RECHTSLEER
DOCTRINE

RECHT EN TECHNOLOGIE/DROIT DE TECHNOLOGIE

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[1]

Olivier Goffard[2]

1. La présente contribution n'engage que l'opinion personnelle de son auteur.
2. Auditeur juridique, juriste d'entreprise.

RÉSUMÉ

Après avoir analysé comment le Sarbanes-Oxley Act requiert des sociétés cotées à la bourse américaine qu'elles mettent en place, moyennant le respect de certaines conditions, des systèmes d'alerte professionnelle destinés à notifier des cas d'irrégularités financières ("whistleblowing lines"), la présente contribution s'attardera sur la position européenne en la matière.

C'est ainsi que nous nous pencherons sur le Document d'Orientation et la Décision d'Autorisation Unique de la Commission Nationale Informatique et Libertés en France, première autorité à s'être prononcée sur le sujet, pour poursuivre par une analyse de l'Avis du Groupe de Travail européen Article 29. Nous terminerons ce tour d'horizon avec la position de la Commission de la Vie Privée belge, matérialisée dans sa Recommandation datée de novembre 2006.

Nous aborderons ensuite les difficultés que les entreprises américaines désireuses de s'installer en Europe rencontrent en tentant de concilier les positions américaine et européenne, pour clôturer par quelques conseils pratiques à destination des sociétés qui souhaitent implémenter un tel mécanisme d'alerte professionnelle.

SAMENVATTING

Deze bijdrage omvat een analyse van de manier waarop de Sarbanes-Oxley Act van Amerikaanse ondernemingen vereist dat zij een professioneel meldsysteem implementeren voor siuaties waarin er vermoedens van financiële onregelmatigheden bestaan ("whistleblowing lines"). Na deze analyse behandelen we het Europese standpunt; i.e. de standpunten van de Franse Commission Nationale Informatique et Libertés (eerste autoriteit die zich heeft uitgesproken over dit onderwerp in een Orientatiedocument en via de Eenmalige Autorisatie Beslissing) en van de Europese Werkgroep Artikel 29. Wij sluiten dit overzicht af met de Aanbeveling die de Commissie voor de Bescherming van de Persoonlijke Levensfeer in november 2006 in dit domein genomen heeft.

Vervolgens gaan we in op de moeilijkheden die Amerikaanse ondernemingen die zich in Europa willen installeren ondervinden als zij zowel aan de Amerikaanse als aan de Europese bepalingen moeten voldoen. Ten slotte sommen we een reeks aanbevelingen op voor de ondernemingen die zo'n professioneel meldsysteem in Europa willen installeren.

INTRODUCTION

1. Dans la période précédant les retentissants scandales financiers[3] des dernières années, les attitudes envers la pratique du *whistleblowing* étaient diamétralement opposées. Ainsi, certains, dont le guru du management Peter Drucker, s'insurgeaient contre cette technique consistant selon eux à mordre la main de celui qui vous nourrit[4]. D'autres, par contre, considéraient les *whistleblowers* comme les gardiens de la responsabilité publique qui permettent d'apporter des changements fondamentaux à l'organisation.

Le concept de *whistleblowing* n'est certainement pas neuf mais a reçu une attention accrue ces derniers temps. Dans les années 1960, peu d'entreprises se montraient tolérantes à cet égard estimant plutôt que leurs employés devaient être loyaux envers elles à tout prix. Dans le courant des années 1970, la définition donnée était alors *"an act of a man or a woman who, believing that the public interest overrides the interest of the organization he serves, blows the whistle that the organization is involved in corrupt, illegal, fraudulent or harmful activity"*[5]. C'est également à cette période qu'apparurent aux États-Unis les premières lois vraiment protectrices des travailleurs qui prévoyaient l'interdiction de sanctionner un travailleur reportant des cas de dysfonctionnements[6]. Les violations reportées devaient cependant en général être limitées aux matières de sécurité et de santé publique.

2. C'est surtout le célèbre Sarbanes-Oxley Act de 2002 (ci-après "SOX Act")[7] qui aura un impact considérable dans le domaine du *whistleblowing*. Il impose en effet à toute entreprise publique américaine ainsi qu'à toute entreprise cotée sur le marché américain de même qu'à leurs filiales – même si celles-ci ne sont pas situées sur le territoire américain – de mettre en place un système d'alerte professionnelle permettant à leurs employés de rapporter toute malversation dans les domaines comptables, de l'audit ou du reporting financier.

En France, où la question de la légalité de ces systèmes d'alerte professionnelle (ligne téléphonique, e-mail, mécanisme internet, fax, …) s'est la première posée, les réactions initiales furent d'abord négatives. Ainsi McDonald et CEAC (Exide Technologies), deux compagnies américaines présentes en France, ont-elles demandé en juin 2005 à la CNIL[8] d'approuver leur projet d'installer des lignes téléphoniques éthiques afin de se mettre en conformité avec une disposition du SOX Act. La CNIL ne donna pas droit à ces demandes considérant entre autre ces systèmes comme contraires à la législation relative à la protection de la vie privée et susceptibles de causer une angoisse excessive aux employés mis en cause au travers d'accusations infondées. Elle estima en substance que ces systèmes d'alerte professionnelle étaient disproportionnés par rapport au but à atteindre étant donné que ces compagnies disposaient déjà d'autres mécanismes anti-fraude moins intrusifs et moins susceptibles d'abus (ex. training, audit, voie hiérarchique, cours et tribunaux).

3. La présente contribution, sans vouloir apporter une vue exhaustive sur le caractère légal *sensu lato* des systèmes d'alerte professionnelle, s'interroge sur leur compatibilité avec les normes de protection de la vie privée. Nous nous attarderons donc successivement sur la situation aux États-Unis (le SOX Act), en Europe (l'Avis du G29), en France (le Document d'Orientation et la Décision d'Autorisation Unique de la CNIL) pour terminer avec la récente Recommandation de la Commission de la Vie Privée belge. Après avoir brièvement adressé certaines normes de *corporate governance* recommandant la mise en place de tels systèmes d'alerte professionnelle, nous clôturerons notre analyse par quelques conseils pratiques pour les entreprises qui envisagent d'implémenter ce genre de dispositif d'alerte.

§ 1. LE SARBANES-OXLEY ACT[9]

I. Introduction

4. Le SOX Act a été adopté par le président Bush dans un souci de protection des investisseurs suite aux scandales financiers Enron et Tyco International. L'objectif poursuivi par ce texte est en effet d'améliorer l'exactitude et la fiabilité des déclarations publiques[10] faites par les entreprises améri-

3. Affaires *Enron*, *WorldCom*, *Parmalat* pour ne citer que les plus importantes.
4. L. RAVUSHANKAR, "Encouraging Internal Whistleblowing in Organizations", Santa Clara Universtity, disponible à l'adresse http://www.scu.edu/ethics/publications/submitted/whistleblowing.html.
5. N. RONGINE, "Toward a coherent legal response to the public policy dilemna posed by whistleblowing", 23 Am Bus LJ, p. 281.
6. Civil Service Reform Act (1978), False Claims Act et Whistleblower Protection Act (1989). Le tableau disponible à l'adresse suivante reprend un synoptique des possibilités de *"whistleblowing"* prévues par les lois fédérales américaines: http://whistleblowerlaws.com/statutes.htm.
7. 18 USC 1514A, 30 juillet 2002, Titre VIII, "Corporate and Criminal Fraud Accountability Act of 2002".
8. Commission Nationale de l'Informatique et des Libertés, http://www.cnil.fr/.
9. Pour une analyse détaillée des dispositions du SOX Act en matière de *whistleblowing*, nous renvoyons le lecteur à l'excellent article de V. Watnick, "Whistleblower protections under the Sarbanes-Oxley Act: A Primer and a Critique", http://law.bepress.com/cgi/viewcontent.cgi?article=8640&context=expresso ainsi qu'à D. Smith et K. Baker, "Sarbanes-Oxley: Better Listen to the Whistleblower", http://library.findlaw.com /2003/Dec/29/133229.html.
10. Traduction du terme anglais *"corporate disclosure"*.

caines en application des *securities laws*[11] et sur lesquelles se basent les actionnaires et les investisseurs pour juger de la "santé financière" de l'entreprise.

