La mise en œuvre de la directive sur les lanceurs d'alerte, un nouveau choc pour la gouvernance d'entreprise ?

Introduction

1. Les gros titres à l'annonce des scandales provoqués par les révélations des lanceurs d'alerte et, pour certains lanceurs d'alerte, les menaces, voire les poursuites en justice dont ils ont fait les frais du fait de cette « dénonciation », sont dans les mémoires. Mais ces affaires médiatisées ne constituent que la face visible de l'iceberg. Bon nombre de signalements ne sont jamais rendus publics, car ils ne quittent jamais la sphère de l'entreprise.

Le phénomène du *whistleblowing* n'est donc pas nouveau. Ce qui fait l'actualité en revanche c'est l'adoption d'une directive européenne formalisant un nouveau cadre juridique pour l'alerte professionnelle[1] et qui est en passe de faire évoluer complètement la culture d'entreprise autour de l'alerte. Si les entreprises regardent encore avec circonspection ce voisin de la dénonciation, la directive tend à une « culture de la bonne communication et de la responsabilité sociale de l'entreprise »[2]. On notera, par exemple, que le *whistleblowing* figure, depuis plusieurs années, en tête des méthodes de détection de la fraude « occupationnelle » (fraude survenant dans un contexte professionnel) dans le rapport annuel de l'*Association of Certified Fraud Examiners*[3].

La directive encadre les signalements en prévoyant trois canaux distincts. Le signalement interne, tout d'abord, est à mettre en place par les entités privées et publiques visées par la législation, sachant qu'il est possible d'externaliser le traitement des signalements en faisant appel à un service externe[4]. Le second canal est le canal externe qui dépendra de la législation transposée dans les États membres puisqu'il leur revient de désigner les autorités compétentes pour recevoir les signalements[5]. La divulgation publique, enfin, vise la mise à disposition dans la sphère publique d'informations sur des violations, par la voie de la presse, d'une organisation non gouvernementale ou d'un parlementaire par exemple[6].

2. La directive aurait dû — sauf en ce qui concerne ses dispositions concernant les entités juridiques du secteur privé de moins de 250 travailleurs — être transposée par la Belgique pour le 17 décembre 2021. Mais, au 17 décembre 2021, seuls cinq États membres étaient en règle, le Danemark étant en tête avec un texte adopté le 24 juin 2021.

Conformément à la lettre de mise en demeure transmise par la Commission en janvier dernier, la Belgique était tenue d'avancer dans les deux mois. Ce coup d'accélérateur a conduit à l'adoption de deux avant-projets de loi au niveau fédéral — l'un concerne le secteur privé, l'autre concerne le secteur public —, mais aussi au niveau des entités fédérées et des pouvoirs locaux. Au total, près de huit textes seraient en cours d'élaboration.

À l'automne 2022, dix États membres seulement étaient en règle[7]. La Belgique n'y figure toujours pas, mais les avant-projets du gouvernement fédéral sont désormais arrivés au Parlement[8].

3. L'objet de cette contribution est d'identifier les principaux enjeux posés par cette nouvelle directive, en tenant compte des orientations données par le projet de loi « secteur privé » actuellement à la Chambre, que ce soit du côté de l'entité qui réceptionne le signalement (I) que de celui du lanceur d'alerte (II).

I. L'impact pour l'entité « réceptrice de l'alerte »

A. Qui doit établir des canaux et procédures de signalement interne ?

4. Les entités juridiques du secteur privé qui comptent 50 travailleurs ou plus ainsi que les entités juridiques du secteur public doivent établir des canaux et des procédures pour le signalement interne et pour le suivi, après consultation des partenaires sociaux et en accord avec ceux-ci lorsque le droit national le prévoit[9].

Le seuil (de 50 travailleurs) n'est pas applicable aux entités du secteur privé relevant déjà du champ d'application des actes sectoriels[10]. C'est le cas, en particulier, des entités soumises au contrôle de la FSMA ou de la BNB[11], ainsi que de celles soumises à la législation AML (*Anti-Money Laundering*)[12].

1 Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, *J.O.U.E.*, L 305 du 26 novembre 2019. Ci-après, la « directive ».

2 Cons. 47 *in fine* de la directive.

3 D'après le dernier rapport de l'ACFE (disponible sur https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf), 42 % des fraudes occupationnelles seraient détectées grâce aux signalements (*tips*), principalement des employés.

