NOTE DE POSITION

ANALYSE ET RECOMMANDATIONS SUR LA TRANSPOSITION DE LA DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL SUR LA PROTECTION DES PERSONNES QUI SIGNALENT DES VIOLATIONS DU DROIT DE L'UNION

Le coût de la corruption pour l'économie de l'Union européenne est estimé à 120 milliards d'euros par an[1]. En Belgique, 4 milliards d'euros sont absorbés annuellement par la corruption dans la fonction publique[2]. Pour le secteur privé, plus de 6 entreprises sur 10 ont été victimes de criminalité économique, perpétrée dans 27% des cas en interne[3]. Le renforcement des interventions publiques pour lutter contre la pandémie de COVID-19 et pour soutenir les citoyens et les entreprises dans la crise économique, accroît considérablement les risques de corruption[4]. Avec la dégradation des finances publiques et de la santé financière des entreprises, une gouvernance plus forte s'érige dès lors comme une priorité absolue.

Pourtant, de sérieuses faiblesses systémiques – normative, institutionnelle et judiciaire – en matière de prévention et de répression de la corruption sont régulièrement mises en lumière par les rapports du Groupe de travail de l'OCDE sur la corruption et le GRECO[5]. La Belgique présente d'importantes lacunes juridiques, un manque alarmant de moyens dans la prévention de la corruption et une répression très faible – voire inexistante –, la reléguant au rang des pires élèves des pays de l'OCDE[6].

Le *whistleblowing* apparaît comme une alternative au silence[7]. L'alerte dont l'importance est reconnue par les instruments internationaux visant à combattre la corruption[8], est l'un des moyens les plus efficaces pour la prévenir et la détecter[9], en particulier lorsque des faiblesses dans l'application de la loi ont été décelées[10]. Les lanceurs d'alerte, qui effectuent un signalement dans l'intérêt général, permettent la détection, la prévention et la révélation de failles et dysfonctionnements au sein de la fonction publique, de l'économie, des systèmes financiers et sanitaires et contribuent ainsi à la transparence, l'intégrité et une meilleure gouvernance citoyenne et démocratique.

Seulement, la plupart des victimes ou témoins de corruption et d'autres actes répréhensibles ne signalent pas les faits par crainte de conséquences juridiques et financières (81%) ou parce qu'ils ignorent comment les signaler (49%)[11]. En outre, le cadre législatif relatif aux lanceurs d'alerte tel qu'il se présente actuellement est fragmenté et inégal d'un domaine d'action à l'autre, les exposant aux risques de représailles ou les réduisant au silence.

La directive européenne sur la protection des lanceurs d'alerte, qui doit être transposée d'ici octobre 2021, offre donc l'opportunité à la Belgique d'agir et de réaffirmer son engagement dans la lutte anticorruption et en faveur de la transparence, de la responsabilité et de l'intégrité au sein de notre société.

[1] Commission Européenne. *Rapport anticorruption de l'UE COM(2014) 38 final*, p.3.
[2] Selon une enquête internationale rapportée en 2016 par De Morgen et Het Laatste Nieuws. Un montant confirmé par Paul Meulemans, commissaire à l'Office central pour la Répression de la corruption (OCRC) jusque fin 2015. [3] PwC. *Global Economic Crime & Fraud Survey Belgian results* (2018), p.6.
[4] Kristalina Georgieva, Managing Director of the International Monetary Fund (IMF) speaking about anti-corruption efforts during COVID-19.
[5] OECD Working Group on Bribery. *Phase 3 report on implementing the OECD Anti-Bribery Convention in Belgium* (2013); GRECO. *Rapport d'évaluation Belgique GrecoEval5Rep(2019)3*.
[6] Transparency International. *Exporting Corruption Report* (2020).

POINTS POSITIFS DE LA DIRECTIVE

S'il est à déplorer que le régime de protection du lanceur d'alerte prévu par la directive ne s'inscrit pas dans un cadre plus large et ambitieux, TI Belgium accueille cette initiative comme un nouvel élan dans la lutte anti-corruption et se félicite qu'elle soit globalement conforme à nos principes. C'est ainsi que la Belgique devrait transposer les dispositions suivantes dans l'esprit de la directive :

- La **terminologie** choisie est positive. Le *whistleblowing* revêt encore une connotation et une perception culturelle négatives. Le choix de la terminologie est donc fondamental pour initier un changement culturel et favoriser son acceptation. Il convient de préconiser les termes « déclaration », « information » ou « signalement » plutôt que « dénonciation »[1].

- Le **champ d'application personnel** couvre un large éventail de lanceurs d'alerte dans le contexte professionnel qui dépasse la relation traditionnelle employé-employeur (art. 4).

- La directive suit une approche à la fois **préventive** et **curative** (art. 5(2)).

- Les **conditions de protection** des auteurs de signalement sont proportionnées et accessibles (art. 6).

- Les auteurs de **signalement malveillant ou abusif** ne sont pas protégés lorsqu'il est établi qu'ils l'ont fait sciemment.

- Les entités juridiques du **secteur public et privé** dépassant une certaine taille sont obligées d'établir des canaux et des procédures de signalement interne (art. 8 et 9).

- Les lanceurs d'alerte peuvent choisir de signaler l'information en **interne** ou **directement aux autorités compétentes** (art. 10). Les **divulgations publiques** sont également autorisées dans certaines circonstances (art. 15).

- Des **normes minimales** sont définies et encadrent les signalements internes et externes (art. 9, 12 et 13). En particulier, la **confidentialité** couvre toutes les informations permettant d'identifier les auteurs de signalement et les personnes concernées (art. 16).

- Une **obligation de suivi** des signalements interne et externe est instaurée (art. 9 et 11(2)).

---

[4] Transparency International Belgium. *Providing an alternative to silence: Towards greater protection and support for whistleblowers in Belgium* (2013). Transparency International Belgium. *Providing an alternative to silence: Towards greater protection and support for whistleblowers in Belgium* (2013). Articles 8, 13 et 33 de la Convention des Nations Unies contre la corruption ; Convention de l'OCDE contre la corruption ; Sections IX.iii et X.C.v, et annexe II de la recommandation de l'OCDE visant à renforcer la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales 2009 ; Article 9 de la Convention civile sur la corruption du Conseil de l'Europe ; Article 22 de la Convention pénale sur la corruption du Conseil de l'Europe.

[5] PwC. *Global Economic Crime & Fraud Survey Belgian results* (2018); ACFE. *Report to the Nations: global study on occupational fraud and abuse (Western Europe)* (2018). KPMG. *Global profile of fraudsters.* (2016); Kroll. *Global Fraud and Risk Report* (2020).

[6] Considérant 3 de la directive.

[7] European Commission. *Factsheet on EU whistleblower protection* (2018), p.2.

[1] Il est intéressant de noter que le législateur ait opté pour la notion de « dénonciation », encore culturellement associée à la délation, dans la législation relative aux lanceurs d'alerte pour les secteurs publics fédéral et flamand, alors qu'il a préféré les termes plus positifs « déclaration » et « information » dans la loi anti-blanchiment et pour le secteur financier. Cette observation donne à réfléchir sur les réelles intentions et motivations des politiques.

- Un large éventail de **mesures de protection contre les représailles** est prévu, y compris contre les formes les plus discrètes (art. 19) ainsi que contre les actions judiciaires en dehors du contexte professionnel notamment via une **exonération limitée de responsabilité** et un **renversement de la charge de la preuve** (art. 21).

- Des **recours** et une **réparation intégrale**, y compris des mesures provisoires, sont envisagés pour les dommages subis par les lanceurs d'alerte (art. 21(6) et 21(8)). Cette réparation doit se faire par le biais de compensations financières (couvrant les pertes financières actuelles et futures) et de mesures correctives (le traitement injuste est déclaré nul et non avenu). Des **mesures de soutien** incluant des informations et des conseils ainsi qu'une **assistance juridique** et **financière** sont envisagés (art. 20).

- Les représailles, les entraves, les procédures abusives et les manquements à l'obligation de confidentialité sont **sanctionnés** (art. 23).

RECOMMANDATIONS D'AMÉLIORATIONS

La directive, bien qu'elle constitue un pas important dans la bonne direction, n'est pas parfaite. Lors de la transposition, il serait souhaitable que le législateur comble les lacunes, renforce les faiblesses de la directive et aille plus loin que ce qu'elle prescrit en faisant de l'alerte un instrument complémentaire et efficace dans la lutte contre la corruption.

