

Faculté de droit et de criminologie

Analyse et conséquences de la directive sur la protection des personnes qui signalent des violations du droit de l'Union

Auteur : **Lescroart** Mathieu

Promoteur : **Jongen** François

Année académique 2020-2021

Master en droit à finalité européenne

Plagiat et erreur méthodologique grave

Le plagiat, fût-il de texte non soumis à droit d'auteur, entraîne l'application de la section 7 des articles 87 à 90 du règlement général des études et des examens.

Le plagiat consiste à utiliser des idées, un texte ou une œuvre, même partiellement, sans en mentionner précisément le nom de l'auteur et la source au moment et à l'endroit exact de chaque utilisation*.

En outre, la reproduction littérale de passages d'une œuvre sans les placer entre guillemets, quand bien même l'auteur et la source de cette œuvre seraient mentionnés, constitue une erreur méthodologique grave pouvant entraîner l'échec.

* A ce sujet, voy. notamment <http://www.uclouvain.be/plagiat>.

Remerciements

Je tiens en premier lieu à remercier mon promoteur, François Jongen, pour sa disponibilité et ses précieux conseils qui ont aidés à guider l'écriture de ce mémoire. Je souhaite également remercier tous les lanceurs d'alerte, connus ou anonymes, dont la détermination à porter toute injustice au public dans un but d'intérêt général m'a inspiré dans le choix de ce sujet de mémoire.

Ce mémoire a une portée symbolique qui va bien au-delà de la rédaction de cet ouvrage étant donné qu'il représente l'aboutissement de mes années d'études universitaires à l'UCLouvain. Dans cet esprit, j'adresse également mes remerciements à mes parents, pour leur soutien tout au long de ce parcours et pour leur aide pour de nombreux travaux (y compris ce mémoire) qu'ils ont relu minutieusement. De manière plus large, mes remerciements vont également à l'ensemble de mon entourage avec qui j'ai partagé des moments de détente qui m'ont donné par la suite la motivation nécessaire pour me consacrer pleinement à mes cours et à mes travaux. J'ai parfois eu la chance de combiner avec certaines personnes une amitié et une relation de travail fructueuse. Enfin, je remercie l'ensemble des professeurs et des assistant.es de la faculté de droit que j'ai croisé durant mon parcours et qui ont su me donner une idée plus précise des domaines pouvant m'intéresser et, par conséquence, une vision plus claire de mon futur.

Table des matières

Introduction	4
 Chapitre 1 – Situation du lanceur d’alerte avant la directive	6
Section 1 – La protection par le droit européen	6
Section 2 – La protection par la Cour européenne des droits de l’Homme.....	9
Section 3 – La protection organisée par le droit belge	10
 Chapitre 2- La directive 2019/1937 sur la protection des personnes qui signalent des violations du droit de l’Union.....	16
Section 1- Historique	16
Section 2 – Champ d’application	18
Sous-section 1 – Champ d’application matériel	18
§1. Matières concernées par la directive	18
§2. Matières exclues par la directive	21
Sous-section 2- Champ d’application personnel.....	23
§1. La personne signalant des violations du droit de l’Union	23
§2. Exclusions du champ d’application personnel.....	26
§3. Comparaisons avec la définition de la Cour européenne des droits de l’Homme	27
Section 3 – Procédures à suivre	29
Sous-section 1 – Le signalement interne	29
Sous-section 2 – Le signalement externe.....	31
Sous-section 3 – Caractéristiques communes des procédures de dévoilement	34
Sous-section 4 – La divulgation publique	36
Section 4 – Mesures de protection envisagées par la directive	39
 Chapitre 3 – Situation du lanceur d’alerte après la directive	43
Section 1 – Impact de la directive sur les textes belges existants	43
Sous-section 1- Maintien ou révision des systèmes existants ?	43
Sous-section 2. Impact sur le champ d’application personnel	45
Sous-section 3. Les procédures sont-elles conformes aux canaux européens ?.....	46
§1- Existence de canaux internes et externes	46
§2- Conformité des canaux belges avec les critères européens	48
§3 – La divulgation publique.....	53
Sous-section 4. Les mesures de protection répondent-elles aux critères européens ?.....	53
Section 2- Avancement de la transposition.....	56

Section 3 – Analyse de la proposition de loi	57
<i>Sous-section 1- Champ d'application</i>	57
<i>§1. Champ d'application matériel</i>	57
<i>§2. Champ d'application personnel</i>	58
<i>Sous-section 2 - Mise en œuvre des procédures</i>	61
<i>Sous-section 3 - Mesures de protection proposées</i>	62
 Conclusion	 67
 Bibliographie	 70

Introduction

Le lanceur d'alerte est un terme relativement nouveau, désignant un personnage prenant de plus en plus d'importance depuis ces quelques dernières décennies. C'est d'abord aux États-Unis que cette catégorie d'individu est reconnue sous la dénomination de « *whistleblower* »¹, avant que le monde francophone commence à s'y intéresser et que le mot « *lanceur d'alerte* » apparaisse pour la première fois dans les années 90 dans le domaine de la sociologie². Francis Chateauraynaud, un sociologue qui fut l'un des premiers à populariser l'usage du terme³, définit le lanceur d'alerte comme étant « *Toute personne ou groupe qui rompt le silence pour signaler, dévoiler ou dénoncer des faits, passés, actuels ou à venir, de nature à violer un cadre légal ou réglementaire ou entrant en conflit avec le bien commun ou l'intérêt général (...)* ».⁴ Cette description ne fait cependant pas l'unanimité et il existe une multitude de définitions proposées par des auteurs de doctrine, des législations nationales ou encore des organisations internationales. Il faut noter à ce stade que, si la plupart retiennent certains éléments en commun, elles divergent sur un certain nombre de points, à savoir le contexte où a été acquise l'information, l'intention du lanceur d'alerte ou encore le fait que celui-ci soit passé par une procédure spécifique.⁵

Les très nombreuses affaires mettant en scène les lanceurs d'alerte démontrent bien le risque de représailles qu'encourent ces personnes du fait de leur divulgation. On peut l'illustrer par la figure la plus connue du « *whistleblower* », Edward Snowden, toujours sous l'objet de poursuites par la justice américaine pour violation du *Espionage Act* pour avoir dévoilé au public les méthodes de surveillance de masse utilisées par la NSA⁶. Nul besoin cependant de traverser l'Atlantique afin de trouver des exemples des difficultés que peuvent rencontrer les divulgateurs : on peut ainsi évoquer le cas de l'affaire *Luxleaks* qui se déroula, comme son nom l'indique, au Luxembourg. Beaucoup se souviendront des problèmes rencontrés par ces deux anciens employés d'une société d'audit poursuivis pour, entre autres, vol de documents et

¹ E. COBBAUT., « Les lanceurs d'alerte : un objet juridique non identifié ? », A&M, 2018, p.42.

² M.BARDIN, « Les « lanceurs d'alerte » à l'ère du numérique : un progrès pour la démocratie ? » in *Protection des données personnelles et sécurité nationale* (sous la dir. de BEAUREGARD-BERTHIER D. et TALEB-KARLSSON A.), Bruxelles, Bruylant, 2017, pp.257-258.

³ A.LACHAPELLE, « Titre 6 – Le lancement d'alerte ou la délation organisée ? » in *Vie privée, liberté d'expression et démocratie dans la société numérique* (sous la dir. de Y.POULLET), Bruxelles, Larcier, 2020, p.212.

⁴ F. CHATEAURAYNAUD, « Lanceur d'alerte », in *Dictionnaire critique et interdisciplinaire de la participation* (I. CASILLO avec R. BARBIERETAL. dir.), Paris, GIS démocratie et participation, 2013, disponible sur www.dicopart.fr (consulté le 24/03/2021).

⁵ E. COBBAUT., A&M, *op.cit.*, pp.47-49.

⁶ E.SNOWDEN, *Mémoires Vives*, Paris, édition du Seuil, pp.332-333.

violation de secret d'affaire à la suite de la révélation par ces derniers à la presse d'une pratique d'optimisation fiscale de grande ampleur ayant bénéficié de la participation de l'administration fiscale luxembourgeoise. La plus haute instance du pays établit finalement l'interdiction d'inculper l'un des employés, Antoine Delcourt, pour les infractions relatives à la divulgation du fait de la reconnaissance de son statut de lanceur d'alerte.⁷ Ces deux affaires font partie d'une longue liste de cas similaires sur lesquels il est inutile de s'étendre davantage.

Ces quelques illustrations prouvent l'importance d'organiser une protection légale pour cette catégorie de personnes. Plusieurs pays ont déjà pris en compte cette nécessité et ont adopté des textes sur la question, que ce soit de manière générale ou plus sectorielle : on peut citer les États-Unis, le Royaume-Uni⁸ ou encore une huitaine d'États membres de l'Union européenne, parmi lesquels nos voisins français et néerlandais⁹. Dernièrement, ce fut au tour de l'Union européenne elle-même de légiférer sur le sujet via sa directive du 23 octobre 2019 « *sur la protection des personnes qui signalent des violations du droit de l'Union* ».

Cet état des faits nous force à nous questionner sur la situation en Belgique et sur les conséquences qu'aura la transposition de cette dernière directive au sein de l'ordre national. Ce mémoire a pour vocation de répondre à ces quelques dernières interrogations. Dans cet objectif, nous examinerons en premier lieu la protection actuelle dont bénéficient les lanceurs d'alerte au sein de notre territoire : nous reviendrons pour ce faire sur plusieurs législations européennes et belges, ainsi que sur la jurisprudence de la Cour européenne des droits de l'Homme sur le sujet. Ensuite, nous analyserons minutieusement le contenu de la directive européenne susmentionnée en expliquant et en commentant son champ d'application (tant personnel que matériel), les procédures de divulgation envisagées et les mesures de protection établis par ce dernier texte. Le troisième chapitre sera focalisé sur la potentielle situation des lanceurs après transposition de la directive. Dans cet objectif, nous comparerons les législations sectorielles belges avec les critères du texte européen : cela nous permettra de savoir, en cas de maintien des procédures existantes, quels éléments modifier afin d'être en conformité avec les demandes du législateur de l'Union. Enfin, nous observerons en détail, et toujours au regard de la directive 2019/1937, la dernière proposition législative belge émise afin d'assurer un statut légal et une protection aux lanceurs d'alerte.

⁷ M.NELLES, « Le procès Luxleaks, prémices d'un retournement de situation en faveur des lanceurs d'alerte ? », note sous Cass.Luxembourg, 11 janvier 2018, *JLMB*, 2018, pp.1803-1806.

⁸ M.BARDIN, op.cit., p.259-261.

⁹ V.MAGNIER, « Avant-propos », *RAE*, 2019, p.678.

Chapitre 1 – Situation du lanceur d’alerte avant la directive

Section 1 – La protection par le droit européen

L’une des premières mesures prises par le législateur de l’Union dans cette matière concernait la protection des lanceurs d’alerte au sein même des institutions européennes : en effet, est établie en 2004 l’obligation pour le fonctionnaire européen ayant pris « *connaissance de faits qui peuvent laisser présumer une activité illégale éventuelle (...) préjudiciable aux intérêts de l’Union* » d’en avertir directement soit un de ses supérieurs au sein de l’institution ou, selon son appréciation, une autorité externe. Le lanceur d’alerte ainsi que la personne relayant l’information à l’Office européen de lutte anti-fraude se voient garantir l’absence de toutes répercussions venant de l’institution à laquelle ils appartiennent, sous condition de leur bonne foi.¹⁰ Un règlement ultérieur de 2013 introduit l’obligation pour les institutions de prévoir une procédure de signalement interne.¹¹

En ce qui concerne les révélations portant sur des faits extérieurs aux institutions, la question a été évoquée à plusieurs reprises par le législateur européen dans plusieurs textes sectoriels spécifiques. Les considérants de la directive de 2019 font directement référence à ces législations éparpillées, dans le but de montrer l’intervention du législateur de l’Union dans la matière ainsi que de prouver que la mise en place d’une protection des lanceurs d’alerte à l’échelle supranationale est bénéfique pour la poursuite de plusieurs objectifs poursuivis par l’Union européenne.¹²

Sont ainsi cités un texte relatif à la sécurité des opérations pétrolières et gazières en mer prévoyant un signalement confidentiel des problèmes de sécurité¹³, une directive demandant aux États membres de mettre en place un système efficace de dénonciation en ce qui concerne

¹⁰ Règlement (CEE) n°31 et (Euratom) n°11 du Conseil du 18 décembre 1961 fixant le statut des fonctionnaires et le régime applicable aux autres agents de la Communauté économique européenne et de la Communauté européenne de l’énergie atomique, article 22 bis et 22 ter, *J.O.U.E.*, 14 juin 1962, R0031, p.1385 ; Règlement (CE, Euratom) n°723/2004 du Conseil du 22 mars 2004 modifiant le statut des fonctionnaires des Communautés européennes ainsi que le régime applicable aux autres agents de ces Communautés, Annexe 1, 25), *J.O.U.E.*, 27 avril 2004, L124, p.12.

¹¹ Règlement (CEE) n°31 et (Euratom) n°11, article 22 quater ; Règlement (UE, Euratom) n° 1023/2013 du Parlement européen et du Conseil du 22 octobre 2013 modifiant le statut des fonctionnaires de l’Union européenne et le régime applicable aux autres agents de l’Union européenne, article 1, 12), *J.O.U.E.*, 29 octobre 2013, L287, p.21

¹² 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, considérants 7 ; 9 ; 10 ; 20 ; 21 et 23, *J.O.U.E.*, 26 novembre 2019, L305, p.17

¹³ Directive 2013/30/UE du Parlement européen et du Conseil du 12 juin 2013 relative à la sécurité des opérations pétrolières et gazières en mer et modifiant la directive 2004/35/CE, article 22, *J.O.U.E.*, 28 juin 2013, L178, p.84.

les infractions aux règles concernant les établissements de crédit et les entreprises d'investissement¹⁴, deux textes sur la protection des lanceurs d'alerte dans les services financiers¹⁵ (qui ont été définir de nouvelles compétences de la FSMA en Belgique, qui seront développées dans la troisième sous-section de cette partie),... Cette liste est non-exhaustive ; le législateur européen cite encore dans les considérants plusieurs autres législations sectorielles établissant des procédures de divulgation et des mesures de protection pour les lanceurs d'alerte, parfois de manière très concise.

Notons également à titre accessoire que la Commission européenne elle-même a mis en place un système permettant aux personnes de lui transmettre des informations en matière d'infraction au droit de la concurrence via sa page internet, de manière anonyme ou non.¹⁶

La thématique de la prise en compte de la situation des lanceurs d'alerte de manière uniforme a surtout été évoquée avec force lorsque la directive sur les secrets d'affaires était sur le point d'être finalisée et que surgirent certaines inquiétudes suivant la première version de ce texte.¹⁷ En effet, pour qu'une information soit considérée comme relevant du domaine des secrets d'affaires, il suffit qu'elle réponde à trois conditions cumulatives : il faut que cette information soit inconnue (ou difficilement accessible) des autres personnes du milieu concerné, qu'elle ait une valeur commerciale du fait de son caractère secret et que la personne disposant de cette information ait pris des « mesures raisonnables » pour protéger ce caractère secret¹⁸. De ce fait, il apparaît qu'il est potentiellement aisé pour une entreprise de poursuivre un lanceur d'alerte sur base de ce texte après la divulgation par ce dernier d'une information pouvant être considérée comme un secret d'affaires du fait de cette définition extrêmement large. Le soulèvement de certaines craintes quant à ce fait, apparues dès la proposition de directive émise

¹⁴ Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE, article 71, *J.O.U.E.*, 27 juin 2013, L176, p.377.

¹⁵ Règlement (UE) No 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, 2003/125/CE et 2004/72/CE de la Commission, article 32, *J.O.U.E.*, 12 juin 2014, L173, p.173 et Directive d'exécution (UE) 2015/2392 de la Commission du 17 décembre 2015 relative au règlement (UE) n° 596/2014 du Parlement européen et du Conseil en ce qui concerne le signalement aux autorités compétentes des violations potentielles ou réelles dudit règlement, *J.O.U.E.*, 18 décembre 2015, L332, pp.126-132.

¹⁶ Voir https://ec.europa.eu/competition-policy/cartels/whistleblower_en (consulté le 14/05/2021).

¹⁷ E. COBBAUT, « L'encadrement de l'alerte et la protection du lanceur d'alerte (whistleblower) : l'affaire Luxleaks à l'aune d'un cadre européen en construction », *RDTI*, 2019, pp.72-73 ; F.COTON et J-F. HENROTTE, « Le lanceur d'alerte : une personne concernée par le traitement de ses données à caractère personnel, mais également par son avenir professionnel... », *RDTI*, 2016, p.50.

¹⁸ Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites, article 2, 1), *J.O.U.E.*, 15 juin 2016, L157, p.10.

par la Commission en 2013, a été pris en compte par le législateur européen au cours du processus législatif.¹⁹

Ainsi, le texte final tente de rassurer sur la situation des lanceurs d’alerte, en établissant en premier lieu dans les considérants la remarque que « *les activités des lanceurs d’alertes* » ne sauraient être paralysées par ces nouvelles règles européennes.²⁰ Ensuite, il est également établi que la directive ne saurait porter atteinte à « *l’exercice du droit à la liberté d’expression* », un fait qui est réitéré par la suite lorsqu’il est énoncé que l’exercice de ce droit empêche « *l’application des mesures, procédures et réparations* » en cas d’obtention, d’utilisation ou de divulgations de secrets d’affaires.²¹ De même, ces mesures ne sont pas accordées lorsque la personne a usé des secrets d’affaires pour « *révéler une faute, un acte répréhensible ou une activité illégale* », pour autant que ce fut fait dans un objectif de protection d’intérêt public, ou encore pour protéger « *un intérêt légitime reconnu par le droit de l’Union ou le droit national* »²² (il faut alors s’interroger sur l’interprétation du terme « *intérêt légitime* »). Enfin, l’obtention, l’utilisation et la divulgation des secrets d’affaires sont rendues licites lorsque ce fait est « *requis ou autorisé par le droit de l’Union ou le droit national* »²³ : on peut légitimement penser que rentre dans cette hypothèse une législation réglant la situation des lanceurs d’alerte.²⁴

Cependant, ces quelques concessions n’ont nullement réussi à faire taire les craintes de certains citoyens européens de voir la protection des lanceurs d’alerte s’estomper en faveur des intérêts des entreprises, ces dernières pouvant potentiellement toujours utiliser la notion de secrets d’affaires pour réduire cette catégorie de personnes au silence.²⁵ On peut de plus estimer que les modifications du texte européen citées plus haut ne sont pas suffisantes, car ne visant pas expressément les lanceurs d’alerte dans les dispositions même et étant rédigées en des termes trop larges.

¹⁹ E.COBBAUT, *RTDI*, *op.cit.*, pp.72-73.

²⁰ Directive (UE) 2016/943 considérant 20, article 1, §2 et article 5 ; Pour voir l’origine de ces amendements : Rapport sur la proposition de directive du Parlement européen et du Conseil sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d’affaires) contre l’obtention, l’utilisation et la divulgation illicites (Rapp : C. LE GRIP), *P.E Doc.*, A8-0199/2015 du 22 juin 2015.

²¹ Directive (UE) 2016/943, article 1, §2 et 5, a).

²² Directive (UE) 2016/943, article 5, b) et d).

²³ Directive (UE) 2016/943, article 3, §2.

²⁴ E.COBBAUT, *RTDI*, *op.cit.*, pp.74-76.

²⁵ V. DE BEAUFORT, *Du lobbying au e-lobbying*, Bruxelles, Larcier, 2019, p.74. Voir également la pétition sur ce sujet au plus de 160 000 signatures sur le site de We Move EU : <https://act.wemove.eu/campaigns/les-lanceurs-d-alerte-en-danger> (consulté le 14/05/2021).

Ces critiques envers le texte de l'Union européenne ne sont cependant pas restées sans réponses : d'un certain point de vue, on peut estimer que ces dernières ont donné l'impulsion nécessaire qui a mené à l'adoption de la directive sur « *la protection des personnes qui dénoncent des infractions au droit de l'Union* ». Le processus d'élaboration de ce texte sera décrit plus longuement dans le second chapitre de ce mémoire.

Section 2 – La protection par la Cour européenne des droits de l'Homme

La jurisprudence de la Cour européenne des droits de l'Homme a un impact direct sur la situation des lanceurs d'alerte au sein du territoire européen pouvant s'étendre au-delà des institutions du Conseil de l'Europe : elle est en effet souvent directement prise en compte par les juridictions nationales. On se rappellera que la Cour d'appel et la Cour de cassation luxembourgeoise font référence tant à l'article 10 de la CEDH qu'à la jurisprudence entourant cette norme dans la fameuse affaire Luxleaks.²⁶ De même, il est déjà arrivé que nos tribunaux domestiques se réfèrent aux enseignements de la Cour européenne afin de déterminer si une personne agit dans le cadre de son droit à la liberté d'expression en tant que lanceur d'alerte.²⁷ Il convient de ce fait d'examiner brièvement les décisions de la Cour de Strasbourg en cette matière afin de déterminer la portée de cette protection.

Cette jurisprudence repose en toute logique sur la base de l'article 10 de la Convention consacré à la liberté d'expression. Cette protection a été proclamée par la Cour dans l'arrêt Guja²⁸ : la Cour, répondant à l'interrogation demandant si l'article 10 pouvait être invoqué par une personne autre que l'auteur de ces lettres, a eu cette déclaration symbolique que « *la protection de l'article 10 s'étend à la sphère professionnelle en général et aux fonctionnaires en particulier* ». ²⁹ Pour cette juridiction, le lanceur d'alerte doit donc avoir eu connaissance des informations dans le cadre de son travail.

La protection n'est cependant pas dans ce cas absolue : en effet, il faut rappeler que l'article 10 supporte certaines restrictions qui peuvent être acceptées pour autant qu'elles respectent les trois phases du test de proportionnalité, à savoir pour rappel qu'elles soient « *prévues par la*

²⁶ Cour d'appel du Luxembourg (5^{ème} ch. Corr.), 15 mai 2018, A&M, 2018, p.102 ; Cass. Luxembourg, 11 janvier 2018, JLMB, 2018, p.1796.

²⁷ C.trav.Bruxelles (4^{ème} ch.), 22 juin 2016, JLMB, 2019, liv.13, p.580.

²⁸ K. BLAY- GRABARCZYK , «Le statut du lanceur d'alerte dans les arrêts de la Cour européenne des droits de l'homme », *RevTrimDH*, 2018, n°116, pp.857-858.

²⁹ Cour.europ. D.H, arrêt Guja c. Moldavie du 12 février 2008, <http://www.echr.coe.int> (19 octobre 2020).

loi », qu'elles poursuivent un but légitime et qu'elles soient « *nécessaires dans une société démocratique* ». ³⁰ La Cour a déjà souvent pris compte dans sa jurisprudence d'autres intérêts contraires qu'elle considère comme but légitime et met en balance avec le droit d'expression, tel que par exemple « *le devoir de loyauté, de réserve et de discrétion* » des salariés à l'égard de leur employeur ³¹ ou encore « *la protection de la réputation et des droits d'autrui* ». ³²

Il a été remarqué que six critères, qui ont été dégagés lors de l'affaire Guja, sont généralement pris en compte par la Cour afin de savoir si la restriction à la liberté d'expression du lanceur est nécessaire ³³. Le lanceur d'alerte devra donc être de bonne foi, dans le sens qu'il devra avoir la conviction que l'information dévoilée est authentique. ³⁴ On tient également compte au sein de cette même jurisprudence de l'intention profonde du lanceur d'alerte, pouvant se manifester par le fait que celui-ci « *aurait été motivé par le désir de retirer un avantage personnel de son acte, qu'il aurait nourri un grief personnel (...) ou qu'il aurait été mû par une quelconque autre intention cachée* » ³⁵. On regarde également, dans cet exercice de balance, au préjudice subi par la personne ou l'entité concernée par l'information du fait de sa divulgation ³⁶. Une attention particulière sera également portée à la manière dont le lanceur a dévoilé l'information : celle-ci devra être communiquée en dernier ressort au public uniquement si la dénonciation à un supérieur ou une autre autorité compétente n'est pas possible. ³⁷ La Cour se penche en outre sur le caractère d'intérêt général ou public que revêt l'information divulguée et, finalement, prend également en compte la sévérité de la sanction imposée au lanceur d'alerte du fait du dévoilement en question. ³⁸

Section 3 – La protection organisée par le droit belge

Le premier texte législatif en Belgique prévoyant un système de dénonciation à la disposition d'éventuels lanceurs d'alerte fut établi en 2004 par la Communauté flamande. Une modification

³⁰ Convention de sauvegarde des droits de l'Homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, approuvée par la loi du 13 mai 1955, article 10, §2, *M.B.*, 19 août 1955, p.5028.

³¹ Cour.europ. D.H, arrêt Soares c.Portugal du 21 septembre 2016 ; <http://www.echrc.coe.int> (19 octobre 2020) ; arrêt Guja c. Moldavie.

³² Cour.europ. D.H. arrêt Heinisch c. Allemagne du 21 octobre 2010, <http://www.echr.coe.int> (19 octobre 2020).

³³ Cour. Europ. D.H arrêt Matùz c. Hongrie du 21 janvier 2015, <http://www.echr.coe.int> (19 octobre 2020) ; arrêt Guja c. Moldavie ; E.Cobbaut, A&M, *op.cit.*, p.54.

³⁴ K. BLAY- GRABARCZYK, *Ibidem*, pp.863-864.

³⁵ Cour.europ. D.H. arrêt Bucur et Toma c. Roumanie du 8 avril 2013, <http://www.echr.coe.int> (19 octobre 2020).

³⁶ Cour.europ. D.H, arrêt Halet c.Luxembourg du 11 mai 2021, <http://www.echr.coe.int> (11 mai 2021).

³⁷ Arrêt Soares c. Portugal.