4 Art. 8.5 de la directive.

5 Art. 11.1 de la directive.

6 Art. 5.6 et cons. 46 de la directive.

7 Pour une mise à jour de l'état d'avancement de la transposition de la directive, voy. le *EU Whistleblowing Monitor*, disponible sur https://www.whistleblowingmonitor.eu/ (consulté le 11 octobre 2022).

8 Projet de loi du 11 octobre 2022 sur la protection des personnes qui signalent des violations au droit de l'Union ou au droit national constatées au sein d'une entité juridique du secteur privé (*Doc. parl.*, Ch. repr., 2022-2023, n° 55-2912) ; Projet de loi du 3 novembre 2022 relatif aux canaux de signalement et à la protection des auteurs de signalement d'atteintes à l'intégrité dans les organismes du secteur public fédéral et au sein de la police intégrée (*Doc. parl.*, Ch. repr., 2022-2023, n° 55-2952).

9 Art. 8 de la directive.

10 Art. 8.4 de la directive.

11 Voy. spéc. la directive (UE) 2013/36 du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement et la directive 2009/138/CE du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice.

12 Directive (UE) 2015/849 du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme. Notons que cette directive, qui établit un dispositif de signalement interne et un dispositif de signalement externe, a depuis lors été remplacée par la directive (UE) 2015/849 (5e directive antiblanchiment) et complétée par la directive (UE) 2018/1673 (6e directive antiblanchiment).

La portée précise de cette exclusion pose question dans la mesure où l'on peut se demander si l'inapplicabilité du seuil vaut uniquement pour le signalement des violations se rapportant aux actes sectoriels ou si elle recouvre toutes les violations couvertes par la directive et ses actes nationaux de transposition. Cela pourrait avoir une grande incidence en pratique, par exemple, pour les notaires, les avocats et les huissiers de justice soumis à la législation AML, mais n'atteignant pas le seuil des 50 travailleurs.

La notion d'entité juridique du secteur privé s'entend largement. D'après le projet de loi « secteur privé », elle couvre toute organisation dotée ou non de la personnalité juridique qui exerce une ou plusieurs activités déterminées, à l'exception des organisations ou des activités qui relèvent d'autres lois particulières relatives à la protection des auteurs de signalement (logique de subsidiarité). C'est le cas des diverses formes juridiques visées par le Code des sociétés et des associations (CSA) ainsi que des personnes qui exercent leurs activités économiques en personnes physiques (entreprises individuelles).

La notion d'entité juridique du secteur public doit pareillement être entendue largement, englobant tous les organismes du secteur public fédéral, à savoir les autorités administratives fédérales, les organes stratégiques et tout autre organisme ou service qui dépend des autorités fédérales et n'appartient pas au secteur privé.

5. La Belgique ayant fait le choix, au niveau fédéral, de distinguer la législation applicable au secteur privé de celle applicable au secteur public, il sera important, en pratique, pour une entité de pouvoir se raccrocher précisément à l'une ou l'autre législation. À l'heure où nous écrivons ces lignes, le critère pris en compte est le statut public ou privé de l'entité, ce qui laisse présager de possibles différences au sein d'un même secteur d'activités, comme c'est le cas pour les universités belges dont certaines sont constituées sous la forme d'entreprises privées et d'autres, publiques.

B. Que peut-on signaler via ces canaux d'alerte interne ?

6. La directive n'a pas pour objet de créer un cadre juridique pour toute violation au droit de l'Union. Seules les violations se rapportant à certains actes de l'Union et à certains domaines politiques sont couvertes[13].

En l'occurrence, les canaux et procédures de signalement interne doivent porter sur les trois catégories de violations suivantes :

1. les violations relevant du champ d'application de certains actes de l'Union (repris en annexe de la directive) dans dix domaines :
   - i. marchés publics ;
   - ii. services, produits et marchés financiers et prévention du blanchiment de capitaux et du financement du terrorisme ;
   - iii. sécurité et conformité des produits ;
   - iv. sécurité des transports ;
   - v. protection de l'environnement ;
   - vi. radioprotection et sûreté nucléaire ;
   - vii. sécurité des aliments destinés à l'alimentation humaine et animale, santé et bien-être des animaux ;
   - viii. santé publique ;
   - ix. protection des consommateurs ;
   - x. protection de la vie privée et des données à caractère personnel, et sécurité des réseaux et des systèmes d'information ;
2. les violations portant atteinte aux intérêts financiers de l'Union ;
3. les violations relatives au marché intérieur, y compris les violations en matière de concurrence et d'aides d'État, de fraude fiscale et d'abus fiscal (dispositifs transfrontières contraires à des dispositions d'impôt des sociétés).

