TITRE 18
Le lancement d'alerte (*whistleblowing*) à l'ère du règlement général sur la protection des données

Amélie LACHAPELLE[1]

Introduction

1. C'est à l'occasion de l'implémentation du « *Sarbanes-Oxley Act* » (ci-après : « *SOX Act* ») que le *whistleblowing* s'est invité, pour la première fois, au sein de l'ordre juridique européen. Adopté en réaction à la faillite de grosses multinationales, ce texte américain oblige les sociétés cotées sur un marché financier américain, qu'elles soient américaines ou non, à mettre en place un dispositif de signalement interne des irrégularités comptables et financières et à protéger les personnes qui effectuent de tels signalements.

2. Depuis lors, le mouvement d'expansion du *whistleblowing* a poursuivi sa route. L'Union européenne a ainsi décidé, à la suite de la crise financière de 2008, de recourir au *whistleblowing* en vue de renforcer le respect des législations financières[2]. Elle a, de plus, étendu ce mécanisme à la sécurité de certains transports. Plus récemment, elle a érigé le *whistleblowing* au rang d'instrument de lutte contre le blanchiment, d'une part, et contre les abus de marché, d'autre part.

---

[1] Doctorante Aspirante F.R.S.-FNRS à l'Université de Namur, co-directrice de l'unité Libertés, Information et Société du CRIDS (Centre de Recherche Information, Droit et Société – UNamur) et Membre associée du CRECO (Centre de Recherche sur l'État et la Constitution – UCL). L'auteure remercie Cécile de Terwangne, professeure à la Faculté de droit de l'UNamur, pour sa relecture attentive du présent texte et ses remarques avisées.

[2] Communication du 8 décembre 2010, « Reinforcing sanctioning regimes in the financial services sector » (COM(2010) 716 final), p. 15.

Du côté de l'opinion publique, c'est davantage l'affaire *Snowden* qui a permis à la figure du lanceur d'alerte de faire son apparition. Vigie citoyenne pour les uns, traître pour les autres[3], cet ancien employé de la CIA et de la NSA a confié à des journalistes des documents confidentiels qui attestent de pratiques de surveillance massive de la part des gouvernements américain et britannique. En particulier, le programme PRISM aurait permis au FBI et à la NSA de surveiller les internautes de la planète entière grâce à la collaboration des Géants de l'Internet tels que Google, Microsoft, Yahoo, Facebook, Skype et Apple[4].

De telles pratiques constituent une violation manifeste des droits de l'homme, en particulier du droit à la vie privée, du droit à la protection des données et de la liberté d'expression[5]. Ce faisant, l'affaire *Snowden* a eu l'effet d'un électrochoc quant à la révision du cadre européen de protection des données, ce qui a été foncièrement pris en compte par la Commission européenne qui étend, dans sa proposition de directive tout récemment dévoilée, la protection des lanceurs d'alerte au domaine de la vie privée et de la protection des données[6].

3. Comme le confirme largement cette proposition de directive, la protection des données à caractère personnel occupe une place cardinale dans le système européen de protection des lanceurs d'alerte[7]. Il n'empêche que

---

[3] Les États-Unis ont lancé un mandat d'arrêt à l'encontre d'Edward Snowden, du chef d'espionnage au sens de l'« *Espionage Act* » de 1917.

[4] G. GREENWALD et E. MACASKILL, « NSA Prism program taps in to user data of Apple, Google and others », *The Gardian.com*, 7 juin 2013 (consulté le 1er mars 2018) ; S. ACKERMAN, « US tech giants knew of NSA data collection, agency's top lawyer insists », *The Guardian.com*, 19 mars 2014 (consulté le 28 février 2018).

[5] Sur cette affaire et les questions suscitées eu égard à la liberté d'expression, voy. not. F. DUBUISSON, « Société de l'information, médias et liberté d'expression », *J.E.D.H.*, n° 2014/3, pp. 359-363.

[6] Proposition de directive du 23 avril 2018 relative à la protection des personnes signalant des violations du droit de l'Union (COM(2018) 218 final) (ci-après : « Proposition de directive du 23 avril 2018 »), art. 1.1.a), (x) et considérant n° 14. Voy. aussi l'annexe de la proposition de directive, p. 8 ainsi que l'*Impact Assessment* accompagnant la proposition de directive (SWD(2018) 116 final), pp. 26-27.

[7] Proposition de directive du 23 avril 2018, considérants nos 43, 44, 48, 53, 55, 58, 79 et 85 et art. 18. Voy., aussi, art. 32. 2 c) du règlement (UE) 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les 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, *J.O.U.E.*, L 173/1 à L 173/61 du 12 juin 2014 ; considérant n° 3 de la directive d'exécution 2015/2392/UE de la Commission du 17 décembre 2015 relative au règlement (UE) 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.*, L 332/126 à L 332/132 du 18 décembre 2015 ; considérants nos 41 et 43 de la directive 2015/849/UE du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du

la compatibilité d'un tel dispositif, qu'il soit mis en place par une entreprise, une administration ou une autorité, avec la protection européenne des données représente une question éminemment complexe, à laquelle nous ne pouvons répondre de façon exhaustive et définitive à l'occasion du présent chapitre. Tant le *whistleblowing* que le RGPD doivent encore être éprouvés en pratique. En outre, le *whistleblowing*, de par l'étendue de son périmètre, dépasse le champ d'application du RGPD.

4. Après avoir clarifié la notion de *whistleblowing* eu égard aux implications de la protection des données (première partie), nous proposons de faire la synthèse des enseignements tirés des orientations fournies par les autorités de protection des données, lus et (ré)interprétés à la lumière du RGPD, d'une part, et de la littérature relative au *whistleblowing*, d'autre part, en ce compris la récente proposition de directive européenne (deuxième partie).

CHAPITRE 1. La notion juridique de « lancement d'alerte » à l'épreuve du RGPD

5. Nous proposons de revenir brièvement, dans un premier point, sur la conception européenne du « lancement d'alerte » et de confronter, dans un second point, cette conception au champ d'application du RGPD.

SECTION 1. – La notion juridique de « lancement d'alerte » ….

6. Quoique les définitions en la matière foisonnent, il n'existe actuellement pas de définition univoque du lancement d'alerte[8]. Le lancement d'alerte à l'européenne se présente, en réalité, comme la convergence de deux notions à l'origine distinctes, le *whistleblowing* et l'alerte éthique.

---

système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission, *J.O.U.E.*, L 141/73 à L 141/117 du 5 juin 2015 (Quatrième Directive anti-blanchiment).

[8] Voy. not. l'*Impact Assessment* accompagnant la proposition de directive du 23 avril 2018, préc., p. 6.

7. D'origine américaine, le *whistleblowing* se définit traditionnellement[9] comme « *the disclosure by organization members (former or current) of illegal, immoral or illegitimate practices under the control of their employers, to persons or organizations that may be able to effect action* »[10].

Par exemple, la Section 301 du *SOX Act* exige des comités d'audit des entreprises publiques américaines et de leurs filiales dans l'Union européenne, ainsi que des sociétés non américaines cotées à une bourse américaine d'établir une procédure permettant aux employés de l'émetteur des titres de soumettre de façon anonyme leurs inquiétudes au sujet de problèmes dans le domaine de la comptabilité et de l'audit[11].

8. L'alerte éthique, de son côté, est une notion d'origine française[12]. Dans ce cadre, celui qui lance l'alerte peut se définir comme « 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 »[13].

9. Au croisement de ces deux notions a progressivement émergé le lancement d'alerte à l'européenne. À la lumière de la Recommandation (2014)7

---

[9] La définition des professeurs Miceli & Near semble être la plus largement acceptée et utilisée outre-Atlantique. En ce sens, voy. not. T.M. Dworkin, « Foreword », in *International Handbook on Whistleblowing Research* (D. Lewis, A.J. Brown *e.a.*, éd.), Cheltenham, Elgar, 2014, p. xx.

[10] « Mécanisme par lequel un employé, ancien ou actuel, révèle des actes répréhensibles commis sous le contrôle de son employeur à quelqu'un qui est capable de faire de quelque chose pour y remédier » (nous traduisons) : J.P. Near et M.P. Miceli, « Organizational dissidence : The case of whistle-blowing », *Journal of Business Ethics, February*, 4 (1), 1985, p. 4, disponible sur www.researchgate.net (consulté le 7 juin 2017).

[11] Parallèlement, la Section 806 du *SOX Act* insère un régime de protection selon lequel les employés, contractants, sous-contractants et agents des sociétés cotées ne peuvent faire l'objet de représailles de la part de leur employeur pour avoir révélé auprès d'un supérieur, ou d'une autre autorité compétente telle qu'énumérée légalement, toute conduite dont on peut croire qu'elle constitue une violation des règles de la Securities and Exchange Commission ou de toute loi fédérale ayant pour objet les fraudes perpétrées à l'encontre des actionnaires.

[12] Voy. not. L. Romanet et L. Benaiche, *Les lanceurs d'alerte, auxiliaires de justice ou gardiens du silence ? L'alerte éthique en droit français*, Paris, Editions de Santé, 2014 ; Conseil d'État français, « Le droit d'alerte : signaler, traiter, protéger », étude adoptée le 25 février 2016 par l'assemblée générale plénière du Conseil d'État, Paris, La Documentation française, 2016.

[13] F. Chateauraynaud, « Lanceur d'alerte », *in Dictionnaire critique et interdisciplinaire de la participation* (I. Casillo avec R. Barbier, L. Blondiaux, F. Chateauraynaud, e.a., dir.), Paris, GIS Démocratie et Participation, 2013, disponible sur www.dicopart.fr (consulté le 17 mai 2017). Voy. aussi l'étude précitée du Conseil d'État français, Annexe 6 – Contribution du professeur Henri Oberdorff sur la notion d'alerte éthique, p. 111.

du Comité des ministres du Conseil de l'Europe[14] et de la toute récente proposition de directive de la Commission européenne[15], le lancement d'alerte à l'européenne peut se définir comme le signalement ou la révélation d'informations concernant des menaces ou un préjudice pour l'intérêt général dans le contexte de la relation de travail. Plus concrètement, la Commission européenne renvoie aux violations actuelles ou potentielles du droit de l'Union dans certains domaines de politiques spécifiques[16].

Au sein du lancement d'alerte, on distingue communément trois types de signalement : le signalement interne, le signalement externe et la révélation publique[17]. Le signalement interne a lieu au sein d'une organisation ou d'une entreprise ; le signalement externe intervient auprès d'organes réglementaires publics, d'autorités de répression ou d'organes de contrôle ; la révélation publique d'informations peut se faire, quant à elle, auprès d'un journaliste, d'une organisation non gouvernementale, d'un parlementaire ou directement via une page web ou une plateforme en ligne[18].

---

[14] Recommandation CM/Rec (2014)7 sur la protection des lanceurs d'alerte, adoptée par le Comité des Ministres du Conseil de l'Europe le 30 avril 2014, Annexe, Section IV, Principe 14.

[15] Proposition de directive du 23 avril 2018, art. 1 et 2.

[16] Proposition de directive du 23 avril 2018, art. 3 (1). Voy. aussi l'annexe (Part I et II) qui accompagne la proposition de directive.

[17] Voy., entre autres, chapitres II et III de la proposition de directive du 23 avril 2018 ; Recommandation CM/Rec (2014)7, Annexe, Section IV, Principe 14 ; Résolution du Parlement européen du 24 octobre 2017 sur les mesures légitimes visant à protéger les lanceurs d'alerte qui divulguent, au nom de l'intérêt public, des informations confidentielles d'entreprises et d'organismes publics (2016/2224(INI)), consid. F ; Groupe des Verts/ALE du Parlement européen, Draft directive « Whistleblower protection in the public and private sector in the European Union », 23 April 2016, art. 6-8 ; Office des Nations Unies contre la drogue et le crime (UNODC), *Resource Guide on Good Practices in the Protection of Reporting Persons*, New York, United Nations, 2015, pp. 29-45 ; Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, David Kaye, sur la protection des sources d'information et des lanceurs d'alerte, A/70/361, 8 septembre 2015, pp. 18-19 ; OECD, *Committing to Effective Whistleblower Protection*, Paris, OECD Publishing, 2016, p. 53. Voy. aussi la jurisprudence de la Cour européenne des droits de l'homme (spéc. Cour eur. D.H. (GC), arrêt *Guja c. Moldavie*, 12 février 2008, req. n° 14277/04 ; Cour eur. D.H., 5e sect., arrêt *Heinisch c. Allemagne*, 21 juillet 2011, req. n° 28274/08 ; Cour eur. D.H, 3e sect., arrêt *Bucur et Toma c. Roumanie*, 8 janvier 2013, req. n° 40238/02). Du côté de la doctrine, voy. not. T. Devine et T. F. Maassarani, *The Corporate Whistleblower's Survival Guide : a handbook for committing the truth*, publié avec l'association Government Accountability Project, San Fransisco, Berrett-Koehler Publishers, chapter 4 ; R. Moberly, « 12.'To persons or organizations that may be able to effect action' : Whistleblowing recipients », in *International Handbook on Whistleblowing Research* (D. Lewis, A.J. Brown e.a., éd.), Cheltenham, Elgar, 2014, pp. 273-297.

