois, comme le montre l'exemple indonésien ci-dessus, les procédures de réclamation publiques peuvent constituer une source supplémentaire d'informations très utile. Elles devraient être connues du public et accessibles à tous, conformément au paragraphe 2 de l'article 13 de la Convention, et les membres du personnel chargés de traiter ces recours devraient les examiner attentivement pour rechercher d'éventuels indices de corruption.

[19] Conseil de l'Europe, Recommandation CM/Rec(2014)7 du Comité des Ministres aux États membres sur la protection des lanceurs d'alerte. Le texte de la recommandation est disponible à l'adresse: https://wcd.coe.int/ViewDoc.jsp?id=2188939&Site=CM.

[20] https://www.bheuu.gov.my/portal/pdf/Akta/Act%20711.pdf.

[21] Conformément à la loi, un lanceur d'alerte ne bénéficie d'aucune protection s'il décide de rapporter son allégation d'irrégularité à une personne autre qu'un service de détection et de répression. La protection peut être annulée si le lanceur d'alerte commet une infraction sanctionnée par la loi, notamment s'il communique le contenu de son signalement à un tiers, révélant ainsi son identité, ce qui rend difficile la protection des informations confidentielles, à savoir l'identité de la source et les informations communiquées.

Tout en faisant largement appel aux connaissances accumulées et aux leçons tirées en matière de protection des personnes révélant des informations qu'elles découvrent dans le cadre de leur travail (dans le secteur public ou privé), le présent Guide présente également des exemples relatifs à d'autres personnes qui communiquent des informations et s'attache à appuyer des stratégies étatiques destinées à gérer ce vaste ensemble de scénarios et de signalements possibles. Il convient d'engager une réflexion sur les meilleurs moyens de protéger les membres du public, qui sont également susceptibles de subir de graves actes d'intimidation et de représailles s'ils osent communiquer des informations ou coopérer de toute autre manière avec les autorités.

D. Résultats du mécanisme d'examen de l'application de la Convention contre la corruption

Le mécanisme d'examen de l'application[22] de la Convention des Nations Unies contre la corruption est un mécanisme intergouvernemental d'examen par des pairs, dans le cadre duquel chaque État partie est examiné par deux autres États parties. L'objectif du mécanisme d'examen est d'aider les États parties à appliquer la Convention en déterminant les succès et bonnes pratiques, les difficultés d'application et les besoins d'assistance technique pour chaque disposition de la Convention. Chaque examen donne lieu à un rapport de pays et à un résumé analytique comprenant des observations et des recommandations sur l'application des dispositions de la Convention[23].

De nombreux examens ont abouti à la formulation de recommandations en vue de l'adoption d'une législation et de mesures appropriées pour la protection des personnes qui communiquent des informations; du renforcement des dispositifs existants pour la protection des lanceurs d'alerte; et de l'inscription explicite des infractions visées par la Convention contre la corruption dans le champ d'application de la loi sur la protection des lanceurs d'alerte[24].

L'importante quantité de renseignements recueillis dans le cadre du mécanisme d'examen permet également d'en savoir davantage sur les tendances régionales et mondiales. Une analyse des examens a montré que l'assistance technique était avant tout nécessaire en ce qui concerne la protection des témoins, les auteurs d'infractions qui coopèrent et la protection des personnes qui communiquent des informations (art. 32, 33 et 37 de la Convention contre la corruption)[25].

Le présent Guide répond aux besoins d'assistance technique recensés par les États parties et vise à leur fournir les ressources et les exemples nécessaires pour mettre en place des mécanismes institutionnels et juridiques efficaces et solides, qui leur permettront d'assister et de protéger les personnes qui communiquent des informations.

[22] http://www.unodc.org/unodc/fr/treaties/CAC/IRG.html.

[23] On trouvera des informations par pays à la page consacrée au profil des pays. Ces informations sont disponibles à l'adresse: http://www.unodc.org/unodc/en/treaties/CAC/country-profile/index.html.

[24] CAC/COSP/IRG/2014/10, Application des chapitres III (Incrimination, détection et répression) et IV (Coopération internationale) de la Convention des Nations Unies contre la corruption: aperçu thématique des recommandations. Texte disponible à l'adresse: http://www.unodc.org/unodc/en/treaties/CAC/IRG-session5.html.

[25] CAC/COSP/IRG/2014/3, Analyse des besoins d'assistance technique qui ressortent des examens de pays, p. 5, disponible à l'adresse: http://www.unodc.org/documents/treaties/UNCAC/WorkingGroups/ImplementationReviewGroup/2-6June2014/V1402637f.pdf. Pour un résumé analytique des observations et recommandations formulées à l'intention des États parties en ce qui concerne l'article 33 de la Convention, voir le document de séance nº 7, intitulé "The state of UNCAC implementation", publié lors de la cinquième session de la Conférence des États Parties à la Convention contre la corruption. Document disponible à l'adresse: http://www.unodc.org/unodc/en/treaties/CAC/CAC-COSP-session5.html.

I.

Évaluation nationale

Les États parties qui prévoient de mettre en place un cadre législatif et institutionnel pour la protection des personnes qui communiquent des informations, ou de réformer le cadre existant, devraient savoir qu'il importe avant tout de procéder à une analyse de la situation actuelle et de consulter les principales parties prenantes. Le présent chapitre a pour objet d'aider les gouvernements à élaborer un plan d'évaluation nationale et à déterminer les personnes les plus indiquées qu'ils devront consulter pour définir les mesures nécessaires. Cette analyse des besoins et des lacunes est essentielle pour prendre des décisions politiques et adopter des réformes juridiques en connaissance de cause. Elle peut également aider les pays à étudier les normes applicables dans d'autres pays qui ont déjà adopté des lois pour protéger les personnes qui communiquent des informations.

Les États parties devraient envisager une approche proactive dès le départ. Les approches adoptées dans les différents pays varient et ont été influencées par des considérations multiples, notamment par des contextes juridiques, culturels et politiques différents. Certaines approches visent essentiellement à lutter contre la corruption et la criminalité organisée; d'autres ont été élaborées en réponse à une catastrophe ou un scandale ayant révélé les failles des systèmes de responsabilisation et de contrôle existants. Les mesures alors mises en œuvre ont été ajustées au fil du temps pour faire face aux nouveaux défis, et ce en fonction des enseignements tirés quant aux mesures les plus efficaces dans la pratique.

Dans certains pays, la société civile et les associations locales jouent un rôle actif pour soutenir les nouvelles lois et veiller à ce qu'elles soient effectivement appliquées. Ces groupes peuvent aider à faire en sorte que les informations relatives aux irrégularités, à la corruption et aux risques soient communiquées et fassent l'objet d'une enquête (voir les exemples fournis au chapitre II). Enfin, il convient également de prendre en considération l'importance du signalement de cas de corruption par les médias, ainsi que l'incidence des nouvelles technologies sur les moyens dont disposent les personnes pour communiquer des informations.

Dans l'ensemble, les particuliers peuvent se poser un certain nombre de questions clés pour décider s'ils doivent ou non signaler une irrégularité:

- Les informations que je possède méritent-elles d'être rapportées? Combien de détails dois-je fournir et de quels facteurs dois-je tenir compte avant de communiquer des informations?

- À qui dois-je communiquer les informations et existe-t-il plusieurs options?
- À quelle forme de protection puis-je m'attendre dans l'immédiat et que se passera-t-il si quelqu'un exerce des représailles à mon encontre ultérieurement?
- Comment les informations seront-elles traitées par les personnes auxquelles je les communique?
- Qui peut m'aider et me conseiller?

Du point de vue d'une personne qui communique des informations, ces questions sont pragmatiques et sérieuses. Du point de vue des gouvernements, étudier les réponses à ces questions est une manière utile de déterminer les besoins auxquels les lois et systèmes nationaux doivent répondre afin qu'il devienne plus facile et plus sûr de signaler des cas de corruption. Tous ces points sont abordés en détail dans le chapitre II.

A. L'importance de prendre des décisions éclairées

Lorsque les États examinent le meilleur moyen de faciliter les signalements et de protéger les personnes qui communiquent des informations, il est important de déterminer les facteurs favorables et défavorables à la participation du public au système en vigueur. Il convient ainsi de déterminer les points forts, la solidité de l'état de droit dans le pays (par exemple l'accès à une procédure judiciaire impartiale, équitable et efficace), et la capacité institutionnelle existante de mener des enquêtes ainsi que de prendre des mesures correctives et protectrices. Un examen complet des mécanismes de signalement existants permettra de trouver le moyen de les améliorer.

L'expérience montre que les lois élaborées en consultation avec les parties prenantes ont plus de chances d'être efficaces. Il est essentiel d'organiser de véritables consultations pour légitimer tout programme de réforme et pour encourager le public à prendre part au système. Cela est d'autant plus important lorsque l'environnement social et culturel est particulièrement hostile, pour des raisons historiques ou autres, à l'idée qu'une personne puisse signaler aux autorités un problème qui ne la concerne pas directement.

> Les "donneurs d'alerte" ne sont pas des "traîtres" mais des personnes courageuses qui préfèrent agir contre les abus dont elles sont témoins plutôt que d'opter pour la facilité en restant silencieuses. Pour cela, il faut infléchir des attitudes culturelles profondément ancrées depuis les régimes sociopolitiques de dictature et/ou de domination étrangère, sous lesquels il était tout à fait normal de se méfier des "informateurs" des autorités méprisées[26].

Un examen complet doit être préparé soigneusement. Les États parties devront définir et circonscrire l'objectif des nouvelles mesures et s'assurer la coopération et la participation des instances nationales et locales et des organismes publics. Ceux qui participent à l'amélioration des systèmes destinés à assister et protéger les personnes qui communiquent des informations attachent généralement beaucoup plus d'intérêt à leur efficacité et seront probablement des partenaires disposés à contrôler et évaluer les mesures dans le temps. Les gouvernements peuvent ainsi avoir plus aisément accès à des informations qualitatives et quantitatives sur l'efficacité des mécanismes et des protections juridiques mis en place.

[26] Assemblée parlementaire du Conseil de l'Europe, La protection des "donneurs d'alerte", rapport de la Commission des questions juridiques et des droits de l'homme, Doc. 12006, 14 septembre 2009, par. 1, disponible à l'adresse: http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=12302&lang=fr.

B. Consultation des parties prenantes

Il est important de solliciter la contribution active des principales parties prenantes tant à l'intérieur qu'à l'extérieur du gouvernement. Une attention particulière doit être accordée à: *a)* celles qui entretiennent des contacts directs avec le public dans un certain nombre de domaines clés, notamment la détection et la répression, la lutte contre la corruption et la prestation de services publics de premier plan; et *b)* celles qui travaillent dans des domaines particulièrement exposés ou associés à la corruption, comme l'éducation, les services de santé, le contrôle aux frontières, les douanes ou les marchés publics. Certaines de ces parties prenantes auront déjà mis en place des mécanismes de signalement, tels que des permanences téléphoniques ou des systèmes en ligne, et seront en mesure de rendre compte du mode et de la fréquence d'utilisation de ces méthodes, et d'indiquer qui les utilisent et dans quel but.

Les syndicats, les groupes juridiques et commerciaux, les organisations de la société civile et les associations locales ont souvent de l'expérience dans l'utilisation des mécanismes de signalement existants ou dans l'appui à ceux qui utilisent de tels mécanismes. Ils peuvent aider le gouvernement à déterminer les aspects qui fonctionnent bien, ceux qui ne fonctionnent pas et les raisons des dysfonctionnements, ainsi que les obstacles qu'il reste à surmonter en matière de signalement. Ils peuvent indiquer au gouvernement les mesures susceptibles d'avoir les retombées les plus significatives. Il peut s'agir de mesures simples et pratiques, comme un accès gratuit à une permanence téléphonique plutôt qu'un portail en ligne, ou la mise en place de points de contact auprès desquels les personnes peuvent directement obtenir des informations et des conseils.

En Bosnie-Herzégovine, une loi sur les lanceurs d'alerte applicable aux agents des institutions étatiques a été adoptée en décembre 2013 après deux ans de campagne publique et politique. Nombre d'organisations de la société civile, de parlementaires issus de divers partis politiques et d'agents publics ont participé à cette campagne. Cette initiative associant diverses parties prenantes a été jugée sans équivalent en Bosnie-Herzégovine[27], où la loi a été adoptée à l'unanimité par le Parlement. Des initiatives semblables sont en cours dans de nombreux autres pays, notamment en Allemagne, en Finlande, en Grèce, en Italie, en République tchèque et en Ukraine.

Les États parties devraient également garder à l'esprit que pour être viables, certaines mesures pratiques qui peuvent être mises en œuvre rapidement doivent encore, dans certains cas, être inscrites dans la loi. De larges consultations aideront toutefois à planifier les réformes, à les adapter au contexte national et à les hiérarchiser (notamment en accordant la priorité aux personnes les plus vulnérables ou aux domaines les plus propices à la corruption).

Ainsi, les efforts déployés immédiatement peuvent être axés sur la création ou l'amélioration des mécanismes de signalement pour les agents publics et sur la formation des personnes chargées de traiter les signalements de corruption. Il peut également devenir évident que la capacité d'une ou de plusieurs autorités existantes doit être sensiblement renforcée afin de mieux protéger les personnes qui communiquent des informations et qui se sont déjà mises en contact avec elles. Certains experts se demandent si un système davantage centralisé serait plus utile dans des environnements où la culture du signalement est faible. Cette question pourrait faire l'objet de futures recherches. Indépendamment de l'approche adoptée, si les États entendent lutter efficacement contre la corruption, il est essentiel de permettre aux personnes de communiquer des informations

[27] Agence des États-Unis pour le développement international, Protecting Whistleblowers in Bosnia and Herzegovina, disponible à l'adresse: http://www.usaid.gov/results-data/success-stories/protecting-whistleblowers-bosnia-and-herzegovina.

en toute sécurité et de faire en sorte que l'obligation de rendre des comptes soit ainsi reconnue et renforcée.

La liste ci-dessous indique les entités qui pourraient participer et qui ont participé aux examens juridiques et institutionnels menés au niveau national:

- Ministères compétents, notamment les ministères de la justice et du travail ou de l'emploi;
- Ministères chargés de domaines sensibles ou touchés par la corruption, comme les ministères chargés des douanes, de l'éducation, des soins de santé et des marchés publics;
- Autres organismes chargés des contrôles et de l'application des lois, par exemple des organismes chargés des normes de santé et de sécurité, ou des normes applicables au commerce;
- Commissaires chargés de l'information, du respect de la vie privée et de la protection des données;
- Commissaires chargés des droits de l'homme et médiateurs;
- Comités d'éthique et d'intégrité, y compris les commissaires chargés de la fonction publique au niveau du gouvernement central et local;
- Syndicats et associations du personnel;
- Groupes chargés de la défense des droits de l'homme, des droits des communautés et des consommateurs;
- Organisations juridiques ou de sensibilisation, notamment celles qui conseillent et protègent les lanceurs d'alerte et traitent les questions de corruption;
- Organismes professionnels pour les juristes, auditeurs, ingénieurs, médecins, etc. (y compris les comités de discipline ou d'éthique);
- Entités judiciaires;
- Organes de détection et de répression, notamment la police, le parquet et les procureurs spécialisés;
- Autorités d'audit nationales et locales;
- Organismes de contrôle par secteur, chargés par exemple de l'éducation, des services sociaux, de la santé et de la sécurité, des finances, des pratiques anticoncurrentielles et des pratiques commerciales loyales;
- Organismes professionnels, par exemple de médecins, de juristes, d'auditeurs;
- Organisations commerciales et associations du secteur privé.

Exemple: Consultation au sujet d'une nouvelle loi (Serbie)

En 2012, le Commissaire à l'information et le Bureau du médiateur ont créé un groupe de travail dont faisait partie l'Agence de lutte contre la corruption afin d'élaborer un projet de loi non officiel de protection des lanceurs d'alerte en Serbie. Une conférence a été organisée pendant deux jours en mai 2013 et a réuni des experts nationaux et internationaux, des universitaires, des juristes, des technologues, des militants et des défenseurs de droits pour étudier les bonnes pratiques. Les médias ont couvert cette conférence qui a été retransmise en temps réel et les contributions des participants ont été publiées en ligne en décembre. Il s'agit du premier livre de ce type publié en serbe.

En 2013, le Ministère de la justice a entamé le processus formel de préparation d'une loi sur les alertes en milieu professionnel et, conformément à une approche multidisciplinaire, a créé un groupe de travail composé de plus de 20 représentants clés des ministères compétents; de juges issus de tous les degrés de juridiction, notamment le vice-président de la Cour suprême; de représentants des principaux syndicats et associations d'employeurs, y compris des chambres de commerce, ainsi que de représentants de la société civile. Deux lanceurs d'alerte serbes faisaient également partie du groupe de travail — un juge et un inspecteur de police. Quatre experts internationaux en matière de la lutte contre la corruption et de protection des lanceurs d'alerte ont été invités à participer à certaines réunions spécifiques du groupe de travail. Une fois prêt, le projet de loi a été publié afin de permettre aux parties intéressées de présenter des observations, avant d'être examiné par le groupe de travail.

La loi a été adoptée par le Parlement serbe en novembre 2014. Une période d'application de six mois a permis au Gouvernement de former les juges à la nouvelle loi, leur laissant ainsi le temps d'élaborer un code de bonnes pratiques que les employeurs ont été tenus de mettre en œuvre à compter de l'entrée en vigueur de la nouvelle loi en juin 2015.

Source: Voir le site Web du Commissaire serbe à l'information, disponible à l'adresse: http://www.poverenik.rs/images/stories/dokumentacija-nova/Publikacije/Uzbunjivaci/zastita%20uzbunjivaca_kraj.pdf. Certains chapitres sont disponibles en anglais sur le site Web de Whistleblowing International Network, à l'adresse: www.whistleblowingnetwork.org et la traduction complète de la publication est prévue.

C. Principaux domaines à examiner

Les trois grands domaines qui devront être traités sont les suivants:

- Législation et dispositifs institutionnels;
- Besoins et lacunes;
- Sensibilisation et confiance.

1. Législation et dispositifs institutionnels

Un nombre croissant d'États parties ont adopté des dispositions juridiques visant la protection des personnes qui communiquent des informations, voire des lois autonomes très spécifiques, la protection se limitant habituellement aux témoins dans le cadre d'un procès pénal ou s'inscrivant le plus souvent dans des règles générales relatives aux obligations dans le secteur public, aux conditions d'emploi ou au droit du travail.

Les États devraient s'efforcer de procéder à une évaluation et un examen complets de leur cadre législatif. Il est important qu'un tel examen permette de déterminer si des lois et des politiques se recoupent, se contredisent ou se nuisent, et menacent par conséquent la protection des personnes qui communiquent des informations en général et des lanceurs d'alerte en milieu professionnel en particulier. Les lois relatives à la diffamation et la calomnie, les règles restrictives en matière de confidentialité, les règles de protection des données et les lois relatives au secret bancaire ou autre secret pourraient notamment poser un problème. Les États parties devraient étudier les moyens d'harmoniser les différentes dispositions. Si l'on ne tient pas compte de la manière dont les multiples devoirs et obligations s'appliquent aux personnes qui communiquent des informations, toute nouvelle mesure risque d'être inefficace. Si les personnes ont des doutes quant aux mesures de protection disponibles et aux circonstances dans lesquelles elles pourront en bénéficier, elles préféreront probablement se taire. L'expérience montre que même les très bons systèmes de signalement ne seront pas utilisés en cas de conflit avec des règles et obligations existantes.

En 2012, le Gouvernement irlandais a décidé de renoncer aux dispositions sectorielles pour la protection des lanceurs d'alerte, et de regrouper et renforcer les protections dans une loi unique (voir l'enquête menée par le Tribunal Mahon au chapitre I[er], section C.2.). Le Ministre chargé des réformes a déclaré que le nouveau projet de loi représentait "une étape importante dans l'exécution du programme gouvernemental de réforme politique", puis a indiqué que ce projet de loi "prévoit pour la première fois une protection complète des lanceurs d'alerte dans tous les secteurs de l'économie, comblant ainsi ce qui a été considéré, aux niveaux national et international, comme une lacune importante dans le cadre juridique irlandais de la lutte contre la corruption[28]". Certains experts estiment qu'une législation complète et autonome peut conférer plus de visibilité à la loi, rendant ainsi sa promotion plus facile pour les pouvoirs publics et les employeurs[29]. Cette approche permet en outre d'appliquer les mêmes règles et procédures aux employés du secteur public et du secteur privé, contrairement à une approche plus fragmentaire reposant sur différentes lois, qui souvent ne s'appliquent qu'à certains employés et à la communication de certains types d'irrégularités.

On trouvera ci-après une liste non exhaustive de lois et de règles dont les États parties devront probablement tenir compte avant d'envisager toute mesure visant à protéger les personnes qui communiquent des informations:

- Lois pénales, notamment en ce qui concerne les poursuites pénales pour diffamation et faux signalement, les sanctions imposées en cas de non-signalement de certaines catégories d'infractions, l'interdiction des représailles contre les personnes qui signalent une infraction, les entraves au bon fonctionnement de la justice, et les lois relatives à la protection des témoins;
- Lois sectorielles, relatives par exemple à la lutte contre la corruption, à la concurrence, à la santé et la sécurité, à la comptabilité, à la protection de l'environnement, aux sociétés et aux valeurs mobilières;
- Mesures spécifiques de lutte contre la corruption, notamment toute loi relative aux conflits d'intérêts, etc.;
- Lois relatives aux droits de l'homme, notamment en ce qui concerne le droit à la liberté d'expression, tel que consacré à l'article 19 du Pacte international relatif aux droits civils et politiques;
- Lois relatives à l'accès à l'information ou au droit à l'information, en particulier en ce qui concerne toute limite à la divulgation d'informations fondée sur des raisons de sécurité nationale ou de relations extérieures, et toute règle qui empêche les agents publics de s'acquitter de leur obligation légale de communiquer des informations;
- Lois relatives aux informations confidentielles ou protégées, au secret professionnel et/ou à la confidentialité, et à la protection des données personnelles;
- Lois relatives aux médias, notamment à la protection des journalistes et de leurs sources, et règles régissant les droits d'auteur;
- Lois relatives aux contrats de travail et à l'emploi, notamment en ce qui concerne la protection contre les manquements à l'obligation de confidentialité ou de

[28]Le Ministre a annoncé que le Gouvernement mettait en œuvre un cadre général unique de protection des lanceurs d'alerte, applicable uniformément dans tous les secteurs de l'économie, et a, à cette fin, mis en œuvre une nouvelle loi intitulée *Protected Disclosures Act* (loi sur les révélations protégées), 2014. Communiqué de presse du 3 juillet 2013 sur la publication du *Protected Disclosures Bill* de 2013 (projet de loi sur les révélations protégées), disponible à l'adresse: http://www.per.gov.ie/publication-of-the-protected-disclosures-bill-2013/.

[29]Banisar, D., Whistleblowing: International Standards and Developments, 2009, p. 19 à 21. Transparency International, Recommended Principles for Whistle-blowing Legislation, Recommendation 23: "Législation spécifique — afin de garantir une application certaine, claire et homogène du cadre, une législation unique est préférable à une approche fragmentaire ou sectorielle".

loyauté; l'interdiction ou l'annulation de tout accord qui vise à empêcher une personne de communiquer ou de divulguer des informations d'intérêt général; la protection contre les licenciements abusifs ou toute autre forme de représailles liées à l'emploi, notamment les actes commis par des pairs ou des collègues;

- Lois et accords relatifs au travail, en particulier en ce qui concerne le droit collectif de signaler ou de divulguer des problèmes d'intérêt général;
- Obligations professionnelles de signalement: protection pour les personnes qui ont des obligations spécifiques de signalement ou de divulgation (par exemple les responsables du contrôle interne, les responsables de la santé et de la sécurité, les administrateurs d'entreprises et les responsables de la protection de l'enfance);
- Codes de conduite: règles de conduite et d'intégrité et règles relatives au signalement des violations de ces règles;
- Politiques et procédures disciplinaires, en particulier en ce qui concerne les infractions (administratives) que constituent les manquements à l'obligation de confidentialité et les actes de diffamation;
- Autres politiques ou règles organisationnelles, notamment l'application des lois relatives à la protection des données, des codes de conduite et d'éthique, des codes disciplinaires, des politiques relatives aux communications dans les médias et règles applicables aux publications.

Les consultations nationales pourraient également contribuer à déterminer les voies de signalement, notamment celles que la population considère comme les plus fiables. Un examen détaillé de ces voies de signalement, pour comprendre comment l'information et la personne qui la communique sont prises en charge, peut être très instructif. On peut citer à titre d'exemples les organismes nationaux d'audit ou d'autres organismes de contrôle indépendants, y compris les médiateurs et les commissaires chargés des questions de respect de la vie privée ou d'information, les organes chargés de l'intégrité professionnelle (comme les commissions chargées de la déontologie judiciaire ou de la fonction publique), les organes de contrôle de la police ou les organismes de contrôle sectoriels (comme les autorités de l'aviation civile).

Dans certains pays, la transparence dans les affaires publiques repose sur une base constitutionnelle ou juridique solide et les obstacles pour parler ouvertement de questions diverses, y compris les irrégularités et les fraudes, sont moins nombreux. De tels contextes laissent généralement moins de place à la réprobation sociale et aux problèmes liés à la divulgation — aux autorités ou au public — d'informations relatives à des irrégularités, ou d'autres questions d'intérêt général. Si des réformes peuvent encore être nécessaires dans ces pays pour renforcer la capacité des personnes de parler ouvertement de problèmes spécifiques, il sera probablement plus simple d'en définir le détail et l'objectif.

Partout dans le monde, les traditions culturelles, juridiques et religieuses reconnaissent également, dans une certaine mesure, l'importance des révélations faites par certaines personnes pour protéger les intérêts d'autres personnes. Par exemple, certains aspects du droit islamique qui soulignent le rôle des témoins pourraient permettre aux "lanceurs d'alerte d'être considérés comme des témoins de la vérité[30]". Au Royaume-Uni, la loi relative à la protection des divulgations d'intérêt général a consacré et modernisé un principe de *common law* datant de 1743, selon lequel "le sceau de la confidence ne

[30]Vaughn, R., *The Successes and Failures of Whistleblower Laws*, Edward Elgar Publishing, États-Unis d'Amérique, 2012, p. 261.

saurait être invoqué en ce qui concerne la divulgation d'une injustice[31]". Ce principe a permis de reconnaître que, lorsqu'un employé apprend que son employeur participe — ou prévoit de participer — à une fraude, il n'est plus lié par l'obligation contractuelle de confidentialité et a le droit de révéler ce qu'il a appris. Aux États-Unis, le *Whistleblower Protection Act* (loi sur la protection des lanceurs d'alerte) est fondé sur le principe d'une liberté publique d'expression qui justifie le droit de faire des révélations protégées. Il est important de dégager ces principes afin de mettre en place un système national viable, sans porter atteinte aux bonnes pratiques existantes.

2. Besoins et lacunes

Au Japon, un certain nombre de scandales ont convaincu les législateurs qu'il était nécessaire de renforcer la protection des lanceurs d'alerte. Parmi ces scandales figuraient le cas de centaines de patients souffrant d'hémophilie contaminés par le VIH/sida dans les années 90, en raison de l'utilisation de sang contaminé lors de transfusions, alors que les agents publics étaient au courant des faits; le refus par Mitsubishi Motors de rappeler tous les véhicules d'un même modèle malgré les plaintes émises par 64 000 clients, l'entreprise ayant préféré occulter le problème en réparant les voitures au cas par cas; et la dissimulation par l'entreprise Tokyo Electric Power Company de dommages causés dans certaines de ses centrales nucléaires en 2003[32].

Un examen détaillé de ces affaires peut permettre d'obtenir des informations essentielles pour déterminer pourquoi les mécanismes de responsabilité ont failli, et connaître les risques et les difficultés rencontrées par ceux qui étaient en mesure ou auraient pu être en mesure de signaler le danger aux autorités ou au public.

Exemple: Tribunal d'enquête (Irlande)

En 2012, en Irlande, le Tribunal Mahon a rendu compte de son enquête sur des versements de pots-de-vin à des hommes politiques dans le cadre de décisions politiques relatives à des permis de construire et des modifications de plans d'urbanisme dans les années 90. Beaucoup ont estimé que ce scandale, ainsi que la faillite des banques irlandaises en 2008, auraient pu être évités si des informations relatives à des irrégularités potentielles avaient été communiquées suffisamment tôt, et si les personnes à l'origine de ces informations avaient bénéficié d'une protection efficace. Cette enquête a été l'enquête publique la plus longue de l'histoire irlandaise en matière de corruption et a exigé la collecte de nombreux éléments de preuve.

Parmi les multiples recommandations issues de l'enquête, un certain nombre visait spécifiquement le renforcement de la protection des lanceurs d'alerte:

a) En mettant en œuvre une loi prévoyant la protection de tous les employés de tous les secteurs qui signalent des infractions et des manquements présumés à des mesures réglementaires, contre toute forme de responsabilité, demande en réparation ou sanction pénale découlant du signalement;

b) En étendant la protection prévue par la version modifiée du *Prevention of Corruption Act* de 2001 (loi relative à la prévention de la corruption) aux entrepreneurs indépendants qui signalent des soupçons de corruption;

[31] Affaire *Gartside* c. *Outram*, 1856, 26 L.J.Ch.113. Il est intéressant de noter que ce principe avait déjà été énoncé en 1743 dans l'affaire *Annesly* c. *the Earl of Anglesea*, 17 State Tr 1139 (L.R. 5 Q.B. 317 n.), dans le cadre de laquelle il a été déclaré qu'"aucune obligation privée ne peut dispenser de l'obligation universelle qui incombe à chaque membre de la société de dévoiler toute intention contraire aux lois de la société et visant à détruire le bien-être public".

[32] Vaughn, R., *The Successes and Failures of Whistleblower Laws*, Edward Elgar Publishing, États-Unis, 2012, p. 243.

c) En supprimant le montant maximum de l'indemnisation qui peut être accordée aux personnes sanctionnées pour avoir lancé une alerte; et

d) En modifiant le *Criminal Justice Act* de 2011 (loi relative à la justice pénale) pour couvrir les personnes qui communiquent des informations ou fournissent des éléments de preuve concernant des infractions visées par le *Public Bodies Corrupt Practices Act* de 1889 (loi relative aux pratiques frauduleuses des organismes publics).

Source: Voir en particulier Tribunal of Inquiry into Certain Planning Matters and Payments (Tribunal Mahon), rapport final et recommandations, recommandations 7 et 8, 2012, p. 2645, disponibles à l'adresse: http://www.planningtribunal.ie/images/finalReport.pdf.

Il peut être très utile d'analyser les affaires pénales concernant des actes de corruption ou d'autres actes illicites graves, que les poursuites aient abouti ou non à une condamnation, afin d'établir les bases d'une réforme. Les affaires peuvent être analysées pour déterminer si, dans quelle mesure et à quel stade, la personne qui a communiqué des informations a joué un rôle; quelles garanties, le cas échéant, ont été offertes ou demandées; et dans quelle mesure la coopération de la personne était nécessaire à l'issue de l'affaire. De plus amples recherches sont nécessaires pour évaluer les retombées des systèmes d'alerte. Le nombre croissant de lois, de modèles institutionnels et de textes de jurisprudence devrait fournir une bonne base pour de futures recherches.

3. Sensibilisation et confiance

Si la sensibilisation est importante, il est essentiel que les personnes qui communiquent des informations soient traitées avec tact et de façon appropriée, et que les informations qu'elles communiquent soient gérées avec professionnalisme. Cela permettra d'instaurer une confiance à long terme dans les mesures mises en œuvre par les États.

La décision d'un État de mettre en place ou non une nouvelle institution ou un nouveau système pour traiter les signalements de cas de corruption dépendra du résultat de l'évaluation nationale. De toute évidence, si le système judiciaire, les services de poursuite, les organes législatifs ou les services de police du pays concerné sont affaiblis, inefficaces ou compromis, ou si la méfiance est grande à l'égard des institutions publiques en général, un organe indépendant à l'abri de toute pression est une possibilité. Toutefois, s'il peut être nécessaire d'imaginer d'autres moyens d'aborder la protection des personnes qui communiquent des informations de manière efficace et à court terme, il est important de ne pas négliger le fait que, à long terme, les systèmes juridiques traditionnels (à savoir des services de police performants, des services de poursuite indépendants et un pouvoir judiciaire impartial) pourraient devenir plus efficaces.

Indépendamment des mesures prises, l'expérience montre qu'en adoptant des pratiques efficaces et proactives et en intégrant dans le système l'obligation de rendre des comptes au public, on gagne la confiance des citoyens. Le Pérou a pris un certain nombre de mesures pour combattre activement la criminalité organisée et la corruption, et les mesures les plus récentes visant à protéger les personnes qui communiquent des informations offrent une étude de cas intéressante.

Exemple: Sistema Nacional de Atención de Denuncias (Pérou)

Le Pérou a adopté une nouvelle Constitution en 1993, après une période de troubles civils et de violence dans les années 80 et au début des années 90, qui a coûté la vie à environ 70 000 personnes. À la fin des années 90, un scandale concernant un réseau de

corruption au sein du service national des douanes, impliquant notamment des agents publics haut placés, a ébranlé le Gouvernement. Sept ministres ont démissionné à la suite d'une enquête menée sur les allégations de corruption. En 2001, le Pérou a centré ses efforts sur un certain nombre de mesures importantes en vue de la consolidation de la démocratie et de la lutte contre la corruption, et a notamment adopté une nouvelle loi relative à la transparence et à l'accès à l'information et renforcé son système de justice pénale. Les réformes ont essentiellement porté sur des programmes de protection des témoins pour encourager les personnes impliquées dans des affaires de corruption et de criminalité organisée à coopérer avec les autorités. Même si ces efforts ont permis de réduire le nombre d'infractions graves, des études menées au début des années 2000 ont montré que 7 Péruviens sur 10 manifestaient un niveau de tolérance élevé ou moyen à l'égard des actes de corruption et que 86 % de la population estimaient qu'il était inutile de signaler des cas de corruption. Les enquêtes ont également révélé le peu de confiance que le public accordait au pouvoir judiciaire, au Congrès et à la police.

En 2010, le Pérou a adopté la loi sur la protection des lanceurs d'alerte. La loi prévoit une protection contre les licenciements ou les blâmes pour les lanceurs d'alerte dans le secteur public, l'anonymat pour les personnes qui signalent des actes de corruption, et une indemnisation dont le montant correspond à un pourcentage des amendes imposées aux personnes reconnues coupables à la suite d'un signalement.

L'auditeur national, à savoir la Contraloría General de la República (Bureau du Contrôleur général de la République), est chargé de gérer les signalements faits conformément à la loi. Il dispose de 23 succursales régionales et de 800 bureaux de contrôle interne répartis au sein d'importantes institutions publiques sur tout le territoire; 824 services sont ainsi en mesure de recevoir des signalements de corruption. Afin de coordonner et de consolider la réception et le traitement des signalements, le Bureau du Contrôleur général a instauré le Sistema Nacional de Atención de Denuncias (SINAD) (système national de traitement des dénonciations) pour offrir une voie de signalement sûre et un système de traitement centralisé.

Trois ans ont été nécessaires pour mettre en place le système, les procédures et la technologie appropriés. Un élément clé du système est la garantie de l'anonymat grâce à un dispositif codé qui empêche les analystes d'identifier la source de l'information.

Le processus du SINAD comprend les étapes suivantes:

1. Réception d'un signalement ou d'une plainte (la technologie permet à la personne qui communique les informations de conserver l'anonymat, tout en engageant une communication à double sens);
2. Évaluation du signalement (déterminer s'il répond aux critères de recevabilité);
3. Articulation de l'affaire (regrouper les renseignements);
4. Préparation pour les vérifications (déterminer les sites à visiter, les documents, les témoins);
5. Vérification et rapport (travail sur le terrain et conclusions);
6. Présenter les conclusions aux lanceurs d'alerte/personnes ayant communiqué les informations.

Une des principales difficultés de l'application des mesures de protection prévues par la loi réside dans la coordination nécessaire entre les différents organes (par exemple les autorités du travail chargées d'enquêter sur les représailles et les autorités fiscales chargées de recouvrer les amendes), et l'interaction entre ce système administratif de signalement des cas de corruption et le droit pénal.

Source: Présentation faite par Fernando Ortega Cadillo, Directeur du Département de la prévention de la corruption, lors de la réunion du groupe d'experts internationaux sur la protection des personnes qui communiquent des informations, organisée à Vienne les 22 et 23 mai 2014.

II.

Faciliter les signalements et protéger les personnes qui communiquent des informations

La meilleure façon de faciliter les signalements dépendra de la nature du groupe cible, de la nature des informations que les personnes concernées sont en mesure de communiquer et des risques auxquels elles peuvent être exposées si elles communiquent ces informations. Différents types de protection (procédurale, physique, préventive ou rétroactive) doivent être envisagés selon les circonstances.

Une évaluation nationale, telle que décrite au chapitre premier, devrait aider les États parties à déterminer les mesures déjà existantes ainsi que les faiblesses ou les lacunes dans leur système national. La loi devrait permettre aux autorités d'avoir recours à des mesures de protection préventives, comme la garantie de l'anonymat pour éviter toutes représailles en premier lieu. De plus, la loi devrait prévoir des voies de droit efficaces pour les personnes qui sont soumises à un traitement injuste ou subissent des représailles lorsque, par exemple, les mesures préventives ont échoué.

Il appartient aux autorités d'expliquer au public la valeur et l'importance de sa participation au système, ainsi que l'assistance et la protection dont il peut bénéficier. Le gouvernement doit être en mesure d'expliquer en quoi une plus grande participation du public à la lutte contre la corruption permettra de réduire sensiblement les risques encourus par toute personne qui communique des informations. L'objectif doit être d'alléger le plus possible le poids du risque qui repose sur les épaules de chaque personne qui communique des informations.

Le présent chapitre expose une gamme de mesures qui ont été mises en œuvre dans différents pays pour faciliter les signalements et protéger les personnes qui communiquent des informations. Le chapitre est divisé en plusieurs grands volets qui sont décrits plus en détail ci-dessous:

A. Contenu et portée des informations
B. Voies de signalement
C. Protection contre les traitements injustifiés
D. Facilitation des signalements
E. Traitement des signalements
F. Conseils

Nombre de réformes et de mécanismes de signalement qui ont été mis en œuvre dans différents pays sont encore relativement récents et tous leurs effets n'ont pas encore été évalués. Le présent chapitre décrit certaines des nouvelles tendances, mais ne constitue pas un examen exhaustif de tous les éléments dont il faudrait tenir compte pour assurer la protection des personnes qui communiquent des informations. Il devrait néanmoins en fournir un bon aperçu aux États parties et leur permettre de disposer d'une base solide pour déterminer les mesures possibles et nécessaires.

Il est également conseillé aux États de mener leurs propres recherches en vue de l'élaboration et de l'amélioration des politiques. La liste des ressources présentée à la fin du Guide peut être utile à cet égard et intéresser toute personne qui étudie plus généralement le signalement de cas de corruption ou le lancement d'alertes.

A. Actes illicites susceptibles d'être signalés: contenu et portée des informations

Au niveau international, la portée des informations pour lesquelles les personnes seront protégées est de plus en plus souvent élargie à tout acte illicite ou toute atteinte potentielle à l'intérêt général. Si la terminologie employée peut varier, il est essentiel d'arrêter une définition large afin de couvrir le plus grand nombre possible de types d'actes répréhensibles.

Si le terme "intérêt général" est plus courant dans certains pays que dans d'autres, il s'entend généralement du "bien-être" du public[33]. Certains décideurs politiques parlent du "bien commun". Au Royaume-Uni, par exemple, la loi applicable est la loi sur les révélations d'intérêt général (*Public Interest Disclosure Act*) et non la loi relative à la protection des lanceurs d'alerte. La protection de l'intérêt général est également un moyen efficace de faire comprendre les effets préjudiciables de la corruption sur la société, et s'applique aux activités des entreprises privées tout comme à celles de l'État. Au sein d'une organisation, par exemple, une information permettant de détecter et de prévenir un acte de corruption peut porter sur tout élément qui compromet la mission de l'organisation envers le public, les parties prenantes, les investisseurs ou les clients.