1. L'approche choisie par la directive est de construire un cadre juridique résolument centré sur la protection du lanceur d'alerte. La transposition doit garantir un juste équilibre entre sa protection et les finalités du système d'alerte. Le régime de protection doit servir une ambition plus large et positive.

2. En Belgique, le cadre juridique relatif aux donneurs d'alerte est fragmenté et inégal d'un domaine d'action à l'autre. La transposition doit veiller à ce que les procédures et les organes d'alerte préexistants soient maintenus et, dans la mesure du possible, harmonisés et alignés sur les normes minimales définies par la directive.

3. En vertu du principe de subsidiarité, le champ d'application matériel est restreint. La transposition doit l'étendre de façon à inclure toute infraction au droit belge, au droit européen et aux conventions internationales ratifiées par la Belgique, ainsi que toute menace ou préjudice grave pour l'intérêt général.

4. La transposition doit désigner les autorités disposant des pouvoirs nécessaires et des ressources suffisantes afin de garantir un ancrage institutionnel complet et cohérent assurant la mise en œuvre efficace de la directive.

5. La directive n'impose pas aux organisations d'obligation formelle d'assister et de protéger dans leur démarche les lanceurs d'alerte. La transposition doit inclure des dispositions supplémentaires visant à (ré)affirmer la responsabilité des organisations dans la mise en œuvre de leur système d'alerte interne.

6. La transposition doit imposer aux entités juridiques du secteur privé et public ainsi qu'aux autorités compétentes d'accepter les signalements anonymes et d'en assurer le suivi.

7. La transposition doit inclure les violations des règles relatives aux marchés publics comportant des aspects relatifs à la défense ou à la sécurité, en prévoyant un régime spécial conforme aux Principes Globaux sur la Sécurité Nationale et le Droit à l'Information.

8. La directive laisse la possibilité d'exempter certaines entités juridiques du secteur public. La transposition doit appliquer l'obligation d'établir des canaux de signalement interne à l'ensemble de celles-ci, sans exception.

9. La directive couvre un champ d'application personnel très large mais omet certaines catégories de personnes s'exposant à un risque de représailles. La transposition doit étendre le régime de protection aux personnes physiques qui, dans un contexte professionnel, ont l'intention d'effectuer un signalement ou que l'on croit ou soupçonne en être l'auteur.

10. La transposition ne doit en aucun cas réduire le niveau de protection offert par la directive et doit maintenir ou renforcer les dispositions relatives aux conditions de protection, à l'accessibilité des voies de signalement, au traitement des données à caractère personnel, aux mesures de soutien et à l'aménagement de la charge de la preuve dans l'esprit de ses considérants.

1 FONDEMENTS ET FINALITÉS

Recommandation : la transposition doit garantir un juste équilibre entre la protection du lanceur d'alerte et les finalités du système d'alerte. Le régime de protection doit servir une ambition plus large et positive, il doit être conçu et développé dans le but de[2] :

– renforcer l'état de droit, et en particulier la répression de la corruption ;

– favoriser la bonne gouvernance, la transparence, l'intégrité et l'obligation de rendre des comptes, et en particulier la prévention et la détection de la corruption ;

– manifester une culture plus ouverte fondée sur la liberté d'expression et d'information.

La notion de *whistleblowing* et les termes qui y sont associés revêtent généralement une connotation et une perception culturelle négatives malgré le rôle clé joué par les lanceurs d'alerte dans la sauvegarde de l'intérêt général[3]. Aussi, la terminologie utilisée, les finalités et les principes qui soustendent la politique seront déterminants pour sa réussite et son acceptation.

La directive vise prioritairement à renforcer l'état de droit dans l'Union en établissant un régime commun de protection minimum du lanceur d'alerte[4]. Compte tenu de son champ d'application personnel, la directive s'inscrit dans le contexte professionnel. TI Belgium se félicite que la directive rende compte de la « vulnérabilité économique » des donneurs d'alerte, du conflit de loyauté auquel ils sont exposés et du « déséquilibre de pouvoir inhérent à la relation de travail »[5]. En effet, ils sont « souvent confrontés à l'indifférence, à l'hostilité, voire, […] à des représailles »[6] lorsqu'ils signalent ou révèlent des informations d'intérêt général. « Assurer une protection équilibrée et efficace des lanceurs d'alerte » est donc essentiel dans « la révélation et la prévention » de la corruption et d'autres actes répréhensibles ainsi que dans la « préservation du bien-être de la société »[7].

---

[2] Conformément aux standards internationaux. Voir Conseil de l'Europe. *Recommandation CM/Rec (2014)7*, p.13; OECD, *Committing to Effective Whistleblower Protection* (2016), p.18; United Nations Office on Drugs and Crime. Resource Guide on Good Practice in the Protection of Reporting Persons (2015), p.22; G20 Anti-Corruption Action Plan. *Protection of Whistleblowers*, p.4.
[3] British Standards Institution. *Whistleblowing Arrangements Code of Practice* (2008), p.11.
[4] Article 1er de la directive.
[5] Considérants 36 et 39 de la directive.
[6] Conseil de l'Europe. *Recommandation CM/Rec (2014)7*, p.14.
[7] Considérant 1er de la directive.

Néanmoins, en adoptant une approche résolument centrée sur la protection du lanceur d'alerte, la directive confond la fin et les moyens. Cette observation doit amener le législateur à s'interroger sur les finalités réelles d'un système d'alerte et met en évidence le besoin d'un renversement de perspective : de l'auteur du signalement vers son contenu. Ce changement de paradigme n'a pas vocation à fragiliser la protection prévue par la directive ; il vise au contraire à la renforcer. Se concentrer essentiellement sur un régime de protection reviendrait à desservir l'objet même de la directive[8] ainsi que les intérêts des donneurs d'alerte, en focalisant l'attention sur leur personne.

Malgré la reconnaissance croissante de l'importance des lanceurs d'alerte au sein de notre société, TI Belgium souligne que « le passage d'une culture stigmatisante à une culture qui encourage et soutient véritablement les lanceurs d'alerte » est loin d'être une réalité[9]. Dans ce contexte, l'approche choisie par la directive ne permet pas de donner l'impulsion nécessaire à ce changement de paradigme. Il ne faudrait pas considérer la protection des lanceurs d'alerte comme une fin en soi, mais comme un moyen qui sert une ambition plus large et constructive, à l'image de la loi dite « Sapin 2 » en France[10] :

1. L'objectif de renforcer l'état de droit consacré par la directive trouve une résonance particulière au regard des faiblesses décelées dans la répression de la corruption en Belgique[11].

2. Les instruments internationaux visant à combattre la corruption reconnaissent l'importance des lois de protection des lanceurs d'alerte dans le cadre d'une lutte active contre la corruption[23]. Les études empiriques montrent que l'alerte permet de révéler entre 20 et 25% des cas de corruption et d'autres crimes économiques[12], faisant du *whistleblowing* l'un des moyens les plus efficaces pour détecter et prévenir la corruption. Il constitue ainsi un outil de bonne gouvernance indispensable, complémentaire – et non substituable aux dispositifs classiques de contrôle[25]– et vise à favoriser la transparence, l'intégrité et l'obligation de rendre des comptes[13].

3. Prévoir un cadre légal en matière d'alerte fait partie d'une démarche favorisant l'émergence de la transparence, de l'intégrité et d'une culture de la prise de parole. L'alerte trouve ses racines dans la liberté d'expression et d'information essentielle au bon fonctionnement d'une société démocratique[14].

Si « la mise en œuvre d'un système d'alerte implique un équilibre délicat dans lequel les intérêts légitimes de toutes les parties concernées doivent être conciliés »[15], il apparaît qu'un système d'alerte adéquatement encadré est bénéfique à l'organisation et à ses parties prenantes. Les retours d'expériences indiquent que le nombre de déclarations abusives ou malveillantes observées est systématiquement marginal par rapport aux préjudices découverts[16]. Plus globalement, le développement d'une culture de la transparence et de l'intégrité reste une priorité absolue à tous les niveaux de la société.