³⁸ Arrêt Guja c. Moldavie, arrêt Matùz c. Hongrie.

de la loi sur les médiateurs flamands a en effet introduit la possibilité pour tout employé d'une des administrations de l'entité fédérée en question de « *dénoncer par écrit ou oralement auprès du service de médiation flamand, des négligences, abus ou délits* »³⁹ lorsque ceux-ci ont déjà tenté d'avertir leur supérieur ou l'Audit interne mais n'ont pas reçu de réponses dans les 30 jours ou encore lorsque ceux-ci sont (ou risquent d'être) victimes d'éventuelles sanctions.⁴⁰ Quelques années plus tard, la Communauté germanophone mit également sur pied un système similaire de possibilité de dénonciation par un fonctionnaire de délits au médiateur de cette même Communauté.⁴¹ À ce jour, la Communauté française n'a quant à elle toujours pas prévu de système de dénonciation mis à disposition pour ses fonctionnaires. Rien n'a non plus été établi au niveau des Régions : le gouvernement wallon ambitionnait de mettre en place un système de dénonciation similaire à celui existant au fédéral, mais le projet n'a connu aucun avancement depuis avril 2019.⁴²

Au niveau fédéral, la première (et unique au moment présent) loi sur les lanceurs d'alerte a été prise en 2013 avec « *la loi relative à la dénonciation d'une atteinte suspectée à l'intégrité au sein d'une autorité administrative fédérale par un membre de son personnel* ». Les travaux préparatoires entourant ce texte font clairement ressortir une inspiration du système instauré par le législateur flamand quelques années auparavant⁴³. Comme son titre l'indique très clairement, son champ d'application ne vise que le secteur public, tandis que les informations divulguées concernent quant à elles uniquement des « *atteintes (suspectées) à l'intégrité* » (à savoir un manquement aux règles applicables aux autorités administratives, un manquement aux obligations professionnelles ou encore un acte « *impliquant un risque inacceptable pour la vie, la santé ou la sécurité des personnes ou pour l'environnement* »⁴⁴) remontant à cinq ans

³⁹ Décret Comm.fl. du 7 juillet 1998 instaurant le service de médiation flamande, article 12 bis, *M.B.*, 25 août 1998, p.27221.

⁴⁰ Décret Comm.fl. du 7 juillet 1998, article 3§2.

⁴¹ Décr. Comm. germ. du 26 mai 2009 instituant la fonction de médiateur pour la Communauté germanophone, article 16.1, *M.B.*, 7 octobre 2009, p.66206.

⁴² Avis de l'autorité de données précédant le projet d'arrêté du gouvernement wallon portant dispositions diverses relatives à l'information, par un membre du personnel, d'une irrégularité au sein d'un service du gouvernement ou d'un organisme d'intérêt public auquel est applicable le décret du 22 janvier 1998 relatif au statut du personnel de certains organismes d'intérêt public relevant de la Région wallonne ; « Enfin une protection pour les lanceurs d'alerte dans la fonction publique wallonne », *Gouvernement Wallon*, 21 février 2019, <https://gouvernement.wallonie.be/home/presse/publications/enfin-une-protection-pour-les-lanceurs-dalerte-dans-la-fonction-publique-wallonne.publicationfull.html> (consulté le 14/05/2021).

⁴³ Rapport sur le projet de loi relatif à la dénonciation d'une atteinte suspectée à l'intégrité au sein d'une autorité administrative fédérale par un membre de son personnel et la proposition de loi modifiant la loi du 22 mars 1995 instaurant les médiateurs fédéraux, en ce qui concerne la protection des fonctionnaires qui dénoncent des irrégularités, *Doc. Parl.*, Ch.repr., sess.ord. 2013-2014, n°2802/002.

⁴⁴ Loi du 5 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, article 2, 2° et 3° *M.B.*, 4 octobre 2013, p.69406.

maximum et fondées sur une présomption raisonnable⁴⁵. De même, ce mécanisme de dénonciation n'est pas ouvert à tous : seuls les membres du personnel, ou les anciens membres dont le service remonte à deux ans maximum, sont invités à dénoncer ces atteintes.⁴⁶

Le système mis en place par cette première législation nationale peut se résumer de la manière suivante : après avoir demandé un avis à une *personne de confiance d'intégrité* au sein de l'administration concernée⁴⁷, le fonctionnaire pourra alerter son supérieur hiérarchique ou, s'il ne le souhaite simplement pas, cette même personne de confiance à qui il a adressé un avis. Dans les deux méthodes de dénonciation, la personne à qui la divulgation est faite a une obligation d'alerter les médiateurs fédéraux.⁴⁸

Ces deux possibilités ne sont cependant ouvertes que pour les membres du personnel voulant transmettre une information concernant une atteinte ayant eu lieu à l'intérieur de l'administration où ces derniers sont occupés. Ainsi, les fonctionnaires voulant dénoncer une atteinte ayant lieu dans une autre administration que celle où ils travaillent, ou encore les anciens fonctionnaires ayant travaillé en cette qualité dans les deux années précédentes, devront porter leur allégation au « *Point de contact central* » (appelé le « *Centre d'intégrité* »⁴⁹), qui est instauré au sein des services des médiateurs fédéraux⁵⁰. Cette possibilité est également ouverte pour les fonctionnaires « *en l'absence d'une personne de confiance d'intégrité* » ou, encore une fois, si ceux-ci ne désirent pas porter l'information relative à l'atteinte à leur supérieur ou à cette personne de confiance.⁵¹ Quelle que soit la situation du fonctionnaire concerné, une demande d'avis au Point de contact central (similaire à celle adressée à la personne de confiance d'intégrité) devra être rédigée au préalable pour pouvoir saisir ce Centre.⁵² Notons que cette demande peut également être adressée après un avis défavorable de la personne de confiance d'intégrité⁵³.

Après communication de l'atteinte aux médiateurs fédéraux, ces derniers entament ensuite une enquête sur le fait sur lequel porte la dénonciation et ont l'obligation de protéger les personnes

⁴⁵ Loi du 5 septembre 2013, article 5.

⁴⁶ Loi du 5 septembre 2013, article 3, §1.

⁴⁷ Loi du 5 septembre 2013, article 6.

⁴⁸ Loi du 5 septembre 2013, article 8, §1.

⁴⁹ <http://www.federaalombudsman.be/fr/integrite#:~:text=Le%20Centre%20Int%C3%A9grit%C3%A9%20aupr%C3%A8s%20du,une%20atteinte%20%C3%A0%20l'int%C3%A9grit%C3%A9> (consulté le 14/05/2021)

⁵⁰ Loi du 5 septembre 2013, article 3, §3.

⁵¹ Loi du 5 septembre 2013, article 8, §2.

⁵² Loi du 5 septembre 2013, article 6.

⁵³ Loi du 5 septembre 2013, article 7.

liées à celle-ci (à savoir entre autres le dénonciateur ou la personne de confiance d'intégrité) d'éventuelles répercussions.⁵⁴

Cette première législation fédérale sur lanceurs d'alerte possède certaines bonnes idées, que l'on retrouvera par ailleurs dans la directive européenne. Une constatation évidente est que, contrairement au système de la Communauté flamande, la procédure de dénonciation au sein des administrations fédérales ne respecte pas un système de « cascade » strict ; le fonctionnaire peut aller porter son atteinte à l'échelon qu'il souhaite, peu importe le niveau où ce dernier se situe. Aucune contrainte de temps maximum de délai de réponse ou de crainte de répercussion n'est établie. On respecte ici la liberté de choix du lanceur d'alerte et on lui fait confiance pour aller porter sa dénonciation à l'acteur le plus pertinent : libre à lui d'estimer si une dénonciation à son supérieur direct sera inefficace ou entraînera des représailles. La procédure d'avis rajoute sans contestation un degré de complexité à cette procédure, mais est néanmoins intéressante en ce qu'elle établit un premier « filtre » dans la réception des accusations (tel était par ailleurs l'objectif affiché lors des discussions parlementaires⁵⁵) permettant de rejeter des informations erronées (un autre incitant pour éviter de telles dérives est la possibilité de sanctions pour les mésinformations). Malgré sa relative longueur (l'avis devant être rendu par l'autorité endéans les 8 semaines), la loi contre tout inconvénient découlant de ces larges délais en prévoyant une protection rétroactive du lanceur d'alerte par les médiateurs fédéraux débutant dès le dépôt de la demande d'avis.⁵⁶ Cependant, une critique évidente envers cette loi de 2013 est la limitation de son champ d'application personnel. En effet, à partir du moment où un membre du personnel peut aller dénoncer une atteinte à l'intégrité n'ayant pas eu lieu au sein de son administration, on peut se demander pourquoi cette possibilité n'est pas ouverte pour toute autre personne ne travaillant pas dans une administration. On pense ici surtout à l'adjudicataire engagé en vertu d'un contrat de marché public qui pourrait potentiellement découvrir une telle atteinte.

Ces quelques textes législatifs mentionnés ci-dessus concernant uniquement le domaine public, on peut légitimement s'interroger sur l'existence d'une protection nationale organisée au sein du secteur privé. Force est de constater que le législateur belge n'a presque jamais envisagé la question, le travailleur employé dans le privé voulant dénoncer une infraction se trouvera généralement, au moment où sont écrites ces lignes, dans l'impossibilité de trouver un

⁵⁴ Loi du 5 septembre 2013, articles 10 et 15.

⁵⁵ Rapport sur le projet de loi relatif à la dénonciation d'une atteinte suspectée à l'intégrité au sein d'une autorité administrative fédérale par un membre de son personnel et sur la proposition de loi modifiant la loi du 22 mars 1995 instaurant les médiateurs fédéraux, en ce qui concerne la protection des fonctionnaires qui dénoncent des irrégularités.

⁵⁶ Loi du 5 septembre 2013, articles 6, §6 ; et 15, § 3.

quelconque canal de signalement officiel. Plusieurs raisons pour ce vide législatif ont déjà été évoquées, notamment le fait que le travailleur puisse se protéger d'éventuelles répercussions par des mécanismes déjà existants : par exemple, le travailleur renvoyé du fait d'une dénonciation quelconque pourra alléguer un licenciement manifestement déraisonnable afin d'obtenir réparation de son préjudice. Une autre explication est que certains considèrent que la signature du contrat de travail par l'employé entraîne de sa part une obligation de loyauté (ce qui est un critère qui avait déjà été mis en avant au sein de la jurisprudence de la Cour européenne⁵⁷) ainsi qu'une restriction volontaire de sa liberté d'expression. Les entreprises peuvent toutefois librement et volontairement établir un système de dénonciation et des mesures de protection des lanceurs d'alerte.⁵⁸

Il existe cependant un secteur privé spécifique, à savoir le secteur financier, à connaître une législation portant sur la protection des lanceurs d'alerte. La loi du 2 août 2002 concernant la surveillance du secteur financier contient en effet un article 69 bis imposant à la FSMA (l'autorité des services et des marchés financiers) de « *mettre en place des mécanismes pour permettre le signalement, à la FSMA, des infractions* » tout en « *préservant le caractère confidentiel de l'identité de la personne qui effectue un signalement* ». La personne faisant le signalement, pour autant qu'elle soit de bonne foi et qu'il ne s'agisse pas d'un avocat rompant le secret professionnel, bénéficiera d'une protection de son identité ainsi que de multiples mesures de protection.⁵⁹ Ce régime ne s'applique cependant que si l'information a été uniquement communiquée à la FSMA ; une divulgation ultérieure à une personne tierce de cette même information aura pour effet de faire perdre au lanceur concerné le bénéfice de la protection prévue par l'article 69 bis.⁶⁰ Nous pouvons critiquer le caractère strict de cette règle, d'autant plus lorsque la transmission de l'information à la FSMA a déjà été effectuée : une analyse cas par cas nous semble plus justifiée.

Si cette communication à la FSMA s'apparente à une signalisation par le biais d'un canal externe, une obligation de mise en place de canaux internes est prévue par l'article 69ter de la même loi de 2002 portant sur les marchés financiers. En effet, ce dernier impose à certains organismes déterminés (en ce compris les établissements de crédit, les entreprises d'assurances,

⁵⁷ Arrêt Guja c. Moldavie, arrêt Soares c. Portugal

⁵⁸ D. CUYPERS, « Klokkenluiders : effectieve rechtsbescherming of niet? » in *Voor recht, rechtvaardigheid en Camus. Liber amoricum Bernard Hubeau*, Brugge, Die keure, 2018, pp.481-483.

⁵⁹ Loi du 2 août 2002 relative à la surveillance du secteur financier et aux secteurs financiers, article 69 bis, *M.B.*, 4 septembre 2002, p.39121.

⁶⁰ P.DE PAUW et A. MECHELYNCK « Les lanceurs d'alerte dans le secteur financier », *D.B.F-B.F.R.*, 2018, p.55.

les sociétés de gestion de portefeuille⁶¹,...) d'instaurer « *des procédures internes appropriées permettant le signalement d'infractions potentielles ou réelles* »⁶². La détermination de cette procédure est cependant laissée aux mains de ces acteurs, la FSMA ayant juste émis une circulaire expliquant à ces entités comment implanter ce système interne de la meilleure manière possible. Il y est simplement demandé d'instaurer ce canal de façon proportionnelle, la personne responsable de ce dernier pouvant varier en fonction des tâches, de la taille ou d'autres spécificités de l'entreprise⁶³. Il faut de plus souligner que le régime de protection détaillé en longueur dans l'article 69bis concernant la dénonciation faite à la FSMA ne s'applique pas ici, chaque institution ayant son propre régime de protection.⁶⁴ De ce fait, à partir du moment où aucune obligation de subsidiarité n'est établie, il est difficile de comprendre pourquoi un employé choisirait cette procédure interne, dont le mécanisme est peu clair ainsi que potentiellement inefficace et qui n'assure pas une protection efficiente, au lieu d'aller porter l'infraction directement à l'attention de la FSMA (si on excepte bien sûr le potentiel nombre non négligeable de demandes que la FSMA se doit de traiter). Il serait opportun d'établir un régime de dénonciation interne commun pour toutes les organisations concernées ; espérons que la transposition de la directive qui nous occupe ici aura cet effet.

Dans une autre procédure, la possibilité est ouverte pour un dirigeant, membre du personnel, représentant ou distributeur d'une entité assujettie de transmettre des informations ou des soupçons relatifs au blanchiment de capitaux ou au financement du terrorisme à la Cellule de traitement des informations financières (ou plus simplement CTIF), lorsque les entités concernées ne transmettent pas elles-mêmes ces soupçons ou informations.⁶⁵ Il est également demandé dans le même cadre à certaines « *autorités de contrôle* » ainsi qu'à des « *entités assujetties* » déterminées de mettre en place des mécanismes permettant aux mêmes personnes visées plus haut, ainsi qu'à tout tiers, de signaler une infraction aux règles concernant le blanchiment des capitaux, le financement du terrorisme, le transfert de fonds ou encore les embargos financiers⁶⁶.

Terminons ce tour d'horizon national en mentionnant la transposition de la directive secrets d'affaires, évoquée lors de la première sous-section, qui a été insérée dans l'ordre juridique

⁶¹ Loi du 2 août 2002, article 45.

⁶² Loi du 2 août 2002, article 69 ter.

⁶³ Circ. FSMA_2017_21 du 24 novembre 2017 relative aux procédures internes appropriées permettant le signalement d'infractions

⁶⁴ S.COOLS, « Klokkenluiden bij de FSMA en de Nationale Bank », *TVR-RPS*, 2018, p.666 et pp.674-675.

⁶⁵ Loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces, articles 47 et 49, *M.B.*, 16 octobre 2017, p.90838.

⁶⁶ Loi du 18 septembre 2017, articles 9 ; 10 ; 36 ; et 90.

belge par une loi du 30 juillet 2018. Alors qu'il était possible pour le législateur d'instaurer un régime plus protecteur à l'égard des lanceurs d'alerte lors de la transposition des exclusions et des dérogations de la directive (incluant enfin une protection générale s'étendant au secteur privé), celui-ci préféra tout simplement reprendre la formulation exacte du législateur européen quant à ces exceptions au sein du Code de droit économique.⁶⁷ Cette occasion manquée pourrait être expliquée par l'envie du législateur belge d'attendre l'adoption finale et l'obligation de transposition du texte européen portant sur la protection des lanceurs d'alerte (la proposition de directive étant sortie en avril de cette même année) avant de commencer à légiférer plus largement sur le sujet.⁶⁸

Notons finalement comme dernier indice pertinent de la protection très insuffisante des lanceurs d'alerte en Belgique que le terme même de « lanceur d'alerte » n'a jamais été défini au sein d'une législation nationale ou même européenne.

Chapitre 2- La directive 2019/1937 sur la protection des personnes qui signalent des violations du droit de l'Union

Section 1- Historique

L'idée d'un texte européen assurant une protection moins fragmentée et plus claire des lanceurs d'alerte flottait dans l'air depuis un certain temps. Ainsi, de 2011 à 2015, le Parlement a émis trois résolutions demandant à la Commission de se pencher sur la question d'une législation portant sur les lanceurs d'alerte, d'abord de manière sectorielle puis générale. Ces dernières n'eurent cependant aucun effet, la Commission n'ayant nullement examiné à cette époque la possibilité d'adopter de tels textes.⁶⁹

Il faudra attendre la sortie de la directive secrets d'affaires pour que le processus législatif commence tout doucement à réellement se mettre en route : on observe une première prise de position de la Commission qui évoque un besoin de protection dans deux de ses documents

⁶⁷ Loi du 30 juillet 2018 relative à la protection des secrets d'affaires, article 6, 1 et 2° ; 7 §2 ; et 9, 1°, 2° et 4° M.B, 14 août 2018, p.64854 ; Code de droit économique, art. XI.332/2, 1° et 2° ; XI.332/3, §2 ; et XI. 332/5, 1°, 2° et 4°.

⁶⁸ V. CASSIERS, « La transposition de la Directive 2016/943/UE du 8 juin 2016 sur la protection des secrets d'affaires en droit belge » in *Droit de la propriété intellectuelle* (sous la coordination de N.BERTHOLD et AL.), Bruxelles, Larcier, 2019, pp.293 et 318.

⁶⁹ D. KAFTERANIS, "The role of the European Parliament in the adoption of the directive on the protection of whistle-blowers", *RAE*, 2020, pp.906-907.

(respectivement une communication portant sur la lutte contre la fraude fiscale⁷⁰ et son plan de travail pour l'année 2017⁷¹) mais le véritable coup d'envoi vers une législation européenne globale est donné par le Parlement en 2017 avec une résolution adoptée le 14 février (ainsi que par un rapport rédigé quelques mois plus tard⁷²). Il est possible de considérer cette résolution comme étant une réponse directe aux inquiétudes mentionnées dans le premier chapitre quant à la directive 2016/943 ; il est en effet dit à son point R que « *la protection des lanceurs d'alerte dans l'Union est une question de plus en plus pressante, dans la mesure où la directive sur le secret des affaires limite les droits des lanceurs d'alerte et peut donc avoir un effet dissuasif non souhaité sur ceux qui veulent signaler des irrégularités liées au financement de l'Union dont certaines entreprises ont pu bénéficier* ». C'est surtout dans sa demande à la Commission que cette résolution attire l'attention : en plus de solliciter cette dernière de mettre en place pour la fin de l'année 2017 une législation protectrice des lanceurs d'alerte dans le domaine de la fraude contre les intérêts financiers de l'Union, elle appelle cette institution « *à présenter sans délai une proposition législative visant à mettre en place un programme européen efficace et complet pour protéger les lanceurs d'alerte* »⁷³.

Cette fois-ci, la requête du Parlement sera bel et bien prise en compte par la Commission qui déposera, le 23 avril 2018, la proposition de directive sur la protection des personnes dénonçant les infractions au droit de l'Union⁷⁴ qui aboutira, après maintes discussions et amendements (on en dénombre en effet 665 !)⁷⁵ au texte final de la directive « *sur la protection des personnes qui signalent des violations du droit de l'Union* », ⁷⁶ adopté en procédure législative ordinaire le 23 octobre 2019 et entré en vigueur le 16 décembre de cette même année.⁷⁷

Le texte étant une directive, sa raison d'être est donc d'harmoniser les textes existants sur cette matière dans les différents États membres afin d'atteindre son objectif « *d'un niveau élevé de*

⁷⁰ Communication de la Commission au Parlement européen et au Conseil sur d'autres mesures visant à renforcer la transparence et la lutte contre la fraude et l'évasion fiscale, C.O.M. (216) 451 final.

⁷¹ Programme de travail de la Commission pour 2017, Répondre aux attentes – Pour une Europe qui protège, donne les moyens d'agir et défend, C.O.M. (2016) 710 final.

⁷² Rapport 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'organisme public (Rapp : V.ROZIERE), P.E Doc, A8-0295/2017 du 10 octobre 2017 ; J.VALLET-PAMAR, « Genève de la directive protégeant les lanceurs d'alerte », RAE, 2019, p.689.

⁷³ Résolution du Parlement européen sur le rôle des lanceurs d'alerte dans la protection des intérêts financiers de l'Union européenne, J.O.U.E., C252 du 18 juillet 2018, pp.58 et 59.

⁷⁴ Proposition de directive du Parlement européen et du Conseil du 23 avril 2018 sur la protection des personnes dénonçant les infractions au droit de l'Union, C.O.M. (2018) 218 final.

⁷⁵ J.VALLET-PAMAR, *op.cit.*, p.689.

⁷⁶ Les références sur les différents textes des institutions européennes menant à cette directive ont été trouvés dans J.VALLET-PAMAR, *op.cit.*, pp.683-689.

⁷⁷ Directive (UE) 2019/1937, article 28 ; <https://eur-lex.europa.eu/legal-content/FR/HIS/?uri=CELEX:32019L1937> (consulté le 14/05/2021).

protection des personnes signalant des violations du droit de l'Union »⁷⁸. On est ici en présence d'une directive d'intensité minimale, laissant ainsi une discrétion aux législateurs nationaux dans la transposition des normes qui servent plutôt de balises générales. Cela est démontré de manière incontestable par les termes employés dans les deux premiers articles parlant de « *normes minimales communes* », ⁷⁹ ainsi que par l'article 25 qui précise cependant que le législateur national ne peut utiliser sa marge de manœuvre que dans un sens plus favorable pour le lanceur d'alerte.⁸⁰

Section 2 – Champ d'application

Sous-section 1 – Champ d'application matériel

§1. Matières concernées par la directive

Le champ d'application matériel de la directive est en réalité résumé grossièrement par son titre, qui émet l'idée que ce dernier porte uniquement sur des « *violations du droit de l'Union* ». Cependant, nous ne pouvons de toute évidence nous arrêter là et il faut préciser chaque mot de cet énoncé.

En premier lieu, les « *violations* ». Le terme peut paraître très simple, tout un chacun sachant que ce dernier désigne une transgression directe des préceptes énoncés par une loi. Le législateur européen fait toutefois également rentrer dans cette notion les « *pratiques abusives* », un terme dégagé par la Cour de Luxembourg⁸¹ désignant des actes qui, sans aller transgresser directement les normes légales, « *vont à l'encontre de l'objet ou de la finalité de la loi* ». ⁸² En outre, il n'y a pas d'obligation que les violations en question se soient déjà produites, mais il faut néanmoins que leur survenance soit très probable.⁸³

Le terme suivant « *du droit de l'Union* » mérite une analyse plus fouillée, étant donné que, contrairement à ce que cet énoncé général laisse supposer, la directive ne s'occupe pas du droit de l'Union en général mais bien des matières spécifiques visées au second article.

⁷⁸ Directive (UE) 2019/1937, article 1.

⁷⁹ Directive (UE) 2019/1937, articles 1 et 2, §1.

⁸⁰ Directive (UE) 2019/1937, article 25.

⁸¹ Arrêt Centros, C-212/97, :EU :C :1999 :26.

⁸² Directive (UE) 2019/1937, considérant 42 et article 5, 1°, ii).

⁸³ Directive (UE) 2019/1937, considérant 43.

Suivant le point a) de cet article, toute dénonciation de violation de normes reliées à dix domaines précis est ainsi concernée par le texte de la présente directive. Ces domaines en question regroupent : « *les marchés publics ; les services, produits et marchés financiers et prévention du blanchiment des capitaux et financement du terrorisme ; la sécurité et conformité des produits ; la sécurité des transports ; la protection de l'environnement ; la radioprotection et sécurité nucléaire ; la sécurité des aliments destinés à l'alimentation humaine et animale, santé et bien-être des animaux ; la santé publique ; la protection des consommateurs ; la protection de la vie privée et des données à caractère personnel, et sécurité des réseaux et des systèmes d'information* »⁸⁴. Toutefois, le texte ne se contente pas de simplement citer ces quelques matières générales et se montre bien plus précis en établissant, en première partie de l'annexe, la liste des normes sur lesquelles devra porter la violation dénoncée. Cette énumération de législations, déjà relativement très étoffée (on peut y compter approximativement plus de 120 textes), peut cependant se révéler encore plus longue qu'elle ne le semble : le considérant 19 précise en effet que fait également partie du champ d'application de la directive 2019/1937 les normes citées comme faisant partie du champ d'application matériel des textes présents dans l'annexe ; ainsi que « *les mesures d'exécution ou de délégation adoptées au niveau national ou de l'Union en application de ces actes* »⁸⁵. À titre d'exemple, la directive 2019/1937 cite comme faisant partie de son champ d'application matériel la directive 2008/99/EC relative à la protection de l'environnement par le droit pénal ; cette dernière établit en annexe plus d'une septantaine de textes dont la violation rentre dans son champ d'application matériel⁸⁶. Par voie de conséquence, tous ces textes peuvent être considérés comme rentrant dans le champ d'application de la directive 2019/1937.

Une autre précision apportée par le même considérant 19 est que la liste présente en annexe est à considérer comme étant une liste « *dynamique* », devant faire référence au nouvel acte si la norme référencée a été supprimée ou modifiée.⁸⁷ Enfin, il faut évidemment garder en tête que cette annexe est amenée à évoluer, comme le précise par ailleurs le considérant 107 qui va un pas plus loin en précisant que, lorsqu'un nouvel acte s'inscrivant dans l'un des dix domaines mentionnés est adopté, l'annexe est non seulement amendée (ce qui peut paraître assez logique

⁸⁴ Directive (UE) 2019/1937, article 2 §1, a).

⁸⁵ Directive (UE) 2019/1937, considérant 19.

⁸⁶ Directive 2008/99/CE du Parlement européen et du Conseil du 19 novembre 2008 relative à la protection de l'environnement par le droit pénal, article 2 renvoyant à l'annexe A et B, *J.O.U.E.*, 6 décembre 2018, L328, p.29 et pp.32-36.