7. Conformément à l'article 2, § 2, de la directive, les États membres sont libres d'étendre l'application des dispositions nationales qui encadrent l'alerte à d'autres actes et domaines que ceux visés par la directive. Le législateur belge a fait le choix d'ajouter le domaine de la lutte contre la fraude fiscale et sociale pour ce qui concerne le projet de loi applicable au secteur privé. Il a, par ailleurs, décidé de supprimer l'exigence que la violation tombe, en outre, sous le coup d'une législation énumérée dans une liste arrêtée légalement. Le rattachement à un des douze domaines mentionnés légalement est suffisant.

C. Quelles sont les exigences concernant les canaux à mettre en place ?

8. L'article 9 de la directive impose un certain nombre d'exigences dans la conception des dispositifs de signalement interne. Elles ont trait à la confidentialité des canaux, aux modalités de signalement, à la désignation d'un gestionnaire de signalement, à l'obligation de fournir un accusé de réception, un *feed-back* (retour d'informations), et d'assurer un suivi diligent, ainsi qu'aux informations à fournir aux destinataires des canaux.

Le signalement doit être facilité par la mise à disposition de divers canaux de signalement. Le signalement doit pouvoir être effectué par écrit (par courrier, via une ou des boîtes à suggestions physiques ou via une plateforme en ligne, qu'il s'agisse d'une plateforme intranet ou internet) et/ou oralement (via une permanence téléphonique ou un autre système de messagerie vocale, ou les deux)[14]. À la demande de l'auteur de signalement, une rencontre en personne, dans un délai raisonnable, doit également pouvoir être programmée.

9. Parmi ces exigences, il y en a une qui n'a pas fini de faire couler de l'encre : la désignation d'une personne ou d'un département pour recevoir et/ou traiter les alertes.

Conformément au considérant 56 de la directive, « le choix des personnes ou des services les plus appropriés au sein d'une entité juridique du secteur privé pour être désignés comme étant compétents pour recevoir les signalements et en assurer le suivi dépend de la structure de l'entité ». La directive ouvre la voie à une certaine forme de pragmatisme en laissant la possibilité de doubles fonctions[15].

13 Cons. 5 de la proposition de directive du 23 avril 2018.

14 Cons. 53 de la directive.

15 Le considérant 56 de la directive indique que, « [d]ans les plus petites

La désignation doit avoir lieu, quoi qu'il en soit, en tenant compte d'une exigence d'indépendance et d'absence de conflit d'intérêts. Le *whistleblowing* étant classiquement présenté comme un outil de contrôle interne et de gestion des risques, on pourrait voir dans l'auditeur interne une personne apte, de par son indépendance et ses qualifications, à recevoir les signalements internes. C'est la voie, en tout cas, que certaines entreprises semblent aujourd'hui emprunter, même si l'auditeur interne n'est pas à l'abri de potentiels conflits d'intérêts, le signalement pouvant porter sur un problème qui aurait dû être détecté par lui (dysfonctionnement d'un service, problème de sécurité informatique, etc.).

10. Une dernière remarque mérite d'être apportée concernant les signalements anonymes, c'est-à-dire les signalements dont personne, pas même son destinataire, ne connaît l'identité de l'auteur.

Sauf si une telle modalité est rendue obligatoire par le droit de l'Union européenne, les États membres décident librement si les entités juridiques et les autorités compétentes doivent accepter les signalements anonymes. Le législateur belge a fait le choix d'autoriser le signalement anonyme auprès des autorités compétentes (signalement externe) ainsi qu'au sein des entités juridiques privées de plus de 250 employés (signalement interne) pour ce qui est de l'avant-projet de loi applicable au secteur privé[16].

II. L'impact pour le « lanceur d'alerte »

A. Qui peut faire usage d'un canal d'alerte interne ?

11. Les canaux et procédures de signalement interne doivent, au minimum, être accessibles pour les travailleurs de l'entité.