Les dispositions de cette loi qui nous intéressent s'appliquent aux sociétés ayant émis des titres au public cotés auprès de la SEC ou qui doivent introduire un rapport auprès de la SEC en vertu du Securities Exchange Act de 1934.

II. La mise en place d'un mécanisme de *whistleblowing* et la protection contre les représailles

Les apports principaux de cette loi en matière de *"whistleblowing"* se trouvent dans ses Sections 301 et 806.

a) Section 301

4. Cette section exige des comités d'audit qu'ils mettent en place un mécanisme qui permet:

– la réception, la rétention et le traitement de plaintes reçues par l'émetteur de titres concernant des irrégularités de nature comptable, touchant au contrôle interne des comptes ou à l'audit; et
– la soumission anonyme par les employés de l'émetteur des titres de notifications ayant trait à des pratiques comptables ou d'audit questionnables[12].

Le champ d'application des systèmes d'alerte professionnelle prévus par la Section 301 doit donc nécessairement être limité au domaine financier *sensu lato*. Il s'agit de ce que nous appellerons l'interprétation limitative des dispositions du SOX Act en matière de *whistleblowing*.

Le SOX Act ne prévoit aucune condition spécifique quant à la procédure à suivre pour émettre ces signalements pour autant toutefois qu'au moins un processus anonyme soit à disposition des employés pour ce faire.

b) Section 806

5. La Section 806 prévoit une protection spécifique pour les employés de sociétés cotées qui communiquent des éléments de fraude par le biais d'un mécanisme de type "Section 301". Elle introduit en effet dans l'arsenal législatif américain une nouvelle action civile tendant à assurer la protection de ces employés contre de possibles représailles.

Pour ce faire, elle rend illégal le fait de renvoyer, suspendre, menacer, harceler ou discriminer un *whistleblower* du simple fait qu'il aurait fourni des informations ou donné son soutien dans une enquête portant sur des agissements qu'il a pu raisonnablement considérer comme constituant une violation des règles de la SEC ou de toute loi fédérale poursuivant comme objectif la protection des actionnaires contre la fraude.

Nous constaterons qu'alors que la Section 301 se limite aux domaines financiers, comptables et d'audit, la Section 806 est quant à elle moins restrictive et vise la violation de toute loi fédérale tendant à éviter que des actionnaires soient victimes de fraude. Cela donna lieu à de nombreuses dérives, des entreprises interprétant cette clause comme leur permettant de mettre sur pied un mécanisme de *whistleblowing* au champ d'application plus étendu que le domaine financier. Il s'agit de ce que nous appellerons, *ceteris paribus,* l'interprétation extensive des dispositions du SOX Act en matière de *whistleblowing*.

Afin de pouvoir bénéficier de la protection conférée par le SOX Act, le *whistleblower* ne peut toutefois fournir ces informations qu' (i) à tout superviseur ou toute personne travaillant pour l'employeur qui a autorité pour enquêter, découvrir ou stopper le méfait, (ii) auprès d'une agence chargée de l'application des lois et régulations fédérales ou enfin (iii) à un membre du Congrés ou un de ses comités.

Cette interdiction de représailles s'applique non seulement en faveur des employés de la société visée mais aussi à ses contractants, sous-contractants et agents[13].

c) Procédure et sanctions[14]

6. Un employé estimant que l'interdiction de représailles à son encontre a été violée peut introduire une plainte auprès du *Secretary of Labor* dans les 90 jours de la violation alléguée. Ce dernier a délégué à la *Occupational Safety and Health Administration* (OHSA) la compétence de faire appliquer les dispositions du SOX Act relatives au *whistleblowing*. Cette administration a émis un document détaillant la procédure à suivre pour traiter ces affaires[15]. Notons que si le *Secretary of Labor* n'émet pas un rapport dans les 180 jours suivant l'introduction de la plainte, et qu'il n'est pas prouvé que ce délai est dû à la mauvaise foi du plaignant,

11. Pour plus d'informations à cet égard, nous renvoyons au site internet de la *U.S. Securities and Exchange Commission* (SEC) qui reprend un aperçu des législations applicables en cette matière ainsi que des déclarations publiques requises: http://www.sec.gov/about/laws.shtml.
12. Section 301 (4) Sarbanes-Oxley Act.
13. Nouvelle Section 1514A du Titre 18, Chapitre 73, a) du United States Code, introduite par la Section 806 du Sarbanes-Oxley Act.
14. Pour une analyse plus détaillée des sanctions prévues par le SOX Act en matière de *whistleblowing*, nous renvoyons le lecteur à J. Lechner et P. Sisco, "Sarbanes-Oxley Criminal Whistleblower Provisions and the *Workplace*: More Than Just Securities Fraud", *The Florida Bar Journal* 2006, vol. 80, p. 85.
15. 29 CFR Part 1980, 69 Fed. Reg. 52104 (24 août 2004).

l'employé pourra introduire une action contre l'employeur devant une cour fédérale de district[16].

7. L'employé obtenant gain de cause aura droit à toute réparation nécessaire afin de le remettre dans la même situation que celle dans laquelle il se trouvait avant les représailles. Cela sous-entend l'obtention de sa réintégration avec tous les droits de séniorité ainsi que les salaires en retard (avec intérêts), mais aussi la réparation de dommages spéciaux tels que les frais d'avocats, d'experts ou d'autres coûts liés au litige[17].

La Section 1107, dernière du SOX Act, précise que toute personne qui prend des actions de représailles en violation des Section 301 et 806 pourra se voir condamner à payer une amende et/ou à purger une peine d'emprisonnement pouvant aller jusque 10 ans[18].

§ 2. L'Avis du Groupe de Travail "Article 29"[19]

Introduction

8. Cette situation difficile où une entreprise ou filiale d'une entreprise américaine située sur territoire européen se trouvait entre le marteau et l'enclume, c'est-à-dire entre l'obligation d'instaurer un système d'alerte professionnelle pour satisfaire aux exigences du SOX Act et la non-compatibilité de ce même système avec les législations européennes protectrices de la vie privée entraîna une réflexion de fond menée par le Groupe de Travail "Article 29" sur la protection des données[20]. Celui-ci a émis début 2006 un avis comprenant des lignes directrices à suivre par les entreprises qui souhaitent mettre en place un système d'alerte professionnelle dans les domaines[21] financier, comptable, bancaire et de blanchiment d'argent (ci-après "l'Avis")[22].

Un des objectifs poursuivis par ce document est d'expliquer aux compagnies listées aux États-Unis et installées en Europe comment respecter les exigences du SOX Act d'une manière compatible avec les exigences européennes en matière de vie privée.

I. Principes à respecter pour mettre en place un système d'alerte professionnelle

9. L'Avis n'autorise la mise en place d'un système d'alerte professionnelle que moyennant le respect d'un certain nombre de principes. Le respect de ces principes devrait apporter une garantie raisonnable et suffisante pour que les systèmes d'alerte professionnelle mis en place assurent une protection adéquate de la vie privée des personnes qui les utilisent.

a) Principe de légitimité

10. Etant donné que la quasi-totalité des procédures d'alerte professionnelle implique le traitement de données à caractère personnel, elles seront donc sujettes aux législations relatives à la protection de la vie privée[23].