[18] Recommandation CM/Rec (2014)7, Annexe, Section IV, Principe 14. Voy. aussi la proposition de directive du 23 avril 2018, art. 3 (6), (7) et (8) et considérant n° 32.

SECTION 2. – … à l'épreuve du RGPD

10. Si les trois types de signalement exposés composent le *whisteblowing* tel qu'entendu actuellement au niveau européen et international, il convient d'attirer l'attention sur le fait que la définition proposée par la Commission belge de la Protection de la Vie Privée (ci-après : CPVP)[19], le Groupe 29, la Commission française de l'Informatique et des Libertés (ci-après : CNIL) et le Contrôleur Européen de Protection des Données (ci-après : CEPD), et l'examen réalisé par ces autorités, ne recouvrent que le signalement interne[20].

C'est donc à juste titre que les autorités de protection des données saisies de la compatibilité du dispositif de *whistleblowing* établi par le *SOX Act* avec la protection des données ont choisi, dans la version française de leur texte, de ne pas se référer à la notion trop large de « lancement d'alerte », pour traduire l'expression « *whistleblowing* ».

11. Il n'empêche que le signalement externe et le signalement public peuvent également tomber sous le coup du RGPD, ce que confirme la Proposition de directive du 23 avril 2018[21].

Tel est par exemple le cas des mécanismes de signalement que les autorités compétentes[22] doivent mettre en place en exécution de l'article 61.1 de la Quatrième directive anti-blanchiment. À côté de ces mécanismes de signalement externe, mentionnons que l'article 61.3 de la Quatrième directive anti-blanchiment exige également des « entités assujetties qu'elles disposent de procédures appropriées permettant à leur personnel ou aux personnes se trouvant dans une situation comparable de signaler en interne les infractions ».

En revanche, le signalement externe effectué auprès d'autorités compétentes à des fins de prévention et de détection des infractions pénales,

---

[19] Conformément au RGPD, l'« Autorité de protection des données » remplace, depuis le 3 décembre 2017, la Commission belge de Protection de la Vie Privée (Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018).

[20] Plus précisément, la CPVP entend par « systèmes d'alerte interne professionnelle » « des dispositions permettant à des individus de signaler un comportement d'un membre de leur organisation contraire, selon eux, à une législation ou à une réglementation ou aux règles primordiales établies par leur organisation » (CPVP, *Recommandation n° 01/2006 du 29 novembre 2006 relative à la compatibilité des systèmes d'alerte interne professionnelle avec la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*, p. 2 (ci-après : recommandation n° 01/2006)).

[21] Proposition de directive du 23 avril 2018, art. 18 et considérants n^{os} 55 et 58.

[22] Pour une illustration, voy. la procédure mise en place sur le site web de la FSMA (https://www.fsma.be/fr/faq/point-de-contact-lanceurs-dalerte (consulté le 20 mars 2018)) ainsi que sur celui de la BNB (https://www.nbb.be/fr/supervision-financiere/prevention-du-blanchiment-de-capitaux-et-du-financement-du-terrorisme-37 (consulté le 23 mars 2018)).

d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales devrait échapper au champ d'application du RGPD et tomber sous le coup de la directive « Police et Justice »[23] dans la mesure où de telles activités ne relèvent pas du champ d'application du droit communautaire.

Pour ce qui est du signalement public, celui-ci devrait, en principe, être soumis au régime spécifique de l'article 85 du RGPD dans la mesure où celui-ci ne représente que le seul exercice du droit à la liberté d'expression[24]. À cet égard, nous renvoyons aux réflexions de Quentin Van Enis livrées dans le présent ouvrage[25]. Ce dernier constate avec regret l'absence d'harmonisation européenne à propos des traitements de données nécessaires à des seules fins de journalisme. Un tel constat est problématique alors que les révélations de ces dernières années montrent que les médias rassemblent de plus en plus leurs moyens humains et techniques en vue d'enquêter sur des affaires de grande ampleur, et ce au-delà encore du cadre européen. L'affaire des *Panama Papers* n'aurait ainsi jamais pu voir le jour si les millions de fichiers confidentiels, transmis par l'énigmatique John Doe à un journal allemand, n'avaient pas pu être décortiqués et analysés par le Consortium International des Journalistes d'Investigation.

Enfin, mentionnons que la directive « *e-privacy* » est par ailleurs susceptible de s'appliquer aux trois types de signalement en ce qu'elle complète la directive « vie privée », que le RGPD a vocation à remplacer[26], dans le domaine des communications électroniques[27].

---

[23] Directive 2016/680/UE 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, *J.O.U.E.*, L 119/89 à L 119/131 du 4 mai 2016.

[24] Dans les faits, on se demande néanmoins si tel est le cas de tout signalement public. Qu'en est-il du signalement effectué auprès d'une organisation non gouvernementale, telle que *Transparency International*, ou auprès de parlementaires, comme l'y invite la plateforme « *EuLeaks* », lancée par le groupe Verts/ALE du Parlement européen ? Même si nous n'y répondons pas, la question méritait assurément d'être posée.

[25] Sur le sujet, voy, dans le présent ouvrage, le chapitre dédié à la conciliation entre le droit à la liberté d'expression et le droit à la protection des données à caractère personnel dans le RGPD.

[26] Signalons que la directive « *e-privacy* » sera prochainement remplacée par un règlement en vue d'assurer la cohérence de ses règles avec le RGPD (Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »), 10 janvier 2017, COM(2017) 10 final).

[27] Art. 1.1 de la directive « *e-privacy* ».

12. Compte tenu du cadre imparti à la présente contribution, nous nous limiterons cependant aux seules implications du RGPD sur le lancement d'alerte.

Les orientations fournies par les autorités de protection des données sous l'empire de la directive 95/46/CE[28] demeurent à cet égard toujours pertinentes[29]. En ce sens, la CPVP et le CEPD n'ont pas jugé utile, dans leurs opinions récentes, de consacrer de nouveaux principes. La CPVP a ainsi choisi de ne pas s'exprimer sur la conformité au RGPD du dispositif de *whistleblowing* imposé par la loi du 18 septembre 2017 estimant manifestement – la CPVP ne l'indique pas explicitement – que les orientations qu'elle avait fournies en 2006 suffisaient[30]. Or, la loi du 18 septembre 2017 transpose, en droit belge, la Quatrième directive anti-blanchiment, laquelle établit, ainsi que nous venons de le voir, un dispositif de signalement interne et un dispositif de signalement externe. Dans son opinion du 29 novembre 2017, le CEPD renvoie, quant à lui, explicitement aux lignes directrices qu'il a rédigées en 2016, ne se prononçant que sur les adaptations requises par le dispositif d'espèce, le dispositif de *whistleblowing* mis en place par l'*European Investment Bank*[31].

À la lumière de ces considérations, il en découle que lesdites orientations devraient également pouvoir s'appliquer au signalement externe et au signalement public lorsque ces derniers relèvent du champ d'application du RGPD.

---

[28] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[29] Quoique le Groupe 29 ait limité son avis au domaine financier, nous sommes d'avis que les orientations proposées dans son opinion n° 1/2006 sont aujourd'hui devenues générales dans la mesure où il avait indiqué à l'époque se pencher rapidement sur les mécanismes internes de dénonciation dans les autres domaines, ce qu'il n'a jamais fait.

[30] CPVP, *Avis n° 24/2017 du 24 mai 2017 concernant l'avant-projet de loi relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces (CO-A-2017-019)*, p. 4, pt 6.

[31] CEPD, *Prior-check Opinion on the Whistleblowing Policy of the European Investment Bank (Case 2016-0381)*, 29 November 2017, p. 1). Voy. aussi son opinion du 29 mars 2017 (CEPD, *Prior-check Opinion on EUIPO Whistleblowing Procedure - Case 2016-1056*, 29 March 2017).

CHAPITRE 2. Principes fondamentaux de conformité des traitements de données effectués dans le cadre d'un dispositif de signalement au RGPD

13. Les principes fondamentaux établis par les autorités de protection des données concernant les traitements de données effectués dans le cadre d'un dispositif d'alerte, tels que lus à lumière des adaptations apportées par le RGPD, portent sur les éléments suivants : la licéité, la loyauté, la transparence, la finalité, la proportionnalité, la sécurité et l'intégrité, les droits de la personne concernée et le respect du principe d'*accountability* par le responsable du traitement.

La responsabilité du respect de ces principes incombe à l'organisation qui décide, ou est tenue, de mettre en place un tel dispositif (responsable du traitement) et le cas échéant, à son fournisseur de service (sous-traitant)[32].

14. Avant de détailler et d'expliciter ces principes, il convient de garder à l'esprit que l'ensemble des règles relatives à la protection des données s'applique aux dispositifs de *whistleblowing* dès lors que ces derniers emportent le traitement de données à caractère personnel. Nous nous attacherons dans le présent chapitre à souligner les spécificités que suscite l'application de ces règles au *whistleblowing*. En outre, il faut noter que la compatibilité d'un dispositif d'alerte avec la protection des données n'emporte pas automatiquement sa légalité. La mise en œuvre d'un tel dispositif suscite effectivement d'autres difficultés juridiques, notamment sur le plan du droit pénal, du droit administratif et du droit social.

SECTION 1. – La licéité du traitement de données effectué dans le cadre d'un dispositif de signalement

15. Tout traitement de données doit se baser sur un fondement légitime tel qu'énoncé à l'article 6 du RGPD afin d'être considéré comme licite. Mis à part le renforcement de l'exigence de consentement quand celui-ci fonde la licéité du traitement, il n'y a pas de grands changements à signaler par rapport à la Directive.

Trois fondements sont susceptibles de légitimer un traitement de données effectués dans le cadre d'un dispositif d'alerte.

[32] Nous verrons que le respect de la protection des données autorise l'externalisation totale ou partielle de la gestion du dispositif d'alerte interne.

§ 1. Soit le traitement de données induit par le dispositif de *whistleblowing* est « nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis »

16. L'article 6.3 du RGPD énonce que le traitement de données qui se fonde sur une obligation légale doit être défini par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis.

À ce propos, la CPVP a précisé, souscrivant à l'avis du Groupe 29[33] et des Commissions de protection de la vie privée française[34] et néerlandaise[35], qu'une obligation légale au sens de la protection des données ne peut reposer sur une disposition étrangère[36]. Toute autre interprétation permettrait, de fait, à des législations étrangères de contourner les règles européennes de protection des données. Il s'ensuit que l'obligation imposée par le *SOX Act* aux entreprises cotées ne peut constituer un fondement licite au sens de l'article 6 c) du RGPD. En revanche, elle peut relever, d'après les autorités de protection, de l'article 6, f) du RGPD (voy. *infra*, n° 18).

17. En l'état actuel du droit[37], l'obligation d'instaurer un dispositif d'alerte interne existe, pour le secteur privé, dans la plupart des États membres de l'Union européenne en vue de mieux réguler le secteur bancaire[38], de lutter contre les abus de marché[39], contre le blanchiment de capitaux et le financement du terrorisme[40] et de garantir la sécurité des

---

[33] Groupe 29, Avis n° 1/2006, p. 8.

[34] CNIL, Autorisation unique n° AU-004, p. 11.

[35] Avis du 16 janvier 2006 relatif à la demande d'autorisation ex. art. 77, al. 2, de la loi néerlandaise WBP du College Bescherming Persoonsgegevens.

[36] CPVP, *Recommandation n° 01/2006*, p. 4. Voy. aussi CPVP, *Avis n° 37/2006 du 27 septembre 2006 relatif à la transmission de données à caractère personnel par la SCRL SWIFT suite aux sommations de l'UST (OFAC)*, p. 20, E.2.1.

[37] Pour une recension de la règlementation internationale et européenne existante, voy. not. F. Coton et J.-Fr. Henrotte, « Le lanceur d'alerte : une personne concernée par le traitement de ses données à caractère personnel, mais également par son avenir professionnel … », *R.D.T.I.*, 2015/61, pp. 45-55.

[38] 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, *J.O.U.E.*, L 176/338 à L 176/436 du 27 juin 2013 (directive bancaire) et directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (Solvabilité II), *J.O.U.E.*, L 335/1 à L335/155 du 17 décembre 2009 (directive Solvabilité II).

[39] Règlement (UE) 596/2014 sur les abus de marché, préc.

[40] Quatrième Directive anti-blanchiment, préc.

opérations pétrolières et gazières en mer[41] ainsi que de l'aviation civile[42]. À la lecture de la Proposition de directive du 23 avril dernier, on peut du reste s'attendre à la création d'une telle obligation dans bien d'autres domaines relevant du droit de l'Union[43], notamment dans le domaine de la lutte contre la fraude et l'évasion fiscales, conformément au rapport de la Commission PANA[44].

En échos au régime de signalement prévu par le *SOX Act*, ces obligations vont de pair avec l'obligation de prévoir des mesures de protection des personnes ayant recours au dispositif d'alerte.

Le secteur public n'est, quant à lui, actuellement affecté que dans un seul domaine, celui de la lutte contre la corruption. Ce domaine n'est régulé par aucun texte de *hard law* en droit de l'Union[45], mais la plupart des États membres se sont dotés d'une législation nationale sur le sujet[46].

