

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

L'encadrement juridique du lancement d'alerte au sein de l'Union européenne

Lachapelle, Amelie

Published in:

Revue du Droit des Technologies de l'information

Publication date:

2020

Document Version

le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

Lachapelle, A 2020, 'L'encadrement juridique du lancement d'alerte au sein de l'Union européenne: commentaire de la directive sur les lanceurs d'alerte', *Revue du Droit des Technologies de l'information*, Numéro 78, p. 15-52.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

DOCTRINE

L'encadrement juridique du lancement d'alerte au sein de l'Union européenne

Commentaire de la directive sur les lanceurs d'alerte

Amélie Lachapelle¹

Longtemps à la traîne, l'Union européenne s'est enfin dotée, à la fin de l'année 2019, d'un régime général de protection des lanceurs d'alerte. La « directive sur la protection des personnes qui signalent des violations du droit de l'Union », en abrégé la « directive sur les lanceurs d'alerte », tend à tirer parti de la protection des lanceurs d'alerte, par l'établissement d'une série de standards communs minimums, en vue de renforcer l'effectivité du droit de l'Union dans certains domaines de politiques spécifiques.

Après avoir fait le point sur le champ d'application de la directive, le présent article livre un examen critique des deux principales normes qui composent la directive : d'une part, la mise en place de canaux spécifiques de dénonciation et, d'autre part, la protection des personnes qui dénoncent des violations du droit de l'Union.



Long lagging behind, the European Union finally adopted, at the end of 2019, a general protection regime for whistleblowers. The « Directive on the protection of persons who report breaches of Union law », in short the « Directive on the whistleblowers », aims at fully exploiting the potential of whistleblower protection, by setting out a set of common minimum standards, with a view to strengthening European law enforcement in specific policy areas.

After taking stock of the scope of the Directive, this article provides a critical review of the two main standards of the Directive : on the one hand, the establishment of specific channels for reporting and, on the other hand, the protection of persons who denounce breaches of Union law.

¹ Assistante de recherche au CRIDS/NaDI et chargée d'enseignement visiteuse en droit économique à l'Université de Namur.

La présente contribution s'intègre dans le cadre de recherches doctorales financées par le F.R.S.-FNRS (ASP) et menées sous la co-promotion des professeurs Cécile de Terwangne (UNamur) et Marc Verdussen (UCLouvain). L'auteure tient à remercier les membres de son comité de thèse – les professeurs Marc Bourgeois et Mark Delanote – ainsi que le professeur Yves Pouillet pour les riches et variés échanges qui ont su alimenter la présente contribution. La dissertation de thèse rédigée dans ce cadre sera publiée en janvier 2021 aux Éditions Larcier sous le titre « La dénonciation à l'ère des lanceurs d'alerte fiscale, de la complaisance à la vigilance ».

INTRODUCTION

1. Soucieuse de répondre aux nombreux appels du Parlement européen², d'organisations de la société civile et de syndicats³ en faveur d'une protection des lanceurs d'alerte, la Commission européenne a présenté, le 23 avril 2018, une proposition de directive «sur la protection des personnes dénonçant les infractions au droit de l'Union»⁴. Adoptée en première lecture par le Parlement européen le 16 avril 2019, la directive a finalement été adoptée par le Conseil de l'Union européenne le 7 octobre 2019. La «directive sur la protection des personnes qui signalent des violations du droit de l'Union», en abrégé la «directive sur les lanceurs d'alerte», a été publiée au *Journal Officiel* le 26 novembre 2019⁵. La plupart de ses

dispositions doivent être transposées en droit national pour le 17 décembre 2021⁶.

La directive sur les lanceurs d'alerte est remarquable⁷. Il s'agit effectivement de l'instrument le plus global à ce jour, et ce à l'échelle planétaire. Ce constat ne doit toutefois pas voiler les ambitions réelles du législateur européen : la directive a pour objet de tirer profit de la protection des lanceurs d'alerte pour renforcer l'application des politiques de l'Union européenne.

2. Une telle approche est symptomatique d'une conception «instrumentale» de la dénonciation⁸ en ce sens que la dénonciation

² Voy. not. Recommandations du Parlement européen sur des actions et des initiatives à entreprendre (rapport final), 2013/2107(INI), 23 octobre 2013, point 14; Résolution du Parlement européen sur les rescrits fiscaux et autres mesures similaires par leur nature ou par leur effet, 2015/2066(INI), Commission TAXE 1, 25 novembre 2015, point 144; Résolution du Parlement européen contenant des recommandations à la Commission en vue de favoriser la transparence, la coordination et la convergence des politiques en matière d'impôt sur les sociétés au sein de l'Union, 2015/2010(INL), P8_TA(2015)0457, 16 décembre 2015, recommandation A7; Résolution du Parlement européen sur les rescrits fiscaux et autres mesures similaires par leur nature ou par leur effet, 2016/2038(INI), Commission TAXE 2, P8_TA(2016)0310, 6 juillet 2016, point 46; Résolution du Parlement européen sur le rôle des lanceurs d'alerte dans la protection des intérêts financiers de l'Union européenne (2016/2055(INI)), P8_TA-PROV(2017)0022, 14 février 2017, point 2.

³ En particulier, *Transparency International*, *Eurocadres*, *European Public Service Union* et *European Federation of Journalist*.

⁴ Proposition de directive du Parlement européen et du Conseil relative à la protection des personnes dénonçant les infractions au droit de l'Union, COM(2018) 218 final, 23 avril 2018 (ci-après : «Proposition de directive du 23 avril 2018»).

⁵ 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, 26 novembre 2019.

⁶ En principe, les États membres doivent mettre en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la directive au plus tard le 17 décembre 2021. En ce qui concerne les entités juridiques du secteur privé comptant 50 à 249 travailleurs, l'article 26, § 2, de la directive sur les lanceurs d'alerte prévoit cependant que les États membres doivent mettre en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à l'obligation d'établir des canaux de signalement interne au plus tard le 17 décembre 2023.

⁷ Pour un premier commentaire, voy. spéc. D. POLLET-PANOUSIS, «La protection renforcée des lanceurs d'alerte dans le cadre de l'Union européenne», *Les Petites Affiches*, 2020, n° 40, pp. 9-15.

⁸ La distinction s'inspire de celle élaborée par Jean-François Foegle au départ de la double conception de la liberté d'expression proposée par Robert Post (R. Post, *Constitutional Domains – Democracy, Community, Management*, Cambridge (MA), Harvard University Press, 1995) : «Là où la conception "démocratique" de la liberté d'expression vise à favoriser la participation des citoyens à la vie publique en garantissant la possibilité d'une expression politique dans la sphère publique, la conception "managériale" de celle-ci est marquée par une logique instrumentale : la liberté d'expression n'est favorisée et rendue possible que dans les hypothèses où celle-ci permet aux pouvoirs publics de mener à bien des objectifs déterminés». Voy. J.-Ph. FOEGLE, «Le lanceur d'alerte dans l'Union européenne : démocratie, management, vulnérabilité(s)», in *Les lanceurs d'alerte. Quelle protection juridique? Quelles limites?* (M. DISANT et D. POLLET-PANOUSIS, dir.), Issy-les-Moulineaux, Lextenso, 2017, p. 110. Dans le même sens, voy. aussi, W. VANDE-

est instrumentalisée par le pouvoir à qui elle est adressée en vue de garantir l'exécution des politiques adoptées par ce dernier. Le dénonciateur agit en qualité de *sujet* du pouvoir en place, qu'il s'agisse d'un pouvoir privé ou public.

À cette conception «instrumentale» de la dénonciation, on peut opposer la conception «démocratique» de la dénonciation. Étroitement liée au mouvement des droits de l'homme, cette conception a commencé à éclore au sortir de la Révolution française pour prendre son essor, à partir des années '70, des deux côtés de l'Atlantique. En son sens «démocratique», la dénonciation, et en particulier le lancement d'alerte, se conçoit comme une extension de la liberté d'expression, laquelle est protégée juridiquement parce qu'elle constitue, pour reprendre l'expression de la Cour européenne des droits de l'homme, «l'un des fondements essentiels d'une société démocratique, l'une des conditions primordiales de son progrès et de l'épanouissement de chacun». Le dénonciateur n'est alors plus considéré comme un sujet fidèle et loyal qui a prêté allégeance au pouvoir, ou à tout le moins de qui on attend un certain patriotisme, mais comme un citoyen qui agit librement et en conscience au nom d'un intérêt qui le dépasse, l'intérêt public.

Le parti pris par le législateur européen rejait sur le champ d'application personnel et matériel de la directive. S'il est extensif, en ce qu'il ne se borne pas au travailleur *sensu stricto*, le champ d'application personnel ne va pas jusqu'à englober les «simples citoyens». Le champ d'application matériel a, quant à lui, été

circonscrit au regard des domaines d'action de l'Union où il est nécessaire de renforcer l'application de la loi parce que des faiblesses y ont été décelées⁹.

3. Après avoir fait le point sur le champ d'application de la directive (I), le présent article livre un examen critique des deux principales normes qui composent la directive: d'une part, l'élaboration d'une procédure spécifique de dénonciation qui envisage le cas spécial de la divulgation publique (II) et, d'autre part, la protection des personnes qui dénoncent des infractions au droit de l'Union (III).

I. LE CHAMP D'APPLICATION DE LA DIRECTIVE

4. Intitulée sobrement «directive sur la protection des *personnes qui signalent* des violations du droit de l'Union (nous soulignons)», la directive ne s'applique pas aux «lanceurs d'alerte» proprement dit. Elle concerne les «auteurs de signalement». La proposition de résolution adoptée par le Parlement européen le 16 avril 2019 renvoyait à la «directive sur la protection des *personnes dénonçant* les infractions au droit de l'Union (nous soulignons)» et proposait de traduire l'expression «lanceur d'alerte» par celle d'«informateur» déjà employée dans le règlement sur les abus de marché¹⁰. Le texte final de la directive se

⁹ Considérants n°s 3 et 5 de la directive sur les lanceurs d'alerte.

¹⁰ Le règlement européen sur les abus de marché, qui implémente aussi un dispositif de protection des lanceurs d'alerte, a également choisi le terme plus neutre d'«informateur» pour traduire l'expression «whistleblower» reprise dans la version anglaise. Les deux termes ne figurent toutefois pas dans le corps du règlement, mais dans les considérants (considérant n° 74 du règlement (UE) n° 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché) et abrogeant la directive 2003/6/CE du Parlement européen et du Conseil et les directives 2003/124/CE,

KERCKHOVE, «Freedom of expression as the "broken promise" of whistleblower protection», *Rev. dr. h.*, n° 10, 2016. Dans la presse, voy. aussi P. MBONGO, «Manning, Snowden... Deux questions sur les "lanceurs d'alerte"», *The Huffington Post.fr*, 31 juillet 2013 (consulté le 8 août 2017).

montre donc plus neutre encore en renvoyant exclusivement au « signalement », l'expression « informateur » étant, quant à elle, délaissée pour celle d'« auteur du signalement »¹¹. En langue anglaise, l'expression plus neutre de « reporting person » a été conservée.

5. Les travaux préparatoires, de même que les considérants de la directive, se réfèrent toute-fois sans la moindre ambiguïté aux « lanceurs d'alerte » (« whistleblowers »). Le texte finalement adopté y renvoie dès le premier considérant. La directive sur les lanceurs d'alerte ne s'applique pas pour autant qu'aux « auteurs de signalement ». Comme nous le verrons lors de l'examen du champ d'application *ratione personae* (A), d'autres personnes peuvent bénéficier, par extension, d'une protection. Après avoir mené cet examen, nous analysons le champ d'application *ratione materiae* de la directive (B).

A. Le champ d'application «*ratione personae*»

6. La directive sur les lanceurs d'alerte s'applique aux personnes qui agissent dans le cadre d'une relation de travail (1). Sont donc exclus les particuliers (2), mais aussi les personnes qui agissent en contrepartie d'une récompense financière (3).

1. Les personnes qui agissent dans le cadre d'une relation de travail

7. La directive sur les lanceurs d'alerte s'applique aux personnes qui agissent dans le cadre d'une relation de travail, en l'occurrence aux travailleurs (a). Elle s'applique également par extension aux proches des auteurs de signalement et aux facilitateurs, ainsi qu'aux entités juridiques avec lesquelles les auteurs

de signalement sont en lien dans un contexte professionnel (b).

a. Les travailleurs

8. La proposition de directive du 23 avril 2018 définissait la notion d'« informateur » comme désignant « une personne physique ou morale (nous soulignons) qui signale ou divulgue des informations sur des infractions qu'elle a obtenues dans le cadre de ses activités professionnelles »¹².

Il n'est pas commun d'accorder le statut de « lanceur d'alerte » à une personne morale. Ce choix peut s'expliquer par la filiation que la notion de lancement d'alerte partage en droit de l'Union avec la conception française de l'alerte éthique. Née dans le contexte de veille sanitaire et environnementale, l'alerte éthique peut être lancée par un citoyen vigilant, un travailleur, une agence publique de surveillance ou encore par une organisation non gouvernementale. Il n'empêche que la loi française « Sapin II », dont le champ d'application personnel est pourtant très large, n'a pas étendu la notion de « lanceur d'alerte » aux personnes morales. Une telle extension n'est de fait pas pertinente. Une personne morale ne s'expose pas à un risque de représailles comparable à celui auquel est confronté un lanceur d'alerte¹³. Or c'est bien ce risque, étroitement lié à la position de vulnérabilité (économique) du lanceur d'alerte, qui justifie l'élaboration

¹² Article 3, § 9, de la proposition de directive du 23 avril 2018.

¹³ En France, les organisations non gouvernementales et les acteurs de la société civile continuent cependant de militer en faveur d'une protection élargie des acteurs de l'alerte, considérant que la protection des personnes morales s'avère cruciale dans les secteurs environnemental et sanitaire. Voy. en ce sens, « Lancement d'alerte. Bilan de l'année et perspectives » (propos de V. ROZIÈRE), in *5^e Salon du livre de lanceuses et lanceurs d'alerte : Des livres et l'alerte*, organisé par le Presse Papier et un collectif de bénévoles, Montreuil, 22, 23 et 24 novembre 2019.

2003/125/CE et 2004/72/CE de la Commission, J.O.U.E., 12 juin 2014, L 173).

¹¹ Article 5, 7), de la directive sur les lanceurs d'alerte.

d'une protection spécifique sur le plan juridique. La directive souligne qu'«en l'absence de déséquilibre de pouvoir inhérent à la relation de travail, par exemple, dans le cas de plaignants ordinaires ou de citoyens observateurs, il est inutile de prévoir une protection contre les représailles»¹⁴.

C'est donc à juste titre que la référence aux personnes morales a disparu dans le texte adopté le 16 avril 2019¹⁵.

9. Dans le sillage de la Recommandation CM/Rec (2014)7¹⁶ et de la jurisprudence *Guja*¹⁷, la

notion de « lanceur d'alerte », ou plus exactement d'« auteur de signalement », renvoie à « une personne physique qui signale ou divulgue publiquement des informations sur des violations qu'elle a obtenues dans le cadre de ses activités professionnelles »¹⁸.

Le « contexte professionnel » s'entend largement comme englobant « 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 »¹⁹.

L'effectivité du droit de l'Union requiert en effet d'appliquer la protection au plus large éventail possible de catégories de personnes qui disposent, en raison de leur activité professionnelle, d'un « accès privilégié à des informations sur des violations qu'il serait dans l'intérêt public de signaler et qui peuvent faire l'objet de représailles si elles les signalent »²⁰. La protection devrait alors couvrir l'ensemble des personnes liées au sens large à l'organisation au sein de laquelle l'infraction s'est produite. Il pourrait s'agir de clients ou de consommateurs qui, sans être soumis à un devoir de loyauté à l'égard de leur prestataire, ont acquis les informations dénoncées dans un cadre privilégié²¹.

¹⁴ Considérant n° 36 de la directive sur les lanceurs d'alerte.

¹⁵ Le Parlement européen renvoyait encore, en novembre 2018, aux personnes morales dans sa définition de l'informateur (article 3, 9), du projet de résolution législative du Parlement européen du 26 novembre 2018). C'est que le Parlement a travaillé en étroite collaboration avec des acteurs français militant en faveur d'une extension de la protection des lanceurs d'alerte aux personnes morales. Voy. « Lancement d'alerte. Bilan de l'année et perspectives » (propos de V. ROZIERE), in *5^e Salon du livre de lanceuses et lanceurs d'alerte: Des livres et l'alerte*, organisé par le Presse Papier et un collectif de bénévoles, Montreuil, 22, 23 et 24 novembre 2019. Ex-députée européenne de nationalité française, Virginie Rozière a mené le combat du Parlement européen en faveur de l'adoption d'une directive européenne en vue de protéger les lanceurs d'alerte.

¹⁶ Recommandation CM/Rec(2014)7 sur la protection des lanceurs d'alerte adoptée par le Comité des ministres du Conseil de l'Europe le 30 avril 2014. Ci-après: Recommandation CM/Rec(2014)7.

¹⁷ Cour eur. D.H. (GC), arrêt *Guja c. Moldova*, 12 février 2008, § 97. Pour un examen de la jurisprudence « *Guja* », voy. not. V. JUNOD, « La liberté d'expression du whistleblower. Cour européenne des droits de l'homme (Grande Chambre), *Guja c. Moldova*, 12 février 2008 », *Rev. trim. dr. h.*, n° 77, 2009, pp. 227-260; V. JUNOD, « Lancer l'alerte: quoi de neuf depuis *Guja*? (Cour eur. dr. h., *Bucur et Toma c. Roumanie*, 8 janvier 2013) », *Rev. trim. dr. h.*, n° 98, 2014, pp. 459-482; K. ROSIER, « Chapitre III: hypothèses dans lesquelles une violation des obligations de secret ou de confidentialité pourrait être admise, Section 1. *Whistleblowing* », in *Secret et loyauté dans la relation de travail* (S. GILSON, K. ROSIER, A. ROGER et S. PALATE, dir.), Waterloo, Kluwer, 2013, pp. 129-150; Q. VAN ENIS, « Une solide protection des sources journalistiques et des lanceurs d'alerte:

une impérieuse nécessité à l'ère dite de la 'post-vérité'? », in *Le secret* (Y. NINANE, dir.), Limal, Anthemis, 2017, pp. 95-151.

¹⁸ Article 5, 7), de la directive sur les lanceurs d'alerte.

¹⁹ Article 5, 9), de la directive sur les lanceurs d'alerte. Le texte est repris quasi intégralement de l'article 3, § 10, de la proposition de directive du 23 avril 2018 et de l'article 6, 9), de la résolution législative du Parlement européen du 16 avril 2019.

²⁰ Considérant n° 37 de la directive sur les lanceurs d'alerte.