Tout traitement de données à caractère personnel n'est autorisé qu'à condition qu'il soit légitime. Il n'en sera pas autrement pour les systèmes d'alerte professionnelle qui devront dès lors présenter eux aussi un caractère légitime. Il s'agit là d'une référence à l'article 7 de la Directive sur la vie privée[24] selon lequel *"les États membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si*

16. Nouvelle Section 1514A du Titre 18, Chapitre 73, b) du United States Code, introduite par la Section 806 du Sarbanes-Oxley Act. Cela peut cependant créer un conflit de décisions car l'OHSA ne sera pas automatiquement déchargé de l'affaire en cas d'introduction d'une plainte devant la cour de district; *cf.* T. Dworkin, "SOX and Whistleblowing", 8 novembre 2006, p. 9 publié par l'université du Michigan et disponible à l'adresse http://www.michiganlawreview.org/symposium/docs/dworkin.pdf.
17. Nouvelle Section 1514A du Titre 18, Chapitre 73, b) du United States Code, introduite par la Section 806 du Sarbanes-Oxley Act.
18. Section 1107 du Sarbanes-Oxley Act.
19. Cet Avis a déjà eu l'occasion d'être commenté par R. Perray et M. Gaudemet, "Requirements of the French Data Protection Authority on Whistleblowing to be applicable throughout the European Union", 20 mars 2006, disponible sur http://www.droit-technologie.org/1_2.asp?actu_id=1166.
20. Ce groupe de travail a été établi sur base de l'art. 29 de la Directive 95/46/CE en tant qu'organe consultatif européen sur la protection des données et de la vie privée.
21. Il apparaît que des discussions sont en cours afin d'étendre le champ d'application de cet Avis à d'autres domaines tels que les ressources humaines, la santé et la sécurité publique; ce qui le distingue de l'avis de la CNIL qui a un champ d'application plus restreint.
22. Avis 1/2006 relatif à l'application des règles de l'Union européenne en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière, 1er février 2006.
23. Avis 1/2006 du Groupe, art. 29, Section III, p. 6.
24. 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, *J.O.C.E.* 23 novembre 1995, n° L. 281, p. 31.

il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis (...), ou si il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévale pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée".

Le Groupe de Travail interprète cet article comme signifiant qu'un système d'alerte professionnelle ne sera légitime que si

– il est mis en place afin de respecter une obligation comprise dans une loi européenne[25]. Selon cette première interprétation, le SOX Act ne constitue donc pas une justification suffisante pour instaurer de tels mécanismes. L'Avis ajoute qu'une obligation légale telle que celle requise peut par contre *prima facie* être trouvée dans le domaine bancaire et en matière de lutte contre la corruption;
– les obligations légales extra-européennes sur lesquelles ce système repose requièrent sa mise en place afin de réaliser l'intérêt légitime poursuivi par le responsable du traitement[26]. Le Groupe de Travail est ainsi d'avis que l'objectif de garantie de la sécurité financière sur les marchés financiers poursuivi par le SOX Act peut être considéré comme un de ces intérêts légitimes. Il considère en effet que *"dans les pays de l'UE qui ne prévoient pas d'obligation légale spécifique d'instaurer des dispositifs d'alerte professionnelle dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit et de la lutte contre la corruption et la criminalité bancaire et financière, les responsables du traitement des données ont toujours un intérêt légitime à mettre en place de tels mécanismes internes dans ces domaines"*[27].

Nous pouvons par conséquent déduire de cette position que seule l'interprétation limitative du SOX Act peut servir de justificatif à la mise en place d'un système d'alerte professionnelle en Europe. Seuls les mécanismes de *whistleblowing* dans les domaines financier, comptable et d'audit seront donc considérés comme légitimes au contraire de ceux permettant de notifier toute violation d'une loi fédérale poursuivant comme objectif l'intérêt de l'actionnaire.

b) Principes de qualité des données, de proportionnalité et de complémentarité

1. Les principes

11. Les responsables des systèmes d'alerte professionnelle doivent s'assurer que le mécanisme mis en place respecte les principes de qualité des données et de proportionnalité issus de l'article 6 de la Directive vie privée. Selon cet article, *"les États membres prévoient que les données à caractère personnel doivent être a) traitées loyalement et licitement; b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités; c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement; d) exactes et, si nécessaire, mises à jour; e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement."*. Cela signifie donc que les sociétés implémentant ce genre de système ne peuvent collecter par ce biais que les données qui ont un rapport direct avec les faits allégués et qui rentrent dans son champ d'application tel qu'initialement défini.

L'Avis recommande ensuite que ce genre de mécanisme ne soit adopté qu'en complément des autres mécanismes de notification classiques tels l'audit interne, la voie hiérarchique, le département RH… *"Il doit donc apparaître comme le complément, et non le substitut, de la gestion interne."*[28]. Il s'agit donc du principe de complémentarité des systèmes d'alerte professionnelle.

2. Les conséquences

12. Ces trois principes se matérialisent en cinq conséquences que les sociétés doivent prendre en compte lors de la mise en place du mécanisme[29]:

– la société doit tout d'abord examiner s'il est opportun de circonscrire le nombre de personnes en droit d'utiliser le mécanisme.
  L'objectif est clairement de limiter les abus et le nombre de notifications erronées ou calomnieuses. Il revient aux autorités nationales de décider si les limitations mises en place sont opportunes. Selon toute vraisemblance, l'accès à ces systèmes doit ainsi être limité aux employés ayant accès à des informations bancaires, comptables, d'audit ou financières;

25. Avis 1/2006 du Groupe, art. 29, Section IV, 1, i, p. 7.
26. Avis 1/2006 du Groupe, art. 29, Section IV, 1, ii, p. 8.
27. Avis 1/2006 du Groupe, art. 29, Section IV, 1, ii, p. 9.
28. Avis 1/2006 du Groupe, art. 29, Section III, p. 6.
29. Avis 1/2006 du Groupe, art. 29, Section IV, 2, i) à v), pp. 10 et s.

– la société doit aussi examiner s'il est opportun de limiter le nombre de personnes susceptibles d'être mises en cause par le biais du mécanisme.
Il adviendra de nouveau aux autorités nationales de décider si les limitations mises en place sont opportunes;
– différence notable avec le SOX Act, l'Avis recommande de donner préférence aux signalements confidentiels dont l'auteur est identifié.
Les signalements anonymes n'ont donc pas reçu la faveur du Groupe de Travail. Il justifie sa position en argumentant que préconiser l'anonymat ne serait pas en ligne avec la nécessaire condition de loyauté que de tels systèmes doivent respecter.
Il va cependant de soi que même si l'employé utilisant le système est tenu de divulguer son identité, il est par contre évident que le mécanisme en place doit assurer la confidentialité des informations reçues.
Nous observerons qu'il ne s'agit pas d'une interdiction formelle des alertes anonymes, celles-ci restant permises de manière exceptionnelle aussi longtemps que cette anonymisation n'est pas obligatoire, que l'anonymat n'est pas préconisé comme étant la règle habituelle et qu'aucune publicité ne soit faite autour de cette possibilité d'anonymisation du signalement;
– les données collectées doivent se limiter aux faits ayant un rapport avec l'objectif général du système, c'est-à-dire garantir le bon gouvernement d'entreprise.
Ainsi, les sociétés doivent définir le type d'informations à divulguer, celles-ci devant toujours se situer dans les domaines financiers et d'audit.
Si des faits sont dénoncés qui ne se rapportent pas à ces domaines, ils pourront toutefois être communiqués aux personnes compétentes mais uniquement si les intérêts vitaux de la personne concernée par ces données sont en jeux ou si, en vertu du droit national, une obligation légale de communiquer ces informations aux pouvoirs publics ou aux autorités de poursuite compétentes existe. Si ces conditions ne sont pas remplies, les données devront être immédiatement détruites;
– les données traitées par le système d'alerte ne peuvent être conservées que pour une durée limitée et doivent être rapidement supprimées, généralement dans un délai de deux mois à compter de l'aboutissement de l'enquête diligentée sur base de ces données sauf si une procédure judiciaire ou disciplinaire est en cours.

c) Principe d'information[30]

13. Ce principe découle de l'article 10 de la Directive vie privée selon lequel: *"Les États membres prévoient que le responsable du traitement doit fournir à la personne auprès de laquelle il collecte des données la concernant: a) l'identité du responsable du traitement; b) les finalités du traitement; c) toute information supplémentaire telle que: les destinataires ou les catégories de destinataires des données, le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences éventuelles d'un défaut de réponse, l'existence de droits d'accès aux données la concernant et de rectification de ces données, dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données"*.