---

[41] 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, *J.O.U.E.*, L 178/66 à L 178/106 du 28 juin 2013, art. 22, considérant n° 41 et annexe IV.

[42] Règlement (UE) 376/2014 du Parlement européen et du Conseil du 3 avril 2014 concernant les comptes rendus, l'analyse et le suivi d'événements dans l'aviation civile, *J.O.U.E.*, L 122/18 à L 122/43 du 24 avril 2014.

[43] Conformément au principe de proportionnalité, la proposition de directive du 23 avril 2018 n'établit des standards minimum communs de protection que dans certains domaines de politique. Ceux-ci ont été sélectionnés sur la base de trois critères : (i) le fait qu'il existe un besoin de renforcer l'effectivité du droit ; ii) la pauvreté des signalements est un facteur clé qui affecte l'effectivité du droit ; iii) les manquements au droit de l'Union peuvent résulter en des atteintes sérieuses à l'intérêt public (*Mémorandum explicatif*, p. 6 et considérant n° 5).

[44] Committee of Inquiry to investigate alleged contraventions and maladministration in the application of Union law in relation to money laundering, tax avoidance and tax evasion (Commission PANA), *Report on the inquiry into money laundering, tax avoidance and tax evasion (2017/2013(INI))*, 16 November 2017, §§ 171-174. Dans le même sens, voy. le rapport de la Commission belge « Panama Papers » (Rapport fait au nom de la Commission spéciale « Fraude fiscale internationale/Panama Papers » : Les Panama Papers et la fraude fiscale internationale, 31 octobre 2017, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-2749/001, recommandation n° 23, p. 28).

[45] Sur le sujet, les instances européennes renvoient elles-mêmes aux travaux de l'ONU, du Conseil de l'Europe et de l'OCDE. Voy. not. le « Rapport anticorruption de l'UE », 3 février 2014, COM(2014) 38 final. Soulignons que ces textes visent tant les travailleurs du secteur public que du secteur privé.

[46] Par exemple, voy., en Belgique, la loi du 15 septembre 2013 relative à la dénonciation d'une atteinte suspectée à l'intégrité au sein d'une autorité administrative fédérale par un membre de son personnel, *M.B.*, 4 octobre 2013. La France a, de son côté, choisi de se limiter, dans un premier temps, aux travailleurs du secteur privé (art. 9 de la loi française n° 2007-1598 du 13 novembre 2007 relative à la lutte contre la corruption, *J.O.R.F.*, n° 264 du 14 novembre 2007). Néanmoins, la loi Sapin II est venue ériger en France un véritable régime juridique général de protection des lanceurs d'alerte. Cette loi a conduit à une adaptation par la CNIL de son autorisation unique n° AU-004 (https://www.cnil.fr/fr/alertes-professionnelles-modification-de-lautorisation-unique-ndegau-004 (consulté le 2 juillet 2018)).

La Proposition de directive du 23 avril 2018 aurait donc pour conséquence de considérablement élargir les obligations dans le secteur[47].

§ 2. Soit le traitement de données induit par le dispositif de *whistleblowing* est « nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers »

18. Étant donné que les traitements de données à caractère personnel effectués par les autorités publiques doivent se fonder sur une base légale, une autorité publique ne pourrait justifier la mise en place d'un dispositif de *whistleblowing* en ce qu'il serait nécessaire aux fins de la poursuite de ses intérêts légitimes[48].

En revanche, une entreprise pourrait prétendre que la mise en place d'un tel dispositif poursuit ses intérêts légitimes. Un tel fondement n'est cependant valable que dans la mesure où ne prévalent point les intérêts ou les libertés et droits fondamentaux de la personne concernée sur le plan de la protection des données à caractère personnel[49]. En tout état de cause, des garanties appropriées doivent être concrètement prévues afin de maintenir un juste équilibre entre l'intérêt légitime poursuivi par le traitement et les droits fondamentaux de la personne concernée[50].

19. Ainsi que nous l'avons annoncé, l'obligation imposée par le *SOX Act* aux entreprises cotées est susceptible de relever de l'article 6, f), du RGPD. Les principales organisations internationales, y compris l'Union européenne[51] et l'OCDE[52], reconnaissent effectivement l'importance des principes relatifs à la bonne gouvernance d'entreprise, laquelle peut reposer sur la mise en place « de procédures appropriées permettant aux employés de signaler au conseil d'administration ou à la commission de vérification des

[47] L'article 1er de la proposition de directive du 23 avril 2018 et son Annexe (Part I et II) énumèrent les multiples domaines de politique pour lesquels les moyennes et grandes entreprises ainsi que les administrations fédérales, régionales et, le cas échéant, communales, doivent établir des canaux de signalement interne.

[48] Considérant n° 47 et art. 6.1, *in fine*, du RGPD.

[49] Art. 6.1, f), du RGPD.

[50] Groupe 29, Avis n° 1/2006, p. 10. En particulier, notons que l'article 21.1 du RGPD prévoit que la personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant fondé sur l'article 6, f).

[51] Recommandation de la Commission du 15 février 2005 concernant le rôle des administrateurs non exécutifs et des membres du conseil de surveillance des sociétés cotées et les comités du conseil d'administration ou de surveillance.

[52] OCDE, *Principes de gouvernement d'entreprise de l'OCDE*, 2004, Première partie, section IV.

comptes toute irrégularité et pratique douteuse en matière de comptabilité ou de vérification des comptes »[53]. Le Groupe 29 ne verse donc pas dans la controverse au sujet du champ d'application extraterritorial du *SOX Act*[54], dans la mesure où les entreprises jouissent d'un intérêt légitime à instaurer un tel dispositif, même en l'absence d'une obligation étrangère.

20. Vu l'expansion tant du *whistleblowing* que du principe de responsabilité sociale, les domaines, dans lesquels une entreprise pourrait légitimement prétendre à un intérêt, sont *a priori* très variés. En effet, le *whistleblowing* à l'européenne ne se cantonne plus à l'exécution de lois spécifiques (par exemple, la loi anti-blanchiment) ou à la protection d'intérêts particuliers (par exemple, les investisseurs), mais tend à la protection des atteintes ou menaces à l'« intérêt général »[55] ou « intérêt public »[56].

§ 3. Soit le traitement induit par le dispositif de *whistleblowing* est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement

21. Qu'en est-il de la licéité d'un dispositif de signalement mis en place par une institution ou un organisme public en l'absence de toute obligation légale expresse ? Dans ce cas, le traitement peut vraisemblablement se fonder sur l'article 6.1, e). du RGPD en ce qu'il « est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ».

En ce sens, il est admis que les traitements de données effectués par les institutions de l'Union européenne dans le cadre de leur dispositif d'alerte interne tirent leur licéité de l'article 5, a), du règlement 45/2001[57], qui constitue le pendant de l'article 6.1, e), du RGPD en ce qui concerne les institutions et organes de l'Union[58]. Les institutions et autres organes de

[53] Groupe 29, Avis n° 1/2006, p. 9.

[54] Sur la portée extraterritoriale du *SOX Act*, voy. not. M. GOLDFAYS, « Les systèmes d'alerte professionnelle, un impératif catégorique ? », *Orientations*, 2013/2, p. 17.

[55] Sur la portée de la notion d'intérêt général, voy. not. Résolution du Parlement européen du 24 octobre 2017, préc., considérant n° 17 ; Recommandation CM/Rec(2014)7, Annexe, Section I, principe 2 ; Consultation publique sur « la protection des lanceurs d'alerte » du 3 mars 2017 au 29 mai 2017, document de travail, p. 2.

[56] En ce sens, voy. la Proposition de directive du 23 avril 2018, not. art. 1er.

[57] Règlement (CE) 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, *J.O.C.E.*, L 8/1 à L 8/22 du 12 janvier 2001.

[58] CEPD, *Opinion on a notification for Prior Checking regarding the European Ombudsman's Whistleblowing Procedure*, préc., p. 3, pt 3.2. Pour un exemple, voy. not. CEPD, *Notification*

l'Union européenne ont tout intérêt à mettre en place un tel dispositif dès l'instant où elles sont tenues, en vertu du règlement de l'Union européenne fixant le statut des fonctionnaires[59], de permettre à tout fonctionnaire ayant connaissance d'une activité illégale éventuelle d'en faire immédiatement le signalement.

Tout comme lorsque le traitement se fonde sur une obligation légale, le RGPD prévoit que le fondement du traitement doit être est défini par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis.

22. Au surplus, il importe de souligner qu'un traitement effectué par une personne qui ne relève pas de l'autorité publique peut également se fonder sur cette hypothèse. C'est particulièrement le cas dans le domaine qui nous occupe, dès lors que le *whistleblowing* vise traditionnellement à soutenir les politiques publiques[60].

§ 4. Exigences supplémentaires pour le traitement de catégories particulières de données

23. Le RGPD prévoit, à l'instar de la directive 95/46/CE, des exigences supplémentaires pour le traitement de catégories particulières de données.

Dès lors que les dispositifs d'alerte ont pour vocation de prévenir et de détecter les infractions à la loi, les données à caractère personnel collectées et traitées dans ce cadre peuvent constituer des « données à caractère personnel relatives aux condamnations pénales et à des infractions ». Tel était l'avis de la CPVP sous l'empire de la Directive[61], à la différence du Groupe 29 qui laissait toutefois la porte ouverte à une telle appréciation[62].

Le traitement de cette catégorie particulière de données ne peut être effectué, en vertu de l'article 10 du RGPD, « que sous le contrôle de l'autorité publique, ou si le traitement est autorisé par le droit de l'Union ou par

---

for prior checking, 5 mai 2017, 2017-0466, disponible sur https://edps.europa.eu/sites/edp/files/register/notification_file/1458-2017-0466_-_notification.pdf (consulté le 8 janvier 2018).

[59] Règlement (CEE, Euratom, CECA) 259/68 du Conseil du 29 février 1968 fixant le statut des fonctionnaires des Communautés européennes ainsi que le régime applicable aux autres agents de ces Communautés, et instituant des mesures particulières temporairement applicables aux fonctionnaires de la Commission, *J.O.U.E.*, L 56/1 à L 56/7 du 4 mars 1968.

[60] En ce sens, l'article 64, § 1er, de la loi belge anti-blanchiment énonce que le traitement des données à caractère personnel effectué en vertu de la loi anti-blanchiment est nécessaire à l'exécution d'une mission d'intérêt public au sens de l'article 5 de la loi vie privée (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, *M.B.*, 6 octobre 2017).

[61] CPVP, *Recommandation n° 01/2006*, p. 3 ; CPVP, Avis n° 03/2007, pp. 2-3, pt 8.

[62] Groupe 29, Avis n° 1/2006, p. 7, note 8.

le droit d'un État membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées ».

SECTION 2. – La transparence du traitement de données effectué dans le cadre d'un dispositif de signalement

24. Axe focal du régime de protection tant des données à caractère personnel[63] que des lanceurs d'alerte[64], le principe de transparence requiert qu'une description précise de la procédure d'alerte soit fournie aux collaborateurs de l'organisation susceptibles d'être impliqués dans le dispositif, à savoir aux travailleurs de l'organisation, mais pas seulement dès lors que le dispositif d'alerte peut être étendu à d'autres personnes ayant un contact avec l'organisation (voy. *infra* n° 37)[65].

25. Cette description figure, en général, dans un code de conduite, le règlement de travail ou une déclaration de bonne gouvernance. Par exemple, la déclaration de gouvernance d'entreprise de la société brassicole AB InBev fait état de l'instauration d'un dispositif d'alerte professionnelle (*whistleblowing*) en vue de lutter contre la fraude et les infractions au sein de l'entreprise[66]. S'agissant du signalement externe, la Proposition de directive du 23 avril 2018 souligne qu'une telle description doit figurer sur le site web des autorités compétentes, dans une section distincte, facilement identifiable et accessible[67].

26. Concrètement, le responsable du traitement des données est tenu de fournir aux personnes concernées des informations sur l'existence, la finalité et le fonctionnement du mécanisme, les destinataires des signalements et les droits d'accès, de rectification et de suppression conférés aux personnes mises en cause, le caractère facultatif et complémentaire du dispositif d'alerte ; les conséquences de signalements justifiés et injustifiés et l'obligation de confidentialité à laquelle le dénonciateur est tenu durant l'introduction et le traitement du signalement[68].

---

[63] Art. 5.1, a), du RGPD.

[64] En ce sens, voy. Proposition de directive du 23 avril 2018, art. 5.1, e), et le considérant n° 47.

[65] En ce sens, voy. Proposition de directive du 23 avril 2018, considérant n° 47.

[66] ANHEUSER-BUSCH INBEV, *Corporate Governance Statement*, 2, pt 1.3.1., www.ab-inbev.com (consulté le 20 février 2017).

[67] Proposition de directive du 23 avril 2018, art. 10.

[68] Groupe 29, Avis n° 1/2006, pp. 13-14. CPVP, *Recommandation n° 01/2006*, p. 7 ; CEPD, *Lignes directrices relatives au traitement d'informations à caractère personnel dans le cadre d'une procédure d'alerte éthique*, 18 juillet 2016 (ci-après : Lignes directrices du 18 juillet

La Proposition de directive du 23 avril 2018 précise encore, pour ce qui est du signalement externe, que l'information doit porter sur le régime de confidentialité applicable au signalement, en particulier eu égard à l'article 13 du RGPD[69], les voies de recours en cas de représailles, la nature du suivi apporté au signalement et l'immunité dont jouissent les personnes ayant fait un signalement conforme à la future directive par rapport aux restrictions de divulgation dont les informations signalées pouvaient être assorties[70].