---

[8] Article 1er de la directive.
[9] Network of European Integrity and Whistleblowing Authorities. *Rome Declaration*, p.2.
[10] 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.
[11] Considérant 3 de la directive.
[12] PwC. *Global Economic Crime & Fraud Survey Belgian results* (2018); ACFE. *Report to the Nations: global study on occupational fraud and abuse (Western Europe)* (2018). KPMG. *Global profile of fraudsters.* (2016); Kroll. *Global Fraud and Risk Report* (2020). [25] Commission de la protection de la vie privée. *Recommandation n° 01 / 2006*, p.6.
[13] Considérant 2 de la directive. Voir aussi, Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, David Kaye en application de la résolution 25/2 du Conseil des droits de l'homme, A/70/361, 8 septembre 2015.
[14] Considérant 31 de la directive.
[15] Commission de la protection de la vie privée. *Recommandation n° 01 / 2006*, p.2.
[16] HTW Chur – EQS Group. *Rapport 2019 sur les alertes professionnelles* (2019).

2 HARMONISATION

Recommandation : la transposition doit veiller à ce que les procédures et les organes d'alerte préexistants soient maintenus et, dans la mesure du possible, harmonisés et alignés sur les normes minimales définies par la directive[17].

Le cadre juridique relatif aux lanceurs d'alerte tel qu'il se présente actuellement en Belgique est fragmenté et inégal d'un domaine d'action à l'autre. Seuls les secteurs publics fédéral et flamand font l'objet d'une législation relative aux lanceurs d'alerte[18]. D'autres dispositions couvrent directement[19] ou indirectement[20] certains aspects de la question de l'alerte.

L'absence d'un cadre national global se traduit par une protection hétérogène et insuffisante des lanceurs d'alerte. Plus fondamentalement, un grand nombre de cas susceptibles de porter gravement atteinte à l'intérêt public passe inaperçu[2122]. L'insécurité juridique et le manque de clarté constituent deux obstacles majeurs au signalement et à la protection des lanceurs d'alerte[35]. La directive offre donc l'opportunité de combler ce vide juridique en disposant d'une législation spécifique, complète et homogène en la matière afin de mieux protéger les auteurs de signalement et d'apporter la visibilité et la lisibilité nécessaires auprès des différents acteurs[23]. Ceci n'implique pas nécessairement d'adopter une loi unique mais plutôt de construire à partir du cadre incomplet existant, un cadre normatif qui « devrait refléter une approche globale et cohérente pour faciliter les signalements et les révélations d'informations d'intérêt général »[24].

Afin de veiller à la cohérence, à la clarté et à la sécurité juridique du système, TI Belgium encourage à maintenir les différentes dispositions et mesures préexistantes et à les aligner sur les normes minimales communes définies par la directive[25]. Les conditions et mesures de protection des lanceurs d'alerte, y compris les dispositions relatives à l'exonération limitée de la responsabilité[39], devraient être, dans la mesure du possible, harmonisées entre le droit pénal, le droit civil et le droit du travail. Dans son ensemble, le cadre normatif « doit être compris comme impliquant de la souplesse et de la synergie plutôt que de la rigidité et de l'uniformité »[2627].

---

[17] Conformément aux standards internationaux. Voir Transparency International. *International Principles for Whistleblowing Legislation* (2013), Principle 24; G20 Anti-Corruption Action Plan. *Protection of Whistleblowers*, p.8; OECD. *Committing to Effective Whistleblower Protection* (2016), p.11.

[18] 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 ; Arrêté du Gouvernement flamand du 13 janvier 2006 fixant le statut du personnel des services des autorités flamandes.

[19] Article 69bis de la 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 ; Chapitre Vbis de la loi du 4 août 1996 relative au bien-être des travailleurs lors de l'exécution de leur travail ; Titre IV Chapitre 2 de la 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 ; Article 27 de la loi du 10 juin 2006 sur la protection de la concurrence économique.

[20] Article 29, paragraphe 1er et 30 du Code d'instruction criminelle ; Articles 16, 17 et 63 de la loi du 3 juillet 1978 relative aux contrats de travail ; Article 1134, alinéa 3, du Code civil ; Loi du 10 mai 2007 tendant à lutter contre certaines formes de discrimination.

[21] Transparency International. *Best Practice Guide for Whistleblowing Legislation* (2018), p.66.

[22] % des personnes interrogées lors d'un Eurobaromètre spécial sur la corruption n'ont pas signalé la corruption dont elles ont été victimes ou témoins, principalement par crainte des conséquences juridiques et financières. 49% ne savaient pas où signaler ces faits. European Commission. *Factsheet on EU whistleblower protection* (2018), p.2.

[23] Banisar. *Whistleblowing: International Standards and Developments* (2009), pp.19-21.

[24] Conseil de l'Europe. *Recommandation CM/Rec (2014)7*, Principe 7, p.31.

[25] Considérant 20 de la directive.

[39] Article 21 de la directive.

[26] Conseil de l'Europe. *Recommandation CM/Rec (2014)7*, p.22.

[27] Conformément aux standards internationaux. Voir Transparency International. *International Principles for Whistleblowing Legislation* (2013), Principle 3; Conseil de l'Europe. Recommandation CM/Rec (2014)7, Principe 2, p.29.; Public Concern at Work. *Report on the Effectiveness of Existing Arrangements for Workplace Whistleblowing in the UK* (2013), p.17.

3 CHAMP D'APPLICATION MATÉRIEL

Recommandation : la transposition doit étendre le champ d'application matériel de façon à inclure toute infraction au droit belge, au droit européen et aux conventions internationales ratifiées par la Belgique, ainsi que toute menace ou préjudice grave pour l'intérêt général, dans les domaines tels que[41] :

- la corruption et les activités criminelles ;
- les violations de la loi et de la réglementation administrative ;
- les risques pour la santé et la sécurité publiques, la protection des consommateurs et de l'environnement ;
- les abus de pouvoir ;
- le détournement ou l'usage abusif de fonds publics ;
- les manquements graves aux obligations professionnelles et/ou déontologiques ou à la bonne gestion ;
- les conflits d'intérêts ;
- les violations des droits de l'Homme ;
- tout acte visant à dissimuler l'un de ces éléments.

En vertu du principe de subsidiarité, le champ d'application matériel de la directive est restreint aux infractions au droit de l'Union dans certains domaines spécifiques[28]. En l'état, les lanceurs d'alerte qui signalent des infractions au droit de l'Union dans d'autres domaines ou au droit belge, ne sont pas protégés. Cette situation accroît le risque de lacunes et d'insécurité juridique ainsi que la confusion et la méfiance des lanceurs d'alerte, ne sachant quelle information reporter ou si leur signalement est protégé[29].

Le maintien de cette approche au niveau belge serait contre-productif à la finalité d'un tel cadre juridique qui est précisément de « faciliter les signalements et les révélations d'informations d'intérêt général »[30] plutôt que de dissuader les lanceurs d'alerte ou d'omettre certaines formes d'actes répréhensibles. A cet effet, la directive encourage et laisse la possibilité[31] aux États membres d'étendre le champ matériel au droit national « en vue de garantir un cadre complet et cohérent »[32].

TI Belgium soutient que le champ matériel doit être le plus clair et le plus large possible de façon à inclure toute infraction au droit belge, au droit européen et aux conventions internationales ratifiées par la Belgique[33], ainsi que toute menace ou préjudice à l'intérêt général[34], en respectant un principe de

[28] Article 2, paragraphe 1 de la directive.
[29] United Nations Office on Drugs and Crime. *Resource Guide on Good Practice in the Protection of Reporting Persons* (2015), p.22; Council of Europe. *Protection of Whistleblowers: A Brief Guide for Implementing a National Framework* (2015), p.8.
[30] Conseil de l'Europe. *Recommandation CM/Rec (2014)7*, Principe 1, p.24.
[31] Article 2, paragraphe 2.
[32] Considérant 5 de la directive. Voir aussi la Communication COM(2018) 214 final.
[33] En particulier la Convention de l'OCDE sur la lutte contre la corruption.
[34] Cette approche est similaire à celle adoptée par la France et la loi dite « Sapin 2 ».

proportionnalité. Le dispositif d'alerte devrait se limiter aux « faits ou situations suffisamment graves qu'il faut [signaler] dans l'intérêt général ou dans celui d'une bonne gouvernance de l'organisation »[35].