En application de cet article, la société devra informer ses employés susceptibles d'utiliser ou d'être mis en cause par ce mécanisme de l'existence, la finalité et le fonctionnement du mécanisme ainsi que des droits d'accès, de rectification et de suppression des données enregistrées.

Il faudra de même communiquer le fait que l'identité de la personne désirant faire usage du système restera confidentielle, que tout abus pourra entraîner des sanctions et que tout signalement émis de bonne foi ne sera passible d'aucune sanction s'il se révèle comme erroné.

Il nous semble que la méthode la plus efficace afin de communiquer ces informations aux employés est de les reprendre dans une *"policy"* approuvée par l'organe de gestion de la société et dont l'existence a été communiquée à l'ensemble du personnel.

La personne mise en cause doit en outre être informée le plus rapidement possible de l'alerte, sauf toutefois s'il existe un risque sérieux que cette notification ne compromette la capacité de la société d'enquêter efficacement sur les faits allégués ou de collecter les preuves nécessaires. Dans ce cas, l'information peut être retardée aussi longtemps que ce risque existe.

d) Droits de la personne mise en cause[31]

14. À côté des dispositions classiques de protection de l'utilisateur du mécanisme, l'Avis pointe le fait que la personne mise en cause doit elle aussi bénéficier des protections conférées par la Directive vie privée et par les législations nationales.

Cette protection consiste plus particulièrement en un droit de la personne mise en cause d'être informée de manière précise et rapide ainsi que, le cas échéant, dans son droit de demander accès, de modifier ou de faire supprimer les données à caractère personnel enregistrées qui la concernent[32].

30. Avis 1/2006 du Groupe, art. 29, Section IV, 3, p. 13.
31. Avis 1/2006 du Groupe, art. 29, Section IV, 4, p. 14.
32. Art. 12 Directive vie privée.

La personne concernée ne pourra toutefois en aucun cas obtenir des informations sur l'identité de la personne ayant effectué le signalement par le biais de l'exercice de son droit d'accès. Ce principe connaît toutefois une exception lorsque la dénonciation a été faite à des fins malveillantes.

e) Principe de sécurité des opérations de traitement[33]

15. En vertu de ce principe tiré de l'article 17 § 1 de la Directive vie privée, la société responsable de la gestion du système d'alerte professionnelle doit mettre en place des mesures de sécurité appropriées pour protéger les données collectées, diffusées ou conservées, contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé. Ces mesures doivent offrir un niveau de sécurité approprié au regard des risques présentés par le traitement et par la nature des données à protéger.

Rappelons que les mesures techniques adoptées, outre l'objectif sécuritaire précité, doivent aussi garantir que l'identité des dénonciateurs reste confidentielle.

f) Gestion des dispositifs d'alerte professionnelle[34]

1. Spécialisation du recueil et du traitement des alertes

16. L'Avis recommande que le système soit géré par des personnes spécialement entraînées et dédicacées à cet effet et qui sont soumises à une obligation (contractuelle) de confidentialité. De surcroît, le système doit faire partie d'un département indépendant séparé qui sera en charge de traiter les notifications et de conduire les enquêtes. Il reviendra aux personnes de ce département de vérifier si les conditions de confidentialité et de sécurité dont mention *supra* ont bien été respectées.

2. Sous-traitance

17. Si une entreprise décide de sous-traiter la gestion de son système d'alerte à une partie tierce, elle devra d'abord s'assurer que les conditions minimales de confidentialité et de sécurité prémentionnées seront respectées par le prestataire. En effet, en vertu de l'article 17 § 2 de la Directive vie privée: *"Les États membres prévoient que le responsable du traitement doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer et qu'il doit veiller au respect de ces mesures."*

Le contrat de sous-traitance devra en outre comprendre les dispositions nécessaires en vue d'assurer que l'ensemble des conditions énumérées dans l'Avis seront effectivement respectées. En ligne avec les principes classiques d'*outsourcing*, l'entreprise restera la partie ultimement responsable des actions réalisées par le sous-traitant ainsi que de la manière dont il respecte les principes fixés dans l'Avis, quitte à se retourner contre lui en vertu du contrat qu'ils ont conclu.

3. Transfert intragroupe d'informations

18. Enfin, le Groupe de Travail est d'avis qu'en cas de signalement survenant dans une entité spécifique d'un groupe d'entreprises, le traitement de ce signalement doit s'effectuer au niveau local. L'objectif est donc d'éviter que les données à caractère personnel ne soient communiquées à trop d'intervenants, éventuellement localisés dans un autre pays que celui d'où provient l'alerte. Toutefois, les informations reçues peuvent être communiquées au sein du groupe si cela est nécessaire aux fins de l'enquête ou découle de la composition du groupe, c'est-à-dire en fonction de la nature sérieuse des faits allégués ainsi que de l'organisation même de la société.

g) Transfert vers les pays tiers[35,36]

19. Nous mentionnerons uniquement le fait qu'en cas de transfert de données vers des pays situés hors de l'Union européenne, il sera nécessaire de respecter les articles 25 et 26 de la Directive vie privée. Selon ces articles, des données à caractère personnel ne peuvent être transférées que vers des pays qui assurent une protection des données correspondant à celle assurée sur le territoire de l'Union européenne. Il faut donc se demander si le niveau de protection assuré dans ces pays tiers est adéquat. La Commission européenne a publié à cet égard une liste évolutive des pays tiers considérés comme présentant un niveau de protection jugé adéquat[37].

33. Avis 2006/1 du Groupe, art. 29, Section IV, 5, p. 15.
34. Avis 2006/1 du Groupe, art. 29, Section IV, 6, p. 16.
35. Avis 2006/1 Groupe, art. 29, Section IV, 7, p. 18.
36. Pour plus de détails quant aux principes en matière de transfert de données à caractère personnel vers des pays situés hors de l'Union européenne, nous renvoyons le lecteur au site de la Commission de la Vie Privée, http://www.privacycommission.be/nieuw%2029-8-2002/FR_transfer%20buiten%20EU.htm.
37. http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_fr.htm.

Notons que même si le niveau de protection n'est pas adéquat, il sera quand même exceptionnellement permis de transférer les données dans ces pays si:

- la personne visée a donné son consentement indubitable;
- le transfert est nécessaire à l'exécution d'un contrat auquel le sujet est partie;
- le responsable du traitement assure un niveau de protection adéquat par voie contractuelle[38];
- le groupe d'entreprises auquel appartiennent les deux sociétés a adopté des règles d'entreprise contraignantes relatives à la protection de données à caractère personnel; et enfin
- dans le cas d'une société américaine, celle-ci a adhéré au principe des *"safe harbors"*[39].

h) Respect des obligations de notification[40]

20. Les sociétés mettant en place un système d'alerte professionnelle devront enfin se conformer aux obligations nationales de notification ou de vérification préalable mises en place par leurs autorités nationales respectives.

§ 3. Le Document d'Orientation et la Décision d'Autorisation Unique de la CNIL

Introduction

21. La CNIL s'est rendue compte que la position qu'elle a défendue dans les affaires McDonald et CEAC était source d'insécurité juridique pour les entreprises américaines ou les filiales de telles entreprises installées en France. Elle a par conséquent revu sa position et a émis fin 2005 un Document d'Orientation[41] et une Décision d'Autorisation Unique[42] fixant les conditions que les systèmes de *whistleblowing* doivent respecter pour être autorisés en France.