²¹ En faveur d'une interprétation large du champ d'application *ratione personae* du lancement d'alerte,

10. La directive distingue trois catégories de personnes qui méritent au moins le bénéfice de la protection²².

En premier lieu, la protection devrait s'appliquer aux personnes ayant le statut de « travailleurs », au sens de l'article 45, paragraphe 1^{er}, du Traité sur le fonctionnement de l'Union européenne tel qu'interprété par la Cour de justice, à savoir « les personnes qui accomplissent, pendant un certain temps, en faveur d'une autre personne et sous la direction de celle-ci, des prestations en contrepartie desquelles elles touchent une rémunération »²³. La protection devrait également être accordée aux travailleurs dans une relation de travail atypique, tels que les travailleurs à temps partiel, les travailleurs à durée déterminée et les travailleurs intérimaires, ainsi qu'aux fonctionnaires, aux employés du secteur public et à toute personne travaillant dans le secteur public²⁴.

En deuxième lieu, la protection devrait également s'appliquer aux personnes physiques qui, sans être des « travailleurs » au sens de l'article 45, paragraphe 1^{er}, du Traité sur le fonctionnement de l'Union européenne, peuvent « jouer un rôle clé en révélant des violations du droit de l'Union et peuvent se trouver dans une situation de vulnérabilité économique dans le contexte de leurs activités professionnelles »²⁵. On pense aux travailleurs indépendants au sens de l'article 49 du Traité précité²⁶, aux collaborateurs indépendants, aux consul-

tants, aux contractants, aux sous-traitants et aux fournisseurs²⁷, mais aussi aux actionnaires et aux membres de l'organe administratif, de direction ou de surveillance d'une entreprise, y compris les membres non exécutifs²⁸, ainsi qu'aux travailleurs dont la relation de travail a pris fin ou n'a pas encore débuté dans les cas où des informations concernant une infraction ont été obtenues lors du processus de recrutement ou des négociations précontractuelles²⁹.

L'extension est justifiée au regard de la pratique. Edward Snowden, dont le statut de lanceur d'alerte est unanimement reconnu en Europe, était effectivement sous-traitant de la NSA. Il ne travaillait donc pas directement pour cet organisme. Il a notamment travaillé pour *Dell* et pour *Booz Allen Hamilton*, deux prestataires de services de la NSA³⁰.

Enfin, en troisième lieu, la protection devrait également s'appliquer aux personnes qui ne se trouvent pas en situation de vulnérabilité économique, mais qui peuvent néanmoins subir des représailles pour avoir dénoncé des infractions. C'est le cas des bénévoles et des stagiaires rémunérés ou non.

11. En théorie, on pourrait penser que la directive sur les lanceurs d'alerte ne devrait pas s'appliquer aux travailleurs qui agissent en vertu d'une obligation légale de dénonciation. La dénonciation par un lanceur d'alerte est en effet nécessairement libre³¹. Le lanceur d'alerte

voy. not. V. JUNOD, « Lancer l'alerte : quoi de neuf depuis Guja ? ... », *op. cit.*, p. 479.

²² Article 4 de la directive sur les lanceurs d'alerte.

²³ Article 4, § 1^{er}, a), de la directive sur les lanceurs d'alerte. Voy. aussi le considérant n° 38 de la directive précitée.

²⁴ Considérant n° 38 de la directive sur les lanceurs d'alerte.

²⁵ Considérant n° 39 de la directive sur les lanceurs d'alerte.

²⁶ Article 4, § 1^{er}, b), de la directive sur les lanceurs d'alerte.

²⁷ Article 4, § 1^{er}, d), de la directive sur les lanceurs d'alerte.

²⁸ Article 4, § 1^{er}, c), de la directive sur les lanceurs d'alerte.

²⁹ Article 4, § 2 et § 3, de la directive sur les lanceurs d'alerte.

³⁰ Il ne s'agissait toutefois que de couvertures, l'informaticien travaillant dans les faits pour la NSA (E. SNOWDEN, *Mémoire vive*, Paris, Seuil, 2019).

³¹ Le lanceur d'alerte agit, par définition, « librement et en conscience » (Conseil d'État français, *Le droit d'alerte : signaler, traiter, protéger*, étude adoptée le 25 février 2016 par l'assemblée générale plénière du

n'est pas un professionnel de la dénonciation³²; il ne relève pas de sa fonction de dénoncer³³. La dénonciation est en vérité conçue, dans notre système juridique, comme étant en principe libre, l'obligation de dénonciation étant une exception³⁴.

Ceci étant, le régime protecteur fixé par la directive devrait s'appliquer « lorsque le droit de l'Union ou le droit national exige que les auteurs de signalement effectuent un signalement auprès des autorités nationales compétentes, par exemple parce que cela relève de leurs responsabilités et devoirs professionnels ou parce que la violation constitue une infraction pénale »³⁵. La directive joue alors un rôle de filet de sécurité dans l'hypothèse où le droit de l'Union ou le droit national n'aurait pas accompagné l'obligation de dénonciation de mesures de protection appropriées.

Si la doctrine s'inquiète de voir le nombre d'obligations légales de dénonciation croître³⁶, à la

faveur, en particulier, du contexte sécuritaire et financier conjugué à l'essor des technologies du numérique³⁷, il faut observer que le mouvement est encore relativement contenu, grâce notamment à la sagesse de la Cour constitutionnelle³⁸.

b. Les proches, les facilitateurs et les entités juridiques en lien avec l'auteur de signalement

12. En novembre 2018, le Parlement européen a suggéré d'amender la proposition de directive de façon à étendre l'application de la protection, le cas échéant, aux « facilita-

Conseil d'État, La Documentation française, 2016, p. 56.

³² À l'appui, il faut remarquer que l'expression « lanceur d'alerte potentiel » est abondamment utilisée dans les considérants de la directive sur les lanceurs d'alerte. Il en découle que tout « travailleur » est susceptible à un moment donné de lancer l'alerte mais que cette activité n'est pas habituelle.

³³ En ce sens, voy. O. LECLERC, *Protéger les lanceurs d'alerte. La démocratie technique à l'épreuve de la loi*, Issy-les-Moulineaux, L.G.D.J., 2017, pp. 20-21.

³⁴ Lorsque la loi prévoit une obligation de dénonciation, celle-ci doit en principe être limitée à certains faits précis dont la gravité justifie l'établissement d'une obligation légale. L'histoire de la dénonciation nous a effectivement montré que l'instauration d'une obligation généralisée de dénonciation était dangereuse.

³⁵ Considérant n° 62 de la directive sur les lanceurs d'alerte. En droit belge, il faut toutefois noter que les articles 29 et 30 du Code d'instruction criminelle, qui établissent la dénonciation officielle et la dénonciation privée, n'érigent pas, au sens strict, d'obligation juridique contraignante.

³⁶ Sur ce constat, voy. not. Y. Poullet, « Titre 1 – Numérique et droit – La vertu du clair-obscur », in *Vie privée, liberté d'expression et démocratie dans la société numérique* (Y. Poullet, dir.), Bruxelles, Larcier, 2020, pp. 47-46.

³⁷ On songe notamment à l'obligation de déclaration des dispositifs transfrontières potentiellement abusifs établie par la directive « DAC 6 » et à l'obligation de déclaration des soupçons de blanchiment établie par la Quatrième directive « anti-blanchiment ». Voy. directive (UE) 2018/822 du Conseil du 25 mai 2018 modifiant la directive 2011/16/UE en ce qui concerne l'échange automatique et obligatoire d'informations dans le domaine fiscal en rapport avec les dispositifs transfrontières devant faire l'objet d'une déclaration (*J.O.U.E.*, L 139, 5 juin 2018) et directive (UE) 2015/849 du Parlement européen et du Conseil 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, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission (*J.O.U.E.*, L 141, 5 juin 2015).

³⁸ La Cour constitutionnelle a ainsi annulé, par un arrêt n° 44/2019 du 14 mars 2019, l'article 46bis/1, paragraphe 3, du Code d'instruction criminelle, inséré par une loi du 17 mai 2017, qui obligeait les membres du personnel des institutions de sécurité sociale – à savoir les travailleurs sociaux des CPAS, des mutuelles ou encore des syndicats – à dénoncer spontanément au Parquet les « informations pouvant constituer des indices sérieux d'une infraction terroriste ». L'article 46bis/1 du Code d'instruction criminelle renvoyant à une « déclaration conformément à l'article 29 », il faut cependant noter qu'il ne s'agissait pas, à proprement parler, d'un *ordre de la loi* au sens de l'article 458 du Code pénal, mais bien d'une *autorisation légale*. L'obligation de dénonciation passive, c'est-à-dire sur demande du procureur du Roi, érigée par le même article, a en revanche été avalisée au regard du droit à la vie privée.

teurs»³⁹. L'amendement a été conservé dans le texte final de la directive. Par «facilitateur», il faut entendre «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»⁴⁰.

La protection s'applique également, le cas échéant, aux «tiers qui sont en lien avec les auteurs de signalement et qui risquent de faire l'objet de représailles dans un contexte professionnel, tels que des collègues ou des proches des auteurs de signalement; et [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»⁴¹.

13. On peut regretter que le texte ne précise pas si la protection de ces lanceurs d'alerte par extension sera conditionnée par la reconnaissance du statut de lanceur d'alerte (ou plus exactement d'«auteur de signalement») à la personne qu'ils ont aidée, ce qui peut représenter une sérieuse source d'insécurité juridique.

Aussi, on ne voit pas très bien en quoi le «facilitateur» se distingue des «collègues ou des proches de l'informateur». Les travaux préparatoires ne permettent pas de clarifier la notion de facilitateur. On peut penser que la différence entre les deux catégories tient dans le concours apporté concrètement à l'auteur de

signalement. Le facilitateur, comme son nom l'indique, facilite activement l'action de l'auteur de signalement. C'est le cas du collègue ou du proche qui prête son concours dans le vol de données, dans l'exploitation des données subtilisées ou encore dans la recherche d'un interlocuteur capable d'enquêter. C'est le cas également du représentant du personnel ou du représentant syndical qui informe quant au cadre légal applicable et conseille l'auteur de signalement sur les modalités à suivre⁴². À l'inverse, le simple «tiers» en lien avec l'auteur de signalement ne participe pas activement au signalement. Il risque néanmoins de faire l'objet de mesures de représailles uniquement par ricochet, en sa qualité de proche de l'auteur de signalement.

14. La protection des entités juridiques ne figurait, quant à elle, ni dans la proposition de la Commission du 23 avril 2018, ni dans la proposition législative du Parlement du 26 novembre 2018. Elle tranche également avec la Recommandation CM/Rec (2014)7 qui limite expressément la protection des lanceurs d'alerte aux personnes *physiques*, excluant de la sorte la question lancinante de l'atteinte à la réputation des organisations mises en cause directement ou indirectement par le signalement. Ce point est désormais résolu, en tout cas sur papier, par la directive sur les lanceurs d'alerte.

2. L'exclusion des personnes privées

15. La directive ne couvre pas les signalements constatés dans le domaine de la vie privée. Il est vrai que l'histoire nous a montré que la dénonciation par une personne

³⁹ Rapport sur la proposition de directive du Parlement européen et du Conseil sur la protection des personnes dénonçant les infractions au droit de l'Union (COM(2018)0218 – C8-0159/2018 – 2018/0106(CNS)), Commission des affaires juridiques, A8-0398/2018, 26 novembre 2018.

⁴⁰ Article 5, 8), de la directive sur les lanceurs d'alerte.

⁴¹ Article 4, § 4, de la directive sur les lanceurs d'alerte. La directive sur les lanceurs d'alerte reprend presque intégralement la version convenue dans la résolution législative du Parlement européen du 16 avril 2019 (article 4, § 4, b) et c)).

⁴² En ce sens, voy. le considérant n° 41 de la directive sur les lanceurs d'alerte qui souligne que les représentants syndicaux et les représentants des travailleurs doivent bénéficier de la protection prévue par la directive lorsqu'ils agissent en tant que travailleurs mais aussi lorsqu'ils fournissent conseils et aide à l'auteur de signalement.

privée exprime rarement l'accomplissement d'un devoir civique. La dénonciation s'apparente ici à de la délation⁴³, en ce qu'elle cible un proche qui dérange: un (ex-)mari, un voisin, un collègue, un concurrent⁴⁴. En outre, des auteurs américains enseignent que ce type de dénonciation, en particulier la dénonciation au fisc d'un voisin suspecté de tricher sur ses impôts sur les revenus, ne constitue pas du *whistle-blowing* au sens strict⁴⁵.

Il n'empêche que la dénonciation par une personne privée existe dans la majorité des États membres de l'Union. La réaction sociale contre le crime est en grande partie organisée autour de la dénonciation⁴⁶. Le titulaire de l'action publique, le ministère public, dispose en effet rarement d'une connaissance personnelle des infractions. Celles-ci lui sont rapportées par procès-verbal, plainte ou dénonciation de tiers⁴⁷. C'est ainsi que l'article 30 du Code

d'instruction criminelle *invite*⁴⁸ toute personne qui aura été témoin d'un attentat, soit contre la sûreté publique, soit contre la vie ou la propriété d'un individu, à «en donner avis au procureur du Roi soit au lieu du crime ou délit, soit du lieu où l'inculpé pourra être trouvé». Vestige des réformes entreprises à la sortie de la Révolution française⁴⁹, l'article 30 établit en droit belge la dénonciation «privée», dite aussi «civique». Il s'agit de la dénonciation qui «émane d'un particulier ou d'un fonctionnaire agissant en dehors de l'exercice de ses fonctions»⁵⁰. Les appels à témoins, forme déguisée d'appels à la dénonciation, sont par ailleurs monnaie courante dans les bureaux de police.

L'administration pénale n'est pas seule à faire reposer la réaction sociale sur la dénonciation. En dehors de tout cadre légal exprès, l'administration fiscale reçoit quotidiennement des lettres de dénonciation⁵¹. La dénonciation sociale peut compter, quant à elle, sur un point de contact spécialement dédié, le «Point de contact pour une concurrence loyale»⁵².

⁴³ Si l'on croise le sens commun prêté au mot «délation» avec celui forgé en sociologie, on peut définir la délation comme la dénonciation méchante ou égoïste d'une personne identifiée ou identifiable. Sur la délation et le lancement d'alerte, voy. A. LACHAPPELLE, «Le lancement d'alerte ou la délation organisée?», in *Vie privée, liberté d'expression et démocratie dans la société numérique* (Y. Poullet, dir.), Bruxelles, Larcier, 2020, pp. 209-213.

⁴⁴ En ce sens, voy. not. P. BETBEDER, «Dénoncer à Paris durant la Seconde Guerre mondiale», in *Citoyens et délateurs. La délation peut-elle être civique?* (J.-P. Brodeur et F. Jobard, dir.), Paris, Autrement, 2005, p. 78.

⁴⁵ M. P. MICELI, S. DREYFUS et J.P. NEAR, «Outsider 'whistle-blowers': Conceptualizing and distinguishing 'bell-ringing' behavior», in *International Handbook on Whistleblowing Research* (D. Lewis, A.J. Brown e.a., eds), Cheltenham, Elgar, 2014, p. 76. À ce sujet, les auteurs renvoient à la littérature de sociologie psychosociale sur le témoignage («*bystander intervention*»).

⁴⁶ S. BRAHY, «Dénonciation officielle et dénonciation civique», mercuriale prononcée le 1^{er} septembre 1978 à l'audience solennelle de la cour d'appel de Liège, *Rev. dr. pén.*, 1978, p. 947.

⁴⁷ Voy. not. R. MERLE et A. VITU, *Traité de droit criminel*, Paris, Cujas, 1967, p. 833; M. FRANCHIMONT, A. JACOBS et A. MASSET, «Chapitre 2 – Les modes de connaissance des infractions», in *Manuel de procédure pénale*, 4^e éd.,

Bruxelles, Larcier, 2012, p. 285; S. BRAHY, *ibidem*, p. 21. Voy. aussi l'article 73 du projet de loi de la proposition de loi contenant le Code de procédure pénale, *Doc., Sén.*, 2005-2006, n° 3-450/21, p. 31.

⁴⁸ Bien que l'article 30 du Code d'instruction criminelle semble ériger, de par sa formulation, une obligation de dénonciation, la doctrine s'accorde à dire qu'il ne s'agit tout au plus que d'une obligation naturelle. En ce sens, voy. not. M. FRANCHIMONT, A. JACOBS et A. MASSET, *ibidem*, p. 286.

⁴⁹ L'article 30 du Code d'instruction criminelle emprunte son contenu à l'article 30 du Code d'instruction criminelle de 1808, qui lui-même reprend en substance l'article 1^{er} de la loi du 27 novembre 1790 sur la police de sûreté, la justice criminelle et l'institution des jurés.

⁵⁰ M. FRANCHIMONT, A. JACOBS et A. MASSET, *op. cit.*, p. 285.

⁵¹ Sur la dénonciation fiscale administrative, voy. not. R. ROSOUX, «Les dénonciations au fisc: quelques réflexions sur les points de vue administratif et judiciaire belges et les pratiques dans deux pays limitrophes», *R.G.C.F.*, 2018, n° 2, pp. 135-149.

⁵² Le Point de contact pour une concurrence loyale est accessible via le lien Internet suivant: www.meldpuntsocialefraude.belgie.be/fr/index.html (consulté le 16 septembre 2019).

16. Dans un tel contexte, on s'interroge : comment le régime établi par la directive sur les lanceurs d'alerte s'articule-t-il avec ces régimes de dénonciation ? L'individu qui prend un risque en vue de révéler des activités criminelles ne mérite-t-il pas d'être protégé ? Si sans doute, et il pourra l'être, mais via d'autres mécanismes légaux que ceux prévus par la directive⁵³. *Quid* en revanche des activités qui ne sont pas réprimées par la loi pénale ? Qu'est-ce qui doit conditionner la protection : le risque pris par le dénonciateur ou l'intérêt public revêtu par l'information divulguée ? La multiplication de canaux de dénonciation est-elle un gage d'efficacité ? d'une meilleure protection ? d'une plus grande transparence ? Aucun des trois il nous semble.

3. L'exclusion des personnes qui agissent en contrepartie d'une récompense

17. Le texte amendé par le Parlement en novembre 2018, tout comme la proposition de directive du 23 avril 2018, éclipsaient totalement la question de l'intéressement du lanceur d'alerte. Les systèmes d'intéressement sont pourtant bien connus en pratique, en particulier dans le domaine criminel et dans celui des douanes et accises.

Si la directive sur les lanceurs d'alerte évoque quant à elle la question, elle la balaie aussitôt, se contentant d'indiquer qu'elle « ne devrait pas s'appliquer aux cas dans lesquels des personnes, qui, sur la base de leur consentement éclairé, ont été répertoriées comme informateurs ou enregistrées comme tels dans

des bases de données gérées par des autorités désignées au niveau national, telles que les autorités douanières, signalent des infractions aux services répressifs contre récompense ou indemnisation »⁵⁴. De tels signalements obéissent effectivement à des « procédures spécifiques qui visent à garantir l'anonymat de ces personnes afin de protéger leur intégrité physique et qui sont distinctes des canaux de signalement prévus par la [...] directive »⁵⁵.