27. Au demeurant, soulignons que la mise sur pied d'un dispositif d'alerte doit se faire en conformité avec les législations sur le droit collectif du travail[71], en informant et en prenant conseil, s'il échet, auprès du conseil d'entreprise, du comité pour la protection et la prévention du travail, de la délégation syndicale ou des comités de négociation ou de concertation[72].

SECTION 3. – La loyauté du traitement de données effectué dans le cadre d'un dispositif de signalement

28. L'exigence de loyauté fait contrepoids aux risques patents de sombrer dans une culture de la délation. Celle-ci emporte en particulier quatre garde-fous.

29. *Primo*, le signalement ne peut se fonder sur de simples rumeurs[73] : il doit se baser sur un motif raisonnable et décrire avec suffisamment de précision les faits dénoncés[74]. Il ne peut, du reste, porter sur des faits dont le donneur d'alerte sait pertinemment qu'ils sont faux. Le lanceur d'alerte

2016), p. 8. Voy. aussi CEPD, *Prior-check Opinion on the Whistleblowing Policy of the European Investment Bank*, préc., p. 2 ; CNIL, Autorisation unique n° AU-004, p. 13.

[69] Ainsi que l'article 13 de la directive Police & Justice et l'article 11 du règlement précité 45/2001.

[70] Proposition de directive du 23 avril 2018, art. 10, d), e), f) et g).

[71] Groupe 29, Avis n° 1/2006, p. 7. En ce sens, voy. aussi European Parliament recommendation of 13 December 2017 to the Council and the Commission following the inquiry into money laundering, tax avoidance and tax evasion (2016/3044(RSP)), pt 182 ; Proposition de directive du 23 avril 2018, art. 4.1.

[72] Un tribunal allemand a ainsi invalidé un dispositif d'alerte qui avait été adopté par une entreprise sans obtenir le consentement des organes de concertation pertinents (C. KUNER, *European Data Protection Law. Corporate Compliance and Regulation*, second edition, Oxford, Oxford University Press, 2007, p. 274).

[73] Voy. not. CPVP, *Recommandation n° 01/2006*, p. 5 ; CEPD, *Decision on internal rules concerning whistleblowing*, 14 December 2015, art. 4.

[74] Comme le souligne la Cour européenne des droits de l'homme, l'exercice de la liberté d'expression, laquelle comprend le droit de lancer des alertes, s'accompagne d'une série de devoirs et de responsabilités.

est en effet tenu d'agir de bonne foi[75]. De fait, toute dénonciation abusive ou malveillante pourra être sanctionnée d'un point de vue disciplinaire, civil et/ou pénal. Enfin, le signalement ne peut porter sur des faits strictement privés sans aucun rapport avec le champ d'application matériel du dispositif d'alerte[76].

30. *Secundo*, le signalement confidentiel devrait être préféré au signalement anonyme. Si dans les deux cas, l'identité du lanceur d'alerte ne peut être révélée, sauf consentement ou obligation légale, elle n'est connue de son destinataire que dans le premier cas[77]. Concrètement, le dispositif d'alerte doit prévoir une interdiction de divulguer l'identité du dénonciateur ou des éléments qui peuvent permettre son identification sans son accord pendant toute la durée du traitement de la dénonciation[78], sauf si les investigations ne peuvent être poursuivies sans révéler l'identité du dénonciateur, par exemple s'il représente un témoin clé en justice[79]. L'identité du dénonciateur peut du reste être révélée en cas de dénonciation injustifiée ou abusive (voy. *infra* n° 49).

Une telle position s'explique par l'incompatibilité apparente du signalement anonyme avec le principe de loyauté[80]. Au-delà de la protection des données, d'autres raisons conduisent les autorités européennes à adopter cette position[81]. Tout d'abord, l'identification du lanceur d'alerte paraît nécessaire en vue d'assurer sa protection contre les représailles. Il peut être aussi utile aux autorités chargées du suivi de pouvoir contacter le lanceur d'alerte pour de plus amples renseignements. Il arrive, par ail-

---

[75] L'exigence de bonne foi est essentielle en droit du *whistleblowing*. Voy. not. Conseil d'État français, *Le droit d'alerte : signaler, traiter, protéger*, préc., p. 73, pt 3.3.3. ; Proposition de directive du 23 avril 2018, *Mémorandum explicatif*, p. 12 et considérant n° 60 ; CEPD, *Decision on internal rules concerning whistleblowing*, 14 December 2015, p. 2 ; CEPD, *Lignes directrices du 18 juillet 2016*, p. 5, pt 6. Voy. aussi Cour eur. D.H., arrêt *Guja*, précité, § 77. T. Boyer, « Les dispositifs d'alerte dans les entreprises : whistleblowing vs droit d'alerte », *Management & Avenir*, 2013/4, n° 62, p. 99 (disponible sur www.cairn.info, consulté le 15 décembre 2017).

[76] CEPD, *Decision on internal rules concerning whistleblowing*, 14 December 2015, art. 4.

[77] Voy. not. Rapport préc., A/70/361, p. 20, § 40.

[78] CPVP, *Recommandation n° 01/2006*, p. 5.

[79] CEPD, *Decision on internal rules concerning whistleblowing*, 14 December 2015, art. 8.

[80] Groupe 29, Avis n° 1/2006, p. 11.

[81] *Idem* ; CPVP, *Recommandation n° 01/2006*, p. 5 ; CEPD, *Lignes directrices du 18 juillet 2016*, p. 6, pt 12 ; CNIL, Autorisation unique n° AU-004, p. 12. Voy. aussi, au-delà du cadre de la protection des données : P. Stephenson et M. Levi, « La protection des « donneurs d'alerte : rapport d'étude sur la faisabilité d'un instrument juridique sur la protection des employés qui divulguent des informations dans l'intérêt public », CDCJ(2012)9FIN, p. 32 ; Recommandation CM/Rec (2014)7, Section V, Principe 18 et Exposé des motifs, § 12 ; Rapport préc., A/70/361, p. 20, § 40.

leurs, que l'anonymat soit dans les faits impossible dans la mesure où les informations dénoncées ne sont connues que par un cercle réduit d'initiés. Du reste, on craint que l'anonymat n'encourage les dénonciations abusives et/ou malhonnêtes. Enfin, on redoute que l'anonymat ne renforce les suspicions mutuelles qui peuvent naître d'un dispositif d'alerte professionnelle et briser de la sorte la nécessaire confiance devant régner au sein d'une organisation.

En pratique, le recours à l'anonymat s'avère cependant indispensable dans certaines circonstances exceptionnelles, notamment pour des raisons liées à la psychologie du lanceur d'alerte[82] ou lorsque la dénonciation n'est pas organisée[83]. Des tiers intervenants à la procédure d'alerte, en qualité de témoins (par exemple, des collègues), pourraient en outre souhaiter bénéficier de l'anonymat[84]. L'utilisation courante d'une plateforme en ligne amène par ailleurs à tolérer l'anonymat dès lors que ce dernier est perçu comme un outil fondamental de sécurisation des activités en ligne[85].

En toutes hypothèses, le signalement anonyme devra être « traité avec une précaution particulière »[86]. Aussi, les organisations ne peuvent en aucun cas promouvoir le signalement anonyme comme étant la règle habituelle[87].

31. *Tertio*, le dispositif ne peut prévoir d'obligation de signalement : le recours au dispositif d'alerte doit toujours être facultatif[88]. Dans la

[82] On observe, par exemple, que la mise en place d'un dispositif ICT de surveillance sur le travail peut saper la volonté des employés de dénoncer des pratiques illégales ou irrégulières, sauf à leur accorder l'anonymat (Groupe 29, Opinion 2/2017 on 8 June 2017 on data processing at work, WP 249, p. 10).

[83] Groupe 29, Avis n° 1/2006, p. 12.

[84] Sur le témoignage anonyme, voy. not. Ch. De Valkeneer, *Manuel de l'enquête pénale*, Larcier avec la collaboration de Politeia, 2005, pp. 91 et 92.

[85] Voy. spéc. 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 ; Déclaration commune de la société civile soumise à la 29e session du Conseil des droits de l'homme des Nations unies : « Assurer la promotion des outils de chiffrement et d'anonymisation en ligne à l'ère numérique », disponible sur le site de RSF : https://rsf.org (consulté le 10 avril 2018). Voy. aussi Déclaration commune de la Commission de réflexion et de propositions sur le droit et les libertés à l'âge numérique de l'Assemblée nationale française et la Commission sur les droits et devoirs sur Internet de la Chambre des députés italienne, Paris, 28 septembre 2015.

[86] Groupe 29, Avis n° 1/2006, p. 12. Voy. aussi CNIL, Autorisation unique n° AU-004, art. 2.

[87] CPVP, *Recommandation n° 01/2006*, p. 5 ; CNIL, Autorisation unique n° AU-004, art. 2.

[88] CNIL, Autorisation unique n° AU-004, art. 8.

négative, on pourrait penser que cela reviendrait à faire supporter sur l'employé la responsabilité de l'employeur d'assurer le respect de son code de conduite (lequel contient le dispositif d'alerte) et, le cas échéant, de la législation pertinente[89]. Cette position ne nous paraît pas si évidente. En effet, on constate que si le délégué à la protection des données est tenu de superviser le respect de la protection des données et de signaler, le cas échéant, les dysfonctionnements à la direction (voy. *infra* n° 65)[90], il n'en devient pas pour autant responsable de la conformité à la protection des données de l'organisation à laquelle il appartient. Le raisonnement pourrait s'appliquer au lanceur d'alerte. Le caractère facultatif de l'alerte procède plus vraisemblablement du droit à la liberté d'expression d'où le droit d'alerte tire sa légitimité[91], et d'un choix politique essentiel : nous ne voulons pas, en Europe, d'une société où la conscience professionnelle serait le fruit d'une surveillance permanente exercée par ses pairs. Bref, nous ne voulons pas d'une société de la délation.

32. *Quarto*, le « gestionnaire de plaintes » (« *Whistleblower Officer* ») doit répondre à certaines garanties, en termes d'indépendance, de confidentialité et de qualification professionnelle[92]. À cet égard, la protection des données occupe une place centrale dans la formation du gestionnaire[93]. Les traitements de données effectués doivent, en particulier, relever d'un département distinct[94]. En pratique, la fonction de *Whistleblower Officer* relève du département « *compliance* », à l'instar du délégué à la protection des données, dont le RGPD impose la désignation dans certains cas (voy. *infra* n° 64)[95].

---

[89] CNIL, Autorisation unique n° AU-004, p. 12. La CNIL se rapporte, à cet égard, à une lettre que le ministère de l'emploi, du travail et de l'insertion professionnelle des jeunes lui a adressée. Voy. aussi O. GOFFARD, « Les systèmes d'alerte professionnelle (*whistleblowing*) et le respect de la vie privée : du Sarbanes-Oxley Act à la recommandation de la Commission de la vie privée », *T.B.H.*, 2007/3, p. 210.

[90] L'article 38.3., *in fine*, du RGPD énonce que « le délégué à la protection des données fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant ».

[91] Voy. la jurisprudence de la Cour européenne des droits de l'homme en matière de lancement d'alerte, spéc. : arrêt *Guja,* arrêt *Heinisch* et arrêt *Bucur*.

[92] Notons que la Proposition de directive du 23 avril 2018 est particulièrement attentive aux garanties que doit présenter le gestionnaire des plaintes d'une autorité compétente (spéc. art. 8). Pour ce qui est des garanties que doit fournir le gestionnaire des plaintes d'une entreprise, voy. considérant n° 45.

[93] En ce sens, voy. not. la Proposition de directive du 23 avril 2018, considérant n° 53.

[94] Groupe 29, Avis n° 1/2006, p. 16 ; CPVP, *Recommandation n° 01/2006*, p. 8.

[95] Voy. not. J. TERSTEGGE, « EU Watch : Data protection and the new face of privacy compliance », *Business Compliance*, 2013/6, p. 34.

Précisons encore que le gestionnaire des plaintes peut faire appel à des instances internes ou externes en vue d'enquêter sur les dénonciations reçues[96]. Il n'est, du reste, pas exclu que la gestion du dispositif d'alerte soit externalisée totalement (*outsourcing*) vers un fournisseur de service externe, même si le Groupe 29 donne la préférence à une gestion interne du dispositif.

L'article 28.1 du RGPD vient amplifier, par rapport à la directive 95/46/CE, les exigences devant figurer dans le contrat unissant le sous-traitant au responsable du traitement. Dans tous les cas, le fournisseur de service devra présenter, en sa qualité de sous-traitant, des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement et garantisse notamment la protection des droits de la personne concernée[97]. Le fournisseur de service devra, au surplus, offrir les mêmes garanties que le gestionnaire de plaintes lui-même, notamment en termes de compétence, confidentialité, sécurité et indépendance[98].