Dans ces documents, la CNIL justifie ses décisions dans les affaires Mc Donald et CEAC par le fait que les droits des personnes mises en cause n'étaient pas garantis au regard des règles relatives à la protection des données à caractère personnel. Il ne s'agissait donc pas d'une interdiction de principe des systèmes d'alerte professionnelle mais plutôt de décisions visant à s'assurer que certains garde-fous minimums soient en place.

I. Applicabilité de la loi informatique et libertés

22. S'ils s'appuient sur le traitement de données à caractère personnel, les dispositifs d'alerte professionnelle seront soumis à la loi informatique et libertés[43], et ce que le traitement soit réalisé sur support informatique ou papier. De surcroît, lorsqu'ils sont automatisés, ils devront faire l'objet d'une autorisation préalable de la CNIL[44]. Or, de manière pragmatique, nous pouvons estimer que la quasi-totalité[45] des systèmes d'alerte professionnelle actuels prévoient le traitement de données à caractère personnel et sont de surcroît par nature automatiques, requérant par conséquent l'autorisation de la CNIL afin d'être mis en œuvre.

II. Principes à respecter pour établir un système d'alerte professionnelle en France

23. Les dispositions du Document d'Orientation et de l'Autorisation Unique se trouvent à l'origine de l'Avis du Groupe Article 29. Nous allons dès lors retrouver beaucoup de similitudes entre ces textes. Les entreprises désirant mettre en place un système d'alerte professionnelle devront respecter différents principes afin de se mettre en conformité avec les dispositions de la loi informatique et libertés.

38. Des contrats-types ont été mis à disposition du public par la Commission européenne, *cf.* note de bas de page 67.
39. Le *U.S. Department of Commerce* a développé en consultation avec la Commission européenne le principe des *"safe harbors"* ainsi qu'un site web destiné à fournir des informations aux entreprises américaines: http://www.export.gov/safeharbor/.
40. Avis 2006/1 Groupe, art. 29, Section IV, 8, p. 19.
41. Document d'Orientation adopté par la Commission le 10 novembre 2005 pour la mise en œuvre de dispositifs d'alerte professionnelle conformes à la loi du 6 janvier 1978 modifiée en août 2004, relative à l'informatique, aux fichiers et aux libertés.
42. Autorisation Unique n° AU-004, Délibération n° 2005-305 du 8 décembre 2005 portant autorisation unique de traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle, *J.O.* n° 3 du 4 janvier 2006.
43. Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *J.O.* 7 août 2004.
44. Art. 25-4° loi informatique et libertés selon lequel *"Sont mis en œuvre après autorisation de la Commission nationale de l'informatique et des libertés les traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire."*
45. Nous estimons en effet que des mécanismes d'alerte professionnelle uniquement basés sur l'envoi de courrier physique ou sur le dépôt de signalements dans une boîte aux lettres physiques ne sont quasiment plus utilisés à notre époque.

a) Document d'Orientation[46]

1. Principes de complémentarité, de finalité (légitimité) et d'usage facultatif[47]

1.1. Complémentarité

24. Le principe de complémentarité ne requiert aucun commentaire. Il s'agit de ne mettre en place un tel système que comme mode complémentaire à côté d'autres processus de gouvernance déjà bien structurés tels la voie hiérarchique, le rapport des commissaires, le département RH, … Un système d'alerte n'est justifié que si les canaux traditionnels ne fonctionnent pas dans certaines circonstances.

1.2. Application restreinte (légitimité)

25. Le concept d'application restreinte, corollaire logique du principe de complémentarité, tend à éviter les systèmes d'alerte à portée générale. Ne seront donc autorisés par la CNIL que les systèmes d'alerte professionnelle légitimes au sens de l'article 7 de la loi informatique et libertés[48], c'est-à-dire ceux qui:

(i) sont mis en œuvre afin de répondre à une obligation législative ou réglementaire de droit français visant à l'établissement de procédures de contrôle interne dans des domaines précisément définis, soit financier, comptable, bancaire et de lutte contre la corruption[49];

(ii) sont par exemple mis en œuvre par les sociétés françaises cotées aux États-Unis dans les domaines comptables et de l'audit en application de la Section 301 du SOX Act. Dans ce cas, le système sera autorisé car poursuivant la réalisation de l'intérêt légitime du responsable du traitement, c'est-à-dire éviter que les actionnaires ne soient victimes de fraude et renforcer la sécurité des marchés financiers. La présence d'un tel système sera ainsi considéré comme légitime s'il est nécessaire afin de poursuivre l'intérêt légitime recherché par le responsable du traitement, sans préjudice toutefois de l'intérêt ou des droits et libertés fondamentales du sujet concerné.

Toutefois, notons que l'article 3 de l'Autorisation Unique permet aussi qu'un dispositif d'alerte initialement implémenté pour recevoir des alertes financières *sensu lato* puisse prendre en compte des alertes qui ne rentrent pas sous ce champ d'application originel si l'intérêt vital de l'entreprise ou l'intégrité physique ou morale de ses employés est en jeu. Il en sera ainsi des alertes relatives au harcèlement, aux discriminations, aux délits d'initié, aux conflits d'intérêts, aux atteintes graves à l'environnement ou à la santé publique, aux risques informatiques graves, à la divulgation d'un secret de fabrique[50].

Quant aux alertes ne présentant pas ce niveau de gravité et ne rentrant pas dans le champ d'application normal du dispositif, leur émetteur sera informé et orienté vers le service compétent. Les données y relatives devront être de suite détruites ou archivées.

26. En conclusion, les systèmes d'alerte professionnelle mis en place dans les domaines financier, comptable, bancaire et de lutte contre la corruption, présumés légitimes, pourront donc bénéficier du système de l'Autorisation Unique (*cf. infra*), alors que les autres devront suivre la procédure d'autorisation et d'analyse normalement diligentée par la CNIL.

Le Document d'Orientation ajoute qu'il revient au responsable du système d'informer clairement les personnes concernées du champ d'application restreint du système et du fait que les alertes sortant hors de celui-ci qui sont néanmoins communiquées par son entremise seront automatiquement dirigées vers le département adéquat.

1.3. Caractère facultatif

27. L'usage du système doit être facultatif, c'est-à-dire non obligatoire sous peine de transférer sur les salariés la charge de l'employeur en matière de respect du règlement intérieur. Il revient en effet à l'employeur de mettre tous les moyens en œuvre afin que son règlement d'intérieur soit respecté (session d'information, communication claire, disponibilité des documents, sanctions communiquées, …). Se reposer uniquement sur les signalements rapportés par les employés ne pourrait de surcroît jamais apporter la même sécurité, le succès de l'utilisation de ces mécanismes étant encore très limité.

---

46. Pour une analyse de ce document, nous renvoyons le lecteur à E. Wéry, "Lignes éthiques et autres whistleblowing: la CNIL propose une solution", 30 novembre 2005, sur http://www.droit-technologie.org/1_2.asp?actu_id=1132.
47. Document d'Orientation du 10 novembre 2005 de la CNIL, p. 2.
48. Selon cet article: *"Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes: 1° le respect d'une obligation légale incombant au responsable du traitement; (...) 5° la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée."*
49. Par exemple l'arrêté du 31 mars 2005 modifiant le règlement du Comité de la réglementation bancaire et financière n° 97-02 du 21 février 1997 relatif au contrôle interne des établissements de crédits et des entreprises d'investissement.
50. CNIL, FAQ sur les dispositifs d'alerte professionnelle, 1er mars 2006, question 10.