Ils peuvent aussi être rendus accessibles pour d'autres potentiels lanceurs d'alerte au sens de la directive, à savoir les indépendants, mais aussi toute une série de personnes impliquées dans la vie de l'entreprise (les membres de l'organe d'administration, de direction ou de surveillance d'une entreprise, y compris les membres non exécutifs, ainsi que les bénévoles et les stagiaires rémunérés ou non rémunérés) ou en contact avec celle-ci (toute personne travaillant sous la supervision et la direction de contractants, de sous-traitants et de fournisseur)[17]. On inclut donc les préposés qui travaillent dans les bureaux de l'entreprise, mais également un membre du personnel d'un fournisseur qui n'a jamais eu accès à ses locaux. La liste n'est pas limitative et les États membres ont donc la liberté d'étendre ce champ d'application personnel. À ce stade, le projet de loi « secteur privé » limite cependant l'accès aux canaux et procédures de signalement internes aux seuls travailleurs de l'entreprise[18].

Les informations partagées via ces canaux doivent avoir été obtenues dans un contexte professionnel[19]. Celui-ci n'est pas limité par l'objet de la fonction ou des tâches confiées à la personne[20]. Une personne peut opérer un signalement sur une violation, fût-elle étrangère à la réalisation de ses propres tâches, pour autant toutefois que cette information ait été obtenue dans le contexte de ses activités.

Une question se pose de savoir si les canaux et procédures sont aussi ouverts à des personnes qui, au moment du signalement, ne se trouvent plus dans un des statuts couverts et qui signalent des violations dont elles ont pris connaissance dans ce contexte professionnel. En effet, on peut imaginer que ces personnes procèdent à un signalement après la fin d'un contrat de travail ou d'entreprise. La directive confirme que le régime protecteur leur est applicable, tout comme lorsque la relation de travail n'a pas encore commencé dans les cas où des informations sur des violations ont été obtenues lors du processus de recrutement ou d'autres négociations précontractuelles[21].

La conséquence directe et juridique de ce champ d'application large est, comme le confirme la directive, que toute clause de confidentialité, qu'elle soit précontractuelle, contractuelle ou à laquelle on donne un effet postcontractuel et à laquelle serait tenu l'auteur d'un signalement, ne peut faire obstacle à la possibilité de signalement ou de divulgation publique dans les conditions fixées par le nouveau régime légal (voy. C, *infra*)[22].

12. Les entreprises sont, par ailleurs, encouragées à mettre en place un canal sur une base volontaire au-delà des domaines couverts par la directive et ses actes nationaux de transposition[23]. Dans ce cas de figure, un auteur de signalement devra se référer aux modalités définies par l'entreprise elle-même, qui pourraient différer de celles prévues par la directive, même si l'on préconisera une approche globale et cohérente de l'alerte.

B. Quel canal de signalement choisir ?

13. Le texte de la directive peut paraître ambigu, de prime abord, quant à la manière dont l'auteur d'un signalement doit sélectionner le canal utilisé. En réalité, il n'est pas prescrit d'utiliser l'un ou l'autre canal. Au terme d'âpres discussions, le législateur européen consacre le « libre choix de la voie la plus appropriée ». Le choix posé par l'auteur de signa-

entités, cette fonction pourrait être une double fonction assumée par un dirigeant d'entreprise bien placé pour rendre compte directement au chef de l'organisation. Il peut s'agir, par exemple, d'un responsable de la conformité ou des ressources humaines, d'un responsable de l'intégrité, d'un responsable juridique ou d'un responsable de la protection de la vie privée, d'un directeur financier, d'un responsable de l'audit interne ou d'un membre du conseil ».

16 Art. 9, § 2, du projet de loi « secteur privé ».

17 Art. 8.2 de la directive.

18 Le secteur financier bénéficie toutefois d'un champ d'application élargi.

19 Sauf pour le secteur financier.

20 Le « contexte professionnel » recouvre « toutes les activités professionnelles passées ou présentes dans le secteur public ou privé par lesquelles, indépendamment de la nature de ces activités, des personnes obtiennent des informations sur des violations et dans le cadre desquelles ces personnes pourraient faire l'objet de représailles si elles signalaient de telles informations » (art. 5, 9), de la directive).

21 Art. 4.2 et 4.3 de la directive. Dans le dernier cas de figure, le projet de loi « secteur privé » prévoit, à ce stade, que le canal de signalement interne ne leur est toutefois pas accessible. Les « futurs » travailleurs sont donc invités à procéder à leur signalement via le canal externe.