⁸⁷ Directive 2019 /1937, considérant 19.

et même élémentaire) mais la nouvelle législation elle-même se devra de préciser dans son texte que la directive 2019/1937 s'applique pour ce dernier.⁸⁸

En conséquence, si le fait que le lanceur d'alerte ne pourrait être protégé que si l'infraction dénoncée violait une norme dans une liste définie pouvait inquiéter quant à l'effectivité de la portée de cette nouvelle directive, la longueur de cette première partie de l'annexe et les précisions apportées par ce considérant s'avère être des éléments rassurants. On peut de même plaider que cette liste introduit une certaine sécurité juridique, la personne concernée sachant exactement si l'information dévoilée porte sur une matière qui lui permettra de bénéficier- ou non- de la protection européenne. Cependant, ce renvoi à cette longue annexe (qui n'est pas entièrement complète comme démontré ci-dessus et qui se devra d'être analysée au vu des autres textes contenus dans les champs d'application des réglementations citées dans l'annexe) nuit quelque peu à la lisibilité du texte, et en ce sens réduit cette même sécurité juridique : s'il peut être relativement aisé pour le juriste expérimenté de retrouver immédiatement le texte concerné, on peut arguer que le non-initié est susceptible de facilement se perdre dans cette annexe.

Le point b) et c) de ce même article, bien qu'étant également assez ciblés, sont quelque peu plus généraux. Rentrent ainsi également dans le champ d'application matériel les dénonciations portant sur des « *violations portant atteinte aux intérêts financiers de l'Union visés à l'article 325 du traité sur le fonctionnement de l'Union européenne et précisés dans les mesures pertinentes de l'Union* » ainsi que celles portant sur des « *violations relatives au marché intérieur visé à l'article 26, paragraphe 2, du traité sur le fonctionnement de l'Union européenne, y compris les violations des règles de l'Union en matière de concurrence et d'aides d'État, ainsi que les violations relatives au marché intérieur en ce qui concerne les actes qui violent les règles applicables en matière d'impôt sur les sociétés ou les dispositifs destinés à obtenir un avantage fiscal qui va à l'encontre de l'objet ou de la finalité de la législation applicable en matière d'impôt sur les sociétés.* »⁸⁹ Il faut noter que cette dernière référence à toute infraction relative au marché intérieur pourrait avoir pour effet d'étendre considérablement le champ d'application de la directive, d'autant plus que les quelques exemples de violation des règles du marché intérieur sont bien précisés ne pas être donné à titre

⁸⁸ Directive 2019/1937, considérant 106.

⁸⁹ Directive 2019/1937, article 2, §1, b) et c).

exhaustif. L'Union européenne s'est en effet déjà emparée dans le passé de cette justification au demeurant assez large afin d'élargir ses compétences.⁹⁰

Si, conformément à notre objectif, ce tour d'horizon du champ d'application matériel sera le plus exhaustif possible au moment de la conclusion de ce mémoire, celui-ci est susceptible d'être élargi ultérieurement. Le considérant 106 rappelle cela en précisant qu'il est possible, sur base de l'application future de la directive, que de nouveaux domaines et/ou actes de l'Union soient rajoutés à son champ d'application.⁹¹ Par cette dernière affirmation, le législateur de l'Union montre encore une fois une volonté affichée de rendre ce texte de loi le plus protecteur possible et de faire en sorte que ce dernier puisse couvrir un maximum de domaines en sa qualité de texte protecteur global. Il reste évidemment à voir si cette déclaration ne constituera pas de simples vœux pieux et si le domaine d'application de cette directive sera véritablement étendu dans le futur.

Enfin, rappelons que ce champ d'application matériel pourrait très bien être élargi lors de la transposition à d'autres domaines non cités dans la directive du fait de son harmonisation à caractère minimal, tel que rappelé par le cinquième considérant.⁹² Un législateur national qui sera plus soucieux de créer ou de renforcer des règles pour les lanceurs d'alerte dans certains domaines et donc voulant établir un cadre plus uniforme ira rallonger le champ d'application matériel lors de la transposition de la directive ; tandis qu'un autre législateur ne partageant pas ce type de préoccupations se contentera de reprendre le champ d'application tel qu'établi par le texte européen (sous réserve d'éventuelles modifications effectuées par ce dernier à cette liste).

§2. Matières exclues par la directive

La directive va explicitement exclure plusieurs domaines de son champ d'application dans son article 3. Ainsi, certaines régulations européennes réglant déjà la situation des lanceurs sont exclues du champ d'application de la directive (de même que, assez logiquement, les textes d'exécution de ces lois sectorielles)⁹³. Ces normes sont établies dans la seconde partie de

⁹⁰ L'un des exemples les plus connus et les plus marquants à cet égard est l'utilisation de cet argument par la Cour de justice afin de valider l'intervention du législateur européen sur le domaine du tabac, et incidemment sur la lutte contre le tabagisme et le domaine de la santé. Sur cette question, voir : A.FOURREZ, "Complainte pour un fumeur – Réflexions à partir des arrêts de la Cour de Justice du 4 mai 2016 », *R.E.D.C.*, 2016, pp.89-92.

⁹¹ Directive 2019/1937, considérant 107.

⁹² Directive (UE) 2019/1937, considérant 5.

⁹³ Y. PACLOT et V.MAGNIER «Un nouveau champ de protection pour les lanceurs d'alerte », *RAE*, 2019, p.703 ; Directive (UE) 2019/1937, considérant 27 et article 3,§1.

l'annexe (portant sur les services, produits et marchés financiers ; la sécurité des transports et la protection de l'environnement) : on peut constater que ces dernières constituent la majorité des textes européens existants organisant une protection sectorielle des lanceurs d'alerte. Le considérant 23 précise en outre que le système de dénonciation à la destination des fonctionnaires européens continue à s'appliquer indépendamment de cette nouvelle directive.⁹⁴ Le législateur européen cherche donc à assurer une protection du lanceur d'alerte dans un maximum de domaines en comblant les vides laissés par les textes sectoriels plutôt qu'en cherchant une uniformisation maximale qui viendrait défaire ce qui a déjà été réalisé auparavant au niveau de l'Union.

La deuxième exclusion réalisée par ce troisième article concerne la sécurité nationale, et plus précisément la responsabilité et les intérêts des États attachés à cette dernière⁹⁵. Cette exception semble pour Julien Gaul assez floue, la responsabilité attachée à la sécurité nationale étant une obligation assez nouvelle. Les intérêts quant à eux pourraient se référer à l'article 346 TFUE, qui introduit notamment une discrétion laissée aux États dans la production et le commerce d'armes ou autre matériel de guerre⁹⁶ (d'où la référence aux « *marchés publics comportant des aspects touchant à la défense ou à la sécurité* » dans ce même article 3⁹⁷).

L'article 3 exclut finalement du champ d'application de la directive une série de domaines : « *la protection des informations classifiées, la protection du secret professionnel des avocats et du secret médical, le secret des délibérations judiciaires, les règles en matière de procédure pénale* » ainsi que certaines règles nationales du droit du travail⁹⁸. Cette exclusion n'a cependant rien de surprenant, étant donné que ces matières sont encore considérées comme faisant partie de la compétence souveraine des États membres.⁹⁹

Il est toutefois important de faire remarquer que, bien qu'il soit indiqué que les règles de la directive ne doivent pas s'appliquer pour ces domaines, il n'en sera pas forcément de même au niveau national. Comme énoncé plus haut, le caractère minimal de l'harmonisation autorise le législateur national à élargir le champ d'application de la directive¹⁰⁰ : rien ne l'empêche donc

⁹⁴ Directive (UE) 2019/1937, considérant 23.

⁹⁵ Directive (UE) 2019/1937, article 3, § 2.

⁹⁶ Traité sur le fonctionnement de l'Union européenne (version consolidée), article 346, *J.O.U.E.*, 26 octobre 2012, C326, p.194 ; J.GAUL, « Les lanceurs d'alerte et les répercussions pour les entreprises actives dans le domaine des marchés publics. Implications, critiques et réflexions », *Endroi*, 2020, pp. 228-229.

⁹⁷ Directive (UE) 2019/1937, article 3, §2.

⁹⁸ Directive (UE) 2019/1937, article 3, §3 et 4.

⁹⁹ Y. PACLOT et V.MAGNIER, *op.cit.*, p.703.

¹⁰⁰ Directive (UE) 2019/1937, article 2, §2.

d'aller inclure dans la loi de transposition ces quelques matières qui ont été exclues du texte européen.

Sous-section 2- Champ d'application personnel

§1. La personne signalant des violations du droit de l'Union

Tel qu'affirmé par le titre de la directive, le champ d'application personnel ne concerne pas à proprement parler les « lanceurs d'alerte » mais bien les « personnes qui signalent des violations du droit de l'Union ». Notons que le législateur européen s'est toujours montré frileux à utiliser ce terme de lanceur d'alerte au sein de ses législations. La raison pour cela n'est précisée nulle part dans la directive, certains ont émis l'hypothèse qu'il s'agirait d'une forme de déférence à l'égard des États membres, qui auraient de ce fait une plus grande liberté dans la définition de ce terme¹⁰¹. Suivant cette même logique, il peut également être pensé que cette absence résulte de la volonté de ne pas contrecarrer les descriptions déjà apportées par les droits nationaux.¹⁰²

En premier lieu, la personne doit logiquement fournir des informations concernant une (voire plusieurs) violation(s) d'une ou de plusieurs normes définies dans le champ d'application matériel de la directive. Un critère évident pour être reconnu comme rentrant dans le champ d'application personnel est que les informations dévoilées ne doivent pas déjà être connues de tout un chacun.¹⁰³

Cette divulgation ne suffira cependant pas pour enclencher la protection européenne : un certain nombre de conditions, établies aux articles 4 et 6 de la directive, se doivent également d'être respectées. Il faut en premier lieu appartenir à une des catégories établies à l'article 4, la première étant celle des « auteurs de signalement (...) qui ont obtenu des informations sur des violations dans un contexte professionnel », que ce dernier soit « dans le secteur privé ou public »¹⁰⁴. Ce groupe comprend tout aussi bien les travailleurs tel que compris par le droit européen et défini à de multiples reprises par la Cour de justice de l'Union européenne (« les personnes qui accomplissent, pendant un certain temps, en faveur d'une autre personne et sous

¹⁰¹ N. BOULALE MADDAINE, « La nouvelle directive 2019/1937 relative à la protection des « lanceurs d'alerte » : d'où elle vient, où elle va peut-être », *SK*, p.471

¹⁰² Par exemple, la définition française établie ici : Loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, article 6, *JORF*, 10 décembre 2016.

¹⁰³ Directive (UE) 2019/1937, considérant 43.

¹⁰⁴ Directive (UE) 2019/1937, article 4, §1.

la direction de celle-ci, des prestations en contrepartie desquelles elles touchent une rémunération »¹⁰⁵) que les indépendants, « les actionnaires et les membres de l'organe d'administration, de direction ou de surveillance d'une entreprise », « les bénévoles et les stagiaires » ainsi que « toute personne travaillant sous la supervision et la direction de contractants, de sous-traitants et de fournisseurs »¹⁰⁶. Il n'y a pas d'obligation que la situation professionnelle soit actuelle, l'article 4 précisant que le signalement peut porter sur des informations obtenues lors d'une activité professionnelle ayant pris fin au moment du lancement de l'alerte, voire sur des informations recueillies par le biais des formalités menant à un emploi¹⁰⁷. Toutes les situations au sein du secteur professionnel semblent ainsi englobées par cette définition, ce qui est bénéfique étant donné que certains lanceurs d'alerte « historiques » n'auraient pas pu rentrer dans la définition de « travailleur » telle qu'établie par la CJUE.¹⁰⁸

Le seul fait de divulguer des informations obtenues dans le cadre professionnel ne suffit cependant pas pour pouvoir bénéficier du système mis en place par le législateur européen : il faut de plus répondre aux conditions supplémentaires énoncées à l'article 6. Le premier critère est d'avoir des raisons de croire que l'information dévoilée est véridique. Cela ne veut pas pour autant dire que la personne doit prouver par tous les moyens la véracité de l'information avancée : il lui suffit de présenter « des préoccupations et des soupçons raisonnables ».¹⁰⁹ La seconde condition est d'avoir transmis cette information par les canaux de signalement prévus par la directive ou par divulgation publique dans certaines situations spécifiques¹¹⁰ : ces procédés seront plus longuement décrits dans le cadre de la prochaine section.

Il existe ensuite trois autres catégories de personnes pouvant bénéficier de la protection de la directive ici analysée : néanmoins, elles sont toutes définies par leur relation avec le divulgateur ayant eu connaissance des violations dans un cadre professionnel, ce qui signifie que ces individus ne peuvent lancer l'alerte par eux-mêmes. Ainsi, deux de ses catégories sont les « tiers qui sont en lien avec les auteurs de signalement et qui risquent de faire l'objet de représailles dans un contexte professionnel » ou encore les facilitateurs¹¹¹ (défini au sens de la directive comme étant « une personne physique qui aide un auteur de signalement au cours du

¹⁰⁵ Directive (UE) 2019/1937, considérant 38 ; Arrêt Lawrie Blum/ Land Baden-Württemberg, C-66/85, :EU :C :1986 :24

¹⁰⁶ Directive (UE) 2019/1937, article 4, §1.

¹⁰⁷ Directive (UE) 2019/1937, article 4, §2 et §3.

¹⁰⁸ A. LACHAPPELLE, *La dénonciation à l'ère des lanceurs d'alerte fiscale*, Larcier, Bruxelles, 2021, p.805.

¹⁰⁹ Directive (UE) 2019/1937, considérant 43.

¹¹⁰ Directive (UE) 2019/1937, article 6, §1.

¹¹¹ Directive (UE) 2019/1937, article 4, §4, a) et b).

processus de signalement dans un contexte professionnel et dont l'aide devrait être confidentielle »).¹¹² Les deux notions se confondent ici, un « facilitateur » pourrait être considéré comme un « tiers » ayant des liens avec l'auteur et courant certains risques de répercussions sur le plan professionnel (et vice-versa, un tiers pourrait être considéré comme étant facilitateur). Une piste apportée par Amélie Lachapelle afin de distinguer les deux notions serait d'apprécier le fait que la personne ait aidé le lanceur dans le dévoilement de la violation à la norme européenne (par une complicité lors de vol de documents par exemple) : tel individu sera considéré comme étant un facilitateur. À l'inverse, une personne n'ayant eu aucun rôle dans l'alerte mais subissant tout de même certaines persécutions professionnelles à la suite de cette dernière sera plutôt réputée comme faisant partie de la catégorie des « tiers »¹¹³ : on pourrait imaginer qu'il puisse s'agir du mari de l'auteure du signalement travaillant dans la même entreprise que son épouse (ou dans une filiale de cette dernière) et qui fait l'objet d'une réduction de son salaire par vengeance de son employeur du fait des actes de sa conjointe, alors même qu'il n'a aucunement contribué à ces derniers. Des exemples de tiers en lien ou de facilitateur sont donnés par la directive même : cela peut ainsi être des collègues, des proches de manière générale ainsi que les représentants syndicaux¹¹⁴.

La dernière catégorie représente uniquement des personnes morales : il s'agit des « *entités juridiques appartenant aux auteurs de signalement ou pour lesquelles ils travaillent, ou encore avec lesquelles ils sont en lien dans un contexte professionnel.* »¹¹⁵ La raison de l'inclusion de cette dernière catégorie s'explique par le fait que malgré qu'une personne morale ne peut, pour des raisons évidentes, par elle-même lancer l'alerte ou même faciliter la divulgation, elle peut cependant également être visée par d'éventuelles représailles¹¹⁶ (« *refus de fournir des services, la mise sur liste noire ou le boycottage d'affaires* »).¹¹⁷

¹¹² Directive (UE) 2019/1937, article 5, 8).

¹¹³ A. LACHAPELLE, « And thus Tax whistleblowing was born! Comment on the Directive on whistleblowers in tax matters », *TFR*, 2020, p.802.

¹¹⁴ Directive (UE) 2019/1937, considérant 41 et article 4, §4, b).

¹¹⁵ Directive (UE) 2019/1937, article 4, §1, c).

¹¹⁶ J. GAUL., *op.cit.*, p.248.

¹¹⁷ Directive (UE) 2019/1937, considérant 41.

§2. Exclusions du champ d'application personnel

Du fait de l'exclusion du champ d'application matériel de « *la protection du secret professionnel des avocats et du secret médical* »¹¹⁸, les avocats et les travailleurs médicaux sont de facto exclus du champ d'application personnel de la directive en ce qui concerne les violations apprises dans le cadre d'une relation avec un client ou un patient. En revanche, toute autre personne tenue à une obligation légale similaire du fait de sa profession pourra être considérée comme lanceur d'alerte tel que défini au sens européen, sans que lui soit opposée cette exigence de secret professionnel.¹¹⁹ De plus, l'avocat et le médecin pourraient être bénéficiaires de la protection européenne s'ils ont connaissance de la violation en question dans leur cadre de leur travail mais dans des circonstances n'impliquant pas le secret professionnel.¹²⁰

En outre, il semble assez évident que les personnes divulguant une information obtenue dans un environnement purement privé en dehors de tout « *contexte professionnel* » ne sauraient être incluses dans le champ d'application personnel. On peut se demander ce qui peut expliquer ce rejet : il est certes plus difficile d'obtenir des informations sur des violations comprises dans le champ d'application matériel de la directive en dehors d'un contexte professionnel mais cela n'est pas pour autant complètement inconcevable. Il a par ailleurs déjà été démontré que nombreuses dénonciations dans des domaines aussi variés que des infractions sociales ou encore pénales émanaient de personnes extérieures à ces secteurs¹²¹. La directive évoque le fait que les travailleurs au sens large ont un besoin de protection que n'a pas le « citoyen ordinaire » qui tomberait par hasard sur les mêmes informations du fait que la première catégorie de personnes encourrait plus de risques du fait de leur relation déséquilibrée économiquement parlant avec leurs supérieurs¹²². Nous n'adhérons cependant pas totalement à cette explication : certes, la plupart des sanctions dans ce type de situation trouvent leurs sources dans la relation de travail. Cependant, des représailles en dehors de tout cadre professionnel peuvent également être envisagées : par exemple, des poursuites judiciaires pour vol de documents ou des atteintes à la réputation, qui se verraient plus vite réglées ou même évitées si le tiers pouvait bénéficier des mesures de protection.

¹¹⁸ Directive (UE) 2019/1937, article 3, § 3, a).

¹¹⁹ J.GAUL, *op.cit.*, pp. 229-230.

¹²⁰ A. LACHAPELLE., 2021, *op.cit.*, pp.818-819.

¹²¹ A. LACHAPELLE, « L'encadrement juridique du lanceur d'alerte au sein de l'Union européenne. Commentaire de la directive sur les lanceurs d'alerte », *RDTI*, 2020, p.23.

¹²² Directive (UE) 2019/1937, considérant 36.

Peut-être est-ce le côté personnel et un peu mesquin de la dénonciation privée qui explique mieux cette exclusion : l'information est dans ces situations souvent dévoilée plus dans une optique de vengeance personnelle que de véritable protection des intérêts publics.¹²³ On verrait dans ce cas ressortir, par le biais de la *ratio legis*, l'influence de la Cour européenne des droits de l'Homme qui prend en compte l'intention du lanceur d'alerte.

§3. Comparaisons avec la définition de la Cour européenne des droits de l'Homme

La transposition de ce texte européen dans les États membres aura très probablement un certain impact sur la Cour européenne des droits de l'Homme, qui jusqu'ici pouvait servir de « filet de protection » pour les lanceurs d'alerte dépourvus de toute protection légale nationale ; ces derniers pouvant utiliser la jurisprudence de la Cour devant les tribunaux de leurs pays ou, dans des cas extrêmes, se rendre à Strasbourg. À présent, du fait du nombre de matières couvert par la directive et de la possibilité du législateur d'aller inclure des domaines supplémentaires dans sa transposition nationale, la Cour ne jouera un rôle que dans les cas assez limités où l'information concernée ne rentre pas dans le champ d'application matériel européen. En revanche, si le lanceur d'alerte ne répond pas à un des critères établis pour rentrer dans le champ d'application personnel de la directive, ce dernier se retrouvera complètement dépourvu de protection et ne saura se diriger vers la juridiction strasbourgeoise, les conditions établies par cette dernière pour la protection de cette catégorie d'individus étant plus strictes que celles dressées par le texte européen. Pourtant, les institutions européennes affirment s'être inspirées de la jurisprudence de la Cour européenne¹²⁴ et certains éléments de la définition de la directive reflètent celle de cette instance internationale : on y retrouve ainsi le fait que le lanceur doit avoir eu connaissance de l'information dans le cadre de son travail, qui peut également être défini de manière très large¹²⁵, ainsi que l'exigence que le lanceur ait la conviction de croire que son alerte porte sur un fait véridique. Enfin, la suite de la directive précise bien que le régime européen prévoit également une divulgation publique en dernier recours¹²⁶.

Pour autant, la juridiction internationale a une conception plus restreinte que celle retenue par la directive : la possibilité que des personnes autres que le travailleur dévoilant l'information

¹²³ A. LACHAPELLE, *RDTI*, *op.cit.*, pp.22-23.

¹²⁴ Directive (UE) 2019/1937, considérant 31.

¹²⁵ Q. VAN ENIS, « Une solide protection des sources journalistiques et des lanceurs d'alerte : une impérieuse nécessité à l'ère dite de vérité ? » in *Le secret*, Limal, Anthemis, 2017, p.124.

¹²⁶ Directive (UE) 2019/1937, article 15.

puissent bénéficier de la même protection n'a jamais été retenue, et le préjudice des personnes concernées ainsi que le degré de sévérité des éventuelles répercussions menaçant le lanceur sont également pris en compte, ce qui n'est pas évoqué dans le texte européen. Concernant l'intention du lanceur d'alerte, le texte de la directive ne semble pas, à première vue, prendre ce dernier critère en compte : cependant, le considérant 30 exclut bel et bien les individus agissants « *en échange d'une récompense ou d'une indemnisation* » pour autant toutefois que ces derniers soient « *identifiés comme informateurs ou enregistrés comme tels dans des bases de données gérées par des autorités désignées au niveau national, telles que les autorités douanières* »¹²⁷. Les implications de cette dernière phrase demeurent pour l'instant assez floues, et la formulation au conditionnel de cette possibilité d'exclusion (« *La présente directive ne devrait pas s'appliquer...* ») laisse penser que les États membres pourront décider de ne pas se pencher sur les revendications pécuniaires du lanceur d'alerte.¹²⁸ Si l'on excepte cependant cette dernière considération, au demeurant peu claire, le législateur européen ne se montre pas aussi strict que la Cour européenne qui considère qu'« *un acte motivé par un grief personnel ou un antagonisme personnel ou l'attente d'un avantage personnel, tel qu'un gain pécunier, ne saurait justifier un niveau particulièrement élevé de protection* ». ¹²⁹

Si la situation immédiate suivant la transposition de la directive peut résulter en un rôle réduit pour la Cour régionale, il est tout autant possible que cette dernière revoie sa jurisprudence en prenant en compte les critères retenus par le texte européen. Tout comme ce dernier évoque une inspiration tirée de la jurisprudence strasbourgeoise, les juges de cette même juridiction ont également par le passé été reprendre des idées initialement émises par l'Union européenne.¹³⁰ La Cour pourrait donc être tentée de se calquer sur la définition proposée par la directive, voire même d'être encore plus souple que cette dernière afin de servir de « filet de protection » pour les personnes ne pouvant bénéficier des dispositions européennes. Ainsi, à l'heure où la rédaction de ce mémoire se finit, deux juges dissidents s'exprimant dans l'arrêt Halet ont déjà demandé à revoir les critères de l'évaluation de la Cour au regard du texte européen¹³¹.

¹²⁷ Directive (UE) 2019/1937, considérant 30.

¹²⁸ A. LACHAPPELLE, 2021, *op.cit.*, p.812 ; Directive (UE) 2019/1937, considérant 30.

¹²⁹ Arrêt Matúz c. Hongrie (traduction libre).

¹³⁰ D. DERO-BUGNY, *Les rapports entre la Cour de justice de l'Union européenne et la Cour européenne des droits de l'homme*, Bruxelles, Bruylant, 2015, pp. 34-40.

¹³¹ Arrêt Halet c. Luxembourg.

Section 3 – Procédures à suivre

Sous-section 1 – Le signalement interne

Le signalement interne, ainsi que le laisse aisément penser son nom, désigne la procédure de divulgation d'informations devant être mise en place au sein même des entités privées et publiques. Comme le démontre la première phrase de l'article 7 (« *En règle générale (...) les informations peuvent être signalées par le biais des canaux et procédures de signalement interne* »), ce type de signalement a été pensé comme étant le mode « traditionnel » de divulgation, devant de préférence être utilisé en premier lieu avant de pouvoir se tourner vers le signalement externe.¹³² Les considérants justifient cette perspective par le fait qu'il serait plus opportun d'informer les personnes près de la source du problème, qui seraient également les plus aptes à solutionner ce dernier efficacement. Il y est de plus expliqué que des études ont démontré que la plupart des lanceurs d'alerte ont en premier lieu choisi d'aller porter les informations qu'ils détenaient au sein de l'entité concernée.¹³³ On peut cependant penser qu'il existe une autre raison sous-tendant la mise en avant du signalement interne comme procédure « par défaut », qui est la négociation serrée portant sur la hiérarchie des deux modes de divulgation. En effet, l'Allemagne, l'Autriche, la France ainsi que l'Italie voulaient que le recours aux canaux de divulgation externes puisse se faire uniquement qu'après l'usage des procédures internes. Dans cette optique, si le lanceur d'alerte décidait d'ignorer cette règle et de tout de même faire immédiatement circuler l'information par le biais des canaux externes, il perdrait toute protection et pourrait être poursuivi. Ce faisant, le mécanisme européen aurait reflété le système mis en place en France par la loi Sapin 2.¹³⁴ Si le texte final n'a pas retenu ce critère de conditionnalité, on peut observer que les demandes de ces pays ont tout de même eu un impact sur la manière dont la directive envisage le fonctionnement des canaux.