2. Principe de limitation des personnes concernées par le système d'alerte[51]

28. Il relève de la responsabilité du chef d'entreprise de définir les catégories de personnes susceptibles d'être concernées par le système (en tant qu'auteur ou que personne mise en cause par l'alerte) et de fixer les contours de la procédure à suivre pour utiliser le système, et ce dans le respect des dispositions pertinentes du droit du travail. La définition du groupe de personnes susceptibles d'être mise en cause par le mécanisme d'alerte professionnelle ne pourra bien entendu pas être disproportionnée par rapport à l'objectif intrinsèque du système tel que communiqué par l'entreprise.

3. Principe d'identification de l'auteur de l'alerte[52]

29. Nous retrouvons le principe selon lequel les dénonciations anonymes doivent être évitées, et ce pour diverses raisons listées par le Document d'Orientation: éviter la délation et les dénonciations calomnieuses, organiser une protection de l'auteur de l'alerte contre les représailles, ou encore assurer un meilleur traitement de l'alerte en demandant à son auteur des précisions complémentaires.

Afin d'atteindre cet objectif, le Document d'Orientation interdit la publicité ventant cette possibilité d'alerte anonyme et recommande de concevoir le système d'une manière telle qu'il favorise l'identification de l'auteur.

Il ne s'agit cependant pas d'une interdiction formelle des alertes anonymes. Si de telles alertes devaient quand même être traitées dans des circonstances exceptionnelles, il serait nécessaire d'entourer ce traitement de précautions particulières telles que leur examen préalable par le premier destinataire, l'analyse de l'opportunité de leur diffusion, la mention claire du caractère anonyme de cette alerte, l'identification des faits plutôt que de la personne mise en cause ("traitement anonyme de la plainte anonyme") pour ne citer que les plus importantes[53].

Corollaire de ce principe d'identification de l'auteur de l'alerte, il faut s'assurer de garantir la confidentialité de son identité, et ce même lorsque la personne mise en cause exerce son droit d'accès et de rectification.

4. Principe d'information claire et complète des utilisateurs potentiels du système d'alerte professionnelle[54]

30. Il est nécessaire d'informer les utilisateurs potentiels du système. Les informations à communiquer sont prévues à l'article 32 de la loi informatique et libertés[55]et comprennent entre autre l'identité du responsable du traitement, les objectifs poursuivis, les domaines concernés, le caractère facultatif du dispositif, les destinataires de l'alerte, les droits d'accès et de rectification, les sanctions en cas d'usage abusif et l'absence de sanction en cas d'usage de bonne foi. L'objectif est ici d'obtenir le consentement éclairé de toute personne faisant usage du système.

Nous estimons de nouveau que l'adoption par la société d'une *"policy"* comprenant entre autre l'ensemble de ces éléments paraît être la solution la plus pragmatique afin de respecter ce principe.

5. Principe de moyens dédicacés[56]

31. Selon ce principe, les alertes doivent être recueillies par des moyens informatisés ou non, mais dédiés au dispositif d'alerte[57]. Cette spécificité rendra plus aisée la vérification du respect des conditions de sécurité et de confidentialité que le système doit garantir.

6. Principe d'alertes pertinentes, adéquates et non excessives[58]

32. En application de ce principe, les informations fournies dans le cadre de l'alerte doivent être objectives, directement liées aux faits allégués et rentrer dans le champ d'application du dispositif. Ce principe est dès lors étroitement lié à la condition de légitimité du système.

7. Principe de spécialisation du recueil et du traitement des données[59]

33. Le recueil et le traitement des alertes doivent être confiés à des spécialistes en place dans un département spécifi-

51. Document d'Orientation du 10 novembre 2005 de la CNIL, p. 4.
52. Document d'Orientation du 10 novembre 2005 de la CNIL, p. 4.
53. Les trois dernières conditions sont issues des FAQ de la CNIL du 1 mars 2006, question 12.
54. Document d'Orientation du 10 novembre 2005 de la CNIL, p. 5.
55. Selon cet article; *"La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant: 1° de l'identité du responsable du traitement et, le cas échéant, de celle de son représentant; 2° de la finalité poursuivie par le traitement auquel les données sont destinées; 3° du caractère obligatoire ou facultatif des réponses; 4° des conséquences éventuelles, à son égard, d'un défaut de réponse; 5° des destinataires ou catégories de destinataires des données; 6° des droits qu'elle tient des dispositions de la section 2 du présent chapitre (droits des personnes à l'égard des traitements de données); 7° le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un État non membre de la Communauté européenne."*
56. Document d'Orientation du 10 novembre 2005 de la CNIL, p. 5.
57. L'objectif de ce principe étant d'éviter tout risque de détournement de finalité et de renforcer la confidentialité des données.
58. Document d'Orientation du 10 novembre 2005 de la CNIL, p. 5.
59. Document d'Orientation du 10 novembre 2005 de la CNIL, p. 5.

que et soumis à un engagement contractuel de confidentialité.

34. Le Document d'Orientation aborde ensuite la question des informations collectées dans un groupe d'entreprises. Il précise que ces informations ne peuvent être communiquées à d'autres entités du groupe que si c'est nécessaire pour le déroulement de l'enquête. Mais même dans ce cas, il faudra au préalable s'assurer que les informations seront traitées avec le niveau nécessaire de sécurité et de confidentialité. Si les informations doivent être communiquées dans un pays situé hors de l'Union européenne, il faudra ici aussi s'assurer que les dispositions en matière de transfert de données prévues par la Directive européenne et la loi informatique et libertés[60] seront respectées.

Si le responsable du traitement désire faire appel à un prestataire tiers pour gérer le dispositif, il devra respecter les principes en matière de sous-traitance tels que décrits *supra*. Les FAQ émises par la CNIL[61] définissent de manière plus précise les obligations auxquelles ces prestataires sont tenues: respecter les règles auxquelles sont soumis les responsables du traitement, ne pas utiliser les données à des fins autres que celles pour lesquelles elles ont été collectées, respecter des obligations de confidentialité strictes, ne communiquer les données qu'à des personnes bien définies au sein de l'organisation chargées de la gestion de ces alertes, respecter la durée de conservation des données et enfin, détruire ou restituer les supports de données à la fin de leur prestation.

Les FAQ précisent en outre que le prestataire n'est pas tenu d'indiquer à la personne utilisant le dispositif qu'elle est en contact avec un prestataire, cette sous-traitance pouvant se faire de manière tout à fait transparente. Autre précision importante, il appartient au responsable du traitement de communiquer au sous-traitant les informations nécessaires lui permettant de transférer à la personne adéquate de l'organisation les informations reçues qui sortent hors du champ d'application du dispositif.

8. Rapports d'évaluation du système d'alerte[62]

35. Le Document d'Orientation ajoute à ces principes déjà repris dans l'Avis du Groupe 29 une disposition ayant trait à la possibilité de faire réaliser des rapports d'évaluation du dispositif. Ainsi, l'entreprise pourra communiquer aux prestataires chargés de cette évaluation toutes informations statistiques utiles à leur mission (typologie d'alertes reçues, mesures correctives prises, …) mais sans bien entendu permettre l'identification des personnes concernées par les alertes. Il serait donc sage de prévoir des standards de rapports contenant les informations pouvant être fournies de manière agrégée.

9. Principe de conservation limitée des données à caractère personnel[63]

36. Les données communiquées dans le cadre d'une alerte jugée infondée devront être supprimées ou archivées immédiatement. Les données relatives aux alertes fondées qui rentrent dans le champ d'application du dispositif ne pourront quant à elles être conservées que pendant deux mois à partir de la clôture des opérations de vérification (sauf toutefois si une procédure judiciaire ou disciplinaire est en cours où elles devront l'être jusqu'à l'aboutissement des procédures).

Le choix entre la suppression ou l'archivage des données après écoulement du délai de conservation raisonnable revient à l'employeur. S'il choisit l'archivage, il devra s'assurer d'utiliser un système d'information distinct à accès restreint. Dans ce cas, les données ne pourront être conservées que pendant trente ans. Seules les personnes chargées du traitement des alertes pourront y avoir accès, et uniquement pour défendre les intérêts de l'entreprise en justice, à la demande d'un tiers autorisé au sens de la loi informatique et libertés ou à la demande des titulaires du droit d'accès et de rectification[64].