Que faut-il en déduire ? La clause doit-elle être interprétée comme si le droit européen distinguait deux systèmes de dénonciation autonomes : le système de dénonciation avec intéressement, d'un côté, et le système de dénonciation sans intéressement, de l'autre ? Le lanceur d'alerte peut-il ou doit-il choisir : soit être protégé, soit être payé ?

Quid de l'informateur qui reçoit une récompense, mais n'est pas répertorié dans une base de données étatique ? *Quid* de l'informateur qui est répertorié dans une base de données étatique, mais sans avoir donné son consentement « éclairé » à cette fin ? *Quid* de l'informateur qui reçoit une récompense de la part d'une personne privée⁵⁶ ? Ces informateurs

⁵³ La loi du 7 juillet 2002 contenant des règles relatives à la protection des témoins menacés et d'autres dispositions organise, quant à elle, la protection des « témoins menacés » (*M.B.*, 10 août 2002). La protection suppose néanmoins que le dénonciateur soit prêt à témoigner, et donc à réitérer publiquement ses allégations. Ceci suppose qu'il renonce à l'anonymat alors qu'une telle mesure est en général réclamée par le lanceur d'alerte en guise de protection.

⁵⁴ Considérant n° 30 de la directive sur les lanceurs d'alerte.

⁵⁵ Considérant n° 30 de la directive sur les lanceurs d'alerte.

⁵⁶ Si le signalement n'a pas accédé à la publicité, la récompense pourrait avoir été octroyée par l'entreprise dont les agissements sont mis en cause : celle-ci pourrait trouver un intérêt, dans le cadre de sa politique de gestion des risques, à allouer une récompense aux dénonciateurs qui s'adressent à elle. On songe ici par exemple au « *Data Abuse Bounty Program* » mis en place par l'entreprise Facebook dans le prolongement de l'affaire des « *Cambridge Analytica Files* » (disponible à l'adresse <https://www.facebook.com/data-abuse> (consulté le 10 avril 2020)). Si le signalement a été rendu public, la récompense pourrait avoir été octroyée par un concurrent : celui-ci pourrait trouver un intérêt à décrédibiliser l'image d'un adversaire au travers de la révélation d'un scandale public.

devraient-ils bénéficier de la protection prévue par la directive ?

18. Il est vrai que dans la tradition européenne, la dénonciation effectuée dans la perspective d'un gain financier est rapprochée de la délation. Héritière de la conception républicaine de la dénonciation civique, la figure du lanceur d'alerte véhicule trois idées maîtresses : la gratuité (le dénonciateur n'agit pas en échange d'une contrepartie), le désintéressement (le dénonciateur agit au nom de l'intérêt général et non par intérêt personnel)⁵⁷ et la spontanéité (le dénonciateur n'est pas un professionnel de la dénonciation, il n'agit par ailleurs pas par obligation légale)⁵⁸.

Cette idéologie semble avoir nourri la réflexion de la Cour européenne des droits de l'homme, celle-ci affirmant sans relâche qu'un acte motivé « par la perspective d'un avantage personnel, notamment un gain pécuniaire, ne justifie pas un niveau de protection particulièrement élevé »⁵⁹. Ceci étant, elle reconnaît que le lanceur d'alerte puisse poursuivre concomitamment des intérêts plus personnels, tels que la volonté d'améliorer ses conditions de travail, à la condition de poursuivre, à titre principal, une finalité d'intérêt général⁶⁰.

B. Le champ d'application « *ratione materiae* »

19. S'inspirant des travaux du Conseil de l'Europe⁶¹, la directive sur les lanceurs d'alerte s'applique au signalement (1) d'informations confidentielles (2) à propos de pratiques qui constituent une atteinte ou une menace (3) à l'intérêt général (4). Elle n'a toutefois pas pour ambition de protéger la dénonciation de n'importe quelle atteinte ou menace à l'intérêt général, mais uniquement des pratiques qui sont considérées comme telles par le législateur européen⁶².

1. La communication orale ou écrite ...

20. La notion de « signalement » (« *report* » dans la traduction anglaise) est définie par la directive comme englobant « la communication orale ou écrite d'informations sur des violations »⁶³.

Alors que la dénonciation s'est longtemps cantonnée à un simple signalement, l'alerte est quasi systématiquement accompagnée de pièces, souvent rassemblées en un dossier étayé. Ces pièces prennent rarement la forme de documents manuscrits. Au XXI^e siècle, elles prennent, dans la majorité des cas, une forme numérique : soit que les informations sont des données numériques, soit que l'information a été numérisée (scannée, photographiée, etc.) pour faciliter sa transmission. La forme numérique permet, de surcroît, de subtiliser des documents sans les faire disparaître. Le vol effectué dans un environnement numérique

⁵⁷ Sur les vertus de gratuité et de désintéressement, voy. not. A. DESRAMEAUX, « La dénonciation fiscale en France et aux États-Unis : un enjeu républicain », *R.E.I.D.F.*, 2018, n° 1, p. 67 ; J.-F. KERLEO, « Qu'est-ce qu'un lanceur d'alerte ? Classification et conceptualisation d'une catégorie juridique insaisissable », in *Les lanceurs d'alerte. Quelle protection juridique ? Quelles limites ?* (M. DISANT et D. POLLET-PANOUSIS, dir.), Issy-les-Moulineaux, Lextenso, 2017, p. 20.

⁵⁸ V. MARTIN, « La révolution française ou l'ère du soupçon », *Hypothèses*, 2009, n° 1, p. 133.

⁵⁹ Nous soulignons. Voy. Cour eur. D.H. (GC), arrêt *Guja c. Moldova*, 12 février 2008, § 77 ; Cour eur. D.H. (5^e sect.), arrêt *Heinisch c. Allemagne*, 21 juillet 2011, § 69 ; Cour eur. D.H. (3^e sect.), arrêt *Bucur et Toma c. Roumanie*, 8 janvier 2013, § 93 ; Cour eur. D.H. (2^e sect.), arrêt *Görmüs et autres c. Turquie*, 19 janvier 2016, § 50.

⁶⁰ Voy. Cour eur. D.H., arrêt *Heinisch*, précité, § 83.

⁶¹ La Recommandation CM/Rec (2014)7 définit le « lancement d'alerte », ou plus exactement le « signalement ou révélation d'informations d'intérêt général » comme « tout signalement d'actions ou d'omissions constituant une menace ou un préjudice pour l'intérêt général, ou toute révélation d'informations sur de tels faits ».

⁶² Article 2 de la directive sur les lanceurs d'alerte.

⁶³ Article 5, 3), de la directive sur les lanceurs d'alerte.

se caractérise en effet par une soustraction frauduleuse sans dessaisissement. En l'occurrence, les *media leaks* examinés tirent tous leur origine de la divulgation illicite d'une très grande quantité de données numériques.

À l'instar de la Recommandation CM/Rec (2014)7, la directive distingue, conformément aux travaux de formalisation du *whistleblowing*⁶⁴, trois types de signalement :

- le signalement interne, à savoir « la communication orale ou écrite d'informations sur des violations au sein d'une entité juridique du secteur privé ou public »⁶⁵, notamment au supérieur hiérarchique ou auprès d'un représentant du personnel ;
- le signalement externe, à savoir « la communication orale ou écrite d'informations sur des violations aux autorités compétentes »⁶⁶, notamment aux autorités réglementaires ainsi qu'aux institutions, organes ou organismes compétents de l'Union ;
- la divulgation publique, à savoir « la mise à disposition dans la sphère publique »⁶⁷ d'informations sur des violations⁶⁸, telle que la divulgation directe au public via des plateformes en ligne ou les médias sociaux, ou aux médias, aux représentants élus, aux organisations de la société civile, aux syndicats ou aux organisations professionnelles

et commerciales (« *professional and business organisations* » dans la version anglaise)⁶⁹⁷⁰.

La protection établie par la directive peut être actionnée pour chacun de ces signalements⁷¹.

21. Quoique la directive précise qu'elle ne porte pas atteinte aux règles nationales qui encadrent le droit des travailleurs de consulter leurs représentants et syndicats, ainsi qu'à la protection prévue dans ce cadre⁷², on peut regretter qu'il ne soit pas fait mention, dans le corps de la directive, du rôle d'accompagnement et de conseil que peuvent remplir les représentants syndicaux et les représentants des travailleurs en faveur des lanceurs d'alerte⁷³.

2. ... d'informations confidentielles ...

22. Le *whistleblowing* porte par nature sur des informations confidentielles, c'est-à-dire des informations qui ne sont pas connues,

⁶⁹ L'expression désigne vraisemblablement les organisations représentatives des employeurs ainsi que celles qui assurent la défense de leurs intérêts commerciaux.

⁷⁰ Considérant n° 45 de la directive sur les lanceurs d'alerte.

⁷¹ Article 6 de la directive sur les lanceurs d'alerte. Voy. aussi le considérant n° 33 de la directive précitée.

⁷² Article 3, § 4, de la directive sur les lanceurs d'alerte.

⁷³ Cette lacune a notamment été pointée par la Confédération française démocratique du travail (Cfdt), le premier syndicat français en nombre d'adhérents. Voy. « Lanceurs d'alerte: de nouvelles règles de protection adoptées au sein de l'Union européenne », *Vos droits > Fil d'actu juridique*, 7 mai 2019, disponible sur www.cfdt.fr (consulté le 6 octobre 2019). Le considérant n° 54 de la directive reconnaît malgré tout que les représentants syndicaux et les représentants des travailleurs puissent recevoir, à la condition qu'ils offrent les qualités appropriées, des signalements pour le compte d'entités publiques ou privées. De plus, le considérant n° 41 souligne que les représentants syndicaux et les représentants des travailleurs doivent bénéficier de la protection prévue par la directive lorsqu'ils agissent en tant que travailleurs mais aussi lorsqu'ils fournissent conseils et aide à l'informateur. Ils agissent alors en tant que « facilitateurs ».

⁶⁴ Voy. spéc. J.P. NEAR et M.P. MICELI, « Organizational dissidence: The case of whistle-blowing », *Journal of Business Ethics*, vol. 4, Iss. 1, 1985, pp. 1-16.

⁶⁵ Article 5, 4), de la directive sur les lanceurs d'alerte.

⁶⁶ Article 5, 5), de la directive sur les lanceurs d'alerte.

⁶⁷ Précisons que l'expression « sphère publique » a été préférée à celle de « domaine public » mentionnée dans la résolution législative du Parlement européen du 16 avril 2019 (article 6, 6), de la résolution précitée.

⁶⁸ Article 5, 6), de la directive sur les lanceurs d'alerte.

difficilement ou pas publiquement accessibles et censées demeurer cachées⁷⁴.

Le dénonciateur peut être entré en possession de ces informations légalement (en raison de sa position dans l'organisation) ou non (en raison de sa proximité avec le détenteur légal de ces informations ou en raison d'une infraction).

La révélation de telles informations est, quoi qu'il en soit, susceptible de mettre à mal le devoir de loyauté, de réserve et de discrétion auquel est astreint tout travailleur vis-à-vis de son employeur, mais aussi le devoir de secret professionnel auquel sont tenus certaines professions. Cette particularité explique que la protection établie par la directive prenne notamment la forme d'une immunité de responsabilité.

23. Certaines informations confidentielles méritent un traitement particulier. À l'instar de la Recommandation CM/Rec (2014)7 et de la plupart des *whistleblowing laws*⁷⁵, la directive exclut le domaine de la sécurité nationale et de la défense ainsi que les mesures concernant la protection des informations classifiées et du secret professionnel des avocats et du secret médical, le secret des délibérations judiciaires et les règles en matière de procédure pénale⁷⁶. Elle précise qu'il n'est pas fait atteinte à la confidentialité d'une correspondance entre un avocat et son client («secret professionnel des avocats») ou d'une communication entre un prestataire de soins de santé et un patient

(«secret médical»)⁷⁷. Il s'ensuit qu'un avocat ou un professionnel de la santé ne pourrait pas, sur pied de la directive, lancer l'alerte à propos de faits qui lui ont été confiés *en sa qualité de dépositaire* du secret professionnel⁷⁸. En revanche, libres à eux de dénoncer les faits dont ils ont connaissance sur leur lieu de travail en raison de leur profession. Dans le contexte sanitaire singulier de ces derniers mois, on songe bien évidemment à un professionnel de la santé qui aurait par exemple connaissance de pratiques frauduleuses dans l'approvisionnement (ou son défaut) de masques et gels hydro-alcooliques ou encore à un avocat qui aurait par exemple connaissance de vices de procédure récurrents dans l'octroi de subsides aux entreprises durement touchées par les mesures de confinement.

Pour ce qui est des membres de professions autres que les avocats et les prestataires de soin de santé, ils «devraient pouvoir prétendre à la protection prévue par la [...] directive lorsqu'ils signalent des informations protégées par les règles professionnelles applicables, à condition que signaler ces informations soit

⁷⁷ Considérant n° 26 de la directive sur les lanceurs d'alerte.

⁷⁸ En droit belge, le secret professionnel peut cependant être levé dans quatre hypothèses : l'ordre de la loi, l'autorisation légale, l'état de nécessité et l'exercice des droits de la défense. Les législations qui encadrent le *whistleblowing*, même ponctuellement comme la directive « secrets d'affaires » et le règlement sur les abus de marché, érigent des autorisations de parler au sens de l'article 458 du Code pénal. En dehors de cette exception, il faut noter que la Cour d'appel du Grand-Duché de Luxembourg a préféré, dans le cadre de l'affaire « Lux Leaks », consacrer le nouveau fait justificatif « du lanceur d'alerte » plutôt que d'admettre l'état de nécessité comme cause de justification à la révélation d'intérêt public à l'œuvre. Si besoin est, précisons que le Grand-Duché de Luxembourg connaît une prescription équivalente à celle de l'article 458 du Code pénal belge. Sur la levée du secret professionnel, voy. not. P. LAMBERT, *Secret professionnel*, Bruxelles, Bruylant, 2005, pp. 41-45.

⁷⁴ En ce sens, voy. not. Comm. eur. D.H., déc. *Haseldine c. Royaume-Uni*, 13 mai 1992.

⁷⁵ Voy. par exemple l'article 6, alinéa 2, de la Loi Sapin II.

⁷⁶ Article 3, §§ 2 et 3, de la directive sur les lanceurs d'alerte. Notons que dans une proposition de résolution récente, des députés Ecolo-Groen recommandent de ne pas exclure ces questions du champ de la loi belge de transposition (proposition de résolution relative à la protection des libertés fondamentales des lanceurs d'alerte et des journalistes, *Doc.*, Ch., 2019-2020, n° 55-1069/001).

nécessaire pour révéler une violation relevant du champ d'application» de ladite directive⁷⁹.

24. Précisons que le «secret d'affaires» n'est pas exclu du champ d'application de la directive.

Aux fins de la directive «secrets d'affaires», on entend par «secret d'affaires», «des informations qui répondent à toutes les conditions suivantes: a) elles sont secrètes en ce sens que, dans leur globalité ou dans la configuration et l'assemblage exacts de leurs éléments, elles ne sont pas généralement connues des personnes appartenant aux milieux qui s'occupent normalement du genre d'informations en question, ou ne leur sont pas aisément accessibles; b) elles ont une valeur commerciale parce qu'elles sont secrètes; c) elles ont fait l'objet, de la part de la personne qui en a le contrôle de façon licite, de dispositions raisonnables, compte tenu des circonstances, destinées à les garder secrètes»⁸⁰. À la lumière des «*trade secrets*» américains, la notion couvre donc des informations très variées, «qui vont des connaissances technologiques aux données commerciales telles que les informations relatives aux clients et aux fournisseurs, les plans d'affaires ou les études et stratégies de marché»⁸¹. Elle couvrirait également des informations sensibles et particulièrement importantes sur le plan sociétal, telles que la composition des médicaments et la traçabilité

des substances et excipients utilisés dans leur fabrication⁸².

Il s'ensuit que le lanceur d'alerte qui signale ou révèle des secrets d'affaires est couvert par la directive s'il respecte les conditions prévues par elle. Dans ce cas, la divulgation doit être considérée comme «autorisée par le droit de l'Union» au sens de la directive «secrets d'affaires», et partant comme licite⁸³.

3. ... à propos de pratiques qui constituent une atteinte ou une menace ...

25. La conception du *whistleblowing* véhiculée par la proposition de directive et ensuite par le texte adopté en première lecture par le Parlement européen a pu paraître trop légaliste en ce qu'elle renvoyait aux *infractions* alors que la version anglaise se référait à la notion plus souple de «*breaches*».

C'est donc à bon escient que la notion d'«infraction» a laissé la place à la notion plus neutre de «violation» dans le texte final de la directive. Entendue indépendamment de la classification au regard du droit national comme étant de nature administrative, pénale ou autre⁸⁴, la notion de «violation» couvre les actes ou omissions qui (i) sont illicites et ont trait aux actes de l'Union et aux domaines relevant du champ d'application matériel visé à l'article 2 de la directive (activités illicites) ou qui (ii) vont à l'encontre de l'objet ou de la finalité des règles prévues dans les actes de l'Union et les domaines relevant du champ d'appli-

⁷⁹ Considérant n° 27 de la directive sur les lanceurs d'alerte.

⁸⁰ Article 2 de la directive «secrets d'affaires». Sur cette définition, voy. not. V. CASSIERS, «La directive 2016/943/UE du 8 juin 2016 sur les secrets d'affaires», *J.T.*, 2017, pp. 387-388.

⁸¹ Communiqué de presse, 3317^e session du Conseil, «Compétitivité (marché intérieur, industrie, recherche et espace)», PRESSE 308, PR CO 29, Bruxelles, 26 mai 2014, p. 7, disponible sur <http://data.consilium.europa.eu> (consulté le 2 novembre 2019).

⁸² En ce sens, voy. not. «Lanceuses d'alerte, "les résistantes"» (propos d'A. DUPEREY et M. MARTIN), in 5^e *Salon du livre de lanceuses et lanceurs d'alerte: Des livres et l'alerte*, organisé par le Presse Papier et un collectif de bénévoles, Montreuil, 22, 23 et 24 novembre 2019.

⁸³ Sur l'articulation entre la directive «secrets d'affaires» et la directive sur les lanceurs d'alerte, voy. le considérant n° 98 de la directive sur les lanceurs d'alerte. Voy. aussi *infra* n° 61.

⁸⁴ Considérant n° 3 de la directive sur les lanceurs d'alerte.

tion matériel visé à l'article 2 de la directive (activités abusives)⁸⁵.