SECTION 4. – La finalité du traitement de données effectué dans le cadre d'un dispositif de signalement

33. Comme sous l'empire de la directive 95/46/CE, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes. Lorsque le dispositif de signalement fonde sa licéité sur une obligation légale ou sur la poursuite d'une mission d'intérêt public, la finalité du traitement effectué dans le cadre de ce dispositif doit être définie précisément par le législateur[99].

Lorsque le dispositif de signalement fonde sa licéité sur l'intérêt légitime du responsable du traitement, la finalité du traitement doit être définie par ce dernier. Nous avons vu que le *whistleblowing* se présentait

[96] *Ibid.*, p. 7.

[97] Groupe 29, Avis n° 1/2006, p. 18. Voy. aussi K. Rosier, « Chapitre III : hypothèses dans lesquelles une violation des obligations de secret ou de confidentialité pourrait être admise, Section 1. *Whistleblowing* », in *Secret et loyauté dans la relation de travail* (S. Gilson, K. Rosier, A. Roger et S. Palate dir.), Waterloo, Kluwer, 2013, p. 148 ; O. Goffard, « Les systèmes d'alerte professionnelle (*whistleblowing*) et le respect de la vie privée : du Sarbanes-Oxley Act à la recommandation de la Commission de la vie privée », *op. cit.*, p. 208.

[98] Groupe 29, Avis n° 1/2006, pp. 15-16 ; CPVP, Avis n° 03/2007, p. 5, pt 26 ; CPVP, *Recommandation n° 01/2006*, p. 7. En ce sens, voy. aussi la proposition de directive du 23 avril 2018, art. 5.2, al. 2.

[99] Art. 6.3 du RGPD.

aujourd'hui comme un nouvel outil de gouvernance. Mais encore faut-il savoir ce que cette notion recouvre. À côté des domaines couverts par le *SOX Act* (voy. *supra* n° 7)[100], on peut se demander, compte tenu des problèmes qui occupent aujourd'hui la communauté internationale, si la lutte contre le réchauffement climatique, la protection de la santé publique et des consommateurs ainsi que la lutte contre la fraude et l'évasion fiscales ne relèvent pas du bon gouvernement d'entreprise. Toujours est-il que de telles finalités entrent dans le champ d'application matériel de la Proposition de directive du 23 avril 2018 au rang de politiques de l'Union européenne[101].

Quid lorsque les faits dénoncés sont étrangers à la finalité pour laquelle le dispositif a été instauré ?

Le Groupe 29 précise qu'ils peuvent être transmis aux organes compétents de l'organisation « si les intérêts vitaux de la personne concernée par ces données ou l'intégrité morale d'employés sont en jeu ». Des cas de harcèlement ou de discrimination au travail pourraient ressortir de la notion d'intégrité morale[102]. Le CEPD confirme cette hypothèse, à tout le moins s'agissant des dispositifs d'alerte mis en place au sein des institutions de l'Union européenne[103].

En outre, le Groupe 29 estime que les faits signalés peuvent également être transmis « s'il existe, en vertu du droit national, une obligation légale de communiquer ces informations aux pouvoirs publics ou aux autorités de poursuites compétentes »[104]. On bascule ici dans le signalement *externe,* qui représente en réalité un nouveau traitement de données amplement justifié par l'obligation légale faite au destinataire de l'information[105]. Une telle obligation de coopération existe en matière pénale dans la plupart des États membres, mais elle ne s'applique en général qu'aux agents de l'État. La précision apportée par le RGPD en son cinquantième considérant s'avère donc utile, sans être suffisante, s'agissant du secteur privé. Selon ce considérant, « le fait, pour le responsable du traitement, de révéler l'existence d'éventuelles infractions pénales ou de menaces pour la sécurité publique et de transmettre à une autorité compétente les données à

[100] Groupe 29, Avis n° 1/2006, p. 12.

[101] Proposition de directive du 23 avril 2018, art. 1er et Annexe (Part I et II).

[102] En ce sens, voy. Groupe 29, Avis n° 1/2006, p. 13.

[103] CEPD, *Lignes directrices du 18 juillet 2016*, p. 10, pt 29.

[104] Groupe 29, Avis n° 1/2006, p. 13.

[105] En ce sens, la Proposition de directive du 23 avril inclut dans la procédure de suivi du signalement la communication aux autorités compétentes (considérant n° 46). Elle précise aussi expressément, dans le texte même de la directive, que les autorités publiques qui reçoivent un signalement pour lequel elles ne sont pas compétentes doivent le transmettre à l'autorité compétente en veillant à en informer le lanceur d'alerte (art. 6.4 et considérant n° 51).

caractère personnel concernées dans des cas individuels ou dans plusieurs cas relatifs à une même infraction pénale ou à des mêmes menaces pour la sécurité publique devrait être considéré comme relevant de l'intérêt légitime du responsable du traitement. Néanmoins, cette transmission dans l'intérêt légitime du responsable du traitement ou le traitement ultérieur des données à caractère personnel devrait être interdit lorsque le traitement est incompatible avec une obligation de confidentialité légale, professionnelle ou toute autre obligation de confidentialité contraignante ».

SECTION 5. – La proportionnalité du traitement de données effectué dans le cadre d'un dispositif de signalement

34. Comme le prévoyait déjà la Directive, les données à caractère personnel traitées dans le cadre d'un dispositif d'alerte doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées »[106] et « exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder »[107].

En particulier, la CPVP souligne que les données doivent rester limitées à la désignation de faits et ne pas contenir, en principe, de jugement de valeur ni d'appréciation subjective et doivent être mentionnées expressément en tant que telles si elles concernent des faits non prouvés[108].

Les données personnelles doivent, d'autre part, être « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées »[109]. Le délai de conservation peut varier en fonction de la nature de l'information traitée et de l'issue de la procédure[110]. Les données non pertinentes pour le traitement de la dénonciation devraient être supprimées dans les plus brefs délais et ne peuvent

[106] Art. 5, c), du RGPD.
[107] Art. 5, d), du RGPD.
[108] CPVP, *Recommandation n° 01/2006*, pp. 6 et 7.
[109] Art. 5, e), du RGPD.
[110] CEPD, *Lignes directrices du 18 juillet 2016*, p. 10, pt 27. Voy. aussi CEPD, *Prior-check Opinion on the Whistleblowing Policy of the European Investment Bank*, préc., p. 3.

pas faire l'objet d'un traitement ultérieur[111]. Les autres données devraient être supprimées rapidement, et généralement dans un délai de deux mois à compter de l'aboutissement des opérations de vérification de la pertinence ou de la recevabilité des faits signalés[112], sauf « si une procédure judiciaire est engagée ou si des mesures disciplinaires sont prises contre la personne mise en cause ou le dénonciateur en cas de fausse déclaration ou de déclaration diffamatoire »[113]. Dans ces cas, les données peuvent être conservées – et même « doivent » selon la proposition de directive du 23 avril 2018[114] – jusqu'au terme de la procédure et à l'expiration des délais de recours[115].

Précisons que ces délais de conservation ne portent pas préjudice à l'application des lois nationales en matière d'archivage.

35. Outre ces exigences classiques, l'application du principe de proportionnalité au lancement d'alerte emporte les trois exigences suivantes : (i) le dispositif de signalement doit être complémentaire des autres dispositifs classiques de contrôle, (ii) son champ d'application doit être strictement limité et (iii) il doit être organisé au plus près du fait dénoncé. Du reste, il découle de la lecture du principe de proportionnalité dans le cadre de la liberté d'expression qu'une procédure par paliers devrait être privilégiée. Cette exigence semble également servir la protection des données, ce pourquoi nous l'évoquons ici.

Il incombe au gestionnaire de plaintes d'assurer le respect de ces exigences[116].

36. Tout d'abord, le système d'alerte doit apparaître comme le complément, et non le substitut, des canaux classiques de gouvernance (voie hiérarchique, auditeurs internes) et de gestion des conflits des travailleurs (représentants du personnel, service des ressources humaine, service de

---

111 CEPD, *Lignes directrices du18 juillet 2016*, p. 6, pt 14 et p. 10, pt 27 ; CNIL, *Autorisation unique n° AU-004*, p. 15. En ce sens, voy. aussi Proposition de directive du 23 avril 2018, art. 18.

112 Groupe 29, Avis n° 1/2006, p. 13 ; CNIL, *Autorisation unique n° AU-004*, p. 15. Après s'être prononcé en faveur d'un délai de deux ans (CEPD, *Decision on internal rules concerning whistleblowing*, 14 December 2015, art. 19), le CEPD s'est finalement aligné sur les recommandations du Groupe 29 en la matière (CEPD, *Lignes directrices du 18 juillet 2016*, p. 10, pt 29 ; CEPD, *Opinion on a notification for Prior Checking regarding the European Ombudsman's Whistleblowing Procedure*, préc., p. 4, pt 3.2).

113 Groupe 29, Avis n° 1/2006, p. 13.

114 Proposition de directive du 23 avril 2018, considérant n° 57.

115 Groupe 29, Avis n° 1/2006, p. 13.

116 CPVP, *Recommandation n° 01/2006*, p. 6.

médiation), lesquels jouissent d'une procédure et d'organes spécifiques réglementés par la loi (par exemple, le harcèlement au travail)[117].

37. Les autorités de protection des données soulignent, ensuite, l'importance de définir strictement le champ d'application du dispositif d'alerte s'agissant tant des faits pouvant être dénoncés que des personnes pouvant dénoncer ou être dénoncées[118].

Ratione materiae, le dispositif d'alerte ne peut s'appliquer qu'aux « faits suffisamment graves » dont la dénonciation est requise par la loi ou la sauvegarde de l'intérêt public. Il ne s'agit pas nécessairement d'infractions à la loi. Des dysfonctionnements sérieux peuvent être visés. Une conduite qui porte gravement atteinte aux intérêts de l'Union européenne ou d'un État membre, ou aux obligations professionnelles et/ou déontologiques du personnel peut constituer un fait « grave »[119].

Ratione personae, il importe de limiter tant le nombre de personnes autorisées à signaler des irrégularités par le biais du dispositif d'alerte que le nombre de personnes susceptibles d'être mises en cause par un tel dispositif. À la différence du CEPD[120], le Groupe 29[121] et la CPVP[122] estiment que seules des personnes qui *font partie de l'organisation* peuvent dénoncer ou faire l'objet d'une dénonciation. Il semblerait donc exclu que des anciens travailleurs, des stagiaires, des fournisseurs ou des clients soient concernés par un dispositif d'alerte. Il n'empêche que la Proposition de directive récemment déposée par la Commission entend largement la notion de lanceur d'alerte (en réalité, « *reporting person* »), et l'étend précisément à ces catégories de personnes qui sont connectées, d'une façon ou d'une autre, à l'organisation, ainsi qu'aux personnes morales[123].

---

[117] Voy. not., Groupe 29, Avis n° 1/2006, p. 6 ; CPVP, *Recommandation n° 01/2006*, p. 6 ; CEPD, *Lignes directrices du 18 juillet 2016*, p. 6, pt 10 ; CEPD, *Prior-check Opinion on the Whistleblowing Policy of the European Investment Bank*, préc., p. 2 ; CNIL, Autorisation unique n° AU-004, p. 10.

[118] CPVP, *Recommandation n° 01/2006*, p. 6 ; CPVP, Avis n° 03/2007, pp. 2 et 3 ; CNIL, *Autorisation unique n° AU-004*, p. 10.

[119] En ce sens, voy. not. CEPD, *Decision on internal rules concerning whistleblowing*, préc., art. 3.

[120] Dans ses lignes directrices, le CEPD mentionne en effet que « les parties extérieures qui concluent un contrat avec les institutions de l'UE ou qui prennent contact avec celles-ci (p.ex. consultants, contractants, chercheurs, etc.) doivent être informées de la possibilité de signaler les suspicions de fraude, de corruption ou d'autres manquements et irrégularités graves » (CEPD, *Lignes directrices du 18 juillet 2016*, p. 4, pt 4). Ce prescrit est également repris dans la décision du CEPD relative au dispositif d'alerte interne qu'il a lui-même mis en place au sein de son organisation (CEPD, *Decision on internal rules concerning whistleblowing*, préc., art. 17).

[121] Groupe 29, Avis n° 1/2006, pp. 10-11.

[122] CPVP, *Recommandation n° 01/2006*, p. 6.

[123] Proposition de directive du 23 avril 2018, art. 3 (9).

38. Le Groupe 29 encourage, par ailleurs, la gestion interne du dispositif. Sauf exception, les personnes les plus proches de la source du problème sont, en effet, les plus à même de solutionner rapidement et efficacement le problème dénoncé[124]. En particulier, le Groupe 29 estime que les groupes multinationaux devraient traiter, en règle générale, « les signalements au niveau local, c'est-à-dire dans un pays de l'UE, plutôt que partager automatiquement toutes ces informations avec d'autres sociétés du groupe »[125].

39. Pour finir, en marge de la protection des données, on préconise habituellement la mise sur pied d'une procédure échelonnée eu égard au devoir de loyauté, de réserve et de discrétion auquel est astreint le lanceur d'alerte[126]. Sauf circonstances exceptionnelles[127], le lanceur d'alerte devrait faire part de ses préoccupations en interne, au sein de son entreprise ou de son administration, avant de les signaler en externe aux autorités[128]. Enfin, la divulgation au public ne devrait, quant à elle, « être envisagée qu'en dernier ressort, en cas d'impossibilité manifeste d'agir autrement »[129].