Afin de définir la portée des informations qui entrent dans la définition de l'intérêt général, la loi doit éviter à la fois un excès de formalisme préjudiciable à son objectif – à savoir faciliter les signalements et les révélations d'informations d'intérêt général –, et une flexibilité excessive laissant la voie ouverte à un afflux de signalements non fondés ou à des divergences d'interprétation[36]. Conformément à l'exigence de bonne foi, la notion d'intérêt général s'applique au contenu du signalement et non aux motivations de son auteur[37].

Le cadre législatif belge sur le lanceur d'alerte illustre les deux approches principalement utilisées pour définir le champ matériel. Si au niveau flamand, il est défini de façon large et général (« exigence, abus ou délit »)[38], au niveau fédéral la définition est plus exhaustive et explicite en listant les catégories couvertes par le régime de protection[53]. Une approche intermédiaire est à préconiser en proposant une liste indicative[3940].

Enfin, la transposition pourrait explicitement exclure les matières déjà réglementées par la loi, tout en imposant aux organisations de les traiter distinctement via les procédures et les organes existants (► **recommandation 2**).

4 ANCRAGE INSTITUTIONNEL

Recommandation : la transposition doit garantir un ancrage institutionnel complet et cohérent et désigner la/les autorités disposant des pouvoirs nécessaires et des ressources suffisantes, et responsables de[55] :

– la réception et du dispatching des signalements externes ;

– leur suivi ;

– l'assistance et du soutien aux lanceurs d'alerte ; – la supervision et du contrôle de l'application de la loi.

La directive impose aux États membres de désigner les autorités compétentes pour mettre en œuvre les obligations prévues par la directive. De ces obligations découlent trois compétences clés à attribuer

[35] Commission de la protection de la vie privée. *Recommandation n° 01 / 2006*, p. 6.
[36] G20 Anti-Corruption Action Plan. *Protection of Whistleblowers*, p.20.
[37] Considérant 32 de la directive.
[38] Arrêté du Gouvernement flamand du 13 janvier 2006 fixant le statut du personnel des services des autorités flamandes. [53] 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.
[39] G20 Anti-Corruption Action Plan. *Protection of Whistleblowers*, p.20; Conseil de l'Europe. *Recommandation CM/Rec (2014)7*, Principe 2, p.29; Transparency International. *Best Practice Guide for Whistleblowing Legislation* (2018), p.13.
[40] Conformément aux standards internationaux. Voir Transparency International. *International Principles for Whistleblowing Legislation* (2013), Principle 27; Conseil de l'Europe. *Recommandation CM/Rec (2014)7*, p.22.

à une ou plusieurs entités distinctes : (1) la réception et le dispatching des signalements externes[41], (2) leur suivi[42] (au sens de l'article 5, point 12) et (3) l'assistance et le soutien aux lanceurs d'alerte[43].

En Belgique, le médiateur endosse un rôle central dans les processus d'alerte réglementés par la loi dans le secteur public fédéral et flamand[44]. Il reçoit les signalements externes ainsi que les plaintes en cas de représailles, en assure le suivi et offre une protection aux donneurs d'alerte. En Flandres, le médiateur est assisté par l'Audit interne de l'Administration flamande (« Audit Vlaanderen ») et par le guichet de bien-être et d'intégrité au travail de l'Autorité flamande (« Spreekbuis »). S'ils reçoivent tous deux les signalements, l'Audit interne mène les enquêtes, alors que le guichet traite les demandes d'information, conseille et redirige vers le service compétent. Au niveau fédéral, le médiateur dispose de responsabilités plus étendues puisque le Comité d'audit de l'Administration fédérale (ACFO-CAAF) n'est pas compétent pour mener les enquêtes[45].

C'est du côté répressif que, sans surprise, le bât blesse. Depuis 2013, le Groupe de travail de l'OCDE sur la corruption pointe le manque grave et systématique de ressources, de personnel et de formation au sein des autorités chargées des enquêtes, des poursuites et des condamnations[46]. Ce constat est partagé par un rapport du Groupe d'États contre la Corruption (GRECO) de 2019[47] selon lequel « la police fédérale est en crise ». Le rapport précise que « ce manque de moyens affecte particulièrement les services chargés de la prévention et de la lutte contre la corruption » et semble refléter qu'il ne s'agit pas d'une priorité politique. Par conséquent, l'Office central pour la répression de la corruption (CDBCOCRC) s'est résigné à devenir uniquement réactif et à négliger le travail pro-actif de prévention[48].

TI Belgium déplore vivement cette situation et rappelle « l'importance des divers éléments normatifs, institutionnels et judiciaires qui forment un tout cohérent dans lequel les voies permettant de signaler et de révéler des informations, les mécanismes d'enquête et de réparation, ainsi que les voies de recours juridiques pour la protection des lanceurs d'alerte s'articulent tous efficacement »[49] (► **recommandation 3**). A cet égard, le Médiateur fédéral et le Médiateur flamand ont souligné que la désignation des autorités compétentes signifie, pour certaines compétences, « la réaffirmation du rôle actuel de certaines autorités » et « pour d'autres, la création de telles autorités »[50].

TI Belgium souscrit aux recommandations du Réseau des autorités européennes en charge des lanceurs d'alerte (NEIWA)[66]. La transposition doit à savoir :

- « Désigner une ou plusieurs autorités chargées de recevoir et d'évaluer les rapports et veiller à ce que les divulgations concernant tous les domaines de politiques, ou impliquant plusieurs autorités, ou présentées par une personne dénonçant une violation, incapable d'identifier l'institution compétente, soient couvertes. » TI Belgium recommande de réviser le rôle existant des médiateurs et de leur octroyer de nouvelles compétences pour recevoir et traiter les

signalements externes, moyennant l'allocation de ressources supplémentaires. Cette option comporte l'avantage de s'appuyer sur l'expertise du Médiateur fédéral et du Médiateur flamand. Pour le secteur public, le Médiateur de la Wallonie et de la Fédération Wallonie-Bruxelles, le Médiateur bruxellois et le Médiateur de la Communauté germanophone devraient

[41] Article 11, paragraphe 2, points a) et b) et paragraphe 6 de la directive.
[42] Article 11, paragraphe 2, points c) à f) et paragraphes 3 à 5 de la directive.
[43] Article 20 de la directive.
[44] Pour mémoire, seuls les secteurs publics fédéral et flamand font l'objet d'une législation sur les lanceurs d'alerte.
[45] Pour une analyse plus exhaustive du cadre normatif belge voir Transparency International Belgium. *Providing an alternative to silence: Towards greater protection and support for whistleblowers in Belgium* (2013).
[46] OECD Working Group on Bribery. *Phase 3 report on implementing the OECD Anti-Bribery Convention in Belgium* (2013).
[47] GRECO. *Rapport d'évaluation Belgique GrecoEval5Rep(2019)3*, p.33.
[48] L'effectif statutaire de l'OCRC est passé de 120 personnes dans les années 2000 à 66 en 2018. Sur ces 66 personnes prévues, le service compte effectivement 39 personnes en 2018, soit un déficit en personnel de 40%. Ibidem.
[49] Conseil de l'Europe. *Recommandation CM/Rec (2014)7*, p.22.
[50] Network of European Integrity and Whistleblowing Authorities. *Rome Declaration*, pp. 2-3.
[66] Ibidem.

encadrer les signalements externes au sein de leurs entités juridiques respectives. Pour le secteur privé, il convient d'adopter une approche régionale selon la préférence linguistique.

- « Veiller à ce que les autorités compétentes disposent des pouvoirs et des capacités nécessaires pour assurer un suivi approprié des rapports à travers des enquêtes, des poursuites ou d'autres mesures correctives, ce qui leur permettrait également de fixer un seuil pour l'ouverture d'une enquête et de donner la priorité aux rapports qui ont le plus grand impact sur la société, tout en révisant régulièrement leurs procédures. » TI Belgium réaffirme le rôle crucial de l'OCRC[51] et demande l'augmentation du financement et des ressources des organismes publics chargés de lutter contre la corruption.

- « Établir qu'au moins une entité est chargée de fournir les informations requises sur les droits et la protection des personnes dénonçant une violation d'une manière compréhensible et reconnaissable et qu'il existe au moins une autorité en mesure de garantir un soutien effectif aux personnes dénonçant une violation contre les représailles, en veillant à ce qu'elle dispose des pouvoirs et des ressources nécessaires, y compris le pouvoir d'enquêter sur les mesures de représailles signalées ». Cette entité devrait également veiller à ce que les auteurs de signalement bénéficient, s'il y a lieu, de mesures de soutien sous la forme d'une assistance juridique et financière dans le cadre des procédures judiciaires.