26. L'effectivité du droit de l'Union requiert d'appliquer la protection prévue par la directive aux infractions réalisées, mais aussi aux «violations qui ne se sont pas encore matérialisées mais qui vont très probablement avoir lieu, [aux] actes ou [aux] omissions que l'auteur de signalement a des motifs raisonnables de considérer comme des violations, ainsi qu'[aux] tentatives de dissimulation de violations»⁸⁶. L'application de la protection aux tentatives de dissimulation d'infractions s'inspire vraisemblablement d'un texte britannique longtemps présenté comme un modèle en la matière, le *Public Interest Disclosure Act* (PIDA)⁸⁷.

Ceci explique que la protection prévue par la directive s'applique aux actes et faits qui représentent une *menace* ou une *atteinte* à l'intérêt général, et ce dans l'optique précise de prévenir, de dissuader et de détecter les

actes répréhensibles. La conception que la directive véhicule de la dénonciation s'inscrit donc pleinement dans les travaux du Conseil de l'Europe, mais aussi des «pères» de l'alerte éthique en France, Francis Chateauraynaud et Didier Torny⁸⁸. Au sens de la directive, la dénonciation vise de fait tant à prévenir les risques (logique de l'alerte) qu'à sanctionner les méfaits (logique de la dénonciation).

27. En revanche, la protection ne devrait pas s'appliquer «aux personnes qui signalent des informations qui sont *déjà entièrement disponibles dans le domaine public* ou des rumeurs ou ouï-dire non fondés (nous soulignons)»⁸⁹.

S'il est parfaitement cohérent d'exclure du champ d'application de la directive les dénonciations légères dénuées de toute vraisemblance, on s'interroge sur la portée de l'exclusion des «informations qui sont déjà entièrement disponibles dans le domaine public»⁹⁰.

L'expression «informations qui sont déjà *entièrement disponibles dans le domaine public*» couvre-t-elle les documents qui sont déjà en possession des pouvoirs publics en raison d'une obligation légale de déclaration – à charge

⁸⁵ Article 5, 1), de la directive sur les lanceurs d'alerte. Voy. aussi le considérant n° 42 de la directive précitée. La précision est particulièrement importante dans le domaine fiscal puisque certaines pratiques fiscales *licites* peuvent être taxées d'*abusives* en raison de leur degré de complexité et/ou du montant d'impôt éludé sur la base d'une disposition anti-abus.

⁸⁶ Considérant n° 43 de la directive sur les lanceurs d'alerte. Voy. aussi la notion d'«informations sur des violations» (article 5, 2), de la directive précitée.

⁸⁷ De son intitulé complet, «*An Act to protect individuals who make certain disclosures of information in the public interest; to allow such individuals to bring action in respect of victimisation; and for connected purposes*», le PIDA insère dans l'*Employment Rights Act 1996* (ERA 1996) une Section IV A spécialement dédiée à la révélation (*disclosure*) d'intérêt public (*public interest*). Le PIDA protège des représailles et du licenciement les «workers» qui dénoncent, moyennant le respect de certaines conditions, des «*qualifying disclosure*», c'est-à-dire toute révélation d'informations qui, selon la croyance raisonnable («*reasonable belief*») du travailleur faisant la révélation, tend à montrer une ou plusieurs des six catégories de faits mentionnées dans la loi. Le texte du PIDA peut être consulté à l'adresse: www.legislation.gov.uk/ukpga/1998/23/contents (consulté le 10 avril 2020).

⁸⁸ Du point de vue des deux sociologues, le lancement d'alerte se présente «comme un cas particulier de rencontre entre une logique de la dénonciation et une logique de l'alerte» (F. CHATEAURAYNAUD et D. TORNÉ, *Les sombres précurseurs. Une sociologie pragmatique de l'alerte et du risque*, 2^e éd., Paris, École des hautes études en sciences sociales (EHESS), 2013, p. 21).

⁸⁹ Considérant n° 43 *in fine* de la directive sur les lanceurs d'alerte.

⁹⁰ Le Parlement européen avait recommandé de renverser cette exclusion, qui figurait dans la proposition de directive du 23 avril 2018 et de prévoir au contraire la protection des «personnes apportant de nouvelles informations concernant des questions qui sont déjà dans le domaine public».

d'un tiers⁹¹ ou du contribuable⁹² – ou d'une enquête administrative ou pénale? Englobe-t-elle plutôt, à la lumière de l'arrêt rendu par la Cour de cassation luxembourgeoise dans le cadre de l'affaire «Lux Leaks», les informations déjà connues du public (en raison ou non d'une précédente fuite)? Cette seconde interprétation est la plus vraisemblable dès l'instant où le texte adopté en première lecture par le Parlement européen le 16 avril 2019 définissait la «divulgation publique» comme «la mise à la disposition du *domaine public* d'informations sur des infractions (nous soulignons)»⁹³.

28. En toute hypothèse, il nous semble totalement exclu d'interpréter le considérant n° 43 *in fine* de la directive sur les lanceurs d'alerte comme validant une quelconque condition d'originalité.

Certes, la condition d'originalité est une condition classique en droit américain de la dénonciation. Elle a d'ailleurs été reprise dans l'article 32, paragraphe 4, du règlement sur les abus de marché, qui s'inspire du *Dodd-Frank Act*, un texte américain. La condition n'est toutefois justifiée qu'au regard du système d'intéressement qui accompagne la plupart des *whistleblowing laws* aux États-Unis. Il n'est effectivement pas utile pour une autorité de recevoir une information déjà en sa possession. La condition intervient donc uniquement en cas de signalement auprès des autorités

compétentes, et non pas en cas de signalement interne ni de révélation publique.

4. ... à l'intérêt général

29. La notion d'«intérêt général» englobe, dans toute l'Europe, les idées de «prospérité» et de «bien-être» du public et de la société⁹⁴. En ce sens, la directive sur les lanceurs d'alerte considère que «les violations du droit de l'Union [...] peuvent porter gravement atteinte à l'intérêt public, *en ce qu'elles engendrent des risques importants pour le bien-être de la société* (nous soulignons)»⁹⁵.

Aussi commune soit-elle pour un juriste, la notion d'intérêt général n'en est pas moins une notion extrêmement vague. S'inspirant de son homologue britannique et du «PIDA», le législateur européen a alors choisi de lister quels étaient les faits à pouvoir faire l'objet d'une dénonciation au sens de la directive, et partant à constituer une atteinte ou une menace à l'intérêt général. Les actes et domaines d'actions énumérés ont été sélectionnés dans la mesure «où:

- il est nécessaire de renforcer l'application de la loi,
- le sous-signalement des violations par les lanceurs d'alerte est un facteur clé affectant l'application de la loi, et

⁹¹ En droit fiscal, on pense, par exemple, à l'obligation de déclaration des soupçons de blanchiment en vertu de la législation anti-blanchiment ou à l'obligation de déclaration des montages transfrontières en vertu de la directive DAC 6. Voy. *supra* note infrapaginale n° 35.

⁹² En droit fiscal, on songe spécialement à l'obligation de déclaration des constructions juridiques étrangères établie par l'article 307 du C.I.R. 92.

⁹³ Article 6, 6), de la résolution législative du Parlement européen du 16 avril 2019. La directive sur les lanceurs d'alerte a cependant opté pour l'expression plus neutre de «sphère publique» (article 5, 6), de la directive).

⁹⁴ Recommandation CM/Rec (2014)7, Exposé des motifs, Annexe – Les 29 principes, point 41; Conseil de l'Europe, *Protection des lanceurs d'alerte: Petit guide pour la mise en œuvre nationale*, août 2016, p. 8.

⁹⁵ Considérant n° 3 de la directive sur les lanceurs d'alerte. La directive sur les lanceurs d'alerte relève aussi qu'«[e]n signalant des violations du droit de l'Union qui portent atteinte à l'intérêt public, ces personnes agissent en tant que «lanceurs d'alerte» et jouent ainsi un rôle clé dans la révélation et la prévention de ces violations et dans la *préservation du bien-être de la société* (nous soulignons)» (considérant n° 1 de la directive).

- des violations du droit de l'Union peuvent porter gravement atteinte à l'intérêt public»⁹⁶.

Il s'agit des domaines suivants :

- « 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 »⁹⁷.

Tenant compte du fait que les signalements qui concernent des intérêts privés sont en général exclus du champ du *whistleblowing*, la directive sur les lanceurs d'alerte indique que les États membres peuvent « prévoir que les signalements de griefs interpersonnels affectant exclusivement l'auteur de signalement, en d'autres termes les griefs concernant des conflits interpersonnels entre l'auteur de signalement et un autre travailleur, peuvent être communiqués via d'autres procédures »⁹⁸. De tels signalements concernent en réalité l'hypothèse de la plainte, qui doit être distinguée de celle de la dénonciation⁹⁹.

À l'heure où nous écrivons ces lignes, certains domaines se démarquent assurément. Ayant à l'esprit l'appel lancé par les médecins chinois Ai Fen et Li Wenliang en décembre 2019, il apparaît particulièrement pertinent de faire figurer le domaine de la santé publique parmi les domaines spécialement protégés. L'utilisation massive des technologies de communication durant la période de confinement et le développement d'applications de traçage en vue de suivre la propagation du Covid-19 confirment également la pertinence de faire figurer le domaine de la « protection de la vie privée et des données à caractère personnel, et sécurité des réseaux et des systèmes d'information »¹⁰⁰.

30. La liste proposée par la directive n'est pas exhaustive. 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 directive¹⁰¹.

Des députés écologistes proposent d'étendre, dans le cadre de la loi belge de transposition, le champ d'application matériel du régime de protection à toutes les infractions à la loi (qu'il s'agisse de la loi belge ou de la loi européenne) ainsi qu'aux actes qui constituent une atteinte ou une menace à l'intérêt général¹⁰².

émane d'une personne qui est lésée par l'infraction ou qui ne l'est pas (G. CORNU (dir.), *Vocabulaire juridique*, Association Henri Capitant, 8^e éd., Paris, P.U.F., 2000, p. 274).

¹⁰⁰ La crise du Covid-19 justifie, selon certaines associations de lutte contre la corruption, de précipiter l'entrée en application du régime de protection établi par la directive sur les lanceurs d'alerte. En ce sens, voy. not. la lettre ouverte, signée par plus d'une cinquantaine d'associations de défense des droits des lanceurs d'alerte et de professeurs engagés, intitulée « Coalition to Make Whistleblowing Safe During Covid-19 and Beyond », disponible à l'adresse <https://phplist.access-info.org/uploadimages/files/2020%2004%2006%20CMWS%20COVID-19%20-%20FINAL%20VERSION.pdf> (consulté le 9 avril 2020).

¹⁰¹ Article 2, § 2, de la directive sur les lanceurs d'alerte.

¹⁰² Proposition de résolution relative à la protection des libertés fondamentales des lanceurs d'alerte et des

⁹⁶ Considérant n° 5 de la directive sur les lanceurs d'alerte. Voy. aussi ses considérants n°s 106 et 107.

⁹⁷ Article 2, § 1^{er}, a), de la directive sur les lanceurs d'alerte.

⁹⁸ Considérant n° 22 de la directive sur les lanceurs d'alerte.

⁹⁹ On parle classiquement de plainte ou de dénonciation selon que la communication d'informations

Au regard des nouvelles pratiques en matière de tests d'intrusion (ou «*pentesting*»), des auteurs plaident en faveur d'une extension de la protection, ou en tout cas de la reconnaissance d'une protection équivalente, en faveur des «pirates éthiques»¹⁰³. Au risque de dénaturer la figure originelle du lanceur d'alerte, il nous semble adéquat de circonscrire l'application de la protection des lanceurs d'alerte aux cas d'intrusion et de signalement spontané, désintéressé et gratuit en veillant à forger une nouvelle étiquette. Celle de «*pirate éthique*» est antinomique, le «pirate» étant par nature une personne intéressée et cupide agissant au regard d'un projet «professionnel»¹⁰⁴.

31. Mais jusqu'où aller ?

Le domaine électoral, pourtant propice aux scandales publics – songeons aux «*Cambridge Analytica Files*» – ne figure pas parmi les domaines couverts par la directive sur les lanceurs d'alerte. L'affaire «*Griveaux*» enseigne que le choix semble judicieux pour ce qui est des questions liées à la «morale publique»¹⁰⁵.

Aussi, il convient de bien s'entendre sur la qualification de «lanceur d'alerte» dans le domaine.

Celui que l'on qualifie parfois de lanceur d'alerte dans cette affaire – Piotr Pavlenski – n'en est pas un : non pas vraiment parce qu'il n'a pas agi dans le contexte d'une relation de travail, mais parce qu'il a uniquement agi au nom d'une valeur nouvellement consacrée, celle de la transparence¹⁰⁶, en publiant une vidéo à caractère sexuel de l'ex-candidat à la mairie de Paris. Sans doute doit-on plus y voir un *leaker*, un activiste de la transparence. Dans le cadre d'une campagne électorale, on peut certes s'interroger : cette contradiction apparente peut-elle faire craindre d'autres contradictions, dans le chef du candidat maire, entre ses paroles et ses actions politiques ? Dans le même temps, on doute que le manque de cohérence dans un contexte intime emporte nécessairement un manque de cohérence dans un contexte public. Les dirigeants dont la

journalistes, *Doc.*, Ch., 2019-2020, n° 55-1069/001.

¹⁰³ En ce sens, voy. J.-F. HENROTTE et P. LIMBRÉE, «Le pirate éthique à l'épreuve du droit pénal et de la protection des données», *Legitech*, 2019, n° 1, p. 24.

¹⁰⁴ Le mot «pirate» vient en effet du latin «*pirata*» qui signifie «celui qui tente la fortune, qui est entreprenant» (*L'encyclopédie libre Wikipédia*, en ligne, consulté le 13 avril 2020). Dans le domaine informatique, le *Dictionnaire Larousse* définit d'ailleurs le «pirate» comme une «personne qui détourne à des fins malveillantes ou même détruit les protections d'un logiciel, d'un ordinateur ou d'un réseau informatique» (*Dictionnaire Larousse*, en ligne, consulté le 13 avril 2020). Ce faisant, parler de «pirate éthique» semble aussi inapproprié que de parler que «délation éthique».

¹⁰⁵ Pour rappel, les faits à l'origine de l'affaire «*Griveaux*» sont les suivants. En mai 2018, Benjamin Griveaux, alors porte-parole du gouvernement français, noue une relation avec une étudiante, Alexandra de Taddeo. Il lui transmet une vidéo à caractère sexuel qui ne peut être regardée que durant un court délai, mais l'étudiante décide de l'enregistrer. Bernard Griveaux est pourtant marié et père de famille, ce qu'il

se plaît à souligner lors de sa campagne à la mairie de Paris, entamée durant l'été 2019. Activiste russe réfugié en France, le compagnon d'Alexandra de Taddeo, Piotr Pavlenski, voit une contradiction entre les déclarations du candidat à la mairie de Paris en tant que père de famille aimant et l'adultère commis avec une étudiante, renforcé par l'envoi d'une vidéo à caractère sexuel. Cette contradiction doit éclater au grand jour. Cela étant, *Mediapart* refuse de publier la vidéo : la contradiction apparente ne justifie pas de briser le principe sacro-saint du droit à la vie privée. L'exercice de la liberté d'expression, en ce compris la liberté de presse, comporte à juste titre des devoirs et des responsabilités. Le 13 février 2020, Piotr Pavlenski décide de diffuser lui-même en ligne la vidéo. Les réactions ne se font pas attendre. Benjamin Griveaux annonce retirer sa candidature dès le lendemain. Pour un résumé de l'affaire, voy. not. «Affaire *Griveaux* : la chronologie d'un scandale», *Franceinfo*, 17 février 2020, disponible sur https://www.francetvinfo.fr/societe/affaire/affaire-griveaux-la-chronologie-d-un-scandale_3830417.html (consulté le 10 avril 2020).

¹⁰⁶ Sur la montée de cette valeur à l'ère numérique, voy. not. Y. PUILLET, «Titre 1 – Numérique et droit – La vertu du clair-obscur», in *Vie privée, liberté d'expression et démocratie dans la société numérique* (Y. PUILLET, dir.), Bruxelles, Larcier, 2020, pp. 15-66.

vision politique remarquable ont contribué à façonner la société du XXI^e siècle étaient-ils tous des hommes de vertu ? On en doute. Aussi, un constat est frappant : la diffusion publique de la vidéo a coupé court à tout débat public. Le principal intéressé a préféré mettre d'abord un terme à sa candidature plutôt que de répondre publiquement de ses actes. Le *leak* n'a ici emporté ni sanction juridique, ni sanction sociale, l'intéressé s'étant lui-même censuré. Or le propre du dénonciateur, et à plus forte raison du lanceur d'alerte, est de vouloir provoquer une réaction.

II. LA MISE EN PLACE DE CANAUX DE SIGNALEMENT

32. Conformément à l'approche « structurelle » du *whistleblowing*¹⁰⁷, le législateur européen oblige les entités privées et publiques à insérer, au sein de leur *structure* même de gouvernance, des canaux exprès de signalement parfois appelés « *whistleblowing hotlines* »¹⁰⁸.

S'ils s'insèrent pleinement parmi les mécanismes de gouvernance classique, les « *whistleblowing hotlines* » représentent en règle un dispositif complémentaire à côté des autres dispositifs habituels de contrôle et de *reporting*

(représentants des travailleurs, ligne hiérarchique, audit, service d'inspection, etc.)¹⁰⁹.

33. La directive sur les lanceurs d'alerte prévoit la mise en place de canaux exprès de communication en ce qui concerne tant le signalement interne (A) que le signalement externe (B). Les obligations relatives à l'établissement de tels canaux devraient s'appuyer autant que possible sur les canaux existants prévus par des actes de l'Union spécifiques, tels que le règlement sur les abus de marché et la Quatrième directive anti-blanchiment¹¹⁰. La directive aborde en outre explicitement la question de la révélation publique, notamment aux médias (C).

A. Le signalement interne

34. D'après l'article 8 de la directive sur les lanceurs d'alerte, les États membres veillent à établir une obligation de mettre en place des canaux et des procédures *internes* pour le signalement et le suivi des signalements à destination¹¹¹ :

- des entités juridiques privées qui comptent 50 travailleurs ou plus¹¹² ;

¹⁰⁷ Sur l'approche structurelle, voy. not. T. M. DWORKIN et A. J. BROWN, « The Money or the Media? Lessons from Contrasting Developments in US and Australian Whistleblowing Laws », *Seattle Journal for Social Justice*, vol. 11, Iss. 2, Art. 8, 2013, p. 679. Voy. aussi A. LACHAPPELLE, « Le lancement d'alerte ou la délation organisée ? », *op. cit.*, pp. 213-215.