Ces procédures internes devront ainsi être prévues dans chaque entité privée employant plus de 49 travailleurs (bien que plusieurs entités ont la possibilité de diviser entre elles les ressources quant à plusieurs critères de cette procédure), sauf si l'État membre en décide autrement en élargissant, après communication à la Commission, cette obligation à certaines (voire à toutes) les entités comptant 49 travailleurs ou moins. De plus, les entités privées, quelle que soit leur taille, se doivent d'établir ces canaux de signalement si elles sont impliquées dans des affaires relatives à la sécurité des transports, à la protection de l'environnement ou encore aux services,

¹³² Directive (UE) 2019/1937, article 7, §1 et § 2.

¹³³ Directive (UE) 2019/1937, considérant 33 et 47.

¹³⁴ J.VALLET-PAMAR, *op.cit.*, pp.696-697 ; Loi n°2016-1691 du 9 décembre 2016, article 8.

produits et marchés financiers ainsi qu'à la prévention du blanchiment de capitaux et du financement du terrorisme.¹³⁵

Pour ce qui est des entités émanant du secteur public, elles se doivent toutes par défaut de mettre en place ces canaux de signalement ; le choix revient aux États membres de dispenser de cette obligation certains établissements (à savoir les entités employant moins de 50 travailleurs, ou encore les administrations communales lorsque moins de 50 personnes y travaillent ou lorsque moins de 10 000 personnes habitent la commune en question). Il est également possible pour les États membres d'admettre que les administrations communales se partagent un même canal « *pour autant que les canaux de signalement interne partagés soient distincts et indépendants des canaux de signalement externe* ». ¹³⁶

La directive précise une série de critères que devront respecter ces canaux de signalement : ceux-ci doivent au moins prévoir un individu ou service impartial en charge de la procédure (ou plusieurs individus/services assurant chacun une partie de la procédure). Cette personne/service peut toutefois être un tiers extérieur à l'entité¹³⁷, à la condition qu'il réponde aux conditions que doivent remplir les canaux internes. La directive donne, dans ses considérants, certains exemples de tiers pouvant s'occuper de la procédure interne¹³⁸ ; parmi ces derniers, on retrouve « *des fournisseurs de plateformes de signalement externe* ». ¹³⁹ Le même service pourrait donc hypothétiquement se retrouver responsable tant du canal interne qu'externe. Ce dernier point nous semble discutable : n'y aurait-il pas alors un risque de surcharge des divulgations adressées à l'autorité en charge du canal externe ? Qu'en est-il de plus des avantages de la procédure interne avancés par le législateur européen (personnes à la source pouvant solutionner plus efficacement le problème, facilité pour les lanceurs d'alerte) ? Des questions pratiques se posent également : une distinction sera-t-elle faite entre les deux types de procédures ou est-ce uniquement exigé pour les communes, comme le laisse penser le texte ? Un individu dont l'allégation est rejetée au stade de la divulgation interne aura-t-il la possibilité de porter la même information au même service mais cette fois au titre de canal externe ? Le cas échéant, il faudra s'interroger sur la pertinence de séparer les deux types de procédures dans cette hypothèse.

¹³⁵ Directive (UE) 2019/1937, article 8, § 3 et §4 ; §6 à 8.

¹³⁶ Directive (UE) 2019/1937, article 8, §9.

¹³⁷ Directive (UE) 2019/1937, article 8, § 5.

¹³⁸ Pourront également être en charge de la procédure interne « *des conseils externes, des auditeurs, des représentants syndicaux ou des représentants des travailleurs* ». Directive (UE) 2019/1937, considérant 54.

¹³⁹ Directive (UE) 2019/1937, considérant 54.

Les autres conditions constituent en « *la mise à disposition d'informations claires et facilement accessibles* », un « *suivi diligent* »¹⁴⁰, un accusé de réception devant être envoyé dans les 7 jours suivant signalement et un « *retour d'information* »¹⁴¹ à l'auteur du signalement devant intervenir endéans les 3 mois suivant l'accusé de réception¹⁴². Pour ce qui est du modèle du canal de signalement, les entités ont l'obligation de prévoir soit une dénonciation par écrit, soit par oral (ou les deux). Si les entités optent pour une procédure de dénonciation par écrit, celle-ci pourra se faire par le biais de courrier et/ou d'une plateforme électronique ; si elles optent pour une procédure par oral, celle-ci devra se faire par une rencontre en personne et via téléphone ou tout autre système de messagerie.¹⁴³

Sous-section 2 – Le signalement externe

La procédure externe est donc logiquement le signalement qui sera exercé en dehors de l'entité concernée, auprès d'une autorité qui sera désignée par l'État membre¹⁴⁴. L'autorité en question pourra être « *une autorité judiciaire, un organisme de réglementation ou de surveillance compétent dans les domaines spécifiques concernés, ou une autorité dotée de compétences plus générales à un niveau central au sein d'un État membre, des services répressifs, des organismes de lutte contre la corruption ou des médiateurs.* »¹⁴⁵ L'État membre dispose donc également d'une certaine marge d'appréciation dans la mise en place de ces canaux externes, pouvant désigner l'entité de son choix qui aura le rôle de l'autorité en charge de la procédure. Cette liberté est toutefois plus balisée que dans le cadre de la divulgation interne, à commencer par la façon dont la divulgation est effectuée : le canal externe se doit en effet de mettre en place des procédés de communication d'informations tant par écrit qu'oralement, là où un choix entre les deux modes de dénonciations était laissé à l'appréciation des entités chargées du canal interne. Une possibilité de rencontre en personne doit également toujours être prévue.¹⁴⁶

¹⁴⁰ Ce dernier étant laissé relativement libre, comprenant les moyens utilisés par l'autorité pour décider de la véracité d'une information et de méthodes pour remédier à l'éventuelle violation, qui peuvent constituer en « *une enquête interne, une enquête, des poursuites, une action en recouvrement de fonds, ou la clôture de la procédure* ». Directive 2019/1937, article 5, 12).

¹⁴¹ Défini comme étant : « *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* ». Directive 2019/1937, article 5, 13).

¹⁴² Directive (UE) 2019/1937, article 9, §1, b) et d) à g).

¹⁴³ Directive (UE) 2019/1937, considérant 53 et article 9, §2.

¹⁴⁴ Directive (UE) 2019/1937, article 11, §1.

¹⁴⁵ Directive (UE) 2019/1937, considérant 64.

¹⁴⁶ Directive (UE) 2019/1937, article 12, §2.

D'autres critères imposés sont en premier lieu les mêmes que pour les canaux internes (accusé de réception, retour d'information...). Le délai pour le retour d'information pourra ici être porté à 6 mois dans des situations justifiées¹⁴⁷. Le texte précise qu'il convient de définir une division des tâches entre les différents membres composant l'autorité, désignant des responsables devant traiter les allégations de violation ou encore ceux formés pour la communication avec le lanceur d'alerte. Seuls les membres autorisés auront de plus le droit d'accéder aux informations communiquées (une condition essentielle pour que l'autorité soit considérée comme étant indépendante et autonome). Si un travailleur non autorisé ou toute autre personne tierce arrive à tout de même avoir connaissance d'une information divulguée, l'autorité doit tout mettre en œuvre pour qu'il ne soit pas porté atteinte à la confidentialité de l'identité de l'auteur du signalement et pour que la procédure puisse le plus vite possible reprendre son cours normal.¹⁴⁸ D'autres critères additionnels que doit présenter ce type de signalement sont les obligations de transmettre au lanceur d'alerte les conclusions de l'enquête ayant découlé de l'information communiquée, d'envoyer ces mêmes informations aux institutions européennes compétentes dans certaines situations spécifiques prévues par la loi et d'établir un site internet contenant toute une série d'informations relatives à la procédure.¹⁴⁹

La directive met cependant en place quelques possibilités de souplesses pouvant être instaurées au sein de la procédure. Ainsi, les États membres pourront prévoir que l'autorité puisse rejeter les informations concernant des violations de moindre importance (ce qui n'enlève cependant pas la protection européenne au lanceur d'alerte concerné) ainsi que les « *signalements répétitifs qui ne contiennent aucune nouvelle information significative sur des violations par rapport à un signalement antérieur* » : en l'absence de précision, le lanceur dans ce cas ne pourra bénéficier de la protection européenne, certainement du fait du caractère connu de l'information. Enfin, dans des situations où l'autorité se retrouve submergée par les divulgations, il est possible que l'État membre autorise cette dernière à traiter les allégations de violations les plus graves en premier lieu et à ignorer le délai de réponse requis par les balises mises en place par ce même texte européen¹⁵⁰. Avec ces assouplissements, le législateur européen prend également en compte le fait que ces autorités puissent être rapidement débordées par une quantité considérable d'allégations diverses, et permet donc un déroulement plus efficace de la procédure prenant en compte les réalités du terrain. Cependant, ces mêmes

¹⁴⁷ Directive (UE) 2019/1937, article 11.

¹⁴⁸ Directive (UE) 2019/1937, article 12, §1 et §3 à 5.

¹⁴⁹ Directive (UE) 2019/1937, articles 11, §2, e) et f) ; et 13.

¹⁵⁰ Directive (UE) 2019/1937, article 11 §3, §4 et §5.

assouplissements peuvent soulever quelques inquiétudes quant à d'éventuels risques de dérives : qu'est-ce qu'exactly une violation « *mineure* » ? Ce terme au demeurant vague ne pourrait-il pas être utilisé pour détourner la directive de son objectif premier et ignorer certaines violations de normes européennes pouvant arranger le pouvoir mis en place, faisant pression sur l'autorité concernée ? Les mêmes questions d'interprétation peuvent se poser sur les violations « *graves* » ou touchant à des « *dispositions essentielles* », qui pourraient permettre de mettre de côté pour un certain temps des allégations pouvant aller à l'encontre des intérêts de membres compétents de l'autorité. Le texte prévoit tout de même certaines garanties afin de résoudre ces quelques problèmes : il y a en premier lieu le fait que l'autorité doit être indépendante et autonome, et doit pour ce faire être « *intègre* »¹⁵¹, ce qui laisse supposer une imperméabilité totale avec le pouvoir politique. De plus, tout choix de l'autorité refusant d'examiner plus longuement un signalement du fait de son caractère répétitif ou mineur se devra d'être motivé (on remarquera cependant que tel n'est pas le cas du traitement prioritaire d'informations graves, ce qui peut soulever certaines interrogations quant à la logique de cette absence).¹⁵² Enfin, les considérants précisent que ces types de décisions doivent pouvoir être contrôlés par des juridictions, conformément à l'article 47 de la Charte des droits fondamentaux de l'Union européenne qui consacre le droit à un recours effectif et à accéder à un tribunal.¹⁵³ Certains se verront rassurés à la vue de ces garanties supplémentaires mais d'autres pourront cependant encore être soucieux : ces dernières sont-elles suffisantes ? Aurait-il fallu préciser la portée de ces différents termes dans l'article consacré aux définitions afin d'éviter tout risque de dérive ? Pourquoi ne pas avoir introduit le droit à un recours effectif dans les articles mêmes au lieu d'uniquement indiquer cette précision dans les considérants ?

L'article 10 précise que l'utilisation des canaux de signalement externe pourra se faire soit directement, soit après utilisation des canaux de signalement interne.¹⁵⁴ Néanmoins, il est précisé au second paragraphe de l'article 7 que les États membres se doivent de promouvoir l'usage de la procédure interne comme prérequis à l'usage de la procédure externe¹⁵⁵ (les mesures d'« *encouragement* » en question, en l'absence de précisions supplémentaires, sont laissées à l'appréciation des États) : on peut ici encore apercevoir les traces de la négociation portant sur la conditionnalité de l'usage du canal externe. Avec la disparition de cette obligation

¹⁵¹ Directive (UE) 2019/1937, article 12, §1.

¹⁵² Directive (UE) 2019/1937, article 11, § 3, §4 et §5.

¹⁵³ Directive (UE) 2019/1937, considérant 103 ; Charte des droits fondamentaux de l'Union européenne, article 47, *J.O.U.E.*, 18 décembre 2000, C364, p.20.

¹⁵⁴ Directive (UE) 2019/1937, article 10.

¹⁵⁵ Directive (UE) 2019/1937, article 7, § 2.

d'alerter un supérieur, qui pourrait lui-même être mal intentionné et avoir la volonté d'empêcher ces informations d'être dévoilées, le risque de représailles sur le plan professionnel se retrouve quelque peu diminué.¹⁵⁶ La directive fait d'ailleurs directement référence à ce danger de canaux internes défaillants qui justifie le maintien de la possibilité pour le lanceur de directement choisir la procédure externe, le signalement interne ne conservant sa place de procédure « de premier choix » qu'en l'absence de tout risque de répression.¹⁵⁷

Enfin, le fonctionnement de ces procédures externes doit être réexaminé par les États membres au moins une fois tous les trois ans.¹⁵⁸

Sous-section 3 – Caractéristiques communes des procédures de dévoilement

Bien qu'établis à des niveaux différents, les deux canaux se doivent de respecter un certain nombre de mêmes garanties. Plusieurs critères en commun se retrouvent déjà dans les articles 9 et 11, mais un accent spécifique est mis sur l'obligation de confidentialité, qui se voit dédier un article complet alors que déjà évoquée au cours de plusieurs articles ultérieurs. L'identité du lanceur doit donc rester totalement confidentielle, ne pouvant être communiquée à d'autres personnes que celles responsables de la réception des informations ou du suivi sans l'accord exprès de l'individu concerné. Cette confidentialité peut cependant être levée dans des cas spécifiques où pareille divulgation est requise pour des enquêtes ou des procédures judiciaires (cette révélation devra cependant être proportionnée et encadrée par des « *mesures de sauvegarde appropriées* »). Ces garanties nous semblent nécessaires étant donné que le lanceur d'alerte peut être obligé de donner son identité aux personnes en charge des canaux de divulgation : les États membres peuvent en effet décider de rejeter (ou à l'inverse, d'accepter) les signalements provenant de sources totalement anonymes dans le cadre des signalements internes.¹⁵⁹

La confidentialité doit également être respectée par les personnes s'occupant des canaux lorsque ces dernières se retrouvent face à un secret d'affaires contenu dans une information dévoilée¹⁶⁰ ; une manière pour le législateur de concilier les objectifs de cette directive et de la

¹⁵⁶ N.BOULALE MADAINÉ, *op.cit.*, p.474.

¹⁵⁷ Directive (UE) 2019/1937, considérants 47 et 62 ; article 7, §2.

¹⁵⁸ Directive (UE) 2019/1937, article 14.

¹⁵⁹ Directive (UE) 2019/1937, article 6, §2.

¹⁶⁰ Directive (UE) 2019/1937, article 16.

réglementation sur les secrets d'affaires, en montrant que le caractère confidentiel de ces dernières est toujours respecté.

Il est également fait référence à la nécessité pour ces deux types de signalements de respecter les règles européennes mises en place dans le traitement de données personnelles, qui se doit de se faire dans les limites strictement nécessaires pour l'analyse du signalement¹⁶¹. Les opérations effectuées dans le cadre de ces canaux correspondent en effet bien en un traitement de données à caractère personnel, étant donné que va aller être recueillie l'identité du lanceur d'alerte¹⁶² ainsi que certaines de ses coordonnées dans le cadre de l'obligation du retour d'information. Les canaux se devront de respecter les prescrits des textes européens cités concernant le traitement de données personnelles (parmi lesquels le fameux règlement général de protection des données) : ainsi, les données se doivent d'être conservées pour une durée limitée « *n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées* » et ne peuvent être utilisées par la suite pour des objectifs autres que le traitement de la violation signalée.¹⁶³ L'application de ces dispositions signifie également que la personne ayant communiqué ces informations bénéficiera de certains droits supplémentaires, tels que celui d'obtenir toute une série d'informations sur le traitement, d'accéder aux données personnelles traitées ou encore de faire rectifier des données inexactes¹⁶⁴. La personne visée par le signalement (à savoir, la personne impliquée dans la violation ou faisant partie du groupe de personnes impliquées) bénéficie également de ces mêmes droits en vertu de l'article 22 de la directive¹⁶⁵ ; il est cependant fort probable que cette dernière se verra refuser l'application de certains de ces derniers du fait de la présence de clauses d'exceptions à ces prérogatives lorsque l'octroi de ces dernières pourrait « *gêner des enquêtes* »¹⁶⁶. Concernant le droit d'information,

¹⁶¹ Directive (UE) 2019/1937, article 17.

¹⁶² F.COTON et J-F. HENROTTE, *op.cit.*, p.62.

¹⁶³ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, article 5, §1, b) et e), *J.O.U.E.*, 4 mai 2016, L119, p.34 ; Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, article 4, §1,b) et e), *J.O.U.E.*, L119, 4 mai 2016, p.107 ; Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE, article 4, §1, b) et e), *J.O.U.E.*, 21 novembre 2018, L259, pp. 57 et 58.

¹⁶⁴ Règlement (UE) 2016/679, articles 12 à 16 ; Directive (UE) 2016/680, articles 12 à 14 et 16 ; Règlement (UE) 2018/1725, articles 14 à 18.

¹⁶⁵ Directive (UE) 2019/1937, article 22, §3.

¹⁶⁶ Directive (UE) 2016/680, articles 13, §3 ; 15, §1 ; et 16, §4.

il a été admis que la personne concernée pourra avoir accès à certaines informations si toutefois il n'existe pas de risque de compromission des preuves¹⁶⁷ (des mesures conservatoires pourraient alors être utiles) ; dans tous les cas, ce droit à l'information ne donne pas l'autorisation de communiquer l'identité du lanceur d'alerte à cette personne (sauf dans des cas spécifiques d'acceptation volontaire ou de diffamation).¹⁶⁸

Est ensuite établie l'obligation d'archiver les informations ainsi que les manières dont cet archivage peut être effectué suivant le mode de communication (enregistrement ou transcription lorsque réalisée par voie de téléphone ou messagerie vocale, enregistrement ou procès-verbal lorsque réalisée par le biais d'une rencontre en face à face) ; ainsi que le fait que les informations archivées doivent respecter l'obligation de confidentialité et que ces dernières « *ne sont pas conservés plus longtemps qu'il n'est nécessaire et proportionné de le faire* »¹⁶⁹. Rien de bien surprenant ou d'inédit ne peut être tiré de cette disposition, qui reprend juste les exigences de l'article 16 de la même directive, ainsi que les obligations sur la conservation des données personnelles découlant des textes cités auparavant dans l'article 17.

Sous-section 4 – La divulgation publique

La directive prévoit également la possibilité d'effectuer une divulgation publique, à savoir donc un signalement fait en dehors des procédures dressées par le législateur européen, et dans « *la sphère publique* »¹⁷⁰. Un signalement qui sera directement effectué sur une plateforme quelconque sur internet (imaginons, par exemple, un post Facebook) rentrera donc dans cette catégorie.

Cette évocation de la possibilité d'apporter l'information à la connaissance du public n'était au départ pas présente dans la proposition de la directive ; un article consacré à la divulgation publique ne fut inséré qu'à la suite de pression venant de plusieurs associations.¹⁷¹ Pour autant, le recours à cette dernière est conditionné à des critères stricts.

¹⁶⁷ Groupe de travail article 29 sur la protection des données, Avis 1/2006 relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière, p.14.

¹⁶⁸ F.COTON et J-F. HENROTTE, *op.cit.*, p.70.

¹⁶⁹ Directive (UE) 2019/1937, article 18.

¹⁷⁰ Directive (UE) 2019/1937, article 5, 6).

¹⁷¹ A. LACHAPELLE, *RDTI*, *op.cit.*, p.38.

La première situation envisagée est le cas où le lanceur a déjà utilisé les deux autres canaux mis en place par la directive (ou seulement le canal externe) mais qu'aucune réponse appropriée n'a été émise dans le délai de retour d'information prévu par les balises mises en place par la directive¹⁷². L'absence de mesures appropriées ne signifie pas simplement qu'aucune réponse n'a été émise : il est en effet possible que la réaction de l'autorité ne suffise pas pour réparer la violation alléguée, cela devant être évalué à la lumière des caractéristiques propres de la situation. D'un autre côté, l'absence de réponse due au rejet total par l'autorité de l'information du fait de son caractère mineur peut être considérée, suivant les circonstances, comme un suivi approprié et, de ce fait, ne peut pas justifier une divulgation publique.¹⁷³ Si rien n'est dit concernant l'exclusion des informations à caractère répétitif, une interprétation téléologique nous suggère que la même conclusion s'applique également à leur égard. Cependant, rien n'est précisé sur la situation à adopter lorsque les délais sont volontairement mis de côté provisoirement afin que l'autorité puisse s'occuper des allégations de violations graves en premier lieu. Notre interprétation suit celle de la lecture littérale du texte qui nous laisse penser que la personne en détention d'une allégation d'une violation estimée de gravité moindre dont l'analyse est postposée pourrait très bien porter cette information au public et se voir tout de même accorder la protection européenne, du fait de l'importance mise sur le respect des délais dans le recours à la divulgation publique.

Une autre circonstance justifiant le recours à la divulgation publique est le cas où le lanceur a des raisons de croire que « *la violation peut représenter un danger imminent ou manifeste pour l'intérêt public* ». Enfin, lorsque le divulgateur pense rationnellement qu'une signalisation externe entraînerait soit des sanctions soit n'aurait aucune conséquence du fait de certaines circonstances comme la complicité de l'autorité, la divulgation publique est également permise¹⁷⁴. Il n'est pas fait référence, dans cette dernière possibilité, à ce même risque se produisant au sein du canal interne car il est sous-entendu, tout au long de cet article, qu'il est nécessaire d'en premier lieu passer au canal externe en cas de défaillance de la procédure interne au lieu de directement aller vers la divulgation publique : on peut encore y voir un relent de la négociation avec certains pays européens désireux d'établir une hiérarchie entre les canaux.

Si une personne a effectué une divulgation publique sans rentrer dans une de ces trois hypothèses, la conséquence est simple : elle ne peut se voir reconnaître le bénéfice de la

¹⁷² Directive (UE) 2019/1937, article 15, §1, a).

¹⁷³ Directive (UE) 2019/1937, considérant 79.

¹⁷⁴ Directive (UE) 2019/1937, article 15, §1, b).

protection européenne. Toutefois, si l'alerte avait été lancée à la presse dans le respect des règles nationales, le lanceur d'alerte ne sera pas considéré comme exclu de la jouissance des prérogatives du texte européen.¹⁷⁵ Les personnes concernées pouvant porter tant la dénomination de lanceur d'alerte que de sources pour les journalistes, on peut voir ici une façon pour le législateur européen de ne pas porter atteinte aux règles existantes concernant la protection des sources journalistiques.¹⁷⁶

La ratio legis de ces restrictions d'accès à la divulgation publique peut aisément se comprendre : il faut en effet veiller à ce que les allégations fassent en priorité l'objet d'examens minutieux afin d'éviter le risque de permettre à des personnes de lancer toutes sortes d'accusations pouvant constituer en des diffamations en place publique, tout en étant protégées par la directive. D'un autre côté, il fallait tout de même prévoir une possibilité d'autoriser la divulgation publique dans les cas où il subsisterait de véritables problèmes au sein de l'autorité en charge de la procédure de signalement externe malgré la présomption d'indépendance et d'autonomie dont elle dispose. Cela répond également à certaines des interrogations que nous avons formulées dans la section consacrée au signalement externe par rapport aux allégations portant sur des violations d'une gravité moindre laissées de côté ; toutefois, quelques inquiétudes peuvent subsister quant aux informations répétitives ou portant sur des violations mineures.

C'est également dans ces règles que l'influence de la jurisprudence de la Cour européenne des droits de l'Homme est sans doute la plus visible ; le recours à telle divulgation publique étant autorisée dans les mêmes circonstances et, en dehors de ces cas spécifiques, la méconnaissance des canaux de divulgation existants entraîne également la non-application de la protection¹⁷⁷. Il a ainsi été établi par la Cour de Strasbourg que l'inertie d'un supérieur qui avait eu connaissance de l'information était de nature à justifier une divulgation publique¹⁷⁸ (ce qui peut correspondre au premier critère européen) ; la même solution s'imposant en cas de haute probabilité qu'une divulgation externe n'apportera aucun résultat¹⁷⁹ (ce qui correspond au troisième critère européen). La possibilité de « *danger imminent et immédiat* » est cependant une nouveauté du texte européen, n'ayant pas été envisagée par les juges strasbourgeois : on peut penser que dans certains cas spécifiques, l'urgence et la dangerosité de la violation justifient que le lanceur ne

¹⁷⁵ Directive (UE) 2019/1937, article 15, §2.

¹⁷⁶ Comme le laisse penser le considérant 46 qui mentionne l'importance des lanceurs d'alerte comme « *sources(...) pour les journalistes d'investigation* ». On peut également penser à l'affaire Luxleaks dans laquelle les informations avaient été relayées à la presse et utilisées dans l'émission « Cash Investigation » (M.NELLES, *op.cit.*, p. 1804).

¹⁷⁷ Arrêt Soares c Portugal.

¹⁷⁸ Arrêt Guja c. Moldavie.

¹⁷⁹ Arrêt Matùz c. Hongrie, arrêt Bucur et Toma c. Roumanie.

peut se permettre d'endurer la relative longueur d'un examen minutieux de l'information par une autorité. Telle appréciation reviendra en premier lieu au divulgateur lui-même à ses risques et périls : s'il est par la suite estimé que l'imminence du danger avait été exagérée, il se retrouvera déchu de la protection. C'est d'ailleurs également l'occasion de faire remarquer que l'identité de la personne ou du service appréciant tant ce côté imminent du danger que le fait que des « *mesures appropriées* » ont été adoptées par l'autorité de signalement n'est nullement établi par le texte européen.¹⁸⁰

Section 4 – Mesures de protection envisagées par la directive

Les articles de la directive consacrés aux mesures de protection constituent très certainement la partie qui intéressera le plus les potentiels lanceurs d'alerte, étant celle ayant le plus d'impact sur leur situation. Cette importance est mesurée par le législateur lui-même qui apporte une nuance à son harmonisation minimale en établissant une clause de non-régression : il est ainsi établi que la transposition « *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.* »¹⁸¹ À titre illustratif, imaginons qu'un pays a prévu dans sa loi nationale qu'une procédure de signalement interne doit être établie pour toutes les entités privées indépendamment de leur taille : le législateur national de cet État membre pourra lors de la transposition soit maintenir cette règle, soit décider d'imposer cette obligation uniquement aux entreprises employant plus de 49 travailleurs. En revanche, si ce même pays a déjà établi qu'un lanceur d'alerte aura droit à une représentation juridique gratuite dans le cadre de procédure judiciaire faisant suite à sa divulgation (allant de ce fait plus loin que la protection européenne), il ne sera pas possible de revenir sur cette règle lors de la transposition.