22 Art. 21.7 de la directive.

23 Une telle approche « devrait contribuer à favoriser au sein des organisations une culture de la bonne communication et de la responsabilité sociale de l'entreprise, les auteurs de signalement étant alors considérés comme des personnes contribuant de manière importante à l'autocorrection et à l'excellence au sein de l'organisation » (cons. 47 *in fine* de la directive).

lement sera toutefois évalué *a posteriori*. En effet, la directive subordonne la possibilité de bénéficier de la protection contre des représailles dans l'hypothèse où le lanceur d'alerte a respecté certaines conditions, parmi lesquelles le respect de la procédure établie en vertu de la directive[24].

Le lanceur d'alerte est censé privilégier le canal interne avant d'utiliser un canal externe, la divulgation publique constituant l'ultime moyen de lancer l'alerte[25]. Ce n'est que lorsque l'auteur a des raisons de penser qu'il n'est pas possible de remédier efficacement à la violation en interne ou qu'il existe un risque de représailles à son encontre qu'il peut utiliser directement un canal externe. Par ailleurs, le considérant 51 de la directive laisse entendre que, dans tous les cas où un canal interne n'a pas été établi par une entreprise, les personnes habilitées à effectuer un signalement peuvent faire usage directement du canal externe auprès des autorités compétentes et devraient bénéficier de la protection contre les représailles prévues par ladite directive. Cela pourrait recouvrir non seulement l'hypothèse où une entreprise est en défaut d'avoir mis en place un canal interne, mais également celui d'une entreprise non tenue par cette obligation et qui n'a, par ailleurs, mis en place aucun canal sur une base volontaire. À suivre cette interprétation, la directive ouvrirait donc très largement la possibilité de faire usage d'un canal externe, même pour des violations dénoncées concernant des petits acteurs qui se trouvent sous le seuil des 50 travailleurs.

Notons que la directive ne prévoit pas de sanction expresse dans l'hypothèse où le lanceur d'alerte ne parvient pas à justifier un choix d'opérer un signalement directement dans un canal externe[26].

C. Quelle est la protection dont bénéficie le lanceur d'alerte ?

14. Il convient d'emblée de signaler que le régime de protection bénéficie tant aux travailleurs qu'aux autres catégories de personnes qui peuvent effectuer et ont effectué un signalement ou une divulgation, et que la directive étend la protection à d'autres catégories d'intervenants.

Une protection est en effet également prévue pour des personnes qui, tout en n'étant pas auteurs du signalement, y sont associées[27]. Il s'agit au premier chef du « facilitateur », entendu comme une personne physique qui aide un auteur de signalement au cours du processus de signalement dans un contexte professionnel et dont l'aide devrait être confidentielle[28]. La directive donne l'exemple des représentants syndicaux et des représentants des travailleurs au motif qu'ils fournissent des conseils et une aide à l'auteur de signalement[29]. De manière plus floue, la directive vise aussi des tiers qui sont en lien avec les auteurs de signalement et qui risquent de faire l'objet de représailles dans un contexte professionnel en prenant l'exemple de collègues ou des proches des auteurs de signalement. À la différence des facilitateurs, ces tiers n'apportent aucun concours actif, mais ils risquent de faire l'objet de représailles uniquement en raison de leur proximité avec l'auteur de signalement. C'est à ce titre qu'ils devraient être protégés, même si la mise en pratique de cette protection — *quid* de la preuve de ce statut ? — ne nous paraît pas évidente.

Enfin, la directive impose aussi une protection aux entités juridiques appartenant aux auteurs de signalement ou pour lesquelles ils travaillent, ou encore avec lesquelles ils sont en lien dans un contexte professionnel. L'idée sous-jacente est de sanctionner d'éventuelles représailles indirectes à l'encontre de l'entité juridique à laquelle appartient l'auteur d'un signalement ou pour laquelle il travaille, par exemple, un fournisseur de l'entreprise dont un membre du personnel aurait opéré un signalement.

15. Quant aux mesures de protection, elles revêtent différentes formes : l'interdiction de mesures de représailles assortie de sanctions en cas de violation de ladite interdiction, des exonérations de responsabilité, la possibilité de bénéficier de mesures correctrices et de recours effectifs en cas de préjudice subi par l'auteur d'un signalement, ainsi que des mesures de soutien qui doivent être prévues par les États membres.

Nous nous pencherons sur les deux premières mesures.

La directive définit de manière large la notion de mesures de représailles en énumérant de façon non exhaustive une série de mesures qui constituent une forme de représailles et en englobant les menaces de représailles et tentatives de représailles[30]. Y sont notamment repris le licenciement, le refus de promotion, le transfert de fonctions, le changement de lieu de travail, l'évaluation de performance de travail négative, la non-conversion d'un contrat de travail temporaire en un contrat permanent, lorsque le travailleur pouvait légitimement espérer se voir offrir un emploi permanent. Toute la question sera donc de déterminer l'articulation qu'il doit y avoir entre le signalement et l'adoption d'une mesure qu'un travailleur, par exemple, estimerait entrer dans le champ de cette interdiction.