¹⁰⁸ L'approche « structurelle » a été transposée dans divers textes américains, notamment le « *Sarbanes-Oxley Act* » et le « *Dodd-Frank Act* », qui ont servi de source d'inspiration au législateur européen et au législateur français dans l'implémentation de dispositifs de dénonciation des irrégularités dans le domaine comptable et financier, ainsi que dans le domaine des abus de marché.

¹⁰⁹ En ce sens, voy. not. N. SMAILL, « Le *whistleblowing* : la solution en gouvernance ? », in *Gouvernance, risques et crise financière* (S. ROUSSEAU, dir.), Montréal, Thémis, 2013, p. 240 ; B. FASTERLING, « Whistleblower protection: A comparative law perspective », in *International Handbook on Whistleblowing Research* (D. LEWIS, A. J. BROWN e.a., eds), Cheltenham, Elgar, 2014, p. 345 ; M. LAUVAUX, V. SIMON et D. STAS DE RICHELLE, *Criminalité du travail : détecter et contrôler les comportements frauduleux – sanctions et responsabilité du travailleur*, Études pratiques de droit social, Waterloo, Kluwer, 2007, p. 129.

¹¹⁰ Considérant n° 68 de la directive sur les lanceurs d'alerte.

¹¹¹ Après consultation des partenaires sociaux et en accord avec ceux-ci, lorsque le droit national le prévoit (article 8, § 1^{er}, de la directive sur les lanceurs d'alerte).

¹¹² Après une évaluation des risques appropriée, les États membres peuvent étendre l'obligation à des entités privées qui comptent moins de 50 travailleurs (petites et microentreprises) (article 8, § 7, et considérant n° 49 de la directive sur les lanceurs d'alerte). En tout état

- des entités juridiques privées relevant du champ d'application des actes de l'Union visés dans l'annexe de la directive¹¹³;
- des entités juridiques publiques, y compris toute entité détenue ou contrôlée par une entité juridique publique, étant entendu que les États membres peuvent exempter de l'obligation les municipalités comptant moins de 10.000 habitants, ou moins de 50 employés, ou les autres entités comptant moins de 50 employés¹¹⁴.

En dehors de cette obligation, une entreprise pourrait parfaitement décider de mettre en place un dispositif d'alerte interne dans le cadre de ses politiques de responsabilité soci(ét)ale d'entreprise. Les organisations pourront prochainement s'aider dans ce cadre de la Norme «ISO/NP 37002 *Whistleblowing management systems*». La mise en place d'un dispositif d'alerte interne est effectivement de plus en plus mise en avant comme un outil de minimisation des risques¹¹⁵.

La notion d'«entité juridique privée» n'a pas été définie. L'expression mérite pourtant qu'on s'y attarde. La notion d'entité privée est-elle réservée aux personnes morales ou englobe-t-elle également les personnes physiques qui exercent des activités économiques durables?

Dans ce cas, la notion d'entité privée doit-elle être rapprochée de celle d'«entreprise», telle que définie dans le Code de droit économique¹¹⁶? La notion d'«entité publique» apporte aussi son lot de difficultés. Une autorité administrative indépendante est-elle une entité publique au sens de la directive sur les lanceurs d'alerte? *Quid* des établissements scolaires? Un établissement d'enseignement primaire est-il soumis à l'obligation? *Quid* d'une université?

35. Les procédures de signalement et de suivi des signalements internes comportent cinq éléments dont certains méritent une note d'explication livrée ci-dessous:

- 1) des canaux de signalements sûrs et confidentiels¹¹⁷;
- 2) un accusé de réception du signalement adressé à l'auteur de signalement et un «retour d'informations» sur le «suivi» apporté au signalement¹¹⁸.

Par «suivi», il faut entendre «toute mesure prise par le destinataire du signalement, ou toute autorité compétente, pour évaluer l'exactitude des allégations formulées dans le signalement et, le cas échéant, pour remédier à la violation signalée, y compris par des mesures telles qu'une enquête interne, une enquête, des poursuites, une action en recouvrement de fonds, ou la clôture de la procédure»¹¹⁹. Le «retour d'in-

de cause, il convient de s'assurer que les personnes qui travaillent dans des entités juridiques privées qui ne doivent pas mettre en place de canaux de signalement interne soient informées de la possibilité de s'adresser directement aux autorités compétentes et de bénéficier dans ce cadre de la protection établie par la directive (considérant n° 51 de la directive sur les lanceurs d'alerte).

¹¹³ Il s'agit notamment des entités privées exerçant leurs activités dans le domaine des services financiers ou vulnérables au blanchiment de capitaux ou au financement du terrorisme.

¹¹⁴ Article 8, § 9, de la directive sur les lanceurs d'alerte.

¹¹⁵ Tel que réformé en 2020, le Code belge de gouvernance d'entreprise intègre en effet le *whistleblowing* parmi les «systèmes de contrôle interne et de gestion des risques» (principe 4.13).

¹¹⁶ Sauf disposition contraire, pour l'application du Code de droit économique, on entend par «entreprise» toute personne physique qui exerce une activité professionnelle à titre indépendant, toute personne morale de droit privé, toute personne morale de droit public qui offre des biens et services sur un marché ainsi que toute organisation sans personnalité juridique qui poursuit un but de distribution (article I.1. du CDE).

¹¹⁷ Article 9, § 1^{er}, a), de la directive sur les lanceurs d'alerte.

¹¹⁸ Article 9, § 1^{er}, b) et f), de la directive sur les lanceurs d'alerte.

¹¹⁹ Article 5, 12), de la directive sur les lanceurs d'alerte.

formations» consiste, quant à lui, dans « la communication à l'auteur de signalement d'informations sur les mesures envisagées ou prises au titre de suivi et sur les motifs de ce suivi »¹²⁰;

- 3) la désignation d'une personne ou d'un service impartial compétent pour recevoir et/ou assurer le suivi des signalements¹²¹. En fonction de la structure de l'entité, il peut s'agir d'un responsable de la conformité (*Chief Compliance*) ou des ressources humaines, d'un responsable de l'intégrité, d'un responsable juridique ou de la protection de la vie privée (*Legal Officer* ou *Data Protection Officer – DPO*), d'un directeur financier exécutif, d'un responsable de l'audit interne ou d'un membre du conseil d'administration («*board*» dans la version en anglais)¹²². Le *Whistleblower Officer* se présente donc comme une nouvelle figure de la gestion de conformité («*compliance management*»), à côté du *Data Protection Officer* et du *Compliance Officer*¹²³;
- 4) un suivi diligent des signalements et, le cas échéant, des signalements anonymes¹²⁴. À l'instar du Conseil de l'Europe¹²⁵, l'Union européenne envisage le suivi du signalement comme un outil capable d'instaurer

la confiance dans le système de dénonciation et de réduire la probabilité de signalements ou de divulgations publiques inutiles¹²⁶;

- 5) des informations claires concernant la procédure interne¹²⁷ et externe de signalement¹²⁸ et facilement compréhensibles et accessibles pour les salariés de l'entité mais aussi – compte tenu de l'interprétation large conférée à la notion d'«auteur de signalement» – dans la mesure du possible, pour les personnes qui entrent en contact avec l'entité dans le cadre de leurs activités professionnelles en tant que prestataires de services, distributeurs, fournisseurs et partenaires d'affaires¹²⁹. L'information peut être fournie sur le site Internet de l'entité.

Il appartient à l'entité juridique qui met en place le signalement de sélectionner le type de procédure qui lui semble le plus approprié. La souplesse est de mise : le signalement peut avoir lieu par écrit, par courrier, via une ou des boîtes à suggestions physiques ou via une plateforme en ligne (intranet ou internet), ou oralement, via une permanence téléphonique ou tout autre système de messagerie vocale et même lors d'une rencontre en personne¹³⁰.

Des tiers peuvent être autorisés à recevoir des signalements pour le compte d'entités publiques ou privées, à condition qu'ils offrent les qualités requises¹³¹. La directive sur les lanceurs d'alerte attire notamment l'attention sur le fait que ces derniers doivent offrir des

¹²⁰ Article 5, 12), de la directive sur les lanceurs d'alerte.

¹²¹ Article 9, § 1^{er}, c), de la directive sur les lanceurs d'alerte.

¹²² Considérant n° 56 de la directive sur les lanceurs d'alerte.

¹²³ Sur ce constat, voy. not. A. LACHAPPELLE, « Le lancement d'alerte (*whistleblowing*) à l'ère du règlement général sur la protection des données », in *Le règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie* (C. DE TERWANGNE et K. ROSIER, dir.), Bruxelles, Larquier, 2018, p. 828; J. TERSTEGGE, « EU Watch: Data protection and the new face of privacy compliance », *Business Compliance*, 2013, n° 6, p. 40.

¹²⁴ Article 9, § 1^{er}, d) et e), de la directive sur les lanceurs d'alerte.

¹²⁵ Recommandation CM/Rec (2014)7, Annexe à la Recommandation, Section VI, Principe 20 (signalement interne) et Exposé des motifs, Annexe – Les 29 principes, point 77 (signalement externe).

¹²⁶ Considérants n°s 57 et 67 de la directive sur les lanceurs d'alerte.

¹²⁷ Article 7, § 3, de la directive sur les lanceurs d'alerte.

¹²⁸ Article 9, § 1^{er}, g), de la directive sur les lanceurs d'alerte.

¹²⁹ Considérant n° 59 de la directive sur les lanceurs d'alerte.

¹³⁰ Article 9, § 2 et considérant n° 53 de la directive sur les lanceurs d'alerte.

¹³¹ Article 8, § 5, de la directive sur les lanceurs d'alerte.

garanties appropriées en termes de protection des données¹³². Il peut s'agir de fournisseurs de plateformes de signalement, de conseils externes, d'auditeurs, de représentants syndicaux ou de représentants des travailleurs¹³³.

B. Le signalement externe

36. D'après l'article 11 de la directive, les États membres désignent les autorités compétentes pour recevoir les signalements *externes*, fournir un retour d'informations sur ceux-ci et en assurer le suivi, tout en mettant des ressources suffisantes à la disposition desdites autorités.

La notion d'« autorité compétente » est large. Il peut s'agir d'autorités judiciaires, d'organismes de réglementation ou de surveillance compétents dans les domaines spécifiques concernés, ou d'autorités dotées de compétences plus générales au niveau de l'État central, de services répressifs, d'organismes de lutte contre la corruption ou de médiateurs¹³⁴.

37. La directive précise que les États membres doivent avoir la possibilité de prendre des mesures visant à réduire la charge de travail des autorités compétentes en cas de signalements de violations manifestement mineures, de signalements à répétition

(aucune nouvelle information significative) ou de signalements sur des règles accessoires (règles de forme)¹³⁵. Dans ces cas, les autorités compétentes devraient pouvoir décider que le signalement ne requiert pas d'autres mesures de suivi, en veillant à en informer l'auteur de signalement¹³⁶. Lorsque la violation est manifestement mineure, la directive précise néanmoins que l'auteur de signalement ne perd pas le bénéfice de sa protection et dispose toujours de la possibilité d'emprunter les autres voies de signalement¹³⁷. Les États membres sont par ailleurs libres de permettre aux autorités compétentes de traiter en priorité, en cas d'afflux important de signalements, les signalements de violations graves ou de violations de dispositions essentielles relevant du champ d'application de la directive sans préjudice du délai légal de retour d'informations¹³⁸.

Dans tous les cas, il importe que de telles décisions fassent l'objet d'un contrôle juridictionnel conformément à l'article 47 de la Charte des droits fondamentaux de l'Union européenne¹³⁹.

L'effectivité du système de dénonciation requiert en outre que l'autorité saisie qui n'est pas compétente transmette, dans un délai raisonnable, le signalement à l'autorité compétente en veillant à en informer l'auteur du signalement¹⁴⁰.

¹³² Considérant n° 54 de la directive sur les lanceurs d'alerte.

¹³³ Par exemple, l'entreprise BDO fournit déjà depuis plus d'un an un service de « *whistleblowing* ». Celui-ci comporte, pour un montant mensuel, la création d'une plateforme sécurisée, la sensibilisation du personnel, la gestion des dénonciations et leur communication auprès d'une autorité désignée au sein de l'entreprise ainsi que la définition d'une politique claire en la matière. La brochure « *Whistleblowing as a service* » est disponible sur: [www.bdo.be/getattachment/Nieuws/2019/Eerste-Belgische-meldpunt-voor-bedrijfsfraude/2019_03_Fiche-Whistleblowing-FR_dig-\(2\).pdf.aspx?lang=fr-BE](http://www.bdo.be/getattachment/Nieuws/2019/Eerste-Belgische-meldpunt-voor-bedrijfsfraude/2019_03_Fiche-Whistleblowing-FR_dig-(2).pdf.aspx?lang=fr-BE) (consulté le 28 juin 2019).

¹³⁴ Considérant n° 64 de la directive sur les lanceurs d'alerte.

¹³⁵ Considérant n° 70 de la directive sur les lanceurs d'alerte.

¹³⁶ Article 11, §§ 3 et 4, de la directive sur les lanceurs d'alerte.

¹³⁷ Article 11, § 3, de la directive sur les lanceurs d'alerte. La directive ne prévoyant pas explicitement le maintien de la protection en cas de signalement répétitif, il n'est pas certain qu'elle sera garantie dans une telle hypothèse.

¹³⁸ Article 11, § 5, de la directive sur les lanceurs d'alerte.

¹³⁹ Considérant n° 103 de la directive sur les lanceurs d'alerte.

¹⁴⁰ Article 11, § 6, de la directive sur les lanceurs d'alerte. Voy. aussi l'article 12, § 3, de la directive précitée qui vise l'hypothèse où le signalement est reçu par l'auto-

38. Les procédures de signalement et de suivi des signalements externes comportent des points communs avec les procédures de signalement et de suivi des signalements internes¹⁴¹.

Comme dans le cas du signalement interne, la souplesse est ici de mise concernant les formes que le signalement peut prendre. Celui-ci peut avoir lieu par écrit ou oralement, par téléphone ou tout autre système de messagerie vocale et même lors d'une rencontre en personne¹⁴².

Les qualités attendues des canaux de signalement sont néanmoins plus rigoureuses. Il importe que les canaux de signalement soient « indépendants et autonomes », c'est-à-dire qu'ils soient « conçus, établis et gérés de manière à garantir l'exhaustivité, l'intégrité et la confidentialité des informations et à empêcher l'accès à ces informations aux membres du personnel de l'autorité compétente non autorisés » et qu'ils « permettent le stockage durable d'informations conformément à l'article 18 afin de permettre que des enquêtes complémentaires soient menées »¹⁴³. Il importe par ailleurs que les membres du personnel chargés du traitement des signalements externes reçoivent une formation spécifique aux fins du traitement des signalements¹⁴⁴, y compris en matière de règles de protection des données applicables¹⁴⁵. Ce principe vaut également, *a*

pari, pour les personnes chargées de la réception et/ou du suivi dans le cadre des procédures internes¹⁴⁶. Les membres du personnel chargés du traitement des signalements, de même que ceux qui ont un accès aux informations fournies par l'auteur du signalement, doivent, du reste, respecter le devoir de secret professionnel et de confidentialité lors de la transmission des données tant à l'intérieur qu'à l'extérieur de l'autorité compétente¹⁴⁷.

39. Conformément aux règles européennes de protection des données, l'obligation d'information est ici renforcée¹⁴⁸. Les autorités compétentes sont tenues de publier dans une section de leur site Internet, aisément identifiable et accessible, au moins les huit informations suivantes :

- les conditions de protection des auteurs de signalement ;
- les coordonnées nécessaires pour l'utilisation des canaux de signalement ;
- les procédures applicables au traitement du signalement (demande d'informations complémentaires, retour d'informations, etc.) ;
- le régime de confidentialité applicable aux signalements, en particulier au regard des règles européennes de protection des données pertinentes ;
- la nature du suivi apporté au signalement ;
- les moyens de recours contre les représailles ;
- un communiqué expliquant clairement les conditions dans lesquelles la responsabilité des personnes qui effectuent un signale-

rité compétente, mais via un canal de signalement non approprié ou par un membre du personnel non habilité. Dans ce cas, le membre du personnel en question doit transmettre rapidement le signalement sans modification aux membres du personnel chargés du traitement des signalements, tout en s'abstenant de divulguer toute information qui permettrait d'identifier l'auteur de signalement ou la personne concernée.

¹⁴¹ Article 11, § 2, de la directive sur les lanceurs d'alerte.

¹⁴² Article 12, § 2, de la directive sur les lanceurs d'alerte.

¹⁴³ Article 12, § 1^{er}, de la directive sur les lanceurs d'alerte.

¹⁴⁴ Article 12, § 5, de la directive sur les lanceurs d'alerte.

¹⁴⁵ Considérant n° 74 de la directive sur les lanceurs d'alerte.

¹⁴⁶ En ce sens, le considérant n° 54 de la directive sur les lanceurs d'alerte mentionne que les tiers chargés de recevoir des signalements pour le compte d'une entité privée ou publique doivent offrir des garanties appropriées en termes de protection des données.

¹⁴⁷ Considérant n° 77 de la directive sur les lanceurs d'alerte.

¹⁴⁸ Considérant n° 75 de la directive sur les lanceurs d'alerte. Voy. aussi l'article 13 de la directive précitée.

ment auprès de l'autorité compétente ne sera pas engagée du fait d'une violation de la confidentialité;

- les coordonnées de l'autorité administrative indépendante unique, le cas échéant¹⁴⁹.

C. La révélation publique

40. À la différence de la proposition de directive du 23 avril 2018, la directive sur les lanceurs d'alerte contient une disposition expresse à propos de la divulgation publique: l'article 15. L'absence d'une disposition expresse dans la proposition de directive avait effectivement été critiquée par le secteur associatif. La protection contre les représailles doit en principe être garantie quelle que soit la voie de signalement choisie, en ce compris lorsqu'elle consiste dans la dénonciation publique¹⁵⁰.

La directive souligne le rôle capital joué par les lanceurs d'alerte qui s'adressent en tant que sources à des journalistes d'investigation en ce qu'ils permettent à ces derniers de jouer leur rôle de sentinelle dans une société démocratique¹⁵¹.

41. Avec les scandales fiscaux de ces dernières années, l'*International Consortium of Investigative Journalists* (ICIJ) a démontré qu'il représentait un destinataire de confiance pour les lanceurs d'alerte. L'ICIJ est une organisation sans but lucratif basée à Washington D.C. aux États-Unis. Il s'agit d'un réseau global de journalistes et organisations de médias qui travaillent ensemble afin d'enquêter sur des affaires de grande ampleur qui ont une dimension transnationale¹⁵².