Le législateur européen se veut également de protéger les personnes visées dans son champ d'application « contre leur volonté », en établissant que ces derniers ne peuvent renoncer aux prérogatives que leur octroie le texte européen.¹⁸² La présence de cette « interdiction de renonciation » peut facilement s'expliquer par le déséquilibre de rapport de force qu'il existe au sein du monde professionnel : on peut en effet facilement imaginer, si telle précision n'avait

¹⁸⁰ P.PORTIER, « Les canaux de signalement interne et externe selon le droit européen, une avancée par rapport à la loi Sapin 2 ? », *RAE*, 2019, p.707.

¹⁸¹ Directive (UE) 2019/1937, article 25, §2.

¹⁸² Directive (UE) 2019/1937, article 24.

pas été apportée par la directive, qu'un employeur impose dans le contrat de travail une clause établissant que le futur employé renonce à son exonération de responsabilité (la même situation peut être envisagée avec par exemple un contrat avec un fournisseur,...).

Une des premières garanties qu'offre la protection européenne est la confidentialité assurée lors de l'analyse de l'allégation par les divers canaux : nul besoin de revenir sur cette prérogative, cette dernière ayant été analysée plus haut.

La directive assure de plus une protection absolue contre toutes représailles (peu importe la source)¹⁸³ comprises au sens large (ainsi, le texte européen interdit également les tentatives et même les menaces de sanctions) ; étant défini comme étant « *tout acte ou omission direct ou indirect qui intervient dans un contexte professionnel (...) et qui cause ou peut causer un préjudice injustifié à l'auteur de signalement* ». Une longue liste non exhaustive de diverses représailles possibles est ensuite établie (licenciement, mesures disciplinaires, orientation vers un traitement psychiatrique, ...).¹⁸⁴ Il faut évidemment un lien direct entre la divulgation et ces mesures pour que ces dernières se voient qualifier de « représailles »¹⁸⁵. La preuve de ce lien ne reposera cependant pas sur les épaules de la personne sanctionnée : ce sera au contraire à la personne ayant pris la sanction de prouver que cette dernière est totalement indépendante par rapport à la fuite et a été prise pour d'autres raisons¹⁸⁶. Le législateur européen prend ainsi en considération la difficulté pour le lanceur d'apporter la preuve de ce lien par lui-même.¹⁸⁷

Les États membres se doivent donc de prendre diverses mesures pour s'assurer que les personnes visées dans son champ d'application puissent bénéficier d'une protection totale contre toutes représailles : ils doivent ainsi apporter des informations sur la manière de se protéger contre les représailles ainsi que des mesures de soutien dans le cadre de procédures judiciaires liées à la divulgation d'informations ; s'assurer que si il y a bien eu représailles, les personnes concernées obtiennent une réparation totale de leur préjudice ; ou encore garantir des « *mesures correctives contre les répressions* »¹⁸⁸. Il est également possible pour les États de mettre sur place une aide financière et des mesures de soutien supplémentaires, entre autres

¹⁸³ A. LACHAPPELLE, *TFR*, *op.cit*, p.815.

¹⁸⁴ Directive (UE) 2019/1937, article 19.

¹⁸⁵ Directive (UE) 2019/1937, considérant 44.

¹⁸⁶ Directive (UE) 2019/1937, article 21, §5.

¹⁸⁷ Directive (UE) 2019/1937, considérant 93.

¹⁸⁸ Directive (UE) 2019/1937, articles 20, §1 ; et 21, §6 et §8.

psychologiques, ainsi que d'instaurer une institution spécifique qui pourrait apporter toutes les mesures de soutien visées par la directive.¹⁸⁹

De plus, la directive prévoit une exonération expresse de toute responsabilité que pourraient encourir les lanceurs d'alerte du fait de leur divulgation, pour autant que la potentielle infraction ou faute n'ait pas été au-delà de ce qui était strictement nécessaire à la communication des divulgations et qu'ils « *aient eu des motifs raisonnables de croire que le signalement ou la divulgation publique de telles informations étaient nécessaire pour révéler une violation* »¹⁹⁰. Pareille exonération s'applique également pour l'obtention des informations divulguées pour autant que cette dernière ne soit pas constitutive d'une « *infraction pénale autonome* », auquel cas « *la responsabilité pénale continue d'être régie par le droit national applicable* »¹⁹¹. Ce dernier point constitue un obstacle à une protection complètement efficiente des lanceurs d'alerte. En effet, les affaires les plus connues concernant les *whistleblower* (Snowden, Luxleaks) montrent bien que le vol est parfois nécessaire afin de procéder à l'alerte et à la divulgation. Cette règle européenne voudrait donc dire que les lanceurs pourraient se voir inculpés¹⁹² pour un élément qui est pourtant une composante intégrale de l'alerte. Comme le fait remarquer Amélie Lachapelle dans son analyse de la directive¹⁹³, cela contredit l'interprétation faite par la Cour de cassation luxembourgeoise de la jurisprudence de la Cour européenne des droits de l'Homme qui reconnaissait une impunité « *en principe* » pour les infractions pénales effectuées dans l'exercice de la liberté d'expression¹⁹⁴. La protection des lanceurs d'alerte serait donc plus précaire dans les pays transposant cette règle de la directive sans en relever le niveau minimal.

Le texte européen revient, dans le cadre des impunités, encore une fois sur la problématique des secrets d'affaire, en déclarant qu'une divulgation de secrets d'affaires dans le cadre d'une des trois procédures visées par le législateur européen sera considérée comme « *licite* » au sens de la directive secrets d'affaires. Il est également établi dans le même texte qu'un lanceur d'alerte se verra exonéré de toute responsabilité liée à des poursuites pour divulgation de secrets d'affaires¹⁹⁵. On peut se demander à quelle responsabilité le texte fait ici référence, des sanctions ne pouvant dans aucune situation être imposées à l'encontre d'une personne en

¹⁸⁹ Directive (UE) 2019/1937, article 20, §2 et §3.

¹⁹⁰ Directive (UE) 2019/1937, article 21, §2.

¹⁹¹ Directive (UE) 2019/1937, article 21, § 3 et §4.

¹⁹² Le vol est en effet une infraction pénale ; en Belgique, elle a été insérée dans le code pénal par les articles 461 et suivants.

¹⁹³ A. LACHAPELLE, *RDTI*, *op.cit.*, pp.47-48.

¹⁹⁴ Cass. Luxembourg, 11 janvier 2018, *JLMB* 2018, p.1796.

¹⁹⁵ Directive (UE) 2019/1937, article 21, §7.

possession licite de secrets d'affaires. Sans doute le législateur européen sacrifie-t-il la cohérence interne de son texte afin de réaffirmer le fait que la réglementation européenne des secrets d'affaires ne fragilise pas la protection des lanceurs d'alerte, ultime référence dans le texte aux événements ayant entraîné son adoption.

Enfin, la directive demande aux États membres de prévoir dans leur ordre national certaines sanctions envers non seulement les personnes (tant physiques que morales) qui ont fait subir des représailles, mais également à l'encontre de celles qui « *entravent ou tentent d'entraver le signalement* », « *intentent des procédures abusives* », ou encore « *manquent à l'obligation de préserver la confidentialité de l'identité des auteurs de signalement* ». Le contenu des sanctions est largement laissé à l'appréciation des législateurs nationaux ; il est juste demandé au niveau européen que celles-ci soient « *effectives, proportionnées et dissuasives* »¹⁹⁶. Ces sanctions pourront donc être soit administratives, civiles ou encore pénales, même si on pourrait rejoindre l'argument de Stéphane Detraz que les sanctions civiles ne peuvent présenter un côté dissuasif suffisant étant donné qu'elles ne visent qu'à la réparation d'un dommage. Le terme « proportionnées » laisse quant à lui penser que les États se devront de prévoir des sanctions différentes suivant le manquement concerné, ou encore suivant la gravité des représailles subies.¹⁹⁷ Il faut enfin également relever que les États membres se doivent d'également prévoir des sanctions pour les individus ayant volontairement fait fuiter de fausses informations. Ces personnes seront donc non seulement démunies de toute protection européenne face à d'éventuelles répercussions car sachant que l'information dévoilée n'est pas véridique, mais se verront également imposer des sanctions et devront indemniser les personnes ayant subi des préjudices du fait de ces informations erronées.¹⁹⁸ Cette précision est nécessaire pour éviter les utilisations frauduleuses du système qui pourraient dériver en un florilège de fausses allégations pouvant boucher les canaux et rendre moins visibles les informations véridiques. Cependant, le considérant 102 laisse penser que les sanctions à l'encontre de ce type de personnes seront moins sévères que pour les autres, étant donné que le côté proportionnel de la sanction impose que cette dernière ne dissuade pas des lanceurs d'alerte légitimes à utiliser le système européen.¹⁹⁹

¹⁹⁶ Directive (UE) 2019/1937, article 23, §1.

¹⁹⁷ S. DETRAZ, « Les sanctions relatives à la violation des règles sur la protection des lanceurs d'alerte selon la directive », *RAE*, 2019, pp.714-715.

¹⁹⁸ Directive (UE) 2019/1937, article 23, §2.

¹⁹⁹ Directive (UE) 2019/1937, considérant 102.

Chapitre 3 – Situation du lanceur d’alerte après la directive

Section 1 – Impact de la directive sur les textes belges existants

Sous-section 1- Maintien ou révision des systèmes existants ?

On peut en premier lieu se demander si le législateur belge se devra de réviser les quelques lois existantes du fait que leurs champs d’application se confondent avec celui établi par le législateur européen.

Le champ d’application matériel du décret de la Communauté flamande est établi de manière tellement succincte que de nombreux domaines peuvent rentrer dans ce dernier : il est ainsi dit que le médiateur flamand peut connaître de toute accusation « *d’abus ou de délits au sein de l’autorité administrative* »²⁰⁰. Il est donc tout à fait possible que des matières listées dans l’article 2 de la directive et la première partie de l’annexe puissent rentrer dans cette simple notion de délits ou d’abus (un terme qui peut faire penser aux pratiques abusives également visées dans le champ d’application européen) : dans le contexte de l’autorité administrative, on peut imaginer que le fonctionnaire tombe sur un abus ou une violation d’une règle européenne concernant les marchés publics ou encore concernant la protection des données à caractère personnel. La même conclusion pourra être tirée pour le législateur germanophone²⁰¹.

Concernant la loi fédérale de 2013 sur les autorités administratives, le champ d’application y est ici plus détaillé que dans la loi flamande. Pour autant, on peut également y faire rentrer plusieurs domaines visés par la directive : la loi belge couvre ainsi les dénonciations relatives aux « *actes (...) impliquant un risque inacceptable pour la vie, la santé ou la sécurité des personnes ou pour l’environnement* »²⁰², cette notion pouvant couvrir des pratiques abusives ou des violations de réglementations européennes consacrées à la sécurité et conformité des produits, des aliments et des transports, à la protection de l’environnement ou encore à la santé publique. De plus, certains termes définis de manière large peuvent se référer à la transposition de règles européennes relatives aux matières visées par la directive (la loi parle ainsi « *d’acte... constituant une infraction aux lois, arrêtés, circulaires (...) applicables aux autorités*

²⁰⁰ Décret Comm. Flam. du 7 juillet 1998, article 3, §2.

²⁰¹ Le décret germanophone parlant quant à lui « d’abus, d’irrégularités, d’actes illicites ou d’infractions commis au sein de l’autorité administrative ». Décret Comm. Germ du 26 mai 2009, article 3, §3.

²⁰² Loi du 15 septembre 2013, article 2, 3°.

administratives (...) qui constituent une menace pour l'intérêt général ou une atteinte à celui-ci"²⁰³).

On peut envisager deux solutions quant au futur de ces procédures pour le secteur public : d'un côté, elles pourraient être maintenues telles quelles par facilité et une exclusion des matières visées par la directive sera effectuée. L'autre éventualité est une révision des régimes existants afin de coller aux exigences européennes : c'est cette situation qui sera analysée dans la suite de cette section. Dans ce cas cependant, la loi fédérale ne saurait restreindre la procédure uniquement aux informations concernant des violations ayant eu lieu dans les 5 dernières années.

Le système de dénonciation à la FSMA est quant à lui dans un régime particulier, étant donné qu'il a été introduit dans la loi du 2 août 2002 relative à la surveillance du secteur financier par une loi du 31 juillet 2017²⁰⁴ qui visait à transposer, par l'instauration de cette procédure, l'article 32 du règlement 596/2014²⁰⁵ sur les abus de marché (règlement se retrouvant dans la liste des textes sectoriels listés dans la seconde partie de l'annexe dont l'application ne doit normalement pas changer du fait de l'entrée en vigueur de la directive lanceur d'alerte), ainsi que la directive d'exécution 2015/2392 mettant en œuvre le signalement prévu par l'article 32 susmentionné : or, il est précisé dans les considérants qu'il est préférable de maintenir les canaux de signalement mis en place par ce dernier texte.²⁰⁶ La difficulté est cependant que le législateur belge, en transposant cette directive d'exécution par l'insertion d'un article 69 bis dans la loi de 2002, a étendu cette procédure à toutes les infractions relevant des domaines d'action de la FSMA²⁰⁷, au lieu de se concentrer sur les règles relatives aux « *opérations d'initiés, à la divulgation illicite d'informations privilégiées et les manipulations de marché* » instaurées par le règlement 596/2014.²⁰⁸ Les infractions soumises à la FSMA par le biais de cette procédure peuvent ainsi concerner tant des matières qui sont explicitement exclues du champ d'application de la directive européenne²⁰⁹ que des matières qui sont expressément incluses dans son champ

²⁰³ Loi du 15 septembre 2013, article 2, 3°.

²⁰⁴ Loi du 31 juillet 2017 modifiant la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers, en vue de mettre en œuvre le Règlement (UE) n° 596/2014 sur les abus de marché et de transposer la Directive 2014/57/UE relative aux sanctions pénales applicables aux abus de marché ainsi que la Directive d'exécution (UE) 2015/2392 concernant le signalement des violations, et portant des dispositions diverses, article 13, *M.B.*, 11 août 2017, p.79443

²⁰⁵ Règlement (UE) No 596/2014, article 32.

²⁰⁶ Directive (UE) 2019/1937, considérant 68.

²⁰⁷ Loi du 2 août 2002, articles 45 et 69 bis.

²⁰⁸ Règlement (UE) 596/2014, article 1.

²⁰⁹ En plus du règlement 596/2014 et de la directive d'exécution 2015/2392, on retrouve ainsi les règles de la directive 2014/65/UE concernant les marchés financiers ainsi que de la directive 2009/65 concernant certains organismes de placement collectif en valeurs mobilières.

d'application²¹⁰. La question est alors de savoir si le maintien de ce canal de divulgation, tel que souhaité par le législateur européen est possible ? Possédait-il déjà les garanties suffisantes pour être conforme à cette nouvelle directive ?

Une troisième option se dessine cependant également pour tous ces textes existants en droit belge, qui est celle de l'abrogation pure et simple en faveur d'un régime unique et homogène de protection des lanceurs d'alerte. Cette solution pourrait être également efficace, évitant de retomber sur le problème de la fragmentation des textes, bien qu'il ne faudrait pas bien entendu effacer les spécificités propres à chaque secteur.

À cet égard, il faut de nouveau mentionner les garanties de protection suivant dénonciation à la Cellule de traitement des informations financières ainsi qu'aux entités assujetties et aux autorités de contrôle qui ont été introduites par la loi du 18 septembre 2017 dans l'optique de transposer des dispositions de la directive 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou de financement du terrorisme.²¹¹ Ce texte se trouvant dans la seconde partie de l'annexe, le législateur pourrait donc maintenir ce système, plus adapté au secteur concerné. Les mécanismes mis en place par cette loi au regard de la directive 2019/1937 ne seront donc pas analysés dans la suite de ce mémoire.

Sous-section 2. Impact sur le champ d'application personnel

Si les procédures existantes sont maintenues, il y aura déjà nécessité de réviser les champs d'application personnel de toutes ces lois, qui sont trop restreints au sens européen. En effet, dans le secteur public, la possibilité de divulgation est uniquement ouverte aux « *membres du personnel* »²¹² (actuels ou anciens dans le cadre de la loi fédérale de 2013²¹³). Même si ces derniers termes étaient dans le futur interprétés de telle manière à rejoindre la notion extensive

²¹⁰ On retrouve ainsi le règlement 2016/1011 concernant les indices utilisés comme indices de référence dans le cadre d'instruments et de contrats financiers ou pour mesurer la performance de fonds d'investissement.

²¹¹ Plus précisément les articles 33, 37 et 38. 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, articles 33 ; 37 ; et 38, *J.O.U.E.*, 5 juin 2015, L141, pp.99-100. Loi du 18 septembre 2017, article 1, §2.

²¹² Décret. Comm. Flam. du 7 juillet 1998, article 3, §2 ; Décret Comm. Germ. du 26 mai 2009, article 3, §3.

²¹³ Loi du 15 septembre 2013, article 2. Le supérieur à qui l'information a été dévoilée ainsi que la personne de confiance d'intégrité sont également concernés par les mesures de protection mises en place par cette même loi (Loi du 15 septembre 2013, article 15).

de « *travailleur* » au sens de la directive européenne²¹⁴, ce qui répondrait à nos critiques concernant l'exclusion de certaines personnes du bénéfice de la procédure de la loi de 2013, le champ d'application reste trop étroit en ce qu'il n'inclut pas les « *tiers en lien avec l'auteur du signalement* », les « *facilitateurs* » ou les « *entités juridiques* ». Le champ d'application personnel actuel de la procédure de divulgation à la FSMA est cependant assez intéressant : si l'interdiction des « *représailles, (de) la discrimination et d'autres types de traitement inéquitable ou de mesure préjudiciable consécutifs ou liés au signalement d'une infraction* » semble réservée aux travailleurs, l'anonymisation et la protection de toute action judiciaire peuvent quand elle bénéficier à « *la personne qui effectue de bonne foi un signalement* ». Cependant, le champ est à nouveau trop restreint car il ignore les trois catégories citées plus haut par les termes « *qui effectue (...) un signalement* ». Cependant, la simple notion de « *personne* » est à retenir ici : elle laisse penser que cette protection n'est pas seulement ouverte aux « *travailleurs* », mais également à toute personne privée, ce qui nous semble bien plus adéquat. Il serait souhaitable que le législateur belge s'inspire de cette formule.

Il ressort clairement des différents textes nationaux que le lanceur ne saurait bénéficier de mesures de protection sans avoir au préalable utilisé les canaux de communication mis à sa disposition, ce qui correspond à l'idéologie européenne. En revanche, seule la loi fédérale de 2013 prévoit l'exigence de la croyance du lanceur en la véracité de l'information qu'il a diffusée.²¹⁵ Cela n'est pas en soi problématique que les autres textes nationaux ne prévoient pas cette obligation, étant donné qu'ils peuvent justifier le maintien de cette absence par la mise en place d'un système plus favorable à l'encontre des lanceurs. Néanmoins, cette exigence européenne nous semble raisonnable et justifiée, en ce qu'elle permet de limiter la propagation d'informations mensongères.

Sous-section 3. Les procédures sont-elles conformes aux canaux européens ?

§1- Existence de canaux internes et externes

Le législateur belge a, pour certains textes, anticipé son homologue européen en établissant des procédures externes et internes au sein des mécanismes existants de divulgation. C'est ainsi la

²¹⁴ Ce qui ne saurait déjà être le cas de la loi du 15 septembre 2013, qui précise que les membres du personnel sont « *le membre du personnel statutaire, le stagiaire ou le membre du personnel occupé en vertu d'un contrat de travail* » ; Loi du 15 septembre 2013, article 2, 1^o.

²¹⁵ Loi du 15 septembre 2013, article 15, §4 et §5.

situation de la procédure de dénonciation fédérale, possédant un canal interne (la personne de confiance d'intégrité) et un canal externe (le Point de contact central auprès des médiateurs fédéraux²¹⁶). Pour ce qui est de la communication de l'information au supérieur hiérarchique, ce dernier ne saurait être assimilé à notre sens au « canal interne » du système européen ; la directive demandant qu'une personne spécifique soit expressément désignée pour gérer la réception des allégations²¹⁷. Cela ne signifie cependant pas que cet acteur est supprimé de la procédure, la directive étant pour rappel de caractère minimal ; il pourra subsister du moment que des canaux internes et externes possédant toutes les qualités requises sont établis. La procédure d'avis ne semble pas contraire aux obligations européennes, celle-ci n'interdisant pas ce type de premier filtre avant de porter l'information à la connaissance du canal interne, mais impose juste la création de tel canal. Tout comme dans la directive européenne, le lanceur d'alerte peut aller porter sa dénonciation soit vers le canal interne soit vers le canal externe, sans qu'aucune subsidiarité ne soit établie. La procédure fédérale pourra donc être maintenue pour ces dernières caractéristiques : en revanche, n'est contenue pour l'instant dans la loi aucune « mesure d'encouragement » demandée par le législateur européen pour utiliser en premier lieu le canal interne. Il faudra donc implanter ces dernières, bien qu'elles ne devront pas obligatoirement se retrouver sous forme législative.

La loi de 2002 relative aux secteurs financiers instaure également en quelque sorte ces deux types de canaux, bien qu'elle établisse en détail la procédure de divulgation externe (par le biais de la FSMA) et émet seulement l'exigence pour certaines entités déterminées de mettre en place des canaux internes. Le lanceur d'alerte pourra ici aussi techniquement se diriger librement vers l'un des deux canaux, l'accès à la procédure externe n'étant pas conditionnée à l'utilisation préalable du canal interne²¹⁸. Il est par ailleurs demandé par la FSMA dans sa circulaire s'adressant à toutes les entités « *agréées ou inscrites auprès de la FSMA* » ou dont les activités sont « *soumises au contrôle de la FSMA* » d'encourager l'utilisation des canaux de signalement interne qu'ils auront mis en place²¹⁹ : une telle demande par le biais de cette circulaire peut correspondre aux mesures d'encouragement que le législateur européen laissait à l'appréciation des États membres. Nous estimons cependant, conformément à notre critique formulée dans

²¹⁶ Les médiateurs étant par ailleurs expressément visés par la directive dans son considérant 64 listant les différentes entités pouvant prendre le rôle de canal externe de divulgation.

²¹⁷ Amélie Lachapelle tient le même raisonnement, estimant que la directive entraînera dans le futur l'obligation pour les entités d'investir une personne particulière de la fonction de *Whistleblower Office*. A.LACHAPELLE, *RDTI*, *op.cit.*, p.35.

²¹⁸ Un fait qui est par ailleurs explicitement énoncé dans la circulaire de la FSMA concernant la mise en place de procédures internes. Circ. FSMA_2017_21, point 1.4.

²¹⁹ Circ. FSMA_2017_21

l'analyse de cette loi dans le premier chapitre, que le côté flou ainsi que l'absence de mesures de protection prédéterminées au sein de ce canal interne constituent au contraire un frein à l'utilisation de la procédure interne.

Les deux lois communautaires établissent un canal externe en la personne des médiateurs. L'obligation d'aller porter en premier lieu l'information à leur supérieur hiérarchique ,et, dans le cas de la Communauté flamande, à l'Audit interne ne peut être considérée comme une mesure d'encouragement de recours au canal interne en premier lieu : le supérieur ne peut, pour les raisons évoquées précédemment, être considéré comme constituant un canal interne ; et l'Audit est une agence commune à l'ensemble du service public flamand²²⁰, ne pouvant donc pas être considérée comme « interne » à l'administration concernée. Cela ne veut cependant pas dire que de nouvelles entités se devront d'être créées : en effet, il a été établi qu'un même service pourra être tant responsable de la procédure externe qu'interne. Il faudra dans cette hypothèse simplement clarifier que les médiateurs et l'Audit interne endossent le double rôle de canaux internes et externes. Les conditions d'accès aux médiateurs dans le système flamand pourront de plus, dans ce cas, constituer un « encouragement » d'utilisation du système interne (l'Audit) avant externe (les médiateurs) ; le législateur européen n'interdisant pas l'imposition de telles conditions préalables.

Il n'y aura donc pas nécessité de création de nouveaux canaux et ceux existants pourront être maintenus : il faudra pour autant réviser ces derniers pour s'assurer qu'ils répondent aux exigences européennes.

§2- Conformité des canaux belges avec les critères européens

Précisons d'emblée que rien n'est dit dans les procédures existantes quant au traitement des données à caractère personnel : certains pourraient toutefois argumenter que ces règles sont automatiquement appliquées, étant donné que les textes cités à ce sujet dans la directive sont tous d'application en Belgique et concernent toutes les données à caractère personnel, peu importe le contexte dans lequel ces dernières sont récoltées²²¹.

²²⁰ Arrêté Gouv. Flam. du 18 octobre 2013 portant création de l'agence autonomisée interne « Audit Vlaanderen » et modifiant divers arrêtés, article 2, *M.B.*, 27 novembre 2013, p.92210.

²²¹ Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, article 4, *M.B.*, 5 septembre 2018, p.68616.

La procédure de canaux internes mis en place par l'article 69ter de la loi de 2002 sur la surveillance du secteur financier et aux services financiers nécessitera incontestablement des travaux législatifs en profondeur : celle-ci n'est en effet actuellement encadrée que par des prescrits généraux établis par une circulaire. Remarquons cependant que la circulaire reprenait déjà certains critères établis par la directive européenne : elle exige ainsi un suivi approprié (sans pour autant donner plus de précisions ou de délai) et la conformité à « *la législation relative à la protection de la vie privée* », ce qui peut correspondre aux exigences sur le traitement des données à caractère personnel. Notons également que la taille de l'entreprise est déjà prise en compte ici, étant donné qu'il est mentionné que les entreprises de petite taille pourront permettre le signalement aux « *personnes chargées de la direction effective* »²²² : on peut imaginer que dans le futur système, soit ces personnes visées se verront désigner comme responsable du canal interne, soit la Belgique décidera de ne pas étendre les obligations européennes aux entreprises comptant moins de 49 personnes afin de permettre dans ces dernières un système de dénonciation plus informel. Néanmoins, le fonctionnement de ce canal reste encore insuffisamment déterminé et répond de manière plus qu'imparfaite aux règles mises en place par la directive. L'établissement d'un texte législatif ou réglementaire reprenant chacune des exigences européennes sera donc certainement nécessaire.