TI Belgium plaide également pour qu'une ou plusieurs autorités responsables de superviser et contrôler l'application de la loi soit désignée(s) et dotée(s) d'un rôle analogue – quoique plus restreint – à celui de l'Agence Française Anticorruption. Ce/ces autorité(s) devrai(en)t disposer des pouvoirs nécessaires et des ressources suffisantes pour participer à la sensibilisation au système d'alerte, élaborer des recommandations et coordonner l'échange des connaissances, contrôler la conformité et l'efficacité des procédures d'alerte interne et, en cas de manquement, de les enjoindre de se conformer à leurs obligations avant de prononcer des sanctions, ainsi que pour collecter et publier les données sur les signalements prévus à l'article 27(2)[5253].

5 RESPONSABILITÉ ORGANISATIONNELLE

Recommandation : outre les normes minimales définies par la directive, la transposition doit inclure des dispositions supplémentaires visant à (ré)affirmer la responsabilité des organisations dans la mise en œuvre de leur système d'alerte interne, et en particulier à[69] :

– adopter des dispositifs de promotion, de communication et de formation du personnel au système de signalement ainsi que des procédures internes de protection des lanceurs d'alerte et d'évaluation de la politique ;

– établir la responsabilité de l'organisation en tant que personne morale en cas de manquement aux obligations prescrites par la directive ;

– prévoir et étendre des sanctions efficaces, proportionnées et dissuasives à l'ensemble des obligations prescrites par la directive pour les personnes physiques et morales.

[51] Pour une discussion complète sur le rôle du CDBC-OCRC voir Transparency International Belgium. *Providing an alternative to silence: Towards greater protection and support for whistleblowers in Belgium* (2013), p.20.
[52] Transparency International. *International Principles for Whistleblowing Legislation* (2013), Principles 28.
[53] Conformément aux standards internationaux. Voir Transparency International. *International Principles for Whistleblowing Legislation* (2013), Principles 15, 27 and 29. British Standards Institution. *Whistleblowing Arrangements Code of Practice* (2008), p.18.

La directive n'impose pas aux organisations d'obligation formelle d'assister et de protéger les lanceurs d'alerte, dans leur initiative. A titre d'exemple, aucune exigence en matière de promotion ou de formation

au dispositif d'alerte n'est envisagée. De même, aucune sanction n'est prévue pour les personnes physiques et morales qui ne respectent pas leurs obligations prévues par la directive. Dans son ensemble, celle-ci manque d'incitants pour que les organisations assument leurs responsabilités.

Lors de la mise en œuvre d'un système d'alerte interne, les organisations doivent prendre un engagement fort qui dépasse la simple conformité juridique et s'inscrit dans une démarche plus large (► **recommandation 1**). Ce n'est pas parce que des procédures sont en place et qu'elles répondent à toutes les exigences prévues par la loi, qu'elles seront en pratique utilisées. Elles doivent s'accompagner d'une culture organisationnelle encourageant la transparence, le dialogue et instaurant un climat de confiance[54]. L'alerte ne doit plus être considérée « comme un manquement à la loyauté, mais comme une responsabilité démocratique »[55] bénéfique, tant pour le personnel que pour l'employeur.

La législation peut néanmoins favoriser et promouvoir l'émergence d'un tel environnement. Il convient dès lors d'imposer certains critères minimums aux organisations tout en leur laissant la latitude nécessaire pour s'approprier et adapter le dispositif d'alerte à leur contexte spécifique[72] (structure, culture et nature des risques), en consultation avec les partenaires sociaux et en accord avec ceux-ci[56]. Si la directive définit des normes minimales strictes, TI Belgium plaide pour une (ré)affirmation de la responsabilité des organisations dans la mise en œuvre de leur système d'alerte interne :

1. Les lanceurs d'alerte privilégient généralement l'alerte interne et les organisations sont souvent les mieux placées pour la traiter[57]. La confiance dans les canaux internes et leur facilité d'accès sont deux éléments essentiels à l'efficacité du système d'alerte[58]. La sensibilisation du personnel à l'existence et au fonctionnement de la politique d'alerte est essentielle. La législation doit imposer aux organisations de communiquer proactivement leurs procédures et de mettre en place une formation régulière du personnel[76]. La direction et le management doivent prendre un engagement clair (formalisé par exemple dans leur Charte de gouvernance d'entreprise[59] ou leur code de conduite/de déontologie) encourageant les travailleurs à exprimer librement leurs préoccupations au sujet d'éventuels dysfonctionnements internes et en faveur d'une tolérance zéro contre les représailles[78].

2. Il incombe aux organisations de prévenir les actes répréhensibles et préjudiciables à l'intérêt général et, dès lors, de soutenir et de protéger les individus qui, de bonne foi, signalent des problèmes dont ils sont témoins conformément au cadre légal[60]. Elles doivent non seulement être tenues juridiquement responsables lorsqu'elles participent elles-mêmes activement aux représailles, mais également lorsqu'elles faillissent à leurs obligations imposées par la directive d'aider et de protéger les auteurs de signalement[61]. Comme c'est le cas pour ces derniers, le fait qu'une organisation ait agi conformément à la directive devrait pouvoir être

[54] OECD. *Committing to Effective Whistleblower Protection* (2016), p.12.
[55] Conseil de l'Europe. Recommandation CM/Rec (2014)7, Principe 2, p.27.
[72] International Chamber of Commerce. *Guidelines on Whistleblowing*, p.5.
[56] Article 8 paragraphe 1er de la directive.
[57] Considérant 33 de la directive.
[58] European Commission. *Factsheet on EU whistleblower protection* (2018), p.2.
[76] Conformément au considérant 59 de la directive.
[59] Pour les entreprises cotées conformément au Code belge de gouvernance d'entreprise 2020
[78] International Chamber of Commerce. *Guidelines on Whistleblowing*, p.4.
[60] Transparency International. *Building on the EU directive for whistleblower protection* (2019), p.10.
[61] Il est clair que seules les obligations prescrites par la directive aux entités juridiques du secteur privé sont ici visées.

invoqué comme moyen de défense dans les cas de poursuites ou comme cause d'exonération de responsabilité en droit pénal ou administratif[62].

3. Des sanctions efficaces, proportionnées et dissuasives devraient s'appliquer aux personnes morales et physiques qui, malgré leur obligation, ne mettent pas en place des canaux de signalement interne ou ne respectent pas les procédures de signalement interne et leur suivi[63].

L'implémentation de cette recommandation [64] requiert la désignation d'une/des autorité(s) compétente(s) pour superviser et contrôler l'application de la loi (► **recommandation 4**).

6 ANONYMAT

Recommandation : la transposition doit imposer aux entités juridiques du secteur privé et public ainsi qu'aux autorités compétentes d'accepter les signalements anonymes et d'en assurer le suivi dans le cadre du champ d'application[83].

La directive prévoit que les États membres puissent décider si les entités juridiques du secteur privé ou public et les autorités compétentes sont tenues d'accepter les signalements anonymes et d'en assurer le suivi[65]. Ce choix reflète le débat controversé autour du signalement anonyme qui est encore culturellement associé à la délation qui existe sous les régimes totalitaires[66]. Par conséquent, l'anonymat peut conduire à une focalisation sur l'auteur du signalement, en lui attribuant une intention malveillante[67]. Cette observation conforte l'importance d'opter pour une terminologie, des fondements et finalités instituant un changement positif dans la perception culturelle de l'alerte et dépassant la narrative traditionnelle (► **recommandation 1**).

En Belgique, la législation en vigueur interdit expressément l'anonymat[68]. A titre de comparaison, environ la moitié des pays de l'OCDE autorise le signalement anonyme dans le secteur public, pour 53% des entreprises disposant de mécanismes de signalement interne dans le secteur privé[69]. Outre la dimension culturelle, la position du législateur belge peut s'expliquer par les motifs notamment exposés par le Groupe 29[70] et repris par la Commission de la protection de la vie privée, pour justifier une « interdiction de principe des signalements anonymes »[90].