Il est en outre plus facile de comprendre et de signaler une irrégularité ou un acte illicite lorsque ces derniers font l'objet d'une définition large. Les États parties qui s'intéressent avant tout aux informations strictement limitées aux infractions de corruption telles que définies par le droit pénal devraient tenir compte des deux points suivants. Premièrement, ils doivent comprendre qu'il peut être difficile pour les profanes de déceler correctement ce type d'informations. Il est fort probable qu'une personne donnée ne sera qu'un simple observateur ou témoin d'une partie du problème, c'est-à-dire des faits laissant supposer un acte de corruption. Plus la définition est restrictive, plus la personne qui communique des informations devra évaluer la qualité et la gravité de ces dernières avant de les transmettre, ce qui augmente également la probabilité qu'elle garde le silence — en particulier si elle n'est pas certaine de bénéficier d'une protection. Dans de telles circonstances, un avis indépendant et confidentiel revêt une extrême importance. Deuxièmement, plus la définition est étroite, moins les autorités compétentes — qui sont les autorités techniques — recevront d'informations et, par conséquent, moins elles auront la possibilité d'établir des faits susceptibles d'aboutir à des enquêtes et des poursuites fructueuses.

[33] Sur le plan juridique et politique, le concept d'"intérêt général" permet aux juges et aux décideurs d'examiner des intérêts en cause qui ne sont pas nécessairement représentés dans le cadre de l'affaire dont ils sont saisis. Cette flexibilité vise à répondre à des facteurs nouveaux ou différents qui influent sur l'intérêt général en fonction des circonstances propres à chaque situation.

Il n'en reste pas moins que le public ne connaîtra pas nécessairement toujours la définition de termes généraux comme "intérêt général". Il est donc logique d'énoncer les différents types d'actes illicites visés. Aux États-Unis, le *Whistleblower Protection Act* (loi sur la protection des lanceurs d'alerte), qui protège les personnes travaillant dans le secteur public fédéral régit, par exemple, les informations relatives à des erreurs graves de gestion, à un gaspillage de fonds flagrant, à un abus de pouvoir, ou à une menace grave et précise pour la santé ou la sécurité publiques. En Australie, le *Public Interest Disclosure Act* de 2013 (loi sur les révélations d'intérêt général) définit l'intérêt général en s'appuyant sur différents critères comme celui de savoir si la révélation permet de favoriser l'intégrité et la responsabilisation du secteur public ou de mettre au jour une incapacité à remédier à une irrégularité grave dans ce secteur.

En Malaisie, le *Whistleblower Protection Act* (loi sur la protection des lanceurs d'alerte) de 2010[34] n'emploie pas le terme "intérêt général" ou "irrégularité", mais renvoie à un large éventail d'informations qui peuvent être considérées comme des révélations protégées conformément à la loi. Cette loi parle de comportement répréhensible, qui s'entend de "tout comportement qui, une fois prouvé, constitue une infraction disciplinaire ou pénale", et une infraction disciplinaire s'entend de "tout acte ou toute omission qui constitue un manquement à la discipline dans un organisme public ou privé, tel que défini par la loi, un code de conduite, un code d'éthique, une circulaire ou un contrat de travail, selon le cas". Selon l'article 6-2, "un comportement répréhensible visé au paragraphe 1 peut également être signalé:

a) Même si la personne qui est à l'origine du signalement n'est pas en mesure d'identifier une personne à laquelle se rapporte la révélation;

b) Même si le comportement répréhensible s'est produit avant l'entrée en vigueur de la présente loi;

c) Par des informations obtenues alors que la personne était employée dans un organisme public ou un organisme privé; ou

d) Si l'auteur du comportement répréhensible est une personne qui, au moment des faits, était employée dans un organisme public ou un organisme privé".

Dans le cadre de la corruption, les infractions pénales sont souvent assorties d'autres types d'irrégularités ou d'actes illicites, et le fait d'en élargir la portée augmente les chances de les détecter et de les combattre. Aux termes du *Guide technique de la Convention des Nations Unies contre la corruption*:

> [L'article 33] s'applique aux personnes qui peuvent posséder des informations qui ne sont pas suffisamment détaillées pour constituer des éléments de preuve au sens juridique du terme. Ces informations sont généralement disponibles aux premiers stades d'une affaire et peuvent également constituer un indice d'irrégularité. Du fait de la complexité des affaires de corruption, ces indices se sont avérés utiles pour alerter les autorités compétentes et leur permettre de décider s'il y a lieu ou non d'ouvrir une enquête[35].

L'article 33, qui porte sur la protection de toute personne qui communique des informations, devrait ainsi être considéré comme un complément de l'article 32, qui vise les témoins, les victimes et les experts qui déposent concernant des infractions de corruption.

[34] https://www.bheuu.gov.my/portal/pdf/Akta/Act%20711.pdf.

[35] *Guide technique de la Convention des Nations Unies contre la corruption*, p. 119.

Compte tenu des recoupements potentiels entre les informations et les éléments de preuve, et de l'évolution d'une affaire à mesure que l'enquête progresse (par exemple, il se peut qu'une personne soit appelée ou non à témoigner lors d'un procès selon que des éléments de preuve nouveaux ou plus pertinents ont été découverts ou non), le *Guide législatif pour l'application de la Convention des Nations Unies contre la corruption* (ci-après dénommé "le Guide législatif") indique que les États parties pourraient souhaiter donner une interprétation large à l'article 32 et devraient s'efforcer de rendre cette disposition applicable à toute personne, comme il convient et dans la limite de leurs moyens. Toute personne qui communique des informations pourrait ainsi être visée (pour plus de détails sur cette question, voir chapitre II, sections C. 8 et C. 9).

> L'expérience des États qui disposent de programmes de protection des témoins montre qu'il sera nécessaire d'appliquer cette prescription de manière plus large en vue d'assurer une protection suffisante aux témoins pour les inciter à coopérer aux enquêtes et aux poursuites. Outre les témoins qui ont effectivement déposé, les programmes de protection devraient généralement s'appliquer: *a)* aux personnes qui coopèrent ou apportent leur concours aux enquêtes jusqu'à ce qu'il soit clair qu'elles ne seront pas appelées à témoigner; et *b)* aux personnes qui fournissent des renseignements utiles, lesquels ne seront cependant pas requis en tant que témoignage ni utilisés au tribunal en raison de craintes pour la sécurité de l'informateur ou d'autres personnes. Les législateurs souhaiteront donc peut-être rendre les dispositions applicables à toute personne qui a ou qui pourrait avoir des renseignements qui sont ou peuvent être utiles pour l'enquête ou les poursuites concernant une infraction de corruption, que ces renseignements soient ou non produits à titre de preuve[36].

Compte tenu de la complexité des enquêtes sur la corruption et du risque que les affaires comportent des éléments transnationaux, les États parties devraient également déterminer dans quelle mesure la loi peut faciliter la communication d'informations relatives à la corruption sans en limiter excessivement la portée par des critères de temps ou d'espace, ou sans ériger d'autres obstacles inutiles ou arbitraires qui entraveraient la communication en raison du contexte ou d'une formalité[37].

Exemple: Conseil de l'Europe, directives internationales relatives à l'intérêt général

La Recommandation sur la protection des lanceurs d'alerte (adoptée en avril 2014) reconnaît qu'il existe, dans de nombreux domaines, un terrain d'entente entre la plupart des États membres pour ce qui relève de l'intérêt général, mais que l'appréciation de ce dernier peut varier dans d'autres domaines. Le principe 2 indique que le champ d'application des informations donnant droit à une protection devrait inclure les violations de la loi et des droits de l'homme, ainsi que les risques pour la santé et la sécurité publiques et pour l'environnement. L'Exposé des motifs fournit une liste non exhaustive de questions habituellement considérées comme relevant des catégories d'informations pour lesquelles les lanceurs d'alerte devraient bénéficier d'une protection:

- La corruption et les activités criminelles;
- Les violations de la loi et de la réglementation administrative;
- Les abus de pouvoir ou de charge publique;
- Les risques pour la santé, les normes alimentaires et la sécurité publiques;
- Les risques pour l'environnement;

[36] *Guide législatif pour l'application de la Convention des Nations Unies contre la corruption*, par. 442 et 443.

[37] Par exemple, au Royaume-Uni, le *Public Interest Disclosure Act* est rédigé de façon à garantir que les informations donnant droit à une protection ne sont pas limitées dans le temps — elles peuvent porter sur des violations ou risques de préjudice passés, présents ou futurs — ni dans l'espace, la loi indiquant qu'il est "sans importance de savoir si la défaillance s'est produite, se produit ou se produira au Royaume-Uni ou ailleurs" (art. 43 B).

- Les erreurs graves de gestion de la part d'organes publics (y compris les associations caritatives);
- Le gaspillage flagrant des fonds publics (y compris ceux d'associations caritatives);
- La dissimulation de l'un de ces actes.

Source: Conseil de l'Europe, Recommandation sur la protection des lanceurs d'alerte, Exposé des motifs, 2014, par. 43, disponible à l'adresse: https://wcd.coe.int/ViewDoc.jsp?id=2188939&Site=CM.

1. Bonne foi et soupçons raisonnables pour communiquer des informations

L'article 33 de la Convention contre la corruption indique que la protection contre tout traitement injustifié devrait être envisagée pour toute personne qui signale des faits aux autorités compétentes, de bonne foi et sur la base de soupçons raisonnables. Partant, si une personne a des motifs raisonnables de croire que les informations indiquent une irrégularité ou une fraude, et qu'il était également raisonnable pour une personne dans sa position de le croire en fonction des informations disponibles, cette personne doit être protégée. Dans de telles circonstances, même si une personne se trompe quant au sens des informations qu'elle a communiquées et qu'aucune corruption ou aucun acte illicite n'est établi, elle doit tout de même bénéficier d'une protection du fait d'avoir communiqué des informations. En revanche, si une personne communique des informations en sachant qu'elles sont fausses, des garanties doivent être mises en place afin que cette personne ne soit pas en mesure de demander une protection légale et qu'elle puisse être sanctionnée en cas de préjudice.

Des approches différentes ont été adoptées concernant le concept de bonne foi et son interprétation. Un certain nombre de pays ont exprimé des craintes quant au risque d'attacher trop d'importance à la bonne foi ou de la confondre avec la "motivation". Si les personnes pensent que la priorité sera donnée à leur motivation et non à l'évaluation même du bien-fondé des informations qu'elles pourraient communiquer de bonne foi, elles risquent purement et simplement de s'abstenir de parler. Compte tenu de ce risque, le Conseil de l'Europe n'a pas inclus la bonne foi dans ses recommandations[38].

Certains États parties ont également précisé ce point dans leur législation nationale. En droit norvégien, par exemple, la mauvaise foi n'exclut pas la légalité des signalements. La loi norvégienne reconnaît que l'intérêt général est respecté si un employé signale des soupçons raisonnables, même si sa motivation personnelle est malveillante. En d'autres termes, les informations pourraient être nécessaires et utiles pour découvrir la corruption, et la motivation de la personne qui communique les informations n'y change rien (par exemple, si une personne communique des informations concernant une autre personne sur la base de soupçons raisonnables, il importe peu de savoir si ces deux personnes entretiennent de bonnes ou de mauvaises relations de travail). Cette approche maintient l'exigence de soupçons raisonnables et peut donc exclure la protection d'une personne qui communique sciemment de fausses informations ou qui aurait dû raisonnablement savoir que les informations étaient fausses.

[38]Le Conseil de l'Europe indique que le terme "bonne foi" n'a pas été employé dans la Recommandation sur la protection des lanceurs d'alerte de "façon [à exclure] que la motivation du lanceur d'alerte pour avoir fait le signalement ou la révélation d'informations, ou sa bonne foi ce faisant, puisse présenter une pertinence au moment de décider si le lanceur d'alerte doit être protégé ou pas" (Exposé des motifs, par. 85). Voir la Recommandation, principe 22: "[l]a personne ayant fait un signalement ou ayant révélé des informations ne devrait pas perdre le bénéfice de sa protection au seul motif qu'elle a commis une erreur d'appréciation des faits ou que la menace perçue pour l'intérêt général ne s'est pas matérialisée, à condition qu'elle ait eu des motifs raisonnables de croire en sa véracité".

En 2013, le Royaume-Uni a supprimé le terme "bonne foi" des dispositions de la loi visant à déterminer si une révélation donne droit à une protection, mais a conservé ce critère pour fixer l'indemnisation ou le remboursement. Si la mauvaise foi est établie, l'indemnisation pour une personne soumise à un traitement injuste après avoir communiqué des informations peut être réduite de 25 % au maximum si la réduction est jugée juste et équitable compte tenu de toutes les autres circonstances[39].

Veiller à ce que la bonne foi ne soit pas confondue avec la motivation peut également permettre d'empêcher des situations dans lesquelles des personnes préfèrent jouer aux détectives amateurs plutôt que de signaler les faits tels qu'elles les comprennent. Sans cela, la personne qui communique des informations peut craindre qu'un signalement "prématuré" soit interprété comme une preuve de mauvaise foi.

Le risque pourrait également être réduit au minimum si l'on définit la bonne foi comme renvoyant au concept d'"honnêteté" ou de "*bona fide*" en rapport avec les informations elles-mêmes, et donc en associant la bonne foi aux informations et non à la motivation personnelle de la personne qui les communique. Tout en conservant la notion de bonne foi, un certain nombre de lois adoptées ces dernières années mettent l'accent sur la qualité des informations communiquées par les lanceurs d'alerte, sans mentionner la motivation, ni préciser ou limiter la question de la motivation:

- En Bosnie-Herzégovine, la loi de 2013 sur la protection des lanceurs d'alerte dans les institutions publiques définit la bonne foi comme "le point de vue du lanceur d'alerte fondé sur des faits et des circonstances que le lanceur d'alerte estime vrais d'après ses propres connaissances".
- En Zambie, le *Public Interest Disclosure Act* de 2010 (loi sur les révélations d'intérêt général) dispose à l'article 22 qu'une révélation protégée est faite de bonne foi par un employé "qui croit raisonnablement que les informations communiquées, et toutes les allégations qui y figurent, sont foncièrement vraies; et qui ne communique pas les informations à des fins personnelles autres que toute récompense qui pourrait lui être versée conformément à la loi".

La Loi type de l'Organisation des États américains (OEA) visant à protéger les lanceurs d'alerte et les témoins qui signalent des actes de corruption adopte une autre approche concernant la bonne foi. La loi prévoit une présomption de bonne foi jusqu'à preuve du contraire[40]. La loi roumaine sur la protection des agents publics qui portent plainte pour violations de la loi est articulée autour de la même présomption. Lorsqu'ils rédigent des lois visant à protéger les personnes qui communiquent des informations, les États parties devraient garder à l'esprit ces différentes approches et opinions concernant la notion de "bonne foi".

2. Droits d'autrui et obligations envers les tiers

La révélation d'actes présumés de corruption ou de fraude protège les intérêts de la société en contribuant à faire en sorte que les informations soient communiquées aux bonnes personnes au bon moment et, si possible, suffisamment tôt pour pouvoir agir avant que des dommages ne soient causés. Il devrait donc y avoir peu de restrictions concernant les faits révélés ou le moment choisi pour les révéler. Les restrictions

[39] Royaume-Uni, *Enterprise and Regulatory Reform Act* (ERRA) de 2013 (loi sur les entreprises et la réforme réglementaire) portant modification du *Public Interest Disclosure Act* (loi sur les révélations d'intérêt général) de 1998 et du *Employment Rights Act* de1996 (loi sur les droits en matière d'emploi).

[40] Organisation des États américains (OEA), Model Law to Facilitate and Encourage the Reporting of Acts of Corruption and to Protect Whistleblowers and Witnesses (Loi type visant à faciliter et encourager le signalement des actes de corruption et à protéger les lanceurs d'alerte et les témoins), 2013, article 2 *h*.

devraient être clairement définies et fondées sur un objectif légitime, nécessaire et adapté aux circonstances. Il s'agit d'un principe général souligné à l'article 13 de la Convention contre la corruption[41].

Lorsque les informations sont communiquées aux autorités compétentes, l'obligation de protéger les intérêts d'autrui auxquels la révélation pourrait porter atteinte (s'agissant, par exemple, de données personnelles) incombe automatiquement auxdites autorités. Toutefois, dans les rares cas où les voies de signalement indiquées ont été testées, sont inutilisables, ou sont elles-mêmes corrompues d'une façon ou d'une autre, et où une voie de signalement plus large est utilisée (par exemple, par l'intermédiaire des médias), la personne qui communique les informations doit veiller avec soin à ce que les intérêts des tiers soient protégés. Ce principe s'applique, par exemple, aux informations médicales privées des patients, aux données de clients juridiques ou, bien entendu, aux données personnelles des clients.

La gravité d'une violation des droits des tiers sera vraisemblablement un des facteurs qu'un tribunal prendra en considération pour déterminer si une révélation publique d'informations par un agent public ou un employé du secteur privé est justifiée et raisonnable (voir le chapitre II, section B.3 sur l'utilisation de voies de signalement plus larges et sur l'obligation de rendre des comptes au public).

C'est l'une des raisons pour lesquelles il est important que les personnes aient accès aux informations et à des conseils impartiaux. Des conseils fournis à un stade précoce permettront de s'assurer que les personnes communiquent des informations de la manière la plus appropriée, afin que le problème soit traité et que, parallèlement, les risques encourus par ces personnes ou par tout autre tiers innocent soient limités.

Il est également important que les personnes soient en mesure de se défendre elles-mêmes contre de fausses allégations formulées dans le domaine public. À titre d'exemple, au Japon, le *Whistleblower Protection Act* (loi sur la protection des lanceurs d'alerte) contient une disposition selon laquelle des efforts doivent être déployés pour ne pas nuire aux intérêts légitimes d'autrui[42]. Une telle disposition peut être un moyen de se prémunir contre les révélations irresponsables, comme la publication de renseignements personnels qui porteraient atteinte à la réputation d'autrui et aux personnes qui doivent bénéficier de la présomption d'innocence. La publication de renseignements personnels ne devrait pas être nécessaire pour traiter une affaire.

Loyauté envers l'employeur

Dans de nombreux pays, et en particulier en ce qui concerne le secteur privé, les employés sont soumis à un devoir de loyauté ou de confidentialité s'agissant des informations techniques ou opérationnelles, ce qui signifie que la communication de telles informations à l'extérieur de l'organisation est souvent constitutive d'une infraction disciplinaire. La réputation commerciale est également très importante. De nombreux employés sont donc soumis à des obligations contractuelles strictes en la matière.

Par conséquent, il est important — surtout lorsqu'il s'agit de communiquer des informations aux autorités compétentes, ou au besoin de révéler des informations dans un cadre plus large — que la loi supprime ou dissipe tout doute en disposant que le signalement d'un acte illicite ou d'une atteinte à l'intérêt général l'emporte sur ces obligations envers l'employeur.

[41] Voir *Informer sur la corruption — Un outil de référence pour les gouvernements et les journalistes*, p. 42 et suiv., disponible à l'adresse: http://www.unodc.org/documents/corruption/Publications/2015/15-00373_Ebook.pdf.

[42] Japon, *Whistleblower Protection Act*, 2004, art. 8.

3. Sécurité nationale

En principe, toutes les informations gouvernementales devraient être accessibles et consultables par le public aux fins d'examen, dans la mesure où cela permet une participation démocratique et l'élaboration de politiques publiques rationnelles, même dans des domaines sensibles comme la sécurité nationale. S'il existe des raisons valables de protéger certaines informations relatives à l'ordre public ou à la sécurité nationale, comme le prévoient également certaines normes internationales, notamment l'alinéa *d* du paragraphe 1 de l'article 13 de la Convention contre la corruption, il faut veiller à ce que cette exception à l'accès aux informations n'ait pas une portée excessivement large au point d'empêcher le public d'examiner attentivement les décisions et l'action des pouvoirs publics et d'en débattre et, pire encore dans ce contexte, au point de rendre plus difficile la détection des actes de corruption au sein des services publics[43].

> L'ancien commissaire kényan chargé de la lutte contre la corruption, John Githongo, a déclaré ce qui suit: "[d]ans de nombreux pays africains, les cas les plus graves de corruption surviennent sous le couvert de ce que l'on appelle la sécurité nationale [...]. La corruption ayant été progressivement éliminée des procédures de passation des marchés publics — par exemple les routes et les grands projets d'infrastructure —, le dernier petit espace dans lequel la corruption se cache est le domaine dit de la "sécurité nationale", ce qui signifie que tout lanceur d'alerte qui commet un manquement dans ce domaine peut très facilement être accusé de trahison".
>
> *Source:* Entretien du mois — *Kenya's anti-corruption tsar*, Transparency Watch, avril 2006, cité dans Banisar, D., "Whistleblowing: International Standards And Developments", dans *Corruption and Transparency: Debating The Frontiers Between State, Market And Society*, World Bank-Institute For Social Research, UNAM, Irma E. Sandoval (dir. publ.), Washington, D. C., 2011, disponible à l'adresse: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1753180.

La recommandation du Conseil de l'Europe de 2014 reconnaît dans l'Exposé des motifs que les États membres peuvent avoir des raisons légitimes de vouloir appliquer un ensemble de restrictions en ce qui concerne les informations liées à la sécurité nationale, mais indique clairement que ces restrictions doivent être fondées sur les informations elles-mêmes et non sur les catégories de personnes concernées (comme les policiers ou le personnel militaire)[44].

La pratique internationale évolue en ce qui concerne la définition de la portée et des limites du pouvoir d'un État de s'abstenir de divulguer des informations pour des raisons de sécurité nationale, et les cas où il convient de sanctionner ceux qui révèlent sans autorisation des informations classifiées. Les principes fondamentaux imposent notamment de s'assurer que les motifs de classification sont appliqués de façon claire et restrictive (par exemple à des informations spécifiques qui protègent un intérêt légitime de sécurité nationale, et non à toutes les informations liées à un département ou à une agence), et que seules les autorités expressément chargées de protéger la sécurité nationale peuvent invoquer la non-communication d'informations pour ces motifs[45]. De plus, toute loi qui régit la divulgation d'informations jugées essentielles pour la sécurité nationale devrait être rendue publique[46]. Aux États-Unis, par exemple, la communication au public d'informations qui ne sont pas classifiées ne peut pas être soumise à des restrictions[47].

---

[43] Voir *Informer sur la corruption — Un outil de référence pour les gouvernements et les journalistes*, p. 27, disponible à l'adresse: http://www.unodc.org/documents/corruption/Publications/2015/15-00373_Ebook.pdf.

[44] Conseil de l'Europe, Recommandation sur la protection des lanceurs d'alerte, Exposé des motifs, 2014, par. 46 et 47, disponible à l'adresse: https://wcd.coe.int/ViewDoc.jsp?id=2188939&Site=CM.

[45] Principes globaux sur la sécurité nationale et le droit à l'information (Principes de Tshwane), Principe 3, disponibles à l'adresse: http://www.opensocietyfoundations.org/fact-sheets/tshwane-principles-national-security-and-right-information-overview-15-points (pour une traduction française, voir: https://www.opensocietyfoundations.org/sites/default/files/tshwane-french-20150209_0.pdf).

[46] Résolution 1551 de l'Assemblée parlementaire du Conseil de l'Europe, 2007.

[47] Le *Whistleblower Protection Act* des États-Unis (loi sur la protection des lanceurs d'alerte) prévoit que les divulgations au public ne peuvent être restreintes en cas d'informations non classifiées (5 USC 2302(b)(13). La disposition applique la définition du *National Security Act* (loi sur la sécurité nationale) selon laquelle les informations classifiées s'entendent des "informations ou documents désignés et clairement marqués ou mentionnés [...] comme devant bénéficier d'un degré spécial de protection contre toute révélation non autorisée pour des raisons de sécurité nationale" (50 USC 426).

Enfin, la révélation par le personnel du secteur public d'informations — classifiées ou non — qui montrent des actes illicites ou relèvent d'un intérêt général important doit être considérée comme "protégée", et il devrait exister des voies efficaces pour que les personnes disposant de telles informations puissent les communiquer en interne et à des organes indépendants du secteur de la sécurité nationale, qui soient impartiaux et soient dotés des pouvoirs et mandats nécessaires pour enquêter sur les allégations et protéger les témoins[48]. Les personnes devraient également disposer du droit de se défendre, au nom de l'intérêt général, pour avoir procédé à une révélation non autorisée.

Exemple: Principes globaux sur la sécurité nationale et le droit à l'information ("Principes de Tshwane")

Les Principes globaux sur la sécurité nationale et le droit à l'information ("Principes de Tshwane") ont été élaborés pour orienter ceux qui participent à la rédaction, la révision ou l'application de lois ou de dispositions relatives au pouvoir de l'État de ne pas divulguer des informations pour des raisons de sécurité nationale ou de sanctionner les personnes qui divulguent de telles informations. Ces principes ont été rédigés par 22 organisations et centres universitaires, en consultation avec plus de 500 experts provenant de plus de 70 pays, lors de 14 réunions organisées dans le monde entier, et sont fondés sur des lois, normes et bonnes pratiques internationales et nationales.

Les Principes de Tshwane présentent une approche proportionnée visant à faciliter le signalement de cas de corruption en interne pour les personnes dont le travail porte sur des informations sensibles, et la protection dont devraient bénéficier ceux qui signalent publiquement des actes illicites ou d'autres informations relevant de l'intérêt général (principes 39 à 46). Point important, les Principes de Tshwane prévoient une exception fondée sur l'intérêt général pour les fonctionnaires, qu'ils remplissent ou non les conditions pour bénéficier de la protection des lanceurs d'alerte telle qu'énoncée dans les Principes, si l'intérêt général à la divulgation l'emporte sur l'intérêt général au maintien de la confidentialité des informations.

Les Principes de Tshwane ont été adoptés par le Parlement européen à titre d'orientations en matière, d'une part, de transparence en tant qu'élément du contrôle démocratique dans le domaine du renseignement et, d'autre part, de protection des divulgations non autorisées d'informations relatives à la sécurité nationale[a]. Au paragraphe 89 des Conclusions principales, il est demandé aux États membres de "faire en sorte que leur législation, notamment dans le domaine de la sécurité nationale, prévoie une alternative sûre au silence pour divulguer ou signaler les actes répréhensibles, y compris la corruption, les infractions pénales, les violations d'obligations juridiques, les erreurs judiciaires et les abus d'autorité, ce qui est également conforme aux dispositions des différents instruments internationaux (Nations Unies et Conseil de l'Europe) de lutte contre la corruption, aux principes établis dans la résolution de l'Assemblée parlementaire du Conseil de l'Europe 1729 (2010), aux principes de Tshwane, etc.".

[a] http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0230&language=EN&ring=A7-2014-0139.

Source: Les Principes de Tshwane ont été traduits dans différentes langues. Ils peuvent être téléchargés en allemand, en arabe (pdf), en espagnol, en français, en japonais (pdf), en mandarin (pdf), en portugais et en serbe à l'adresse: http://www.right2info.org/exceptions-to-access/national-security/global-principles.

[48] Principes de Tshwane. Voir le Principe 39.

Le droit pénal danois prévoit une exception fondée sur l'intérêt général pour la publication de secrets d'État si la personne intervient "dans la défense légitime d'un intérêt général évident[49]", ce qui a été interprété comme signifiant que cet intérêt doit l'emporter sur l'intérêt à maintenir la confidentialité des informations[50]. Au Canada, conformément à la Loi sur la protection de l'information, un agent public commet une infraction s'il communique des renseignements opérationnels spéciaux sans autorisation, mais l'intérêt général peut être invoqué s'il divulgue des informations dans l'intérêt public[51].

B. Voies de signalement

Afin de reconnaître les différences entre les systèmes nationaux, la Convention contre la corruption parle d'autorités ou d'organes "compétents" (voir les articles 8, 13 et 33 de la Convention), laissant aux États parties suffisamment de latitude pour définir les modalités de création et de désignation des voies de signalement.

Lesdites modalités dépendront dans une large mesure des différentes autorités compétentes déjà en place et de leur efficacité, ainsi que de questions spécifiques ayant trait, par exemple, aux droits en matière de travail et d'emploi, ou des garanties constitutionnelles comme la liberté d'expression et la protection des médias.

Les États parties devraient également garder à l'esprit les différents scénarios possibles lorsqu'ils réformeront leurs lois ou élaboreront de nouvelles lois pour protéger les personnes communiquant des informations. Si une personne communique des informations en interne à son employeur et subit des représailles par la suite, est-elle protégée? La situation est-elle différente si la personne communique des informations à une autorité compétente comme un organisme de contrôle, une agence de lutte contre la corruption ou un service de détection et de répression? Et quelles circonstances exceptionnelles justifieraient la protection d'une personne qui communique des informations à l'extérieur, par exemple aux médias ou sur Internet? Il convient de répondre à ces questions tant pour les employés du secteur privé que pour ceux du secteur public et, dans une certaine mesure, pour d'autres personnes également. Les affaires internationales soulèvent d'autres questions, par exemple si l'employé d'une entreprise multinationale communique des informations aux autorités d'un autre État dans lequel l'entreprise est enregistrée ou mène des activités.

La manière la plus efficace de mettre en évidence les lacunes potentielles et d'étudier les mesures visant à renforcer le système est d'examiner les différents scénarios point par point. Certains États parties protègent la révélation d'informations aux autorités compétentes, mais négligent le fait que les employés peuvent également avoir besoin de protection lorsqu'ils communiquent des informations en interne et subissent des représailles. D'autres États parties disposent de lois applicables au secteur public, mais laissent le secteur privé dans une zone grise.

[49] Code pénal (Danemark), 2010, article 152 *e*.

[50] Amanda Jacobsen, *National Security and the Right to Information in Europe*, 2013, (enquête menée par l'Université de Copenhague, en collaboration avec l'Open Society Justice Initiative) p. 48 et 49, disponible à l'adresse: http://www.right2info.org/resources/publications/national-security-page/national-security-expert-papers/jacobsen_nat-sec-and-rti-in-europe.

[51] La Loi sur la protection de l'information du Canada prévoit une exception fondée sur l'intérêt général pour les personnes qui sont normalement astreintes au secret. La Loi prévoit que nul ne peut être déclaré coupable d'une infraction prévue aux articles 13 et 14 — à savoir lorsqu'une personne "astreinte au secret à perpétuité" communique ou confirme des "renseignements opérationnels spéciaux" intentionnellement et sans autorisation — si l'intéressé établit qu'il "a agi dans l'intérêt public". Cela signifie qu'une personne doit établir qu'elle a agi afin de révéler une infraction et que "les motifs de l'intérêt public en faveur de la révélation l'emportent sur ceux en faveur de la non-révélation".

Dans la plupart des pays, il existe différents responsables et autorités qui sont en mesure de recevoir les signalements de corruption ou d'autres types d'actes illicites. Il est impératif que ceux-ci soient non seulement "compétents" pour recevoir ces signalements, mais également habilités à y donner suite et tenus comptables de leur action. L'évaluation nationale devrait permettre d'identifier les acteurs concernés, ceux qui reçoivent la plupart des signalements, et de déterminer si leur réponse est efficace. Cette tâche est importante pour s'assurer que les nouvelles réformes ne portent pas atteinte à la bonne pratique déjà existante.

Arguments en faveur d'un régime de divulgation en plusieurs étapes ou à plusieurs niveaux

En Irlande et au Royaume-Uni, par exemple, il a été décidé d'adopter un système à trois niveaux pour protéger les lanceurs d'alerte en milieu professionnel dans le secteur public et dans le secteur privé: le premier niveau est le signalement interne à l'employeur ou à une autre personne conformément à la procédure autorisée par l'employeur; le deuxième est la communication d'informations à une personne autorisée ou au Ministre; et le troisième est la communication d'informations par des canaux plus larges (en externe). Conformément au système juridique et aux mécanismes de contrôle des deux pays, le signalement interne bénéficie de la protection la plus solide, ce qui signifie essentiellement qu'il sera plus facile de justifier le bien-fondé d'une protection en cas de présomptions. Ainsi, bien qu'elle n'exige pas la divulgation par voie interne en premier lieu, la loi est conçue de manière à exprimer une préférence pour cette forme de signalement, qui permettrait d'obtenir plus facilement la protection nécessaire. Dans les deux pays, les lanceurs d'alerte en milieu professionnel peuvent divulguer des informations aux médias dans des circonstances exceptionnelles, mais uniquement si des conditions précises sont réunies. Il faut notamment que la personne ait des motifs raisonnables de croire qu'elle subirait des représailles de la part de l'employeur si le problème était signalé en interne ou à une autorité compétente.

En 1996 et dans le cadre de la bonne gouvernance, le Committee of Standards in Public Life (comité de déontologie de la fonction publique) du Royaume-Uni[52], dont les travaux ont inspiré et influencé la pratique en matière de signalements au sein et au-delà du secteur public au Royaume-Uni, a fait observer que:

> Il est essentiel qu'un système d'alerte permette aux membres du personnel, d'une part, de contourner la hiérarchie directe, dans la mesure où cette hiérarchie peut fort bien être à l'origine de leurs soupçons et, d'autre part, de se tourner vers des personnes externes à l'organisation s'ils estiment que la direction dans son ensemble se livre à des actes répréhensibles[53].

L'Assemblée parlementaire du Conseil de l'Europe a affirmé qu'une personne devrait être protégée contre toute sanction pour avoir divulgué des informations au public "lorsqu'il n'existe pas de voies internes pour donner l'alerte, ou qu'elles ne fonctionnent pas correctement, voire qu'il ne serait pas raisonnable de s'attendre qu'elles fonctionnent

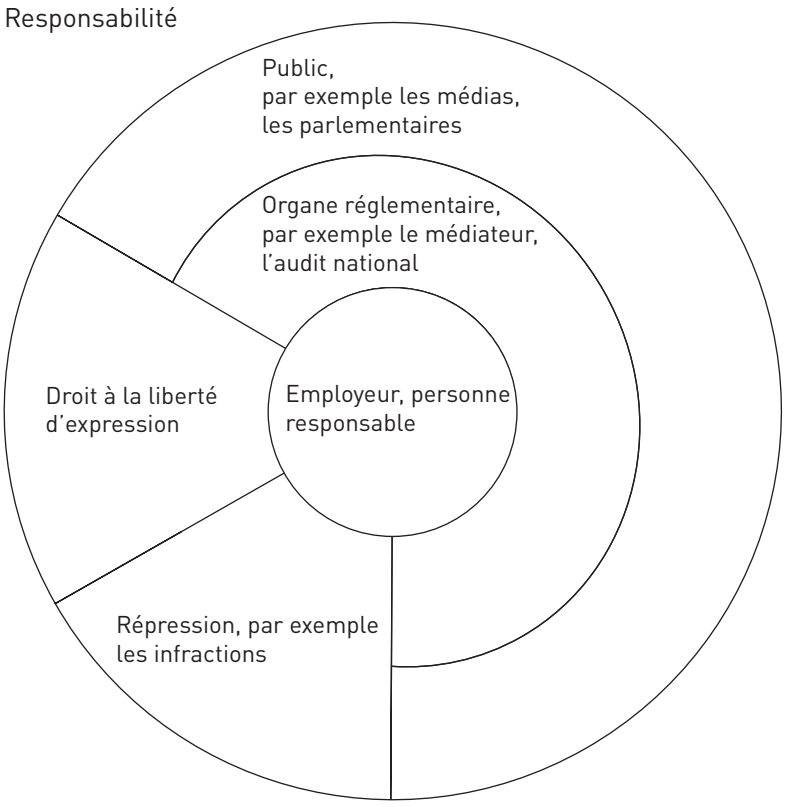
[52] Le Committee on Standards in Public Life du Royaume-Uni a été créé en 1994. Il ne s'agit pas d'un comité parlementaire, mais il fait rapport au Premier Ministre. Son mandat consiste à "examiner les problèmes relatifs aux normes de conduite de tous les titulaires de charges publiques, notamment les modalités concernant des activités financières et commerciales, et à recommander les modifications qu'il faudrait éventuellement apporter aux modalités en vigueur pour garantir les normes de respectabilité les plus strictes dans la fonction publique".

[53] Committee on Standards in Public Life, *Third Report*, 1996, p. 48.

correctement étant donné la nature du problème dénoncé par le donneur d'alerte[54]". Cela signifie que les institutions du secteur public et du secteur privé devraient envisager la création et le bon fonctionnement d'un système de signalement, et étudier la meilleure manière d'offrir d'autres solutions, notamment une protection si de tels mécanismes n'existent pas, ne fonctionnent pas correctement ou s'il n'est pas raisonnable de s'attendre qu'ils fonctionnent correctement.

Un régime de divulgation en plusieurs étapes ou à plusieurs niveaux, qui s'applique à la protection d'une personne qui communique des informations, est particulièrement utile pour les personnes qui effectuent des signalements dans le cadre de leur travail et qui peuvent être soumises à des obligations spécifiques de confidentialité ou de loyauté envers leur employeur. S'agissant de faciliter les signalements par des membres du public, il convient d'envisager différents niveaux en se demandant qui doit répondre de l'acte illicite et qui devrait recevoir de tels signalements. L'accès à la protection peut varier si les informations sont communiquées directement au grand public et non à une autorité compétente.

Figure III. Responsabilité et voies de signalement possibles



Source: Repris de la Recommandation du Conseil de l'Europe sur la protection des lanceurs d'alerte, Exposé des motifs, par. 61.

[54] Assemblée parlementaire du Conseil de l'Europe, résolution 1729, adoptée le 29 avril 2010, art. 6.1.2, 6.2.3. Sept pays européens au moins (Albanie, Allemagne, France, Pays-Bas, Roumanie, Royaume-Uni et Serbie) prévoient comme moyen de défense ou circonstance atténuante, pour les personnes renvoyées ou traitées de manière préjudiciable dans le cadre de leur travail, le fait qu'elles ont tenté d'utiliser ou ont effectivement utilisé des voies internes avant de procéder à des révélations publiques. Amanda Jacobsen, *National Security and the Right to Information in Europe*, 2013, disponible à l'adresse: http://www.right2info.org/resources/publications/national-security-page/national-security-expert-papers/jacobsen_nat-sec-and-rti-in-europe.

Un cadre législatif et institutionnel qui facilite le signalement des actes de corruption et protège les personnes qui communiquent des informations, tel qu'énoncé dans la Convention contre la corruption, devrait prévoir un nombre raisonnable de voies de signalement efficaces qui puissent éventuellement se substituer les unes aux autres. De cette façon, les employés pourront contourner leur hiérarchie ou communiquer des informations à l'extérieur de leur organisation, notamment si le problème vient de cette dernière, et éviter ainsi la création d'un engorgement ou d'un éventuel point de rupture dans le mécanisme de contrôle ou le système judiciaire. Il a été proposé dans certains pays que les personnes soient en mesure d'interjeter appel contre la décision d'une autorité compétente de ne pas enquêter ou si elles ont des raisons de croire que l'enquête n'est pas conforme aux normes acceptables. Il pourrait s'agir, en quelque sorte, d'une solution autre que les voies de signalement parallèles, surtout dans les plus petits pays qui comptent moins d'autorités compétentes.

Pour les États parties, la difficulté consiste à garder tous ces différents aspects à l'esprit, à établir des règles et procédures claires et coordonnées pour offrir différentes solutions aux personnes qui communiquent des informations, et à rendre les signalements plus sûrs (on trouvera de plus amples informations sur la coordination entre institutions et le traitement des signalements au chapitre II, section E).

Exemple: Liste des personnes compétentes pour recevoir les signalements (Ghana)

Au Ghana, le *Whistleblowers Act* de 2006 (loi 720 sur les lanceurs d'alerte) s'applique à toutes les personnes qui communiquent spontanément des informations sur le lieu de travail ou en dehors du lieu de travail. Un guide sur la loi, élaboré par l'Anti-Corruption Agency (agence de lutte contre la corruption) en 2010, explique que toute personne peut signaler une irrégularité aux personnes ou institutions énumérées ci-dessous et bénéficier d'une protection. Le guide reflète le système de responsabilisation existant au Ghana:

- Un employeur;
- Un policier;
- Le Conseiller juridique principal du Gouvernement;
- Le Vérificateur général des comptes;
- Un membre du personnel de l'un des services de renseignement;
- Un parlementaire;
- Le Serious Fraud Office (bureau chargé des fraudes graves);
- La Commission on Human Rights and Administrative Justice (commission des droits de l'homme et de la justice administrative);
- La National Media Commission (commission nationale chargée des médias);
- L'Organe de contrôle des stupéfiants;
- Un chef;
- Le chef de famille ou un aîné de la famille du lanceur d'alerte;
- Le dirigeant d'un organe religieux reconnu;
- Un membre d'une assemblée de district;
- Un ministre d'État;
- Le Cabinet du Président;
- La Ghana Revenue Commission (l'autorité fiscale nationale);
- L'administrateur d'un district.