Toujours au niveau du canal interne, il faut également examiner le degré de conformité de la personne de confiance d'intégrité. La forme dans laquelle doit se faire la dénonciation n'a pas été fixée par le législateur ; en revanche, la demande d'avis devra nécessairement se faire sous forme écrite, en ce qu'elle devra être « *signée par le membre du personnel* ».²²³ En l'absence d'indications contraires, tout laisse penser ici qu'une dénonciation anonyme n'est pas possible. Un accusé de réception n'est nullement prévu dans le cadre de cette procédure. Quant au retour d'information devant être effectué dans les 3 mois suivant l'accusé de réception (ou expiration du délai de 7 jours après signalement), on peut arguer que l'obligation de « *communiquer (...) son avis* » dans les huit semaines à une demande d'avis pourrait partiellement répondre à cette condition, étant donné que cette dernière consiste en la communication à l'auteur de mesures de suivi, cette dernière notion reprenant « *toute mesure prise (...) pour évaluer l'exactitude des allégations formulées* »²²⁴. Certaines informations concernant l'enquête (et faisant également partie de l'obligation de retour d'information) devront également être communiquées au lanceur

²²² Circ. FSMA _2017_21, 2.4 et 2.5.

²²³ Loi du 15 septembre 2013, article 6, §3.

²²⁴ Directive 2019/1937, article 5, 12).

mais par le biais des médiateurs fédéraux²²⁵ et non de la personne de confiance : on pourrait envisager que l'avis contienne mention de l'ouverture de cette enquête. L'obligation de confidentialité semble ici respectée, étant donné qu'il est dit que le lanceur peut choisir une procédure dite de « *dénonciation confidentielle* », dans laquelle la personne de confiance d'intégrité garde l'identité du lanceur secrète, « *la protège au maximum et ne la révèle à personne, dans les limites de la législation en vigueur, sans l'autorisation écrite expresse du membre du personnel concerné.* » Une procédure de « dénonciation publique » (sans lien avec la divulgation publique) dans laquelle la confidentialité n'est pas de mise est également possible mais uniquement sous accord exprès du lanceur d'alerte²²⁶. Au niveau de l'archivage, il est prévu qu'un rapport anonymisé reprenant les allégations doit être rédigé annuellement.²²⁷

En ce qui concerne les canaux externes, le Point de contact central présente certains des mêmes critères de (non) conformité avec la personne de confiance d'intégrité, étant donné que les deux procédures de divulgation sont mises en place par la même loi. Ainsi, l'accusé de réception n'est pas établi, et le retour d'information²²⁸ ainsi que les règles de confidentialité sont instaurés de la même manière. Cependant, il faut également s'assurer que cet acteur respecte les règles spécifiques propres aux canaux externes : ainsi, il faudra préciser que la dénonciation peut se faire sous toute forme et, si on considère que la procédure d'avis est part intégrante de la procédure de dénonciation, veiller à ce que cette dernière puisse se faire autrement qu'uniquement par écrit. Il n'est pas précisé si une division des tâches sera faite et l'obligation de réserver l'accès aux informations aux membres autorisés n'est pas établie. Les conclusions de l'enquête doivent ici bel et bien être transmises au lanceur d'alerte²²⁹. Concernant la mise à disposition d'informations, il est bien prévu que le Point de contact central informe le lanceur²³⁰, mais rien n'est indiqué sur la mise en place d'une section spécifique sur un site internet. En pratique cependant, une section spécifique a bien été installée sur le site Fedweb et sur le site du médiateur fédéral comprenant certaines informations concernant la procédure de divulgation, mais omettant de reprendre certaines notions demandées par le législateur européen

²²⁵ Loi du 15 septembre 2013, articles 12 et 14.

²²⁶ Loi du 15 septembre 2013, article 8, §1, al. 2.

²²⁷ Arrêté Royal du 9 octobre 2014 portant exécution de l'article 3 §2 de la loi du 15 septembre 2013 relative à la dénonciation d'une atteinte suspectée à l'intégrité au sein d'une autorité administrative fédérale par un membre de son personnel, article 3, 6°, *M.B.*, 12 novembre 2014, p.89980.

²²⁸ Toutefois, le retour d'information par les médiateurs est ici complètement acceptable, ces derniers constituant le canal externe.

²²⁹ Loi du 15 septembre 2013, article 14.

²³⁰ Loi du 15 septembre 2013, article 4.

(cordonnées du Point contact central, régime de confidentialité applicable...)²³¹. De plus, au contraire de la personne de confiance d'intégrité, un archivage n'est pas prévu au niveau du Point de contact central mais uniquement au stade de l'enquête, lorsque les médiateurs effectuent un rapport écrit.²³² Cela est problématique car tous les signalements ne sont pas archivés, à l'inverse de ce qui est demandé dans la directive : sont en effet mises de côté les allégations rejetées durant la procédure d'avis. Par ailleurs, relevons que cette procédure précitée peut rejeter les dénonciations irrecevables mais non « *manifestement non fondées* »²³³ : il est parfaitement imaginable que cette procédure de filtre puisse servir, par le biais de cette formule assez floue, à rejeter les demandes répétitives ou portant sur des violations de moindre importance. Il nous paraît important, pour éviter des risques de dérive de personnes mal intentionnées se servant de cette phrase pour rejeter certaines violations en dehors de ces dernières hypothèses, de préciser si cette possibilité européenne est bien mise en œuvre ou non au sein de la procédure fédérale.

Au niveau des systèmes prévus par les deux Communautés, une révision complète sera nécessaire étant donné que quasiment aucune des garanties établies par le texte européen n'est indiquée dans les décrets instaurant les services de médiation ou l'audit interne flamand ; la seule rapidement évoquée étant l'obligation de confidentialité, l'identité des lanceurs ne devant pas être dévoilée au sein du rapport annuel destiné au Parlement communautaire recueillant toutes les recommandations du médiateur²³⁴. Cela n'est cependant pas suffisant pour satisfaire les requêtes européennes sur ce dernier point.

Enfin, le canal de divulgation externe concernant les infractions relatives aux compétences de la FSMA semble être la procédure la plus en phase avec les prescrits européens, ce qui vient certainement du fait que ce système a été mis en place en suivant les demandes d'une autre directive européenne.²³⁵ Ainsi, la dénonciation peut se faire, de manière anonyme ou non, sous les trois formes prévues par la directive (la dénonciation par écrit étant possible tant par courrier

²³¹

https://fedweb.belgium.be/fr/a_propos_de_l_organisation/administration_federale/mission_vision_valeurs/politique_federale_d_integrite/melding_van_een_integriteitsschending (consulté le 15/05/2021) ; http://www.mediateurfederal.be/sites/1070.b.fedimbo.belgium.be/files/procedure_de_denonciation.pdf (consulté le 15/05/2021).

²³² Loi du 15 septembre 2013, article 14.

²³³ Loi du 15 septembre 2013, article 6, §6, al.2.

²³⁴ Décret Comm. Flam du 7 juillet 1998, article 18 ; Décret Comm. Germ. du 26 mai 2009, art.23.

²³⁵ La loi de 2002 précise en effet que les règles de procédure devront être établies « *en tenant compte en particulier de la Directive (UE) 2015/2392.* » Loi du 2 août 2002, article 69 bis, §1, al.2.

que par voie électronique)²³⁶. Il est également établi qu'une section spécifique du site internet de la FSMA doit préciser une série d'informations, qui semble correspondre seulement partiellement à celles devant être prévues pour respecter les prescrits de la directive²³⁷. Cependant, le site internet reprend bel et bien toutes les informations demandées par le législateur européen²³⁸, saisissant la possibilité accordée par le règlement mettant en place la procédure d'afficher des informations supplémentaires. Le règlement exige également que soient désignés des membres du personnel formés pour les tâches de réception et de communication, reprend les exigences européennes de confidentialité, et impose une obligation d'archivage, ici sous forme de registre des dénonciations reçues.²³⁹

Pour autant, certains éléments de la procédure se devront d'être révisés au regard de la récente directive. Ainsi, un accusé de réception est prévu²⁴⁰, mais le délai de 7 jours prévu par la directive européenne n'est mentionné nulle part ici pour l'instant. Une réponse est également envoyée s'il s'avère que la violation alléguée est bien réelle²⁴¹, mais à nouveau, aucun délai n'est mentionné pour le moment et cette communication s'avère trop légère pour constituer un « *retour d'information* » au sens européen (les mesures de remédiation ne sont pas indiquées). En outre, le règlement prévoit une disposition complètement contraire à l'obligation européenne d'informer sur le résultat de l'enquête ayant découlé de l'information, estimant que le lanceur d'alerte ne peut être tenu au courant de ces résultats « *eu égard au secret professionnel de la FSMA* ». ²⁴² Une telle contradiction de la volonté du législateur européen se devra bien entendu d'être retirée au plus vite. Tel que dit plus haut, rien n'est précisé concernant le traitement des données à caractère personnel : cependant, la FSMA a révisé sa politique en matière de vie privée afin de coller aux prescrits introduits par le RGPD²⁴³, montrant bien sa volonté de respecter les règles européennes en la matière.

²³⁶ Règlement du 5 septembre 2017 de l'Autorité des services et marchés financiers précisant les règles de procédure applicables à la réception et au traitement des signalements d'infraction, articles 5 et 11, *M.B.*, 28 septembre 2017, p.89027.

²³⁷ Règlement du 5 septembre 2017, article 4.

²³⁸ <https://www.fsma.be/fr/faq/point-de-contact-lanceurs-dalerte> (consulté le 15/05/2021).

²³⁹ Règlement du 5 septembre 2017, articles 3 ; 8 ; 9 ; 12 ; et 13 ; Loi du 2 août 2002, article 74.

²⁴⁰ Règlement du 5 septembre 2017, article 14.

²⁴¹ Règlement du 5 septembre 2017, article 7.

²⁴² Règlement du 5 septembre 2017, article 10.

²⁴³ <https://www.fsma.be/fr/faq/politique-vie-privee-de-la-fsma> (consulté le 15/05/2021).

§3 – La divulgation publique

Aucun des textes en vigueur actuellement ne prévoit la possibilité de divulgation publique. Ce mode de signalement pourra être établi par une loi indépendante (générale ou sectorielle) et/ou introduite dans les textes cités par le biais d'amendements. La procédure de la dénonciation à la FSMA pose cependant question en ce que le lanceur d'alerte sera déchu de la protection légale en cas de transmission de l'information à une autre entité ou personne que l'Autorité. D'un côté, cette règle est cohérente avec la déchéance de la protection prévue par le droit européen en cas de divulgation publique lorsque le lanceur ne remplit pas une des trois hypothèses fixées par le texte. Cependant, cette condition est pour l'instant trop stricte en ce qu'elle ne prend justement pas en compte ces situations où la divulgation est permise : une révision de ce principe s'impose donc.

Sous-section 4. Les mesures de protection répondent-elles aux critères européens ?

On ne reviendra pas ici sur l'anonymisation, ayant été abordée au cours de la sous-section précédente et étant garantie pour rappel par les canaux du système fédéral, la FSMA ainsi que de manière imparfaite par les Communautés.

Les deux systèmes communautaires prévoient que le lanceur peut être « *mis... sous la protection du médiateur* » à sa demande. Un protocole ou un procès-verbal doit ensuite être rédigé, comprenant certaines mesures de protection. Les décrets citent ensuite quelques mesures de protection minimales que doit obligatoirement contenir ce document : la première consistant en la « *suspension des procédures disciplinaires* », ce qui répond assez bien aux exigences européennes, constituant une mesure de protection envers des représailles considérées comme interdites et répondant à l'exonération de responsabilité pour les faits relatifs à la dénonciation. Les autres mesures visent « *des règles en matière d'attribution de la preuve* », un terme vague pouvant désigner le fait que l'absence de lien entre la divulgation et une sanction devra être prouvée par la personne ayant imposé cette dernière, ainsi que la « *possibilité d'une mutation volontaire du membre du personnel* » concerné²⁴⁴, ce qui n'est pas expressément prévu par la directive mais devra être maintenu en vertu de la clause de non-régression. On peut ici

²⁴⁴ Décret Comm.Fl. du 7 juillet 1998, article 17 bis ; Décret Comm. Germ. du 26 mai 2009, article 16.1.

facilement faire la constatation que ces trois mesures ne sont pas suffisantes pour assurer une protection contre toutes les représailles, ainsi que pour assurer une exonération totale de toute responsabilité liée directement à la divulgation : précisons cependant à nouveau que ces mesures sont non seulement minimales mais également non exhaustives. Des mesures supplémentaires peuvent donc être établies par les médiateurs communautaires ; nous estimons toutefois dans un souci de clarté qu'il serait préférable que l'ensemble des mesures possibles soit explicité par les législateurs flamand et germanophone.

La procédure fédérale met sur pied des mesures de protection déjà conformes en plusieurs points avec les exigences européennes. Ainsi, la loi de 2013 établit également en premier lieu que le dénonciateur sera protégé contre toute mesure négative suivant l'alerte en dressant une liste non exhaustive des représailles interdites, qui correspondent par ailleurs sur de multiples points aux mesures de la liste de la directive²⁴⁵. Il revient au « *responsable hiérarchique le plus élevé de l'autorité administrative* » (qui n'est donc pas forcément la personne ayant fait subir des représailles) de démontrer que la sanction a été imposée indépendamment de la dénonciation ; si les médiateurs fédéraux arrivent cependant à la conclusion qu'une corrélation entre les deux éléments existe bel et bien, la personne ayant imposé des sanctions sera soumise à une procédure disciplinaire²⁴⁶. Telle sanction est également prévue pour le membre du personnel qui a « *agi ou pris des décisions dans le seul but d'entraver, de compliquer et/ou de clôturer l'enquête* », celui qui a donné de fausses informations aux médiateurs dans le cadre de leur enquête ainsi que la personne ayant utilisé les canaux existants afin de propager de fausses allégations²⁴⁷. Nous pouvons considérer que ces procédures disciplinaires répondent à la demande européenne de sanctions. Si le lien est donc prouvé, il sera demandé au supérieur hiérarchique le plus élevé « *d'annuler ou de compenser la mesure* » ; une proposition qu'il pourra refuser, s'exposant ainsi à une recommandation à « *l'autorité administrative concernée* » ainsi que le « *ministre responsable* ». Relevons également qu'à l'instar des mesures communautaires, il est également prévu ici la possibilité de mutation volontaire²⁴⁸. Afin d'être absolument en adéquation avec le texte européen, il faudra également prévoir des sanctions pour la personne de confiance d'intégrité ou les médiateurs violant l'obligation de confidentialité, tout comme il faudra inclure des règles relatives à l'exemption de responsabilité du lanceur, des mesures de soutien, ainsi qu'une disposition de non-renoncement des droits.

²⁴⁵ Loi du 15 septembre 2013, article 15, §2.

²⁴⁶ Loi du 15 septembre 2013, article 16, §5.

²⁴⁷ Loi du 15 septembre 2013, article 17.

²⁴⁸ Loi du 15 septembre 2013, article 16, §5 et §7.

Une révision de la procédure fédérale sera en outre nécessaire afin d'éviter qu'elle ne contredise l'esprit de la directive qui semble se concentrer sur une protection inconditionnelle. Or, la loi de 2013 prévoit que les mesures de protection peuvent être levées à tout moment par les médiateurs, et que celles-ci devront être levées quoiqu'il arrive dans les 3 ans suivant la conclusion du rapport de l'enquête des médiateurs, une « décision judiciaire définitive » ou encore la cessation des fonctions de la personne de confiance d'intégrité lorsque les mesures de protection ciblent cette dernière. Ces règles devront être supprimées en raison de leur non-conformité avec le texte européen, mais également du fait de leur incohérence : ainsi, une personne pourrait attendre l'écoulement du délai de 3 ans avant de faire subir une sanction au lanceur bien plus aisément en l'absence des mesures de protection. La procédure se montre en outre trop sévère en excluant le bénéfice de ces mesures au divulgateur ayant pris part dans la violation alléguée²⁴⁹ ; une condition qui n'est jamais envisagée par le législateur européen.

Les mesures de protection mises en place auprès de la FSMA, quant à elles, sont déjà très complètes même si elles ne répondent pas encore à l'entière des balises mises en place par la directive. On y retrouve également une interdiction totale des représailles ainsi que de manière générale tout « *autres types de (...) mesure préjudiciable consécutifs (...) au signalement des infractions* », avec encore une fois les mêmes règles en matière de charge de la preuve. Cependant, on retrouve à nouveau une limite de temps en ce que la preuve de l'absence de lien reposera sur la personne ayant fait subir la sanction uniquement dans les 12 mois suivant le signalement. À nouveau, ce genre de condition n'est pas compatible avec la conception qu'a le législateur européen de ces mesures de protection. Le lanceur d'alerte ayant subi une de ces mesures préjudiciables aura droit à une réparation qui pourra prendre la forme d'une demande de rétablissement des conditions de travail telles qu'elles existaient avant la sanction, ou la forme d'une indemnisation, pouvant être attribuée non seulement après refus de la demande mais également en tout temps. La loi précise également que le divulgateur pourra se faire assister par la FSMA, un terme vague qui pourrait englober les mesures de soutien prévues au sein du texte européen. On retrouve également parmi les mesures de protection l'exemption de toute responsabilité du fait de la divulgation, étant donné qu'il est dit au sein du texte que le dénonciateur ne saurait faire « *l'objet d'aucune action civile, pénale ou disciplinaire* » et qu'il ne peut être reconnu comme « *violant une quelconque restriction à la divulgation ou communication d'informations imposée par un contrat ou par une disposition législative, réglementaire ou administrative* ». Enfin, la loi établit également une interdiction de

²⁴⁹ Loi du 15 septembre 2013, article 15, §3 à 6.

renonciation à ces quelques mesures de protection en ce que toutes dispositions ou clauses contractuelles allant dans ce sens sont nulles²⁵⁰.

Section 2- Avancement de la transposition

Selon l'article 26 de la directive, les États membres se devront de transposer le texte de cette directive au sein de leur ordre national avant la date butoir du 17 décembre 2021²⁵¹. Ce délai maximum est donc de 2 ans à partir de la date suivant l'entrée en vigueur du texte européen, ce qui est le délai standard en droit européen²⁵². Cependant, cela ne veut pas forcément dire que le texte belge sera prêt dans les délais : il n'est en effet pas rare que les États membres, et spécialement notre pays, dépassent les dates limites de transposition. Le retard belge peut notamment s'expliquer du fait de son système fédéral enchevêtré comprenant plusieurs entités compétentes à différents niveaux de pouvoir.²⁵³

Cette particularité de la construction de notre pays vient également jouer un rôle ici : en effet, bien que le législateur fédéral soit compétent pour de nombreux domaines établis au sein du champ d'application matériel, certaines matières reviennent au législateur régional, qui a par ailleurs déjà transposé plusieurs directives visées dans le champ d'application.²⁵⁴ La spécificité de la matière implique cependant une participation de tous les législateurs du pays, en ce compris les législateurs communautaires. Il est en effet impensable d'imaginer que des infractions à des matières régies par différents législateurs (concernant par exemple, les marchés publics) ne peuvent être commises (ou apprises) au sein d'administrations relevant des Communautés. Une procédure de dénonciation devra donc également être envisagée par le législateur communautaire, les Communautés flamande et germanophone ayant l'avantage d'avoir déjà des législations réglant partiellement le sujet.

Au moment où ces lignes sont écrites, 2 propositions de résolutions (déposées par les groupes Ecolo/Groen et Défi) ont déjà demandé au gouvernement belge de transposer la directive

²⁵⁰ Loi du 2 août 2002, article 69bis, §2, 3 et 4.

²⁵¹ Directive (UE) 2019/1937, article 26, §1.

²⁵² V-L BENABOU, « La transposition des directives en droit interne : l'exemple du droit d'auteur », *Legicom* 2004, p.25.

²⁵³ T. MATERNE, « La résolution non contentieuse des procédures d'infraction par la Belgique », *Rev. Aff. Europ.*, 2013, pp.754-755.

²⁵⁴ Des compétences relatives à la sécurité des produits, la sécurité des transports et la protection de l'environnement : Loi spéciale de réformes institutionnelles du 6 août 1980, article 6, II, VI, 4° ; X, 10° et 11° ; XII, *M.B.*, 15 août 1980, p.9434.

européenne. Dans le même temps, une proposition de loi fédérale « *tendant à assurer un statut légal et une protection aux lanceurs d'alerte* » a également été déposée par le groupe PTB/PVDA et est actuellement encore pendante devant la Chambre des représentants. Cette proposition présente un intérêt incontestable pour ce mémoire, en premier lieu car elle constitue l'ébauche de la première loi de protection transversale des lanceurs d'alerte, et ensuite, car elle affirme vouloir s'appuyer sur les normes minimales de la directive 2019/1937 afin d'établir un régime législatif exhaustif dans le domaine. Pour autant, il est difficile de parler stricto sensu d'une transposition du texte européen, étant donné que certaines composantes importantes de ce dernier ne sont pas reprises par les rédacteurs de la proposition.

Au niveau régional, le parlement bruxellois a affirmé, dans l'annexe à l'exposé général du budget des recettes et des dépenses pour l'année 2021, avoir pour objectif d'adopter un texte transposant la directive pour cette année²⁵⁵. Rien n'a encore été proposé ou avancé du côté wallon et flamand ainsi qu'au niveau des Communautés.

Section 3 – Analyse de la proposition de loi

Sous-section 1- Champ d'application

§1. Champ d'application matériel

Les deux propositions de résolution déposées à ce jour sont en faveur d'un élargissement maximal du champ d'application²⁵⁶. C'est également le souhait exprimé dans la proposition de loi qui désire « *garantir un cadre complet et cohérent de protection des lanceurs d'alerte au niveau national* ». Ce document revient en outre sur la notion de « violation », en demandant que soient couvertes toutes les informations « *secrètes en vertu d'une législation ou d'un contrat* » : l'intérêt public de ces dernières ne devra pas non plus être établi avec certitude par le lanceur d'alerte²⁵⁷. Cette position nous semble hautement critiquable. Si nous sommes en

²⁵⁵ Annexe à l'exposé général, partie 2, Parl. Rég. Brux.-Cap., sess. ord. 2020-2021, A-268/2, p.203. Un avis juridique a été rendu en mars sur la transposition de la directive par le ministre des Finances et du Budget : Compte rendu intégral provisoire, séance plénière du vendredi 19 mars 2021 (matin), Parl. Rég. Brux.-Cap., sess.ord. 2020-2021.

²⁵⁶ Proposition de résolution relative à la protection des libertés fondamentales des lanceurs d'alerte et des journalistes, pp.8-9, *Doc. Parl.*, Ch.repr., sess.ord. 2019-2020, n°1069/001 ; Proposition de résolution relative aux mesures légitimes visant à protéger les lanceurs d'alerte qui divulguent, au nom de l'intérêt général, des informations confidentielles d'organisations publiques et d'entreprises, p.8., *Doc.Parl.*, Ch.rep., sess.ord. 2020-2021, n°1730/001.

²⁵⁷ Proposition de loi tendant à offrir un statut légal et une protection aux lanceurs d'alerte, pp 11-13 et 15, article 2, *Doc Parl.*, Ch.repr., sess.ord. 2019-2020, n°1380/0001.

faveur d'un élargissement du champ d'application pour une question de sécurité et de clarté, un agrandissement d'un tel écart nous semble contredire le but premier de la loi. Quel intérêt en effet de protéger celui qui diffuserait une information qui, bien qu'étant secrète, est tout à fait légale, n'est pas constitutive d'un abus de droit et est de plus susceptible de ne pas relever de l'intérêt public ? Ce système pourrait ainsi constituer une porte ouverte à non seulement l'impunité, mais également à la protection de personnes divulguant des informations pouvant potentiellement porter atteinte à la vie privée ainsi qu'à la liberté d'entreprendre. Retenons en dernier lieu un autre élément intéressant de la proposition de loi, qui inclut une notion de territorialité par l'ajout de la précision : « *Les faits ou les menaces en cause ne doivent pas nécessairement s'être produits, se produire ou menacer de se produire dans le Royaume de Belgique* ».²⁵⁸ On pouvait évidemment se douter que le législateur européen s'attendait que la transposition puisse concerner des violations de droit européen ne se produisant pas forcément dans l'État membre où l'information a été dévoilée. C'est cependant la première fois où ce fait est bien précisé et où la territorialité est même élargie : les informations peuvent même concerner des faits se situant au-delà de l'Union européenne. On voit ici la première affirmation de l'intention de placer la Belgique sur la scène internationale comme un pays protecteur de l'ensemble des lanceurs d'alerte, toutes nationalités confondues.

§2. Champ d'application personnel

À l'inverse de la directive qui ne mentionne le terme « lanceur d'alerte » que dans ses considérants pour ensuite utiliser le mot « auteur de divulgation » dans ses articles, la proposition de loi parle immédiatement de « lanceur d'alerte » et utilise cette notion tout le long de son texte. Cela n'est pas négligeable : non seulement cela constitue la première insertion du terme dans la loi nationale, mais c'est également encore un indice de la volonté belge d'aller vers la direction d'une loi de protection uniforme.

La proposition va même jusqu'à aller établir une définition (la première en Belgique !) du lanceur d'alerte, comme étant « *toute personne ou groupe qui signale ou divulgue des informations secrètes en vertu d'une législation ou d'un contrat* »²⁵⁹. Comme indiqué auparavant, le lanceur d'alerte ne devra donc pas forcément communiquer une ou des

²⁵⁸ Proposition de loi, article 3, al.4.