10. Principe d'information rapide de la personne mise en cause[65]

37. En conformité avec les articles 6 et 32 de la loi informatique et libertés, il sera nécessaire d'informer immédiatement (soit dès l'enregistrement des données) la personne concernée par l'alerte afin de lui permettre de se défendre et, le cas échéant, de s'opposer au traitement. Toutefois, la personne concernée pourra exceptionnellement être informée plus tard si des mesures conservatoires préalables doivent être prises.

11. Principe des droits d'accès et de rectification[66]

38. En respect des articles 39 et 40 de la loi informatique et libertés, la personne mise en cause par l'alerte doit se voir accorder le droit d'accéder aux données personnelles la concernant et, le cas échéant, de les corriger si nécessaire.

60. Art. 68 à 70 loi informatique et libertés.
61. FAQ sur les dispositifs d'alerte professionnelle, 1er mars 2006.
62. Document d'Orientation du 10 novembre 2005 de la CNIL, p. 6.
63. Document d'Orientation du 10 novembre 2005 de la CNIL, p. 6.
64. CLINL, FAQ sur les dispositifs d'alerte professionnelle, 1er mars 2006, question 17.
65. Document d'Orientation du 10 novembre 2005 de la CNIL, p. 6.
66. Document d'Orientation du 10 novembre 2005 de la CNIL, p. 7.

III. Décision d'Autorisation Unique[67]

39. L'Autorisation Unique reprend pour son compte les principes développés dans le Document d'Orientation mais de manière structurée. En effet, selon le principe de l'autorisation unique repris dans l'article 25 de la loi informatique et libertés, les dispositifs qui répondent à l'ensemble des principes décrits dans le Document d'Orientation et repris dans l'Autorisation Unique bénéficieront automatiquement d'une autorisation unique de la CNIL alors que ceux qui ne les respectent pas seront soumis à une analyse en détail de leur validité.

Afin de bénéficier de l'autorisation unique, le responsable du traitement devra adresser à la CNIL un engagement de conformité à l'Autorisation Unique. Il recevra alors par retour de courrier un accusé de réception et pourra dès ce moment mettre en place le dispositif. Il s'agit d'une grande simplification par rapport à la procédure standard d'autorisation qui nécessite quant à elle le dépôt d'un dossier devant être examiné par une séance plénière de la CNIL dans les deux mois suivant ce dépôt.

40. L'Autorisation Unique contient une série de spécificités par rapport au Document d'Orientation:

– elle donne ainsi une définition de l'alerte professionnelle qu'il faut entendre comme *"le système mis à la disposition des employés d'un organisme public ou privé pour les inciter, en complément des modes normaux d'alerte sur les dysfonctionnements de l'organisme, à signaler à leur employeur des comportements qu'ils estiment contraires aux règles applicables et pour organiser la vérification de l'alerte ainsi recueillie au sein de l'organisme concerné"*[68];
– elle liste les catégories de données à caractère personnel pouvant être enregistrées dans le cadre du dispositif d'alerte, soit l'identité, la fonction et les coordonnées de l'émetteur de l'alerte et de la personne visée, des personnes recevant et traitant l'alerte; les faits signalés; les éléments recueillis dans le cadre de la vérification des faits, le compte rendu des opérations de vérification ainsi que les suites données à l'alerte[69];
– elle précise les protections à garantir en cas de transfert de données à caractère personnel en dehors de l'Union européenne: lorsque la société américaine a adhéré au principe américain de *"Safe Harbors"*, lorsque le destinataire a conclu un contrat de transfert basé sur les clauses contractuelles types émises par la Commission européenne[70] ou enfin lorsque le groupe de sociétés a adopté des règles internes dont la CNIL a préalablement reconnu qu'elles garantissent un niveau de protection suffisant[71];
– enfin, elle définit les mesures de sécurité à mettre en œuvre. L'accès aux données doit ainsi être protégé par un mot de passe régulièrement renouvelé ou par tout autre moyen d'authentification individuel. Ces accès doivent être enregistrés et leur régularité contrôlée.

§ 4. La Recommandation de la Commission de la Vie Privée

41. Fin novembre 2006 la Commission de la Vie Privée a à son tour défini sa position envers les systèmes d'alerte professionnelle et leur compatibilité avec la loi sur la vie privée de 1992 dans une Recommandation[72].

Nous allons passer en revue les principaux éléments de cette Recommandation.

I. Définition

42. La Recommandation définit les systèmes d'alerte professionnelle comme *"des dispositifs 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"*.

On notera que cette définition ne se limite pas aux domaines financier et d'audit mais s'applique à toute violation d'une loi ou régulation ou encore d'une des règles internes adoptées par la société. De surcroît, la Recommandation ne

67. Pour une analyse de ce texte, nous renvoyons le lecteur à L. Rapp et R. Perray, "Whistleblowing ou dénonciation: la CNIL sépare le bon grain de l'ivraie", *Revue Lamy droit de l'immatériel* 2006, p. 46.
68. Préambule Autorisation Unique n° AU-004 du 8 décembre 2005 de la CNIL.
69. Art. 3 Autorisation Unique n° AU-004 du 8 décembre 2005 de la CNIL.
70. Décision 2001/497/CE du 15 juin 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE, *J.O.C.E.* 10 janvier 2002, p. 6, modifiée par la décision 2004/915/CE du 27 septembre 2004 modifiant la décision 2001/497/CE en ce qui concerne l'introduction d'un ensemble alternatif de clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers, *J.O.C.E.* 29 décembre 2004, p. 385.
71. Art. 5 Autorisation Unique n°AU-004 du 8 décembre 2005 de la CNIL.
72. Recommandation n°1/2006 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.

s'applique pas uniquement aux cas d'infractions dans le sens légal du terme mais aussi aux simples violations des normes appliquées par l'entreprise.

II. Applicabilité de la Loi sur la Vie Privée de 1992 (ci-après "LVP")[73]

43. La Recommandation explique que, en application de l'article 3 § 1 LVP[74], cette dernière trouve à s'appliquer car l'utilisation d'un système d'alerte professionnelle implique dans la quasi majorité des cas un traitement de données à caractère personnel. Elle liste ensuite les dispositions pertinentes de cette loi que doit respecter chaque système d'alerte afin de se conformer à la LVP puis les analyse au cas par cas.

a) Principes d'admissibilité, de loyauté, de licéité et de finalité

1. Principe d'admissibilité

44. L'article 5 LVP fournit deux motifs pouvant justifier l'installation d'un système d'alerte professionnelle[75]:

- l'existence d'une exigence légale ou réglementaire belge imposant à l'entreprise de traiter des données à caractère personnel via de tels systèmes (ou encore si le traitement est nécessaire pour la gestion des contentieux propres de l'organisation) (art. 5, c) LVP);
- ou, en l'absence d'une telle exigence si il existe un intérêt légitime dans le chef de l'entreprise pour mettre en place un système d'alerte professionnelle, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne mise en cause (art. 5, f) LVP).

Elle précise que si le SOX Act ne peut constituer une exigence légale au sens de l'article 5, c) LVP, il peut par contre constituer un exemple d'intérêt légitime au sens de l'article 5, f) LVP. Elle justifie cette position en précisant que la nature légitime de l'intérêt au sens de l'article 5, f) LVP – qui se juge en fonction de la gravité des faits reprochés ainsi que des principes de proportionnalité et de subsidiarité – est présente pour les sociétés cotées à la bourse américaine vu que la mise en place d'un tel système est nécessaire afin d'assurer le respect d'une des dispositions obligatoires du SOX Act. Les conséquences liées au non-respect de la législation étrangère invoquée doivent donc être prises en compte. *In casu*, la Commission de la Vie Privée estime que seule l'interprétation limitative du SOX Act est susceptible de fournir une justification légitime à l'installation d'un mécanisme d'alerte professionnelle.