L'un des principaux risques invoqués est d'alimenter une culture de dénonciation et d'entraîner une dégradation du contexte social. En réalité, les organisations autorisant l'anonymat n'ont ni subi une détérioration du climat social, ni observé une culture de signalements anonymes malveillants. Les faits

[62] Voir par exemple Australia Treasury Laws Amendment (Enhancing Whistleblower Protections) Act 2019.
[63] Soit respectivement les dispositions prévues par les articles 9 et 10 de la directive. Il est à noter que ces sanctions sont déjà prévues par la directive si l'on interprète *lato sensu* le point a) du paragraphe 1er de l'article 23.
[64] Transparency International. *International Principles for Whistleblowing Legislation* (2013), Principles 13 and 18.
[65] Article 6, paragraphe 2 de la directive.
[66] United Nations Office on Drugs and Crime. *Resource Guide on Good Practice in the Protection of Reporting Persons* (2015), p.51.
[67] Groupe de travail «ARTICLE 29» sur la protection des données, *Avis 1/2006*, p.11.
[68] Article 6, paragraphe 6 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 II 2, paragraphe 2 de l'arrêté du Gouvernement flamand du 13 janvier 2006 fixant le statut du personnel des services des autorités flamandes.
[69] OECD. *Survey on Business Integrity and Corporate Governance* (2015).
[70] Groupe de travail «ARTICLE 29» sur la protection des données, *Avis 1/2006*, p.11. [90] Commission de la protection de la vie privée. *Recommandation n° 01 / 2006*, p. 6 [91] NAVEX Global, *Risk & Compliance Hotline Benchmark Report* (2020), p.26.

se sont en moyenne révélés (au moins partiellement) fondés et justifiés dans 50% des cas lorsqu'ils étaient rapportés ouvertement, contre 38% anonymement[91].

Un autre écueil potentiel concerne la difficulté d'enquêter et d'agir lorsque la source n'est pas identifiée, particulièrement dans l'évaluation de la crédibilité des informations ainsi que dans toute demande de clarification ou d'information supplémentaire. Les nouvelles technologies permettent néanmoins un suivi efficace des signalements anonymes dès lors que l'anonymat est perçu comme un outil de sécurisation des activités en ligne[71]. Tel est par exemple le cas en Allemagne, aux Pays-Bas, en Autriche et en Hongrie où des fonctionnalités avancées assurent un dialogue anonyme tout au long de l'enquête[72].

En pratique, le recours à l'anonymat s'avère cependant efficace. Pour une détection et une prévention efficaces, « il est essentiel que les informations pertinentes parviennent rapidement à ceux qui sont les plus proches de la source du problème, les plus aptes à enquêter et qui disposent des pouvoirs nécessaires pour y remédier, si possible. Les auteurs de signalement devraient, dès lors, être encouragés à utiliser en premier lieu les canaux de signalement interne et à effectuer un signalement auprès de leur employeur »[73]. Or, l'anonymisation est pour beaucoup une condition préalable à l'alerte. De fait, les études empiriques montrent que le nombre de signalements est environ 2,5 fois plus important lorsque les signalements anonymes sont acceptés[74].

S'il est recommandé de permettre les signalements anonymes et leur suivi, TI Belgium s'accorde sur le fait qu'ils doivent être traités avec une « précaution particulière »[75]. Celle-ci emporte plusieurs gardefous renforcés par les recommandations précédentes :

1. L'exigence de « motifs raisonnables » exclut de fait les signalements fondés sur de simples rumeurs et impose de décrire avec suffisamment de précision les faits signalés[97]. En outre, le signalement ne peut porter sur des griefs strictement personnels sans aucun rapport avec le champ d'application matériel du dispositif d'alerte (► **recommandation 3**). Ensuite, la directive ne prévoit pas d'obligation de signalement : « le recours au dispositif d'alerte doit toujours être facultatif »[76]. Enfin, les personnes qui ont constaté des actes répréhensibles ou des risques sur leur lieu de travail et souhaitant faire état de leurs préoccupations ne veulent pas ou n'ont pas toutes besoin de recourir à l'anonymat[99].

2. Les signalements anonymes seront d'abord filtrés par le premier destinataire qui « se penche sur son admissibilité » et examine « s'il convient d'enquêter », avant de considérer « l'opportunité de sa diffusion »[77] (► **recommandation 4**). Sur ce point, les autorités compétentes sont soumises au devoir de confidentialité et à des obligations très strictes en matière de traitement des données à caractère personnel de tous les protagonistes[78]. En

---

[71] Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, David Kaye sur l'usage du chiffrement et de l'anonymat dans l'exercice des droits à la liberté d'opinion et d'expression à l'ère numérique, A/HRC/29/32, 22 mai 2015, présenté au Conseil des droits de l'homme le 17 juin 2015.

[72] Voir par exemple www.nlconfidential.org; https://www.bkms-system.net/bkwebanon/report/clientInfo?cin=1at21&c=1&language=ger; Act CLXV of 2013 on Complaints and Public Interest Disclosures, Article 6.

[73] Considérant 47 de la directive.

[74] Autrement dit, entre 50 et 60% des signalements internes sont anonymes lorsqu'ils sont autorisés. Expolink. *Whistleblowing Benchmarking Report* (2019), p.9; NAVEX Global, *Risk & Compliance Hotline Benchmark Report* (2020), p.22; WhistleB. *Annual customer survey on organisational whistleblowing* (2020), p.7.

[75] Commission de la protection de la vie privée. *Recommandation n° 01 / 2006*, p. 6

[97] Considérants 32, 43 et 57 de la directive.

[76] Lachapelle. *Le lancement d'alerte (whistleblowing) à l'ère du règlement général sur la protection des données* (2018), p.11.

[99] United Nations Office on Drugs and Crime. *Resource Guide on Good Practice in the Protection of Reporting Persons* (2015), p.51.

[77] Groupe de travail «ARTICLE 29» sur la protection des données, *Avis 1/2006*, p.12.

[78] Ibidem.

particulier, « les droits de la personne concernée devraient être protégés afin d'éviter des atteintes à la réputation ou d'autres conséquences négatives »[79].

3. Les organisations ne doivent pas activement encourager les employés à faire part de leurs préoccupations de manière anonyme[80]. Le système d'alerte doit plutôt s'accompagner d'un réel engagement en faveur d'une culture organisationnelle ouverte qui favorise la transparence et le dialogue[104] (► **recommandation 5**). Il convient de rappeler aux utilisateurs qu'ils ne subiront aucun préjudice en raison de leur action et que leur identité demeure strictement confidentielle à tous les stades du processus. Le service en charge du traitement des signalements doit également veiller à ce qu'ils comprennent les limites du système[81] afin d'accroître leur confiance et de réduire les signalements anonymes.

En France, depuis l'entrée en vigueur le 1er juin 2017 de la loi dite « Sapin 2 » imposant notamment aux grandes entreprises l'obligation d'adopter un dispositif d'alerte interne, environ la moitié des entreprises du CAC40 ont décidé d'accepter l'anonymité sous ces conditions[82]. Ceux-ci doivent donc une nouvelle fois être considérés comme un outil complémentaire aux mécanismes de contrôle interne existants, en particulier dans la lutte contre la corruption[83]. Accepter l'anonymat sert au mieux les intérêts des organisations pour prévenir, détecter et répondre au plus grand nombre possible d'incidents en interne et à un stade précoce[84], en évitant que les informations potentiellement dommageables entrent dans le domaine public par le biais d'une divulgation publique. Finalement accepter l'anonymat a comme conséquence logique que les lanceurs d'alerte qui effectuent un signalement anonyme, bénéficient du régime de protection, instauré par la nouvelle loi.

7 MARCHÉS PUBLICS DE DÉFENSE OU DE SÉCURITÉ

Recommandation : la transposition doit inclure les violations des règles relatives aux marchés publics comportant des aspects relatifs à la défense ou à la sécurité, en prévoyant un régime spécial conforme aux Principes Globaux sur la Sécurité Nationale et le Droit à l'Information (Principes de Tshwane)[108].

La directive exclut les violations des règles relatives aux marchés publics afférentes à la défense et à la sécurité, rappelant la souveraineté des États membres à assurer leur sécurité nationale[85]. Elle entrevoit la possibilité d'une extension du champ d'application à ce domaine[86] en mettant en place des « dispositions spécifiques visant à protéger les intérêts essentiels de sécurité nationale »[111].