²⁵⁹ Proposition de loi, article 2, 1°.

violations ; toutefois, la condition européenne que ces informations ne soient pas publiquement connues est rencontrée en l'espèce, vu l'accent mis sur le caractère secret de ces dernières. De plus, la proposition met de côté l'exigence européenne que le lanceur d'alerte ait eu connaissance des informations dans un cadre professionnel, ce qui est préférable à notre sens. Rien n'est précisé quant à la situation du secret médical et du secret professionnel des avocats : cependant, au vu du champ d'application matériel extrêmement large d'« *informations secrètes en vertu d'une législation ou d'un contrat* », on peut considérer que ces derniers individus peuvent également être considérés comme lanceurs d'alerte dans cette situation. Il convient cependant de prendre en compte la formule de la Cour Constitutionnelle énoncée alors qu'elle examinait la conformité de l'obligation des avocats de communiquer des violations à la CTIF avec le secret professionnel : « *la règle du secret professionnel ne doit céder que si cela peut se justifier par un motif impérieux d'intérêt général et si la levée du secret est strictement proportionnée* ». ²⁶⁰

La proposition reprend également les catégories d'« *entités juridiques* » (en parlant ici de « *personne morale ou association de fait* ») et de « *facilitateurs* ». Bien qu'elle ne cite pas explicitement le concept de « *tiers en lien* » risquant également d'être frappé par des répercussions, on peut considérer qu'elle substitue ce dernier par la notion de « *famille* » du lanceur d'alerte ²⁶¹, une idée cohérente avec l'interprétation d'Amélie Lachapelle du tiers étant une personne passive au signalement mais subissant tout de même des représailles du fait de ce dernier. Cela exclut cependant la possibilité, explicitement prévue par la directive européenne, que le collègue (ou une autre personne en dehors du cercle familial) puisse faire partie de cette catégorie : une hypothèse pourrait être envisagée où un collègue très proche du lanceur d'alerte et étranger au signalement se voit « puni » pour la divulgation des informations par son employeur, conscient de l'amitié reliant les deux individus. En revanche, il est permis de penser que la proposition de loi étend indirectement la protection aux membres de la famille du facilitateur, étant donné qu'il y est écrit que le facilitateur sera « *assimilé* » au lanceur d'alerte et qu'il est également énoncé que le lanceur ainsi que sa famille bénéficient de plusieurs mesures de protection. ²⁶² La proposition précise également que les individus qui participent uniquement à la divulgation (« *notamment l'écrivain, le journaliste, le documentariste, le*

²⁶⁰ C.C, 24 septembre 2020, n°114/2020, *JLMB* 2020, p.1634.

²⁶¹ La proposition de loi établit que rentrent dans cette notion de « famille », les « *grands-parents, parents (père et mère), enfants, frères et sœurs (fratrie), demi-frères, demi-sœurs, marâtre et parâtre ainsi que la personne avec qui le lanceur d'alerte forme un couple.* »

²⁶² Proposition de loi, article 2, 2° et 3°.

réalisateur ou le producteur ») peuvent bénéficier des mesures de protection²⁶³ : dans la directive, il est clairement entendu que ce n'est le cas que si ces personnes ont connaissance des violations dans le cadre de leur travail et ont utilisé les canaux de signalement à leur portée. De plus, ces individus bénéficient déjà de plusieurs protections : la protection de la liberté de presse²⁶⁴ qui enclenche une interdiction de censure, l'article 10 de la CEDH qui leur impose des conditions moins strictes que les lanceurs d'alerte et un « droit à la collecte d'informations », qui peut également être détaché par l'analyse de textes et jurisprudences tant nationales qu'internationales.²⁶⁵ Relevons enfin qu'ils ne risqueront pas non plus de se voir poursuivre pour violation de secrets d'affaires en raison des exclusions et dérogations effectuées par le texte.²⁶⁶ En l'état actuel, l'ajout de protections supplémentaires ne nous semble pas essentiel sans être toutefois complètement inopportun.

La détermination du statut de lanceur d'alerte, en tant que condition préliminaire pour pouvoir bénéficier (et faire bénéficier aux membres de la famille) des conditions de protection, est dans la proposition effectuée de manière plus formalisée. En effet, une chambre spécifique, auprès du tribunal de première instance, composée « *d'un juge professionnel ainsi que de deux représentants d'associations de défense des droits de l'homme* », devra statuer sur l'attribution ou non de ce statut ; une reconnaissance sans laquelle aucune mesure de protection ne pourra être enclenchée²⁶⁷. Cette chambre judiciaire présenterait l'avantage de restreindre le risque de propagation de fausses informations en n'attribuant pas immédiatement le statut de lanceur à toute personne pouvant répondre à la définition générale donnée par la future loi belge. De plus, une reconnaissance juridique de ce statut enverrait un signal fort, qui découragerait déjà certaines sanctions éventuelles. Il faudrait toutefois s'assurer que cette procédure de décision reste dans des délais raisonnables afin d'éviter que des personnes voulant se faire reconnaître comme lanceurs d'alerte ne subissent déjà certaines représailles, et donc dans certaines situations demander à statuer en référé au stade de la détermination du statut. Nous nous interrogeons également sur la mise en œuvre pratique de la création de cette chambre : est-il en effet véritablement envisageable de trouver deux représentants d'associations de défense des droits de l'Homme disponibles auprès de tous les tribunaux de première instance pour chaque demande de reconnaissance du statut de lanceur d'alerte ?

²⁶³ Proposition de loi, article 3, al.1.

²⁶⁴ Constitution, articles 19 et 25.

²⁶⁵ Q. VAN ENIS, *La liberté de presse à l'ère du numérique*, Bruxelles, Larcier, 2015, pp.42-49 ; 62-94 ; 135-238 et 508- 563.

²⁶⁶ Directive (UE) 2016/943, articles 1 et 5.

²⁶⁷ Proposition de loi, article 4.

Très peu de précisions sont apportées par la proposition sur les critères que cette chambre devra prendre en compte afin d'accorder ce statut. Il est évident que cette reconnaissance n'est pas conditionnée à l'utilisation d'un quelconque canal de divulgation, étant donné que la proposition ne met aucune procédure de signalement en place. La situation est moins claire pour la conviction du lanceur d'alerte en la véracité de l'information signalée, en l'absence d'une confirmation explicite du texte sur la nécessité de ce critère. Il est toutefois permis de penser que cette condition aura une certaine importance dans cette évaluation, même si amoindrie par rapport aux indications de la directive, étant donné qu'il est clairement mentionné que le but des signalements est de « *dénoncer des faits ou des menaces passées* »²⁶⁸. Les critères établis par la jurisprudence de la Cour européenne des droits de l'Homme de prise en compte de l'intérêt public et de la bonne foi du lanceur sont aussi abandonnés dans l'évaluation proposée : finalement, « *le seul critère essentiel (...) reste, en définitive, le contexte de l'affaire* »²⁶⁹. Par cela, la proposition tend à laisser la détermination du statut entièrement aux mains de la chambre spécialisée, dans un but sous-entendu de ne pas exclure de la protection des situations qui n'auraient pas été envisagées au moment de la rédaction des travaux législatifs. Si cet objectif est légitime, il nous semble cependant inopportun en l'état actuel de laisser une telle marge de manœuvre à cette juridiction : au vu du peu de balises contenues dans la proposition de loi, le juge ainsi que les deux représentants de la société civile iraient plus loin que de la simple interprétation en créant de la loi, violant par ce fait tant le principe de division des pouvoirs que celui de la sécurité juridique.

Sous-section 2 - Mise en œuvre des procédures

Tel que déjà énoncé dans la première sous-section, les procédures de dénonciation sont les grandes absentes de cette proposition de loi. Les développements font pourtant bien référence à ces dernières, énonçant que les rédacteurs ne sont pas contraires à l'instauration de canaux internes pour autant que le lanceur d'alerte ne soit pas obligé d'utiliser ce type de procédure en premier lieu.

Il est difficile d'établir avec certitude les raisons derrière l'absence de précisions concernant l'instauration de ces procédures. D'une part, il est possible de penser que les rédacteurs

²⁶⁸ Proposition de loi, article 2, 1°.

²⁶⁹ Proposition de loi, pp.11-13.

n'envisageaient pas la mise en place de canaux externes et étaient plutôt favorables à autoriser une divulgation publique en tout temps : on remarque en effet qu'il n'est nullement fait mention d'une procédure externe et que la reconnaissance du statut, ainsi que les mesures de protection en découlant, ne sont pas conditionnés à l'usage d'un quelconque canal. De plus, les développements justifient le choix de ne pas exiger au préalable l'utilisation de la procédure interne par « *le risque de collusion (...) avec l'auteur de l'infraction ou avec la participation de l'autorité compétente* »²⁷⁰. Nous comprenons et partageons également ces préoccupations, mais nous défendons l'argument que déroger à cette procédure serait plus néfaste que bénéfique pour le lanceur d'alerte, ce qui irait donc à l'encontre de l'objet du texte européen. En effet, le canal externe nous semble utile afin que la personne en possession d'une information puisse avoir quelqu'un vers qui facilement se tourner lorsque l'utilisation du canal interne peut se révéler dangereuse (absence d'impartialité, risque de représailles et/ou de censure...). De plus, le canal externe pourrait permettre une analyse minutieuse de la violation et de ses conséquences, ce qui a pour conséquence d'avancer des solutions pouvant mettre un terme à ces atteintes. Ce processus a également pour avantage de distinguer les violations véridiques des fausses informations, évitant ainsi la propagation de mésinformations sur la place publique. Enfin, ces procédures présentent des garanties de confidentialité de l'identité de l'auteur ainsi que parfois d'anonymisation ; des protections qui peuvent s'avérer essentielles pour le lanceur d'alerte.

D'un autre côté, il est tout aussi possible que la proposition fasse un choix volontaire de mettre la question des procédures temporairement sur le côté afin d'y revenir plus tard – que ce soit par texte législatif ou par arrêté lié à la présente proposition. Il est également envisageable que les procédures existantes soient maintenues sous réserve des modifications exposées plus haut, et servent de modèle pour des canaux supplémentaires sectoriels.

Sous-section 3 - Mesures de protection proposées

Bien que la proposition ne s'accorde pas avec la directive sur plusieurs points, les deux textes se rejoignent sur la nécessité de protéger le lanceur d'alerte et ses proches de toutes mesures prises pour sanctionner le signalement ; la proposition précisant par ailleurs que sont également interdites les représailles « *indirectes* » ou encore les « *préjudices* », deux termes encore flous

²⁷⁰ Proposition de loi, p.13.

mais avec une potentielle interprétation large qui pourrait également viser les menaces. On retrouve ensuite dans les deux documents une liste de mesures réputées être interdites : l'inventaire établi au sein de la proposition comprend une large partie des mesures reprises par la directive et se révèle de même être non exhaustif du fait de l'inclusion au sein de ces représailles de « *toute ingérence à la liberté d'expression* »²⁷¹, terme général pouvant englober toutes les situations qui n'avaient pas été envisagées par les rédacteurs au moment de l'émission de la proposition. Autre point de concordance entre les deux textes, la présence d'une disposition rendant nulle toute clause empêchant le lanceur d'alerte de profiter de ses droits et des mesures de protection.²⁷²

La proposition établit ensuite des règles concrètes mettant en œuvre « *les mesures nécessaires* » demandées par le texte européen « *pour garantir que les [lanceurs] soient protégés contre les représailles* ». ²⁷³ Dans les cas où un lanceur d'alerte reconnu ou un membre de sa famille est victime (ou risque d'être victime) de représailles du fait du signalement, ces individus peuvent saisir en référé le président du tribunal de première instance. Il n'y aura pas besoin dans ce cas de vérifier l'urgence de la demande qui justifie la saisie en référé étant donné que celle-ci est présumée du fait du statut de lanceur d'alerte. Le juge pourra alors prendre les mesures nécessaires pour stopper les représailles ainsi que punir la personne imposant ces dernières, sauf si ce dernier prouve que les mesures prises à l'encontre du lanceur d'alerte ne sont aucunement liées à la fuite d'information. Cette mesure nous semble être une solution adéquate pour prévenir tout risque qu'encourt le lanceur d'alerte et ses proches, permettant à la fois une réaction rapide à l'imposition de n'importe quelles représailles ainsi que la mise en œuvre des sanctions réclamée par la directive contre les personnes faisant subir des représailles. De plus, le texte parlant de « prévenir » les représailles, cette mesure peut être en toute logique utilisée contre des tentatives de représailles, rejoignant l'interdiction absolue de toute forme de représailles établie à l'article 19 de la directive. L'usage de l'outil juridictionnel est également un bon choix en ce qu'il peut permettre aux personnes concernées par l'information (dans les cas où ils sont également les auteurs des mesures assimilées aux représailles) de bénéficier des droits de la défense et d'être entendues comme le demande la directive : la proposition précise en effet bien que les parties se doivent d'être « *dûment convoquées* »²⁷⁴ et exclut donc la possibilité de procédure unilatérale.

²⁷¹ Proposition de loi, article 3.

²⁷² Proposition de loi, article 4.

²⁷³ Directive (UE) 2019/1937, article 21, §1.

²⁷⁴ Proposition de loi, article 6, §1.

Si la proposition laisse le soin au juge de déterminer quelles mesures prendre en fonction des représailles subies, elle impose tout de même une réparation spécifique en cas de résiliation du contrat de travail. En effet, dans ces cas-ci, l'individu ayant eu reconnaissance du statut de lanceur d'alerte (et non pas un membre de sa famille ici, ce qui peut être critiqué) peut demander « *au président de la juridiction du travail statuant en urgence* », après convocation des parties, « *de constater la nullité de la résiliation du contrat de travail et (...) de requérir la réintégration du travailleur sous peine d'astreinte* »²⁷⁵. À nouveau, cette mesure proposée semble efficace, répondant aux exigences européennes de mise en place de mesures de protection efficaces contre les représailles ; de sanctions effectives, proportionnées et dissuasives ainsi que de respect des droits de la personne impliquée. Il est possible d'établir un parallèle avec les mesures de protection établies par la FSMA où un travailleur a la possibilité de demander réintégration, en cas de licenciement mais également de modification unilatérale du contrat de travail, aux conditions prévalant avant l'imposition de la sanction. Il serait peut-être avantageux de davantage s'inspirer de cette procédure afin de bien préciser que les conditions doivent être les mêmes que celles d'avant représailles et d'étendre cette demande de réintégration à la modification unilatérale des conditions de travail.

La proposition reprend les mesures de soutien de la directive tout en les étoffant : les lanceurs auront ainsi droit à « *des informations et des conseils complets, indépendants et facilement accessibles au public, sans frais* » sur les différentes possibilités de protection face aux représailles ainsi que « *d'une aide juridique (...) totalement gratuite pour toute procédure entrant dans le champ d'application de la protection* » découlant du statut accordé par la loi. Prouvant encore une fois son objectif d'accorder la protection la plus large possible aux lanceurs, le texte met également en œuvre les possibilités laissées par la directive tout en les étendant en établissant « *des organismes d'intérêt public spécialisés dans l'assistance et la protection des lanceurs d'alerte* » offrant une assistance sur plusieurs niveaux « *notamment judiciaire, administratif et psychosocial* » et pouvant agir « *en justice au nom et pour cause du lanceur d'alerte* ». ²⁷⁶

Une autre mesure de protection en lien avec le texte européen et accordée dès la reconnaissance du statut de lanceur d'alerte est une impunité totale au civil pour une faute « *ayant un lien connexe avec les faits ayant conduit à l'octroi du statut* » ainsi qu'au pénal pour une infraction possédant la même connexité, sauf si l'infraction en question constitue un homicide ou des

²⁷⁵ Proposition de loi, article 6, §2.

²⁷⁶ Proposition de loi, article 7.

coups et blessures volontaires ou involontaires, de la torture ou encore des traitements inhumains ou dégradants.²⁷⁷ C'est un moyen astucieux d'éviter la limitation de protection des lanceurs qui aurait eu lieu si les termes européens concernant les infractions pénales étaient repris tels quels, tout en faisant bien savoir que la divulgation d'informations ne peut justifier certains actes hautement répréhensibles. Pour autant, nous pensons que l'utilisation du terme vague « *lien connexe* » présente des dangers d'excuser les lanceurs de fautes ou d'infractions qui pouvaient être évitables. Nous estimons donc qu'il serait utile d'ajouter les précisions se trouvant dans le texte européen concernant la non-exonération lorsque le lanceur ne disposait d'aucun motif pour penser que la divulgation publique était nécessaire afin de révéler les informations ou pour un fait ayant été au-delà de ce qui était nécessaire pour la divulgation de l'information.

Tel qu'énoncé plus haut, l'absence des canaux a également entraîné la disparition de toute garantie de confidentialité, ce qu'on pourrait regretter. En revanche, la proposition met sur pied une dernière mesure de protection forte, n'étant pas envisagée par la directive et à portée internationale. En effet, il est exigé de l'État belge d'accueillir les lanceurs d'étranger au sein du pays, leur accordant un visa humanitaire et leur offrant toutes les mesures fournies aux nationaux ayant ce même statut, moyennant les mêmes procédures avec assistance de l'État. Ces lanceurs se verront accorder un permis de séjour d'un an, pouvant être renouvelé chaque année, avec l'optique d'une possibilité de demande de permis de séjour illimité au bout de 5 ans.²⁷⁸ La directive n'aurait évidemment pu suggérer telle mesure, étant donné qu'il a été clairement énoncé par le passé que la matière des visas humanitaires de longue durée (plus de 90 jours) était en dehors de son champ de compétences²⁷⁹. Pourtant, malgré cette absence au niveau européen, cette volonté d'octroi de visa humanitaire se retrouve également dans les deux propositions de résolution déposées à ce jour²⁸⁰ : il est donc fort probable que ce point, faisant l'unanimité entre plusieurs partis, se retrouve bien dans la future loi belge sur le sujet.

Ces visas humanitaires ne concernent pas le citoyen européen et les membres de sa famille qui bénéficient de droits de séjour de durée variable si ceux-ci suivent certaines conditions établies

²⁷⁷ Proposition de loi, article 5 ; Code pénal, articles 392 ; 417bis ; et 418.

²⁷⁸ Proposition de loi, article 8.

²⁷⁹ Arrêt X et X c. État Belge, C-638/16, :EU :C :2017 :173.

²⁸⁰ Proposition de résolution relative à la protection des libertés fondamentales des lanceurs d'alerte et des journalistes, p.13 ; Proposition de résolution relative aux mesures légitimes visant à protéger les lanceurs d'alerte qui divulguent, au nom de l'intérêt général, des informations confidentielles d'organisations publiques et d'entreprises, p.8.

par la directive 2004/38, qui sont indépendantes de la qualité de lanceur d'alerte²⁸¹. La proposition établit cependant également une protection nationale pour les étrangers européens : il est ainsi affirmé que l'état belge ignore le mandat d'arrêt européen lorsque ce dernier demande la remise d'un lanceur d'alerte.²⁸² L'exécution d'un mandat d'arrêt européen peut déjà être refusée dans plusieurs cas dressés de manière exhaustive par la loi belge, reprenant les exemptions listées dans la décision-cadre européenne : la non-remise du lanceur d'alerte pourrait être justifiée par une de ces causes, ne nécessitant ainsi pas une modification de la loi qui pourrait s'avérer contraire au texte européen. L'état belge pourrait ainsi décider de ne pas remettre cet individu car « *l'autorité judiciaire belge a décidé soit de ne pas engager des poursuites pour l'infraction faisant l'objet du mandat d'arrêt européen soit d'y mettre fin* » en raison de l'exonération de responsabilité ou, si le lanceur a également effectué une infraction pénale interdite par la proposition, parce que « *la personne (...) est poursuivie en Belgique pour le même fait que celui qui est à la base du mandat d'arrêt européen* »²⁸³. On peut également se trouver dans le cas où l'infraction avancée par les autorités mettant en place le mandat d'arrêt est soupçonnée être un prétexte afin de pouvoir sanctionner le lanceur d'alerte de ces révélations : dans ce cas, les autorités belges peuvent mettre en avant le fait de vouloir protéger les droits fondamentaux du lanceur d'alerte.²⁸⁴ Cependant, cette dernière solution ne devra être retenue qu'en dernier recours afin d'éviter d'éventuels conflits avec la Cour de Luxembourg qui estime qu'en raison du principe de confiance mutuelle, les droits fondamentaux ne peuvent justifier la suspension du mandat d'arrêt européen uniquement dans des situations exceptionnelles²⁸⁵. Ces mesures envoient un signal fort à la communauté internationale que notre pays est un État ultra-protecteur des lanceurs d'alerte et de la liberté d'expression en général.

²⁸¹ Directive 2004/38/CE du Parlement européen et du Conseil du 29 avril 2004 relative au droit des citoyens de l'Union et des membres de leur famille de circuler et de séjourner librement sur le territoire des États membres modifiant le règlement (CEE) no 1612/68 et abrogeant les directives 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE et 93/96/CEE, articles 6 à 21 et 27 à 33, *J.O.U.E.*, 30 avril 2004, L158, pp.92-110 et 113-119.

²⁸² Proposition de loi, article 8, 2°.

²⁸³ Décision-cadre du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres, article 4, 2° et 3°, *J.O.U.E.*, 18 juillet 2002, L190, pp. 2 et 4 ; Loi du 19 décembre 2003 relative au mandat d'arrêt européen, article 6, 1° et 2°, *M.B.*, 22 décembre 2003, p.60075

²⁸⁴ Décision-cadre du 13 juin 2002, articles 1, 3° ; Loi du 19 décembre 2003, articles 4, 5°.

²⁸⁵ C. RIZCALLAH, « « Arrêt LM » : un risque de violation du droit fondamental à un tribunal indépendant s'oppose-t-il à l'exécution d'un mandat d'arrêt européen ? », *J.D.E.*, 2018, pp.348-350.

Conclusion

La Belgique possède actuellement très peu de textes organisant la protection des lanceurs d'alerte, étant donné qu'on ne dénombre pour l'instant que deux législations prises au niveau fédéral portant sur des domaines bien particuliers et deux législations au niveau du secteur financier. Au niveau européen, le législateur a uniquement pris en compte la situation des lanceurs dans des situations diverses et très ciblées, créant un cadre général assez flou. Pour les domaines non visés par ces diverses législations sectorielles nationales et européennes, le lanceur d'alerte pourra uniquement se reposer sur la jurisprudence de la Cour européenne des droits de l'Homme. Or, celle-ci impose la réunion d'un nombre non négligeable de critères stricts en l'absence desquelles il est possible d'estimer que les représailles subies par le lanceur constituent l'exercice d'une restriction autorisée à la liberté d'expression. Il existe donc encore de trop nombreux domaines où le lanceur d'alerte se retrouve désarmé juridiquement face à certaines répercussions.

L'obligation de transposer la directive européenne sur la protection des personnes qui signalent des violations du droit de l'Union pourrait donner l'impulsion nécessaire permettant d'organiser une protection uniforme des lanceurs d'alerte. En effet, malgré le fait que le champ d'application déjà très large du texte européen laisse certaines matières de côté, le caractère d'intensité minimale de son champ d'application permet au législateur belge d'englober encore plus de domaines avec sa loi de transposition. C'est ce qui est prévu par la proposition de loi, qui élargit exagérément son champ d'application aux actes simplement secrets, ce qui est critiquable sur de nombreux points. Cette transposition pourrait également permettre de réviser la majorité des quelques procédures belges existantes afin de garantir un maximum d'efficacité dans la façon dont les révélations seront effectuées ainsi que dans la protection des divulgateurs.

La directive a pour avantage de mettre sur pied un champ d'application personnel large, étant bien moins restrictif que ceux proposés par la jurisprudence de la Cour européenne et par les législations belges existantes. En effet, il est seulement exigé du lanceur qu'il ait eu connaissance de l'information dans un contexte professionnel, qu'il croie en la véracité de son allégation et qu'il utilise les canaux de divulgation. Les facilitateurs ayant aidé à la divulgation et les tiers en lien avec le lanceur sont également protégés. Cependant, on peut estimer que ce champ reste trop restreint, en ce qu'il ne prend pas en compte les personnes pouvant avoir connaissance de l'information dans un contexte privé. Il faut espérer que la transposition belge résoudra cet inconvénient : c'est en tout cas le sens dans lequel va la proposition de loi, qui ne

reprend pas cette condition de « cadre professionnel », limite de plus les tiers en lien à la notion de famille et étend la protection aux personnes uniquement concernées par la divulgation. Le statut du lanceur d'alerte sera en outre déterminé par une chambre spécifique composée d'un juge professionnel et de deux représentants d'associations de défense des droits de l'Homme. Peu de critères sont donnés quant à l'évaluation faite par cette chambre, ce qui est inquiétant au regard des principes de division de pouvoir et de sécurité juridique.

Le texte européen envisage également la manière dont le lanceur pourra porter son alerte, ayant le choix d'utiliser soit un canal interne, soit un canal externe ; même si l'usage du premier type de canal en premier lieu est recommandé. La divulgation publique est également envisagée, mais uniquement dans trois hypothèses déterminées.

Le canal interne doit être instauré dans toutes les entités privées de minimum 50 travailleurs et dans toutes les entités publiques, même si l'État membre peut décider d'imposer cette obligation plus largement dans le secteur privé et/ou plus étroitement pour certains établissements publics. Malgré quelques balises, la directive laisse une liberté relative dans l'instauration de ce canal privé ; une marge de manœuvre qui est plus restreinte en ce qui concerne le canal externe. Les États peuvent cependant autoriser les autorités en charge de cette procédure de mettre sur le côté certaines informations, indéfiniment pour certaines, mais cette possibilité formulée de manière floue inquiète quant à la possibilité de dérives de la part d'autorités mal intentionnées. Des canaux similaires sont déjà prévus par les législations sectorielles belges. Même si les procédures communautaires ne mettent en place qu'une procédure externe, on peut imaginer que cela est acceptable au regard du texte européen qui estime qu'un fournisseur de canal externe peut également s'occuper des mécanismes internes. Tous les canaux belges se devront cependant d'être révisés en cas de maintien, ne répondant en effet que de manière imparfaite aux balises mise en place par la directive. En ce qui concerne les autres secteurs non visés par une loi spécifique, rien n'a encore été proposé quant à l'instauration de canaux de signalement.