Le régime applicable sera à définir dans le droit national, mais l'article 21, § 5, de la directive donne déjà les grandes lignes de l'articulation. Il est présumé que le préjudice subi par un auteur de signalement a été causé en représailles au signalement ou à la divulgation publique lorsque celui-ci introduit une procédure devant une juridiction ou auprès d'une autre autorité à deux conditions. D'une part, l'auteur de signalement doit apporter la preuve du préjudice subi (licenciement, rétrogradation, etc.). D'autre part, il doit démontrer qu'il a effectué un signalement ou fait une divulgation publique conforme à la directive. Il appartiendra dès lors à la personne qui a pris la mesure préjudiciable, le plus souvent l'employeur, d'établir que cette mesure était fondée sur des motifs dûment justifiés. La preuve sera sans doute plus aisée à apporter si le signalement a été fait sous le bénéfice de l'anonymat, puisque dans ce cas, personne, pas même le récepteur de l'alerte, n'a connaissance de l'identité de l'auteur de signalement.

24 Art. 6 de la directive.

25 Art. 7.2 de la directive.

26 *Cf.* art. 10 de la directive qui indique que le lanceur d'alerte peut utiliser le canal externe après avoir effectué un signalement via le canal interne ou directement via le canal externe.

27 Art. 4.4 de la directive.

28 Art. 5.8 de la directive.

29 Partant, on se demande si une personne extérieure à l'entreprise, telle qu'un journaliste ou un juriste qui travaillerait pour une organisation de défense, pourrait bénéficier du statut de facilitateur.

30 Art. 19 de la directive.

À l'instar d'autres régimes de protection, le fait de prendre une mesure entrant dans la catégorie des mesures de représailles fait naître un risque pour un employeur — ou plus généralement une entreprise — puisque les mesures de rétorsion sont susceptibles de donner lieu à des sanctions également pour les autres catégories de personnes susceptibles d'utiliser un canal de signalement. Contrairement à d'autres mécanismes dans lesquels les personnes protégées sont clairement identifiées (par exemple, en cas de plainte auprès d'un conseiller en prévention, ce dernier informe l'employeur de la plainte de l'identité de son auteur[31]), un des éléments clés de la gestion des signalements est la protection de l'identité de l'auteur, même lorsque le signalement n'est pas réalisé sous le couvert de l'anonymat (régime de confidentialité *a minima*). Les entreprises ont donc tout intérêt à mûrement réfléchir à la façon dont la gestion des signalements est assurée et est dissociée de la gestion des ressources humaines[32].

16. Pour ce qui est de l'exonération de responsabilité, le principe veut que les actes qui ont été nécessaires afin d'opérer un signalement ou une divulgation publique ne peuvent engager la responsabilité de l'auteur du signalement ou de la divulgation publique[33]. Ce principe sera applicable pour se défendre tant face à une accusation de violation d'une obligation contractuelle qu'en cas de manquement reproché découlant d'une obligation générale ou spécifique de confidentialité[34].

D. Quels sont les risques courus par le lanceur d'alerte ?

17. Les risques sont principalement de deux ordres. Le premier est de ne pas pouvoir bénéficier du régime de protection de la directive en cas de mesures de représailles ou de mise en cause de la responsabilité de l'auteur du signalement ou de la divulgation par exemple (1). Le second est de s'exposer à des sanctions spécifiques prévues en droit national en cas de signalement abusif (2).

1. Limites du régime de protection de l'auteur d'un signalement ou d'une divulgation

18. Aussi large soit-elle, la protection conférée par la directive n'est pas illimitée.

Une première limite est liée à la nature de l'information. La protection instituée par la directive ne s'applique pas lorsque l'information révélée est couverte par une obligation de secret en droit national résultant de la protection des informations classifiées, de la protection du secret professionnel des avocats et du secret médical, du secret des délibérations judiciaires et des règles en matière de procédure pénale[35]. Cela étant, cela ne signifie pas que l'alerte est impossible pour ces informations et/ou qu'aucune protection n'est prévue. Mais l'adoption de telles règles relève de la souveraineté des États membres.