Un tel séquençage est susceptible de participer, à notre sens, au respect de la protection des données et de la vie privée en ce qu'il permet de traiter l'alerte au plus près des personnes concernées et de la façon la plus discrète possible. Il permet, par ailleurs, de mettre fin, rapidement et efficacement, à la menace dénoncée pour l'intérêt public et contribue également à la prévention des atteintes injustifiées à la réputation qui pourraient résulter d'une révélation publique[130].

---

[124] En ce sens, voy. aussi Proposition de directive du 23 avril 2018, considérant n° 38.

[125] Groupe 29, Avis n° 1/2006, p. 18.

[126] En ce sens, voy. not. Cour eur. D.H., arrêt *Heinisch*, § 65 ; arrêt *Guja*, § 73 ; Recommandation CM/Rec (2014)7, Exposé des motifs, § 67 ; Proposition de directive du 23 avril 2018, art. 13. Sur cette procédure échelonnée, voy. not. V. JUNOD, « La liberté d'expression du whistleblower. Cour européenne des droits de l'homme (Grande Chambre), Guja c. Moldova, 12 février 2008 », *Rev. trim. dr. h.*, 2009/77, pp. 227-260 ; K. ROSIER, « Chapitre III : hypothèses dans lesquelles une violation des obligations de secret ou de confidentialité pourrait être admise, Section 1. *Whistleblowing* », *op. cit.*, p. 134.

[127] Pour une illustration, voy. par exemple Cour eur. D.H, arrêt *Bucur*, §§ 96-97.

[128] Pour une illustration, voy. not. Cour eur. D.H., arrêt *Heinisch*, §§ 73-76 ; Cour eur. D.H., 5e sect., arrêt *Soares c. Portugal*, 21 juin 2016, req. n° 79972/12, § 48.

[129] Cour eur. D.H., arrêt *Heinisch*, § 65 ; arrêt *Guja*, § 73.

[130] En ce sens, voy. Proposition de Directive du 23 avril 2018, considérant n° 61.

SECTION 6. – L'intégrité et la confidentialité du traitement de données effectué dans le cadre d'un dispositif de signalement

40. Comme le préconisait déjà la directive 95/46/CE[131], le responsable du traitement et le sous-traitant sont tenus, en application du RGPD, de traiter les données à caractère personnel de façon à en garantir une sécurité appropriée « à l'aide de mesures techniques ou organisationnelles appropriées »[132]. À cet égard, la confidentialité de l'identité du lanceur d'alerte, de la personne mise en cause et du signalement constitue une garantie majeure au sein du système de protection élaboré tant par les autorités européennes de protection des données[133] que par les autres instances européennes[134]. En particulier, il apparaît que le système d'alerte ne saurait être efficace, compte tenu des risques de représailles qui pèsent sur le lanceur d'alerte, si ce dernier craignait de voir révélés à des tiers son identité ainsi que le contenu de son signalement.

41. Au demeurant, mentionnons que les données relatives au signalement ne peuvent être transférées vers un autre pays de l'Union européenne que dans le respect des dispositions régissant la protection des données, et spécialement des obligations de sécurité et de confidentialité[135]. Un tel transfert doit être nécessaire aux besoins de l'enquête et résulter de l'organisation du groupe, eu égard à la nature et à la gravité des faits[136]. Les dispositions régissant les flux transfrontières sont, de surcroît, d'application lorsque les données sont transférées vers un pays tiers hors Union européenne[137]. Vu son origine, le *whistleblowing* se pratique actuellement davantage dans les groupes américains. Il est dès lors probable que les données personnelles soient transférées, pour le traitement de la dénonciation, vers le siège social de l'entreprise situé aux États-Unis. Suite aux révélations du lanceur d'alerte Edward Snowden, notons que la Commission européenne a conclu un nouvel accord avec ce pays, le

131 Art. 17 de la directive 95/46/CE.

132 Art. 5.1, f), du RGPD.

133 Voy. not. Groupe 29, Avis n° 1/2006, pp. 12 et 15.

134 Voy. not. Proposition de directive du 23 avril 2018, considérants n^{os} 44, 48 et 55 et art. 5.1, 6.2 et 9. Le Comité des Ministres du Conseil de l'Europe consacre le principe de confidentialité pour le seul lanceur d'alerte (Recommandation CM/Rec (2014) 7, Annexe, Section V, Principe 18).

135 Groupe 29, Avis n° 1/2006, p. 18.

136 CNIL, *Autorisation unique n° AU-004*, p. 14.

137 Groupe 29, Avis n° 1/2006, pp. 15-16 ; CPVP, *Recommandation n° 01/2006*, p. 8.

« *Privacy Shield* », dans le but de garantir le respect de règles de protection substantiellement équivalentes à la protection européenne des données[138].

SECTION 7. – Les droits de la personne concernée par un traitement de données effectué dans le cadre d'un dispositif de signalement

42. Les parties intervenantes, à savoir le lanceur d'alerte, la personne mise en cause et les tiers éventuels – tels que les témoins – jouissent, en règle, des « droits de la personne concernée » prévus au chapitre III du RGPD (§ 1). À ce propos, rappelons que le droit à la protection des données n'est reconnu qu'aux personnes physiques. Ainsi, si l'entreprise ou l'institution ébranlée par un signalement peut subir un préjudice, notamment en cas de rupture de la confidentialité, c'est à d'autres ressources juridiques, telles que le droit de la responsabilité voire un jour le droit du lancement d'alerte[139], qu'elle devra faire appel.

Comme à l'époque de la Directive, des dérogations aux droits de la personne concernée demeurent permises (§ 2).

§ 1. Portée des droits de la personne concernée

43. Les droits de la personne concernée comprennent le droit d'information, le droit d'accès, le droit d'opposition, le droit de rectification et le droit d'effacement[140]. Leur effectivité, soulignons-le, repose en amont sur une information individuelle des parties intervenantes de l'instance auprès de laquelle leurs droits peuvent être exercés. Il peut, par ailleurs, être utile de spécifier le délai dans lequel une réaction doit être attendue[141].

---

[138] Sur le régime des flux transfrontières et le *Privacy Shield*, voy. C. DE TERWANGNE et C. GAYREL, « Flux transfrontières de données et exigence de protection adéquate à l'épreuve de la surveillance de masse. Les impacts de l'arrêt Schrems », *Cahiers de Droit Européen*, 2017/11, pp. 35-81 et la contribution consacrée à cette question au sein du présent ouvrage.

[139] De fait, la Proposition de directive du 23 avril 2018 définit la personne concernée comme « une personne physique ou morale désignée dans le signalement ou la révélation comme étant la personne responsable du manquement ou comme y étant associée » (nous traduisons) (art. 3 (11)).

[140] Voy. le chapitre du présent ouvrage dédié aux droits des personnes concernées.

[141] CEPD, *Opinion on a notification for Prior Checking regarding the European Ombudsman's Whistleblowing Procedure*, préc., p. 4, pt 3.2.

a) Le droit d'information du lanceur d'alerte et des autres personnes concernées

44. Les informations prévues aux articles 13.1 (collecte directe) et 14.1 (collecte indirecte) du RGPD doivent être transmises au lanceur d'alerte, d'une part, et à la personne dénoncée et aux tiers impliqués, d'autre part. Parmi ces informations figurent les destinataires ou catégories de destinataires des données. En l'occurrence, il peut s'agir du service d'audit interne ou d'un tiers externe si le gestionnaire de plaintes se fait assister dans le cadre de sa mission ; d'un organe de la société mère, en cas de groupe d'entreprises, si le dispositif d'alerte prévoit un tel transfert en cas d'irrégularités graves. Dans le secteur public, il peut par ailleurs être nécessaire, en fonction du droit national, de prévoir la communication aux autorités judiciaires et pénales.

Dans la mesure où elles sont « nécessaires pour garantir un traitement équitable et transparent », les informations complémentaires suivantes doivent être transmises en application des articles 13.2 et 14.2 du RGPD : les durées possibles de conservation des données et les critères utilisés pour déterminer cette durée ; la portée des droits de la « personne concernée » et leurs modalités d'exercice ainsi que l'instance auprès de laquelle ces droits peuvent être exercés ; le droit d'introduire une réclamation auprès d'une autorité de contrôle. Vu les orientations du Groupe 29, de la CNIL, de la CPVP et du CEPD, on ne saurait que conseiller la communication de ces informations complémentaires.

45. La personne mise en cause, largement oubliée des textes américains, fait l'objet d'une attention particulière de la part des autorités européennes de protection des données[142]. Les dispositifs d'alerte professionnelle lui font, en effet, « courir un risque très grave de stigmatisation et de victimisation […] au sein de son organisation »[143].

En particulier, la personne mise en cause devrait être informée le plus rapidement possible de : « [1] l'entité responsable du mécanisme de dénonciation, [2] les faits dont il est accusé, [3] les directions ou services qui pourraient recevoir le signalement au sein de sa société ou d'autres entités ou sociétés du groupe dont sa société fait partie, et [4] de la manière d'exercer ses droits d'accès et de rectification »[144]. En revanche,

[142] La Proposition de directive du 23 avril 2018 lui consacre de même une disposition expresse (art. 16).

[143] Groupe 29, Avis n° 1/2006, pp. 7 et 14. Voy. aussi CEPD, *Opinion on a notification for Prior Checking regarding the European Ombudsman's Whistleblowing Procedure*, préc., p. 5, pt 3.4.

[144] Groupe 29, Avis n° 1/2006, p. 14. Voy. aussi CNIL, *Autorisation unique n° AU-004*, p. 15 ; CPVP, *Recommandation n° 01/2006*, p. 7.

l'obligation de confidentialité de l'identité du dénonciateur (voy. *supra* n° 40) devrait faire obstacle à ce que la personne mise en cause reçoive, conformément à l'article 14.2, f), du RGPD, « la source d'où proviennent les données à caractère personnel ».

En toutes hypothèses, l'article 14.3 du RGPD prévoit que cette information a lieu dans un délai raisonnable après obtention des données personnelles, mais ne dépassant pas un mois, eu égard aux circonstances particulières dans lesquelles les données sont traitées.

Cependant, s'il s'avère que l'information de la personne mise en cause risque de compromettre la réalisation de l'enquête ou la collecte de preuves, elle peut être différée aussi longtemps que ce risque existe, conformément à l'article 14.5, b), du RGPD[145]. À l'instar de Fanny Coton et Jean-François Henrotte, on se demande si la suspension de l'information de la personne mise en cause ne constitue finalement pas la règle, plutôt que l'exception, dans le cadre d'un dispositif d'alerte interne[146]. Enfin, notons que la décision de suspension, comme toute restriction aux droits de la personne concernée, doit être prise au cas par cas et être suffisamment documentée[147]. Elle devrait, par ailleurs, être prise après consultation du délégué à la protection des données si une telle personne a été désignée. Une telle exigence peut poser problème dans l'hypothèse où les fonctions de *Whistleblower Officer* et de DPO sont exercées par la même personne (voy *infra* n° 65).

46. Au demeurant, précisons que la CPVP a également tiré, de la protection des données, le droit du lanceur d'alerte de savoir ce qu'il advient de son signalement ainsi que les suites qui y sont données[148]. La reconnaissance d'un tel droit tend à éviter, selon l'autorité belge, « que l'auteur de la dénonciation n'ait le sentiment (subjectif) que celle-ci n'est pas prise au sérieux et que pour cette raison, il transgresse intentionnellement la confidentialité de sa propre dénonciation, ce qui aura pour conséquence de violer la vie privée des personnes dénoncées et des tiers éventuels »[149]. Déçu du traitement de son signalement, le dénonciateur pourrait, en effet,

---

[145] Groupe 29, Avis n° 1/2006, p. 14. Voy. aussi CEPD, *Decision on internal rules concerning whistleblowing*, préc., art. 14 ; CNIL, *Autorisation unique n° AU-004*, p. 15.

[146] F. Coton et J.-Fr. Henrotte, « Le lanceur d'alerte : une personne concernée par le traitement de ses données à caractère personnel, mais également par son avenir professionnel … », *op. cit.*, p. 78.

[147] CEPD, *Lignes directrices du 18 juillet 2016*, p. 8, pt 20. Voy. aussi CEPD, *Prior-check Opinion on the Whistleblowing Policy of the European Investment Bank*, préc., p. 3

[148] CPVP, *Recommandation n° 01/2006*, p. 6. En faveur de la reconnaissance d'un droit de suivi au lanceur d'alerte, voy. aussi Résolution du Parlement européen du 24 octobre 2017, préc., pt 32 ; T. Devine et T. F. Maassarani, *The Corporate Whistleblower's Survival Guide : a handbook for committing the truth*, *op. cit.*, p. 202.

[149] CPVP, *Recommandation n° 01/2006*, p. 6.