Les lanceurs d'alerte peuvent également compter, en Belgique, sur la plateforme de dénonciation «www.sourcesure.eu» qui permet l'envoi anonyme d'informations confidentielles vers le média francophone de son choix¹⁵³. Participent au projet *Le Monde, France TV Info, La Libre, L'Observateur, RTBF.be, l'avenir.net, Le Soir, RTS*¹⁵⁴. Des journalistes et des citoyens ont par ailleurs créé, en janvier 2019, une a.s.b.l., dénommée «*Xpress*», «en vue de soutenir les journalistes, lanceurs d'alerte et leurs sources faisant l'objet d'intimidations ou d'attaques»¹⁵⁵. Cette a.s.b.l. complète l'action de l'Association des journalistes professionnels (AJP).

42. La révélation aux médias ne s'épuise toutefois pas dans la procédure établie par la directive. Cette dernière ne s'applique pas aux «cas dans lesquels une personne divulgue directement des informations à la presse selon les dispositions nationales spécifiques établissant un système de protection relatif à la liberté d'expression et d'information»¹⁵⁶.

La directive n'harmonise donc pas la question de la divulgation aux médias, mais se contente d'en reconnaître la légitimité.

III. LA PROTECTION DU LANCEUR D'ALERTE

43. La directive sur les lanceurs d'alerte établit des normes minimales assurant un niveau élevé de protection des auteurs de signalement, et le cas échéant des facilitateurs, des tiers en lien avec les auteurs de signale-

¹⁴⁹ Article 13 de la directive sur les lanceurs d'alerte.

¹⁵⁰ Considérant n° 45 de la directive sur les lanceurs d'alerte.

¹⁵¹ Considérant n° 46 de la directive sur les lanceurs d'alerte.

¹⁵² Cinq journalistes belges sont membres de l'ICIJ: Kristof Clerix (*Knack*), Alain Lallemand (*Le Soir*),

Lars Bové (*De Tijd*), Xavier Counasse (*Le Soir*) et Joël Matriche (*Le Soir*).

¹⁵³ Consulté le 31 décembre 2019.

¹⁵⁴ Cette plateforme alimentait par exemple les dossiers traités dans le cadre de l'émission «Question à la Une» sur la chaîne de télévision publique *La Une*.

¹⁵⁵ «À propos», disponible sur <https://xpress.be> (consulté le 10 février 2019).

¹⁵⁶ Article 15, § 2, de la directive sur les lanceurs d'alerte.

ment et des entités juridiques avec lesquelles les auteurs de signalement sont en lien dans un contexte professionnel (A). La protection conférée par la directive n'est pas absolue : elle est soumise à deux conditions issues de notre tradition juridique (B).

Même si le présent article cible la protection du lanceur d'alerte, il y a lieu de noter que l'approche européenne du lancement d'alerte se caractérise par une attention soutenue à la protection des « personnes concernées », c'est-à-dire les personnes, physiques ou morales, mentionnées dans le signalement ou la divulgation en tant que personnes auxquelles la violation est attribuée ou auxquelles elle est associée¹⁵⁷.

A. Les conditions de protection

44. Les auteurs de signalement bénéficient de la protection prévue par la directive pour autant qu'ils aient été de bonne foi au moment du signalement (1) et qu'ils aient respecté la procédure de signalement prévue par la directive (2).

Que la dénonciation soit anonyme ne devrait, par contre, pas faire obstacle à la protection prévue par la directive. Prenant acte du constat selon lequel les signalements anonymes se sont produits, se produisent et se produiront encore, la directive sur les lanceurs d'alerte laisse les États membres libres de décider s'ils acceptent ou non les signalements anonymes d'infractions relevant du champ d'application de la directive¹⁵⁸. En toute hypothèse, les personnes qui font un tel signalement dans le cadre du champ d'application de la directive et dans le respect des conditions prévues devraient néanmoins bénéficier de la protection établie par la directive si leur identité est

révélee et s'ils font l'objet de représailles¹⁵⁹. En outre, la directive rappelle que le droit de l'Union contient lui-même des dispositions qui obligent à mettre en place un dispositif de signalement anonyme¹⁶⁰.

1. La croyance raisonnable du lanceur d'alerte

45. S'il est une constante au cours de l'histoire, c'est que le dénonciateur qui agit de bonne foi est le seul dénonciateur à mériter une protection. La directive sur les lanceurs d'alerte ne déroge pas à la règle. Pressé par la société civile, spécialement l'ONG *Transparency International – France*, le législateur européen a cependant troqué le critère formel de la « bonne foi » pour celui plus objectif de « croyance raisonnable »¹⁶¹. Une telle conception de la « bonne foi » coïncide également avec celle défendue dans la Recommandation CM/Rec (2014)7¹⁶² et dans le *UK Public Interest Disclosure Act – PIDA 1998*¹⁶³ dont la directive s'inspire.

D'après l'article 6 de la directive, les auteurs de signalement bénéficient ainsi de la protection prévue par la directive s'ils avaient des *motifs raisonnables* de croire que les informations communiquées étaient véridiques au moment du signalement *et que ces informations*

¹⁵⁹ Article 6, § 3, de la directive sur les lanceurs d'alerte. Voy. aussi le considérant n° 34 de la directive précitée.

¹⁶⁰ Voy. par exemple l'article 61, § 3, de la Quatrième directive anti-blanchiment à propos du signalement interne.

¹⁶¹ L'expression « bonne foi » n'apparaît ainsi qu'à deux reprises dans les considérants de la version francophone de la directive (considérants n°s 9 et 32) tandis que l'expression « *good faith* » a totalement disparu de la version anglophone de la directive, remplacée, le cas échéant, par l'expression « *honest mistake* ».

¹⁶² Recommandation CM/Rec (2014)7, Exposé des motifs, Annexe – Les 29 principes, point 85.

¹⁶³ Section 43B of the ERA 1996. Le texte du PIDA peut être consulté sur le site Internet du gouvernement britannique : www.legislation.gov.uk/ukpga/1998/23/contents (consulté le 4 juillet 2019).

¹⁵⁷ Article 5, 10), de la directive sur les lanceurs d'alerte.

¹⁵⁸ Article 6, § 2, de la directive sur les lanceurs d'alerte. Voy. aussi le considérant n° 34 de la directive précitée.

entraient dans le champ de la directive¹⁶⁴. Ce faisant, le lanceur d'alerte ne devrait pas perdre le bénéfice de la protection au seul motif que le signalement effectué de bonne foi s'est avéré inexact ou infondé. Dans le même ordre d'idées, le lanceur d'alerte devrait bénéficier de la protection établie en vertu de la directive s'il avait des motifs raisonnables de croire qu'il entrerait dans le champ d'application de la directive¹⁶⁵.

46. Alors que la Cour européenne des droits de l'homme considère qu'«un acte motivé par un grief ou une animosité personnels ou encore par la perspective d'un avantage personnel, notamment un gain pécuniaire, ne justifie pas un niveau de protection particulièrement élevé»¹⁶⁶, la directive précise que «les motifs amenant les auteurs de signalement à effectuer un signalement devraient être sans importance pour décider s'ils doivent recevoir une protection»¹⁶⁷. Une telle clause a été proposée

par le Parlement européen en novembre 2018 et maintenue dans le texte de la directive¹⁶⁸. Des voix de plus en plus nombreuses s'élèvent effectivement pour affirmer que ce qui importe lors de l'appréciation de la protection du lanceur d'alerte, ce n'est pas sa motivation, mais bien «la pertinence et l'intérêt de l'information portée à la connaissance de l'organisation concernée, des autorités compétentes ou du public»¹⁶⁹.

En revanche, il importe de continuer de dissuader les signalements malveillants et de préserver la crédibilité du système de dénonciation¹⁷⁰. La directive énonce ainsi que les États membres doivent prévoir «des sanctions effectives, proportionnées et dissuasives applicables aux auteurs de signalement lorsqu'il est établi qu'ils ont sciemment signalé ou divulgué publiquement de fausses informations. Les États membres prévoient également des mesures d'indemnisation pour les dommages

¹⁶⁴ Considérant n° 32 de la directive sur les lanceurs d'alerte.

¹⁶⁵ Cette dernière précision est particulièrement importante dans le domaine fiscal. Vu la complexité du droit fiscal, il peut être particulièrement malaisé pour une personne non initiée, et même parfois pour un fiscaliste, de dire si un comportement viole ou non une disposition fiscale.

¹⁶⁶ Voy. Cour eur. D.H. (GC), arrêt *Guja c. Moldavie*, 12 février 2008, § 77; Cour eur. D.H. (5^e sect.), arrêt *Heinisch c. Allemagne*, 21 juillet 2011, § 69; Cour eur. D.H. (3^e sect.), arrêt *Bucur et Toma c. Roumanie*, 8 janvier 2013, § 93; Cour eur. D.H. (2^e sect.), arrêt *Görmüs et autres c. Turquie*, 19 janvier 2016, § 50; Comm. eur. D.H., déc. *Haseldine c. Royaume-Uni*, 13 mai 1992. Le critère de la motivation est central dans l'appréciation de la Cour puisqu'il peut conduire à dénier le bénéfice du statut de «lanceur d'alerte». Pour une illustration, voy. not. Cour eur. D.H. (5^e sect.), arrêt *Rubins c. Lettonie*, 13 janvier 2015, § 87; Cour eur. D.H. (5^e sect.), arrêt *Langner c. Allemagne*, 17 septembre 2015, § 46; Cour eur. D.H. (5^e sect.), décision *Bathelier c. France*, 12 octobre 2010, p. 7; Cour eur. D.H. (5^e sect.), déc. *Balenović c. Croatie*, 30 septembre 2010, p. 28.

¹⁶⁷ Considérant n° 32 de la directive sur les lanceurs d'alerte.

¹⁶⁸ Considérant n° 64bis du projet de résolution législative du Parlement européen du 26 novembre 2018. En ce sens, voy. aussi la résolution du Parlement européen sur les mesures légitimes visant à protéger les lanceurs d'alerte qui divulguent, au nom de l'intérêt public, des informations confidentielles d'entreprises et d'organismes publics (2016/2224(INI)), 24 octobre 2017, point 47.

¹⁶⁹ Considérant n° 64bis du projet de résolution législative du Parlement européen du 26 novembre 2018. En faveur d'une telle approche, voy. not. Rapport «Promotion et protection du droit à la liberté d'opinion et d'expression» du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression (David Kaye) pour l'année 2015, note du Secrétaire général, A/70/361, Assemblée générale des Nations Unies, 70^e sess., 8 septembre 2015, p. 16; F. CHALTIEL TERRAL, *Les lanceurs d'alerte*, Paris, Dalloz, 2018, p. 49. *Contra* voy. not. V. BOUHIER, «Lanceurs d'alerte», *J.D.E.*, n° 243, 2017, p. 349 (l'auteur estime *a contrario* que le caractère désintéressé, la motivation du lanceur d'alerte, doit être pris en compte).

¹⁷⁰ Considérant n° 102 de la directive sur les lanceurs d'alerte.

résultant de ces signalements ou divulgations publiques conformément au droit national»¹⁷¹.

La dénonciation mensongère est déjà sanctionnée en droit belge au travers des délits de calomnie et diffamation (article 443 du Code pénal), de dénonciation calomnieuse (article 445 du Code pénal) et d'injure-délict (article 448 du Code pénal).

2. Le respect de la procédure de signalement

47. Dans sa première mouture, la directive sur les lanceurs d'alerte prescrivait le respect d'une procédure *échelonnée* («*tiered-level reporting procedure*»). Le bien-fondé d'une telle procédure avait pourtant donné lieu à des réponses pour le moins contrastées de la part des parties prenantes interrogées dans le cadre des consultations publiques¹⁷². Cette exigence avait même suscité une levée de boucliers de la part des organisations de médias et des organisations non gouvernementales¹⁷³.

Emboitant le pas au Comité des ministres du Conseil de l'Europe¹⁷⁴, le législateur européen est venu corriger le tir, supprimant toute idée de «palier» entre les trois voies de signalement. Désormais, l'auteur du signalement a le droit de «choisir le canal de signalement le plus approprié en fonction des circonstances particulières de l'affaire»¹⁷⁵. Il n'empêche qu'il est tenu, s'il souhaite bénéficier de la protection prévue par la directive, d'effectuer son signalement – interne, externe ou public – conformément à la procédure établie par la directive¹⁷⁶.

48. En pratique, le signalement interne continue de demeurer la voie la plus habituelle et la plus sûre. En règle toujours possible¹⁷⁷, c'est la voie *a priori* la plus à même de produire rapidement une réaction. Le respect de la procédure échelonnée peut du reste contribuer à démontrer la bonne foi du lanceur d'alerte¹⁷⁸. Tant l'employeur que le lanceur d'alerte tirent un avantage de la mise en place d'une procédure interne. L'employeur échappe au risque d'une atteinte à sa réputation¹⁷⁹; le lanceur d'alerte limite le risque de représailles dès lors qu'on ne peut lui reprocher d'avoir violé une règle de confidentialité¹⁸⁰.

¹⁷¹ Article 23, § 2, de la directive sur les lanceurs d'alerte. Ces sanctions peuvent revêtir une forme pénale, civile ou administrative (considérant n° 102 de la directive précitée).

¹⁷² Proposition de directive du 23 avril 2018, Annexe 2, pp. 68-69.

¹⁷³ Voy. not. Q. VAN ENIS, *Robust whistleblower protection is a crucial challenge for the European democracy*, European Federation of Journalists, 2018, disponible sur <https://europeanjournalists.org> (consulté le 3 novembre 2019); XNET – EDRI (European Digital Rights), «Analysis and recommendations for key modifications in the draft EC Directive for the Protection of Whistleblowers», 12 juin 2018, disponible sur <https://xnet-x.net/en/recommendations-modifications-draft-ec-directive-protection-whistle-blowers/> (consulté le 25 juin 2018); T. DEVINE, «Response to proposed EU Directive on protecting whistleblowers», WIN (Whistleblowing International Network) EU MEMORANDUM 1: 19 June 2018, disponible sur <https://whistlenetwork.files.wordpress.com/2018/10/win-memo-1-legal-assessment-of-eu-proposed-wb-directive-19-06-18.pdf> (consulté le 20 décembre 2018).

¹⁷⁴ Considérant n° 61 du projet de résolution législative du Parlement européen du 26 novembre 2018.

¹⁷⁵ Considérant n° 33 de la directive sur les lanceurs d'alerte.

¹⁷⁶ Article 7 (signalement interne), article 10 (signalement externe) et article 15 (divulcation publique) de la directive sur les lanceurs d'alerte.

¹⁷⁷ Article 7, § 1^{er}, de la directive sur les lanceurs d'alerte.

¹⁷⁸ En ce sens, voy. Cour eur. D.H., arrêt *Heinisch*, précité, § 86; Cour eur. D.H., arrêt *Bucur*, précité, § 117.

¹⁷⁹ En ce sens, voy. not. A. HÜMEYRA ÇAKIR, M. BETÜL GÖKÇE et L. BIN, «Whistleblowing: Ethical or not», *Delft University of Technology Project Management EPA 1412*, p. 3, disponible sur www.academia.edu (consulté le 27 mars 2018).

¹⁸⁰ En ce sens, voy. V. JUNOD, «Lancer l'alerte: quoi de neuf depuis Guja? (Cour eur. dr. h., *Bucur et Toma c. Roumanie*, 8 janvier 2013)», *Rev. trim. dr. h.*, n° 98, 2014, p. 476.

À la lumière de ces considérations, la directive invite les États membres à encourager « le signalement par le biais de canaux de signalement interne avant un signalement par le biais de canaux de signalement externe, lorsqu'il est possible de remédier efficacement à la violation en interne et que l'auteur de signalement estime qu'il n'y a pas de risque de représailles »¹⁸¹. Ce principe vaut que les canaux de signalement aient été mis en place en vertu du droit, européen ou national, ou non¹⁸².

49. Si la directive fait l'éloge du signalement interne, elle reconnaît dans le même temps qu'une telle voie n'est pas toujours envisageable. Il arrive en effet qu'aucun canal de signalement interne n'ait été prévu ou que les canaux internes prévus s'avèrent en pratique déficients ou qu'on ne puisse pas raisonnablement s'attendre à ce que les canaux internes fonctionnent correctement. Il arrive aussi que le droit de l'Union ou le droit national impose lui-même aux auteurs de signalement de s'adresser directement aux autorités compétentes. La directive précise, à ce propos, que la protection établie s'applique aussi « lorsque le droit de l'Union ou le droit national exige que les auteurs de signalement effectuent un signalement auprès des autorités nationales compétentes, par exemple parce que cela relève de leurs responsabilités et devoirs professionnels ou parce que la violation constitue une infraction pénale »¹⁸³. C'est le cas lorsqu'un fonctionnaire public prend connaissance d'un crime ou d'un délit dans le cadre de l'exercice de ses fonctions ou encore lorsqu'un Compliance Officer prend connaissance d'infractions à la législation financière dans son entreprise.

50. Lorsque le signalement est public, la directive conditionne la protection au respect d'exigences supplémentaires. L'auteur de signalement bénéficie de la protection établie par la directive dans deux hypothèses distinctes¹⁸⁴:

- soit que l'auteur de signalement a signalé les faits en interne et à l'externe, soit qu'il a directement dénoncé les faits via les canaux externes, dans les deux cas sans qu'une suite appropriée¹⁸⁵ ne soit donnée dans un délai raisonnable¹⁸⁶;
- soit que l'auteur de signalement avait des motifs raisonnables de croire que l'infraction pouvait représenter un danger imminent ou manifeste pour l'intérêt public, tel qu'une situation d'urgence ou un risque de préjudice irréversible, notamment une atteinte à l'intégrité physique¹⁸⁷, ou que le signalement externe comportait un risque de représailles ou d'absence de suivi diligent¹⁸⁸.

¹⁸⁴ Article 15, § 1^{er}, de la directive sur les lanceurs d'alerte.

¹⁸⁵ Le considérant n° 79 de la directive sur les lanceurs d'alerte précise que le caractère « approprié » du suivi devrait être évalué au cas par cas à l'aune de critères objectifs « liés à l'obligation incombant aux autorités compétentes d'évaluer l'exactitude des allégations et de mettre un terme à toute violation éventuelle du droit de l'Union ». Ainsi, « une décision par laquelle les autorités considèrent qu'une violation était clairement mineure et ne requérait pas d'autre suivi que la clôture de la procédure, pourrait constituer un suivi approprié au sens de la [...] directive (considérant n° 79 de la directive sur les lanceurs d'alerte).

¹⁸⁶ En cas de signalement interne, un suivi doit être fourni au lanceur d'alerte dans un délai n'excédant pas trois mois à compter de l'accusé de réception du signalement ou, si aucun accusé de réception n'a été transmis, à compter de l'expiration de la période de sept jours suivant le signalement (article 9, § 1^{er}, f), de la directive sur les lanceurs d'alerte). En cas de signalement externe, un suivi doit être fourni à l'informateur dans un délai n'excédant pas trois mois ou six mois dans des cas dûment justifiés (article 11, § 2, d), de la directive sur les lanceurs d'alerte).