Source: Ghana Anti-Corruption Coalition, *A Guide to Whistleblowing in Ghana*, 2010, disponible aux adresses: http://wacmn.gaccgh.org/downloads/files/A%20Guide%20to%20Whistleblowing%20in%20Ghana1.pdf et http://www.track.unodc.org/LegalLibrary/pages/LegalResources.aspx?country=Ghana.

1. Dispositifs de signalement interne

Même dans les pays où la loi protège spécifiquement les personnes qui signalent des irrégularités à une autorité compétente autre que leur employeur, la plupart des personnes préfèrent d'abord communiquer les informations relatives à une irrégularité ou autre acte illicite au sein de leur lieu de travail à un superviseur, à un chef de département ou à une personne chargée d'enquêter sur ces questions[55].

Secteur public

Il est de plus en plus considéré comme une bonne pratique pour les employeurs de tous secteurs d'encourager leurs employés à communiquer toute information ou préoccupation susceptible de porter atteinte au service qu'ils sont censés fournir, notamment des informations concernant la corruption ou toute autre irrégularité ou fraude. La Recommandation du Conseil de l'Europe sur la protection des lanceurs d'alerte, qui s'applique aux employés du secteur public et du secteur privé, énonce ce qui suit dans l'Exposé des motifs:

> L'encouragement au signalement interne figure dans la recommandation parce que la mise en place de dispositifs de signalement interne efficaces fait partie des bonnes pratiques de gestion et de gouvernance transparentes, et, tout comme le signalement aux organes réglementaires publics, aux autorités de répression et aux organes de contrôle, le signalement interne peut contribuer dans de nombreux cas à la résolution rapide et efficace des risques pour l'intérêt général[56].

Il est intéressant de noter que, selon des travaux de recherche, lorsque des sociétés ou des services publics veillent à ce que les employés puissent signaler un problème, y compris la mauvaise qualité de certains services, des risques systémiques ou des actes répréhensibles, ces sociétés ou services non seulement bénéficient d'une plus grande confiance de la part de leurs employés et du public, mais sont également perçus comme fournissant un service de meilleure qualité[57].

En Australie, le *Federal Public Interest Disclosure Act* de 2013 (loi fédérale sur les révélations d'intérêt général), et la plupart des lois adoptées au niveau de ses différents États depuis les années 90, contiennent un cadre solide qui oblige tous les organes publics à mettre en place et appliquer des procédures de signalement interne et de protection. Ces procédures doivent être conformes aux meilleures pratiques formulées par les agences

[55] D'après des recherches menées en 2013 par Public Concern at Work et l'Université de Greenwich sur 1 000 affaires britanniques de signalement, dans 82 % des cas, les personnes ont commencé par signaler le problème à leur employeur. Voir Public Concern at Work et University of Greenwich, *Whistleblowing: The Inside Story — A study of the experiences of 1,000 whistleblowers*, PCaW, Londres, 2013, disponible à l'adresse: http://www.pcaw.org.uk/whistleblowing-the-inside-story. Il ressort d'un rapport publié en 2010 par l'Ethics Resource Center qu'aux États-Unis 4 % uniquement des lanceurs d'alerte ont révélé des informations en dehors de l'entreprise, et 3 % uniquement ont eu recours à des permanences téléphoniques; 46 % sont allés voir leur superviseur. Voir Ethics Resource Center, *Reporting: Who's Telling You What You Need to Know, Who Isn't, and What You Can Do About It*, Supplemental Research Brief — 2009 National Business Ethics Survey, 2010, disponible à l'adresse: http://ethics.org/files/u5/Reporting.pdf.

[56] Conseil de l'Europe, Recommandation CM/Rec(2014)7 du Comité des Ministres aux États membres sur la protection des lanceurs d'alerte, p. 39, disponible à l'adresse: https://wcd.coe.int/ViewDoc.jsp?id= 2188939&Site=CM.

[57] Au Royaume-Uni, une enquête menée à petite échelle en 2008 auprès d'infirmières du National Health Service (service national de santé) a montré que 80 % des infirmières ayant déclaré que leur organisation encourageait les signalements avaient également indiqué que leur organisation entretenait des relations ouvertes, voire très ouvertes, avec les usagers. Dans le cas des organisations qui n'encouragent pas les signalements, 34 % uniquement des infirmières ont donné des réponses semblables. Voir http://www.pcaw.org.uk/nhs-care-papers. En 2010, le Corporate Executive Board a communiqué des précisions sur son enquête menée auprès de 500 000 employés dans plus de 85 pays, ayant conclu à un lien direct entre une culture d'intégrité sur le lieu de travail et un nombre moins important d'actes répréhensibles. Douze indicateurs ont été utilisés, et l'indicateur ayant la plus forte corrélation avec un niveau élevé de rentabilité pour les actionnaires sur le long terme (plus de dix ans) était le fait pour les employés de se sentir à l'aise pour communiquer des informations. L'absence de crainte de représailles a été mentionnée comme un élément essentiel pour mettre les employés en confiance. Disponible à l'adresse: http://news.executiveboard.com/index.php?s=23330&item=50990.

de contrôle centrales et sont généralement vérifiées et surveillées au niveau central[58]. Parmi les bonnes pratiques internationales, on peut citer le fait de prendre les dispositions nécessaires pour que les signalements puissent être faits en toute confiance auprès des hauts responsables et en temps utile, en contournant ainsi la hiérarchie normale, si nécessaire[59]. Cet aspect est important, dans la mesure où certains pays demandent aux agents publics de signaler les cas de corruption à leur superviseur par écrit. Si ces deux exigences (forme écrite et voie de signalement unique) reposent probablement sur des intentions louables, elles peuvent en réalité avoir l'effet inverse. Le fait de limiter les voies de signalement possibles risque de restreindre les signalements internes.

Le Committee on Standards in Public Life du Royaume-Uni a recommandé les bonnes pratiques internes suivantes:

- Fournir des exemples permettant de distinguer les alertes des griefs;
- Donner au personnel la possibilité de signaler un problème en dehors du cadre hiérarchique;
- Donner un accès à une permanence téléphonique qui propose des conseils en toute confidentialité;
- Garantir au personnel un droit à la confidentialité lorsqu'il signale des problèmes;
- Expliquer quand et comment un problème peut être soulevé en toute sécurité en dehors de l'organisation (par exemple auprès d'une autorité de contrôle);
- Prévoir que les actes suivants relèvent du domaine disciplinaire: *a)* soumettre un lanceur d'alerte de bonne foi à un traitement injuste; et *b)* rapporter de fausses allégations par malveillance (à savoir communiquer intentionnellement des informations en sachant qu'elles sont fausses)[60].

Toute obligation imposant aux services publics ou à d'autres organisations de mettre en œuvre des dispositifs internes de signalement devrait être proportionnelle à la taille de ces services ou organisations et au niveau de risque que leurs activités font peser sur l'intérêt général (par exemple, élimination de déchets toxiques), ou à leur vulnérabilité à la corruption (par exemple des projets d'infrastructures d'un montant élevé). Les procédures de signalement devraient être claires et simples, car des procédures lourdes et complexes auront un effet dissuasif sur les lanceurs d'alerte.

Des exemples tirés de différents pays démontrent qu'il existe un certain nombre de méthodes pour encourager une culture plus ouverte au signalement des problèmes et pour offrir d'autres solutions claires lorsque les voies ordinaires sont bloquées, délibérément ou non. Dans le secteur public, les départements de l'administration centrale ou locale peuvent désigner une personne de rang élevé ou une personne extérieure à la hiérarchie, qui est habilitée à ouvrir une enquête et peut prendre des mesures pour protéger le personnel contre les représailles. Il peut s'agir de conseillers institutionnels en déontologie, de médiateurs ou d'autres rôles similaires.

---

[58]Voir, en général, Brown, A. J., "Towards "ideal" whistleblowing legislation? Some lessons from recent Australian experience ", *E-Journal of International and Comparative Labour Studies,* volume 2, nº 3, septembre/octobre 2013, par. 153 à 182. Pour des exemples illustrant le contenu minimum et recommandé de telles procédures, voir les Public Interest Disclosures Guidelines du New South Wales Ombudsman, Australie, élaborées conformément au *Public Interest Disclosures Act* (loi sur les révélations d'intérêt général) de 1994 (Nouvelle-Galles du Sud), à l'adresse: https://www.ombo.nsw.gov.au/news-and-publications/ publications/guidelines/public-interest-disclosures.

[59]Il existe un certain nombre de ressources disponibles concernant les dispositifs internes, notamment: OCDE, CleanGovBiz Toolkit on Whistleblower Protection, 2012, disponible à l'adresse: http://www.oecd.org/ corruption/ethics/whistleblower-protection.htm#Resources; British Standards Institute, *Whistleblowing Arrangements Code of Practice,* 2008, disponible à l'adresse: http://shop.bsigroup.com/forms/PASs/PAS-1998/; Public Concern at Work, The Whistleblowing Commission, *Code of Practice (for effective whistleblowing arrangements)*, 2013, disponible à l'adresse: http://www.pcaw.org.uk/whistleblowing-commission. Des ressources supplémentaires sont énumérées dans l'annexe du présent Guide.

[60]Voir PAS 1998:2008 — *Whistleblowing Arrangements Code of Practice,* 2008, British Standards Institute, p. 3. Disponible à l'adresse: http://shop.bsigroup.com/forms/PASs/PAS-1998/.

Dans certains pays, par exemple, le rôle du médiateur est très important et, dans le secteur public, un médiateur doté de pouvoirs indépendants qui communique des informations directement au parlement est généralement considéré comme appartenant à la fonction publique et non comme un acteur externe à celle-ci. En Belgique, par exemple, le Gouvernement flamand a fait participer le médiateur à son système de protection des lanceurs d'alerte[61].

Exemple: Code de déontologie du Gouvernement flamand (Belgique)

Le Gouvernement flamand a mis en œuvre un Code de déontologie qui énonce les principes, règles et accords généraux que les membres du personnel doivent respecter. Le Code indique que les modalités et principes de conduite sont fondés sur des valeurs issues du règlement flamand du personnel et sur les compétences liées à ces valeurs; et explique qu'il renvoie à la législation en vigueur et à d'autres codes relatifs à l'intégrité au sein des autorités flamandes.

La section intitulée "Signaler des irrégularités" décrit ce que les membres du personnel peuvent et devraient faire face à un dilemme éthique ou à une irrégularité plus grave, et comment ils peuvent les signaler. Chaque département dispose également de conseillers en déontologie auxquels les membres du personnel peuvent poser des questions en toute confiance ou demander des informations concernant la marche à suivre dans ces circonstances particulières. L'approche non seulement comporte une dimension préventive, en encourageant le personnel à communiquer des informations rapidement, mais permet aussi de détecter des irrégularités graves (fautes ou actes délictueux).

Signaler des irrégularités

Dans une organisation respectueuse de la déontologie, chacun assume ses responsabilités. Pensez aux différentes valeurs et normes applicables à une situation concrète. En cas de doute, consultez votre superviseur et cherchez avec lui une solution convenable. En cas d'irrégularités, l'obligation de communiquer des informations s'applique. Si vous observez des violations des règles déontologiques, vous prenez les mesures nécessaires, en fonction de la gravité des violations. Vous abordez, si nécessaire, la question avec vos collègues et vous signalez les violations aux organes compétents.

Tout dépend de la nature de la violation. S'agit-il d'un collègue qui fait une photocopie pour un usage privé ou d'un véritable cas de fraude? Il est également important de savoir si vous avez simplement des soupçons de violation ou si vous êtes en mesure de présenter des preuves tangibles de la violation.

Sur le site Web http://www.bestuurszaken.be/integriteit, vous trouverez les différents points de contact et départements auxquels vous pouvez adresser vos questions concernant l'éthique et signaler des violations. Vous trouverez également des renseignements supplémentaires sur le régime de protection des lanceurs d'alerte dont vous pouvez bénéficier en adressant une demande au service du médiateur flamand, lequel vous offrira une protection si vous craignez de subir des conséquences négatives du fait du signalement.

Source: Voir la page Web du Gouvernement flamand consacrée au coordonnateur chargé de l'intégrité, disponible à l'adresse: http://www.governance-flanders.be/integrity-0.

Secteur privé

Beaucoup de grandes entreprises disposent de mécanismes de signalement interne et les autorités de contrôle exigent parfois le respect de certaines normes, notamment des systèmes d'alerte, afin que les entreprises puissent être cotées en bourse. Les points

[61] Voir le site Web du Parlement flamand, à l'adresse: http://www.vlaamsparlement.be/Proteus5/showPersbericht.action?id=8792.

mentionnés précédemment en ce qui concerne le secteur public, en particulier le fait que les mécanismes doivent être proportionnels à la taille de l'organisation et que des solutions de remplacement doivent être proposées, s'appliquent également au secteur privé, l'élément clé étant qu'un employé doit savoir à qui faire part des irrégularités présumées.

L'étape suivante consiste à déterminer comment un employé peut être protégé s'il signale une irrégularité en interne et subit des représailles par la suite. À titre d'exemple, en Irlande et au Royaume-Uni, la loi prévoit une protection pour cette situation.

Dans le secteur privé aux Pays-Bas, les syndicats et les employeurs ont élaboré un code de bonnes pratiques pour guider l'action des employeurs et encourager une utilisation responsable des dispositifs et politiques par les employés. Ces initiatives reposent sur des valeurs communes de service et de comportement existant sur tous les lieux de travail. Il est évident que les employeurs et chefs de services dans tous les secteurs devraient s'efforcer, d'une part, de garantir une formation suffisante pour que les personnes chargées de tout dispositif d'alerte ou de signalement sachent comment gérer les signalements et les personnes concernées de manière équitable, et, d'autre part, de veiller à ce que les dispositifs soient clairement expliqués à tous les membres du personnel et partenaires (par exemple les bénévoles, les sous-traitants, etc.).

Exemple: Déclaration de la Fondation du travail sur le traitement des soupçons de fraude dans les sociétés (Pays-Bas)

Aux Pays-Bas, le Ministère des affaires sociales et du travail a commandé une étude qui a permis d'établir que les employeurs et les employés voulaient un code de conduite pour les aider à mettre en place les mécanismes nécessaires de signalement. Il a été demandé à la Stichting van de Arbeid (Fondation du travail) de se charger de ce projet, qui a abouti à la Déclaration sur le traitement des soupçons de fraude dans les sociétés (datée du 3 mars 2010 et actualisée en août 2012, voir la version anglaise intitulée *Statement on Dealing with Suspected Malpractices in Companies*). Voici un extrait de l'introduction de la Déclaration:

> La Fondation du travail est fière de répondre à cette demande. Elle estime qu'il est important de fixer les conditions permettant aux employés de révéler des fraudes commises au sein de leur entreprise sans se mettre en danger et offrant aux employeurs la possibilité de remédier à ces fraudes. Une telle démarche est non seulement plus sûre pour les employés, mais défend également les intérêts des sociétés dans la mesure où la hiérarchie devrait être informée des soupçons de fraude aussitôt que possible pour pouvoir prendre des mesures correctives. De plus, le problème peut être résolu avant que l'employé ne soit contraint de lancer une alerte (à savoir en dehors de la société). La Déclaration de la Fondation du travail constitue un premier pas vers la création de directives à l'intention des sociétés ou des secteurs d'activité en matière de signalement de soupçons de fraude.

2. Communication des informations aux autorités compétentes

Le rôle des autorités compétentes, notamment des médiateurs, des autorités indépendantes de contrôle et des services de détection et de répression, est essentiel dans la mesure où leur mandat de surveillance se place au-dessus des relations de travail dans le secteur public et d'autres organisations, ou entre le secteur public et d'autres organisations, et bien souvent transcende aussi la politique nationale. Les dirigeants de ces autorités sont généralement des experts dans leur domaine et leur expérience permet de

s'assurer que les informations qui leur sont communiquées sont traitées avec efficacité et professionnalisme. De plus, pour que les activités ou les organes placés sous leur supervision fonctionnent correctement, les autorités de contrôle et de surveillance sont tributaires des informations qu'elles recueillent ou reçoivent de sources multiples, y compris directement des organes concernés.

Les membres du public constituent une source d'informations pour les autorités compétentes. Ils communiquent généralement des informations en se plaignant d'un service de mauvaise qualité qui les affecte directement.

> Les plaintes peuvent provenir de clients mécontents ou contrariés ou d'autres parties prenantes. Elles peuvent néanmoins fournir aux agences des informations précieuses concernant des actes spécifiques de corruption ou des comportements répréhensibles. Elles peuvent également permettre d'identifier des membres du personnel ou des services peu performants. Le fait de détecter ces mauvaises pratiques et d'y remédier pourrait réduire les possibilités de corruption[62].

Certains usagers contourneront le service qui, d'après eux, est concerné par le problème et signaleront ce dernier directement à une autorité compétente, et ce peut-être du fait que l'autorité propose un mécanisme de signalement, comme une permanence téléphonique. Certes, certains signalements ne relèveront pas de la compétence de l'autorité et d'autres seront mieux gérés à titre de plainte nécessitant une mesure de réparation individuelle. Quoi qu'il en soit, en cas de doute sur la meilleure façon de procéder, il semble prudent de demander à la personne concernée la suite qu'elle entend donner à la question. En Nouvelle-Zélande, les informations peuvent circuler entre les autorités, mais la personne à l'origine du signalement doit en être informée[63].

Les informations issues de sources internes (des personnes travaillant dans un secteur ou une branche d'activité particuliers, par exemple) peuvent aider les autorités compétentes à concentrer leurs efforts et leurs ressources plus efficacement. En Nouvelle-Zélande, l'Office of the Ombudsman (bureau du médiateur) a compétence pour recevoir des "révélations protégées" et joue un rôle de premier plan dans l'orientation des personnes qui communiquent des informations et dans le suivi des enquêtes menées par des organisations du secteur public, notamment en reprenant la direction des enquêtes si nécessaire ou en les transmettant à des instances supérieures, par exemple à une autre agence ou à un ministère[64]. La loi énumère d'autres "personnes responsables" qui sont compétentes dans des domaines particuliers, notamment le Commissioner of Police (directeur de la police), le Controller and Auditor-General (contrôleur et vérificateur général des comptes) et le Health and Disability Commissioner (commissaire à la santé et à l'invalidité), à qui les informations peuvent être communiquées.

Au Royaume-Uni, la loi unique de protection des employés dans tous les secteurs comprend une liste des "personnes désignées" ou organes désignés, auxquels les intéressés peuvent communiquer des informations plutôt que de les communiquer à un employeur ou d'avoir recours à une voie de signalement créée par l'employeur. Au Royaume-Uni, comme dans de nombreux autres pays qui ont adopté des lois spécifiques de protection des lanceurs d'alerte, nul n'est tenu de communiquer les informations préalablement en interne. Au Royaume-Uni, parmi les organes "désignés" figurent la Financial Conduct

[62] Voir le site Web de l'Independent Commission against Corruption (commission indépendante chargée de la lutte contre la corruption) de la Nouvelle-Galles du Sud (Australie), à l'adresse: http://www.icac.nsw.gov.au/ preventing-corruption/detecting-corrupt-conduct/complaints-and-grievances/4881.

[63] Nouvelle-Zélande, *Protected Disclosures Act* (loi sur les révélations protégées), 2000, art. 16.

[64] Voir Nouvelle-Zélande, *Protected Disclosures Act*, 2000, disponible à l'adresse: http://www.legislation.govt.nz/act/public/2000/0007/latest/DLM53466.html.

Authority (autorité de réglementation financière), l'Office of Rail Regulation (bureau de la réglementation ferroviaire), la National Crime Agency (agence nationale de lutte contre la criminalité) et le Children's Commissioner for England (commissaire à l'enfance)[65].

Dans la plupart des cas, les informations qui relèvent de la compétence d'une autorité donnée sont automatiquement admises, indépendamment de la source. Aux États-Unis, par exemple, dans le cadre de la *Dodd-Frank Law* (loi Dodd-Frank) de 2010, un nouveau bureau chargé des lanceurs d'alerte (appelé Office of the Whistleblower) a été ajouté à l'autorité de contrôle existante, à savoir la Securities and Exchange Commission (Commission fédérale de contrôle des opérations boursières), pour gérer spécifiquement son programme de protection des lanceurs d'alerte.

Dans de nombreux pays, des organes ont été créés et dotés de mandats spécifiques pour lutter contre la corruption et recevoir les signalements de cas de corruption ou des informations liées à des cas de corruption provenant du public, conformément au paragraphe 2 de l'article 13 de la Convention contre la corruption. L'Anti-Corruption and Civil Rights Commission (commission de lutte contre la corruption et de défense des droits civils) de la République de Corée est intéressante en termes d'innovations récentes visant à associer lutte contre la corruption et alertes d'intérêt général.

Exemple: Anti-Corruption and Civil Rights Commission (République de Corée)

L'Anti-Corruption and Civil Rights Commission de la République de Corée (commission de lutte contre la corruption et de défense des droits civils) a été créée en 2008 en regroupant l'Independent Commission against Corruption (commission indépendante de lutte contre la corruption), le médiateur et l'Administrative Appeals Commission (commission des appels administratifs). De ce fait, les cas de corruption et un large éventail de questions d'intérêt général peuvent être signalés à l'Anti-Corruption and Civil Rights Commission, qui n'enquête pas elle-même sur les signalements de corruption mais les transmet à d'autres organes. Fait important, elle supervise les affaires et contrôle les délais applicables à leur traitement.

En République de Corée, deux lois régissent la protection des personnes qui communiquent des informations et des lanceurs d'alerte en milieu professionnel: la loi de 2002 sur la lutte contre la corruption, qui couvre les alertes dans le secteur public, et la loi de 2011 sur la protection des lanceurs d'alerte d'intérêt général.

Les employés du secteur public peuvent communiquer des informations relatives à la corruption ou à toute violation du code de déontologie. Conformément à la loi sur la protection des lanceurs d'alerte d'intérêt général, les questions d'intérêt général couvrent un large éventail d'informations, relatives notamment à des questions de santé publique et de consommation, aux risques environnementaux, etc., et les violations se rapportant à 180 lois nationales.

Entre 2002 et 2013, environ 28 000 signalements ont été déposés auprès de l'Anti-Corruption and Civil Rights Commission. Parmi ces signalements, 1 000 ont été renvoyés à des organismes d'enquête et 9 680 à d'autres organismes. Sur les 1 000 cas ayant fait l'objet d'une enquête, 907 ont été établis (leur lien avec la corruption ayant été prouvé) et des violations de codes de déontologie ont été établies dans 430 cas.

Au cours de la même période, l'Anti-Corruption and Civil Rights Commission a reçu 181 demandes de protection, dont 146 liées à des inquiétudes en matière d'emploi, 22 demandes de protection physique et 13 demandes de garantie d'anonymat. Elle a ordonné des mesures correctives à la suite de représailles de nature professionnelle

[65] La loi énumère plus de 65 "personnes désignées"; voir https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies--2.

dans 48 cas. Elle est habilitée à prendre de telles mesures conformément à l'article 62 de la loi sur la protection des lanceurs d'alerte d'intérêt général, en demandant au Ministère de l'administration publique et de la sécurité ou au responsable de l'organisation publique concernée de prendre les mesures nécessaires et de lui communiquer les résultats. L'Anti-Corruption and Civil Rights Commission a également assuré la protection physique des 22 personnes l'ayant demandé; elle peut demander des mesures de protection au commissaire général de la police nationale, au chef d'une agence de police locale ou au chef du commissariat de police compétent (art. 64). La loi indique aussi clairement qu'il est interdit à tout employé de l'Anti-Corruption and Civil Rights Commission ou tout organisme d'enquête saisi d'une affaire de corruption de "divulguer ou de suggérer l'identité de l'informateur, du plaignant ou du lanceur d'alerte" sans son consentement. Des mesures disciplinaires ont été prises dans quatre affaires dans lesquelles l'identité des personnes avait été révélée.

En 2006, l'Anti-Corruption and Civil Rights Commission a introduit la possibilité pour les personnes qui communiquent des informations de recevoir une récompense sous forme monétaire. Une personne peut recevoir jusqu'à 2 millions de dollars des États-Unis si son signalement permet directement à des organismes publics de recouvrer des fonds, d'augmenter leurs recettes ou de réduire leurs dépenses. Cette commission peut également accorder ou recommander le paiement d'une récompense si l'alerte a servi l'intérêt général. Le montant total des sommes versées dans 63 affaires depuis 2006 s'élève à environ 487 000 dollars des États-Unis. Toutefois, depuis 2002, le montant récupéré par l'Anti-Corruption and Civil Rights Commission grâce aux 220 signalements de cas de corruption s'élève à environ 60 millions de dollars des États-Unis.

L'Anti-Corruption and Civil Rights Commission procède actuellement à un changement de modèle de protection et passe d'un système rétroactif à un système préventif. À cette fin, elle centre ses efforts sur:

- Les bases d'un système de protection en recommandant que les organismes établissent leurs propres politiques et dispositifs de protection;
- La promotion de l'importance des alertes grâce à des activités sur mesure et des programmes d'éducation pour les entreprises, les organisations publiques et le public en général (en signant des mémorandums d'accord avec les plus grandes entreprises);
- L'introduction d'un système de suspension de toute action qui désavantagerait un lanceur d'alerte pendant une enquête;
- La question de savoir s'il convient ou non de toujours accorder une récompense.

Pour de plus amples renseignements sur l'Anti-Corruption and Civil Rights Commission et les lois qui régissent ses fonctions, voir: http://www.acrc.go.kr/eng/index.do.

Si les pays possédant des systèmes juridiques et culturels semblables ont tendance à adopter des mécanismes de signalement et des modèles de protection également semblables, il est recommandé aux États de ne pas partir du principe que ces mécanismes et modèles pourront toujours être intégrés rapidement dans leur système existant. Les États doivent avoir préalablement mené les consultations et évaluations nécessaires concernant leur propre situation nationale.

Certains facteurs essentiels sont considérés comme jouant un rôle central dans l'efficacité de tout organisme compétent, comme la possibilité pour ce dernier d'exercer ses fonctions de manière impartiale et à l'abri de toute influence indue; des pouvoirs clairs et sans équivoque lui permettant de remplir ses fonctions — qu'il s'agisse de mener des enquêtes et des poursuites concernant les irrégularités ou de protéger les personnes qui communiquent des informations si elles subissent des représailles, ou les deux —; la

publication des résultats de ses travaux et les ressources nécessaires pour remplir son mandat.

En Nouvelle-Zélande, le *Protected Disclosures Act* (loi sur les révélations protégées) porte modification du *Human Rights Act* (loi sur les droits de l'homme) et interdit d'imposer à des personnes qui communiquent des informations en interne un traitement moins favorable qu'à d'autres personnes se trouvant dans une situation comparable. Le système néo-zélandais distingue, d'une part, le traitement du contenu du signalement et l'enquête à son sujet et, d'autre part, le traitement des plaintes pour représailles infligées suite au signalement. Si une personne qui a communiqué des informations porte plainte pour traitement injuste, sa plainte est traitée dans un premier temps par la Human Rights Commission (commission néo-zélandaise des droits de l'homme) (pour de plus amples renseignements, voir le chapitre II, section E.2).

3. Révélations d'informations par d'autres canaux (signalement externe) et obligation de rendre des comptes au public

Dans tous les pays, il peut arriver que les informations relatives à des actes illicites ne soient pas dûment évaluées ou examinées par les personnes spécifiquement chargées de le faire. Partout dans le monde, des personnes se sont mises en danger pour alerter les autorités et le public en général et leur signaler des problèmes graves, notamment des cas de corruption. Au Canada, par exemple, un fonctionnaire a communiqué des soupçons de fraude à son superviseur et à son syndicat, ce qui a permis de mettre au jour le détournement de millions de dollars canadiens de fonds publics dans le cadre d'un scandale de commandites touchant jusqu'aux plus hauts responsables du parti politique au pouvoir[66].

S'il est préférable que les soupçons d'irrégularités soient traités rapidement et par une personne proche de la source du problème, cela n'est pas toujours possible, et d'autres voies de signalement devraient être envisagées conformément aux normes internationales relatives aux droits de l'homme. En pratique, dans certaines circonstances, seules les révélations publiques permettent de détecter véritablement les cas de corruption et de prendre des mesures efficaces.

L'article 33 de la Convention contre la corruption vise les affaires dans lesquelles des informations sont communiquées aux autorités compétentes, et les États parties doivent également tenir compte des obligations qui leur incombent en vertu de l'article 13 de la Convention, qui les enjoint à prendre des mesures appropriées pour encourager la société à participer activement à la lutte contre la corruption, notamment en prenant des mesures consistant à "assurer l'accès effectif du public à l'information", conformément à l'alinéa *b* du paragraphe 1, et à "respecter, promouvoir et protéger la liberté de rechercher, de recevoir, de publier et de diffuser des informations concernant la corruption", conformément à l'alinéa *d*.

Associations locales et organisations non gouvernementales

Les personnes possédant des informations relatives à des actes illicites peuvent choisir de prendre contact avec une association locale ou une ONG, soit parce qu'elles

[66]Commission d'enquête sur le programme de commandites et les activités publicitaires (Commission Gomery), 2006, chapitre VII: Vérifications et enquêtes, disponible à l'adresse: http://epe.lac-bac.gc.ca/100/ 206/301/pco-bcp/commissions/sponsorship-ef/06-02-10/www.gomery.ca/en/phase1report/default.htm.

connaissent mieux ces interlocuteurs, soit parce qu'elles sont méfiantes à l'égard des autorités compétentes. Souvent, les groupes de la société civile travaillent au sein de leur communauté et acquièrent des compétences spécialisées en défendant la cause des populations locales afin d'améliorer notamment l'accès à l'éducation, à la santé et à l'eau, ou de protéger les droits civils et l'environnement. Ces groupes centrent de plus en plus leurs efforts sur la lutte contre la corruption au niveau local et au niveau national, car ils estiment que la corruption empêche la réalisation de progrès durables.

Certaines ONG communiquent des informations relatives à des actes illicites directement aux autorités sans désigner leur source; d'autres recueillent des informations auprès d'un certain nombre de sources différentes, effectuent leurs propres recherches puis s'engagent dans des actions de défense à partir de ces informations. Si la plupart de ces initiatives sont respectées et efficaces, dans certains pays les ONG ne sont pas en mesure d'offrir autre chose qu'une protection limitée aux personnes qui communiquent des informations — en garantissant généralement la confidentialité des informations qu'elles reçoivent.

Toutefois, la société civile exploite de plus en plus les nouvelles technologies de manière novatrice afin de détecter les actes illicites et de protéger les personnes qui communiquent des informations. Elle met également en place des organisations hybrides qui associent journalisme d'enquête et défense des droits, et certains groupes font de la protection des lanceurs d'alerte une de leurs missions principales. Une bonne connaissance du système juridique et des compétences spécialisées sont alors nécessaires.

Si la société civile peut jouer un rôle important pour faciliter la transmission d'informations et veiller à ce qu'elles soient communiquées au bon endroit, son action ne remplace pas les travaux des autorités compétentes qui mènent des enquêtes officielles, traduisent les auteurs d'infractions en justice ou amorcent des réformes réglementaires dans le cadre de leurs fonctions essentielles. Les services de détection et de répression, par exemple, doivent disposer de capacités, de ressources et de pouvoirs suffisants pour mener des enquêtes sur les actes illicites et protéger les personnes qui communiquent des informations, ce qui permet de renforcer la confiance accordée au système de justice.

Médias

Il ressort de certaines études que la divulgation d'actes illicites aux médias peut être plus efficace que le signalement interne (à savoir signaler des soupçons à l'employeur) pour inciter à prendre des mesures correctives[67]. Les gouvernements doivent comprendre ce phénomène et déterminer ce qu'ils peuvent faire pour favoriser une réponse plus rapide et plus efficace aux signalements de cas de corruption ou d'autres soupçons d'irrégularités. On peut également considérer que les conclusions des études viennent souligner la nécessité de renforcer l'efficacité et la fiabilité des mécanismes de gestion des informations communiquées en interne et aux autorités compétentes.

Certaines autorités, en particulier celles qui travaillent dans le domaine de la corruption, surveillent les médias à la recherche d'informations concernant des irrégularités ou

[67] Une étude a montré que 44 % des personnes qui ont communiqué des informations directement à l'autorité compétente ou aux médias estiment que leur organisation a par la suite modifié ses pratiques en conséquence. La même étude a montré que 27 % seulement des personnes qui ont signalé une irrégularité à leur employeur estiment que leur démarche a entraîné un changement. Voir Rothschild, J. et T. D. Miethe, "Whistle-blower Disclosures and Management Retaliation", *Work and Occupations*, volume 26, nº 1, 1999, p. 107 à 128. Une autre étude a indiqué que le fait de signaler des irrégularités directement à une autorité de contrôle ou aux médias était plus efficace, dans la mesure où cela incitait l'organisation à mener une véritable enquête et à prendre d'autres mesures correctives. Voir Dworkin, T. M. et M. S. Baucus, "Internal vs. External Whistleblower: A Comparison of Whistleblowing Processes", *Journal of Business Ethics*, volume 17, nº 12, 1998, p. 1281 à 1298.

risques éventuels, et utilisent ces informations pour lancer leurs propres enquêtes. Le droit de la presse de communiquer des informations sur des questions d'intérêt général, y compris la corruption, est une garantie essentielle de l'intérêt public, et les États parties sont encouragés à garantir la liberté de la presse, ainsi que la protection des journalistes et de leurs sources, conformément aux normes internationales[68]. Pour les personnes qui communiquent des informations, il s'agit clairement d'un moyen de s'assurer que les informations seront traitées et de bénéficier d'une certaine protection.

Certaines lois nationales autorisent, sous certaines conditions, la communication d'informations aux médias ou à d'autres entités externes, tout en prévoyant une protection juridique pour les lanceurs d'alerte. Parmi ces lois figurent le *Protected Disclosures Act* (loi sur les révélations protégées) adopté par l'Irlande en 2014, dont l'article 10 prévoit des conditions spécifiques; la loi sur la protection des agents publics qui portent plainte contre des violations de la législation, adoptée par la Roumanie en 2004; et la loi sur la protection des lanceurs d'alerte adoptée par la Serbie en 2014. La loi roumaine est remarquable en ce sens qu'elle autorise les communications aux médias sans aucune restriction.

Même si aujourd'hui la Suède ne dispose d'aucune loi sur la protection des lanceurs d'alerte, sa Constitution et sa loi sur la liberté de la presse protègent le droit des agents publics de communiquer des informations directement aux médias ou à d'autres entités externes en tant que moyen favorisant la transparence et la responsabilité envers le public. Ainsi, sous réserve de certaines exceptions limitées (liées par exemple à la sécurité nationale), un employeur du secteur public n'a pas le droit d'imposer une mesure disciplinaire à un employé qui communique des informations aux médias ni de s'enquérir si quelqu'un est entré en contact avec les médias. Toute personne qui viole intentionnellement cette dernière interdiction peut se voir imposer une amende ou une peine d'emprisonnement d'un an maximum. Le système dépend dans une large mesure de l'Ombudsman du Parlement et du Ministre de la justice, qui mènent des investigations sur les affaires de représailles et sur toute enquête illégale concernant les sources des médias. Si les poursuites sont rares, les employeurs du secteur public qui se livrent à de telles activités interdites sont "désignés et dénoncés" dans les décisions publiques. Le principe constitutionnel s'applique aux employés de sociétés municipales et d'organes spécifiques dont la liste figure dans une annexe de la loi suédoise régissant le secret des documents officiels[69]. Conformément à cette protection constitutionnelle, les employeurs du secteur public peuvent également se voir imposer une amende ou une peine d'emprisonnement s'ils exercent des représailles contre un employé qui a signalé des irrégularités. Le fait d'ériger les représailles en infraction est relativement récent et, bien que l'on recense plusieurs affaires, aucune n'a abouti à une condamnation[70]. Ainsi, même si plusieurs autorités publiques suédoises disposent de systèmes d'alerte, elles ne peuvent jamais contourner le droit constitutionnel de communiquer des informations aux médias.

Dans le domaine des droits de l'homme, la jurisprudence relative à la liberté d'opinion et à la liberté d'expression fournit d'autres orientations utiles aux États parties pour examiner la question de la protection des lanceurs d'alerte.

[68] Le droit à la protection des sources découle de la Déclaration universelle des droits de l'homme et du Pacte international relatif aux droits civils et politiques. Aux termes du paragraphe 2 de l'article 19 du Pacte: "[t]oute personne a droit à la liberté d'expression; ce droit comprend la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce, sans considération de frontières, sous une forme orale, écrite, imprimée ou artistique, ou par tout autre moyen de son choix". L'article dispose cependant que ce droit est assorti de conditions et qu'il peut donc être soumis à certaines restrictions qui doivent toutefois être expressément fixées par la loi et doivent être nécessaires: *a)* au respect des droits ou de la réputation d'autrui; *b)* à la sauvegarde de la sécurité nationale, de l'ordre public, de la santé ou de la moralité publiques.

[69] Suède, *Public Access to Information and Secrecy Act* (loi sur l'accès du public aux informations et sur le secret), 2009, disponible à l'adresse: http://www.government.se/content/1/c6/13/13/97/aa5c1d4c.pdf.

[70] Jugement de la Cour suprême du 29 octobre 2001, affaire no B619-01/*NJA 2001 s. 673*.

a) *Droit relatif aux droits de l'homme*

L'article 13 de la Convention contre la corruption trouve sa source dans les instruments internationaux relatifs aux droits de l'homme dont il corrobore certains principes, notamment en ce qui concerne la liberté d'expression et l'accès à l'information[71]. Parmi ces instruments figurent la Déclaration universelle des droits de l'homme, le Pacte international relatif aux droits civils et politiques, les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme, la Déclaration de l'Organisation internationale du Travail relative aux principes et droits fondamentaux au travail, la Déclaration des Nations Unies sur les défenseurs des droits de l'homme, et d'autres instruments régionaux relatifs aux droits de l'homme, notamment la Charte africaine des droits de l'homme et des peuples, la Convention américaine relative aux droits de l'homme, la Convention européenne des droits de l'homme et la Charte des droits fondamentaux de l'Union européenne.

Ces dernières années, la Cour européenne des droits de l'homme (CEDH) a rendu un certain nombre de décisions[72] relatives aux personnes qui communiquent des informations, au motif d'ingérences dans leur droit à la liberté d'expression consacré à l'article 10 de la Convention européenne des droits de l'homme[73]. Il convient d'observer cependant que ces affaires étaient généralement liées à des informations diffusées au public et que de telles révélations ne sont protégées que dans des circonstances exceptionnelles. Les affaires concernent le plus souvent des personnes qui, dans le cadre d'une relation professionnelle, rendent publiques des informations (en passant généralement, mais pas toujours, par l'intermédiaire d'un journaliste) dont elles pensent qu'il n'y sera pas donné suite autrement. La personne est alors sanctionnée — renvoyée ou poursuivie — au motif qu'elle a violé ses propres obligations ou qu'il a été porté atteinte à d'autres intérêts ou droits importants. Il peut notamment s'agir du droit des tiers au respect de leur vie privée ou de leur réputation, et de l'intérêt des employeurs ou de l'État à garder certaines informations confidentielles ou secrètes.

Exemple: Protection d'un agent public qui a divulgué des documents à la presse

M. Iacob Guja dirigeait le service presse du parquet général de Moldova. Après que des poursuites ont été abandonnées contre quatre policiers accusés de mauvais traitements sur des suspects, M. Guja a envoyé deux lettres à la presse concernant cette affaire,

[71] Pour de plus amples renseignements à ce sujet, voir également: ONUDC, *Informer sur la corruption — Un outil de référence pour les gouvernements et les journalistes*.