---

[79] Considérant 100 de la directive.
[80] Groupe de travail «ARTICLE 29» sur la protection des données, *Avis 1/2006*, p.12.
[104] OECD. *Committing to Effective Whistleblower Protection* (2016), p.12.
[81] L'anonymat ne fait pas toujours obstacle à ce que d'autres puissent deviner l'identité de l'auteur du signalement et il peut être nécessaire de divulguer leur identité dans le cadre d'une procédure judiciaire. Banisar. *Whistleblowing: International Standards and Developments* (2011).
[82] Sur base des informations disponibles sur leur site internet, au moins 17 entreprises autorisent l'anonymat (Bouygues, Capgemini, Carrefour, Danone, Dassault Systèmes, Engie, Essilor, Groupe PSA, Legrand, Michelin, Publicis Groupe, Safran, Sanofi, Schneider Electric, Société Générale, Veolia et Vivendi).
[83] Article 13, paragraphe 2 de la Convention des Nations Unies contre la corruption.
[84] Conformément aux standards internationaux. Voir Transparency International. *International Principles for Whistleblowing Legislation* (2013), Principle 19. Voir Conseil de l'Europe. *Recommandation CM/Rec (2014)7*, Principe 5, p.29; G20 AntiCorruption Action Plan. *Protection of Whistleblowers*, p.33; United Nations Office on Drugs and Crime. *Resource Guide on Good Practice in the Protection of Reporting Persons* (2015), p.28.
[85] Article 3, paragraphe 2 de la directive, conformément à l'article article 346 du traité sur le fonctionnement de l'Union européenne.
[86] Article 2, paragraphe 2, de la directive.
[111] Considérant 24 de la directive.

En Belgique, le législateur a explicitement interdit au niveau flamand de communiquer des « faits portant sur la sécurité du pays et la protection de l'ordre public »[87]. Ce n'est pas le cas au niveau fédéral. Cette exclusion est probablement due à l'importance des enjeux liés à la sécurité nationale et à leur caractère sensible.

Les marchés publics sont une composante majeure de l'économie et supposent une interaction étroite entre le secteur public et privé, ce qui les rend particulièrement exposés à la corruption, aux risques de fraude et d'utilisation abusive des fonds publics[88]. S'il est difficile de le quantifier avec exactitude, le risque de corruption dans ce domaine, est à lui seul évalué à 43 millions d'euros par an pour la Belgique[89]. En outre, il est estimé que la corruption augmente le coût des marchés publics de 4 à 15 %[90]. Les lanceurs d'alerte jouent ainsi un rôle prépondérant dans la révélation et la prévention de fraudes dans la passation de marchés publics. Les avantages potentiels d'un régime de protection efficace se situent annuellement aux alentours de 130 millions d'euros pour l'État belge[91].

Les marchés publics relatifs à la défense et à la sécurité ne font pas exception. Le secteur apparaît comme l'un des plus vulnérables[92], étant donné le montant des dépenses publiques (elles s'élevaient à 828,7 millions d'euros pour les marchés publics liés à la défense en 2014[93]) et le passif de notre pays en la matière (cf. affaire Agusta-Dassault).

TI Belgium déplore que les sanctions dans le secteur de la défense soient trop faibles – voire inexistantes – pour constituer un moyen de dissuasion efficace contre les pratiques de corruption. Un rapport de TI datant de 2016[94] indique que la Belgique n'avait condamné aucune entreprise pour corruption depuis 2004 alors que près de 100 enquêtes sur l'Armée belge ont été ouvertes pour des infractions relatives aux marchés publics commises entre 1996 et 2005[95]. Pour ces raisons, TI Belgium demande que le champ d'application matériel n'exclue pas les violations des règles relatives aux marchés publics de défense et de sécurité. Etant donné le caractère sensible des informations, des dispositions spécifiques et des précautions supplémentaires sont nécessaires à leur traitement. Ainsi, les Principes de Tshwane pourraient constituer la base de ce régime spécial[121]. Le Parlement Européen a appelé les États membres à prévoir « dans le domaine de la sécurité nationale, […] une alternative sûre au silence pour divulguer ou signaler les actes répréhensibles, y compris la corruption, les infractions pénales, les violations d'obligations juridiques, les erreurs judiciaires et les abus d'autorité » notamment conformes à ces principes[9697].

---

[87] Article II 2, paragraphe 2 de l'arrêté du Gouvernement flamand du 13 janvier 2006 fixant le statut du personnel des services des autorités flamandes.
[88] Considérant 6 de la directive.
[89] European Parliament. *The Cost of Non-Europe in the area of Organised Crime and Corruption – Annex II* (2016), p.59.
[90] Mendes and Fazekas. *Towards More Transparent and Efficient Contracting - Public Procurement in the EU* (2017).
[91] European Commission. *Estimating the Economic Benefits of Whistleblower Protection in Public Procurement* (2017), p.15.
[92] European Commission. *COM(2014) 38 final EU anti-corruption report*.
[93] European Commission, *SWD(2016) 407 final Evaluation of Directive 2009/81/EC on public procurement in the fields of defence and security*, p.10.
[94] Transparency International. *Evaluation of the functioning and impact of the EU Defence and Security Public Procurement Directive (2009/81/EC) across 20 EU states* (2016), p.17.
[95] Si 31 membres du personnel et entrepreneurs ont été inculpés, 15 ont finalement été condamnés. Les sanctions comprenaient des confiscations et des peines de prison, qui ont toutes été suspendues. Les entreprises ont manifestement pu échapper aux condamnations pour corruption en trouvant un accord avec le procureur du Roi. Dans certains cas, ces accords ont permis au contractant d'éviter toute reconnaissance de culpabilité. Dans d'autres, les entreprises ont pu plaider coupable de crimes moins graves. Globalement, les amendes infligées dans ces accords ou ces condamnations moins sévères sont insuffisantes pour éliminer l'avantage économique des activités exercées. Il est peu probable que cette situation soit conforme aux sanctions « pénales efficaces, proportionnées et dissuasives » prévues à l'article 3 de la Convention de l'OCDE contre la corruption. [121] Ces principes The Global Principles on National Security and the Right to Information.
[96] Résolution du Parlement européen du 12 mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures (2013/2188(INI)).
[97] Conformément aux standards internationaux. Voir Transparency International. *International Principles for Whistleblowing*

8 ENTITÉS JURIDIQUES PUBLIQUES

Recommandation : la transposition doit appliquer l'obligation d'établir des canaux de signalement interne à l'ensemble des entités juridiques du secteur public, sans exception[123].

La directive impose d'établir des canaux de signalement interne aux entités juridiques du secteur privé de 50 travailleurs ou plus[98] et à toutes les entités juridiques du secteur public avec une possibilité pour les États membres d'exempter les « municipalités comptant moins de 10 000 habitants ou moins de 50 travailleurs » ou d'autres entités juridiques du secteur public comptant moins de 50 travailleurs[99].

Opter pour cette possibilité reviendrait à exempter la majorité des administrations locales et des pouvoirs locaux[100] en Belgique. Une telle exemption est particulièrement préoccupante quand on sait que les collectivités territoriales prennent quotidiennement des décisions d'intérêt local et à la lumière des nombreux scandales de gouvernance publique au sein des intercommunales (cf. affaire Nethys). En outre, la plupart assure des missions comportant des risques pour la santé publique et la protection de l'environnement, domaines identifiés par la directive comme nécessitant une vigilance accrue[127]. Enfin, et plus fondamentalement, la corruption au sein de la fonction publique s'élèverait à 4 milliards d'euros par an[101]. L'impact des projets de travaux publics de moindre importance pour lesquels des fonctionnaires hiérarchiquement inférieurs sont compétents, n'est pas à sous-estimer.

Par conséquent, TI Belgium ne voit donc pas de raison d'exempter certains pouvoirs locaux de cette obligation[102], dans la mesure où la directive permet de partager ou d'exploiter conjointement les canaux de signalement interne[130].

9 PERSONNES EXPOSÉES AU RISQUE DE REPRÉSAILLES

Recommandation : la transposition doit étendre le régime de protection aux personnes physiques qui, dans un contexte professionnel, ont l'intention d'effectuer un signalement ou que l'on croit ou soupçonne en être l'auteur.