¹⁸⁷ Considérant n° 80 de la directive sur les lanceurs d'alerte.

¹⁸⁸ Considérant n° 81 de la directive sur les lanceurs d'alerte.

¹⁸¹ Article 7, § 2, de la directive sur les lanceurs d'alerte.

¹⁸² Considérant n° 47 de la directive sur les lanceurs d'alerte.

¹⁸³ Considérant n° 62 de la directive sur les lanceurs d'alerte.

En tout état de cause, la dénonciation publique surgit en tant que soupape de sécurité en vue de dénoncer un problème systémique qui implique à la fois une organisation, privée ou publique, et une émanation de l'autorité publique¹⁸⁹.

B. Les principes de protection

51. Si la confidentialité de l'identité des lanceurs d'alerte fait, de prime abord, office de rempart contre les représailles (1)¹⁹⁰, c'est dans le principe d'interdiction des représailles (2) et dans l'immunité conférée en cas de litige (3) que réside tout l'intérêt de la protection du lanceur d'alerte. Le principe d'interdiction étant insuffisant en lui-même pour protéger le lanceur d'alerte, il convient néanmoins de lui donner accès à des voies de recours appropriées et à une indemnisation, le cas échéant (4).

Au-delà de ces mesures, une chose est sûre c'est que la transposition de la directive « ne devrait, en aucun cas, constituer un motif pour abaisser le niveau de protection déjà accordé aux auteurs de signalement par le droit national dans les domaines auxquels elle s'applique »¹⁹¹ (clause de non-régression ou de *stand-still*). Les États membres peuvent en outre adopter des dispositions plus favorables à l'égard du lanceur d'alerte, sans préjudice des droits de la personne concernée (clause de traitement plus favorable)¹⁹².

1. L'exigence de confidentialité

52. La directive énonce que l'identité de l'auteur du signalement ne peut pas être divulguée « sans le consentement exprès de celui-ci à toute personne autre que les membres du personnel autorisés compétents pour recevoir des signalements ou pour en assurer le suivi »¹⁹³. Les membres du personnel des entités tenues de mettre en place des dispositifs d'alerte interne, de même que ceux des autorités externes, doivent par ailleurs veiller à ce que l'identité de chaque personne concernée et des tiers mentionnés dans le signalement, par exemple des témoins ou des collègues, soit protégée à tous les stades de la procédure¹⁹⁴.

La divulgation doit, de plus, procéder d'une « obligation nécessaire et proportionnée imposée par le droit de l'Union ou le droit national dans le contexte d'enquêtes d'autorités nationales ou de procédures judiciaires »¹⁹⁵. L'obligation de confidentialité ne peut en effet faire obstacle à l'application des droits de la défense de la personne concernée. En toute hypothèse, la divulgation de l'identité de l'informateur et de toute autre information permettant de déduire son identité est soumise à des mesures de sauvegarde appropriées en vertu des règles applicables¹⁹⁶.

¹⁸⁹ En ce sens, voy. « Lancement d'alerte. Bilan de l'année et perspectives » (propos de V. ROZIERE), in *5^e Salon du livre de lanceuses et lanceurs d'alerte: Des livres et l'alerte*, organisé par le Presse Papier et un collectif de bénévoles, Montreuil, 22, 23 et 24 novembre 2019.

¹⁹⁰ Le considérant n° 82 de la directive sur les lanceurs d'alerte souligne que la confidentialité est une mesure *ex ante* essentielle pour éviter les représailles.

¹⁹¹ Considérant n° 104 de la directive sur les lanceurs d'alerte. La clause de non-régression figure concrètement à l'article 25, § 2, de la directive précitée.

¹⁹² Article 2, § 2, et considérant n° 104 de la directive sur les lanceurs d'alerte. La clause de traitement plus favorable figure concrètement à l'article 25, § 1^{er}, de la directive précitée.

¹⁹³ Article 16, § 1^{er}, de la directive sur les lanceurs d'alerte.

¹⁹⁴ Considérant n° 76 de la directive sur les lanceurs d'alerte. S'agissant du signalement interne, l'accent n'est mis que sur l'identité de l'auteur du signalement (considéranants n°s 53 et 54 de la directive sur les lanceurs d'alerte).

¹⁹⁵ Article 16, § 2, de la directive sur les lanceurs d'alerte. En vue de conférer un effet utile à la directive « secrets d'affaires », la directive sur les lanceurs d'alerte précise encore que les autorités compétentes « qui reçoivent des informations sur des violations qui comportent des secrets d'affaires n'utilisent pas ou ne divulguent pas ces secrets d'affaires à des fins allant au-delà de ce qui est nécessaire pour assurer un suivi approprié » (article 16, § 4, et considérant n° 98 de la directive sur les lanceurs d'alerte).

¹⁹⁶ Article 16, § 3, de la directive sur les lanceurs d'alerte.

53. Les règles européennes relatives à la protection des données doivent, de surcroît, être respectées dès l'instant où le fonctionnement d'un dispositif d'alerte repose sur la collecte et l'exploitation de données à caractère personnel¹⁹⁷. Ceci est presque toujours le cas dans la mesure où la gestion des signalements passe, à l'ère numérique, quasi nécessairement par un outil informatique de traitement automatisé¹⁹⁸. L'article 18 de la directive fixe encore les règles applicables à l'archivage des signalements, et spécialement les règles selon lesquelles un signalement oral ou un compte-rendu de la rencontre peut être consigné par les entités juridiques (signalement interne) et les autorités compétentes (signalement externe). Le respect du cadre légal dans la conservation des signalements est important puisque ces derniers devraient pouvoir être utilisés comme éléments de preuve dans le cadre d'actions juridiques, le cas échéant¹⁹⁹.

2. L'interdiction de représailles

54. La directive sur les lanceurs d'alerte établit le principe d'interdiction des représailles à l'égard des lanceurs d'alerte et, le cas échéant, des tiers en lien avec les auteurs de signalement et les entités juridiques avec lesquelles les auteurs de signalement sont en lien dans un contexte professionnel²⁰⁰.

Au-delà de sa portée symbolique, le fait de consacrer légalement le principe d'interdiction des représailles a un effet dissuasif important²⁰¹ qui est renforcé par la mise en cause de la responsabilité personnelle de l'auteur des représailles et la mise en place de sanctions effectives, proportionnées et dissuasives en cas de non-respect²⁰².

55. L'effectivité du droit de l'Union exige que la notion de «représailles» soit entendue largement. Il importe que l'auteur de signalement soit protégé contre «tout acte ou omission intervenant dans le contexte professionnel et causant un préjudice aux auteurs de signalement»²⁰³. La notion de «représailles», qui exprime le lien étroit de cause à effet entre le signalement et le traitement défavorable subi corrélativement par l'auteur de signalement, est alors définie comme «tout acte ou omission direct ou indirect qui intervient dans un contexte professionnel, [...] suscité par un signalement interne ou externe ou une divulgation publique, et qui cause ou peut causer un préjudice injustifié à l'auteur de signalement»²⁰⁴. La directive couvre ainsi tant les mesures qui mettent fin à la relation professionnelle (mise à pied, licenciement, résiliation anticipée, ...) que les mesures disciplinaires ou encore les mesures qui visent à disqualifier l'informateur sur le plan professionnel (refus de promotion, transfert de fonction, mise sur liste noire, ...), mais aussi privé (orientation vers une prise en charge psychiatrique ou médicale)²⁰⁵.

¹⁹⁷ Proposition de directive du 23 avril 2018, article 18 et considérants n°s 55 et 58.

¹⁹⁸ Sur les exigences tirées du RGPD applicables au *whistleblowing*, voy. spéc. A. LACHAPPELLE, «Le lancement d'alerte (*whistleblowing*) à l'ère du règlement général sur la protection des données», in *Le Règlement général sur la protection des données (RGPD / GDPR). Analyse approfondie* (C. DE TERWANGNE et K. ROSIER, dir.), 1^{re} éd., coll. du CRIDS, Bruxelles, Larcier, 2018, pp. 797-836.

¹⁹⁹ Considérant n° 86 de la directive sur les lanceurs d'alerte.

²⁰⁰ Article 19 de la directive sur les lanceurs d'alerte, lu à la lumière de son article 4, § 4.

²⁰¹ Considérant n° 88 de la directive sur les lanceurs d'alerte.

²⁰² Article 23, § 1^{er}, de la directive sur les lanceurs d'alerte. Ces sanctions peuvent revêtir une forme pénale, civile ou administrative (considérant n° 102 de la directive sur les lanceurs d'alerte).

²⁰³ Considérant n° 44 de la directive sur les lanceurs d'alerte.

²⁰⁴ Article 5, 11), de la directive sur les lanceurs d'alerte.

²⁰⁵ Article 19 de la directive sur les lanceurs d'alerte. Notons que cette liste, non exhaustive, est plus détaillée que celle figurant dans la proposition de

La directive n'interdit pas seulement les représailles commises *par l'employeur* à l'encontre des lanceurs d'alerte. Elle interdit largement « toute forme de représailles, directes ou indirectes, qui seraient encouragées ou tolérées par leur employeur, leur client, ou le destinataire de leurs services et par des personnes travaillant pour ou au nom de ces derniers, y compris les collègues et les dirigeants de la même organisation ou d'organisations avec lesquelles l'auteur de signalement est en contact dans le cadre de ses activités professionnelles »²⁰⁶. Dans une culture où ceux qui dénoncent et prennent la parole sont encore largement désavoués, l'employeur n'est effectivement pas le seul individu dont le lanceur d'alerte doit craindre des représailles. Le lanceur d'alerte peut craindre de la part de collègues de travail des mesures de rétorsion, parfois diffuses et insidieuses, pour lesquelles une action ferme de la part de l'employeur est requise.

56. À la différence de la proposition du 23 avril 2018, la directive dédie spécialement un article, l'article 20, aux mesures de soutien dont doit bénéficier l'auteur de signalement.

Les mesures de soutien peuvent notamment prendre la forme de conseils complets et indépendants sur les procédures et recours disponibles en matière de protection contre les représailles, ainsi que sur les droits de la personne concernée, d'une assistance efficace de la part des autorités compétentes ainsi que d'une assistance juridique dans le cadre des procédures judiciaires²⁰⁷. Comme dans la Recommandation CM/Rec (2014)7, l'accès à des conseils avisés est envisagé comme une façon de garantir un traitement des signalements en temps opportun et selon les voies les

plus appropriées²⁰⁸. Il est aussi gage de sécurité juridique pour l'auteur de signalement²⁰⁹.

Les États membres peuvent aussi prévoir une assistance financière et un soutien, notamment psychologique, pour les lanceurs d'alerte dans le cadre de procédures judiciaires²¹⁰. Cette assistance financière ne devrait pas prendre la forme d'une récompense dès l'instant où les auteurs de signalement qui agissent dans la perspective d'une récompense sont en règle exclus du champ d'application de la directive. L'objectif de cette mesure est de garantir le droit à la protection des lanceurs d'alerte qui ont de sérieux besoins financiers et ne pourraient, à tout le moins au début de la procédure, assumer les frais juridiques²¹¹ en application de la directive (UE) 2016/1919 du Parlement européen et du Conseil²¹².

57. Les mesures de soutien peuvent être confiées à un centre d'information ou à une autorité administrative indépendante unique²¹³.

La Belgique s'est déjà dotée d'un point de contact compétent pour recevoir les dénonciations de lanceurs d'alerte conformément à

²⁰⁸ Considérant n° 89 de la directive sur les lanceurs d'alerte.

²⁰⁹ Dans certains cadres nationaux, la certification pourrait représenter un outil capable de donner au lanceur d'alerte les garanties qu'il satisfait aux conditions de la directive (considérant n° 90 de la directive sur les lanceurs d'alerte).

²¹⁰ Article 20, § 2, de la directive sur les lanceurs d'alerte. En novembre 2018, le Parlement européen recommandait, en outre, de prévoir un soutien financier en cas de perte temporaire de revenus (article 15, § 8, du projet de résolution législative du 26 novembre 2018).

²¹¹ Considérant n° 99 de la directive sur les lanceurs d'alerte.

²¹² Directive (UE) 2016/1919 du Parlement européen et du Conseil du 26 octobre 2016 concernant l'aide juridictionnelle pour les suspects et les personnes poursuivies dans le cadre des procédures pénales et pour les personnes dont la remise est demandée dans le cadre des procédures relatives au mandat d'arrêt européen, *J.O.U.E.*, L 297, 4 novembre 2016.

²¹³ Article 20, § 3, de la directive sur les lanceurs d'alerte.

directive initiale adoptée le 23 avril 2018 par la Commission européenne.

²⁰⁶ Considérant n° 87 de la directive sur les lanceurs d'alerte.

²⁰⁷ Article 20, § 1^{er}, de la directive sur les lanceurs d'alerte.

la directive sur les lanceurs d'alerte et pour les orienter, ensuite, vers les autorités compétentes en vue d'une protection²¹⁴. Il s'agit de l'«Institut fédéral pour la protection et la promotion des droits humains» créé par la loi du 12 mai 2019 portant création d'un Institut fédéral pour la protection et la promotion des droits humains²¹⁵. L'article 6, paragraphe 2, 2°, de la loi du 12 mai 2019 portant création d'un Institut fédéral pour la protection et la promotion des droits humains énonce que l'Institut «entend toute personne, obtient toute information et tout document nécessaire à l'appréciation de situations relevant de sa compétence». Lors des travaux parlementaires, il a été recommandé de mentionner expressément que «toute personne» incluait notamment les lanceurs d'alerte, mais la formulation a été considérée comme suffisamment claire et englobante²¹⁶. Reste à voir comment les missions confiées à cet institut s'articuleront avec celles dévolues à l'Ombudsman fédéral dans le cadre 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 personnel²¹⁷, modifiée par une loi du 8 mai 2019²¹⁸.

À l'échelle européenne, le Parlement européen a invité la Commission, dans une résolution de 2017, à mettre en place un organe chargé de coordonner les actions des États membres, en particulier dans les situations transfrontières. Cet organe doit disposer d'un budget suffisant lui permettant d'enquêter sur la crédibilité des signalements, d'orienter les lanceurs d'alerte et de publier des recommandations contraignantes²¹⁹. The *Network of European Integrity and Whistleblowing Authorities* (NEIWA) a vu le jour le 24 mai 2019 à La Haye. Ce réseau vise à permettre l'échange de connaissances et d'expériences entre autorités nationales, spécialement dans le contexte de la transposition de la directive sur les lanceurs d'alerte²²⁰. Pour la Belgique est actuellement membre de ce réseau l'Ombudsman fédéral. Celui-ci exerce un rôle de point de contact sur pied de la loi du 15 septembre 2013 précitée.

3. L'exonération limitée de responsabilité

58. Le cœur de la protection de l'auteur de signalement réside dans l'article 21, paragraphe 2, de la directive sur les lanceurs d'alerte qui énonce que les personnes qui font un signalement ou une divulgation publique conformément à la directive :

«ne sont pas considérées comme ayant enfreint une restriction à la divulgation d'informations et n'encourent aucune responsabilité d'aucune sorte concernant ce

²¹⁴ Proposition de loi portant création d'un Institut fédéral pour la protection et la promotion des droits de l'homme, *Doc.*, Ch., 2018-2019, n° 54-3670/001, p. 19.

²¹⁵ Loi du 12 mai 2019 portant création d'un Institut fédéral pour la protection et la promotion des droits humains, *M.B.*, 21 juin 2019.

²¹⁶ Proposition de loi portant création d'un Institut fédéral pour la protection et la promotion des droits de l'homme, Rapport de la première lecture fait au nom de la Commission des relations extérieures, *Doc.*, Ch., 2018-2019, n° 54-3670/005, p. 17.

²¹⁷ 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, *M.B.*, 4 octobre 2013. Pour un commentaire de la loi du 15 septembre 2013, voy. spéc. G. VANDE WALLE, G. VYNCKIER et P. DE BAETS, «Melden en klokkenluiden : weten waar de klepel hangt», *Orde van de dag*, liv. 72, 2015, pp. 3-93.

²¹⁸ Loi du 8 mai 2019 modifiant 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, *M.B.*, 17 juin 2019.

²¹⁹ Résolution du Parlement européen sur les mesures légitimes visant à protéger les lanceurs d'alerte qui divulguent, au nom de l'intérêt public, des informations confidentielles d'entreprises et d'organismes publics (2016/2224(INI)), P8_TA-PROV(2017)0402, 24 octobre 2017, § 61.

²²⁰ Home < Nieuws < Europees netwerk over integriteit en klokkenluiden, disponible sur <https://huisvoorklokkenluiders.nl> (consulté le 22 juin 2019).

signalement ou cette divulgation publique pour autant qu'elles aient eu des motifs raisonnables de croire que le signalement ou la divulgation publique de telles informations était nécessaire pour révéler une violation en vertu de la [...] directive (nous soulignons)».

Il convient de mettre en exergue que la portée de l'immunité diffère suivant que le lanceur d'alerte engage sa responsabilité en raison du *signalement ou de la divulgation* publique d'informations sur des violations, d'une part, ou en raison de *l'obtention* d'informations qui sont signalées ou divulguées publiquement ou de *l'accès* à de telles informations, d'autre part.

59. Dans le premier cas, l'exonération de responsabilité est complète puisqu'elle vise toute forme de responsabilité, qu'elle soit civile, pénale, administrative ou disciplinaire²²¹. L'article 23, paragraphe 7, de la directive sur les lanceurs d'alerte prévoit en particulier que les lanceurs d'alerte et les personnes assimilées n'encourent aucune responsabilité du fait des signalements ou des divulgations publiques effectués au titre de la directive «dans les procédures judiciaires, y compris 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 [...] Ces personnes ont le droit d'invoquer ce signalement ou cette divulgation publique pour demander l'abandon de la procédure, à condition qu'elles aient eu des motifs raisonnables de croire que le signalement ou la divulgation publique était nécessaire pour révéler une violation en vertu de la [...] directive».

L'immunité concédée en cas de signalement ou de divulgation n'est toutefois pas générale en ce sens qu'elle est liée au signalement ou à la révélation publique de faits couverts par la directive. Ainsi, l'article 21, paragraphe 4, de la directive prévoit que «toute autre responsabilité éventuelle des auteurs de signalement découlant d'actes ou d'omissions *qui ne sont pas liés au signalement ou à la divulgation publique ou qui ne sont pas nécessaires pour révéler une violation* en vertu de la [...] directive continue d'être régie par le droit de l'Union ou le droit national applicable (nous soulignons)».

60. Dans le second cas, l'exonération de responsabilité est partielle. L'article 21, paragraphe 3, de la directive énonce à cet égard que :

«[I]es auteurs de signalement n'encourent aucune responsabilité en ce qui concerne l'obtention des informations qui sont signalées ou divulguées publiquement, ou l'accès à ces informations, à *condition que cette obtention ou cet accès ne constitue pas une infraction pénale autonome*. Au cas où cette obtention ou cet accès constitue une infraction pénale autonome, la responsabilité pénale continue d'être régie par le droit national applicable (nous soulignons)».