[72] Voir les affaires *Sosinowska* c. *Pologne*, (requête nº 10247/09, 18 octobre 2011); *Poyraz* c. *Turquie* (requête nº 15966/06, 7 décembre 2010); *Kudeshkina* c. *Russia* (requête nº 29492/05, 26 février 2009); *Marchenko* c. *Ukraine* (requête nº 4063/04, 19 février 2009).

[73] La Cour européenne des droits de l'homme a soutenu que "l'article 10 s'impose non seulement dans les relations entre employeur et employé lorsque celles-ci obéissent au droit public mais peut également s'appliquer lorsque ces relations relèvent du droit privé […]" et que "l'État a l'obligation positive de protéger le droit à la liberté d'expression contre des atteintes provenant même de personnes privées" (affaire *Fuentes Bobo* c. *Espagne*, requête nº 39293/98, 29 février 2000, par. 38).
L'article 10 prévoit que l'exercice de ce droit est assorti de conditions qui autorisent l'ingérence dans le droit d'une personne à la liberté d'expression, dans certaines circonstances et dès lors que: *a)* l'ingérence est prévue par la loi; *b)* elle répond à un but légitime (comme protéger la réputation ou les droits d'autrui, la sécurité nationale ou l'intégrité territoriale, ou empêcher la divulgation d'informations confidentielles); et *c)* elle est une mesure nécessaire et proportionnée dans une société démocratique. Il a été établi que la Cour doit déterminer "si "l'ingérence" incriminée correspondait à un "besoin social impérieux", si elle était "proportionnée au but légitime poursuivi", si les motifs fournis par les autorités nationales pour la justifier étaient "pertinents et suffisants" au regard de l'article 10. À cette fin, la Cour s'est assurée que les autorités nationales appliquaient des normes conformes aux principes consacrés à l'article 10 et, de plus, qu'elles se fondaient sur une évaluation acceptable des faits pertinents […]", *Sunday Times* c. *Royaume-Uni* (nº 1), 26 avril 1979, par. 62, Séries A, nº 30.

indiquant que les poursuites auraient été abandonnées pour des motifs illégitimes. Une de ces lettres provenait d'un représentant de haut rang du Parlement. M. Guja a été révoqué au motif que les lettres étaient secrètes (même si elles n'étaient pas classées comme telles) et qu'il n'avait pas consulté ses supérieurs avant de les communiquer à la presse.

M. Guja a intenté une action en réintégration, soutenant, notamment, que les lettres "n'étaient pas des documents secrets au regard de la loi", qu'il n'était pas tenu de consulter les responsables des autres services avant de prendre contact avec la presse et que sa révocation emportait violation de son droit à la liberté d'expression (par. 22). La Cour d'appel de Chișinău le débouta de son action, décision confirmée par la Cour suprême de justice au motif que "l'obtention d'informations au moyen d'un abus de fonctions ne relevait pas de la liberté d'expression" (par. 25).

Dans le cadre de la requête dont elle a été saisie, la Cour européenne des droits de l'homme a déclaré (par. 72) que "[...] les agents de la fonction publique [...] peuvent être amenés, dans l'exercice de leur mission, à prendre connaissance d'informations internes, éventuellement de nature secrète, que les citoyens ont un grand intérêt à voir divulguer ou publier. [La Cour] estime dans ces conditions que la dénonciation par de tels agents de conduites ou d'actes illicites constatés sur leur lieu de travail doit être protégée dans certaines circonstances. Pareille protection peut s'imposer lorsque l'agent concerné est seul à savoir — ou fait partie d'un petit groupe dont les membres sont seuls à savoir — ce qui se passe sur son lieu de travail et est donc le mieux placé pour agir dans l'intérêt général en avertissant son employeur ou l'opinion publique".

La Cour a soutenu qu'il y avait eu violation de l'article 10 et que, dans les circonstances de l'espèce, une divulgation à l'extérieur, "même à un journal", pouvait se justifier. Elle a notamment: *a)* noté l'importance des questions, dont l'opinion publique avait un intérêt légitime à être informée et qui relevaient du débat politique (par. 88); et *b)* observé que ni la législation moldave ni le règlement intérieur du parquet général ne contenaient de dispositions concernant la divulgation d'irrégularités par des salariés, et qu'il n'existait aucun élément de nature à invalider la thèse du requérant selon laquelle il ne disposait d'aucun autre moyen effectif [les instances supérieures du parquet ou le Parlement] dans les circonstances propres à l'affaire (par. 80 à 84).

Source: Affaire *Guja* c. *Moldova*, Cour européenne des droits de l'homme, 12 février 2008. Arrêt disponible à l'adresse: http://hudoc.echr.coe.int/fre#{"fulltext":["guja"],"itemid":["001-85017"]}

Dans l'affaire *Guja* c. *Moldova*, la CEDH a défini six principes pour déterminer si une ingérence dans les droits consacrés à l'article 10 était "nécessaire dans une société démocratique". Ces principes directeurs ont depuis été appliqués dans un certain nombre d'affaires, notamment l'affaire *Heinisch* c. *Allemagne*[74], qui concernait une infirmière du secteur privé qui avait divulgué des informations concernant les soins aux patients en portant plainte au pénal et, par la suite, en diffusant des tracts. On peut aussi citer

[74] *Heinisch* c. *Allemagne* (requête nº 28274/08, 21 juillet 2011). Mme Heinisch travaillait en tant qu'infirmière dans un foyer pour personnes âgées. Elle a été licenciée lorsque, après avoir averti la direction de graves dysfonctionnements dans les soins proposés aux patients, sans obtenir de réponse, elle a déposé une plainte pénale pour fraude. La Cour d'appel allemande a confirmé son licenciement, indiquant que la plainte pénale constituait une réaction disproportionnée au refus de son employeur de reconnaître la situation de sous-effectif et qu'elle avait manqué à son devoir de loyauté à l'égard de son employeur. Dans son arrêt, la Cour européenne des droits de l'homme a reconnu que les employés avaient un devoir de loyauté et a déclaré ce qui suit: "il importe que la personne concernée procède à la divulgation d'abord auprès de son supérieur ou d'une autre autorité ou instance compétente. La divulgation au public ne doit être envisagée qu'en dernier ressort, en cas d'impossibilité manifeste d'agir autrement". La Cour a examiné cette affaire en tenant compte des principes établis dans le cadre de l'affaire *Guja* et a conclu à une violation de l'article 10.

l'affaire *Bucur et Toma* c. *Roumanie*[75], dans laquelle un employé du Service roumain du renseignement a divulgué des informations concernant de graves irrégularités dans les registres d'écoute et les motifs justifiant l'interception de communications téléphoniques de plusieurs journalistes, hommes politiques et hommes d'affaires (M. Toma était un journaliste dont les communications téléphoniques avaient été interceptées).

Le dernier arrêt de la CEDH relatif à la protection des lanceurs d'alerte a été rendu en janvier 2015. La Cour a conclu que la Lettonie avait violé les droits d'Andris Rubins, professeur de médecine à l'Université Stradiņa de Riga, consacrés à l'article 10. En 2010, l'Université a supprimé le département dont M. Rubins était le chef, après que ce dernier eut rapporté des allégations de mauvaise gestion des finances de l'Université et de manque de contrôle de la gestion. Les juges ont voté 5 contre 2 en sa faveur et lui ont accordé 10 280 euros pour frais et dépens[76].

Principes directeurs définis par la Cour européenne des droits de l'homme

1. La question de savoir si l'intéressé disposait ou non d'autres moyens pour procéder à la divulgation

Dans l'affaire *Heinisch* c. *Allemagne*, la Cour a souligné quelques éléments clés: on ne peut raisonnablement attendre d'un employé qu'il signale préalablement des faits au sein de l'entreprise s'il a connaissance d'un délit dont la non-dénonciation l'aurait exposé à des poursuites pénales. De plus, le signalement préalable des faits au sein de l'entreprise n'est pas requis lorsqu'il n'existe aucun espoir réel de résolution du problème. Si, par exemple, l'employeur n'a pas remédié à une pratique illicite même si l'employé l'en a averti, ce dernier n'est plus lié par son devoir de loyauté envers son employeur. La Cour a en outre signalé que le même raisonnement apparaissait dans les principes directeurs de l'Assemblée parlementaire relatifs à la protection des lanceurs d'alerte, qui prévoient que lorsqu'il n'est pas raisonnable de s'attendre à ce que les voies internes fonctionnent correctement, il convient de protéger celui qui utilise des voies externes.

2. L'intérêt général que présente la divulgation des informations

Dans l'affaire *Guja* c. *Moldova*, la Cour a noté que "[d]ans un système démocratique, les actions ou omissions du gouvernement doivent se trouver placées sous le contrôle attentif non seulement des pouvoirs législatif et judiciaire, mais aussi des médias et de l'opinion publique. L'intérêt de l'opinion publique pour une certaine information peut parfois être si grand qu'il peut l'emporter même sur une obligation de confidentialité imposée par la loi".

[75] *Bucur et Toma* c. *Roumanie* (requête nº 40238/02, 13 juin 2013). Le texte suivant est la traduction d'une version révisée du résumé disponible en anglais à l'adresse: http://www.right2info.org/cases/r2i-bucur-and-toma-v.-romania. En 1996, M. Bucur a signalé des irrégularités à son chef de département concernant des registres d'écoute remplis au crayon et n'offrant aucune justification pour la mise sur écoute des téléphones de plusieurs journalistes, hommes politiques et hommes d'affaires. Il a été réprimandé. Il a ensuite pris contact avec un député, membre de la commission parlementaire de contrôle du SRI (par. 10), qui lui a conseillé de se diriger vers la presse. M. Bucur a tenu une conférence de presse au cours de laquelle il a rendu publiques 11 cassettes audio. La conférence de presse a eu un écho retentissant dans les médias internationaux. M. Bucur a été poursuivi puis condamné par un tribunal militaire à deux ans d'emprisonnement pour vol, collecte et transmission illégales d'informations à caractère secret ou touchant à la vie privée, à l'honneur et à la réputation du SRI (par. 41). Finalement, la Cour européenne des droits de l'homme a été saisie. Elle a reconnu la légitimité du but affiché par le Gouvernement — prévenir et réprimer des infractions touchant à la sûreté de l'État (par. 82) — mais a conclu que l'ingérence n'était pas "nécessaire" dans une société démocratique, dès lors que les informations communiquées revêtaient une grande importance pour l'intérêt général (par. 120). La Cour a ajouté que M. Bucur avait des motifs légitimes de penser que les informations étaient vraies (par. 113), que l'intérêt général à la divulgation d'agissements illicites au sein du SRI l'emportait sur l'intérêt qu'il y a à maintenir la confiance du public dans cette institution (par. 115), et que M. Bucur avait agi de bonne foi (par. 118).

[76] Arrêt, affaire *Rubins* c. *Lettonie*, Cour européenne des droits de l'homme, Strasbourg, 13 janvier 2015, disponible à l'adresse: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-149204#{%22itemid%22: [%22001-149204%22]}.

3. L'authenticité de l'information divulguée

Dans l'affaire *Guja* c. *Moldova*, la Cour a rappelé que la liberté d'expression comportait des responsabilités, et que quiconque choisit de divulguer des informations doit vérifier avec soin, dans la mesure où les circonstances le permettent, qu'elles sont exactes et dignes de crédit. Dans l'affaire *Bucur et Toma* c. *Roumanie*, la Cour avait à l'esprit la Résolution 1729 (2010) de l'Assemblée parlementaire du Conseil de l'Europe et le besoin de protéger les donneurs d'alerte, sous réserve qu'ils aient des "motifs raisonnables" de penser que l'information divulguée était vraie.

4. Le préjudice causé à l'employeur

Dans une société démocratique, la divulgation publique est-elle si importante qu'elle l'emporte sur le préjudice subi par l'employeur? Dans les affaires *Guja* c. *Moldova* et *Bucur et Toma* c. *Roumanie*, l'employeur était un organisme public, et la Cour a mis en balance l'intérêt général à maintenir la confiance du public dans ces organismes et l'intérêt général à divulguer les informations faisant état de leurs agissements illicites, puis s'est prononcée en faveur de l'intérêt général à divulguer les informations.

5. La question de savoir si la divulgation est faite de bonne foi

Dans l'affaire *Guja* c. *Moldova*, la Cour a déclaré qu'il était important d'établir si la personne concernée, en procédant à la divulgation, a agi de bonne foi et avec la conviction que l'information était authentique, si la divulgation servait l'intérêt général et si l'auteur disposait ou non de moyens plus discrets pour dénoncer les agissements en question.

6. La sévérité et les conséquences de la sanction infligée à la personne qui a procédé à la divulgation

Dans l'affaire *Heinisch* c. *Allemagne*, par exemple, la Cour a déclaré que la sanction pouvait avoir un effet inhibiteur sur les autres employés du secteur, effet qui allait "à l'encontre des intérêts de l'ensemble de la société et [que] la Cour [devait] en tenir compte pour apprécier la proportionnalité — et donc la justification — de la sanction infligée à la requérante".

Remarque: L'ordre de présentation de ces six principes est celui utilisé par la CEDH dans l'affaire *Heinisch* c. *Allemagne* (voir ci-dessus, note 74).

Par conséquent, il est important que les États parties réfléchissent au moyen d'étendre la protection aux personnes qui signalent des actes illicites aux médias ou en informent le public de toute autre manière, s'il est justifié et raisonnable d'agir ainsi compte tenu de circonstances exceptionnelles[77]. De cette manière, les États reconnaissent que, dans certains cas, l'intérêt général à la divulgation peut l'emporter sur la nécessité de préserver la confidentialité des informations. Les États parties pourront donc s'acquitter de l'obligation qui leur incombent en vertu du droit international relatif aux droits de l'homme de protéger la liberté d'expression et, en vertu de l'alinéa *d* du paragraphe 1 de l'article 13 de la Convention contre la corruption, de respecter, promouvoir et protéger la liberté de rechercher, de recevoir, de publier et de diffuser des informations concernant la corruption.

[77] Dans des cas qui ne relevaient pas de la sécurité nationale, cette approche a été adoptée par le Royaume-Uni dans le *Public Interest Disclosure Act* (loi sur les révélations d'intérêt général) de 1999, à l'article 43 G) intitulé "Disclosure in other cases" (révélations dans d'autres cas). Voir également la note d'orientation sur la page Web du Commissariat à l'intégrité du secteur public du Canada, disponible à l'adresse: http://www.psic.gc.ca/fra/actes-reprehensibles.

b) *Protection des sources des journalistes*

Si la protection des personnes qui communiquent des informations et la préservation du droit des journalistes de protéger leurs sources sont des concepts différents, ceux-ci peuvent se recouper dans certaines situations. Il est de plus en plus considéré comme une bonne pratique (voire exigé par la Constitution de certains pays) de protéger les révélations aux médias comme l'une des voies de signalement des actes illicites. De nombreux pays prévoient une telle protection si l'acte répréhensible n'est pas dûment traité par une organisation ou par les autorités compétentes. Une fois les informations divulguées, un journaliste devrait avoir le droit et le devoir de protéger ses sources conformément aux normes et à la jurisprudence internationales relatives aux droits de l'homme. Dans l'affaire *Tillack* c. *Belgique*, la Cour européenne des droits de l'homme a souligné que le droit des journalistes de taire leurs sources n'était pas un "simple privilège qui leur serait accordé ou retiré" et qu'il s'agissait d'une des pierres angulaires de la liberté de la presse[78]. Il s'agit véritablement d'un outil supplémentaire dont l'État dispose pour veiller à ce que les personnes qui communiquent des informations et les membres du public puissent participer à la lutte contre la corruption en toute sécurité. À l'ère de la mondialisation économique, un journalisme d'enquête de qualité sur la corruption s'avère indispensable non seulement pour sensibiliser le public aux dangers et aux actes illicites, mais également pour servir de base à des actions efficaces et rapides de la part des gouvernements et des services de détection et de répression.

> "La corruption est aujourd'hui un phénomène éminemment complexe. Une affaire de corruption qui se produit sur le plan local peut prendre une dimension internationale car il suffit désormais d'appuyer sur un bouton pour envoyer de l'argent d'un pays à un autre. Le bureau d'une société basé dans un pays donné peut servir de couverture pour des opérations illicites dans le monde entier, les individus peuvent dissimuler leurs biens dans les méandres de mécanismes complexes…la liste des exemples est sans fin[79]."

Il est conseillé aux États parties de consulter le guide de l'ONUDC intitulé "*Informer sur la corruption — Un outil de référence pour les gouvernements et les journalistes*" pour obtenir de plus amples renseignements et prendre connaissance de ressources supplémentaires sur cet aspect important de la lutte contre la corruption[80].

C. Protection contre les traitements injustifiés

1. Risques encourus par les personnes qui communiquent des informations

Toutes les catégories de personnes qui communiquent des informations peuvent s'exposer à des risques personnels et professionnels lorsqu'elles signalent des actes de corruption ou coopèrent avec les autorités pour lutter contre des fraudes de toute sorte. Cela étant, certaines études montrent également qu'une personne sera prête à prendre des risques

[78] *Tillack* c. *Belgique*, Cour européenne des droits de l'homme (requête nº 20477/05, 27 novembre 2007).

[79] ONUDC, *Informer sur la corruption — Un outil de référence pour les gouvernements et les journalistes*, 2014, p. 1, disponible à l'adresse: http://www.unodc.org/unodc/fr/corruption/publications.html.

[80] Ibid.

si elle pense que son action fera une différence[81], et c'est précisément cette différence qui constitue un facteur décisif dans sa décision de coopérer ou non. Il est ressorti d'une étude consacrée au signalement d'abus commis en milieu professionnel dans le secteur privé que la crainte de représailles, telles que licenciement, harcèlement par des collègues ou restrictions en matière de conditions de travail et d'accès, est la principale raison pour laquelle des informateurs potentiels décident de garder le silence[82]. Ces deux aspects doivent être pris au sérieux et devraient être examinés.

Si toutes les personnes qui communiquent des informations ne pâtiront pas de leur geste, l'expérience montre que, trop souvent, ces personnes subissent de lourdes représailles et sont soumises à un traitement injuste, qui peuvent avoir de graves répercussions sur leur vie et leurs moyens de subsistance, voire sur leur famille, leurs amis et leurs collègues. De telles situations ont un effet dissuasif sur d'autres personnes qui, sans cela, auraient envisagé de signaler des cas de corruption, mais décident finalement que le risque n'en vaut pas la peine. Par conséquent, les États parties doivent mûrement réfléchir aux mesures qu'ils peuvent prendre en droit et dans la pratique afin de permettre aux membres du public, aux agents publics et aux employés d'autres organisations de parler en toute sécurité. Il est également important de veiller à protéger les personnes qui communiquent des informations et leurs proches contre le harcèlement physique et d'autres menaces pesant sur leur bien-être.

Une étude réalisée par la Columbia Business School de l'Université de Columbia a analysé des données empiriques issues d'une expérience de laboratoire sur la propension à signaler des mensonges et sur les conséquences d'un tel signalement[83]. Il est ressorti de cette étude que tant que les groupes restaient inchangés, suffisamment d'individus se disaient prêts à dénoncer des mensonges, de sorte qu'il ne servait à rien de mentir. Or, lorsque les groupes ont pu choisir leurs membres, la donne a changé: les individus qui avaient signalé des mensonges se retrouvaient généralement mis à l'écart, même par des groupes où personne n'avait menti. Selon les auteurs de l'étude:

> Il s'agit là d'une constatation importante car elle donne à entendre que le signalement des actes malhonnêtes coûte très cher dans la mesure où les personnes qui les dénoncent peuvent être ostracisées, même par des organisations où prévaut l'honnêteté. Cela permet d'expliquer les piètres carrières des employés qui sont des lanceurs d'alerte, et exige de faire preuve de prudence en ce qui concerne la politique consistant à révéler l'identité des lanceurs d'alerte. Comme nous l'avons relevé, éviter les personnes qui communiquent des informations est une attitude propre aux individus [peu enclins à mentir] qui sont généralement honnêtes mais savent qu'ils pourraient être tentés de mentir. […] Des individus honnêtes pourraient préférer quitter leur travail plutôt que de dénoncer des collègues, ou se faire licencier avant d'avoir eu la possibilité de signaler des mensonges, ce qui pourrait générer davantage de malhonnêteté.

Afin d'inspirer de nouvelles réformes et décisions, il serait intéressant et fort utile de mener davantage de recherches dans ce domaine, y compris sur la façon dont le public perçoit les personnes qui communiquent des informations, sur les effets des modifications apportées à la politique et à la législation, ainsi que sur des analyses d'exemples de cas.

---

[81] Par exemple, aux États-Unis, des enquêtes réalisées auprès d'employés fédéraux dans les années 80 ont montré à maintes reprises que la crainte de représailles n'est que la deuxième raison pour laquelle quelque 500 000 employés choisissent de ne pas dénoncer des abus, la première raison étant qu'ils pensent que "rien ne sera fait pour remédier à la situation". Voir T. Devine, "Whistleblowing in the United States: The gap between vision and lessons learned", in *Whistleblowing Around the World*, Dehn, G. et R. Calland (dir. publ.), Londres, British Council, 2004, p. 81.

[82] Miceli, M. P. et J. P. Near, "What makes whistleblowers effective?", *Human Relations*, volume 55, nº 4, 2002; US National Business Ethics Survey, "Retaliation: The cost to your company and its employees", 2009.

[83] Ernesto Reuben et Matt Stephenson, "Nobody likes a rat: On the willingness to report lies and the consequences thereof", *Journal of Economic Behavior & Organization*, volume 93, 2013, p. 384 à 391.

Les traitements injustifiés ou représailles peuvent prendre, sans s'y limiter, les formes suivantes:

- Mesures coercitives, d'intimidation ou de harcèlement à l'encontre de la personne qui communique des informations ou de ses proches;
- Discrimination, désavantage ou traitement injuste;
- Dommages corporels ou autres infractions passibles de la peine capitale;
- Dommage matériel;
- Menace de représailles;
- Suspension, mise à pied ou licenciement;
- Rétrogradation ou perte de la possibilité d'obtenir une promotion;
- Transfert de fonctions, mutation, diminution du salaire ou modification des horaires de travail;
- Imposition de mesures disciplinaires, de blâmes ou de toute autre sanction (dont sanction pécuniaire);
- Mise à l'index (accord formel ou informel passé à l'échelle du secteur ou de la branche d'activité qui empêche un individu de trouver un autre emploi);
- Poursuites devant la justice civile ou pénale pour violation du secret, diffamation et calomnie.

2. Vue d'ensemble des divers moyens de protection

Le type de protection que nécessite une personne variera en fonction de la gravité des informations qu'elle a fournies, de l'individu à qui elle en a fait part et de la manière avec laquelle le signalement est traité. Certaines des mesures exposées ci-après permettent également de protéger la personne contre des actions que les individus visés par une enquête sur des actes illicites pourraient prendre à son encontre afin de détourner l'attention.

La liste ci-dessous n'est pas exhaustive et ne contient pas uniquement des mesures dites "de protection" au sens juridique du terme. Certaines d'entre elles sont des mesures pratiques dont il est démontré qu'elles ont une forte composante protectrice, tandis que d'autres relèvent de présomptions juridiques. Par exemple, le simple fait que des autorités compétentes soient tenues d'évaluer les informations qui leur sont communiquées et d'y donner suite peut être perçu comme une forme de protection dans la mesure où la responsabilité d'examiner la question ne repose plus sur les épaules de la personne qui a communiqué les informations, mais sur les autorités compétentes. Aux États-Unis, le chef de l'Office of the Whistleblower (bureau chargé des lanceurs d'alerte) de la Securities and Exchange Commission a également indiqué qu'un retour d'information rapide et régulier constitue un élément de "protection" important.

Les mesures visant à encourager les signalements et à fournir une protection une fois des informations révélées comprennent les éléments suivants:

- Cadre législatif et institutionnel clair;
- Existence de plusieurs voies de signalement;
- Accès à des informations et à des conseils objectifs;
- Acceptation de signalements anonymes;

- Garantie de confidentialité;
- Reconnaissance publique ou récompense;
- Protection physique;
- Protection contre la responsabilité civile ou pénale.

Parmi les mesures correctives proposées aux personnes victimes de représailles, on peut citer notamment les suivantes:

- Changement de superviseur ou redistribution des tâches sur le lieu de travail afin d'assurer sécurité et bien-être;
- Transfert provisoire ou permanent vers un poste offrant les mêmes responsabilités et le même salaire;
- Accès gratuit à un soutien psychologique ou à d'autres services de santé ou de protection sociale;
- Réintégration dans l'emploi précédent;
- Rétablissement d'un permis, d'une autorisation ou d'un contrat annulé;
- Sanction, transfert ou licenciement de toute personne dont il est établi qu'elle a infligé un traitement injuste ou exercé des représailles;
- Présomption de bonne foi;
- Présomption de détriment (à savoir renversement de la charge de la preuve);
- Indemnité pour représailles ayant force exécutoire (en Norvège, par exemple, une indemnité peut être réclamée indépendamment de la faute de l'employé);
- Indemnité pour pertes financières et perte de perspectives de carrière (au Royaume-Uni, il n'y a pas de limite à l'indemnité financière pour licenciement abusif);
- Octroi de dommages-intérêts pour la souffrance causée.

Si un dispositif de protection plus exceptionnel, tel qu'une protection policière, a tendance à être davantage associé à la protection des témoins ou à des procédures pénales afférentes à la criminalité organisée, il peut toutefois être nécessaire dans des affaires impliquant d'autres types d'actes délictueux et de corruption. Une personne qui communique des informations, un membre de sa famille ou un autre individu, comme un collègue, pourrait en avoir besoin, non pas parce que son témoignage est forcément nécessaire aux fins du procès, mais plutôt parce qu'ils sont la cible de graves représailles (voir ci-dessous, "Protection contre les menaces à l'intégrité physique", chapitre II, section C.8).

3. Mesures procédurales de protection visant à faciliter les signalements

En veillant à ce que les mécanismes de signalement soient accessibles, sûrs et sécurisés et que les informations communiquées soient traitées avec professionnalisme, on contribuera à empêcher tout traitement injustifié d'une personne ayant signalé des actes illicites. Ce sont les faits qui déterminent si les personnes accordent leur confiance au système et continuent à collaborer avec lui ou non.

L'importance de protéger l'identité des personnes qui communiquent des informations constitue un enjeu de taille. Dans le présent contexte, les personnes qui traitent les signalements doivent comprendre la différence entre confidentialité et anonymat.

Les différents types de signalements

Signalement ouvert

Signalement dans le cadre duquel un individu communique ou révèle ouvertement des informations, ou déclare ne pas exiger ou chercher à obtenir que son identité soit tenue secrète.

Signalement confidentiel

Signalement dans le cadre duquel le nom et l'identité de l'individu qui communique des informations sont connus de la personne qui reçoit le signalement, mais ne seront pas divulgués sans le consentement de l'intéressé, à moins que la loi ne l'exige.

Signalement anonyme

Signalement dans le cadre duquel la source des informations communiquées n'est pas connue.

a) *Confidentialité*

En matière de signalement, la sûreté et la sécurité sont des éléments essentiels d'un système visant à protéger les personnes qui communiquent des informations, et permettront d'entretenir une communication et une coopération avec celles-ci. Il est indispensable de bien faire les choses dès le début. En outre, les protections prévues par la loi doivent être assorties, dans la pratique, de systèmes et de procédures adaptés.

Le fait de proposer et d'offrir des garanties de confidentialité permettra de rassurer les personnes qui communiquent des informations et de s'assurer que l'accent reste mis sur le contenu plutôt que sur l'auteur du signalement. Par souci d'équité et pour maintenir la confiance, les limites de la confidentialité devraient être clairement expliquées en amont. Par exemple, il conviendrait d'expliquer qu'une garantie consistant à ne pas révéler l'identité d'une personne sans son consentement n'empêche pas que certains individus devinent qui pourrait être la source de l'information, ou que l'identité de la personne ayant communiqué l'information puisse être évidente en raison de l'information elle-même.

Un nombre croissant de lois destinées à protéger les personnes qui communiquent des informations imposent désormais aux autorités compétentes et aux autres personnes responsables l'obligation de maintenir la confidentialité de l'identité des auteurs de signalements, et de ne la révéler qu'avec le consentement éclairé des intéressés ou en exécution d'une décision judiciaire. Par exemple, conformément aux articles 1 et 8 du *Whistleblower Protection Act* de la Malaisie (loi sur la protection des lanceurs d'alerte), les agents qui recueillent un signalement ne doivent pas communiquer d'informations confidentielles, telles que: "*a)* des informations concernant l'identité, l'activité professionnelle, le lieu de résidence, le lieu de travail ou le lieu où se trouve i) un lanceur d'alerte; et ii) une personne qu'un lanceur d'alerte a dénoncée pour comportement répréhensible; *b)* des informations divulguées par un lanceur d'alerte; et *c)* des informations dont la divulgation pourrait causer un préjudice à toute personne".

En temps normal, la confidentialité est considérée comme le premier rempart dans la protection offerte aux personnes qui communiquent des informations. Si la confidentialité est assurée, il est alors possible qu'aucun autre mécanisme de protection ne soit nécessaire. Bien que cela puisse exiger plus de travail de la part de l'autorité concernée, il est essentiel de faire preuve de diligence à l'égard des procédures régissant le traitement

des informations et la protection des intérêts de la personne qui les communique. Dans la plupart des cas, les limites d'une garantie de confidentialité ne sont mises à l'épreuve que lorsqu'il apparaît clairement que l'affaire ne saurait être dûment traitée si la source originale de l'information ne participe pas au processus (par exemple, lorsque le témoignage d'une personne qui communique des informations peut être nécessaire afin d'ouvrir une enquête ou engager des poursuites pénales). Dans pareil cas, il faudrait avant toute autre chose obtenir le consentement éclairé de l'intéressé ou une décision judiciaire. Le fait que la plupart des personnes signalent un acte illicite afin que des mesures correctives soient prises à cet égard signifie que, dans beaucoup de cas, il est possible d'obtenir leur coopération en leur expliquant clairement pourquoi celle-ci est nécessaire et en leur donnant des garanties solides en ce qui concerne leur propre situation.

En règle générale, les preuves émanant de sources qui ne souhaitent pas que leur identité soit communiquée sont difficilement recevables à un procès pénal en raison du droit à un procès équitable dont jouissent les accusés. Toutefois, même lorsqu'il peut être nécessaire de révéler à la défense l'identité d'une personne qui a communiqué des informations et qui apporte son témoignage à ce titre, cette dernière pourrait avoir droit aux mesures de protection des témoins requises à l'article 32 de la Convention contre la corruption. Comme il a déjà été mentionné dans le présent Guide, la protection des lanceurs d'alerte et la protection des témoins peuvent comporter des éléments communs (voir aussi chapitre II, section C.4 à ce sujet). Les mesures de protection des témoins peuvent comprendre la protection de l'identité d'un lanceur d'alerte au cours d'un procès grâce à des moyens techniques[84].

Des efforts ont été déployés pour mettre en balance les droits de l'accusé avec les intérêts et le bien-être des témoins et des victimes. En l'affaire *Doorson*, la Cour européenne des droits de l'homme a expliqué ce qui suit:

> […] l'article 6 [de la Convention européenne des droits de l'homme] ne requiert pas explicitement que les intérêts des témoins en général, et ceux des victimes appelées à déposer en particulier, soient pris en considération. Toutefois, il peut y aller de leur vie, de leur liberté ou de leur sûreté, comme d'intérêts relevant, d'une manière générale, du domaine de l'article 8 […] de la Convention. Pareils intérêts des témoins et des victimes sont en principe protégés par d'autres dispositions, normatives, de la Convention, qui impliquent que les États contractants organisent leur procédure pénale de manière que lesdits intérêts ne soient pas indûment mis en péril. Cela posé, les principes du procès équitable commandent également que, dans les cas appropriés, les intérêts de la défense soient mis en balance avec ceux des témoins ou des victimes appelés à déposer[85].

Dans l'arrêt *Doorson*, la Cour a également relevé que, même là où des procédures faisant contrepoids (par exemple, le témoin est interrogé par un juge d'instruction en présence des deux conseils mais en l'absence du prévenu) sont jugées compenser de manière suffisante les obstacles auxquels se heurte la défense, une condamnation pénale ne peut se fonder uniquement, ni dans une mesure déterminante, sur des déclarations anonymes.

b) *Signalement anonyme*

Il ne faudrait pas confondre le principe de confidentialité avec l'anonymat, situation dans laquelle nul ne connaît la source de l'information.

---

[84] ONUDC, *Bonnes pratiques de protection des témoins dans les procédures pénales afférentes à la criminalité organisée*, disponible à l'adresse: https://www.unodc.org/documents/organized-crime/09-80620_F_ebook.pdf.

[85] Le précédent de la CEDH faisant autorité en la matière est l'Arrêt rendu le 26 mars 1996 dans l'affaire *Doorson* c. *Pays-Bas*, Requête nº 20524/92, Recueil 1996-11, par. 70 et 76. Voir aussi: ONUDC, *Bonnes pratiques de protection des témoins dans les procédures pénales afférentes à la criminalité organisée*, p. 31 et suiv.

Dans la pratique, lorsque la source de l'information est inconnue de tous, il s'ensuit, du moins à court terme, que cette source peut difficilement être la cible de représailles. Le paragraphe 2 de l'article 13 de la Convention contre la corruption exige des États parties, lorsqu'il y a lieu, de faire en sorte que les organes de prévention de la corruption soient accessibles au grand public afin qu'il puisse signaler une infraction, y compris sous couvert d'anonymat. En Australie, le récent *Public Interest Disclosure Act* de 2013 (loi sur les révélations d'intérêt général) indique clairement qu'une révélation d'intérêt général peut être faite oralement ou par écrit, ainsi que sous couvert d'anonymat. Cette loi prévoit également qu'un individu peut révéler des informations sans déclarer qu'il le fait en vertu de cette loi[86].

Un aspect positif est que ces systèmes de signalement permettent aux personnes qui ne leur font pas confiance, ou pensent que leur signalement ne sera pas traité avec sérieux, de dénoncer quand même des actes délictueux si elles ont la possibilité de conserver l'anonymat.

L'aspect négatif est que l'anonymat pose certaines difficultés pour enquêter sur des actes illicites, en particulier parce qu'il est plus difficile d'obtenir des précisions supplémentaires et d'évaluer la crédibilité de l'information fournie sans en connaître la source (de nouveaux outils permettent de remédier à ces difficultés, tels que des systèmes mandataires de messagerie électronique autorisant une communication à double sens). Dès lors, il peut se révéler plus compliqué pour des autorités de prendre des mesures sur la base d'une information anonyme. D'aucuns craignent également que le signalement anonyme ne donne lieu à davantage de signalements ou à des signalements motivés par des fins personnelles.

Cela dit, de nombreux pays disposent d'une permanence téléphonique permettant d'effectuer des signalements, et certains, comme la Bosnie-Herzégovine, ont désormais des systèmes en ligne qui facilitent une communication à double sens. Pour illustrer l'efficacité des signalements anonymes, le Ministère de la défense de la Bosnie-Herzégovine a déclaré avoir reçu 28 signalements anonymes faisant état d'actes illicites au sein du Ministère et des forces armées, et ce en l'espace de quatre mois (de décembre 2013 à mars 2014). Des enquêtes ont été menées à terme dans 19 affaires et suffisamment de preuves ont été réunies pour que 3 affaires fassent l'objet d'une procédure plus poussée. Une affaire qui avait été confiée à des enquêteurs portait sur l'acceptation d'une somme d'argent en échange de l'admission dans les forces armées. Ces 28 signalements portaient sur des pratiques abusives (8); des irrégularités en matière de personnel et de recrutement (7); des violations de procédures internes (4); des cas de corruption (3); des irrégularités financières et comptables (1); des irrégularités en matière de passation de marchés (1); un vol (1); un discours haineux (1) et d'autres actes illicites (2)[87].

Au Mexique, par exemple, la Dirección General de Atención Ciudadana (direction générale des services aux citoyens) gère des bureaux spécialisés et des centres d'appels, et utilise des outils technologiques, tels que des courriers électroniques et des applications Web, pour recevoir des signalements de corruption[88].

[86]Australie, *Public Interest Disclosure Act*, 2013, art. 28, disponible à l'adresse: http://www.comlaw.gov.au/ Details/C2013A00133.

[87]Omeragić, Daniel, "Etička linija MOBiH: Među prijavljenim i general Milojčić", *Oslobodjenje*, 25 mars 2014, disponible à l'adresse: www.oslobodjenje.ba/vijesti/bih/eticka-linija-mobih-medju-prijavljenim-i-general-milojcic.

[88]Chevarria, F. et M. Silvestre, Sistemas de denuncias y de protección de denunciantes de corrupción en América Latina y Europa, Documento de Trabajo nº 2, Serie: Análisis, Área: Institucionalidad Democrática, Eurosocial, Madrid, 2013, p. 37, disponible à l'adresse: http://sia.eurosocial-ii.eu/files/docs/1400663798-DT2.pdf.

Exemple: Service en ligne anonyme géré par des procureurs spécialisés (Autriche)

Au printemps 2013, une plateforme de signalement en ligne a été lancée en Autriche pendant une période d'essai de deux ans afin de permettre au public de dénoncer des actes de corruption et des infractions pénales connexes. Cette plateforme est gérée par le Ministère public chargé de la criminalité en col blanc et de la corruption (WKStA). Le système de signalement sur le Web utilise une technologie qui assure l'anonymat (les autorités ne peuvent retrouver aucune donnée d'identification à l'aide du système), tout en permettant une communication à double sens.

Ce service en ligne n'enregistre que les signalements portant sur les infractions pénales dans les domaines suivants: *a)* corruption; *b)* criminalité économique; *c)* fraude sociale; *d)* criminalité financière; *e)* fraude comptable; *f)* criminalité liée aux marchés financiers; et *g)* blanchiment d'argent.

En l'espace d'une année, 1 200 signalements ont été effectués, avec les résultats suivants:

- 5% des signalements relevaient de la compétence du WKStA;
- 32% des signalements étaient du ressort d'autres ministères publics et leur ont été transférés;
- 26% des signalements ont été transférés à des autorités financières; 29% n'ont pas fait l'objet d'une procédure plus poussée, à savoir l'ouverture d'une procédure (pénale); et 6% ont atteint le seuil minimal pour être examinés.

À ce jour, il n'y a que peu d'informations, voire aucune, indiquant combien de ces signalements ont abouti à une enquête approfondie ou à des poursuites.

Source: Exposé présenté par le Bureau fédéral autrichien de lutte contre la corruption (BAK) à l'Académie internationale de lutte contre la corruption, Vienne, septembre 2014.

Toutefois, l'expérience montre que même avec une technologie garantissant l'anonymat, des individus peuvent involontairement révéler des informations qui permettent de les identifier comme les personnes ayant effectué le signalement. L'autorité qui reçoit les signalements doit veiller à ce que les utilisateurs du système comprennent ses limites. Il est tout aussi important d'avoir conscience que les personnes qui communiquent des informations ne voudront pas toutes conserver l'anonymat ou n'en auront pas toutes besoin.

Par conséquent, la question de savoir comment intégrer des outils de signalement anonyme dans un système visant à assister et à protéger les personnes qui communiquent des informations devrait être soigneusement examinée et abordée avec les principales parties prenantes. Les deux types de systèmes de signalement (confidentiel et anonyme) sont déjà utilisés dans maintes juridictions qui les considèrent comme des outils précieux pour recueillir des informations. Leur efficacité en termes de protection des personnes qui communiquent des informations est moins bien comprise. Dans certains pays, les signalements anonymes continuent à susciter des controverses et il se peut qu'à long terme ce mode de signalement mette en péril l'obligation interne et externe de rendre des comptes.

Voici certains des problèmes liés à la responsabilité et à l'obligation de rendre des comptes en cas d'anonymat qu'il conviendra d'étudier au moment d'établir des systèmes de signalement:

- Bien que le mode de signalement choisi (par exemple, sous enveloppe ou au moyen d'un service en ligne crypté) puisse protéger l'identité de la source de

l'information, cela ne signifie pas pour autant que l'identité ne pourra être déduite ou devinée à partir de l'information elle-même.