Enfin, le texte européen demande une protection contre les représailles découlant de la divulgation, la preuve de la non-existence d'une telle corrélation devant être rapportée par la personne ayant imposé la sanction. Cette protection passe par plusieurs mesures telles que la confidentialité de l'identité du divulgateur, une exonération de responsabilité civile et pénale pour les faits relatifs à la divulgation (mais uniquement civile pour les faits relatifs à l'obtention de l'information), des sanctions envers les personnes imposant des représailles et bloquant le signalement ainsi que diverses mesures de soutien. Les législations belges ont déjà mis en place plusieurs mesures de protection à l'encontre des lanceurs : elles s'accordent ainsi toutes sur les

règles en matière de charge de la preuve. Néanmoins, elles sont toutes incomplètes sur plusieurs points et les mesures mises en place au fédéral et au niveau de la FSMA limitent la protection dans le temps, ce qui est contraire à l'idéologie européenne. La proposition de loi, quant à elle, esquisse des mesures de protection enthousiasmantes et potentiellement efficaces, reprenant chaque possibilité laissée par le texte européen, à l'exception de la confidentialité. La proposition va même un pas plus loin en prévoyant l'octroi de visas humanitaires aux lanceurs étrangers non européens ainsi que le refus d'exécuter un mandat d'arrêt européen pour les lanceurs étrangers européens.

En conclusion, mettons-nous un instant à la place du législateur et décrivons ce que nous voudrions voir dans la future loi belge de transposition. Afin d'assurer une protection maximale des lanceurs d'alerte, nous souhaiterions inclure dans le champ d'application toutes les violations à la loi et les abus de droit, à l'exception des domaines visés par les procédures déjà mises en place pour un secteur particulier si ces dernières se sont révélées efficaces. Au niveau du champ d'application, nous reprendrions les catégories de facilitateurs et de tiers en lien ainsi que les conditions européennes : cependant, nous ne restreindrions pas le statut de lanceur d'alerte aux travailleurs et l'accorderions aux personnes privées, suivant l'information dévoilée et la conviction des personnes en la véracité et l'illégalité ou le caractère abusif du fait divulgué. Le président du tribunal de première instance apprécierait ces critères pour reconnaître ce statut en référé. Au niveau des canaux, nous instaurerions les procédures internes et externes au niveau de plusieurs secteurs, à l'égard de la procédure prévue par la FSMA. Le lanceur pourra choisir de saisir le canal de son choix, même si l'accent serait mis dans les informations incluses sur le site internet sur l'importance de d'abord passer par le canal interne en l'absence de risque de représailles direct. Il sera possible de communiquer l'information tant par écrit (mail ou courrier) que par téléphone ou par rencontre pour les deux canaux. La possibilité, pour les autorités en charge de la procédure externe, de rejeter les informations répétitives ou portant sur des violations mineures ainsi que de mettre de côté les allégations portant sur des violations de gravité moindre ne pourrait être mise en œuvre qu'après avoir établi une définition plus précise de ces différents termes pour éviter toute dérive. Les procédures sectorielles belges existantes seront maintenues sous réserve d'amendement comblant les manquements décrits au sein de ce mémoire. Enfin, pour les mesures de protection, il serait opportun de reprendre les mesures décrites dans la proposition de loi, en y rajoutant la confidentialité et la possibilité de réintégration dans les mêmes conditions de travail pour tout licenciement ou modification unilatérale des conditions de travail.

Bibliographie

Législation

Législation internationale

- Convention de sauvegarde des droits de l'Homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, approuvée par la loi du 13 mai 1955, article 10, *M.B.*, 19 août 1955, p.5028.

Législation européenne

- Traité sur le fonctionnement de l'Union européenne (version consolidée), articles 114 et 346, *J.O.U.E.*, 26 octobre 2012, C326, p.194.
- Charte des droits fondamentaux de l'Union européenne, article 47, *J.O.U.E.*, 18 décembre 2000, C364, p.20.
- Décision-cadre du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre Etats Membres, articles 1 et 4, *J.O.U.E.*, 18 juillet 2002, L190, pp. 2 et 4.
- Règlement (CEE) n°31 et (Euratom) n°11 du Conseil du 18 décembre 1961 fixant le statut des fonctionnaires et le régime applicable aux autres agents de la Communauté économique européenne et de la Communauté européenne de l'énergie atomique, articles 22 bis et 22 ter, *J.O.U.E.*, 14 juin 1962, R0031, p.1385.
- Règlement (CE) n°723/2004 du Conseil du 22 mars 2004 modifiant le statut des fonctionnaires des Communautés européennes ainsi que le régime applicable aux autres agents de ces Communautés, Annexe 1, *J.O.U.E.*, 27 avril 2004, L124, p.12.

- Règlement (UE, Euratom) n ° 1023/2013 du Parlement européen et du Conseil du 22 octobre 2013 modifiant le statut des fonctionnaires de l'Union européenne et le régime applicable aux autres agents de l'Union européenne, article 1, *J.O.U.E.*, 29 octobre 2013, L287, p.21.

- Règlement (UE) No 596/2014 du Parlement 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, 2003/125/CE et 2004/72/CE de la Commission, articles 1 et 32, *J.O.U.E.*, 12 juin 2014, L173, pp.16 et 50.
 - Directive d'exécution (UE) 2015/2392 de la Commission du 17 décembre 2015 relative au règlement (UE) n° 596/2014 du Parlement européen et du Conseil en ce qui concerne le signalement aux autorités compétentes des violations potentielles ou réelles dudit règlement, *J.O.U.E.*, 18 décembre 2015, L332, pp.126-132.

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, articles 4 ; 5 ; et 12 à 16, *J.O.U.E.*, 4 mai 2016, L119, pp.33 ; 35-36 ; 39-43.

- Règlement (UE) 2016/1011 du Parlement européen et du Conseil du 8 juin 2016 concernant les indices utilisés comme indices de référence dans le cadre d'instruments et de contrats financiers ou pour mesurer la performance de fonds d'investissement et modifiant les directives 2008/48/CE et 2014/17/UE et le règlement (UE) n° 596/2014, *J.O.U.E.*, 29 juin 2016, L171, pp.1-65.

- Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE, articles 4 ; et 14 à 18, *J.O.U.E.*, 21 novembre 2018, L259, pp. 57-58, et 61-64.

- Directive 2004/38/CE du Parlement européen et du Conseil du 29 avril 2004 relative au droit des citoyens de l'Union et des membres de leur famille de circuler et de séjourner librement sur le territoire des Etats membres modifiant le règlement (CEE) no 1612/68 et abrogeant les directives 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE et 93/96/CEE, articles 6 à 21 ; et 27 à 33, *J.O.U.E.*, 30 avril 2004, L158, pp.92-110 et 113-119.
- Directive 2008/99/CE du Parlement européen et du Conseil du 19 novembre 2008 relative à la protection de l'environnement par le droit pénal, article 2 renvoyant à l'annexe A et B, *J.O.U.E.*, 6 décembre 2008, L328, p.29 et pp.32-36.
- Directive 2009/65/CE du Parlement européen et du Conseil du 13 juillet 2009 portant coordination des dispositions législatives, réglementaires et administratives concernant certains organismes de placement collectif en valeurs mobilières (OPCVM), *J.O.U.E.*, 17 novembre 2009, L302, pp.32-96.
- Directive 2013/30/UE du Parlement européen et du Conseil du 12 juin 2013 relative à la sécurité des opérations pétrolières et gazières en mer et modifiant la directive 2004/35/CE, article 22, *J.O.U.E.*, 28 juin 2013, L178, p.84.
- Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE, article 71, *J.O.U.E.*, 27 juin 2013, L176, p.377.
- Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE, *J.O.U.E.*, 12 juin 2014, L173, pp.349-496.
- 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, articles 33 ; 37 ; et 38, *J.O.U.E.*, 5 juin 2015, L141, pp.99-100.

- Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, articles 4 ; 12 à 16, *J.O.U.E.*, L119, 4 mai 2016, pp.107 et 110-112.
- Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites, articles 1 à 3 ; et 5, *J.O.U.E.*, 15 juin 2016, L157, pp.5, 9,10 et 11.
 - Rapport sur la proposition de directive du Parlement européen et du Conseil sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites (Rapp : C. LE GRIP), *P.E Doc*, A8-0199/2015 du 22 juin 2015.
- 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, considérants 5 ; 7 à 12 ; 18 à 23 ; 27 ; 30 ; 31 ; 33 ; 36 ; 38 ; 41 à 44 ; 46 ; 47 ; 49 ; 53 ; 54 ; 62 ; 64 ; 67 ; 68 ; 79 ; 93 ; 102 ; 103 ; 106 ; 107 ; articles 1 à 26 ; et 28, *J.O.U.E.*, 26 novembre 2019, L305, p.17, 46
 - Résolution du Parlement européen sur l'examen à mi-parcours de la stratégie européenne 2007-2012 pour la santé et la sécurité au travail, *P.E Doc*, A7-0409/2011 du 15 décembre 2011.
 - Résolution du Parlement européen sur la criminalité organisée, la corruption et le blanchiment de capitaux : recommandations sur des actions et des initiatives à entreprendre (rapport final), *P.E Doc.*, A7-0307/2013 du 23 octobre 2013.
 - Résolution du Parlement européen sur les rescrits fiscaux et autres mesures similaires par leur nature ou par leur effet, *P.E Doc*, A8-0317/2015 du 25 novembre 2015.

- Communication de la Commission au Parlement européen et au Conseil sur d'autres mesures visant à renforcer la transparence et la lutte contre la fraude et l'évasion fiscale, *C.O.M.* (216) 451 final.

- Programme de travail de la Commission pour 2017, Répondre aux attentes – Pour une Europe qui protège, donne les moyens d'agir et défend, *C.O.M.* (2016) 710 final.

- Résolution du Parlement européen sur le rôle des lanceurs d'alerte dans la protection des intérêts financiers de l'Union européenne, *J.O.U.E.*, C252 du 18 juillet 2018, pp.58 et 59.

- Rapport 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'organisme public (Rapp : V.ROZIERE), *P.E Doc*, A8-0295/2017 du 10 octobre 2017.

- Proposition de directive du Parlement européen et du Conseil du 23 avril 2018 sur la protection des personnes dénonçant les infractions au droit de l'Union, *C.O.M.* (2018) 218 final.

Législation nationale

- Constitution, articles 19 ; 25 et 150.
- Code de droit économique, art. XI.332/2 ; XI.332/3 ; et XI. 332/5.
- Code pénal, articles 392 ; 417bis ; 418 ; et 461 et suivants.
- Loi spéciale de réformes institutionnelles du 6 août 1980, article 6, *M.B.*, 15 août 1980, p.9434.
- Loi du 22 mars 1995 instaurant des médiateurs fédéraux, article 14, *M.B.*, 7 avril 1995, p.8741.
- Loi du 2 août 2002 relative à la surveillance du secteur financier et aux secteurs financiers, articles 45 ; 69 bis ; 69 ter ; et 74, *M.B.*, 4 septembre 2002, p.39121.
- Loi du 19 décembre 2003 relative au mandat d'arrêt européen, articles 4 et 6, *M.B.*, 22 décembre 2003, p.60075.

- Loi du 5 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, articles 2 à 10 ; 12 ; et 14 à 17 *M.B.*, 4 octobre 2013, p.69406.
 - Rapport sur le projet de loi relatif à la dénonciation d'une atteinte suspectée à l'intégrité au sein d'une autorité administrative fédérale par un membre de son personnel et sur la proposition de loi modifiant la loi du 22 mars 1995 instaurant les médiateurs fédéraux, en ce qui concerne la protection des fonctionnaires qui dénoncent des irrégularités, *Doc. Parl*, Ch.repr., sess.ord. 2013-2014, n°2802/002.
- Loi du 31 juillet 2017 modifiant la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers, en vue de mettre en œuvre le Règlement (UE) n° 596/2014 sur les abus de marché et de transposer la Directive 2014/57/UE relative aux sanctions pénales applicables aux abus de marché ainsi que la Directive d'exécution (UE) 2015/2392 concernant le signalement des violations, et portant des dispositions diverses, article 13, *M.B.*, 11 août 2017, p.79443.
- Loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces, articles 1 ; 9 ; 10 ; 36 ; 47 ; 49 ; 57 à 59 ; et 90, *M.B.*, 16 octobre 2017, p.90838.
- Loi du 30 juillet 2018 relative à la protection des secrets d'affaires, article 6 ; 7 ; et 9, *M.B.*, 14 août 2018, p.64854.
- Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018, p.68616.
- Décret Comm.fl. du 7 juillet 1998 instaurant le service de médiation flamande, articles 3 ; 12 bis ; 17 bis ; et 18, *M.B.*, 25 août 1998, p.27221.
- Décr. Comm. fl. du 7 mai 2004 modifiant le décret du 7 juillet 1998 instaurant le service de médiation flamand, en ce qui concerne la protection de fonctionnaires qui dénoncent des irrégularités, *M.B.*, 11 juin 2004, p.44014.
- Décr. Comm. germ. du 26 mai 2009 instituant la fonction de médiateur pour la Communauté Germanophone, articles 3 ; 16.1 ; et 23, *M.B.*, 7 octobre 2009, p.66206.

- Arrêté Gouv. Flam. du 18 octobre 2013 portant création de l'agence autonomisée interne « Audit Vlaanderen » et modifiant divers arrêtés, article 2, *M.B.*, 27 novembre 2013, p.92210.
- Arrêté royal du 9 octobre 2014 portant exécution de l'article 3 §2 de la loi du 15 septembre 2013 relative à la dénonciation d'une atteinte suspectée à l'intégrité au sein d'une autorité administrative fédérale par un membre de son personnel, article 3, *M.B.*, 12 novembre 2014, p.89980.

Travaux préparatoires belges n'ayant pas encore abouti à un texte législatif

- Proposition de loi tendant à offrir un statut légal et une protection aux lanceurs d'alerte, *Doc. Parl.*, Ch.repr., sess.ord. 2019-2020, n°1380/0001.

- Avis de l'autorité de données précédant le projet d'arrêté du gouvernement wallon portant dispositions diverses relatives à l'information, par un membre du personnel, d'une irrégularité au sein d'un service du gouvernement ou d'un organisme d'intérêt public auquel est applicable le décret du 22 janvier 1998 relatif au statut du personnel de certains organismes d'intérêt public relevant de la Région wallonne

- Annexe à l'exposé général, partie 2, Parl. Rég. Brux.-Cap., sess. ord. 2020-2021, A-268/2, p.203.

- Compte rendu intégral provisoire, séance plénière du vendredi 19 mars 2021 (matin), Parl. Rég. Brux-Cap., sess.ord. 2020-2021.

Législation française

- Loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, articles 6 et 8, *JORF*, 10 décembre 2016.

Jurisprudence

Jurisprudence de la Cour européenne des droits de l'Homme

- Cour.europ. D.H, arrêt Guja c. Moldavie du 12 février 2008, <http://www.echr.coe.int> (19 octobre 2020).
- Cour.europ. D.H. arrêt Heinisch c. Allemagne du 21 octobre 2010, <http://www.echr.coe.int> (19 octobre 2020).
- Cour.europ. D.H. arrêt Bucur et Toma c. Roumanie du 8 avril 2013, <http://www.echr.coe.int> (19 octobre 2020).
- Cour. Europ. D.H arrêt Matùz c. Hongrie du 21 janvier 2015, <http://www.echr.coe.int> (19 octobre 2020).
- Cour.europ. D.H, arrêt Soares c.Portugal du 21 septembre 2016 ; <http://www.echrc.coe.int> (19 octobre 2020).
- Cour. Europ. D.H, arrêt Catalan c. Roumanie du 9 avril 2018, <http://www.echr.coe.int> (28 janvier 2021).
- Cour.europ. D.H, arrêt Halet c.Luxembourg du 11 mai 2021, <http://www.echr.coe.int> (11 mai 2021).

Jurisprudence européenne

- Arrêt Lawrie Blum/ Land Baden-Württemberg, C-66/85, :EU :C :1986 :24.
- Arrêt Centros, C-212/97, :EU :C :1999 :26.
- Arrêt X et X c. État Belge, C-638/16, :EU :C :2017 :173.

Jurisprudence belge

- C.C, 24 septembre 2020, n°114/2020, *JLMB*, 2020, liv.35, p.1634
- C.trav.Bruxelles (4^{ème} ch.), 22 juin 2016, *JLMB*, 2019, liv.13, p.580

Jurisprudence luxembourgeoise

- Cass. Luxembourg, 11 janvier 2018, *JLMB*, 2018, p.1796.
- Cour d'appel du Luxembourg (5^{ème} ch. Corr.), 15 mai 2018, *A&M*, 2018, p.102.

Doctrine

- BARDIN M., « Les « lanceurs d'alerte » à l'ère du numérique : un progrès pour la démocratie ? » in *Protection des données personnelles et sécurité nationale* (sous la dir. de BEAUREGARD-BERTHIER D. et TALEB-KARLSSON A.), Bruxelles, Bruylant, 2017, pp.249-274.
- BENABOU V-L, « La transposition des directives en droit interne : l'exemple du droit d'auteur », *Legicom* 2004, pp.23-36.
- BLAY- GRABARCZYK K., «Le statut du lanceur d'alerte dans les arrêts de la Cour européenne des droits de l'homme », *RevTrimDH*, 2018, pp.855-871.
- BOULALE MADAINÉ N., « La nouvelle directive 2019/1937 relative à la protection des « lanceurs d'alerte » : d'où elle vient, où elle va peut-être », *SK*, pp.459-475.
- CASSIERS V., « La transposition de la Directive 2016/943/UE du 8 juin 2016 sur la protection des secrets d'affaires en droit belge » in *Droit de la propriété intellectuelle* (sous la coordination de N.BERTHOLD et AL), Bruxelles, Larcier, 2019, pp.253-318.

- COBBAUT E., « Les lanceurs d’alerte : un objet juridique non identifié ? », *A&M*, 2018, pp.41-70.
- COBBAUT E., « L’encadrement de l’alerte et la protection du lanceur d’alerte (whistleblower) : l’affaire Luxleaks à l’aune d’un cadre européen en construction », *RDTI*, 2019, pp.47-85.
- COOLS S., « Klokkenluiden bij de FSMA en de Nationale Bank », *TVR-RPS*, 2018, pp.656-678.
- COTON F. et HENROTTE J-F., « Le lanceur d’alerte : une personne concernée par le traitement de ses données à caractère personnel, mais également par son avenir professionnel... », *RDTI*, 2016, pp.43-78.
- CUYPERS D., « Klokkenluiders : effectieve rechtsbescherming of niet?” in *Voor recht, rechtvaardigheid en Camus. Liber amoricum Bernard Hubeau*, Brugge, Die keure, 2018, pp.475-488.
- DERO-BUGNY, *Les rapports entre la Cour de justice de l’Union européenne et la Cour européenne des droits de l’homme*, Bruxelles, Bruylant, 2015.
- DETRAZ S., « Les sanctions relatives à la violation des règles sur la protection des lanceurs d’alerte selon la directive », *RAE*, 2019, pp.713-715.
- DE BEAUFORT V., *Du lobbying au e-lobbying*, Bruxelles, Larcier, 2019.
- DE PAUW P et MECHELYNCK A. « Les lanceurs d’alerte dans le secteur financier », *D.B.F-B.F.R.*, 2018, pp.52-64.
- FOURREZ A., “Complainte pour un fumeur – Réflexions à partir des arrêts de la Cour de Justice du 4 mai 2016 », *R.E.D.C*, 2016, pp.89-98.

- GAUL J., «Les lanceurs d’alerte et les répercussions pour les entreprises actives dans le domaine des marchés publics. Implications, critiques et réflexions », *Endroi*, 2020, pp.223-253.
- KAFTERANIS D., “The role of the European Parliament in the adoption of the directive on the protection of whistle-blowers”, *RAE*, 2020, n°4, pp.903-911.
- LACHAPELLE A., « Titre 6 – Le lancement d’alerte ou la délation organisée ? » in *Vie privée, liberté d’expression et démocratie dans la société numérique* (sous la dir. de Y.POULLET), Bruxelles, Larcier, 2020, pp.209-244.
- LACHAPELLE A., « L’encadrement juridique du lanceur d’alerte au sein de l’Union européenne. Commentaire de la directive sur les lanceurs d’alerte », *RDTI*, 2020, pp.15-52.
- LACHAPELLE A., « And thus Tax whistleblowing was born! Comment on the Directive on whistleblowers in tax matters”, *TFR*, 2020, pp.798-818.
- LACHAPELLE A., *La dénonciation à l’ère des lanceurs d’alerte fiscale*, Larcier, Bruxelles, 2021.
- MAGNIER V., « Avant-propos », *RAE*, 2019, pp.677-680.
- MATERNE T., « La résolution non contentieuse des procédures d’infraction par la Belgique », *Rev. Aff. Europ.*, 2013, pp.751-760.
- NELLES M., « Le procès Luxleaks, prémices d’un retournement de situation en faveur des lanceurs d’alerte ? », note sous Cass.Luxembourg, 11 janvier 2018, *JLMB*, 2018, pp.1803-1806.
- PACLOT Y. et V.MAGNIER «Un nouveau champ de protection pour les lanceurs d’alerte », *RAE*, 2019, pp.699-703.

- PORTIER P., « Les canaux de signalement interne et externe selon le droit européen, une avancée par rapport à la loi Sapin 2 ? », *RAE*, 2019, pp.705-708.
- RIZCALLAH C., « « Arrêt LM » : un risque de violation du droit fondamental à un tribunal indépendant s'oppose-t-il à l'exécution d'un mandat d'arrêt européen ? », *J.D.E*, 2018, pp.348-350.
- SNOWDEN E., *Mémoires Vives*, Paris, Editions du Seuil, 2019.
- VALLET-PAMAR J., « Genèse de la directive protégeant les lanceurs d'alerte », *RAE*, 2019, pp.681-697.
- VAN ENIS Q., *La liberté de presse à l'ère du numérique*, Bruxelles, Larcier, 2015.
- VAN ENIS Q., « Une solide protection des sources journalistiques et des lanceurs d'alerte : une impérieuse nécessité à l'ère dite de vérité ? » in *Le secret*, Limal, Anthemis, 2017, pp.95-152.

Divers

- Groupe de travail article 29 sur la protection des données, Avis 1/2006 relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière, adoptée le 1^{er} février 2006, p.14.
- Recommandation CM/REC (2014)7 du Comité des ministres aux États membres sur la protection des lanceurs d'alerte adoptée le 30 avril 2014.
- Règlement du 5 septembre 2017 de l'Autorité des services et marchés financiers précisant les règles de procédure applicables à la réception et au traitement des signalements d'infraction, articles 3 ; 4 ; 5 ; 7 ; 8 ; 9 ; 10 ; 11 ; 12 ; 13 ; et 14, M.B, 28 septembre 2017, p.89027.
- Circ. FSMA_2017_21 du 24 novembre 2017 relative aux procédures internes appropriées permettant le signalement d'infractions.

- Proposition de résolution relative à l'octroi de l'asile politique à Julian Assange, *Doc. Parl.*, Ch. Repr., sess. ord. 2019-2020, n°0977/001.
- Proposition de résolution relative à la protection des libertés fondamentales des lanceurs d'alerte et des journalistes, *Doc. Parl.*, Ch.repr., sess.ord. 2019-2020, n°1069/001.
- Proposition de résolution relative aux mesures légitimes visant à protéger les lanceurs d'alerte qui divulguent, au nom de l'intérêt général, des informations confidentielles d'organisations publiques et d'entreprises, *Doc.Parl.*, Ch.rep., sess.ord. 2020-2021, n°1730/001.

Sites Internet (dans l'ordre de leur apparition dans le mémoire)

- CHATEAURAYNAUD F., « Lanceur d'alerte », in Dictionnaire critique et interdisciplinaire de la participation (I. CASILLO avec R. BARBIERETAL. dir.), Paris, GIS démocratie et participation, 2013, disponible sur www.dicopart.fr (consulté le 24/03/2021).
- Page du site internet de la Commission permettant aux lanceurs d'alerte de communiquer des infractions relatives au droit de la concurrence (Whistleblower Communication Tools) : https://ec.europa.eu/competition-policy/cartels/whistleblower_en (consulté le 14/05/2021).
- Pétition sur le site de We Move EU demandant de prendre en compte la situation des lanceurs d'alerte dans le texte européen consacré aux secrets d'affaires : <https://act.wemove.eu/campaigns/les-lanceurs-d-alerte-en-danger> (consulté le 14/05/2021).
- « Enfin une protection pour les lanceurs d'alerte dans la fonction publique wallonne », 21 février 2019, <https://gouvernement.wallonie.be/home/presse/publications/enfin-une-protection-pour-les-lanceurs-dalerte-dans-la-fonction-publique-wallonne.publicationfull.html> (consulté le 14/05/2021).
- Page du médiateur fédéral informant sur la possibilité pour les membres du personnel de porter une atteinte au Point de contact central : <http://www.federaalombudsman.be/fr/integrite#:~:text=Le%20Centre%20Int%C3%A9grité%20aupr%C3%A8s%20du,une%20atteinte%20%C3%A0%20l'int%C3%A9grité%20%C3%A9> (consulté le 14/05/2021).
- Aperçu des procédures ayant menées à l'adoption de la directive 2019/1937 : <https://eur-lex.europa.eu/legal-content/FR/HIS/?uri=CELEX:32019L1937> (consulté le 14/05/2021).
- Section du site Fedweb consacrant certaines informations sur la procédure de dénonciation organisée par la loi fédérale de 2013 :

https://fedweb.belgium.be/fr/a_propos_de_l_organisation/administration_federale/mision_vision_valeurs/politique_federale_d_integrite/melding_van_een_integriteitssche nding (consulté le 15/05/2021)

- Section du site du médiateur fédéral consacrant certaines informations sur la procédure de dénonciation organisée par la loi fédérale de 2013 : http://www.mediateurfederal.be/sites/1070.b.fedimbo.belgium.be/files/procedure_de_denonciation.pdf (consulté le 15/05/2021).
- Section du site de la FSMA consacrant les informations relatives à la procédure de dénonciation à l'Autorité : <https://www.fsma.be/fr/faq/point-de-contact-lanceurs-dalerte> (consulté le 15/05/2021).
- Section du site de la FSMA consacré à sa politique de vie privée : <https://www.fsma.be/fr/faq/politique-vie-privee-de-la-fsma> (consulté le 15/05/2021).