être tenté de le porter en dehors de l'organisation, et notamment dans les médias. Pour les mêmes raisons, la Commission européenne consacre, dans sa Proposition de directive du 23 avril dernier, l'obligation de tenir informé le lanceur d'alerte du suivi apporté à son signalement[150].

b) Le droit d'accès du lanceur d'alerte et des autres personnes concernées

47. L'exercice du droit d'accès, préalable essentiel au droit de rectification, dépend de l'état d'avancement de l'enquête, de la nature des informations demandées et du statut du demandeur (lanceur d'alerte, personne visée par le signalement, tiers impliqué)[151]. L'organisation sollicitée doit évaluer au cas par cas chaque demande et documenter sa réponse.

48. Le Groupe 29 et le CEPD insistent sur le fait que le droit d'accès ne peut permettre d'accéder aux données personnelles d'autrui, sauf si celui-ci a donné son accord exprès. Ainsi, le lanceur d'alerte ne peut pas accéder aux données à caractère personnel de la personne mise en cause ni des tiers, sauf si ces personnes ont donné leur accord[152]. À l'inverse, la personne mise en cause ne peut pas connaître l'identité du dénonciateur ou celle des tiers, ni leurs données personnelles, sauf si ces personnes ont donné leur accord[153]. Comme nous l'avons relevé plus haut, la confidentialité constitue effectivement une garantie majeure dans le domaine du lancement d'alerte.

49. Toujours est-il que l'interdiction de divulguer l'identité des parties impliquées doit pouvoir être levée en cas de fausses déclarations, qu'elles proviennent du lanceur d'alerte, de la personne mise en cause ou de tiers[154]. Partant, la technologie utilisée par l'entreprise ou l'administration (logiciel, plateforme, etc.) devrait toujours permettre, même en cas de

---

[150] Proposition de directive du 23 avril 2018, art. 5.1 d) (signalement interne), 6.2 b), 6.3 et 9.1 b) (signalement externe). Voy. aussi considérant n° 46 (signalement interne) et considérants n^{os} 49-50 (signalement externe).

[151] CEPD, *Lignes directrices du 18 juillet 2016*, p. 9. Voy. aussi CEPD, *Opinion on a notification for Prior Checking regarding the European Ombudsman's Whistleblowing Procedure*, préc., p. 5.

[152] *Idem*. Voy. aussi l'article 9 de la Proposition de directive du 23 avril 2018 qui le prévoit s'agissant du signalement externe.

[153] Voy. not. Groupe 29, Avis n° 1/2006, p. 15 ; CEPD, *Lignes directrices du 18 juillet 2016*, pp. 6-7.

[154] CEPD, *Opinion on a notification for Prior Checking regarding the European Ombudsman's Whistleblowing Procedure*, préc., p. 5. Voy. aussi l'article 9 de la proposition de directive du 23 avril 2018 qui le prévoit s'agissant du signalement externe.

cryptage, de remonter à l'auteur du signalement. Enfin, la levée de l'interdiction devrait être prise après consultation du délégué à la protection des données si une telle personne a été désignée[155]. La même difficulté que celle soulevée plus haut à l'égard de la suspension du droit d'information se pose dans le cas où les fonctions de *Whistleblower Officer* et de DPO sont exercées par la même personne (voy. *infra* n° 65)

c) Le droit d'opposition de la personne visée par la dénonciation

50. Lorsque le traitement de données est nécessaire à l'exécution d'une mission d'intérêt public ou aux fins des intérêts légitimes poursuivis par le responsable du traitement (voy. *supra*, n^os^ 18-21), l'article 21.1 du RGPD énonce que la personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, au traitement des données à caractère personnel la concernant. En l'occurrence, la personne dénoncée est la plus susceptible d'exercer ce droit.

Cependant, l'article 21.1 du RGPD permet au responsable du traitement, à la différence de l'article 14 de la directive 95/46/CE, de continuer de traiter les données s'il « prouve qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, *ou pour la constatation, l'exercice ou la défense de droits en justice* » (nous soulignons). Une telle justification pourra vraisemblablement être invoquée par le responsable du traitement dans le cas qui nous occupe et réduire considérablement de la sorte la portée du droit d'opposition de la personne concernée.

d) Le droit à l'oubli et le droit de rectification du lanceur d'alerte et des autres personnes concernées

51. Le droit à l'effacement, plus connu sous l'expression « droit à l'oubli », permet à la personne concernée de demander au responsable du traitement d'effacer les données à caractère personnel la concernant[156]. La personne mise en cause n'est pas seule à souhaiter exercer ce droit. Pensons en effet à la surmédiatisation dont ont pâti Antoine Deltour et Raphaël Hallet, les deux lanceurs d'alerte de l'affaire *LuxLeaks*, et aux difficultés consécutives qu'ils rencontrent dans leur vie privée et professionnelle.

---

[155] CEPD, *Decision on internal rules concerning whistleblowing*, 14 December 2015, art. 8. Voy. à cet égard l'art. 38.1 du RGPD.

[156] Sur le droit à l'oubli, voy. not. D. DECHENAUD (dir.), *Le droit à l'oubli numérique. Données nominatives – approche comparée*, Bruxelles, Larcier, 2015. Voy. aussi le chapitre du présent ouvrage dédié aux droits des personnes concernées.

52. Les personnes concernées ont enfin le droit de rectifier leurs données, lorsque le traitement de celles-ci dans le cadre du dispositif de signalement n'est pas conforme aux dispositions du RGPD, en raison notamment de la nature incomplète ou inexacte des données[157]. Dans le cas qui nous occupe, il est évident que ce droit ne pourrait être détourné par la personne mise en cause pour procéder, en dehors de la procédure de lancement d'alerte, à la modification du signalement à son encontre.

§ 2. Limitation des droits du lanceur d'alerte et des autres personnes concernées

53. À côté des limitations spécifiques à l'un ou l'autre droit prévues directement dans les dispositions mêmes du RGPD qui consacrent ces droits, l'article 23.1 du RGPD prévoit, de façon transversale, que le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent, par la voie de mesures législatives, limiter la portée des droits de la personne concernée « lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir » un objectif important d'intérêt public général de l'Union ou d'un État membre.

L'article 23 du RGPD vient doublement élargir la possibilité de restreindre les droits reconnus à la personne concernée : d'une part, en allongeant la liste des objectifs importants jugés d'intérêt public général, d'autre part, en faisant de cette liste une liste non exhaustive.

54. Le Groupe 29 estime, à l'aune de l'article 13 de la directive 95/46/CE, que l'exercice des droits de la personne concernée peut être restreint afin d'assurer la protection des droits et des libertés d'autres personnes impliquées dans le système. Parmi les objectifs définis par le RGPD, les objectifs suivants sont également susceptibles de justifier une limitation des droits de la personne concernée dans le cadre de la mise en œuvre d'un dispositif de *whistleblowing* :

– la prévention et la détection de manquements à la déontologie des professions réglementées, ainsi que les enquêtes et les poursuites en la matière (art. 23.1, g) ;
– une mission de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique (art. 23.1, h) ;

[157] Groupe 29, Avis n° 1/2006, p. 15.

– d'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale (art. 23.1., e).

Ainsi que nous l'avons souligné dans la première partie, l'instauration de dispositifs de *whistleblowing* est encouragée dans le but de renforcer l'exécution des politiques publiques et la bonne gouvernance d'entreprise, et de protéger, de la sorte, dans un monde toujours plus globalisé, les intérêts de l'Union et des États membres. La dernière hypothèse (art. 23.1., e) est donc ici particulière prégnante, et cette dernière gagne encore du terrain à la lumière de la proposition de directive du 23 avril dernier[158].

55. Conformément au principe de légalité, soulignons enfin que toute restriction doit être prévue par le droit de l'Union européenne ou le droit national. Une telle restriction est, par exemple, prévue dans le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme par les articles 39.1 et 41.4 de la Quatrième Directive anti-blanchiment[159].

SECTION 8. – La mise en œuvre du principe d'*accountability* par le responsable d'un traitement de données effectué dans le cadre d'un dispositif de signalement

56. Comme pour tout traitement de données, les organisations sont dorénavant tenues, dans la conception et l'application de leur dispositif d'alerte, de mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que les traitements de données induits par le dispositif sont effectués conformément au RGPD[160].

En particulier, il convient de s'interroger sur la nécessité de réaliser une analyse d'impact, au sens de l'article 35 du RGPD, préalablement à la mise

[158] La Proposition de directive du 23 avril 2018 a pour objectif de s'appuyer sur le *whistleblowing* en vue de lutter contre les manquements au droit de l'Union sachant que de tels manquements peuvent porter gravement atteinte à l'intérêt public (*Mémorandum explicatif*, p. 1 et considérant n° 1).

[159] Voy. aussi considérant n° 46 de la Quatrième Directive anti-blanchiment.

[160] Art. 24.1 du RGPD.

en place d'un dispositif de *whistleblowing* (§ 1). Le cas échéant, il convient par ailleurs d'associer le délégué à la protection des données à la conception du dispositif d'alerte. Des réflexions plus prospectives s'imposent à cette occasion (§ 2).

57. Au surplus, mentionnons que le CEPD encourage les organisations, dans la droite ligne du principe d'*accountability*, à tenir compte des implications du dispositif d'alerte du point de vue de la protection des données dès sa conception[161], ce que l'article 25.1 du RGPD prescrit désormais expressément. Avant même que l'adoption du RGPD ne soit envisagée, le Groupe 29 soulignait, du reste, que le droit fondamental à la protection des données à caractère personnel doit « être garanti d'un bout à l'autre du processus »[162], faisant allusion, de la sorte, au principe de protection des données par défaut, dorénavant consacré à l'article 25.2 du RGPD. Depuis lors, la Proposition de directive du 23 avril 2018 est venue confirmer l'importance de ces préoccupations dans le domaine du lancement d'alerte[163].

§ 1. La nécessité de réaliser une analyse d'impact préalablement à la mise en place d'un dispositif de signalement

58. « Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques », l'article 35 du RGPD impose au responsable du traitement d'effectuer, « avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel ».

On peut alors s'interroger : la mise en place d'un dispositif d'alerte requiert-elle d'effectuer préalablement une analyse d'impact ? Les traitements de données personnelles effectués dans le cadre de la mise en œuvre d'un tel dispositif sont-ils susceptibles « d'engendrer un risque élevé pour les droits et libertés des personnes physiques » ?

59. L'article 35.3, a), du RGPD précise qu'une telle analyse est, notamment, requise dans le cas d'une « évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ».

---

[161] CEPD, *Lignes directrices du 18 juillet 2016*, p. 12, pt 39.
[162] Groupe 29, Avis n° 1/2006, p. 20.
[163] Proposition de directive du 23 avril 2018, considérant n° 79.

En l'occurrence, les traitements de données résultant d'un dispositif d'alerte sont susceptibles de relever de ce cas de figure. Les signalements recueillis font, en effet, l'objet d'une évaluation systématique et approfondie sur la base de laquelle l'employeur va décider, en connaissance de cause, des mesures correctives à prendre[164]. Lorsqu'ils concernent une personne physique[165], ils emportent l'analyse d'aspects personnels et peuvent conduire, quand ils s'avèrent fondés, à la prise d'une décision « produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire », telle qu'une sanction disciplinaire.

60. Au demeurant, d'autres traitements que ceux figurant à l'article 35.3 du RGPD peuvent présenter un risque élevé. Parmi les critères d'appréciation identifiés par le Groupe 29, plusieurs critères sont pertinents dans le cas qui nous intéresse. En particulier, il apparaît qu'un traitement de données effectué à l'occasion de la mise en œuvre d'un dispositif d'alerte :

- peut représenter une évaluation ou une notation (critère n° 1) portant notamment sur des aspects concernant la fiabilité ou le comportement de la personne mise en cause ;
- est susceptible d'emporter une décision produisant « des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire » (critère n° 2) ;
- est susceptible de porter sur des données à caractère personnel relatives aux condamnations pénales ou aux infractions (critère n° 4) sachant que le Groupe 29 cite, à titre d'exemple, « les informations sur des auteurs d'infractions que peut détenir un enquêteur privé »[166] ; aussi, un tel traitement est susceptible, à notre sens, de porter sur des données sensibles (au sens commun du terme) dans la mesure où leur violation pourrait avoir des conséquences graves sur la vie professionnelle de la personne mise en cause (risque de stigmatisation, etc.) ;
- porte sur des données concernant des personnes vulnérables (critère n° 7), sachant que les employés sont considérés comme tels, et spécialement les lanceurs d'alerte ;

---

[164] Conseil d'État français, *Le droit d'alerte : signaler, traiter, protéger*, préc., p. 24.

[165] Pour rappel, nous avons vu plus haut que la CNIL encourageait le signalement « d'informations relatives à des faits plutôt qu'à des personnes » (CNIL, *Autorisation unique n° AU-004*, p. 13).

[166] Groupe 29, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679, 17/FR, WP 248 rév.01, adoptées le 4 avril 2017, telles que modifiées et adoptées en dernier lieu le 4 octobre 2017, p. 11.

– emporte l'application de nouvelles solutions organisationnelles (critère n° 8) dès lors que le recours au *whistleblowing* est relativement récent en Europe et est considéré comme sensible en raison des risques de délation qu'il renferme.

Le Groupe 29 est d'avis que le responsable du traitement peut considérer qu'un traitement satisfaisant à deux critères nécessite une analyse d'impact.