Un deuxième facteur qui pourrait être invoqué à l'encontre d'un lanceur d'alerte concerne la manière dont il est entré en possession de l'information qui a fait l'objet d'un signalement ou d'une divulgation. La directive précise que l'exonération de responsabilité ne joue pas dans le cas où l'accès ou l'obtention desdites informations constitue une infraction pénale autonome[36]. Le signalement ou la divulgation d'une information obtenue par le biais d'un *hacking* externe, par exemple, pourrait être reproché à l'auteur d'un signalement[37].

Une troisième limite réside dans le fait que la directive exige que l'auteur du signalement ait eu des motifs raisonnables de croire que le signalement ou la divulgation publique de telles informations était nécessaire pour révéler une violation[38]. L'on vise sous le couvert de cette limite le cas où le signalement était inutile (par exemple, parce que les informations étaient déjà entièrement disponibles dans le domaine public[39]) ou que l'auteur ne pouvait raisonnablement penser que ces informations étaient véridiques ou exactes (par exemple, lorsque les informations résultent de ouï-dire ou de rumeurs infondées[40]). La question de la motivation de l'auteur est, en revanche, considérée comme n'étant pas pertinente pour évaluer si ce dernier peut recevoir une protection, que celle-ci prenne la forme d'une exonération de responsabilité ou non[41].

Enfin, une quatrième limite se dégage des conditions de protection de l'auteur d'une divulgation publique. S'il n'y a pas de sanction prévue en lien avec l'usage d'un canal externe plutôt qu'un canal interne, lorsque l'auteur fait le choix d'une divulgation publique, il est susceptible de se voir refuser le régime de protection de la directive s'il a directement recours à une divulgation publique sans passer par un signalement par un canal interne ou externe. C'est ce qui résulte en substance de l'article 15 de la directive qui subordonne la protection dans ce cas à la condition que la personne ait eu des motifs raisonnables de croire que la violation pouvait représenter un danger imminent ou manifeste dans l'intérêt du public ou encore qu'en cas de signalement externe, soit il y ait un risque de représailles, soit il y avait peu de chances

31 Voy. l'article I.3-22 du Code du bien-être au travail.

32 L'externalisation vers un partenaire spécialisé dans l'alerte et garant de la confidentialité de l'identité de l'auteur d'un signalement offrirait cet avantage.

33 Voy. en particulier art. 21.2 et 21.7 de la directive.

34 Sont ainsi spécifiquement visées : les procédures pour diffamation, violation du droit d'auteur, violation du secret, violation des règles en matière de protection des données ou divulgation de secrets d'affaires, ou pour des demandes d'indemnisation fondées sur le droit privé, le droit public ou le droit collectif du travail (art. 21.7 de la directive).

35 Art. 3.3 de la directive.

36 Art. 21.3 de la directive.

37 Soulignons que cette infraction est établie sur la base d'un simple dol général (à la différence du *hacking* interne qui requiert un dol spécial, c'est-à-dire une intention de nuire).

38 Art. 21.2 de la directive.

39 *Cf.* cons. 43 de la directive.

40 *Cf.* cons. 32 de la directive.

41 Sur ce point, le régime de la directive est plus protecteur que la jurisprudence de la Cour européenne des droits de l'homme lorsqu'elle évalue l'existence d'une violation de l'article 10 de la CEDH dans le contexte d'un lancement d'alerte. Comme le relève la doctrine, la Cour requiert que le lanceur d'alerte ait agi au moins en partie et principalement dans l'intérêt général (E. Cobbaut, « L'encadrement de l'alerte et la protection du lanceur d'alerte (*whistleblower*) : l'affaire *Luxleaks* à l'aune d'un cadre européen en construction », *RDTI*, n° 75, 2019, p. 67). Selon une jurisprudence constante, « un acte motivé par un grief ou une animosité personnels ou encore par la perspective d'un avantage personnel, notamment un gain pécuniaire, ne justifie pas un niveau de protection particulièrement élevé » (voy. not. Cour eur. D.H. (gde ch.), arrêt *Guja c. Moldavie*, 12 février 2008, § 77 ; Cour eur. D.H. (5e sect.), arrêt *Heinisch c. Allemagne*, 21 juillet 2011, § 69).

que le signalement permette une remédiation à la violation signalée[42].

2. Sanctions en cas de signalement abusif

19. Indépendamment des limites du régime de protection précitées, les auteurs de signalement peuvent encourir des sanctions spécifiques dans le cas où il serait prouvé qu'ils ont sciemment signalé ou divulgué publiquement de fausses informations.