- Les informations fournies par des sources anonymes ne sont que rarement considérées comme des preuves recevables devant des tribunaux (voir ci-après).
- Lorsqu'une divulgation est anonyme, il se peut qu'une tierce personne soit suspectée d'en être à l'origine et qu'elle en subisse les conséquences.
- Les systèmes de signalement anonyme ont suscité des préoccupations quant à la collecte loyale des données à caractère personnel, en particulier au sein des autorités européennes de protection des données, ce qui a entraîné l'imposition de conditions supplémentaires aux compagnies qui gèrent des permanences téléphoniques/services en ligne, par exemple, en ajoutant des règles visant à limiter la durée de conservation de telles informations[89].
- Des travaux de recherche indiquent que les personnes qui reçoivent des informations d'une source anonyme leur attribuent une crédibilité moindre et leur allouent moins de ressources à des fins d'enquête[90].
- Les alertes lancées sous couvert d'anonymat restent étroitement associées à la pratique de la délation (souvent concernant des voisins) qui existait ou existe sous des régimes totalitaires, ou aux informateurs malveillants qui communiquent des renseignements sur des opposants politiques.
- Si les systèmes de signalement ne disposent pas de fonctionnalités avancées, l'anonymat ne permet pas de rester en contact avec le lanceur d'alerte, d'obtenir des précisions ou de plus amples informations, de le rassurer sur sa situation ou de le tenir informé de la suite donnée à son signalement[91].
- Les systèmes de signalement anonyme peuvent toutefois permettre d'obtenir des informations précieuses (pistes d'enquête et analyses de cas de corruption).
- Des voies de communication indirectes (par des systèmes mandataires) peuvent être utilisées pour encourager un lanceur d'alerte anonyme à se manifester ultérieurement si son signalement devait être produit en tant que preuve.

La question de la protection de l'identité d'une personne qui communique des informations peut également se poser dans le contexte d'une procédure disciplinaire interne eu égard au principe de justice naturelle selon lequel les personnes accusées de corruption

[89] Groupe de travail "ARTICLE 29" sur la protection des données, Avis 1/2006 relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière, WP 117, 2006.

[90] Hunton, J. E. et J. M. Rose, "Effects of Anonymous Whistleblowing and Perceived Reputation Threats on Investigations of Whistleblowing Allegations by Audit Committee Members", *Journal of Management Studies*, volume 48, nº 1, 2011.

[91] Stephenson, P. et Michael Levi, La protection des donneurs d'alerte — Rapport d'étude sur la faisabilité d'un instrument juridique sur la protection des employés qui divulguent des informations dans l'intérêt public, commandité par le Conseil de l'Europe à la demande du Comité européen de coopération juridique, CDCJ(2012)9FIN, 2012.

ont droit à ce que leur cause soit entendue de manière équitable. Au Royaume-Uni, l'affaire *Linfood Cash and Carry Ltd* c. *Thompson* a posé des principes directeurs de base sur la manière de maintenir un juste équilibre entre les droits des témoins et ceux des personnes accusées d'avoir commis des irrégularités[92].

c) *Modes de signalement*

À bien des égards, l'apparition de nouvelles technologies (ordinateurs, messageries électroniques, SMS, téléphones intelligents et applications pour appareils mobiles) a changé la façon dont les individus communiquent entre eux ainsi qu'avec les pouvoirs publics à l'échelon local et national. Il est aujourd'hui possible d'échanger des informations et des données en plus grandes quantités et plus rapidement que jamais.

Il existe de nombreux exemples de la manière dont les nouvelles technologies facilitent les signalements et contribuent à offrir des "espaces sûrs" aux personnes qui communiquent directement avec les autorités. Cependant, ces systèmes de communication ne diffèrent en rien des autres outils: il demeure indispensable que les personnes qui les mettent en œuvre soient formées comme il se doit au traitement des informations et soutiennent en toute impartialité et avec professionnalisme les personnes qui communiquent des informations. Si les attentes en matière de protection ne sont pas satisfaites ou que l'information n'est pas traitée convenablement, les usagers perdront confiance dans ces systèmes, comme dans tout autre, et les personnes à qui ces systèmes s'adressent cesseront de les utiliser. Cela posé, dans certains pays où la population n'a pas accès à certaines technologies ou à des réseaux de téléphonie mobile, d'autres méthodes visant à faciliter les signalements doivent être utilisées.

Des organisations, telles que Hermes Center for Transparency and Digital Human Rights et bien d'autres encore dans le monde (voir l'exemple ci-dessous), s'appuient sur la technologie et utilisent des programmes libres comme GlobaLeaks pour encourager la participation du public. Des gouvernements se mettent aussi à utiliser de tels outils[93]. Parmi les dizaines d'organisations qui emploient des outils cryptés de signalement en ligne afin de permettre la transmission anonyme d'informations et de documents figurent Organised Crime and Corruption Reporting Project, International Consortium of Investigative Journalists, 100Reporters, Balkan Investigative Reporting Network, AfriLEAKS et Méxicoleaks.

---

[92] En l'affaire *Linfood Cash and Carry Ltd* c. *Thompson* (IRLR 235, 1989), l'Employment Appeals Tribunal (la Cour d'appel britannique pour les conflits du travail) a énuméré 10 étapes à suivre:

1. Limiter les informations fournies lors d'un signalement à une ou plusieurs déclarations écrites;
2. Veiller à ce que les informations importantes, la date et l'heure de chaque incident, etc., soient consignées, et indiquer si l'accusé a causé des torts à la personne qui l'a dénoncé;
3. Mener une enquête plus poussée pour confirmer ou infirmer les informations;
4. Mener des enquêtes en faisant preuve de tact afin de vérifier la crédibilité de l'informateur;
5. Confirmer le point de savoir si la personne qui a communiqué les informations est prête à assister à une audience disciplinaire. Si elle refuse et que ses craintes sont légitimes, décider s'il convient de continuer ou non;
6. Si la décision de continuer est prise, le responsable de l'audience devrait interroger la personne qui a communiqué des informations et déterminer le poids à leur accorder;
7. Mettre les déclarations à la disposition de l'accusé, au besoin dans leur version expurgée afin de protéger les identités concernées;
8. Si l'accusé soulève des questions pertinentes, le responsable de l'enquête les soumet à la personne qui a communiqué les informations;
9. Prendre des notes complètes et détaillées de tous les actes de la procédure;
10. Dans la mesure du possible, les preuves qu'un enquêteur a relevées lors d'une audience devraient être consignées sous forme écrite.

[93] Pour savoir comment des services étatiques, des sociétés ainsi que des ONG utilisent l'application libre de GlobaLeaks, voir: http://logioshermes.org/home/projects-technologies/globaleaks/.

Exemple: L'Inde

Janaagraha est une organisation à but non lucratif basée à Bangalore et créée en 2001 qui a décidé de recourir à la technologie et à la production participative pour en savoir plus sur la corruption locale. Comme elle l'indique dans son rapport annuel pour 2012-2013, ce qui a commencé par une tentative non dénuée d'ironie visant à révéler le prix du marché de la corruption est aujourd'hui devenu une innovation internationalement reconnue. Lancé en 2010, le site Web "I Paid a Bribe" (j'ai versé un pot-de-vin) avait déjà reçu 22 000 signalements de pot-de-vin en 2013 en provenance de 493 villes indiennes. Au départ simple mécanisme anonyme de "signalement", ce site s'est aussi progressivement transformé en un outil favorisant la participation active des citoyens. Début 2013, sa politique de confidentialité a été actualisée afin de permettre aux utilisateurs de communiquer leur nom s'ils le souhaitent au moment d'effectuer un signalement. En outre, les noms des fonctionnaires et départements concernés par des signalements ne sont plus expurgés afin de rendre cette plateforme plus transparente et de permettre aux autorités de prendre des mesures, obligeant ainsi le secteur public à rendre davantage de comptes. De surcroît, Janaagraha commence à adapter ce site Web pour qu'il réponde aux besoins de ses différents publics. En 2013, un service en ligne appelé "Bribe Hotline" a été mis en place pour que les utilisateurs puissent poser des questions sur les procédures administratives à des agents et responsables de services étatiques.

Source: www.ipaidabribe.com.

4. Mesures de protection sur le lieu de travail

Si la protection contre des traitements injustifiés sur le lieu de travail est habituellement liée aux actes de l'employeur (à savoir un supérieur hiérarchique de la personne qui communique des informations), cela n'est pas toujours le cas. Par conséquent, il est raisonnable et avisé de faire en sorte que la responsabilité de l'employeur en matière de protection s'applique également aux actes de représailles commis par des collègues de travail (comme le prévoit la législation aux Pays-Bas et au Royaume-Uni)[94].

Il peut également être raisonnable de veiller à ce que la responsabilité des employeurs couvre les représailles commises par des tiers qui sont liés à l'employeur, comme le prévoient le Luxembourg dans la loi de 2011 renforçant les moyens de lutte contre la corruption[95] et l'Irlande dans le *Protected Disclosures Act* de 2014 (loi sur les révélations protégées)[96].

Dans la pratique, l'efficacité des mesures de protection prévues par la loi dépend généralement de la manière dont elles sont respectées et ancrées dans les obligations des organisations et les règlements et procédures des organismes d'enquête, ainsi que de la facilité avec laquelle les personnes qui communiquent des informations peuvent faire

[94]Pour les Pays-Bas, voir Stephenson et Levi, *Rapport d'étude sur la faisabilité d'un instrument juridique sur la protection des employés qui divulguent des informations dans l'intérêt public*, 2012, par. 3.23, disponible à l'adresse: http://www.coe.int/t/dghl/standardsetting/cdcj/Whistleblowers/CDCJ(2012)9F_Final.pdf.

Pour le Royaume-Uni, voir les articles 17 à 20 du *Enterprise and Regulatory Reform Act* de 2013 (loi sur les entreprises et la réforme réglementaire) portant modification du *Public Interest Disclosure Act* (loi sur les révélations d'intérêt général), 1998. L'article 19 prévoit des mesures de protection pour que les lanceurs d'alerte ne soient pas intimidés ou harcelés par leurs collègues de travail. Voir: http://www.legislation.gov.uk/ ukpga/2013/24/part/2/crossheading/ protected-disclosures/enacted.

[95]Luxembourg, Loi du 13 février 2011 renforçant les moyens de lutte contre la corruption et portant modification 1) du Code du Travail; 2) de la loi modifiée du 16 avril 1979 fixant le statut des fonctionnaires de l'État; 3) de la loi modifiée du 24 décembre 1985 fixant le statut général des fonctionnaires communaux; 4) du Code d'instruction criminelle et; 5) du Code pénal, disponible à l'adresse: http://www.legilux.public.lu/leg/a/ archives/2011/0032/index.html.

[96]Irlande, *Protected Disclosures Act*, 2014, art. 12-1.

valoir leurs droits. À cette fin, des mesures aussi bien préventives que rétroactives sont nécessaires. Les mesures préventives consistent notamment à mettre en place des procédures organisationnelles et des systèmes de signalement solides, et à cerner et gérer les risques auxquels une personne qui communique des informations s'expose dès le moment où elle se manifeste. Quant aux mesures rétroactives, elles visent à réparer un préjudice (par exemple en réintégrant l'employé ou en l'indemnisant) lorsque des mesures de protection n'ont pas été correctement mises en œuvre ou n'étaient pas disponibles.

Par exemple, en Australie, la législation fédérale et du territoire de la capitale impose expressément à tous les organismes publics d'établir des procédures visant à évaluer le risque que des représailles soient commises contre des personnes qui révèlent des informations[97]. Une ONG britannique spécialisée, Public Concern at Work, a mis sur pied une commission chargée d'examiner l'état actuel des alertes lancées au Royaume-Uni. Cette commission a recommandé au Gouvernement britannique d'adopter un code de bonnes pratiques à l'intention de tous les employeurs. Il ne s'agirait pas d'un code ayant valeur de loi mais plutôt d'un cadre dont les juridictions devraient tenir compte lorsqu'elles tranchent des questions relatives à l'octroi d'une réparation en faveur de toute personne ayant été victime d'un traitement injuste de la part de son employeur du fait qu'elle a donné l'alerte[98].

Droit de désobéir

Le droit d'une personne de refuser d'obéir à un ordre illégal est un principe relativement bien établi au sein de la fonction publique. En vertu de ce droit, les fonctionnaires peuvent et devraient signaler tout aspect ou tout ordre qu'ils estiment incompatible avec leur devoir de faire respecter la loi, et devraient donner l'alerte s'ils pensent que l'exécution d'un ordre est contraire à la loi. Il n'en reste pas moins que dans d'autres contextes, comme dans le secteur privé en règle générale, un individu qui refuse d'obéir à un ordre au motif qu'il serait illégal de le suivre n'est guère protégé contre le risque de se voir imposer une sanction, et devra donc assumer les conséquences de son refus. Un mécanisme permettant de refuser de suivre un ordre et de chercher à obtenir rapidement l'avis d'un supérieur ou d'une autorité compétente sur la légalité de l'ordre en question constitue un puissant outil de prévention de la corruption et d'autres actes illicites, qui peut empêcher purement et simplement la commission de l'infraction même.

Indemnisation

Il pourrait être utopique d'attendre d'un employé qu'il continue à travailler pour un supérieur ou un employeur, ou encore avec des collègues, qui ont exercé des représailles à son encontre. Dans de tels cas de figure, il faudrait peut-être donner à cet employé la possibilité d'être transféré dans un autre service ou bureau afin qu'il ait véritablement une chance de prendre un nouveau départ.

En Slovénie, par exemple, la loi prévoit que toute personne victime de représailles ou de conséquences préjudiciables peut exiger une indemnisation à son employeur. La Commission slovène de lutte contre la corruption peut aider la personne qui communique des informations à établir le lien de causalité entre le signalement et toutes mesures de

[97] Commonwealth d'Australie, *Public Interest Disclosure Act* de 2013 (loi sur les révélations d'intérêt général), art. 59-1. Voir aussi le *Public Interest Disclosure Act* de 2012, art. 33 2). Voir Brown, A. J., "Towards "ideal" whistleblowing legislation? Some lessons from recent Australian experience", *E-Journal of International and Comparative Labour Studies*, volume 2, nº 3, septembre/octobre 2013, p. 153 à 182.

[98] Public Concern at Work, *The Whistleblowing Commission: Report on the effectiveness of existing arrangements for workplace whistleblowing in the UK*, PCaW, Londres, 2013. La commission était dirigée par Sir Anthony Hooper et comprenait des représentants d'entreprises, de syndicats, de la profession juridique, de l'Église d'Angleterre et des lanceurs d'alerte. Disponible à l'adresse: http://www.pcaw.org.uk/whistleblowing-commission.

représailles, et peut enjoindre à l'employeur de mettre immédiatement un terme à ces mesures ou de transférer l'employé qui a effectué le signalement vers un autre poste aux fonctions équivalentes[99]. Nombre d'organismes spécialisés dans la lutte contre la corruption et dans les alertes sont investis de pouvoirs similaires.

Même lorsqu'une autorité n'a pas le pouvoir d'indemniser un individu pour un préjudice subi, des organismes de contrôle peuvent prendre des mesures punitives à l'encontre d'une organisation qui ne facilite pas les dénonciations internes, ou tente d'empêcher une dénonciation ou d'user de représailles contre un lanceur d'alerte.

Exemple: Office of Special Counsel (États-Unis)

L'Office of Special Counsel des États-Unis (bureau du conseil spécial) est un organisme fédéral indépendant chargé d'enquêter et d'engager des poursuites. Il tire ses pouvoirs de quatre lois fédérales: *Civil Service Reform Act* (loi sur la réforme de la fonction publique), *Whistleblower Protection Act* (loi sur la protection des lanceurs d'alerte), *Hatch Act* (loi Hatch) et *Uniformed Services Employment and Reemployment Rights Act* (loi sur les droits en matière d'emploi et de réintégration professionnelle pour les services en uniforme).

Ce bureau reçoit des allégations de pratiques interdites en matière de personnel, mène des enquêtes à leur sujet et engage des poursuites, en accordant une attention particulière à la protection des lanceurs d'alerte du Gouvernement fédéral. Il s'efforce d'obtenir des mesures correctives et des réparations (comme une indemnisation et une réintégration professionnelle) pour les préjudices subis par des lanceurs d'alerte et d'autres plaignants, et est habilité à déposer des plaintes auprès du Merit Systems Protection Board (conseil qui supervise les promotions dans la fonction publique) afin qu'une procédure disciplinaire soit engagée contre ceux qui se livrent à des pratiques interdites en matière de personnel. Ce bureau offre un mode alternatif de règlement des litiges, une forme de médiation, pour donner aux parties la possibilité de résoudre leur différend sans passer par une enquête longue ou coûteuse. La médiation est un processus volontaire mené par un médiateur indépendant qui ne jouit d'aucun pouvoir décisionnel formel. C'est aux parties qu'il appartient de prendre une décision définitive.

L'Office of Special Counsel fournit également une voie de communication protégée grâce à sa Disclosure Unit (unité chargée des signalements), qui permet aux employés fédéraux de communiquer des informations concernant diverses pratiques professionnelles abusives, y compris des violations de la législation et de la réglementation, de graves erreurs de gestion et des gaspillages flagrants de fonds, des abus de pouvoir ou une menace grave pour la santé ou la sécurité publiques.

5. Protection contre la responsabilité civile ou pénale

Des questions de diffamation et calomnie peuvent se poser lorsque des informations sont communiquées à des tiers ou, plus généralement, rendues publiques. Pour cette raison, les États parties devraient envisager d'édicter des règles disposant très clairement que les personnes qui ont communiqué des informations à des autorités compétentes bénéficient d'une protection. La protection des droits individuels à un procès équitable et, dans certains cas, la protection contre une atteinte à la réputation peuvent être considérées comme une raison légitime de restreindre la liberté d'expression. Toutefois, il est important de veiller à ce que les personnes qui communiquent des informations ne soient

[99] Slovénie, *Integrity and Prevention of Corruption Act* (loi sur l'intégrité et la prévention de la corruption), 2010, art. 25.

pas injustement prises pour cible alors qu'elles ont signalé des soupçons d'irrégularités ou de corruption conformément au système en place.

Afin de lever toute ambiguïté à cet égard, certains États ont expressément adopté des dispositions législatives pour que la responsabilité civile et pénale des personnes qui communiquent des informations ne puisse être mise en cause en cas de révélations protégées. En Irlande, la loi sur la diffamation a été modifiée pour conférer une immunité relative en cas de révélations protégées[100]. De surcroît, lorsque des poursuites sont engagées pour infraction à une interdiction ou à une restriction dont est frappée la révélation d'une information, l'accusé peut se défendre en démontrant que sa révélation est protégée, ou qu'il a des motifs raisonnables de croire qu'elle l'est[101].

Exemple: L'Australie

Le *Public Interest Disclosures Act* de 2013 (loi sur les révélations d'intérêt général) protège les lanceurs d'alerte de la fonction publique fédérale et leur confère une immunité contre toute responsabilité civile, pénale ou administrative (y compris contre une procédure disciplinaire) lorsqu'ils ont révélé des informations d'intérêt général, et interdit l'exercice de tout droit ou recours d'ordre contractuel ou autre à l'encontre d'une personne ayant révélé de telles informations. Les personnes qui font des révélations d'intérêt général jouissent d'une immunité absolue contre les actions en diffamation et il ne peut être mis fin à un contrat au motif qu'une révélation d'intérêt général a été faite. Il existe des exceptions, notamment si une personne donne délibérément des informations fausses ou trompeuses, ou si en faisant des révélations en dehors du cadre interne elle enfreint toute restriction en matière de publication, et ce pour autant que la personne ait eu connaissance de cette restriction et qu'elle ne soit pas capable de fournir une bonne raison à ses révélations. La loi dispose que "[p]our prévenir toute ambiguïté, la question de savoir si la révélation faite par un individu au sujet de son propre comportement relève d'une révélation d'intérêt général n'a aucune incidence sur le fait qu'il doit répondre de son comportement".

6. Interdiction des actes visant à empêcher les révélations et des clauses visant à imposer le silence

Les clauses stipulées dans les accords de compromis ou de règlement conclus dans certains pays, qui visent à empêcher les employés de signaler toute irrégularité en dehors du cadre professionnel, suscitent des préoccupations. Elles peuvent être considérées comme particulièrement problématiques dans le domaine de la lutte contre la corruption. La difficulté tient en partie à la formulation vague de ces clauses et à l'absence d'explications indiquant que lesdites clauses ne s'appliquent pas aux informations concernant des irrégularités ou des fraudes. Au Royaume-Uni, le National Audit Office (bureau d'audit national) a déclaré: "À l'heure où les finances publiques sont soumises à une pression constante et les services sont de plus en plus fournis dans des conditions normales de concurrence, il est important que les accords de compromis ne donnent pas aux membres du personnel l'impression d'être muselés, ou ne récompensent pas les manquements d'un employé ou d'une organisation[102]".

Il existe d'autres exemples de clauses imposant le silence dans des contrats de travail et dans certaines lois limitant le droit des individus de communiquer des informations

[100] Irlande, *Protected Disclosures Act*, 2014, art. 14.

[101] Irlande, *Protected Disclosures Act*, 2014, art. 15.

[102] Public Concern at Work, *The Whistleblowing Commission: Report on the effectiveness of existing arrangements for workplace whistleblowing in the UK*, PCaW, Londres, 2013, disponible à l'adresse: http://www.pcaw.org.uk/whistleblowing-commission.

sur des pratiques opérationnelles propres à une branche ou à un secteur d'activité particulier. Les États parties doivent faire preuve de vigilance à l'égard de telles dispositions afin de s'assurer qu'elles ne compromettent pas leur capacité de lutter efficacement contre la corruption et de protéger l'intérêt général ainsi que les personnes qui communiquent des informations. Une modification a été apportée à la législation néo-zélandaise en 2009 afin de résoudre ce problème. L'article 23 prévoit que la loi s'applique nonobstant toute clause contraire contenue dans tout accord ou contrat, et que tout accord ou contrat imposant à un employé de retirer ou d'abandonner une révélation faite en vertu de ladite loi est sans effet[103]".

Interdire tout acte destiné à empêcher d'éventuelles révélations est un autre aspect important dans certains pays. Ainsi, le droit norvégien protège ceux qui ont "l'intention" de communiquer ou de révéler des informations, alors même qu'ils ne l'ont pas encore fait[104]. Il est expressément précisé dans le *Whistleblower Protection Enhancement Act* (loi sur l'amélioration de la protection des lanceurs d'alerte), adopté par les États-Unis en 2012, qu'aucune forme de restriction préexistante ne saurait prévaloir sur les protections que cette loi offre. De même, ce type de disposition devrait s'appliquer aux personnes désignées à tort comme étant des lanceurs d'alerte ou comme ayant signalé des actes illicites. En cas de représailles, ces personnes devraient être protégées et traitées de la même façon que tout individu ayant agi en conformité avec les procédures et les lois applicables.

L'Irlande, la Jamaïque, Malte, la République de Corée et la Zambie figurent au rang des autres pays disposant d'une législation applicable aux lanceurs d'alerte qui l'emporte sur les clauses de confidentialité. L'article 14 du *Protection of Public Interest Whistleblowers Act* (loi sur la protection des lanceurs d'alerte défendant l'intérêt général), adopté en 2011 par la République de Corée, prévoit ce qui suit: "Les dispositions interdisant ou limitant les alertes d'intérêt général et autres, qui sont contenues dans une convention collective, un contrat de travail, un contrat de fourniture, etc., sont réputées nulles et non avenues".

7. Responsabilité personnelle pour actes de représailles

Engager la responsabilité personnelle des individus usant de représailles peut également être une façon efficace de prévenir les violations répétées des droits dont jouissent les personnes qui interviennent dans l'intérêt général[105]. Le *Model Law Protecting Freedom of Expression against Corruption* (loi type visant à protéger la liberté d'expression contre la corruption) de l'Organisation des États américains recommande d'engager également la responsabilité de ceux qui agissent de mauvaise foi en ne protégeant pas les lanceurs d'alerte[106]. Une autre option consiste à autoriser les lanceurs d'alerte à introduire une demande reconventionnelle en sanction disciplinaire, y compris en licenciement[107]. Le droit d'action en responsabilité civile dans les systèmes *common law* est une innovation intéressante en matière de protection des lanceurs d'alerte. En Irlande, ce droit est

[103] Article 23: remplacé le 6 mai 2009 par l'article 12 du *Protected Disclosures Amendment Act* (loi sur les révélations d'intérêt général, telle que modifiée), adopté en 2009 par la Nouvelle-Zélande (2009, nº 11).

[104] Voir Stephenson et Levi (2012), par. 3.28: "Aspect novateur, la loi norvégienne protège aussi les employés qui *préviennent* qu'ils comptent signaler des soupçons d'inconduite, par exemple en reproduisant des documents ou en affirmant qu'ils feront connaître une pratique illicite s'il n'y est pas mis fin. La loi norvégienne couvre ainsi la phase préalable au signalement proprement dit. Elle impose aussi aux organisations (publiques comme privées) de mettre en œuvre des procédures qui facilitent le signalement".

[105] Il pourrait s'agir, par exemple, de dommages-intérêts punitifs.

[106] Organisation des États américains, Model Law Protecting Freedom of Expression against Corruption, 2004, disponible à l'adresse: http://www.oas.org/juridico/english/model_law_whistle.htm.

[107] Devine, T., "The Whistleblower Protection Act Burdens of Proof: Ground rules for Credible Free Speech Rights", E-Journal of International and Comparative Labour Studies, volume 2, nº 3, septembre/octobre 2013.

consacré par le *Protected Disclosures Act* (loi sur les révélations protégées), dont le texte énonce que lorsqu'un individu use de représailles contre une personne au motif qu'elle-même, ou un tiers, a fait une révélation protégée, la victime des représailles peut intenter une action contre l'individu concerné en vue d'obtenir réparation[108].

Certains pays imposent également une responsabilité pénale aux personnes qui ont commis des actes de représailles. L'article 25 de la Convention contre la corruption exige des États parties qu'ils confèrent le caractère d'infraction pénale au fait d'entraver le bon fonctionnement de la justice, et la plupart des pays ont érigé en infraction le fait de causer ou de menacer de causer un préjudice à quiconque témoigne dans un procès pénal, ou le fait de tenter, de toute autre manière, d'arrêter ou de détourner le cours de la justice. Il s'agit là d'un autre outil au service de la protection des personnes qui communiquent des informations. Bien que ces mesures existent dans de nombreux États, il y a peu d'informations sur leur efficacité en ce qui concerne les personnes qui communiquent des informations. En Hongrie et aux États-Unis, des individus peuvent être tenus pénalement responsables pour avoir usé de représailles à l'encontre d'une personne ayant communiqué des informations lorsque leur comportement peut être considéré comme un acte relevant d'une entrave à la justice.

Aux États-Unis, un acte de représailles commis à l'encontre de toute personne qui fournit des informations concernant la commission effective ou présumée d'une infraction à un service de détection et de répression est considéré comme une infraction pénale punissable d'une amende ou d'une peine d'emprisonnement[109]. La loi Sarbanes-Oxley interdit expressément d'exercer des pressions sur un lanceur d'alerte et les peines d'emprisonnement sont passées de un à dix ans depuis l'adoption de la loi. La législation australienne applicable aux lanceurs d'alerte érige depuis longtemps en infraction pénale le fait de prendre des mesures de représailles contre un lanceur d'alerte ou toute personne qui lui est associée.

En Australie, un fonctionnaire commet aussi une infraction lorsqu'il dévoile l'identité d'une personne ayant révélé des informations dans l'intérêt général. Cette infraction est passible d'une peine d'emprisonnement pouvant aller jusqu'à six mois[110]. Dévoiler l'identité de toute personne qui bénéficie d'une protection spéciale en République de Corée est une infraction passible d'une peine d'emprisonnement pouvant aller jusqu'à trois ans. Il existe des exemples similaires dans d'autres pays, notamment en Malaisie.

8. Protections contre les menaces à l'intégrité physique

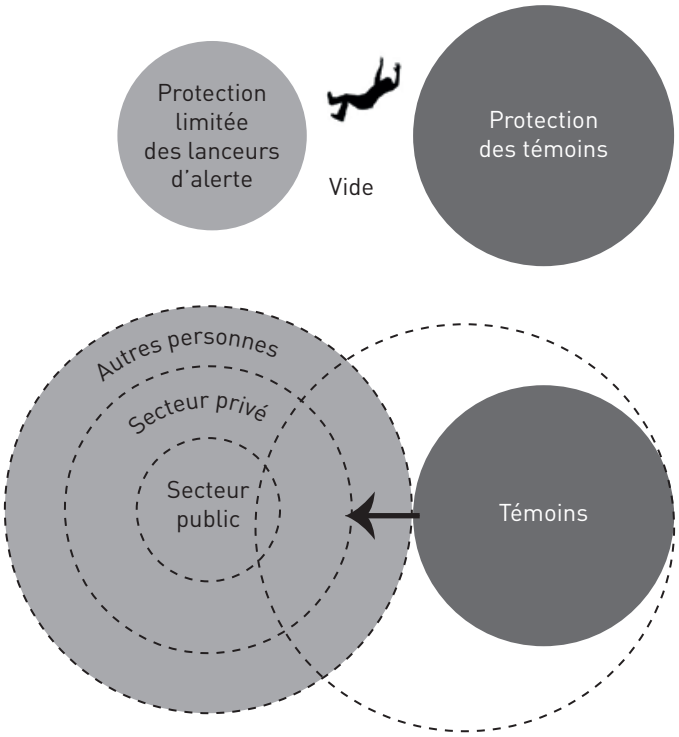
Un dispositif de protection contre les menaces à l'intégrité physique est le plus souvent mis en place lorsque des personnes communiquent des informations relatives à la criminalité organisée et que certaines affaires de corruption sont susceptibles de présenter un lien avec la criminalité organisée. Certaines personnes peuvent également craindre pour leur intégrité physique si les informations qu'elles communiquent portent sur des allégations de corruption à grande échelle, et il se peut aussi que des individus se livrent à des manœuvres d'intimidation physique dans d'autres contextes.

[108] Irlande, *Protected Disclosures Act*, 2014, art. 13.

[109] Voir Code pénal des États-Unis, Titre 18, par. 1513.

[110] Australie, *Public Interest Disclosure Act*, 2013, art. 20, disponible à l'adresse: http://www.comlaw.gov.au/ Details/C2013A00133.

Figure IV. Vous qui communiquez des informations: attention au vide!



Protection accordée à toute personne qui communique des informations

Protection de toute personne qui communique des informations [...] afin qu'elle ne soit pas victime d'un traitement injustifié (y compris les lanceurs d'alerte des secteurs public et privé qui signalent des irrégularités en milieu professionnel).

Protection des témoins élargie

En principe, une telle protection se limite aux procédures pénales et aux mesures de protection propres à ce type de procédure (sécurité procédurale et physique).

Le *Guide législatif* recommande aux législateurs de rendre les dispositions applicables à toute personne qui a ou qui pourrait avoir des renseignements qui sont ou peuvent être utiles pour l'enquête ou les poursuites concernant une infraction de corruption, que ces renseignements soient ou non produits à titre de preuve.

Étude de cas: Michael Woodford, ancien PDG d'Olympus

Michael Woodford a travaillé pendant trente ans chez Olympus, une société qu'il avait rejointe en 1980 en tant que vendeur. Après avoir gravi les échelons, il est devenu directeur exécutif de la branche européenne ainsi que président et chef d'exploitation début 2011. M. Woodford était l'une des quatre personnes d'origine non japonaise à diriger une compagnie japonaise de premier plan. C'est dans un article publié dans la revue japonaise FACTA qu'il a appris pour la première fois qu'Olympus était accusée d'irrégularités financières. Les allégations semblaient provenir de sources sûres. Après avoir mené sa propre enquête, il a entrepris d'obtenir des réponses de la part des autres

administrateurs d'Olympus concernant des dépenses dépassant 1 milliard de dollars des États-Unis. M. Woodford raconte que deux semaines à peine après avoir été nommé PDG et alors qu'il persistait à chercher des réponses à ses questions, les membres du Conseil d'administration lui ont enjoint, lors d'une réunion au cours de laquelle il n'avait pas le droit de s'exprimer, de quitter son appartement de Tokyo, de rendre ses ordinateurs portables ainsi que ses téléphones et de prendre le bus pour l'aéroport.

Craignant pour sa sécurité et celle de sa famille en raison de possibles liens entre les paiements en cause et la criminalité organisée au Japon, M. Woodford, de retour au Royaume-Uni, a demandé et obtenu des conseils et orientations auprès de la cellule de lutte contre la criminalité organisée de la police métropolitaine de Londres. Après avoir rendu les informations publiques, Olympus a tout d'abord affirmé que M. Woodford, son premier PDG non japonais, n'avait pas compris le style de gestion de la société, mais a ensuite été contrainte de reconnaître que les versements qu'il avait mis en doute faisaient partie d'une fraude comptable s'élevant à 1,7 milliard de dollars des États-Unis et visant à dissimuler des pertes sur investissements historiques.

Au final, le scandale a obligé l'ensemble des membres du Conseil d'administration d'Olympus à démissionner et plusieurs hauts responsables ont été arrêtés, y compris le précédent PDG ainsi que des banquiers et l'ancien commissaire aux comptes de la société. Michael Woodford est devenu l'un des plus hauts cadres à avoir donné l'alerte, et les irrégularités qu'il a aidé à révéler au grand jour sont devenues l'un des plus grands et plus longs scandales financiers visant à dissimuler les pertes d'une société que le Japon ait connus. Il a déclaré ce qui suit:

> "En tant que président d'une grande société multinationale, il était plus probable qu'on écoute réellement ce que j'avais à dire. Le vrai problème c'est de savoir comment mieux permettre à un assistant comptable qui a trois enfants et une grosse hypothèque, par exemple, de signaler des actes illicites [...]. Aujourd'hui, les grandes compagnies de ce monde sont nombreuses à faire appel à mes services pour que je les conseille sur la manière d'éviter ce genre de situation. Cela m'intéresse dans la mesure où je veux apporter un changement. Les grandes compagnies doivent prouver qu'elles disposent d'un mécanisme de signalement indépendant de la direction et connu des salariés".

Remarque: M. Woodford a engagé une action pour discrimination et licenciement abusif en vertu du *Public Interest Disclosure Act* (loi sur les révélations d'intérêt général) du Royaume-Uni. Le montant de l'accord auquel il est parvenu avec Olympus serait d'environ 10 millions de livres sterling.

Source: "Japan: Business as usual, but not for Olympus whistleblower Michael Woodford", paru dans *Japan Today*, 3 mars 2014, disponible à l'adresse: http://www.japantoday.com/category/executive-impact/view/japan-business-as-usual-but-not-for-olympus-whistleblower-michael-woodford; "Whistleblower Woodford settles for £10m after his Olympus sacking", paru dans *The Independent*, 9 juin 2012, disponible à l'adresse: http://www.independent.co.uk/news/business/news/whistlelower-woodford-settles-for-10m-after-his-olympus-sacking-7831972.html; "Whistleblower Michael Woodford settles with Olympus", paru dans *The Telegraph*, 29 mai 2012, disponible à l'adresse: http://www.telegraph.co.uk/finance/financial-crime/9298027/Whistleblower-Michael-Woodford-settles-with-Olympus.html; *The Guardian*, 23 novembre 2012.

Les autorités compétentes doivent se demander comment fournir une protection en cas de menace ou d'atteinte à l'intégrité physique. L'autorité saisie par le lanceur d'alerte pourrait prendre directement contact avec des services de police ou des cellules d'enquête spéciales qui luttent contre la corruption, lesquels sont susceptibles d'apporter leur aide ou des conseils sur la meilleure façon d'agir.

Pour officialiser une telle protection, la République de Corée a inclus une disposition dans son *Protection of Public Interest Whistleblowers Act* de 2011 (loi sur la protection

des lanceurs d'alerte défendant l'intérêt général), qui prévoit que les lanceurs d'alerte, leurs conjoints et leur famille peuvent bénéficier d'une protection policière rapprochée s'ils ont été exposés à un grave danger physique, ou sont susceptibles de l'être. Il s'agit là d'une solution fort intéressante qui reconnaît et traite à titre préventif les risques que peuvent encourir certains lanceurs d'alerte.

Une autre option consiste à élargir la portée des lois relatives à la protection des témoins afin qu'elles protègent d'autres personnes qui ont fourni des informations ou qui peuvent avoir besoin d'une protection[111].

Exemple: Mesures de protection définies en fonction de l'entité mise en cause (Chili)

Le Ministère public chilien a mis sur pied une division spéciale qui aide les victimes et les témoins sur l'ensemble du territoire, et a élargi cette protection aux personnes qui signalent des cas de corruption.

Le système chilien offre différentes mesures de protection en fonction de la nature de l'entité mise en cause et du niveau de protection dont la personne concernée a réellement besoin.

Certaines mesures autonomes sont fournies par le Ministère public, telles que, entre autres, protection policière, mécanismes d'appel d'urgence, changement d'adresse, changement de numéro de téléphone et protection de la résidence de la personne qui a communiqué des informations.

En outre, d'autres mesures sont imposées par le tribunal pénal, telles que détention préventive, interdiction de se rendre dans certains lieux ou de voir certaines personnes, changement d'identité, et différents dispositifs pendant le procès (protection de l'identité, audiences à huis clos, interdiction faite à des personnes spécifiques d'assister aux audiences, etc.).

Source: Chevarria, F. et M. Silvestre, Sistemas de denuncias y de protección de denunciantes de corrupción en América Latina y Europa, Documento de Trabajo nº 2, Serie: Análisis, Área: Institucionalidad Democrática, Eurosocial, Madrid, 2013, p. 51, disponible à l'adresse: http://sia.eurosocial-ii.eu/files/docs/1400663798-DT2.pdf.

Quelles que soient les règles qui régissent l'accès à des mesures de protection contre les menaces à l'intégrité physique, on ne saurait nier l'étroite interdépendance qui existe entre, d'une part, les systèmes qui protègent les personnes qui communiquent des informations et, d'autre part, ceux qui protègent les témoins et les victimes (voir aussi chapitre II, section A et ci-après).

Comme il a déjà été dit, conformément à l'article 25 de la Convention contre la corruption, de nombreux pays ont conféré le caractère d'infraction pénale au fait d'entraver le bon fonctionnement de la justice. De ce fait, un individu qui menace, intimide ou influence de toute autre manière (par exemple en la soudoyant) une personne qui a dénoncé un cas de corruption, ou qui déposera en tant que témoin dans une affaire de corruption, peut se rendre coupable d'une infraction pénale.

[111] Voir, par exemple, l'article 2 du *Witness Protection Act* (loi sur la protection des témoins) adopté en 2009 par la Malaisie, disponible à l'adresse: http://www.agc.gov.my/Akta/Vol.%2014/Act%20696%20-%20Witness%20Protection%20Act%202009.pdf.

9. Protection des témoins et protection des auteurs d'infractions qui coopèrent

Pour la Convention contre la corruption, les programmes d'assistance aux témoins et de protection des témoins sont des éléments essentiels d'un système de justice pénale complet. Tant la Convention contre la corruption que la Convention des Nations Unies contre la criminalité transnationale organisée[112] exigent des États parties qu'ils prennent les mesures appropriées pour protéger les témoins d'infractions de corruption.

Il se peut que des personnes qui communiquent des informations soient amenées à participer à une enquête criminelle, auquel cas l'article 32 de la Convention contre la corruption, qui porte sur la protection des témoins, entre en jeu. Par exemple, une personne qui a initialement fait part de soupçons d'irrégularités ou d'actes de corruption sur son lieu de travail peut être amenée à déposer lors d'une audience dans le cadre d'une procédure pénale ou civile. Si cette personne dit craindre sérieusement pour son intégrité physique ou doit être protégée contre des manœuvres d'intimidation, elle doit pouvoir bénéficier d'une assistance et de mesures de protection. En tout état de cause, il importe que toutes les options soient envisagées et clairement expliquées. Les *Bonnes pratiques de protection des témoins dans les procédures pénales afférentes à la criminalité organisée*, publiées par l'ONUDC, constituent un outil précieux et utile pour tous ceux qui sont concernés par l'assistance et la protection offertes aux témoins[113].