Cela signifie que le lanceur d'alerte bénéficie d'une immunité de responsabilité lorsqu'il signale ou révèle des informations qu'il a obtenues ou auxquelles il a eu accès de façon licite. Cette immunité vaut également lorsque le lanceur d'alerte révèle des informations qu'il a obtenues ou auxquelles il a eu accès en contravention à des dispositions de droit civil, de droit administratif ou de droit du travail. C'est par exemple le cas lorsque le lanceur d'alerte consulte les courriers électroniques d'un collègue ou des dossiers qu'il n'utilise normalement pas dans le cadre de son travail, photographie les locaux de son entreprise ou

²²¹ Considérant n° 91 de la directive sur les lanceurs d'alerte.

accède à des lieux auxquels il n'a normalement pas accès²²².

En revanche, il demeure soumis au droit national lorsque l'obtention d'informations ou l'accès à ces informations constitue une infraction pénale en soi.

61. La solution proposée par cette disposition est difficilement conciliable avec la solution adoptée par la Cour de cassation luxembourgeoise dans le cadre de l'affaire «Lux Leaks»²²³. Elle risque également de mener à des incohérences flagrantes d'un pays à un autre. Pour rappel, la Cour de cassation luxembourgeoise a jugé que «la reconnaissance du statut de lanceur d'alerte doit s'appliquer en principe à toutes (nous soulignons) les infractions du chef desquelles une personne, se prévalant de l'exercice de son droit garanti par l'article 10 de la Convention, est poursuivie, sous peine de vider la protection devant résulter du statut de lanceur d'alerte de sa substance»²²⁴. Il s'ensuit que le fait justificatif du lanceur d'alerte doit neutraliser l'ensemble des actions composant le processus de dévoilement et ayant donné lieu à des accusations pénales.

Si le lanceur d'alerte des «Lux Leaks», Antoine Deltour, était jugé sous l'empire de la directive sur les lanceurs d'alerte, il pourrait vraisemblablement être poursuivi, nonobstant son statut de lanceur d'alerte, du chef de vol domestique et de fraude informatique. Qu'il ait agi dans un but d'intérêt général serait en effet sans effet dès lors que les deux infractions précitées ne

requièrent pas, en droit luxembourgeois, de dol spécial²²⁵. Le juge luxembourgeois serait toutefois libre de reconnaître, conformément au droit national, la cause justificative du lanceur d'alerte de façon à annihiler le caractère illicite du vol domestique et de la fraude informatique.

Ce faisant, il nous semble que les États membres qui interprètent la jurisprudence de la Cour européenne des droits de l'homme dans les mêmes termes que la Cour de cassation luxembourgeoise ont deux options: soit ils révisent les infractions pénales qui sanctionnent l'obtention d'informations confidentielles ou leur accès de telle sorte que l'infraction ne puisse pas être établie lorsque l'auteur a agi dans l'intérêt public (exigence d'un dol spécial); soit ils laissent le juge apprécier la façon la plus opportune d'accueillir en droit national la figure du lanceur d'alerte, comme le juge luxembourgeois l'a déjà fait. La première solution est évidemment préférable sur le plan de la sécurité juridique même si la notion d'intérêt public laisse au juge une large marge d'appréciation.

62. Un vent favorable aux critiques émises par certaines ONG a provoqué l'ajout d'une disposition expresse dans le texte de la directive en vue de régler l'articulation entre la directive sur les lanceurs d'alerte et la directive «secrets d'affaires»²²⁶. Les deux directives

²²² Considérant n° 92 de la directive sur les lanceurs d'alerte.

²²³ Pour un commentaire, voy. E. COBBAUT, «L'encadrement de l'alerte et la protection du lanceur d'alerte (*whistle-blower*): l'affaire *Luxleaks* à l'aune d'un cadre européen en construction», *R.D.T.I.*, 2019, n° 2, pp. 47-85.

²²⁴ Cour de cassation du Grand-Duché de Luxembourg, arrêt du 11 janvier 2018 dans le cadre de l'affaire dite «LuxLeaks», disponible sur <https://justice.public.lu> (consulté le 2 juillet 2019).

²²⁵ Rappelons que le droit belge se différencie du droit luxembourgeois en ce qu'il distingue la fraude informatique *interne* de la fraude informatique *externe*. La première est le fait d'outrepasser ses habilitations en accédant à un système informatique avec une intention frauduleuse ou dans le but de nuire (dol spécial). La seconde est le fait d'accéder à un système informatique ou de s'y maintenir sans autorisation. Aucun dol spécial n'est ici requis. Sur l'impact de cette distinction au regard de la problématique des «pirates éthiques», voy. J.-F. HENROTTE et P. LIMBREE, *op. cit.*, pp. 20-21.

²²⁶ Notons que l'article 15, § 7, de la proposition de directive du 23 avril 2018 contenait déjà une disposition sur le sujet mais elle était nettement moins précise.

doivent être considérées comme complémentaires²²⁷.

Trois hypothèses doivent être distinguées.

L'article 21, paragraphe 7, alinéa 2, de la directive sur les lanceurs d'alerte prévoit explicitement que le *signalement ou la divulgation* publique d'informations qui comportent des secrets d'affaires sur des violations au droit de l'Union et qui relèvent du champ d'application de la directive sur les lanceurs d'alerte, est considéré comme « licite » dans les conditions énoncées à l'article 3, paragraphe 2, de la directive « secrets d'affaires »²²⁸ du moment que l'auteur du signalement remplit les conditions de la directive sur les lanceurs d'alerte.

L'obtention, l'utilisation et la divulgation illicite d'informations qui comportent des secrets d'affaires qui ne relèvent pas du champ d'application de la directive sur les lanceurs d'alerte, autrement dit qui ne portent pas sur des violations au droit de l'Union, continuent en revanche de tomber sous le coup de la directive « secrets d'affaires » et, le cas échéant, de l'article 5²²⁹. Si besoin est, précisons que l'article 5 de la directive « secrets d'affaires » prévoit les hypothèses – parmi lesquelles figure l'activité de *whistleblowing* – dans lesquelles une action civile intentée pour violation du secret d'affaires doit être tenue en échec.

La discussion n'est pas pour autant close dès l'instant où la directive sur les lanceurs d'alerte ne dit rien quant à un cas de figure fréquent – c'est notre troisième hypothèse – à savoir *l'obtention et l'utilisation* d'informations

qui comportent des secrets d'affaires relevant du champ d'application de la directive qui devraient selon toute vraisemblance intervenir en amont du signalement ou de la divulgation publique lorsque la violation du secret d'affaires est sanctionnée pénalement en droit interne²³⁰. Au contraire, nous avons vu que la directive énonce que « les auteurs de signalement n'encourent aucune responsabilité en ce qui concerne l'obtention des informations concernées ou l'accès à ces informations, pour autant que cette obtention ou cet accès ne constitue pas une infraction pénale en soi. Dans ce dernier cas, la responsabilité pénale demeure régie par le droit national applicable (nous soulignons) ». L'article 5, point b), de la directive « secrets d'affaires » n'est à cet égard pas de grand secours. Certes, il fait obstacle à l'application des mesures, procédures et réparations prévues par la directive précitée « lorsque l'obtention, l'utilisation ou la divulgation alléguée du secret d'affaires a eu lieu pour révéler une faute, un acte répréhensible ou une activité illégale, à condition que le défendeur ait agi dans le but de protéger l'intérêt public général », mais lesdites mesures, procédures et réparations concernent uniquement les actions en responsabilité civile intentées sur pied de la directive « secrets d'affaires ».

Si la directive « secrets d'affaires » et la directive sur les lanceurs d'alerte se font échos, cherchant à ménager un juste équilibre entre la protection du secret d'affaires et la défense de l'intérêt public, il faut reconnaître en définitive que des zones d'ombre subsistent lorsque l'affaire prend une tournure pénale.

²²⁷ Considérant n° 98 de la directive sur les lanceurs d'alerte.

²²⁸ L'article 3, § 2, de la directive « secrets d'affaires » énonce que « l'obtention, l'utilisation ou la divulgation d'un secret d'affaires est considérée comme licite dans la mesure où elle est requise ou autorisée par le droit de l'Union ou le droit national ».

²²⁹ Considérant n° 98 de la directive sur les lanceurs d'alerte.

²³⁰ Si la violation du secret d'affaires n'est pas sanctionnée pénalement, on tombe dans le champ de l'article 21, paragraphe 3, de la directive sur les lanceurs d'alerte.

4. L'accès à des voies de recours

63. Au-delà de l'interdiction explicite de représailles, il y a lieu de donner au lanceur d'alerte accès à des voies de recours appropriées. L'effectivité du principe d'interdiction des représailles tient en effet dans l'existence d'un contrôle juridictionnel approprié et efficace.

Le caractère approprié du recours est déterminé en fonction du type de représailles. Le recours sera approprié s'il prend la forme « d'actions en réintégration, par exemple en cas de licenciement, de mutation ou de rétrogradation, de suspension de formation ou de refus de promotion, ou en rétablissement d'un permis, d'une licence ou d'un contrat annulés; d'un dédommagement des pertes financières actuelles et futures, par exemple pour les pertes de salaires antérieurs, mais aussi les pertes de revenus futurs, et des coûts liés à un changement de profession; et l'indemnisation d'autre préjudice économique, tels que les frais de justice et les frais médicaux, ainsi que du préjudice immatériel tel que douleur et souffrances »²³¹.

Les lanceurs d'alerte doivent, du reste, avoir accès à une réparation intégrale des préjudices subis, en fonction du cadre juridique national, d'une manière qui soit dissuasive et proportionnée au préjudice subi²³². L'octroi d'une indemnisation ne peut être considéré *in abstracto* comme une compensation adéquate. Il convient de mener un examen *in concreto*. Capables de supporter le coût d'une indemnisation, de grandes entreprises pourraient effectivement proposer systématiquement d'indemniser le lanceur d'alerte licencié, ce

qui reviendrait à autoriser le licenciement d'un lanceur d'alerte en raison de son signalement, moyennant indemnisation, et donc à décourager les lanceurs d'alerte potentiels²³³.

64. Dans le sillage de la Recommandation CM/Rec (2014)7²³⁴, la directive établit également un renversement de la charge de la preuve dans le cadre d'une procédure engagée devant une juridiction ou auprès d'une autorité en ce qui concerne un préjudice subi par le lanceur d'alerte. Sous réserve pour lui d'établir « qu'il a effectué un signalement ou fait une divulgation publique et qu'il a subi un préjudice, il est présumé que le préjudice a été causé en représailles au signalement ou à la divulgation publique. En pareil cas, il incombe à la personne qui a pris la mesure préjudiciable d'établir que cette mesure était fondée sur des motifs dûment justifiés »²³⁵.

Le renversement de la charge de la preuve est justifié au motif que l'auteur des représailles se trouve, dans la majorité des cas, en situation de force par rapport à l'auteur du signalement²³⁶. C'est pourquoi il est également prévu que les lanceurs d'alerte et les facilitateurs aient accès à des mesures correctives, en ce compris provisoires, dans l'attente d'un règlement judiciaire de leur situation dès lors que l'issue du règlement judiciaire peut requérir plusieurs années²³⁷. En particulier, il semble difficile de renverser, une fois qu'une longue période de temps s'est écoulée, une mesure de licenciement

²³³ Considérant n° 95 de la directive sur les lanceurs d'alerte.

²³⁴ Recommandation CM/Rec (2014)7, Annexe à la Recommandation, Section VII, Principe 25 et Exposé des motifs, Annexe – Les 29 principes, § 88.

²³⁵ Article 21, § 5, de la directive sur les lanceurs d'alerte.

²³⁶ Considérant n° 93 de la directive sur les lanceurs d'alerte.

²³⁷ Article 21, § 6, de la directive sur les lanceurs d'alerte. Voy. aussi le considérant n° 96 de la directive précitée. En ce sens, voy. aussi Recommandation CM/Rec (2014)7, Exposé des motifs, Annexe – Les 29 principes, § 89.

²³¹ Considérant n° 94 de la directive sur les lanceurs d'alerte.

²³² Article 21, § 8, de la résolution législative du Parlement européen du 16 avril 2019. Voy. aussi le considérant n° 101 de la directive sur les lanceurs d'alerte.

ment alors qu'une telle mesure, vu le préjudice financier, peut sérieusement décourager les lanceurs d'alerte potentiels.

CONCLUSION

65. En se dotant, avec la directive sur les lanceurs d'alerte, d'un instrument horizontal de protection, l'Union européenne fait figure d'exception dans le paysage juridique de l'alerte.

Mêlant habilement tradition et modernité, les principes de base de la directive peuvent être résumés comme suit.

Le lanceur d'alerte est, en principe, une personne qui agit dans le cadre d'une relation de travail, car c'est cette position particulière qui lui fait prendre un risque, le plaçant dans une situation de vulnérabilité justifiant une protection particulière. Les lanceurs d'alerte bénéficient de la protection prévue par la directive pour autant qu'ils aient eu des motifs raisonnables de croire que les informations signalées sur les violations étaient véridiques au moment du signalement et que ces informations entraînent dans le champ d'application de la directive et qu'ils aient effectué un signalement – interne, externe ou public – conforme aux exigences de la directive. Peuvent bénéficier, par extension, de la protection prévue par la directive les proches du lanceur d'alerte, les personnes de son entourage qui ont facilité le signalement ainsi que les entités juridiques appartenant aux auteurs de signalement ou pour lesquelles ils travaillent, ou encore avec lesquelles ils sont en lien dans un contexte professionnel.

Sur le plan matériel, la directive fait preuve de souplesse. Elle s'applique à des domaines aussi variés que la santé publique, la protection de l'environnement, la protection de la vie privée et des données à caractère personnel et la

sécurité des réseaux et des systèmes d'information. Ceci étant, fidèle à l'approche instrumentale de la dénonciation qui est la sienne, l'Union européenne ne voit dans le lanceur d'alerte qu'un auxiliaire de justice. On attend donc de lui qu'il signale des violations au droit de l'Union. Son rôle n'est pas proprement dit de défendre l'intérêt public, même si on lui prête volontiers, dans l'opinion publique, cette mission.

La directive sur les lanceurs d'alerte aborde, mais ne règle encore que très partiellement, les questions les plus débattues en pratique, en l'occurrence l'obligation de suivre une procédure échelonnée, la recevabilité des dénonciations anonymes et l'octroi de récompenses. Il semble par contre désormais acquis que « les motifs amenant les auteurs de signalement à effectuer un signalement devraient être sans importance pour décider s'ils doivent recevoir une protection »²³⁸.

66. Face à la levée de boucliers provoquée, dans un premier temps, par la réception juridique du *whistleblowing* en Europe²³⁹, la voie empruntée par l'Union européenne, et avant elle par la France avec la Loi Sapin II²⁴⁰, a de quoi surprendre.

²³⁸ Considérant n° 32 de la directive sur les lanceurs d'alerte.

²³⁹ Au regard des règles européennes de protection des données, l'autorité française de protection des données (CNIL) a ainsi purement et simplement condamné les dispositifs d'alerte professionnelle aménagés par des entreprises françaises, considérant que leur implémentation « pourrait conduire à un système organisé de délation professionnelle » (CNIL, Délibération n° 2005-110 du 26 mai 2005 relative à une demande d'autorisation de McDonald's France pour la mise en œuvre d'un dispositif d'intégrité professionnelle, p. 4; CNIL, Délibération n° 2005-111 du 26 mai 2005 relative à une demande d'autorisation de la Compagnie européenne d'accumulateurs pour la mise en œuvre d'un dispositif de « ligne éthique », p. 3).

²⁴⁰ Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et

L'Europe aurait-elle fini par faire le deuil de son passé ?

En vérité, il ne faut pas se méprendre sur la vocation d'un cadre juridique dans le domaine de la dénonciation. L'objectif de la directive sur les lanceurs d'alerte n'est pas tant de protéger les lanceurs d'alerte que de décourager les délateurs. L'élaboration d'un régime général de dénonciation a le mérite non négligeable, si celui-ci est bien conçu, de diminuer le nombre de dénonciations méchantes (en raison du risque de sanction) et d'accroître le nombre de dénonciations utiles (en raison de la définition du champ d'application du dispositif). Un tel régime a, par ailleurs, pour effet d'augmenter la transparence quant au phénomène de la dénonciation dès lors qu'il doit nécessairement inclure une obligation de rapportage à charge des autorités qui gèrent le dispositif. Aussi heurtant soit le système américain eu égard à notre tradition juridique, il faut admettre que l'on peut se donner une idée de son fonctionnement, et notamment des récompenses allouées, au travers des rapports publiés annuellement par l'administration²⁴¹, ce qui n'est assurément pas le cas en Belgique.

Le phénomène des lanceurs d'alerte a jeté un nouvel éclairage, résolument positif, sur une

pratique millénaire, celle de promouvoir la dénonciation en vue de renforcer l'application de la loi. On admet désormais, même en Europe où les préjugés en la matière ont la vie dure, que la dénonciation n'est pas nécessairement un manquement à la loyauté. La dénonciation peut également être un acte de responsabilité démocratique. Mais encore faut-il que cela se confirme en pratique. La crise sanitaire rencontrée nous rappelle avec acuité que l'homme est toujours rongé par les mêmes démons. Les comportements individualistes se multiplient et la dénonciation d'intérêt public coexiste dangereusement avec la délation. À l'horizon, le corpus des droits humains amène cependant une lueur d'espoir. L'appréhension de la dénonciation sous l'angle du droit à la liberté d'expression amène inévitablement à ménager un juste équilibre entre les droits, libertés et intérêts des personnes concernées, ce qui présuppose *in fine* de rechercher, ou plutôt de construire, un (notre) idéal démocratique (de demain).

à la modernisation de la vie économique, *J.O.R.F.*, 10 décembre 2016. Bien que le contenu de la Loi Sapin II relève essentiellement de la matière financière, le chapitre relatif à la protection des lanceurs d'alerte dépasse largement ce cadre et crée, en droit français, un véritable régime juridique général de protection des lanceurs d'alerte. Sur les dispositions de la Loi Sapin II relatives aux lanceurs d'alerte, voy. not. Transparency International France, *Guide pratique à l'usage du lanceur d'alerte français* (2009) et *Guide pratique à l'usage du lanceur d'alerte français # 2* (2017), tous deux disponibles sur <https://transparency-france.org> (consulté le 1^{er} novembre 2019).

²⁴¹ Voy. par exemple les rapports annuels du ministre des Finances au Congrès, disponibles à l'adresse <https://www.irs.gov/compliance/whistleblower-office-annual-reports> (consulté le 8 avril 2020).