61. Ceci étant, le RGPD précise qu'une analyse d'impact n'est, en principe, pas obligatoire lorsque le traitement se fonde sur une base juridique dans le droit de l'Union ou dans le droit de l'État membre (art. 35.10 du RGPD)[167]. Or, la plupart des dispositifs d'alerte se fonde sur une base juridique, soit que cette dernière prévoit une obligation légale de mettre en place un dispositif d'alerte, soit qu'elle rend un tel dispositif nécessaire à l'exécution d'une mission d'intérêt public. Dans ce cas, il faut néanmoins qu'une analyse d'impact relative à la protection des données ait déjà été effectuée dans le cadre d'une analyse d'impact générale réalisée dans le cadre de l'adoption de la base juridique en question[168].

62. En matière de lutte contre le blanchiment et le financement du terrorisme, en Belgique la CPVP n'a pas jugé utile de se prononcer sur le mécanisme de *whistleblowing* prévu par l'avant-projet de loi anti-blanchiment, estimant qu'un tel mécanisme était suffisamment encadré et n'emportait pas de traitements de données à caractère personnel qui impliqueraient des risques très élevés pour les droits des personnes concernées[169]. Il s'ensuit qu'une analyse d'impact ne devrait pas être obligatoire dans le cadre de la mise en œuvre de la loi du 18 septembre 2017, qui transpose en droit belge la Quatrième Directive anti-blanchiment. L'avis de la CPVP a de quoi surprendre, voire inquiéter. Du point de vue de la protection des données, tout dispositif d'alerte présente en effet le même danger, c'est celui de conduire à la sanction de la personne dénoncée et de ternir l'image de l'organisation concernée. D'ailleurs, le CEPD estime, s'agissant des dispositifs d'alerte mis sur pied au sein des institutions et organes de l'Union européenne, que l'opération de traitement qui s'ensuit « est susceptible de présenter des

[167] Le RGPD précise du reste qu'une analyse d'impact n'est pas obligatoire « si le traitement concerne les données à caractère personnel de patients ou de clients par un médecin, un autre professionnel de la santé ou un avocat exerçant à titre individuel » (considérant n° 91 du RGPD). Si nous avons vu que le gestionnaire de plaintes devait être soumis à une obligation de confidentialité, les deux hypothèses ne sont pas comparables dès l'instant où tant le médecin que l'avocat visent la défense des intérêts de la personne concernée, ce qui n'est pas le cas du gestionnaire de plaintes qui doit agir à charge et à décharge.

[168] Art. 35.10, *in fine*, du RGPD.

[169] CPVP, Avis n° 24/2017, p. 4, pt 6.

risques particuliers et est donc soumise au contrôle préalable du Contrôleur européen de la protection des données »[170].

Dans les autres cas, on ne peut que conseiller de faire précéder la mise en place d'un dispositif d'alerte d'une analyse d'impact[171]. En cas de doute sur l'obligation d'effectuer une analyse d'impact, le Groupe 29 recommande en effet d'en effectuer une dès l'instant où une telle analyse constitue un outil efficace de protection des données[172].

63. Enfin, l'analyse d'impact devrait associer, le cas échant, le délégué à la protection des données[173] ainsi que les organes de concertation conformément au droit du travail[174]. Le responsable du traitement sera, du reste, tenu de consulter l'autorité de contrôle préalablement au traitement si l'analyse d'impact effectuée « indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque »[175].

§ 2. L'articulation des fonctions de Data Protection Officer, Compliance Officer et Whistleblower Officer

64. Lorsqu'un délégué à la protection des données doit être désigné[176], la personne désignée à cette fonction devra travailler côte à côte avec le gestionnaire de plaintes au sein du département « *compliance* ». En particulier, le responsable du traitement devra consulter le délégué à la protection des données avant d'instaurer un dispositif d'alerte au sein de son organisation. Vu les implications de la protection des données sur la mise en œuvre du dispositif d'alerte (en particulier, concernant l'exercice des droits de la personne concernée), le délégué à la protection des données sera probablement fréquemment sollicité par le gestionnaire de plaintes.

---

[170] CEPD, *Lignes directrices du 18 juillet 2016*, p. 4, pt 5.

[171] En l'état actuel du droit, Fanny Coton et Jean-François Henrotte recommandent de faire une analyse d'impact pour tout dispositif d'alerte interne (F. Coton et J.-Fr. Henrotte, « Le lanceur d'alerte : une personne concernée par le traitement de ses données à caractère personnel, mais également par son avenir professionnel … », *op. cit.*, p. 73).

[172] Groupe 29, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679, préc., p. 9.

[173] Art. 35.2 du RGPD.

[174] Art. 35.9 du RGPD.

[175] Art. 36.1 du RGPD.

[176] Voy. aussi le chapitre du présent ouvrage dédié à la fonction de délégué à la protection des données. Voy. aussi, D. De Bot, « De DPO of functionaris voor gegevensbescherming in de AVG – gevolgen voor de Belgische praktijk », in *Data Protection & Privacy : le GDPR dans la pratique/ De GDPR in de praktijk* (N. Ragheno dir.), Limal, Anthemis, 2017, pp. 87-103.

65. Les fonctions de délégué à la protection des données et de gestionnaire de plaintes se présentent donc comme de nouvelles figures de la gestion de la conformité (« *compliance management* »), à côté du (*Chief*) *Compliance Officer*[177].

Ces trois fonctions jouissent de garanties légales similaires, notamment en termes de qualification professionnelle, de confidentialité et d'indépendance. Par ailleurs, le *Data Protection Officer*[178], le *Whistleblower Officer*[179] et le *Compliance Officer*[180] assurent leur mission sous la responsabilité de la direction effective de l'organisation au sein de laquelle ils travaillent. La responsabilité du respect des législations respectives – protection des données, législation désignée dans le dispositif d'alerte et législation financière et bancaire[181] – continue de peser sur l'entreprise responsable.

Dans les petites structures, il est d'ailleurs probable que les trois fonctions soient exercées par une même personne, le *Chief Compliance Officer*[182].

66. À la lumière du sujet qui nous occupe, précisons certaines incongruités dont souffre la fonction de *Data Protection Officer* : tantôt agent de l'État, en ce qu'il « facilite » la conformité aux dispositions de la règlementation au sein de l'organisation du responsable du traitement[183]

---

[177] Originaire des pays anglo-saxons, la fonction de « compliance » a émergé dans les années 1990 dans le secteur financier. Elle s'est depuis lors étendue à d'autres domaines, tels que la concurrence et l'environnement. Sur le sujet, voy. not. *Régulation, supervision, compliance* (M.-A. Frison-Roche dir.), Paris, Dalloz, 2017.

[178] Voy. not. K. Rosier, « Délégué à la protection des données : une nouvelle fonction, un métier en devenir », in *Vers un droit européen de la protection des données* (B. Docquir, coord.), Bruxelles, Larcier, 2017, p. 136.

[179] Cela ressort de la logique qui précède la mise en place d'un dispositif d'alerte, qui est d'assurer, pour l'organisation, le respect des législations auxquelles elle est soumise.

[180] Voy. par exemple, en droit belge, l'article 87*bis*, § 1er, alinéa 2, de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers et l'article 1er, 8° du règlement de l'Autorité des services et marchés financiers relatif à l'agrément des *compliance officers* du 20 juillet 2016.

[181] La fonction de *Compliance Officer* s'étend toutefois désormais à d'autres domaines, tels que la concurrence et l'environnement.

[182] La Proposition de directive du 23 avril 2018 l'envisage expressément pour ce qui est des fonctions de *Whistleblower Officer* et de *Compliance Officer* (considérant n° 45). Par ailleurs, l'article 38.6 du RGPD permet au délégué à la protection des données d'exécuter d'autres missions et tâches à la condition que ces dernières n'entrainent pas de conflit d'intérêts.

[183] K. Rosier, « Délégué à la protection des données : une nouvelle fonction, un métier en devenir », *op. cit., p. 136 ;* Groupe 29, Lignes directrices concernant les délégués à la protection des données (DPD), 16/FR WP 243 rev.01, adoptées le 13 décembre 2016, version révisée et adoptée le 5 avril 2017, p. 5.

et fait office de point de contact pour l'autorité de contrôle[184] ; tantôt *Whistleblower Officer* en ce qu'il peut recevoir des personnes concernées leurs préoccupations relatives au traitement de leurs données à caractère personnel et à l'exercice des droits que leur confère le RGPD ; tantôt *Whistleblower*[185] en ce qu'il doit faire « directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant »[186] et doit « coopérer avec l'autorité de contrôle »[187].

Vu la sensibilité de sa fonction, l'article 38.3 du RGPD prévoit d'ailleurs que « le délégué à la protection des données ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions ».

À cet égard, le retour d'expérience sur la mise en œuvre de la fonction de *Compliance Officer* offre sans nul doute des pistes intéressantes[188].

Conclusion

67. La mise en place de dispositifs d'alerte en Europe est particulièrement controversée. Si certains y voient de nombreux avantages, d'autres n'y voient qu'une forme cachée et dangereuse de délation[189]. Toujours est-il que la Proposition de directive déposée par la Commission européenne le 23 avril 2018 laisse augurer une inévitable implémentation. Le respect du droit à la vie privée et à la protection des données représente, à cet égard, un enjeu majeur dans le façonnage d'un véritable *whistleblowing* à l'européenne[190]. Celui-ci se distingue, entre autres du *whistleblowing* à américaine, par le souci de protéger à la fois le lanceur d'alerte et les personnes concernées par l'alerte[191], ainsi que par la préférence accordée dans

[184] Art. 39.1, e), du RGPD.

[185] Dans le cadre de cette obligation, Jeroen Terstegge qualifie *expressis verbis* le délégué à la protection des données de *whistleblower* (J. TERSTEGGE, « EU Watch : Data protection and the new face of privacy compliance », *op. cit.*, p. 40).

[186] Art. 38.3 du RGPD.

[187] Art. 39.1, d), du RGPD.

[188] J. TERSTEGGE, « EU Watch : Data protection and the new face of privacy compliance », *op. cit.*, p. 40.

[189] Sur les avantages et inconvénients du *whistleblowing*, voy. not. V. JUNOD, « Lancer l'alerte : quoi de neuf depuis Guja ? », *op. cit.*, p. 462 et.

[190] Pour rappel, une disposition lui est consacrée (art. 18) dans la proposition de directive du 23 avril 2018.

[191] Voy. not. les articles 15 et 16 de la proposition de directive du 23 avril 2018.

les textes à la confidentialité, en lieu et place de l'anonymat[192], et ce pour des raisons principalement culturelles et historiques. Si la Proposition de directive du 23 avril 2018 entérine avec soin ces spécificités, on regrette néanmoins qu'une plus grande attention n'ait pas été accordée à la problématique de l'anonymat à l'ère d'Internet, lequel représente un outil fondamental de sécurisation des activités en ligne[193].

68. Au-delà du droit européen à la protection des données, la multiplication des dispositifs de signalement et la montée des lanceurs d'alerte témoignent d'un mouvement visant à faire reposer sur la collectivité le respect de l'intérêt général[194]. Une telle évolution constitue un changement sociétal de taille qu'il convient d'endiguer rapidement, par la voie législative[195], afin de ne pas voir resurgir, quand il sera trop tard, les stigmates de la délation.

À ce propos, réjouissons-nous que la Proposition de directive déposée par la Commission européenne ait pris le soin d'établir une série de garde-fous, notamment en obligeant les États membres à prévoir des sanctions effectives, proportionnées et dissuasives, non seulement à l'encontre des auteurs de représailles, mais aussi à l'égard des personnes effectuant délibérément un faux signalement[196]. L'objectif poursuivi par la proposition est bien « de décourager les dénonciations malveillantes et abusives qui affectent l'effectivité et la crédibilité du système tout entier de protection des lanceurs d'alerte, ainsi que de prévenir les dommages injustifiés à la réputation des personnes concernées »[197]. Puisse cet objectif être réalisé.

---

[192] Soulignons toutefois que le signalement anonyme est aussi controversé aux États-Unis (en ce sens, J.-Ph. Foegle, « Les lanceurs d'alerte. Etude comparée France – États-Unis », *La Revue des droits de l'homme [online]*, 2014/6, p. 84).

[193] Voy. spéc. Rapport préc. A/HRC/29/32 ; Déclaration commune de la société civile soumise à la 29e session du Conseil des droits de l'homme des Nations unies, préc.

[194] Voy. not. J.-F. Kerléo, « Qu'est-ce qu'un lanceur d'alerte ? Classification et conceptualisation d'une catégorie juridique insaisissable », in *Les lanceurs d'alerte. Quelle protection juridique ? Quelles limites ?* (M. Disant et D. Pollet-Panoussis dir.), Issy-les-Moulineaux, Lextenso, 2017, p. 11.

[195] Dans le sens d'une intervention législative, voy. not. F. Coton et J.-Fr. Henrotte, « Le lanceur d'alerte : une personne concernée par le traitement de ses données à caractère personnel, mais également par son avenir professionnel … », *op. cit.*, p. 78.

[196] Proposition de directive du 23 avril 2018, art. 17.

[197] Proposition de directive du 23 avril 2018, *Mémorandum explicatif*, p. 13 et considérant n° 78.