L'auteur d'une infraction qui coopère (à savoir une personne qui a participé à la commission d'une infraction et qui fournit aux autorités compétentes des informations utiles à des fins d'enquête et de recherche de preuves) devrait également pouvoir bénéficier des mesures de protection offertes aux témoins (voir l'article 37 de la Convention contre la corruption). Par exemple, l'auteur d'une infraction qui coopère pourrait, dans un premier temps, avoir participé à la commission de cette infraction avant de décider de ne pas continuer et de finalement chercher une "issue ". Au nombre des mesures qui pourraient être considérées comme une manière d'encourager ces personnes à révéler et à fournir des informations privilégiées utiles à des fins d'enquête et de poursuite pourrait figurer la réduction de la peine ou l'octroi d'une immunité pour tout ou partie des infractions commises. Des règles à cet effet devraient être énoncées de manière à laisser au procureur ou au juge un pouvoir d'appréciation en fonction de facteurs tels que le moment choisi pour effectuer le signalement, la qualité des informations fournies ou le degré de coopération apportée pour détecter les activités criminelles ou recouvrer le produit du crime.

La première étape pour déterminer les mesures de protection dont a besoin un témoin consiste à évaluer le risque que celui-ci court. De nombreux États parties n'ignorent rien de la nécessité de soutenir les témoins qui peuvent être vulnérables ou exposés à des risques d'intimidation, mais qui ne remplissent toutefois pas tous les critères pour être admis à un programme complet de protection des témoins. Il existe un certain nombre d'autres mesures de sécurité que les États pourraient offrir, notamment des conseils en matière de sécurité, la mise en place de patrouilles ou d'escorte policières, une réinstallation temporaire, si nécessaire, et une aide financière modique[114]. Dans certaines circonstances, il est possible de protéger, durant l'audience, l'identité d'une personne qui communique des informations et livre un témoignage ou des preuves dans un procès en lui permettant de déposer derrière un écran, par vidéoconférence ou avec brouillage de la voix ou du visage. Le recours à de telles mesures est généralement décidé au cas par

[112] Convention des Nations Unies contre la criminalité transnationale organisée, art. 24.

[113] ONUDC, *Bonnes pratiques de protection des témoins dans les procédures pénales afférentes à la criminalité organisée,* 2008, disponible à l'adresse: https://www.unodc.org/documents/organized-crime/ 09-80620_F_ebook.pdf.

[114] Ibid., p. 21 et 27.

cas: un juge doit les estimer adaptées à la situation et elles ne doivent pas enfreindre le droit à un procès équitable.

Dans la plupart des États, il faut que les témoins fassent l'objet de menaces graves à leur intégrité physique pour être admis à un programme de protection. En pareil cas, il importe moins de savoir quel type de témoin ils sont (informateur, auteur qui coopère, victime ou personne qui communique des informations)[115]. Les programmes complets de protection des témoins impliquent des mesures relativement extrêmes telles qu'un changement d'identité et la fourniture d'un nouveau domicile et, de ce fait, les critères d'admission à ces programmes ont tendance à être très stricts. En règle générale, ils sont souvent considérés comme une solution de dernier recours lorsque les autres moyens de protection disponibles ont été épuisés ou semblent insuffisants.

Les mesures d'assistance aux témoins ne visent pas à protéger l'intégrité physique des témoins mais sont davantage conçues pour assurer l'efficacité des poursuites. Quoi qu'il en soit, elles font partie des mesures susceptibles d'apporter un élément de protection en ce qu'elles contribuent à réduire une partie de la pression et du stress liés au fait de participer à un procès[116].

Dans certains pays où il est nécessaire de préciser le statut juridique d'une personne en droit pénal, les victimes et les témoins d'une infraction auront accès aux dispositifs d'assistance ou de protection disponibles, contrairement aux personnes qui communiquent des informations au sujet d'une infraction (et qui ne déposent pas au procès). Dès lors que des personnes qui communiquent des informations peuvent être exposées à de graves actes de représailles ou de harcèlement, il est important que les États parties envisagent d'élargir cette protection aux personnes qui signalent des actes illicites.

Exemple: Conditions posées à la protection des personnes qui communiquent des informations (loi type de l'Organisation des États américains)

Compte tenu de l'expérience de pays tels que le Mexique et le Pérou, l'Organisation des États américains (OEA) a proposé dans sa loi type d'évaluer l'importance et la pertinence des informations communiquées par des personnes qui signalent des actes illicites. Cette évaluation est une condition à la fourniture de toute mesure de protection en faveur des personnes qui communiquent des informations, et permet d'examiner l'utilité de l'information pendant le procès pénal. L'évaluation permettrait d'obtenir les résultats suivants:

- Empêcher qu'un acte de corruption ne se poursuive, n'ait lieu ou ne soit mené à bien, ou réduire substantiellement l'ampleur ou les conséquences de la commission d'un tel acte;
- Empêcher ou neutraliser de futurs actes de corruption;
- Cerner les circonstances dans lesquelles l'acte de corruption a été planifié et exécuté, ou est en train d'être planifié ou exécuté;
- Identifier les auteurs et les complices d'un acte de corruption qui a été commis ou est sur le point de l'être, ou les membres d'une organisation criminelle et son fonctionnement afin de la démanteler, de l'affaiblir ou d'arrêter l'un ou plusieurs de ses membres;

[115] Ibid., p. 61.

[116] Ibid., p. 28. Dans ses bonnes pratiques de protection des témoins, l'ONUDC décrit les services fournis au Royaume-Uni par le Victim Support, un organisme de bienfaisance indépendant des services d'enquête et de poursuites. Ce service offre des informations et une assistance aux témoins ainsi qu'aux victimes d'une infraction. Pour de plus amples informations, voir: https://www.victimsupport.org.uk/.

- Localiser les instruments, les biens, les effets et le produit de l'acte de corruption, ou découvrir leur lieu de destination, et dévoiler les sources de financement d'organisations criminelles;
- Remettre aux autorités les instruments du crime, ainsi que les effets, le produit ou les biens découlant des actes de corruption;
- Apporter des preuves aux autorités compétentes afin qu'elles autorisent la poursuite de l'enquête.

10. Droit de requête et droit de recours

La loi devrait permettre aux personnes qui communiquent des informations et subissent des représailles de demander le soutien et l'assistance d'une autorité compétente et, si nécessaire, de réclamer des réparations devant une juridiction. Dans certains cas, des services de médiation peuvent également être proposés afin de donner aux parties — en particulier à celles qui entretiennent des relations de travail — la possibilité de résoudre leur différend sans passer par une longue enquête ou une procédure judiciaire coûteuse. Toutefois, la médiation doit être volontaire, et si les parties ne parviennent pas à un accord, celles-ci conservent le droit de demander des mesures correctives, ainsi que leur droit de requête ou de recours.

Exemple: Instances et voies de recours (Ghana)

Le *Whistleblower Act* de 2006 (loi 720 sur les lanceurs d'alerte) permet à toute personne qui — en raison des révélations qu'elle a faites — estime honnêtement et raisonnablement avoir été traitée de façon injuste, ou apprend qu'il y a des risques qu'elle le soit, de déposer dans un premier temps une plainte devant la Commission on Human Rights and Administrative Justice, dont les ordonnances à cet égard emportent les mêmes effets et ont la même force exécutoire qu'un jugement ou une ordonnance rendue par la High Court (Haute Cour).

Lorsque la Commission reçoit une plainte de cet ordre, elle diligente une enquête et peut prendre des mesures provisoires. Après avoir entendu les parties et d'autres personnes, si elle le juge nécessaire, la Commission peut rendre toute ordonnance qu'elle considère adaptée aux circonstances de l'espèce, y compris: *a)* ordonner la réintégration de l'employé; *b)* annuler un transfert ou transférer le lanceur d'alerte vers un autre établissement; ou *c)* ordonner le versement d'une récompense à partir d'un fonds établi à cet effet en application de la loi 720.

De surcroît, un lanceur d'alerte qui a été traité de façon injuste peut également saisir la Haute Cour et réclamer des dommages-intérêts pour rupture de contrat, ou une autre forme de réparation ou de dédommagement à laquelle il peut prétendre, après avoir déposé une plainte devant la Commission.

Dans la pratique, la procédure applicable à la résolution des différends devrait être aussi rapide et simple que possible. En Afrique du Sud, par exemple, le caractère judiciaire des procédures de résolution des différends impliquant des lanceurs d'alerte a été critiqué pour avoir rendu ce processus coûteux et difficilement accessible. Certains observateurs ont affirmé que cela "permet aux employeurs de se livrer à des manœuvres dilatoires, ce qui constitue un abus de procédure[117]".

[117] Martin, P., *The Status of Whistleblowing in South Africa — Taking Stock*, Open Democracy Advice Centre, le Cap, 2010, p. 9, disponible à l'adresse: http://openjournalismworkshop.files.wordpress.com/2013/03/ odac_whistleblowing_report_web.pdf.

Il est préférable de recourir à des tribunaux du travail plutôt que de saisir en premier lieu des tribunaux civils ordinaires. Dans certains pays, comme aux États-Unis et en Slovénie, c'est un organisme public qui est chargé d'aider le lanceur d'alerte (s'il le souhaite) à porter le litige devant un tribunal, dispositif qui peut se révéler extrêmement efficace.

Toutefois, si des comités ou instances spécialisés présentent l'avantage de permettre au lanceur d'alerte de bénéficier des services et connaissances d'experts, il est important qu'il conserve son droit de recours devant un tribunal ou une juridiction supérieure. Par exemple, aux États-Unis, le *Whistleblower Protection Act* (loi sur la protection des lanceurs d'alerte), qui s'applique aux employés fédéraux, ne prévoyait aucun accès normal aux cours d'appel. Les législateurs américains ont reconnu que cela causait de sérieux problèmes aux lanceurs d'alerte qui voulaient demander des réparations, et le droit de recours a été ajouté à titre expérimental dans le *Whistleblower Protection Enhancement Act* de 2012 (loi sur l'amélioration de la protection des lanceurs d'alerte). Aux États-Unis, le système utilisé par le Département du travail pour statuer sur les réclamations déposées par des lanceurs d'alerte victimes de représailles pour avoir signalé des irrégularités au sein de leur société a également accusé des retards considérables. Par ailleurs, depuis que la loi Sarbanes-Oxley a été adoptée en 2004 comme suite à la faillite d'Enron, chaque loi applicable aux personnes qui signalent des abus commis par leur société consacre le droit de la partie requérante d'engager des poursuites devant un tribunal fédéral si aucune décision administrative n'a été rendue dans les 180 jours.

11. Mesures provisoires/administratives

Pour que des mesures de protection paraissent crédibles, il conviendrait d'envisager d'autoriser la prise de mesures provisoires tant que la procédure n'est pas terminée. De telles mesures sont particulièrement importantes pour les personnes qui communiquent des informations concernant leur lieu de travail car elles peuvent contribuer à protéger les relations professionnelles et empêcher qu'elles ne volent en éclats. Les mesures provisoires pourraient comprendre toute mesure nécessaire pour sauvegarder le poste occupé par l'individu concerné jusqu'à ce qu'une audience puisse avoir lieu, comme la réintégration dans un emploi similaire (par exemple, si nécessaire avec un supérieur différent ou dans un autre service de la compagnie) ou toute autre mesure visant à annuler ou du moins à limiter les effets des actes de représailles aussi rapidement que possible. Compte tenu de la longueur de certaines procédures, si l'individu concerné ne bénéficie pas de telles mesures jusqu'à ce qu'une décision judiciaire ou administrative définitive soit rendue, il est possible qu'il ne puisse pas continuer à exercer son travail ou subvenir financièrement à son existence. L'Annexe 1 du *Protected Disclosures Act* adopté en 2014 par l'Irlande (loi sur les révélations protégées)[118] contient des dispositions concernant des mesures provisoires qui peuvent être prises en attendant qu'un recours pour licenciement abusif soit tranché.

Cependant, si les effets des actes de représailles ne peuvent être raisonnablement annulés, une indemnité financière adaptée doit alors être versée. Compte tenu de la possibilité qu'un lanceur d'alerte qui signale des abus sur son lieu de travail puisse occuper n'importe quel poste au sein de la hiérarchie d'une organisation et perdre son travail en raison de ses révélations, l'indemnité accordée devrait être proportionnelle à la perte financière réelle et ne pas être limitée arbitrairement. Dans les cas où un employeur n'est pas à même de verser une indemnité, certains pays ont entrepris de créer un fonds public permettant d'honorer les ordonnances d'indemnisation, comme c'est le cas en République de Corée.

[118] http://www.per.gov.ie/protected-disclosures-i-e-whistleblowing/.

12. Charge de la preuve

Un système qui oblige un employé à prouver qu'il a été traité injustement parce qu'il a signalé des actes illicites fait peser sur lui une charge qui peut être très lourde à porter. Si la plupart des systèmes imposent à la personne qui communique des informations pouvant laisser présumer qu'elle a signalé un problème et subi un préjudice (harcèlement, absence de promotion, rétrogradation, licenciement, etc.), l'intéressé peut ne pas être en mesure de prouver les motifs pour lesquels son employeur a agi de la sorte. En effet, il est possible que seuls les employeurs ou d'autres individus ayant exercé des représailles puissent apporter des preuves solides attestant que le préjudice infligé n'avait rien à voir avec les motifs avancés par le plaignant et que les mesures prises étaient justifiées dans les circonstances de l'espèce.

C'est pour cette raison que de nombreux pays ont adopté un principe communément appelé "renversement de la charge de la preuve", en vertu duquel la loi exige de l'employeur qu'il prouve que la personne qui a communiqué des informations a été traitée d'une certaine manière pour des motifs valables, et ce après que le plaignant a établi qu'il avait subi un préjudice. Toutefois, dans la majeure partie des cas, il ne s'agit pas réellement d'un renversement de la charge de la preuve à proprement parler, mais plutôt de la charge normale de la preuve associée à d'autres dispositions juridiques telles que l'interdiction en droit de porter tout préjudice à un individu du fait qu'il a dénoncé des irrégularités présumées. Selon ces dispositions, un employé qui aurait été licencié après avoir signalé des abus n'aurait qu'à prouver qu'il a été renvoyé, qu'il a signalé des irrégularités et qu'il est probable que ces deux événements soient liés (présomption d'actes de représailles). Il reviendrait alors à l'employeur d'établir que la mesure contestée n'était pas préjudiciable et que, de toute façon, l'employé aurait été licencié même s'il n'avait pas donné l'alerte.

On trouve des dispositions en ce sens dans les lois relatives aux lanceurs d'alerte et aux signalements d'actes de corruption adoptées par l'Afrique du Sud, la Croatie, les États-Unis[119], la France, le Luxembourg, la Norvège, la Nouvelle-Zélande, la République de Corée, le Royaume-Uni et la Slovénie, et tant le Conseil de l'Europe[120] que le G20[121] recommandent cette approche.

Le *Whistleblower Protection Act* (loi sur la protection des lanceurs d'alerte), adopté par la Malaisie, offre un autre exemple de gestion de la charge de la preuve. La loi énonce la présomption suivante: "[u]ne personne est réputée prendre des mesures préjudiciables à l'endroit d'un lanceur d'alerte ou de toute personne liée ou associée à celui-ci si elle prend ou menace de prendre les mesures préjudiciables en question au motif que le lanceur d'alerte a révélé un comportement répréhensible; ou si elle croit qu'un lanceur d'alerte a révélé ou entend révéler un comportement répréhensible".

[119] La législation américaine approfondit cette approche à deux égards. D'une part, la charge de la preuve qu'elle fait peser sur l'employé est limitée en ce qu'il doit établir pour l'essentiel, ou à première vue, que son action est bien fondée et que le fait qu'il a lancé l'alerte était "un facteur parmi d'autres" ayant abouti à la mesure de représailles en cause, ce qui signifie que la décision contestée est "en tout état de cause" entachée d'illégalité. D'autre part, la charge de la preuve qui incombe à l'employeur répond à des normes élevées qui exigent "des preuves claires et convaincantes", soit environ 70 à 80 % du dossier de l'affaire. Voir Devine, T., "The Whistleblower Protection Act Burdens of Proof: Ground rules for Credible Free Speech Rights", *E-Journal of International and Comparative Labour Studies*, volume 2, nº 3, septembre/octobre 2013.

[120] Assemblée parlementaire, Résolution 1729 (2010), "La protection des "donneurs d'alerte", par. 6.3., disponible à l'adresse: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-FR.asp?fileid=17851&lang=FR.

[121] G20 Compendium of best practices and guiding principles for legislation on the protection of whistleblowers, disponible à l'adresse: http://www.coe.int/t/dghl/standardsetting/cdcj/Whistleblowers/ G20%20COMPENDIUM%20OF%20BEST%20PRACTICES%20AND%20GUIDING%20PRINCIPLES%20FOR%20LEGISLATION%20(3).pdf.

D. Autres mesures tendant à faciliter les signalements

1. Existe-t-il une obligation de signalement?

Il convient de préciser que le fait de "faciliter" les signalements ne revient pas à imposer une obligation de signalement. Dans la plupart des pays, l'obligation de signaler des irrégularités est inhérente à des fonctions, charges et professions données, par exemple, aux agents de police, médecins, fonctionnaires, avocats et comptables. Certaines catégories d'employés peuvent également se voir dans l'obligation légale de signaler des abus en particulier, par exemple de signaler des cas soupçonnés de maltraitance d'enfants ou de négligence en matière de soins de santé ou d'assistance sociale, ou de signaler des soupçons de blanchiment d'argent dans le secteur financier. Le manquement à une telle obligation peut avoir de graves conséquences professionnelles, dont la suspension, l'interdiction d'occuper une charge similaire à l'avenir ou l'interdiction d'exercer sa profession. Ces obligations de signalement sont souvent limitées en raison soit de la profession (comme lorsque le rôle spécifique tenu dans la société revêt un caractère sensible et responsable), soit de la nature du type d'informations demandé (par exemple sa valeur et son importance pour la société).

Si l'option consistant à imposer à tous les employés une obligation de signaler des irrégularités ou des manquements peut séduire, il existe aussi des arguments contre une telle démarche, notamment qu'elle est susceptible d'encourager les employés à signaler des abus de façon excessive et permet de s'en prendre à d'autres pour en faire des boucs émissaires. Une telle obligation peut mener des organisations à se focaliser sur les personnes qui n'ont rien dit au lieu de s'intéresser à l'information rapportée ou à l'efficacité de leur dispositif de signalement ou d'alerte[122]. Cela ne veut pas dire qu'on ne s'attend pas qu'un employé signale des irrégularités, mais uniquement qu'il pourrait se révéler difficile, voire contre-productif dans certains cas, d'imposer une obligation générale de donner l'alerte.

En outre, il faut reconnaître que même les personnes qui ont un réel devoir de signalement peuvent être la cible de graves actes de représailles.

Étude de cas: Les auditeurs internes et la corruption (Afrique du Sud)

Les auditeurs internes occupent une place unique et importante dans la lutte contre la corruption. Non seulement ils sont employés pour mettre en place des mesures visant à renforcer les mécanismes de gouvernance des compagnies, mais ils peuvent également lancer l'alerte lorsqu'ils découvrent des activités frauduleuses.

D'un point de vue déontologique et juridique, les auditeurs sont tenus de signaler les activités suspectes. C'est précisément pour accomplir cette fonction qu'ils sont employés. En Afrique du Sud, l'*Auditing Profession Act* (loi sur la profession d'auditeur) sanctionne un auditeur qui ne signale pas "une irrégularité devant être dénoncée", ce qui inclut tout cas de fraude ou toute violation du devoir fiduciaire.

Les auditeurs s'exposent aussi à des sanctions pénales s'ils ne dénoncent pas tout un éventail d'activités ou de transactions illégales, ou même suspectes, qui sont réprimées par le *Financial Intelligence Centre Act* (loi sur le centre de renseignement financier) et

[122] Public Concern at Work, The Whistleblowing Commission, Code of Practice (for effective whistleblowing arrangements), 2013, p. 13, disponible à l'adresse: http://www.pcaw.org.uk/whistleblowing-commission.

le *Prevention and Combating of Corrupt Activities Act* (loi visant à prévenir et combattre la corruption).

Par conséquent, il est primordial que les auditeurs internes puissent dénoncer des cas de corruption chaque fois qu'ils en rencontrent, et ce sans crainte de répercussions professionnelles, voire personnelles. Malheureusement, dans la pratique, ce n'est pas toujours le cas. L'Institute of Internal Auditors South Africa (institut sud-africain des auditeurs internes) a signalé qu'il était arrivé que des auditeurs chargés de vérifier les comptes de certaines municipalités fassent l'objet de manœuvres d'intimidation et se soient vu demander d'"étouffer" certaines irrégularités.

En 2013, Lawrence Moepi, un auditeur juricomptable, a été abattu sur le parking de sa société à Houghton. À cette époque, il participait à un certain nombre d'enquêtes très délicates et certains observateurs ont laissé entendre que sa mort pouvait être liée au fait qu'il avait contribué à révéler des actes de corruption.

Le *Protected Disclosures Act 26 of 2000* (loi sur les révélations protégées) est la principale loi sud-africaine qui protège les lanceurs d'alerte contre des traitements injustes, des actes de représailles et des manœuvres discriminatoires. Cette loi protège les personnes du secteur privé et du secteur public qui dénoncent des conduites délictueuses et d'autres actes illégaux commis sur leur lieu de travail. Elle impose également aux employeurs de mettre en place des mesures tendant à protéger les lanceurs d'alerte contre des traitements injustes ou un licenciement en raison des révélations qu'ils ont faites.

Cette loi n'a qu'une faible portée et la protection qu'elle offre ne s'applique qu'à des salariés. Par conséquent, elle ne couvrira que les auditeurs internes qui sont employés par la compagnie et ne s'étendra pas aux sous-traitants indépendants ou bénévoles.

Toutefois, le *Companies Act* (loi sur les sociétés) offre d'autres garanties importantes: l'article 159 prévoit une protection pour un vaste éventail de personnes associées à une compagnie. Cette disposition s'applique à la dénonciation faite par un employé ou un fournisseur de biens ou services.

Source: "Corruption Watch: Help for auditors who report crime", paru dans *Business Day (BDLive)*, 16 mars 2014, disponible à l'adresse: http://www.bdlive.co.za/businesstimes/2014/03/16/corruption-watch-help-for-auditors-who-report-crime. Voir aussi Jane Duncan, "The Auditor and the hitmen", 6 novembre 2013, disponible à l'adresse: http://sacsis.org.za/site/article/1833.

Avant d'envisager de réformer ou de modifier la législation sur la protection des personnes qui communiquent des informations suite à la découverte d'un cas de corruption dans le cadre de leur travail, les États parties devraient réaffirmer leur engagement et approfondir leur compréhension s'agissant de la portée et du rôle de l'obligation de signaler des cas de corruption ainsi que des protections attachées à cette obligation.

2. Mesures incitatives visant à encourager les signalements: honneurs et récompenses

Honneurs

Les gouvernements nationaux du monde entier décernent des distinctions honorifiques aux personnes dont les actions ont largement contribué au bien commun du pays; certaines juridictions et certains services de détection et de répression distinguent ou récompensent également les individus qui ont pris des risques pour protéger ou servir les intérêts d'autrui. Les personnes qui signalent des irrégularités, des cas de corruption ou des dangers et, partant, protègent l'intérêt général devraient être considérées comme des individus qui méritent une reconnaissance publique. Une telle reconnaissance permettrait

d'aider à normaliser leurs actes comme relevant de la "bonne citoyenneté". Par exemple, la législation indonésienne "témoigne sa gratitude" aux lanceurs d'alerte qui ont contribué aux efforts visant à prévenir et à combattre la corruption[123].

Primes ou récompenses

Un certain nombre de pays ont adopté des systèmes qui offrent des récompenses pécuniaires aux personnes qui ont communiqué des informations ayant permis d'intenter des actions réussies. Un exemple bien connu est celui que la Securities and Exchange Commission des États-Unis (SEC) a mis en place en vertu de la loi Dodd-Frank: ce système offre une compensation financière en échange d'informations sur des violations de la législation boursière afin d'encourager les lanceurs d'alerte à se manifester. Certains observateurs ont estimé que ce modèle modifie la finalité des signalements, qui est normalement de servir l'intérêt général, pour mettre l'accent sur le gain personnel des lanceurs d'alerte. En 2014, aux États-Unis, l'Office of the Whistleblower a reçu 3 620 dénonciations, ce qui représente une hausse de plus de 20 % par rapport aux deux années précédentes. La loi interdit aux employeurs d'exercer des représailles à l'encontre de salariés qui fournissent à la SEC des "informations de première main" (à savoir des informations qui ne sont pas publiques ou connues de la SEC) concernant d'éventuelles infractions à la législation boursière. Toute personne qui fournit volontairement des informations de première main à la SEC concernant une infraction à la loi fédérale sur les valeurs mobilières, qui a été commise, est en train d'être commise ou est sur le point de l'être, peut prétendre à une récompense pour avoir donné l'alerte. Le montant de cette récompense est proportionnel à la somme recueillie par la SEC comme suite à la procédure ouverte grâce aux informations communiquées, et il est également fonction de la qualité des informations fournies[124]. Depuis le lancement de son programme destiné aux lanceurs d'alerte, la SEC a autorisé l'octroi de récompenses à 14 lanceurs d'alerte et, en septembre 2014, elle a autorisé le versement de plus de 30 millions de dollars des États-Unis à un lanceur d'alerte qui avait fourni des informations de première main essentielles, ayant permis de prendre des mesures de sanction efficaces[125].

En Malaisie, conformément au *Whistleblower Protection Act* de 2010 (loi sur la protection des lanceurs d'alerte), les lanceurs d'alerte qui ont révélé des informations ayant abouti à des poursuites ou permis de détecter des irrégularités peuvent recevoir des récompenses, si le Gouvernement le juge approprié.

S'il est vrai que des systèmes incitatifs visant à encourager les alertes sont relativement bien établis aux États-Unis et existent dans d'autres pays comme en République de Corée, leur adoption ne va pas de soi dans le reste du monde. Certains ont critiqué ce modèle qu'ils voient comme une transaction commerciale destinée à obtenir des informations. Pour eux, il s'agit davantage d'un marché de l'information qui est largement indépendant de la liberté d'expression ou de l'intérêt général. En tout état de cause, si un État envisage d'introduire un système de récompenses, il devrait le considérer comme un dispositif qui vient compléter les mesures visant à assurer une protection aux lanceurs d'alerte.

[123] Law No. 31 of 1999 on the Eradication of the Criminal Act of Corruption (loi sur l'éradication des actes délictueux de corruption), art. 42.

[124] Selon le programme de la SEC, les lanceurs d'alerte pouvant prétendre à récompense ont droit à une prime comprise entre 10 et 30 % du produit des sanctions pécuniaires imposées au terme de la procédure engagée par la SEC et des actions connexes intentées par d'autres services de détection et de répression. Toutefois, pour qu'il y ait récompense, la procédure engagée par la SEC sur la base des informations fournies par le lanceur d'alerte doit emporter des sanctions monétaires excédant 1 million de dollars des États-Unis. Le dispositif de récompenses de la SEC s'applique également aux citoyens non américains.

[125] États-Unis d'Amérique, Securities and Exchange Commission, 2014 Annual Report to Congress on the Dodd-Frank Whistleblower Program, disponible à l'adresse: http://www.sec.gov/about/offices/owb/annual-report-2014.pdf.

Si un État entend mettre en place des systèmes incitatifs alors que sa législation ne protège pas les révélations motivées par un gain personnel, il serait souhaitable qu'il précise que toute récompense ou autre mesure d'incitation prévue par la loi n'est pas réputée constituer un gain personnel. La Zambie a expressément consacré cette exception dans son *Public Interest Disclosure Act* de 2010 (loi sur les révélations d'intérêt général)[126].

Principe *qui tam*

Le principe *qui tam* (en vertu duquel des individus peuvent dénoncer des fraudes commises par des sociétés ou des organisations aux dépens de l'État) constitue une branche distincte et séparée de la législation applicable aux lanceurs d'alerte. Aux États-Unis notamment, il a permis d'exercer un contrôle sur les dépenses publiques impliquant le secteur privé. Ce modèle réglementaire diffère des systèmes de primes ou de récompenses qui offrent une compensation financière en échange d'informations mais ont tendance à conférer un rôle passif à la personne ayant communiqué des informations[127].

Le *False Claims Act* des États-Unis (loi sur les demandes de paiement frauduleuses) est considéré comme l'un des textes de loi applicables aux lanceurs d'alerte les plus efficaces au monde. Si son champ d'application se limite aux fraudes et aux actes de corruption commis en rapport avec la commande publique, c'est l'une des rares lois qui met des ressources directement à la disposition des particuliers afin qu'ils puissent ensuite décider d'introduire une action civile contre de puissants transgresseurs. Dans le cadre de ce type d'action, une partie privée appelée "*relator*" (quasi-demandeur) intente un procès pour le compte du Gouvernement américain. Si le Gouvernement prend les rênes du procès, la partie privée reçoit 15 à 20 % du montant de tout dommage-intérêt recouvré; si cette dernière agit seule, ce pourcentage se situe alors entre 25 et 30 %. Dans les deux cas, la partie privée doit prendre en charge ses propres frais d'avocats[128], bien que le Gouvernement soit considéré comme le vrai plaignant et non le quasi-demandeur. En 1986, avant que la loi ne soit modernisée, le Département de la justice des États-Unis avait recouvré au civil 26 millions de dollars suite à des fraudes. Ces 25 dernières années, quelque 45 milliards de dollars ont été recouvrés[129]. Des observateurs ont relevé que le *False Claims Act* uniformise aussi dans une certaine mesure les règles du jeu en incitant des avocats qualifiés à accepter des affaires concernant des signalements dès lors que ces actions peuvent se révéler extrêmement lucratives s'ils ont gain de cause.

E. Traitement des signalements et coopération

Afin d'instaurer un climat de confiance, il est primordial de traiter les signalements avec professionnalisme, d'évaluer le contenu de l'information communiquée et de prendre les mesures qui s'imposent pour s'attaquer à tout acte illicite. Il s'agit là de l'un des aspects les plus importants de la protection offerte aux personnes qui communiquent des informations. Si toutes ces conditions sont dûment respectées, il sera moins nécessaire d'impliquer plus avant l'individu concerné, et celui-ci aura moins de souci à se faire pour sa situation. S'il est toutefois jugé nécessaire de faire appel à l'intéressé de manière continue — par exemple, parce que son témoignage est indispensable pour prouver devant une juridiction qu'un acte illicite a été commis —, il sera essentiel pour s'assurer

[126] Zambie, *Public Interest Disclosure Act*, 2010, art. 22: une révélation est réputée protégée lorsqu'elle est faite de bonne foi par un employé […] "qui ne révèle pas l'information dans le but d'en tirer un gain personnel, à l'exception de toute récompense exigible en vertu d'une quelconque loi".

[127] Hutton, David, Shooting the Messenger, Parkland Institute, Canada, 2011, disponible à l'adresse: http://parklandinstitute.ca/research/summary/shooting_the_messenger.

[128] Vaughn, R., *The Successes and Failures of Whistleblower Laws*, Edward Elgar Publishing, États-Unis, 2012, p. 131.

[129] http://www.taf.org/TAF-testimony-Burns-1-2014-WV%20Final.pdf.

sa coopération de répondre avec tact et comme il se doit à toute inquiétude qu'il pourrait avoir concernant sa sécurité ou celle de ses proches.

Le succès de toute disposition juridique dépendra dans une large mesure de la façon dont l'information communiquée a été traitée et de la question de savoir si les mesures adéquates ont été prises pour s'attaquer à tout acte illicite. Par conséquent, il est crucial de veiller à ce que les systèmes mis en œuvre par les autorités compétentes pour traiter les informations communiquées par des lanceurs d'alerte répondent à des normes de qualité et d'équité, et que les personnes responsables de ces tâches soient qualifiées et dûment formées. Il est également nécessaire d'instaurer une coopération efficace entre les services concernés afin de s'assurer que les normes de protection sont respectées lorsque des informations sont transférées d'une institution à une autre.

Ayant reconnu que de nombreux signalements effectués selon les règles par des lanceurs d'alerte restent sans réponse, le Conseil de l'Europe a affirmé qu'il est envisageable de donner aux tribunaux les moyens d'imposer une sanction ou d'infliger une amende ou une peine à un employeur ou à toute autre personne responsable de ne pas avoir mené une enquête rapide et appropriée[130].

Les États, les autorités compétentes et les employeurs ont une obligation de diligence envers les personnes qui s'engagent à leurs côtés pour lutter contre la corruption ou d'autres actes illicites. La présente section expose certains des principaux éléments qui devraient être pris en considération pour garantir que les signalements de cas de corruption ou d'autres actes illicites sont traités convenablement. Nombre d'entre eux seront déjà connus puisqu'il s'agit des principes fondamentaux d'une enquête et d'un procès équitables.

1. Des procédures claires pour le signalement initial et pour les demandes de mesures de protection

Il importe de bien clarifier les modalités de signalement d'irrégularités ou de fraudes afin que les membres du personnel et d'autres personnes qui communiquent des informations sachent quelles informations fournir, quand les fournir, à qui les fournir, etc. Toutefois, de nombreuses organisations ne réfléchissent pas suffisamment aux processus qui doivent être mis en place pour qu'elles puissent donner suite en temps voulu à un signalement de cas de corruption ou d'actes illicites et diligenter une enquête à cet égard. Si le mandat de nombre d'autorités compétentes inclut déjà certaines fonctions d'enquête, d'autres autorités ont une expérience limitée du traitement des signalements directs, tandis que certaines n'ont jamais été confrontées à ce genre de situation.

Pour remédier à ces difficultés, bon nombre de lois nationales adoptées ces dernières années comprennent des procédures spécifiques, et détaillées par étape, sur la manière dont les autorités et les organes de contrôle devraient assurer le suivi des révélations effectuées selon les règles par des lanceurs d'alerte.

En Jamaïque, le *Protected Disclosures Act* de 2011 (loi sur les révélations protégées) impose aux destinataires de révélations de déterminer si une enquête est nécessaire et, dans l'affirmative, d'ouvrir l'enquête. Le destinataire est tenu d'enquêter sur la question de manière équitable, d'informer le lanceur d'alerte tous les 30 jours au moins des progrès de l'enquête, de transmettre ses conclusions au lanceur d'alerte ainsi qu'aux autres personnes et organisations concernées, de recommander des mesures correctives et de prendre des dispositions pour remédier à un comportement répréhensible, ainsi que

[130] Conseil de l'Europe, Recommandation sur la protection des lanceurs d'alerte, Exposé des motifs, 2014.

pour offrir une réparation, infliger des sanctions disciplinaires et limiter les possibilités que le comportement répréhensible ne se reproduise.

Des procédures et exigences de cet ordre sont prévues, par exemple, dans la loi australienne de 2013 sur les révélations d'intérêt général (*Public Interest Disclosure Act*), la loi coréenne de 2011 sur la protection des lanceurs d'alerte défendant l'intérêt général (*Protection of Public Interest Whistleblowers Act*) et la loi malaisienne de 2010 sur la protection des lanceurs d'alerte (*Whistleblower Protection Act*).

Quelle que soit l'autorité qui reçoit l'information, il semble primordial de respecter certaines normes lors du traitement des signalements. Ces normes comprennent les principes de justice naturelle (équité de la procédure) concernant la confidentialité, les règles de preuve, les critères d'établissement de la preuve, l'observation des lois et politiques, ainsi que les réglementations en matière de santé et de sécurité[131].

Lorsqu'une organisation mène une enquête interne, par exemple, son objectif est de découvrir ce qui s'est passé et de déterminer quelle mesure doit être prise pour protéger le public, le salarié concerné ou l'organisation afin qu'aucune perte ni aucun préjudice ne soient à déplorer. Que l'enquête interne soit déclenchée par le signalement d'un membre du personnel ou d'un membre du public, son objectif doit consister à établir les faits; il ne s'agit ni d'un procès ni d'un tribunal.

Au niveau des autorités compétentes, il faudrait envisager de mettre au point des systèmes qui simplifient le processus de signalement et soient parfaitement adaptés aux dispositifs de contrôle ou de surveillance en vigueur. Il pourrait s'agir d'un système consistant à transmettre l'information lorsque l'autorité qui la reçoit en premier lieu n'a pas compétence pour agir. Dans de tels cas, la personne qui a communiqué l'information devrait être tenue informée de la suite donnée à son signalement, la confidentialité de son identité devrait rester garantie et elle devrait continuer à bénéficier de la protection de la loi applicable à sa révélation initiale.

En ce qui concerne les autorités compétentes, leur site Web et d'autres supports d'information devraient expliquer en détail comment le public peut les contacter et comment toute information communiquée sera traitée. Le délai de réponse devrait être clairement indiqué, tout comme les types de mesures de protection disponibles et les modalités de leur mise en œuvre.

Il est tout aussi important que les États parties examinent et réglementent les modalités de présentation d'une demande de mesures de protection dans les cas où, par exemple, une personne a été victime de représailles. En République de Corée, l'article 17 du *Protection of Public Interest Whistleblowers Act* (loi sur la protection des lanceurs d'alerte défendant l'intérêt général) prévoit que "la demande tendant à obtenir des mesures de protection doit être déposée dans un délai de trois mois à compter de la date à laquelle les mesures défavorables ont été prises […]". Des décrets présidentiels apportent de plus amples informations sur les méthodes et procédures à suivre.

[131] Pour des recommandations concernant les enquêtes menées en interne, voir le site Web de l'Independent Commission against Corruption de la Nouvelle-Galles du Sud (Australie), à l'adresse: http://www.icac.nsw.gov.au/preventing-corruption/responding-to-corrupt-conduct/internal-investigations/ 1535.

Exemple: Office of the Whistleblower de la Commission fédérale de contrôle des opérations boursières (SEC) aux États-Unis

L'Office of the Whistleblower a été créé en 2010. Il est responsable de l'administration du programme de la SEC destiné aux lanceurs d'alerte. En outre, il est notamment chargé d'obtenir des informations et une assistance de la part de lanceurs d'alerte qui ont eu vent d'éventuelles infractions à la législation boursière, de les protéger s'ils coopèrent avec la SEC et de leur accorder une récompense financière dans certains cas.

En plus de renvoyer au règlement du programme destiné aux lanceurs d'alerte, le site Web de la SEC apporte des réponses aux questions que certains peuvent se poser concernant le programme et, plus précisément, sur ce qui se passera s'ils communiquent des informations. Voici une liste des questions auxquelles le site Web apporte une réponse à l'heure actuelle:

- Qu'est-ce que le programme de la SEC destiné aux lanceurs d'alerte?
- Quels sont les critères à remplir pour être considéré comme un lanceur d'alerte?
- Que signifie communiquer "volontairement" des informations?
- Qu'est-ce qu'une "information de première main"?
- Comment l'information que je communique peut-elle "permettre" à la SEC d'intenter une action réussie?
- La compagnie pour laquelle je travaille dispose d'un processus interne de conformité. Puis-je effectuer un signalement interne et encore prétendre recevoir une récompense pour avoir lancé l'alerte?
- J'ai communiqué des informations à la SEC avant l'adoption de la loi Dodd-Frank le 21 juillet 2010. Puis-je prétendre à récompense?
- Comment puis-je communiquer des informations dans le cadre du programme de la SEC destiné aux lanceurs d'alerte?
- Puis-je communiquer une information sous couvert d'anonymat?
- La SEC préservera-t-elle le caractère confidentiel de mon identité?
- Comment savoir si je peux demander une récompense?
- Comment puis-je demander une récompense?
- Quels sont les facteurs que la SEC prend en considération pour fixer le montant de la récompense?
- Puis-je faire appel de la décision de la SEC concernant ma récompense?
- Quels sont mes droits si mon employeur prend des mesures de représailles à mon encontre du fait que j'ai communiqué des informations à la SEC?

L'Office of the Whistleblower tient également une permanence téléphonique publique pour répondre aux questions des lanceurs d'alerte ou de leurs avocats au sujet du programme destiné aux lanceurs d'alerte ou de la marche à suivre pour communiquer des informations à la SEC. En 2014, le bureau a répondu à plus de 2 731 appels de membres du public.