Legislation (2013), Principle 19. Voir Conseil de l'Europe. *Recommandation CM/Rec (2014)7*, Principe 5, p.29; G20 AntiCorruption Action Plan. *Protection of Whistleblowers*, p.33; United Nations Office on Drugs and Crime. *Resource Guide on Good Practice in the Protection of Reporting Persons* (2015), p.28.

[98] En vertu du paragraphe 3 de l'article 8, ce seuil n'est pas applicable à certains secteurs prévus par la directive.

[99] Article 8 de la directive.

[100] On pense par exemple aux administrations communales, provinciales ainsi qu'aux intercommunales.

[127] Considérants 10 et 13.

[101] Selon une enquête internationale rapportée en 2016 par De Morgen et Het Laatste Nieuws. Un montant confirmé par Paul Meulemans, commissaire à l'Office central pour la Répression de la corruption (OCRC) jusque fin 2015.

[102] D'autres États membres comme l'Italie, l'Irlande et la Slovaquie imposent à toutes les entités publiques, sans exception, de mettre à disposition des dispositifs de signalement interne. [130] Article 8, paragraphe 9, alinéa 3.

Le régime de protection ne devrait pas uniquement se limiter aux auteurs d'alerte ayant procédé conformément à la directive, mais doit s'étendre à l'ensemble des personnes physiques impliquées dans le processus de signalement susceptibles d'être exposées à un risque de représailles. La directive couvre un champ d'application personnel très large mais omet certaines catégories[103], notamment les personnes, qui ont l'intention d'effectuer un signalement ou, que l'on croit ou que l'on soupçonne, même à tort, d'être un lanceur d'alerte[104]. TI Belgium recommande que ces personnes puissent bénéficier du régime de protection en cas de traitement injuste.

En effet, il est assez fréquent que les employés signalent en premier lieu des dysfonctionnements à leur supérieur hiérarchique ou à leurs collègues, plutôt que de recourir aux canaux de signalement prévus. Ceci peut s'expliquer par le fait que ces personnes ne disposent que d'informations partielles et/ou ne se rendent pas compte qu'elles signalent une violation relevant du champ d'application de la législation. Ce cas de figure peut également se présenter lorsque le personnel n'est pas (bien) informé de l'existence des canaux de signalement interne et de la façon de les utiliser. En outre, lorsqu'une personne envisage de faire ou de préparer un signalement, il n'est pas rare qu'elle demande conseil à ses collègues ou à ses supérieurs, qu'elle pose des questions qui révèlent sa connaissance d'un acte potentiellement répréhensible, ou même qu'elle fasse part de son intention d'effectuer un signalement[133].

Finalement, il est recommandé de ne pas étendre le régime de protection aux personnes autre que la personne physique telle que définie à l'article 5 (8) de la directive.

10 RÉGIME DE PROTECTION

Recommandation : la transposition ne doit en aucun cas réduire le niveau de protection offert par la directive et doit maintenir ou renforcer les dispositions relatives aux conditions de protection, à l'accessibilité des voies de signalement, au traitement des données à caractère personnel, aux mesures de soutien et à l'aménagement de la charge de la preuve dans l'esprit de ses considérants.

La formulation de certaines dispositions pourrait être sujette à interprétation et engendrer une compréhension superficielle et/ou erronée qui nuirait au bon fonctionnement de la loi. La transposition doit « adopter ou maintenir des dispositions plus favorables aux auteurs de signalement que celles prévues par la directive » et ne doit, en aucun cas réduire le niveau de protection offert par celle-ci[134]. Les éléments suivants devraient être mis en œuvre conformément aux considérants de la directive :

- La transposition ne devrait pas imposer d'autres conditions que celles énumérées dans la directive[105] pour bénéficier du régime de protection. En particulier, la notion de « motifs raisonnables de croire » s'applique aux « informations signalées et non aux motifs amenant les auteurs de signalement à effectuer un signalement, qui devraient être sans importance »[106]. Ainsi, l'examen du caractère raisonnable doit se fonder sur un critère objectif (et non subjectif) : celui du point de vue d'une personne raisonnable placée dans les mêmes circonstances[107]. Par ailleurs, le Code pénal[108] encadre spécifiquement les déclarations

[103] Article 4 de la directive.
[104] Transparency International. *International Principles for Whistleblowing Legislation* (2013), Principle 4. [133] Transparency International. *Building on the EU directive for whistleblower protection* (2019), p.6.
[134] Article 25 de la directive.
[105] Article 6 de la directive.
[106] Considérant 32 de la directive. Voir aussi Transparency International. *International Principles for Whistleblowing Legislation* (2013), Principle 5.
[107] European Federation of Journalists. *Implementing the new EU Whistleblower Directive: A Transposition Guide for Journalists* (2020), p.13.
[108] Chapitre V, articles 443 à 453-bis.

sciemment fausses et prévoit des « sanctions effectives, proportionnées et dissuasives » conformes à celles requises par la directive[109]. Aussi, il n'est pas nécessaire que la transposition introduise d'autres sanctions.

- La transposition doit veiller à garantir l'accessibilité de différentes voies de signalement (interne, externe et divulgation publique sous certaines conditions) sans restriction supplémentaire pour les lanceurs d'alerte dans le choix du « canal de signalement le plus approprié en fonction des circonstances particulières de l'affaire »[140]. Une procédure non-échelonnée doit donc être maintenue, contrairement aux procédures existantes réglementées par la loi belge qui prévoient une approche par paliers[110]. Il convient en outre d'éviter de reprendre le régime d'alerte fédéral qui se préoccupe davantage de la procédure que du signalement. Cette approche trop complexe et trop restrictive expose inutilement le lanceur d'alerte à des erreurs de procédure et lui impose une charge procédurale importante[111]. Adopter une réglementation excessive serait contre-productif et entraverait sérieusement la mise en œuvre et l'application efficaces de la loi.

- La transposition doit exiger, dans la mesure du possible, le consentement explicite de l'auteur de signalement lors de la transmission de son signalement, il ne suffit pas de l'en informer[112]. Dans ce cas, le premier destinataire doit attendre le consentement explicite avant de transmettre le signalement ou simplement rediriger le donneur d'alerte vers l'autorité compétente, en lui laissant le choix de transmettre son signalement par cette voie. Lorsque la nature de la préoccupation soulevée exige qu'elle soit transmise sans délai à l'autorité compétente, le destinataire doit enregistrer une note officielle des raisons de la transmission et informer le lanceur d'alerte de cette décision[113].

- La transposition doit adopter les mesures de soutien prévues par la directive[114] sous la forme d'une assistance juridique et financière pour les auteurs de signalements dans le cadre des procédures judiciaires[115]. « Les frais juridiques peuvent représenter un coût important pour les auteurs de signalement contestant les mesures de représailles prises à leur encontre dans le cadre d'une procédure judiciaire […]. L'assistance dans les procédures pénales […] et, plus généralement, l'octroi d'une aide […] pourraient être déterminants, dans certains cas, pour la mise en œuvre effective de leur droit à la protection. »[116]

- La transposition doit maintenir l'aménagement de la charge de la preuve prévu par la directive[117]. Le renversement de la charge de la preuve implique qu'il « devrait incomber à la personne qui engage [une action à l'encontre de l'auteur d'un signalement] de prouver [que celui-ci] ne satisfait pas aux conditions fixées dans la directive »[118]. De même, « la personne qui a pris la mesure préjudiciable […] devrait […] être tenue de démontrer que la mesure prise n'était en rien liée au signalement ou à la divulgation publique »[119].

---

[109] Article 23, paragraphe 1er de la directive.
[140] Considérant 33 de la directive.
[110] 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 ; Arrêté du Gouvernement flamand du 13 janvier 2006 fixant le statut du personnel des services des autorités flamandes.
[111] Transparency International Belgium. *Providing an alternative to silence: Towards greater protection and support for whistleblowers in Belgium* (2013), p.15.
[112] Article 11, paragraphe 6 de la directive.
[113] Conseil de l'Europe. *Recommandation CM/Rec (2014)7*, Principe 18, p.39-40.
[114] Article 20, paragraphe 2 de la directive.
[115] Transparency International. *International Principles for Whistleblowing Legislation* (2013), Principle 20.
[116] Considérant 99 de la directive.
[117] Article 21, paragraphe 5 de la directive.
[118] Considérant 97 de la directive.
[119] Considérant 93 de la directive.