C'est ce que prévoit l'article 23 de la directive qui impose aux États membres de prévoir des sanctions effectives, proportionnées et dissuasives, l'idée étant que la proportionnalité de ces sanctions devrait garantir qu'elles n'aient pas d'effet dissuasif sur les lanceurs d'alerte potentiels, tout en préservant la crédibilité du système pour prévenir les signalements « malveillants »[43] autrement dit, les délations.

Les sanctions ne sont pas uniquement pénales, mais peuvent aussi revêtir une forme civile ou administrative[44].

Conclusion

20. La mise en application des exigences de la directive impliquera pour nombre d'entreprises un bouleversement de la gouvernance, au même titre que celui provoqué par le RGPD.

Les entités concernées devront ouvrir un canal sécurisé et confidentiel pour recevoir des signalements et donner un retour sur la suite réservée à celui-ci aux auteurs. La mise en œuvre de ces obligations impose une réflexion sur les moyens techniques et opérationnels à mettre en place pour encadrer un traitement des signalements, mais elle va également inévitablement pousser à la normalisation d'une forme de responsabilité de l'entité vis-à-vis d'un large nombre d'acteurs susceptibles de porter à sa connaissance des violations visées par la directive. Sur ce point, un parallèle existe avec le RGPD qui impose notamment la transparence vis-à-vis des personnes concernées et un principe de responsabilité (*accountability*) en matière de traitement de données[45].

21. Du point de vue de la liberté d'expression, la directive offre l'indéniable avantage de faciliter du point de vue pratique la communication de signalements par l'instauration des différents canaux, avec l'obligation pour l'entreprise d'accuser réception, d'assurer un suivi diligent et de donner un feed-back. De telles exigences visent à rassurer le lanceur d'alerte sur la prise en compte de son signalement. Le deuxième point fort de la nouvelle réglementation est la protection offerte à l'auteur de signalement. Celle-ci évacue certaines questions qui pouvaient se poser lorsque le principal cadre légal de référence était l'article 10 de la CEDH relatif à la liberté d'expression. Tel est le cas de la question de l'appréciation de l'intérêt public que présente ou non l'information divulguée et qui est pris en compte dans la jurisprudence de la Cour[46]. De même, la question de la motivation de l'auteur de signalement n'intervient pas dans l'appréciation des conditions de protection. Lancer l'alerte devient quasiment un droit exempt du poids de l'appréciation des bonnes intentions de l'auteur. Seules demeurent la croyance raisonnable de l'auteur ainsi que l'absence de commission d'infractions pour obtenir les informations divulguées.

Ceci étant, nous avons montré qu'il subsistait encore à ce stade des questions pratiques importantes concernant la mise en œuvre des principes énoncés dans la directive et qui auront une influence tant sur l'efficacité de la protection que sur l'effectivité des signalements. De surcroît, le nouveau dispositif restera lettre morte sans un changement substantiel de mentalité au sein des entreprises, faisant de la transparence une nouvelle vertu au service de la responsabilité sociétale d'entreprise.

Amélie Lachapelle
Chargée de cours à l'UNamur
Chercheuse senior au CRIDS/NaDI

Karen Rosier
Avocate au barreau du Brabant wallon
Maître de conférences à l'UNamur

42 *Cf. supra*, point I. Ajoutons que la directive laisse ouverte une possibilité de divulgation à la presse sans respecter les conditions de l'article 15, dans l'hypothèse où le droit national établit spécifiquement un système de protection relatif à la liberté d'expression ou d'information (*cf.* art. 15.2 de la directive). On vise ici, entre autres, le régime de protection des sources journalistiques tel qu'il existe en droit belge.

43 Comme précisé au considérant 102 de la directive, étant entendu que le terme malveillant ne fait pas référence à la motivation du lanceur d'alerte, mais au fait que l'auteur opère un signalement alors qu'il sait les informations signalées ou divulguées erronées.

44 Cons. 102 de la directive.

45 Notons par ailleurs que les canaux d'alerte internes ne peuvent être mis en œuvre que dans le respect du RGPD (art. 17 de la directive).

46 Notons que le critère de l'intérêt public continue d'être pris en compte dans le projet de loi « secteur public » dans le prolongement de la loi du 15 septembre 2013 relative à la dénonciation d'une atteinte suspectée à l'intégrité au sein d'une autorité administrative fédérale par un membre de son personnel.