Source: United States Securities and Exchange Commission, *2014 Annual Report to Congress on the Dodd-Frank Whistleblower Program*, disponible à l'adresse: http://www.sec.gov/about/offices/owb/annual report-2014.pdf.

2. L'autorité qui reçoit des plaintes concernant des représailles doit-elle être distincte de l'autorité qui enquête sur les révélations?

Il conviendrait de se demander s'il faut séparer la fonction consistant à enquêter sur le contenu d'une révélation de celle consistant à examiner toute plainte pour représailles déposée par la personne qui a effectué ladite révélation, et dans l'affirmative comment procéder. Une telle séparation à un stade précoce peut aider à définir les différentes compétences et spécialisations qui peuvent être exigées du personnel chargé d'accomplir ces fonctions.

Une séparation fonctionnelle de ces deux tâches contribue à garantir que des personnes dûment formées peuvent se concentrer sur leur domaine de compétence et acquérir des connaissances spécialisées, y compris en matière d'actes de représailles, et qu'il n'existe aucun conflit d'intérêts apparent entre la façon dont l'information est gérée et la manière dont la personne qui l'a communiquée est traitée. L'Office of Special Counsel des États-Unis[132] ou l'Anti-Corruption and Civil Rights Commission de la République de Corée (cette commission de lutte contre la corruption et de défense des droits civils est décrite au chapitre II, section B.2) séparent, dans une certaine mesure, l'enquête sur les actes illicites de l'enquête concernant les représailles, bien que ces institutions constituent le point de contact principal pour ces deux questions.

L'Office of Special Counsel est habilité à enquêter et à engager des poursuites concernant des violations de la réglementation protégeant les employés fédéraux contre des représailles exercées par suite des alertes qu'ils ont lancées (conformément au *Whistleblower Protection Act*). Il joue également un rôle de surveillance essentiel en examinant les enquêtes menées par les autorités publiques sur d'éventuels comportements répréhensibles. Sur la base d'une plainte déposée par un lanceur d'alerte, ce bureau peut enjoindre à un organisme d'enquêter sur des irrégularités alléguées, même si celui-ci est peu disposé à le faire. Partant du principe que les lanceurs d'alerte eux-mêmes sont le plus souvent des experts à part entière de l'objet de leur préoccupation, le bureau les invite à se prononcer sur la qualité de l'enquête menée par l'organisme désigné et les mesures correctives prescrites. Le bureau reste également en contact avec l'organisme d'enquête afin de s'assurer que les mesures prises sont raisonnables et répondent aux préoccupations soulevées par les lanceurs d'alerte.

En Nouvelle-Zélande, les signalements d'irrégularités et les plaintes déposées suite à des actes de représailles sont traités par deux organismes distincts. Si des révélations protégées peuvent être communiquées aux autorités compétentes, y compris à l'Office of the Ombudsman, il revient à la Human Rights Commission de veiller à l'application des dispositions en matière de protection contre les représailles, énoncées dans le *Human Rights Act* de 1993 (loi sur les droits de l'homme), qui sont applicables aux lanceurs d'alerte. Cette solution réduit également le risque de partialité apparente à l'endroit d'un lanceur d'alerte car l'évaluation de sa plainte pour représailles est clairement dissociée de l'enquête sur le signalement d'une suspicion de fraude, et ne saurait donc être influencée par l'enquête, en particulier si aucune irrégularité n'est avérée.

Ainsi, même si le contexte juridique et institutionnel existant aura une grande influence, les États parties devront se demander si les autorités compétentes devraient être habilitées tant à enquêter sur les signalements d'irrégularités et de cas de corruption qu'à protéger les individus qui leur signalent de tels actes. Cette question est particulièrement importante dans la mesure où une plus grande attention est accordée dans le monde entier au

[132] Voir le site Web de l'Office of the Special Counsel, à l'adresse: https://osc.gov.

rôle que jouent les autorités compétentes dans les enquêtes sur des irrégularités et dans le fait que les services ou compagnies qu'elles contrôlent sont tenus de répondre de toute fraude signalée.

Enfin, la plupart des autorités compétentes ne sont pas en mesure d'enquêter sur chacun des signalements portés à leur attention. Elles ne disposent tout simplement pas des ressources à cette fin et doivent hiérarchiser les questions à traiter. Elles doivent décider s'il convient ou non d'ouvrir une enquête en fonction de toute une série de facteurs, et notamment en examinant les points suivants:

- L'autorité compétente peut-elle connaître de l'affaire?
- Un autre organisme est-il compétent? Dans l'affirmative, est-il préférable que ce soit lui qui mène l'enquête?
- À quand remontent les faits allégués? Sera-t-il possible de rassembler suffisamment de preuves crédibles si beaucoup de temps s'est écoulé depuis?
- Une enquête servirait-elle l'intérêt général?
- Les conséquences pour le plaignant ou d'autres personnes sont-elles importantes?
- La plainte soulève-t-elle des problèmes de nature systémique?
- Serait-ce une utilisation judicieuse des ressources que d'ouvrir une enquête?[133]

L'autorité compétente doit pouvoir exposer clairement les raisons pour lesquelles elle enquêtera ou refusera d'enquêter sur un signalement en particulier. Elle devrait également faire part de sa décision à cet égard à la personne qui a effectué le signalement, et garder une trace de ces démarches. Si de plus amples informations sont recueillies, peut-être lorsqu'une tierce personne communique d'autres informations, il est possible de lancer ou de rouvrir une enquête. L'enjeu principal reste de faire en sorte que les informations soient examinées sur le fond.

Si des informations doivent être communiquées à d'autres autorités, il conviendrait de prévoir des garanties appropriées. En 2009, la Nouvelle-Zélande a modifié le *Protected Disclosures Act* (loi sur les révélations protégées) afin de combler certaines lacunes en la matière. Les nouvelles dispositions autorisent le transfert d'informations entre autorités et exigent que la personne qui communique les informations soit informée de tout transfert et que les informations transmises soient toujours considérées comme une révélation protégée[134].

L'Anti-Corruption and Civil Rights Commission de la République de Corée suit un modèle différent: comme elle supervise les enquêtes de toutes les autres autorités, ses attributions lui permettent automatiquement de communiquer avec les autres organismes et de conserver le pouvoir de protéger à ce titre les personnes qui effectuent des signalements.

[133] Un certain nombre de guides et de sources d'informations concernant l'ouverture d'enquêtes sont disponibles en ligne. Voir, par exemple, le site Web de l'Independent Commission against Corruption de la Nouvelle-Galles du Sud (Australie), à l'adresse: http://www.icac.nsw.gov.au/, ainsi que le guide en matière d'enquêtes préparé par l'Asian Pacific Forum concernant les enquêtes sur des violations des droits de l'homme (Asia Pacific Forum, 2012).

[134] Nouvelle-Zélande, *Protected Disclosures Act*, 2000, art. 16.

Au Pérou, le Sistema Nacional de Atención de Denuncias (système national de traitement des dénonciations; voir chapitre Ier, section C.2) est conçu de telle manière qu'il est possible d'examiner l'information provenant d'une seule source (à savoir la personne qui la communique) à la lumière d'autres informations se trouvant dans ce système. Il s'agit là d'un moyen de vérification et de corroboration des signalements reçus par le système, mais aussi d'une méthode visant à mettre l'information communiquée en rapport avec des données ou informations existantes qui ont été recueillies auprès d'autres sources.

3. Devoirs et obligations

Tous les signalements devraient être examinés sur le fond et les personnes à l'origine de ces signalements devraient être tenues informées des décisions prises, par exemple concernant le point de savoir si une enquête sera ouverte ou non ou si la question est du ressort d'un autre organisme. Dans le secteur public, les lois visant à protéger les révélations d'intérêt général peuvent inclure des obligations d'enquêter avec équité et rigueur et de rendre compte des résultats obtenus. Par exemple, en Australie, le *Public Interest Disclosure Act* (loi sur les révélations d'intérêt général) fait peser l'obligation d'enquêter sur le "principal responsable" de l'organisme public et prévoit des délais dans lesquels il doit rendre compte des résultats obtenus ou faire part de toute décision de ne pas enquêter. Il est possible de déposer une plainte auprès de l'ombudsman concernant une décision ou la conduite de l'enquête[135].

S'il n'est pas facile d'imposer une obligation d'enquêter sur tous les signalements d'abus commis sur un lieu de travail[136], il n'est guère difficile de veiller à ce que des autorités compétentes mettent en place des mécanismes, enregistrent les informations et passent en revue toutes les révélations afin de déterminer s'il existe à première vue un cas de fraude ou non.

Afin que le public continue à accorder sa confiance aux systèmes de signalement, les autorités compétentes ont généralement le devoir de veiller à publier chaque année diverses informations concernant leur système de signalement et son fonctionnement. Des efforts devraient être consentis afin de publier autant d'informations que nécessaire tout en prenant soin de protéger le caractère confidentiel de l'identité des personnes qui effectuent des signalements ou des données personnelles de tierces parties. Le genre d'informations pouvant être mis à la disposition du public comprend le nombre de signalements effectués, les types de problèmes signalés, le nombre de signalements ayant conduit à une enquête plus poussée et le nombre de signalements ayant abouti à des mesures, ainsi que des informations générales et des données statistiques concernant les types de sanctions. Il conviendrait aussi de donner des informations au sujet du nombre et du type de mesures prises pour protéger les personnes ayant effectué les signalements.

[135] Australie, *Public Interest Disclosure Act*, 2013, art. 47 à 50.

[136] La disposition C.3.5. du *Code of Corporate Governance* du Royaume-Uni (code de gouvernance des entreprises) en est un exemple. Cette disposition prévoit que "[l]e comité d'audit examine le dispositif en vertu duquel les membres du personnel de la compagnie peuvent, à titre confidentiel, faire part de leurs préoccupations concernant d'éventuelles pratiques abusives en matière d'établissement d'états financiers ou dans d'autres domaines. L'objectif du comité d'audit devrait consister à s'assurer qu'un dispositif est en place pour permettre de mener une enquête indépendante et proportionnée concernant de telles pratiques, et de prendre des mesures de suivi adaptées". Le code est disponible à l'adresse: https://www.frc.org.uk/Our-Work/ Publications/Corporate-Governance/UK-Corporate-Governance-Code-2014.pdf.

Extrait d'un entretien avec Bertrand de Speville, ancien responsable de l'Independent Commission Against Corruption (Hong Kong)

"Premièrement, lorsqu'un citoyen a pris son courage à deux mains pour venir vous donner des informations, si vous n'accordez aucune importance ni à lui ni à sa plainte, il ne reviendra jamais vous voir. Vous l'avez perdu et vous avez probablement aussi perdu tous ses amis. On ne saurait gagner la lutte contre la corruption sans obtenir de bonnes informations de la part de la communauté [...].

La deuxième raison [d'enquêter sur toutes les allégations de corruption] est la suivante: des enquêteurs chevronnés vous diront qu'une affaire qui peut de prime abord paraître insignifiante se révèle bien plus grave lorsqu'ils l'examinent de plus près. Seule la pointe de l'iceberg vous est montrée [...]. Lorsque [des enquêteurs] commencent à creuser, ils peuvent finir par découvrir une affaire de grande envergure.

La troisième raison est peut-être la plus importante [...]: si l'organisme de lutte contre la corruption donne l'impression de choisir à son gré dans quels cas il faut ouvrir une enquête ou non, il perdra très rapidement la confiance du public qui ne le verra plus comme un organisme impartial et indépendant.

La quatrième raison comporte une certaine dimension éthique: il n'est pas juste [...] qu'un organisme de lutte contre la corruption laisse entendre à la communauté que certains cas de corruption comptent tandis que d'autres non. Il ne saurait y avoir deux poids deux mesures [...].

La cinquième raison découle de l'amère expérience que nous avons faite, à savoir que même un acte de corruption anodin peut avoir des conséquences désastreuses. Il suffit de songer au domaine de la sécurité ou de la santé publiques pour prendre la mesure de l'effet papillon."

Source: Université de Princeton, entretien avec Bertrand de Speville dans le cadre de l'initiative "Innovations for Successful Societies", Oral History Programme, Bobst Center for Peace and Justice, 2013, disponible à l'adresse: http://successfulsocieties.princeton.edu/sites/successfulsocieties/files/interviews/transcripts/3552/bertrand_despeville.pdf.

On trouvera ci-après un aperçu des nombreux devoirs et obligations qui incombent actuellement aux autorités compétentes dans le cadre de leur mandat consistant à assister et protéger les personnes qui communiquent des informations:

- Préserver la confidentialité de l'identité des personnes qui communiquent des informations.
- Mettre en place une procédure claire pour traiter les signalements et faire part aux personnes qui communiquent des informations de la suite donnée à l'affaire:
  - Fixer des délais pour l'évaluation initiale;
  - Pour les affaires retenues, convenir d'un système régulier de retour d'informations et s'y conformer.
- Faire figurer les données suivantes dans des rapports publiés régulièrement:
  - Nombre et type de problèmes rapportés;
  - Nombre de mesures coercitives déclenchées grâce aux personnes ayant communiqué des informations (si possible en ventilant les données en fonction des différentes catégories de personnes ayant communiqué des informations);
  - Nombre et type de plaintes concernant la décision d'enquêter ou la façon dont l'enquête sera menée;

- Nombre d'affaires portant sur les préjudices subis par des personnes ayant communiqué des informations dont l'autorité a été saisie, et affaires portées devant la justice pour traitement injuste;
- Nombre d'organisations (secteurs réglementés) n'ayant pas mis en place un dispositif d'alerte efficace;
- Mesures prises pour promouvoir ou mettre en œuvre un tel dispositif.

F. Fourniture d'une aide et de conseils

Les protections offertes par la loi aux personnes qui communiquent des informations contribuent largement à rassurer celles-ci quant au fait qu'il est sûr et acceptable de signaler des cas de corruption présumés ou d'autres actes illicites susceptibles d'être rapportés. Toutefois, des questions subsisteront toujours sur la façon dont de telles lois s'appliquent dans chaque cas. Il arrive que les personnes concernées ne sachent pas avec certitude si elles doivent faire part de leurs préoccupations, comment procéder ou à qui s'adresser. Elles peuvent douter de la nature de ce qu'elles ont vu ou se demander si leur employeur ou les autorités compétentes accueilleront favorablement les informations qu'elles détiennent. Elles peuvent être au courant de la façon dont d'autres personnes ont été traitées après avoir soulevé des questions similaires, et craindre pour leur propre situation.

Il est possible de régler nombre de problèmes en donnant des informations et des conseils à un stade précoce. Sur le lieu de travail, les syndicats et des points de contact internes tels que les conseillers en déontologie constituent de bonnes sources d'informations. Il est toutefois plus difficile de donner accès à des conseils impartiaux.

Informations et conseils

Avoir accès à des informations et à des conseils à un stade précoce peut aider à résoudre des questions ou des problèmes qui, s'ils demeurent sans réponse, risquent de dissuader des individus de consciencieusement faire part de leurs préoccupations. Ceux-ci peuvent douter de la pertinence de l'information qu'ils détiennent ou ne pas savoir à qui s'adresser. Leur apporter des conseils les aide à comprendre les termes pratiques de la loi ainsi que les risques et opportunités d'un signalement. Il arrive que l'autorité compétente fasse clairement savoir qu'un conseiller peut entreprendre les premières démarches, comme c'est le cas en République de Corée[137].

Alors que les autorités compétentes peuvent fournir des informations sur la façon dont elles traiteront les signalements et donner des précisions sur le sens de la loi, elles ne sont pas en mesure de donner des conseils juridiques impartiaux ou individuels. Certains États parties se sont penchés sur la manière de fournir de tels conseils. Par exemple, en République de Corée, l'Anti-Corruption and Civil Rights Commission peut demander à l'ordre des avocats coréens de fournir des conseils en matière de droit et de procédure judiciaire au titre de l'aide juridique. Les Pays-Bas sont l'un des rares pays où le Gouvernement a directement alloué des ressources à un centre de conseil juridique destiné à guider les lanceurs d'alerte.

[137] République de Corée, *Act on Anti-Corruption* (loi modifiée en 2012), art. 39.

Exemple: Centre de conseil pour les lanceurs d'alerte, financé par le Gouvernement néerlandais

Afin d'aider et d'encourager de potentiels lanceurs d'alerte à signaler des fraudes ou des irrégularités, le Gouvernement néerlandais et des partenaires sociaux (dont des organisations représentatives d'employeurs et de salariés) ont décidé qu'il était nécessaire de leur apporter gratuitement des conseils et un soutien. L'Adviespunt Klokkenluiders (centre de conseil pour les lanceurs d'alerte) a été ouvert en octobre 2012 et a fait l'objet d'une évaluation à la mi-2014. Cette évaluation a révélé que le Centre avait acquis une solide réputation dans le domaine qui est le sien, et il a été recommandé d'adopter une loi visant à assurer sa pérennité.

Le Centre de conseil, qui est doté de la personnalité juridique, est financé par le Ministère de l'intérieur et le Ministère des affaires sociales et de l'emploi, tout en demeurant indépendant vis-à-vis de ceux-ci. Il comprend un comité de trois membres qui représentent le secteur privé, le secteur public et les syndicats, ainsi qu'une petite équipe composée d'un directeur, de trois conseillers juridiques principaux, d'un consultant en communication qui travaille à temps partiel, d'un secrétaire et d'un assistant administratif. Le rapport annuel du Centre et d'autres documents sont disponibles en anglais sur son site Web (www.adviespuntklokkenluiders.nl).

Les conseillers en déontologie et les syndicats constituent d'autres importantes sources d'informations et de conseils pour les personnes qui effectuent des signalements. Les services du médiateur fournissent également des informations à des particuliers sur leur lieu de travail et en dehors de celui-ci. Un certain nombre d'organisations et de groupes de la société civile offrent des conseils juridiques, des renseignements et un soutien aux lanceurs d'alerte. Au rang des initiatives apportant un soutien direct aux lanceurs d'alerte on citera notamment les suivantes: Government Accountability Project (États-Unis), Public Concern at Work (Royaume-Uni), Open Democracy Advice Centre (Afrique du Sud), Canadians for Accountability, Whistleblower-Netzwerk (Allemagne) et Whistleblowers Australia. Dans le domaine de la corruption en particulier, des Advocacy and Legal Advice Centres (centres de sensibilisation et de conseil juridique) ont été créés dans le cadre des volets nationaux de l'organisation Transparency International. À l'heure actuelle, des centres sont opérationnels dans 60 pays, y compris en Irlande, en Russie et dans beaucoup de pays d'Amérique latine (comme au Guatemala et au Honduras, par exemple). Ils offrent des informations et des conseils aux personnes qui souhaitent signaler des cas de corruption[138]. Il existe également des organisations dont l'action à une portée internationale, telles que Blueprint for Free Speech[139], et de nouveaux réseaux, à l'instar du Whistleblowing International Network, qui s'emploient à renforcer les capacités locales en matière de conseil et de défense des lanceurs d'alerte.

[138] Une liste des Advocacy and Legal Advice Centres de Transparency International est disponible à l'adresse: http://www.transparency.org/getinvolved/report.

[139] Voir Government Accountability Project (www.whistleblower.org); Public Concern at Work (www.pcaw.org.uk); Open Democracy Advice Centre (www.opendemocracy.org.za); Canadians for Accountability (canadians4accountability.org); Whistleblower-Netzwerk (www.whistleblower-net.de); Whistleblowers Australia (www.whistleblowers.org.au); et Blueprint for Free Speech (https://blueprintforfreespeech.net). Pour des informations concernant d'autres organismes non gouvernementaux qui travaillent dans ce domaine, voir le Whistleblowing International Network, à l'adresse: www.whistleblowingnetwork.org.

III.

Mise en œuvre

A. Formation et spécialisation

Les services de signalement interne ainsi que les organismes désignés, tels que les organismes de lutte contre la corruption ou les unités de police, constituent les principaux points de contact des personnes qui communiquent des informations. Si ces services et organismes font correctement leur travail, les personnes qui communiquent des informations seront moins en proie au stress et à l'anxiété, et plus enclines à signaler des actes illicites.

Il est nécessaire que les États parties s'interrogent sur la façon de répartir les compétences et d'instaurer un cadre institutionnel pour faciliter leur travail. Une solution consiste à désigner une autorité principale qui a compétence pour recevoir les signalements et enquêter à leur sujet, et pour s'assurer que ces signalements sont orientés vers la bonne autorité, le cas échéant. Il est aussi possible de désigner une autorité de surveillance qui sera chargée de veiller à ce que d'autres autorités mettent correctement en œuvre les règles régissant la protection des personnes qui communiquent des informations, et de suivre leur efficacité au fil du temps. Dans certains pays, le rôle du médiateur peut très probablement se prêter à cette tâche. Aux Pays-Bas, par exemple, on a préconisé la création d'un organisme unique consacré aux lanceurs d'alerte. Cela étant, l'existence d'une institution "principale" ne signifie pas que les personnes qui communiquent des informations devraient perdre leur droit à une protection si elles signalent des actes illicites à un autre organisme compétent, d'autant plus que l'expérience a montré que le fait de restreindre ainsi le dispositif de protection compromet la crédibilité et l'efficacité du système dans son ensemble.

De nombreux États disposent de diverses autorités compétentes chargées de contrôler certains secteurs ou branches d'activité. Si nombre d'entre elles reçoivent déjà des informations concernant des abus, elles n'ont pas forcément conscience qu'il est nécessaire de traiter ces signalements autrement qu'en passant par leurs systèmes habituels de réclamations du public. Si aucune distinction n'est opérée entre les réclamations et les signalements, d'importantes informations concernant des cas de corruption peuvent passer inaperçues.

Certains pays ont créé des organismes indépendants dotés de pouvoirs spécialisés en matière de détection et de répression afin de lutter expressément contre la corruption. Même si un point de contact unique peut offrir des avantages en termes de clarté pour les personnes qui communiquent des informations, il peut présenter deux inconvénients. Premièrement, comme indiqué précédemment, il existe un risque qu'un organisme unique se voie attribuer le monopole du pouvoir. Dans un tel cas de figure, il sera nécessaire de soumettre cet organisme à des règles claires de responsabilité vis-à-vis du public afin d'assurer son bon fonctionnement. Le deuxième inconvénient n'est pas tant lié au risque d'abus ou d'engorgement qu'à la façon dont le rôle de l'organisme est perçu. Les attentes du public eu égard à son efficacité peuvent être bien supérieures à ce qu'une institution unique peut accomplir en réalité. En outre, la création d'un point de contact unique peut compromettre la faculté, la capacité ou même la volonté de toute autre institution ou de tout autre organisme d'assumer la responsabilité de s'attaquer à la corruption et à d'autres actes illicites ou risques.

Les États parties devront nécessairement prendre en considération les implications financières de toute mesure qu'ils mettent en place. Les ressources nécessaires pour instaurer un système efficace peuvent paraître conséquentes au début, mais les économies globales qu'un tel système permettra de dégager en prévenant les gaspillages et les dommages peuvent se révéler importantes. Si des poursuites aboutissent, il se peut aussi que d'importantes sommes d'argent soient recouvrées.

La formation revêt une importance cruciale et sera incontournable pour les personnes qui travaillent avec des dispositifs internes, comme ceux des administrations, ainsi que pour les autorités compétentes. La formation proposée doit porter sur plusieurs sujets, notamment:

- Le cadre juridique;
- Le respect de la confidentialité;
- La différenciation des besoins des différentes sources d'informations;
- Les retours d'information et les mesures destinées à rassurer;
- La conservation des données et les garanties pour se prémunir contre les fuites;
- Les questions touchant à la responsabilité interne et externe.

B. Activités de promotion et de sensibilisation

Des activités efficaces de sensibilisation, de communication, de formation et d'évaluation doivent être menées auprès de l'ensemble des parties prenantes afin de soutenir les lois destinées à protéger les personnes qui communiquent des informations. Il faut que les employés et les employeurs des secteurs public et privé connaissent leurs droits et leurs responsabilités en matière de signalement d'irrégularités et d'enquêtes à ce sujet. Les employés et les personnes qui travaillent avec des organisations doivent avoir connaissance des dispositifs en place, de leur droit de signaler directement des abus à une autorité compétente, de la manière d'obtenir des conseils à titre confidentiel et des mesures de protection à leur disposition, ainsi que des restrictions à ces mesures. Il est nécessaire que les individus qui seraient tentés d'exercer des représailles contre des personnes ayant communiqué des informations — que ce soit sur leur lieu de travail ou en dehors de celui-ci — soient informés des peines et sanctions qui peuvent leur être infligées.

Une évaluation nationale entreprise au début de chaque programme de réforme aidera les États parties à mieux faire connaître les nouvelles mesures une fois qu'elles sont en

place. Une campagne de sensibilisation de l'opinion est un moyen d'instaurer une certaine perception culturelle des lanceurs d'alerte afin que le public les considère comme des personnes qui agissent pour le bien commun et par loyauté envers leur organisation, leur profession et leur société, plutôt que comme des traitres ou des informateurs.

C'est pourquoi le principe fondamental veut que la protection des personnes qui communiquent des informations fasse fond sur la liberté d'expression et le droit à l'information (tels qu'exposés en détail au chapitre II), comme l'entend la Convention contre la corruption (paragraphe 1 de l'article 13). Dans de nombreux pays, des organisations de la société civile spécialisées dans les signalements d'abus et des domaines apparentés apporteront leur concours afin de promouvoir l'idée d'un système de protection pour les personnes qui communiquent des informations. Par exemple, la Convention de l'Union africaine sur la prévention et la lutte contre la corruption impose aux États parties de "[m]ettre en place et renforcer des mécanismes visant à promouvoir l'éducation des populations au respect de la chose publique et de l'intérêt général et la sensibilisation à la lutte contre la corruption et infractions assimilées, y compris des programmes scolaires et la sensibilisation des médias, et à créer un environnement propice au respect de l'éthique[140]".

Exemples: La sensibilisation du public

Ghana

La Ghana Anti-Corruption Coalition (coalition ghanéenne de lutte contre la corruption) a lancé une campagne de lutte contre la corruption intitulée "Speak up" (ne gardez pas le silence) afin de faire connaître aux citoyens ghanéens la législation anticorruption de leur pays, plus précisément le *Whistleblower Act* de 2006 (loi 720 sur les lanceurs d'alerte). Cette coalition travaille en collaboration avec Global Media Alliance, et notamment avec e.tv Ghana ainsi que deux programmes radiophoniques.

Le projet "Speak up" vise à encourager les Ghanéens à intervenir et à dénoncer des cas de corruption de toutes sortes, particulièrement dans les secteurs de l'éducation et de la santé. Il a été conçu comme un projet purement interactif qui permet au public de donner son avis et de poser des questions sur le *Whistleblower Act* et la corruption en général, et ce, en appelant l'émission, en envoyant des SMS au 1721 depuis tous les réseaux et au 1821 pour les utilisateurs d'Airtel, ainsi qu'en réagissant sur la page Facebook officielle du projet.

Monténégro

Au Monténégro, la Direction chargée de l'initiative de lutte contre la corruption (DACI) a mené de nombreuses campagnes de sensibilisation ces dernières années. Pour sa campagne "Ne versez pas un centime de pot-de-vin", lancée en 2012, la DACI a recours à des dépliants contenant les numéros de permanences téléphoniques, des panneaux d'affichage, des vidéos télévisées, des affiches, des brochures et des messages publicitaires sonores, et émet des "billets de banque n'ayant aucune valeur" afin de décourager la corruption. Dans le cadre de la campagne "La corruption n'est pas une option", l'administration des douanes a distribué 20 000 prospectus. La DACI a mené d'autres campagnes intitulées "Ouvrez les yeux et dénoncez les cas de corruption", "Éradiquez le virus en dénonçant les cas de corruption", "Dénoncer la corruption = la bonne décision" et "Il existe toujours un moyen de dénoncer la corruption".

Source: Izvještaj o broju prijava o korupciji za period jul-decembar 2013. Godine (rapport sur le nombre de cas de corruption signalés entre juillet et décembre 2013), Direction chargée de l'initiative de lutte contre la corruption au Monténégro, janvier 2014. Suite de la campagne "Ne versez pas un centime de pot-de-vin", Direction chargée de l'initiative de lutte contre la corruption, 23 juillet 2014, disponible à l'adresse: antikorupcija.me/en/index.php?option=comcontent&view=article&id=277:campaign-not-a-cent-for-bribe-continued&catid=42:daci-news&Itemid=291.

[140] Paragraphe 8 de l'article 5 de la Convention de l'Union africaine sur la prévention et la lutte contre la corruption.

C. Coopération internationale

Les États parties devraient également se pencher sur les questions susceptibles de se poser en matière de signalements internationaux, à savoir lorsqu'une personne qui se trouve dans un pays communique des informations aux autorités d'un autre pays. Cela s'est déjà produit, par exemple, en Suisse et au Liechtenstein où des employés de banque ont divulgué des informations — parfois en échange de récompenses — à des autorités fiscales d'autres pays. Au Royaume-Uni, par exemple, le *Public Interest Disclosure Act* (loi sur les révélations d'intérêt général) s'applique aux personnes qui ont un contrat de travail, indépendamment de l'endroit où la fraude a été commise et du fait de savoir si le manquement à une obligation juridique relève de la législation britannique ou de la législation applicable d'un autre pays. Cette approche, que l'Irlande a également consacrée dans son *Protected Disclosures Act* (loi sur les révélations protégées), peut aider à assurer une couverture plus complète et cohérente des affaires internationales.

Bien que les organismes de contrôle habilités à recevoir des révélations n'aient qu'une compétence nationale, on pourrait s'attendre qu'ils transmettent à des autorités étrangères toute information relative à des actes illégaux commis à l'étranger. Il pourrait être nécessaire de prendre des précautions supplémentaires au moment de partager de telles informations, notamment de protéger l'identité de la personne qui les a communiquées, et les autorités pourraient demander des garanties fiables quant à la confidentialité des informations ainsi qu'à la sécurité et la protection de l'intéressé afin qu'il ne subisse pas de représailles dans le pays qui reçoit les informations. À titre d'exemple, certaines affaires de corruption d'envergure internationale ont mis en lumière des lacunes en matière de protection des lanceurs d'alerte dans un contexte international, une situation qui appelle des mesures de suivi[141].

D. Suivi et évaluation

Il importe que les États parties contrôlent l'efficacité des réformes ou initiatives mises en place. Le processus de consultation mené au moment de l'évaluation initiale avant d'entreprendre des réformes aide à obtenir des données de référence importantes à partir desquelles il est possible d'évaluer toutes les nouvelles mesures qui sont mises en œuvre[142]. Une analyse régulière de la jurisprudence ou des décisions judiciaires pertinentes peut également être une source d'informations fort utile. La plupart des lois, y compris bon nombre de celles qui sont citées en exemple dans le présent Guide, sont encore relativement récentes, et peu de leçons peuvent être tirées de leur mise en œuvre pour le moment.

L'obligation faite aux autorités compétentes de rendre compte de leurs activités garantira que des données sont disponibles pour pouvoir mener un contrôle efficace. Ces données, conjuguées à d'autres indicateurs présentés ci-après, devraient aider les États parties à mieux appréhender la façon dont le système fonctionne et à savoir si des améliorations ou des changements devraient lui être apportés.

[141] Voir par exemple au Royaume-Uni l'affaire *Foxley* c. *GPT Project Management Ltd.* portée devant l'Employment Tribunal (juridiction du travail), nº 22008793/2011 (12 août 2011). Un résumé des principaux problèmes soulevés est disponible dans le rapport de phase 3 sur la mise en œuvre par le Royaume-Uni, publié par l'OCDE, par. 197 à 203, disponible à l'adresse: http://www.oecd.org/fr/daf/anti-corruption/ RoyaumeUniPhase3FR.pdf.

[142] OCDE, Revisiting Whistleblower Protection in OECD Countries: from Commitments to Effective Protection, éditions OCDE, Paris (à paraître).

Indicateurs d'efficacité

Dans son récent rapport sur la protection des lanceurs d'alerte et la Convention des Nations Unies contre la corruption, l'organisation Transparency International a dressé une liste de questions que les États parties et les praticiens peuvent utiliser pour évaluer l'efficacité de la législation et des mécanismes en place destinés à favoriser le lancement d'alertes[143]. La liste ci-dessous s'inspire de ces questions mais a été adaptée pour s'appliquer de manière générale aux personnes qui communiquent des informations (et non pas uniquement aux lanceurs d'alerte qui signalent des abus sur leur lieu de travail):

- Quelles mesures ont été prises pour veiller à ce que la législation soit bien connue?
- Des études ont-elles été publiées sur l'impact de la législation (y compris des études et recherches indépendantes)?
- Y a-t-il des exemples d'affaires de corruption importantes qui ont été découvertes par des personnes ayant communiqué des informations et des lanceurs d'alerte ayant effectué un signalement sur leur lieu de travail?
- Y a-t-il des exemples d'affaires de corruption importantes qui n'ont pas fait l'objet de signalements à un stade initial? Qu'est-ce qui a empêché les personnes au courant de se manifester plus tôt?
- Combien de signalements les institutions publiques ont-elles reçus de la part de particuliers?
- Combien d'appels tendant à obtenir des informations et des conseils sur les signalements les autorités compétentes ont-elles reçus? Quelle activité enregistre le site Web de l'autorité compétente (notamment le nombre de visiteurs qui ont consulté des pages concernant les signalements et les mesures de protection)?
- Dans combien de cas des mesures de protection ont-elles été demandées pour parer à des actes de représailles?
- Combien y a-t-il eu de primes de compensation et quel était leur montant?
- Quels sont les exemples de politiques et procédures organisationnelles mises en œuvre?
- Que pense la société civile de leur impact?

En ce qui concerne les protections dont les personnes qui communiquent des informations peuvent bénéficier sur leur lieu de travail, l'exhaustivité et les forces de différentes dispositions législatives ont été examinées, d'une part, par Transparency International en 2013 s'agissant de l'ensemble de l'Union européenne[144] et, d'autre part, par l'Organisation de coopération et de développement économiques (OCDE) en 2011 pour tous les pays du G20[145]. La suite à donner au plan d'action du G20 a été abordée dans un rapport préparé en 2014 par un consortium de chercheurs et d'ONG qui a évalué, en se basant sur 14 critères principaux, l'exhaustivité des régimes de protection en faveur des lanceurs d'alerte mis en place dans les pays du G20[146]. Même s'il n'existe pas de point de

[143] Transparency International, Whistleblower Protection and the UN Convention Against Corruption, Berlin, 2013, disponible à l'adresse: http://www.transparency.org/whatwedo/publication/whistleblower_protection_and_the_un_convention_against_corruption.

[144] Worth, M., Whistleblowing in Europe, Legal Protections for Whistleblowers in the EU, Transparency International, 2013, disponible à l'adresse: http://www.transparency.org/whatwedo/publication/whistleblowing_in_europe_legal_protections_for_whistleblowers_in_the_eu.

[145] OCDE, *Study on Whistleblower Protection Frameworks, Compendium of Best Practices and Guiding Principles for Legislation*, 2011, disponible à l'adresse: http://www.oecd.org/g20/topics/anti-corruption/ 48972967.pdf.

[146] Wolfe, S., M. Worth, S. Dreyfus et A. J. Brown, *Whistleblower Protection Laws in G20 Countries: Priorities for Action,* Blueprint for Free Speech, Griffith University, Université de Melbourne, Transparency International Australia, 2014, disponible à l'adresse: https://blueprintforfreespeech.net.

comparaison unique à l'échelon international pour évaluer de telles dispositions législatives, les critères utilisés dans ces études pour comparer la teneur des lois destinées à protéger les lanceurs d'alerte devraient aider les États parties à étudier les mesures de protection qui s'appliquent de manière plus générale aux personnes qui communiquent des informations.

La recommandation du Conseil de l'Europe sur la protection des lanceurs d'alerte propose un ensemble de principes directeurs qui peuvent aider les États parties à vérifier si leurs cadres nationaux, institutionnels et juridiques sont suffisamment robustes pour aider et protéger les personnes qui communiquent des informations dans un contexte professionnel.

Tableau 1. Critères d'évaluation basés sur les principes du Conseil de l'Europe

Définitions	
	Définition du terme "lanceur d'alerte"
	Définition de l'expression "signalement ou révélation d'informations d'intérêt général"
	Définition du terme "signalement"
	Définition de l'expression "révélation d'informations"
Champ d'application matériel	
1	Le cadre national devrait établir des règles destinées à protéger les droits et les intérêts des lanceurs d'alerte
2	Champ d'application de l'intérêt général
Champ d'application personnel	
3	Définition large des relations de travail
4	Inclut les personnes dont la relation de travail a pris fin ainsi que les personnes se trouvant à un autre stade de la négociation précontractuelle
5	Les règles qui s'appliquent aux informations relatives à la sécurité nationale sont conformes à la jurisprudence de la Cour européenne des droits de l'homme
6	Pas d'atteinte aux règles garantissant la protection du secret professionnel
Cadre normatif	
7	Approche globale et cohérente pour faciliter les alertes
8	Les restrictions ou exceptions ne devraient pas aller au-delà de ce qui est nécessaire
9	Veiller à ce que des mécanismes effectifs de réaction aux signalements et aux révélations d'informations d'intérêt général soient en place
10	Conservation de la protection et des voies de recours offertes en vertu des règles de droit général aux personnes ayant subi un préjudice du fait d'avoir lancé une alerte
11	Les employeurs ne peuvent se prévaloir des obligations légales ou contractuelles d'une personne pour l'empêcher de faire une révélation d'informations d'intérêt général, ou pour la sanctionner pour cette action
Voies de signalement et de révélation d'informations	
12	Mesures favorisant un environnement qui encourage à faire ouvertement toute révélation d'informations
13	Des voies clairement établies pour le signalement sont mises en place
14	Les différentes voies de signalements comprennent la possibilité de révéler des informations au public, notamment par l'intermédiaire des médias
15	Les employeurs sont encouragés à mettre en place des procédures internes

16	Les travailleurs doivent être consultés sur les procédures internes
17	En règle générale, les révélations d'informations et les signalements internes faits aux organes réglementaires sont à encourager
Confidentialité	
18	Les personnes qui communiquent des informations ont droit à la confidentialité de leur identité
Réaction au signalement et à la révélation d'informations	
19	Les signalements devraient donner rapidement lieu à une enquête
20	Les personnes qui communiquent des informations devraient être informées de l'action entreprise
Protection contre les représailles	
21	Il convient d'assurer une protection contre toutes formes de représailles
22	La personne qui a eu des motifs raisonnables de signaler une inconduite particulière ne devrait pas perdre le bénéfice de sa protection au motif qu'elle a commis une erreur d'appréciation
23	Pouvoir d'invoquer le fait que la révélation d'informations a été faite conformément au cadre national
24	Le fait de ne pas avoir eu recours au dispositif interne peut être pris en considération lorsqu'il s'agit de décider des voies de recours
25	La charge de la preuve pèse sur l'employeur en cas d'allégation d'acte préjudiciable ou de représailles
26	Des mesures provisoires devraient pouvoir être sollicitées
Conseil, sensibilisation et évaluation	
27	Le cadre national devrait faire l'objet d'une large promotion
28	Des conseils confidentiels devraient être proposés (de préférence gratuitement)
29	Évaluations périodiques de l'efficacité du cadre national

Source: Recommandation CM/Rec(2014)7 du Comité des Ministres aux États membres sur la protection des lanceurs d'alerte (adoptée par le Comité des Ministres le 30 avril 2014, lors de la 1198e réunion des délégués des Ministres), disponible à l'adresse: https://wcd.coe.int/ViewDoc.jsp?id=2188939&Site=CM.

Voir aussi: Conseil de l'Europe, document technique, *Expert opinion on the draft law on protection of whistleblowers*, préparé par Paul Stephenson et Wim Vandekerckhove, 2014, p. 22 à 25, disponible à l'adresse: http://www.coe.int/t/dghl/cooperation/economiccrime/corruption/Projects/PACS-Serbia/Technical%20Paper/TP8%202014%20PACS%20Expert%20Opinion-draft%20Law-Protection-Whistleblowers_EN.pdf.

L'efficacité d'un dispositif de protection dépendra de la manière dont les organisations et les autorités compétentes le mettent en œuvre. Certains pays disposent de normes officielles pour de telles procédures et ils peuvent les mettre à profit à des fins d'évaluation et d'analyse comparative. Par exemple, l'organisation Standards Australia a élaboré en 2003 une norme pour les programmes de protection des lanceurs d'alerte relevant du secteur privé[147], et le British Standards Institute a créé en 2008 un code de bonnes pratiques pour les dispositifs internes d'alerte[148]. Au Royaume-Uni, c'est le National Audit Office qui évalue les procédures des agences publiques[149], et en Australie, des chercheurs indépendants financés par le Gouvernement ont eu recours à des normes de

[147] Voir AS 8004-2003, disponible à l'adresse: http://infostore.saiglobal.com/store/Details.aspx?ProductID =323803.

[148] British Standards, PAS 1998:2008 — Whistleblowing Arrangements Code of Practice, 2008, disponible aux adresses: http://pcaw.org.uk/bsi et http://shop.bsigroup.com/forms/PASs/PAS-1998/.

[149] National Audit Office, Making a whistleblowing policy work: Report by the Comptroller and Auditor General, document HC 1152, Londres, Royaume-Uni, mars 2014, disponible à l'adresse: http://www.nao.org.uk/wp-content/uploads/2015/03/Making-a-whistleblowing-policy-work.pdf.

cette nature pour évaluer les procédures de nombreuses agences publiques[150]. Or, l'élaboration de nouveaux critères et de travaux de recherche destinés à rendre plus cohérents l'évaluation et le suivi de l'efficacité organisationnelle en matière de protection des lanceurs d'alerte est un domaine qui nécessite encore des travaux plus poussés.

Dans le contexte de la Convention contre la corruption, les évaluations devraient tenir compte des mesures mises en place au profit des différents types de personnes qui communiquent des informations (voir les figures I et II). La possibilité de ventiler les données permettrait de vérifier d'où provient la grande majorité des informations, quelles sont les mesures de protection qui ont été requises et si des modifications doivent être apportées au système.

Même si le but est de protéger les individus contre des actes de représailles et de rendre inutile toute demande d'indemnisation ou toute autre demande de réparation, il est également important de suivre les procédures juridiques qui ont été engagées. S'il s'avère que très peu d'actions intentées à raison de traitements injustes ou d'actes de représailles infligés suite à une alerte sont tranchées en faveur des personnes qui ont communiqué des informations, il convient d'ouvrir une enquête approfondie à ce sujet, dans la mesure où une telle situation est susceptible de décourager de futurs signalements ou alertes concernant des abus commis en milieu professionnel. Pour permettre de telles recherches et analyses, les États parties devraient rendre les jugements pertinents accessibles. Au Royaume-Uni, c'est une organisation non gouvernementale qui contrôle la mise en œuvre du *Public Interest Disclosure Act* (loi sur les révélations d'intérêt général) et l'exécution des jugements qui en découlent[151]. Des chercheurs issus du milieu universitaire pourraient également mener des évaluations utiles.

Réaliser des enquêtes plus larges auprès du public sur la façon dont il perçoit les personnes qui signalent des irrégularités, des actes de corruption ou des menaces permettra aussi d'obtenir de bons indicateurs de l'impact de la loi sur l'amélioration des conditions sociales et culturelles dans lesquelles les individus coopèrent avec les autorités.

[150] Brown, A. J., P. Roberts et J. Olsen, Whistling While They Work: A good-practice guide for managing internal reporting of wrongdoing in public sector organisations, Australia and New Zealand School of Government (ANZSOG), Australie, 2011, disponible à l'adresse: http://press.anu.edu.au/titles/australia-and-new-zealand-school-of-government-anzsog-2/whistling_citation/.

[151] Is the law protecting whistleblowers? A review of PIDA claims, 2011-2013, disponible à l'adresse: http://www.pcaw.org.uk/files/PIDA%20REPORT%20FINAL.pdf.

IV.

Conclusion et aperçu des principaux enseignements à tirer

Les initiatives nationales de lutte contre la corruption ne sont efficaces qu'à condition que le public leur accorde son soutien et sa confiance. Les lois et mesures que les États parties mettent en œuvre pour protéger les personnes qui communiquent des informations doivent être considérées comme légitimes par la société tout entière. Cela signifie qu'elles doivent concorder avec les besoins des personnes qui communiquent des informations et être soigneusement adaptées au contexte national qui est le leur. Il est essentiel — pour la réussite de tout système de lutte contre la corruption qui repose sur la participation du public — que les autorités compétentes soient dotées de mandats clairs et équilibrés, et disposent des pouvoirs et ressources nécessaires pour traiter comme il se doit les informations reçues, ainsi que pour protéger à titre préventif les personnes qui les communiquent. Les mesures visant à protéger les personnes qui communiquent des informations devraient être conçues de façon à surmonter les obstacles qui sont dressés sur le chemin d'une communication ouverte et sécurisée, en particulier lorsque des actes de corruption et autres actes illicites touchent à la chose publique.

Il est recommandé aux États parties de se garder de croire qu'il existe une seule solution idéale ou une formule unique qui fonctionnera en toutes circonstances ou qui continuera d'être efficace au fil du temps. Le présent Guide a adopté une approche générale tout en tendant vers un but précis: il est en effet à espérer que les États parties procéderont à leurs propres recherches et analyses à l'aide des informations qu'il fournit. Un examen approfondi de leur contexte national aidera les États parties à réfléchir à la meilleure façon de mettre en œuvre des dispositifs visant à faciliter les signalements et à protéger ceux qui les utilisent. Étant donné que tous les États font face à des défis communs et que certains principes juridiques peuvent être universellement appliqués, il est primordial que les États parties examinent ceux-ci soigneusement et mènent une vaste consultation pour s'assurer que les mesures qu'ils appliquent sont bien adaptées à leurs contextes nationaux respectifs.

Les auteurs d'actes de corruption tirent parti des faiblesses des systèmes — que ceux-ci soient politiques, économiques, sociaux ou culturels — et modifient leurs pratiques lorsque des lacunes sont comblées ou de nouvelles failles découvertes. Les États parties doivent être prêts à évaluer régulièrement les dispositifs et mesures qu'ils mettent en place afin de déterminer si ceux-ci sont suffisamment solides et souples pour s'adapter à des changements de circonstances, ou s'il est nécessaire d'adopter une nouvelle stratégie.

Aspect plus important encore, la corruption prospère lorsque les individus qui s'en rendent coupables pensent qu'ils peuvent compter sur le silence de ceux qui les entourent, un silence qui bien trop souvent peut être renforcé par un manque de transparence, un accès limité du grand public à l'information et un contrôle insuffisant de la part des citoyens. Les lois qui se limitent à essayer de gérer et de contrôler l'information n'aideront pas à rompre ce silence, pas plus qu'elles ne satisferont aux normes internationales en matière de bonnes pratiques ou ne permettront de prévenir et de combattre la corruption. S'agissant de la participation du public, la protection des personnes qui communiquent des informations doit s'inscrire et être appréhendée dans un cadre général de responsabilité des autorités publiques et de défense des droits de l'homme. L'adoption de mesures énergiques en la matière, tant sur le plan juridique et politique que pour protéger l'intérêt général, permettra aux États parties, aux autorités et aux organisations de tous les secteurs d'identifier et de poursuivre les auteurs d'actes illicites, et contribuera surtout à éviter en premier lieu que la corruption ne prenne racine, et ce pour le bien de tous. Au moment d'envisager de créer ou de réformer des lois et des systèmes pour protéger les personnes qui communiquent des informations, les États parties devraient garder à l'esprit les points ci-après, tels qu'exposés dans le présent Guide:

Introduction

- La Convention contre la corruption donne une définition assez large de l'expression "personnes qui communiquent des informations"; ce concept comprend les personnes qui travaillent dans les secteurs public et privé, les membres du public, ainsi que les témoins, les experts et les victimes.
- Les mesures de protection doivent répondre aux besoins et à la situation de la personne qui communique des informations.
- Le signalement est "facilité" s'il est protégé en droit et clair dans la pratique.

Chapitre premier. Évaluation nationale

- Examiner le cadre juridique et les dispositifs institutionnels qui sont en place afin de renforcer les bonnes pratiques existantes et de déceler les lacunes.
- Mener de larges consultations auprès des représentants concernés des pouvoirs publics, du monde des entreprises, des syndicats, du monde juridique et de la société civile afin de prévoir des réformes avisées et viables.

Chapitre II. Faciliter les signalements et protéger les personnes qui communiquent des informations

- Protéger une grande diversité d'informations susceptibles d'être communiquées, à savoir tout acte répréhensible ou préjudice à l'intérêt général, y compris lorsque l'information communiquée est classée secrète ou de toute autre manière considérée comme confidentielle, et ce afin de:
  - Prévenir la corruption;
  - Ne plus faire peser la charge du risque sur la personne qui communique des informations; et
  - Préserver l'obligation de l'État et des entreprises d'être comptables de leurs actes à l'égard du public.
- Proposer un choix adapté de voies de signalement efficaces afin de fournir une alternative sûre au silence et prévenir tout engorgement ou toute rupture du système.

- Protéger les individus qui révèlent au public des informations concernant des actes illicites, conformément aux principes de la responsabilité démocratique et aux droits de l'homme.
- Examiner la meilleure façon d'utiliser les nouvelles technologies et les méthodes de communication traditionnelles pour faciliter les signalements.
- Les dispositifs de protection devraient comprendre des mesures judiciaires, procédurales et organisationnelles.
- Examiner la manière de fournir des conseils aux personnes qui communiquent des informations.
- Les mesures devraient être préventives afin d'empêcher qu'une personne qui communique des informations ne soit victime d'un traitement injuste, d'un préjudice ou de mesures de représailles. Elles devraient également être rétroactives afin d'accorder une réparation pour tout dommage ou préjudice causé à cette personne en raison du signalement.
- Envisager des moyens novateurs pour encourager les signalements et faire en sorte que la société voie d'un meilleur œil les personnes qui signalent des actes illicites (par exemple en remerciant, en distinguant et en récompensant ces personnes).

Chapitre III. Mise en œuvre

- Veiller à ce que les autorités compétentes aient le mandat, la capacité, les ressources et le pouvoir voulus pour recevoir des signalements, enquêter sur des actes illicites et protéger les personnes qui communiquent des informations.
- Veiller à ce que le personnel des autorités compétentes ait une formation adaptée et dispose de compétences spécialisées afin d'être en mesure de traiter les signalements et de protéger les personnes qui communiquent des informations.
- Veiller à ce que les autorités compétentes soient à l'abri de toute influence indue et puissent s'acquitter de leurs fonctions avec impartialité.
- Envisager de créer ou de désigner une autorité principale ou de surveillance afin de s'assurer que les règles régissant la protection des personnes qui communiquent des informations sont correctement mises en œuvre et suivies au fil du temps.
- Examiner et évaluer périodiquement l'efficacité des dispositifs juridiques et institutionnels visant à protéger les personnes qui communiquent des informations, et s'assurer que le public continue à leur accorder sa confiance.

Ressources

Les États Membres et d'autres parties intéressées disposent d'un certain nombre d'outils pour les aider à étudier la meilleure façon d'encourager et de protéger, dans leurs systèmes et contextes nationaux, les personnes qui communiquent des informations et les lanceurs d'alerte qui signalent des abus commis sur leur lieu de travail. On trouvera ci-après une sélection de quelques-unes des ressources disponibles, classées par grands thèmes, puis une liste de sites Web qui offrent de plus amples informations.

Orientations internationales en matière de protection des lanceurs d'alerte/ personnes qui communiquent des informations

- États-Unis d'Amérique, Government Accountability Project, *International Best Practices for Whistleblower Policies*, GAP, Washington, D. C., 2013, disponible à l'adresse: http://www.whistleblower.org/sites/default/files/Best_Practices_Document_for_website_revised_April_12_2013.pdf.
- Organisation de coopération et de développement économiques (OCDE), *G20 Anti-Corruption Action Plan* (point d'action nº 7: protéger les lanceurs d'alerte), 2010, disponible à l'adresse: http://www.oecd.org/g20/topics/anti-corruption/G20_Anti-Corruption_Action_Plan.pdf.
- OCDE, *Study on Whistleblower Protection Frameworks, Compendium of Best Practices and Guiding Principles for Legislation*, éditions OCDE, Paris, 2011, disponible à l'adresse: http://www.oecd.org/g20/topics/anti-corruption/48972967.pdf.
- OCDE, *Whistleblower protection: encouraging reporting*, CleanGovBiz Initiative, éditions OCDE, Paris, 2012, disponible à l'adresse: www.oecd.org/cleangovbiz/toolkit/50042935.pdf.
- Conseil de l'Europe, Recommandation CM/Rec(2014)7 du Comité des Ministres aux États membres sur la protection des lanceurs d'alerte, disponible à l'adresse: https://wcd.coe.int/ViewDoc.jsp?id=2188939&Site=CM.
- Conseil de l'Europe, Recommandation sur la protection des lanceurs d'alerte, Exposé des motifs, 2014, disponible à l'adresse: https://wcd.coe.int/ViewDoc.jsp?id=2170171&Site=CM.

- Conseil de l'Europe, Résolution 2060 (2015) de l'Assemblée parlementaire, "Améliorer la protection des donneurs d'alerte", disponible à l'adresse: http://assembly.coe.int/nw/ xml/XRef/X2H-Xref-ViewPDF.asp?FileID=21931&lang=fr.
- Transparency International (2013). W*histleblower Protection and the UN Convention against Corruption*, Berlin, 2013, disponible à l'adresse: http://www.transparency.org/whatwedo/publication/whistleblower_protection_and_the_unconvention_against_ corruption.
- Transparency International, *International Principles for Whistleblower Legislation*, 2013, disponible à l'adresse: http://www.transparency.org/whatwedo/publication/international_principles_for_whistleblower_legislation.
- Organisation des États américains, *Model Law to Facilitate and Encourage the Reporting of Acts of Corruption and to Protect Whistleblowers and Witnesses* (loi type visant à faciliter et encourager le signalement des actes de corruption et à protéger les lanceurs d'alerte et les témoins), Washington, D. C., 2013, disponible à l'adresse: http://www.oas.org/juridico/english/draft_model_reporting.pdf.

Droit à l'information, gouvernement transparent et protection des lanceurs d'alerte

- "Principes globaux sur la sécurité nationale et le droit à l'information ("Principes de Tshwane")", 2012, disponible à l'adresse: https://www.opensocietyfoundations.org/sites/default/files/tshwane-french-20150209_0.pdf.
- Voir les principes 37 à 43 concernant la protection des lanceurs d'alerte et les informations classifiées.
- Open Government Guide (ressource en ligne), disponible à l'adresse: http://www.opengovguide.com/topics/whistleblower-protection/.

Réglementation applicable au secteur privé et ayant une portée internationale

- États-Unis d'Amérique, *An Act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes* (loi visant à protéger les investisseurs en améliorant la précision et la fiabilité des révélations d'ordre commercial faites en application de la législation applicable aux titres, ainsi qu'à d'autres fins), 2012 (aussi connu sous le nom de "loi Sarbanes-Oxley").
- États-Unis d'Amérique, *Dodd-Frank Wall Street Reform and Consumer Protection Act* (loi sur la réforme de Wall Street et la protection des consommateurs), 2010 (aussi connu sous le nom de "loi Dodd-Frank").
- Royaume-Uni, *Bribery Act* (loi anticorruption), 2010 (c. 23).

Protection des données et des lanceurs d'alerte/personnes qui communiquent des informations

- Groupe de travail "ARTICLE 29" sur la protection des données, Avis relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements, article 29 donnant des orientations sur les mécanismes de dénonciation, WP 117, 2006, disponible à l'adresse: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_fr.pdf.

Protection des sources

- ONUDC, "*Informer sur la corruption — Un outil de référence pour les gouvernements et les journalistes*", disponible à l'adresse: http://www.unodc.org/documents/corruption/ Publications/2015/15-00373_Ebook.pdf.

Protection des témoins

- ONUDC, "*Bonnes pratiques de protection des témoins dans les procédures pénales afférentes à la criminalité organisée*", publication des Nations Unies, Vienne, 2009, disponible à l'adresse: https://www.unodc.org/documents/organized-crime/ 09-80620_F_ebook.pdf.

Orientations à l'intention des particuliers

- Devine, T. et T. Maassarani, *The Corporate Whistleblower's Survival Guide: A Handbook for Committing the Truth,* Brett-Koehler, Californie, 2011.
- Devine, T., *The Whistleblower's Survival Guide: Courage Without Martyrdom*, Fund for Constitutional Government, Washington, D. C., 1977.
- Ghana Anti-Corruption Coalition, *A Guide to Whistleblowing in Ghana,* 2010, disponible à l'adresse: http://wacmn.gaccgh.org/downloads/files/A%20Guide%20to%20Whistleblowing%20in%20Ghana1.pdf.
- Kohn, S., *The Whistleblower's Handbook: A Step-by-step Guide to Doing What's Right and Protecting Yourself*, Lyons Press, États-Unis d'Amérique, 2011.
- Transparency International France, "Guide pratique à l'usage du lanceur d'alerte français", 2014, disponible à l'adresse: http://www.agircontrelacorruption.fr/wp-content/uploads/2014/12/GP-a%CC%80-lusage-du-lanceur-dalerte-franc%CC%A7ais-v.5_pages.pdf
- Transparency International Ireland, *Speak Up Safely, Transparency International Ireland's Guide to Whistleblowing and Making a Protected Disclosure*, 2014, disponible à l'adresse: http://transparency.ie/sites/default/files/14.12.02_Speak_Up_Safely_Final.pdf.

Dispositifs internes de signalement/d'alerte

- British Standards, *PAS 1998:2008 — Whistleblowing Arrangements Code of Practice*, 2008, disponible aux adresses: http://pcaw.org.uk/bsi et http://shop.bsigroup.com/forms/PASs/ PAS-1998/.
- Stichting van de Arbeid, *Statement on Dealing with Suspected Malpractices in Companies*, publication nº 1/10, 3 mars 2010 (traduction anglaise mise à jour en août 2012), disponible à l'adresse: http://www.stvda.nl/en/~/media/Files/Stvda/Talen/Engels/2012/20120829_EN.ashx.
- Royaume-Uni, National Health Service, *Speak up for a healthy NHS* (orientations à l'intention des employeurs), 2005, disponible à l'adresse: http://www.nhsemployers.org/~/media/Employers/Documents/SiteCollectionDocuments/Speak%20up%20for%20a%20healthy%20NHS.pdf.
- ONUDC, "Un programme de déontologie et de conformité contre la corruption pour les entreprises: Guide pratique", 2013, disponible à l'adresse: http://www.unodc.org/ documents/corruption/Publications/2013/13-86071_F_ebook.pdf.
- Royaume-Uni, The Whistleblowing Commission, *Code of Practice*, 2013, disponible à l'adresse: http://www.pcaw.org.uk/files/PCaW_COP_FINAL.pdf.

- *Anti-Corruption Ethics Compliance Handbook*, publication conjointe de l'OCDE, de l'ONUDC et de la Banque mondiale, p. 60 et suiv., disponible à l'adresse: http://www.unodc.org/documents/corruption/Publications/2013/Anti-Corruption EthicsComplianceHandbook.pdf.
- ONUDC, "Un programme de déontologie et de conformité contre la corruption pour les entreprises: Guide pratique", 2013, p. 93 et suiv., disponible à l'adresse: http://www.unodc.org/documents/corruption/Publications/2013/13-86071_F_ ebook.pdf.

Documents émis par des autorités compétentes (quelques exemples)

- Union européenne, "Décision de la Médiatrice européenne sur des règles internes en matière de divulgation dans l'intérêt général ("alerte éthique")", 2015, disponible à l'adresse: http://www.ombudsman.europa.eu/fr/cases/correspondence.faces/fr/59102/ html.bookmark.
- Hong Kong, Independent Commission Against Corruption (ressource en ligne), *Guide to Reporting Corruption*, disponible à l'adresse: http://www.icac.org.hk/en/report_corruption/grc/.
- Nouvelle-Zélande, Office of the Ombudsman, *Making a Protected Disclosure — "blowing the whistle"*, 2012, disponible à l'adresse: http://www.ombudsman.parliament.nz/resources-and-publications/guides/good-administration-guides.
- États-Unis d'Amérique, Office of the Special Counsel (ressource en ligne), *Disclosure of Wrongdoing* et *FAQs*, disponibles à l'adresse: https://osc.gov/Pages/DOW.aspx.
- États-Unis d'Amérique, Securities and Exchange Commission, SEC Whistleblower Practice Guide, Navigating the SEC Whistleblower Program and the Rules and Procedures that can lead to Financial Rewards for Reporting Security Violations, 2014, disponible à l'adresse: http://www.kmblegal.com/wp-content/uploads/SEC-Whistleblower-Practice-Guide.pdf?730971.

Sélection de recherches/d'études

Banisar, D., "Whistleblowing: International Standards and Developments", dans *Corruption and Transparency: Debating The Frontiers Between State, Market and Society*, World Bank-Institute for Social Research, UNAM, Sandoval, I. (dir.publ.), Washington, D. C., 2011, disponible sur le SSRN, à l'adresse: http://ssrn.com/abstract=1753180.

Brown, A. J., P. Roberts et J. Olsen, *Whistling While They Work: A good-practice guide for managing internal reporting of wrongdoing in public sector organisations*, Australia and New Zealand School of Government (ANZSOG), Australie, 2011, disponible à l'adresse: http://press.anu.edu.au/titles/ australia-and-new-zealand-school-of-government-anzsog-2/whistling_citation/.

Brown, A. J., D. Lewis, R. Moberly et W. Vandekerckhove (dir. publ.), *International Handbook On Whistleblowing Research,* Edward Elgar Publishing, Cheltenham, 2014.

Chevarria, F. et M. Silvestre, *Sistemas de denuncias y de protección de denunciantes de corrupción en América Latina y Europa*, Documento de Trabajo nº 2, Serie: Análisis, Área: Institucionalidad Democrática, Eurosocial, Madrid, 2013, disponible à l'adresse: http://sia.eurosocial-ii.eu/files/docs/1400663798-DT2.pdf.

Dworkin, T. M. et M. S. Baucus, “Internal vs. External Whistleblowers: A Comparison of Whistleblowing Processes”, *Journal of Business Ethics*, volume 17, nº 12, 1998, p. 1281 à 1298.

Ethics Resource Center, *Reporting: Who’s Telling You What You Need to Know, Who Isn’t, and What You Can Do About It*, Supplemental Research Brief — 2009 National Business Ethics Survey, 2010, disponible à l’adresse: http://ethics.org/files/u5/Reporting.pdf.

G20, *G20 Anti-Corruption Action Plan* (point d’action nº 7: protéger les lanceurs d’alerte), 2010, disponible à l’adresse: http://www.oecd.org/g20/topics/anti-corruption/G20_Anti-Corruption_ Action_Plan.pdf.

Hutton, D., *Shooting the Messenger*, Parkland Institute, Canada, 2011, disponible à l’adresse: http://parklandinstitute.ca/research/summary/shooting_the_messenger.

Martin, P., *The Status of Whistleblowing in South Africa — Taking Stock*, Open Democracy Advice Centre, le Cap, 2010, disponible à l’adresse: http://openjournalismworkshop.files.wordpress.com/2013/03/odac_whistleblowing_report_web.pdf.

Omtizgt, P., *“La protection des “donneurs d’alerte”*, rapport du rapporteur de la Commission des questions juridiques et des droits de l’homme, Assemblée parlementaire, Conseil de l’Europe, Doc. 12006, 2009, disponible à l’adresse: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-FR.asp?fileid=12302&lang=FR.

Osterhaus, A. et C. Fagan, *Alternative to Silence: Whistleblower Protection in 10 European Countries*, Transparency International, Berlin, 2009, disponible à l’adresse: http://www.transparency.org/whatwedo/publication/alternative_to_silence_whistleblower_protection_in_10_european_countries.

Oživení, *About Us, With Us: Protection of whistleblowers in the Czech context and in comparison with other countries*, Oživení, République tchèque, 2014, disponible à l’adresse: http://www.bezkorupce.cz/wp-content/uploads/2014/04/whistleblower_ENG.pdf. Également disponible en tchèque à l’adresse: http://www.bezkorupce.cz/wp-content/uploads/2014/04/ WB_CZE-FINAL_REVISED.pdf.

Public Concern at Work, *The Whistleblowing Commission: Report on the effectiveness of existing arrangements for workplace whistleblowing in the UK*, PCaW, Londres, 2013, disponible à l’adresse: http://www.pcaw.org.uk/whistleblowing-commission.

Public Concern at Work et University of Greenwich, *Whistleblowing: The Inside Story — A study of the experiences of 1,000 whistleblowers*, PCaW, Londres, 2013, disponible à l’adresse: http://www.pcaw.org.uk/whistleblowing-the-inside-story.

Pagnattaro, M. et E. Peirce, “Between A Rock And A Hard Place: The Conflict Between U.S. Corporate Codes Of Conduct and European Privacy And Work Laws”, *Berkeley Journal of Employment and Labor Law*, volume 28, nº 2, 2007, p. 375 à 428.

Rinaldi, T. et consorts, *Fighting Corruption in Decentralized Indonesia — Case Studies on Handling Local Government Corruption*, Banque mondiale, Washington, D. C., mai 2007.

Rohde-Leibenau, B., “The Value of an Ombuds System in Whistleblowing Situations”, dans *Whistleblowing and Democratic Values* (livre numérique), D. Lewis, D. et W. Vandekerckhove (dir. publ.), International Whistleblower Research Network, Londres, 2011, p. 70 à 85, disponible à l’adresse: http://ssrn.com/abstract=1998293.

Rohde-Liebenau, B., *Whistleblowing Rules: Best Practice, Assessment and Revision of Rules Existing in EU Institutions*, Parlement européen, Unité d'assistance budgétaire, Bruxelles, 2006.

Rothschild, J. et T. D. Miethe, "Whistle-Blower Disclosures and Management Retaliation", dans *Work and Occupations*, volume 26, nº 1, 1999, p. 107 à 128.

Schaffer, I., "An International Train Wreck Caused in Part by a Defective Whistle: When the Extraterritorial Application of SOX Conflicts with Foreign Laws", dans *Fordham Law Review*, volume 75, 2006, p. 1829, disponible à l'adresse: http://ir.lawnet.fordham.edu/flr/vol75/iss3/27.

Stephenson, P. et Michael Levi, "La protection des donneurs d'alerte — Rapport d'étude sur la faisabilité d'un instrument juridique sur la protection des employés qui divulguent des informations dans l'intérêt public", CDCJ(2012)9FIN, Conseil de l'Europe, Strasbourg, 2012, disponible à l'adresse: http://www.coe.int/t/dghl/standardsetting/cdcj/Whistleblowers/CDCJ(2012)9F_Final.pdf.

Vandekerckhove, W. et D. Lewis, Dave (dir. publ.), *Whistleblowing and democratic values*, International Whistleblowing Research Network, Londres, 2011, ISBN 978-0-9571384-0-7 (livre numérique), disponible à l'adresse: http://ssrn.com/abstract= 1998293.

Wolfe, S., M. Worth, S. Dreyfus et A. J. Brown, *Whistleblower Protection Laws in G20 Countries: Priorities for Action,* Blueprint for Free Speech, Griffith University, Université de Melbourne, Transparency International Australia, septembre 2014, disponible à l'adresse: https://blueprintforfreespeech.net.

Worth, M., *Whistleblowing in Europe, Legal Protections for Whistleblowers in the EU*, Transparency International, Berlin, 2013, disponible à l'adresse: http://www.transparency.org/whatwedo/publication/whistleblowing_in_europe_legal_protections_for_whistleblowers_in_the_eu.

Sélection de sites Web

Adviespunt Klokkenluiders (Pays-Bas): http://www.adviespuntklokkenluiders.nl/

Blueprint for Free Speech (Australie): https://blueprintforfreespeech.net/

Government Accountability Project (États-Unis d'Amérique): http://www.whistleblower.org/

Whistleblower Netzwerk E.V. (Allemagne): http://www.whistleblower-net.de/

Open Democracy Advice Centre (Afrique du Sud): http://www.opendemocracy.org.za/

Public Concern at Work (Royaume-Uni): http://www.pcaw.org.uk

Whistleblowing International Network: http://www.whistleblowingnetwork.org

Annexe. Normes internationales

Convention des Nations Unies contre la corruption[a]

Articles relatifs à la protection des personnes qui communiquent des informations et autres dispositions qui apportent des éléments concernant les personnes qui communiquent des informations ou ont trait à ce sujet

Article 33. Protection des personnes qui communiquent des informations

Chaque État Partie envisage d'incorporer dans son 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 établies conformément à la présente Convention.

Article 8. Codes de conduite des agents publics

[…]

4. Chaque État Partie envisage aussi, conformément aux principes fondamentaux de son droit interne, 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.

[a] http://www.unodc.org/unodc/fr/treaties/CAC/index.html.

Article 13. Participation de la société

1. Chaque État Partie prend des mesures appropriées, dans la limite de ses moyens et conformément aux principes fondamentaux de son droit interne, pour favoriser la participation active de personnes et de groupes n'appartenant pas au secteur public, tels que la société civile, les organisations non gouvernementales et les communautés de personnes, à la prévention de la corruption et à la lutte contre ce phénomène, ainsi que pour mieux sensibiliser le public à l'existence, aux causes et à la gravité de la corruption et à la menace que celle-ci représente. Cette participation devrait être renforcée par des mesures consistant notamment à:

[…]

d) Respecter, promouvoir et protéger la liberté de rechercher, de recevoir, de publier et de diffuser des informations concernant la corruption. Cette liberté peut être soumise à certaines restrictions, qui doivent toutefois être prescrites par la loi et nécessaires:

i) Au respect des droits ou de la réputation d'autrui;

ii) À la protection de la sécurité nationale ou de l'ordre public, ou de la santé ou de la moralité publiques.

2. Chaque État Partie prend des mesures appropriées pour veiller à ce que les organes de prévention de la corruption compétents mentionnés dans la présente Convention soient connus du public et fait en sorte qu'ils soient accessibles, lorsqu'il y a lieu, pour que tous faits susceptibles d'être considérés comme constituant une infraction établie conformément à la présente Convention puissent leur être signalés, y compris sous couvert d'anonymat.

Article 32. Protection des témoins, des experts et des victimes

1. Chaque État Partie prend, conformément à son système juridique interne et dans la limite de ses moyens, des mesures appropriées pour assurer une protection efficace contre des actes éventuels de représailles ou d'intimidation aux témoins et aux experts qui déposent concernant des infractions établies conformément à la présente Convention et, s'il y a lieu, à leurs parents et à d'autres personnes qui leur sont proches.

2. Les mesures envisagées au paragraphe 1 du présent article peuvent consister notamment, sans préjudice des droits du défendeur, y compris du droit à une procédure régulière:

a) À établir, pour la protection physique de ces personnes, des procédures visant notamment, selon les besoins et dans la mesure du possible, à leur fournir un nouveau domicile et à permettre, s'il y a lieu, que les renseignements concernant leur identité et le lieu où elles se trouvent ne soient pas divulgués ou que leur divulgation soit limitée;

b) À prévoir des règles de preuve qui permettent aux témoins et experts de déposer d'une manière qui garantisse leur sécurité, notamment à les autoriser à déposer en recourant à des techniques de communication telles que les liaisons vidéo ou à d'autres moyens adéquats.

3. Les États Parties envisagent de conclure des accords ou arrangements avec d'autres États en vue de fournir un nouveau domicile aux personnes mentionnées au paragraphe 1 du présent article.

4. Les dispositions du présent article s'appliquent également aux victimes lorsqu'elles sont témoins.

5. Chaque État Partie, sous réserve de son droit interne, fait en sorte que les avis et préoccupations des victimes soient présentés et pris en compte aux stades appropriés de la procédure pénale engagée contre les auteurs d'infractions d'une manière qui ne porte pas préjudice aux droits de la défense.

Article 37. Coopération avec les services de détection et de répression

1. Chaque État Partie prend des mesures appropriées pour encourager les personnes qui participent ou ont participé à la commission d'une infraction établie conformément à la présente Convention à fournir aux autorités compétentes des informations utiles à des fins d'enquête et de recherche de preuves, ainsi qu'une aide factuelle et concrète qui pourrait contribuer à priver les auteurs de l'infraction du produit du crime et à récupérer ce produit.

2. Chaque État Partie envisage de prévoir la possibilité, dans les cas appropriés, d'alléger la peine dont est passible un prévenu qui coopère de manière substantielle à l'enquête ou aux poursuites relatives à une infraction établie conformément à la présente Convention.

3. Chaque État Partie envisage de prévoir la possibilité, conformément aux principes fondamentaux de son droit interne, d'accorder l'immunité de poursuites à une personne qui coopère de manière substantielle à l'enquête ou aux poursuites relatives à une infraction établie conformément à la présente Convention.

4. La protection de ces personnes est assurée, *mutatis mutandis*, comme le prévoit l'article 32 de la présente Convention.

5. Lorsqu'une personne qui est visée au paragraphe 1 du présent article et se trouve dans un État Partie peut apporter une coopération substantielle aux autorités compétentes d'un autre État Partie, les États Parties concernés peuvent envisager de conclure des accords ou arrangements, conformément à leur droit interne, concernant l'éventuel octroi par l'autre État Partie du traitement décrit aux paragraphes 2 et 3 du présent article.

Article 38. Coopération entre autorités nationales

Chaque État Partie prend les mesures nécessaires pour encourager, conformément à son droit interne, la coopération entre, d'une part, ses autorités publiques ainsi que ses agents publics et, d'autre part, ses autorités chargées des enquêtes et des poursuites relatives à des infractions pénales. Cette coopération peut consister:

a) Pour les premiers à informer, de leur propre initiative, les secondes lorsqu'il existe des motifs raisonnables de considérer que l'une des infractions établies conformément aux articles 15, 21 et 23 de la présente Convention a été commise; ou

b) Pour les premiers à fournir, sur demande, aux secondes toutes les informations nécessaires.

Article 39. Coopération entre autorités nationales et secteur privé

1. Chaque État Partie prend les mesures nécessaires pour encourager, conformément à son droit interne, la coopération entre les autorités nationales chargées des enquêtes

et des poursuites et des entités du secteur privé, en particulier les institutions financières, sur des questions concernant la commission d'infractions établies conformément à la présente Convention.

2. Chaque État Partie envisage d'encourager ses ressortissants et les autres personnes ayant leur résidence habituelle sur son territoire à signaler aux autorités nationales chargées des enquêtes et des poursuites la commission d'une infraction établie conformément à la présente Convention.

Aperçu d'autres normes internationales relatives à la protection des personnes qui communiquent des informations

Organisation des États américains (OEA) — Convention interaméricaine contre la corruption[b]

Article III. Mesures préventives

Aux fins visées à l'article II de la présente Convention, les Parties conviennent d'envisager, à l'intérieur de leurs systèmes institutionnels, l'applicabilité de mesures destinées à créer, à maintenir et à renforcer: […]

8. Les systèmes de protection des fonctionnaires et des particuliers qui dénoncent de bonne foi les actes de corruption, y compris la protection de leur identité, conformément à leur Constitution et aux principes fondamentaux de leur système juridique interne.

Voir aussi: Lois types de l'OEA relatives à la protection des lanceurs d'alerte et des témoins (2004 et 2013)[c].

Conseil de l'Europe — Convention pénale sur la corruption[d]

Article 22. Protection des collaborateurs de justice et des témoins

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour assurer une protection effective et appropriée:

a) aux personnes qui fournissent des informations concernant des infractions pénales établies en vertu des articles 2 à 14 ou qui collaborent d'une autre manière avec les autorités chargées des investigations ou des poursuites;

b) aux témoins qui font une déposition concernant de telles infractions.

---

[b] La Convention interaméricaine contre la corruption a été ratifiée par 29 pays d'Amérique latine et d'Amérique du Sud, ainsi que par les États-Unis d'Amérique et le Canada. Elle est disponible à l'adresse: http://www.oas.org/juridico/français/b-58.htm.

[c] Model Law Protecting Freedom of Expression against Corruption (loi type visant à protéger la liberté d'expression contre la corruption), 2004, disponible à l'adresse: http://www.oas.org/juridico/english/ model_law_whistle.htm; Model Law to Facilitate and Encourage the Reporting of Acts of Corruption and to Protect Whistleblowers And Witnesses (loi type visant à faciliter et encourager le signalement des actes de corruption et à protéger les lanceurs d'alerte et les témoins), 2013, disponible à l'adresse: http://www.oas.org/juridico/english/law_reporting.htm.

[d] Le Conseil de l'Europe, qui compte 47 États membres, a mis en place un mécanisme d'évaluation contre la corruption — le Groupe d'États contre la corruption (GRECO) — en application d'un accord partiel et élargi permettant à des États qui ne sont pas membres du Conseil de l'Europe d'y adhérer. Fort de ses 49 États membres, le GRECO veille au respect de la Convention civile sur la corruption de 1999 (disponible à l'adresse: http://conventions.coe.int/Treaty/fr/Treaties/Html/174.htm) et de la Convention pénale sur la corruption de 1999 (disponible à l'adresse: http://conventions.coe.int/Treaty/fr/Treaties/Html/173.htm).

Conseil de l'Europe — Convention civile sur la corruption

Article 9. Protection des employés

Chaque Partie prévoit dans son droit interne une protection adéquate contre toute sanction injustifiée à l'égard des employés qui, de bonne foi et sur la base de soupçons raisonnables, dénoncent des faits de corruption aux personnes ou autorités responsables.

Voir aussi: Recommandation sur la protection des lanceurs d'alerte (2014)[e].

Convention de l'Union africaine sur la prévention et la lutte contre la corruption[f]

Article 5. Mesures législatives et autres mesures

Aux fins de l'application des dispositions de l'article 2 de la présente Convention, les États parties s'engagent à: […]

5. Adopter des mesures législatives et autres pour protéger les informateurs et les témoins dans les cas de corruption et d'infractions assimilées, y compris leur identité;

6. Adopter des mesures afin de s'assurer que les citoyens signalent les cas de corruption, sans craindre éventuellement des représailles; […]

Protocole de la Communauté de développement de l'Afrique australe contre la corruption[g]

Article 4. Mesures préventives

1. Aux fins énoncées à l'article 2 du présent Protocole, chaque État partie s'engage à adopter les mesures appropriées afin de mettre en place, maintenir et consolider: […]

e) des systèmes de protection des particuliers qui, de bonne foi, rapportent les actes de corruption; […]

Protocole de la Communauté économique des États de l'Afrique de l'Ouest sur la lutte contre la corruption

Article 5. Mesures préventives

Afin de réaliser les objectifs définis à l'Article 2 ci-dessus, chaque État partie s'engage à prendre des mesures pour mettre en place et consolider: […]

c) les lois et autres mesures estimées nécessaires pour assurer une protection effective et adéquate des personnes qui, agissant de bonne foi, fournissent des informations sur des actes de corruption; […]

---

[e] Conseil de l'Europe, Recommandation CM/Rec(2014)7 du Comité des Ministres aux États membres sur la protection des lanceurs d'alerte, disponible à l'adresse: https://wcd.coe.int/ViewDoc.jsp?id=2188939&Site= CM.

[f] Cette Convention, qui a été ratifiée par 31 États africains, exige de ceux-ci qu'ils adoptent des mesures "afin de s'assurer que les citoyens signalent les cas de corruption, sans craindre éventuellement des représailles". Le texte de la Convention est disponible à l'adresse: http://www.peaceau.org/uploads/convention-combating-corruption-fr.pdf.

[g] En vertu de ce Protocole, 13 pays africains s'engagent à protéger les personnes qui signalent des actes de corruption. Son texte est disponible à l'adresse: http://www.afrimap.org/english/images/treaty/sadc_protocole_contre_la_corruption.pdf.

ONUDC
Office des Nations Unies
contre la drogue et le crime

Centre international de Vienne, Boîte postale 500, 1400 Vienne (Autriche)
Tél.: (+43-1) 26060-0, Fax: (+43-1) 26060-5866, www.unodc.org

V.15-8935