2. Principes de loyauté, licéité et finalité

45. Ces principes se matérialisent dans deux des caractéristiques principales que doit présenter tout système d'alerte afin d'être déclaré compatible avec la LVP: un champ d'application précisément défini et le caractère confidentiel du traitement des alertes.

2.1. Champ d'application du système[76]

46. Tout système d'alerte doit avoir un contour précisément défini. Par conséquent, les éléments suivants doivent faire l'objet d'une définition claire et précise:

- le champ d'application et la finalité du système[77];
- la procédure d'introduction et de traitement des signalements;
- les conséquences liées aux alertes justifiées et injustifiées;
- la désignation explicite du responsable du traitement;
- le caractère facultatif et complémentaire du système;
- le principe selon lequel le dénonciateur doit se baser sur plus que de simples rumeurs mais vraiment sur un motif raisonnable; et enfin
- le principe de précision des informations fournies.

De manière logique, la Recommandation reprend ensuite l'interdiction de principe des dénonciations anonymes ainsi que l'argumentation du Groupe 29 afin de justifier exceptionnellement leur traitement.

2.2. Confidentialité du traitement des signalements et traitement dédicacé[78]

47. La Recommandation impose de maintenir confidentielle l'identité de la personne ayant fait usage du système.

73. Pour une analyse de cette loi, nous renvoyons le lecteur à Th. Léonard et Y. Poullet, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995", *J.T.* 1999, p. 377 ainsi qu'à D. Lambrecht, "De bescherming van de privacy in de Belgische wetgeving. Overzicht van de bestaande wetgeving en een blik vooruit naar de op handen zijnde veranderingen", *Jura Falc.*, http://www.law.kuleuven.be/jura/37n3/lambrecht.htm.

74. En vertu de cet article: *"La présente loi s'applique à tout traitement de données à caractère personnel automatisé en tout ou en partie, ainsi qu'à tout traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier."*

75. Recommandation n° 1/2006 du 29 novembre 2006 de la Commission de la Vie Privée, p. 3.

76. Recommandation n° 1/2006 du 29 novembre 2006 de la Commission de la Vie Privée, p. 5.

77. Les finalités de ces systèmes peuvent être de favoriser le respect des règles de contrôle interne, améliorer l'image de la société et éviter des systèmes de dénonciation anarchiques.

78. Recommandation n° 1/2006 du 29 novembre 2006 de la Commission de la Vie Privée, p. 5.

Cette obligation est concrétisée par une interdiction de communiquer son identité ou des éléments qui peuvent permettre son identification à toute personne autre que le gestionnaire des plaintes sans son accord.

Elle précise en outre que les signalements doivent être traités par un gestionnaire des plaintes spécialement dédicacé à cet effet qui doit être tenu par un engagement de confidentialité spécifique. Notons qu'il devra cesser de traiter une plainte à partir du moment où le dénonciateur aura lui-même intentionnellement violé l'obligation de confidentialité de son identité.

Corollaire de cette confidentialité, le gestionnaire des plaintes doit pourvoir bénéficier d'une certaine indépendance par rapport à l'organisation. Des garde-fous doivent en effet être mis en place afin de garantir l'absence d'incompatibilités dans sa fonction. Sa responsabilité doit être clairement définie et est susceptible d'être engagée en cas de violation, par exemple, de son obligation de confidentialité[79]. Il doit de plus être protégé contre les pressions de la direction ou des syndicats.

Cette indépendance du gestionnaire des plaintes ne doit cependant pas être absolue. Elle ne peut en effet aucunement signifier qu'il peut agir sans le moindre contrôle. La Recommandation précise en effet que le système d'alerte doit prévoir une protection de la personne utilisant le système et de celle mise en cause à l'encontre d'éventuelles fautes du gestionnaire de plainte. Ce mécanisme de recours pourrait par exemple être décrit dans la *"policy"*.

3. Principe de proportionnalité et de complémentarité

48. La Recommandation précise que le système d'alerte professionnelle ne peut servir que pour des problèmes ne pouvant manifestement pas être traités par la voie hiérarchique normale et pour lesquels il n'existe par de procédure ou d'organe spécifique réglementé légalement.

Elle précise en outre que les faits rapportés doivent être suffisamment graves, traduisant un dysfonctionnement (et non pas uniquement une infraction) sérieux qu'il faut dénoncer dans l'intérêt général ou dans celui d'une bonne gouvernance de l'organisation et pour lesquels l'utilisateur estime ne pas pouvoir suivre la voie traditionnelle.

Troisième volet de ce principe de proportionnalité, le champ d'application *rationae personae* du système (utilisateurs et personnes mises en cause) se limite aux personnes qui font partie de l'organisation. La Recommandation ne donne cependant pas plus de détails quant aux personnes visées. Nous estimons qu'afin que l'objectif du système soit atteint, c'est-à-dire éviter les fraudes financières, les agents contractuels, consultants, intérimaires ainsi que toute autre personne employée par la société devraient y avoir accès.

4. Principes d'exactitude et de précision

49. Le gestionnaire des plaintes doit veiller à ce que les données à caractère personnel destinées au traitement des signalements soient exactes et précises.

Il doit de même veiller à ce qu'elles soient adéquates, pertinentes et non excessives. Elles doivent en outre se limiter à la description du fait, et ce sans jugement de valeur. Ainsi, si le signalement concerne des faits non prouvés, il sera nécessaire de le mentionner de manière expresse.

Enfin, le gestionnaire devra s'assurer que les données à caractère personnel collectées via le système d'alerte professionnelle ne seront conservées que pour une durée n'excédant pas celle nécessaire au traitement du signalement. Nous noterons toutefois qu'à la différence de la CNIL, la Commission de la Vie Privée n'a pas jugé nécessaire de préciser de délais maximum de conservation[80].

5. Principe de transparence

50. Au niveau collectif, ce principe couvre l'obligation pour la société d'informer les membres du personnel tout en respectant les législations sur le droit du social. Il faudra ainsi entre autre informer le conseil d'entreprise ou encore le comité de prévention et de protection du travail[81].

Au niveau individuel, cela couvre entre autre l'information plus détaillée des collaborateurs de l'organisation susceptibles d'être impliqués dans le système d'alerte. Devront ainsi entre autre leur être communiqués le champ d'application, la finalité, la procédure d'introduction, les conséquences des signalements justifiés et injustifiés, la manière dont les droits d'accès peuvent être exercés et l'instance auprès de qui ils peuvent l'être, les tiers à qui des données personnelles peuvent être transmises dans le cadre du traitement du signalement mais aussi l'obligation de traitement confidentiel à laquelle le système et le gestionnaire des plaintes sont tenus.

La personne incriminée doit être informée le plus rapidement possible par le gestionnaire des plaintes de l'existence d'un signalement et des faits qui lui sont reprochés. Toutefois, il est permis de reporter cette notification lorsque des circonstances exceptionnelles le requièrent.

79. Recommandation n° 1/2006 du 29 novembre 2006 de la Commission de la Vie Privée, p. 5.
80. Recommandation n° 1/2006 du 29 novembre 2006 de la Commission de la Vie Privée, p. 6.
81. Recommandation n° 1/2006 du 29 novembre 2006 de la Commission de la Vie Privée, p. 7.

6. Principe de sécurité[82]

51. Le système doit prévoir des garanties pour que les données ne soient pas traitées à une autre fin. Il faut donc s'assurer qu'elles feront l'objet d'un traitement distinct. Afin de garantir le respect de ce principe de sécurité, les données ne devront être traitées que dans le cadre des notifications rentrant dans son champ d'application et le système devra faire montre d'un niveau minimal de confidentialité, d'intégrité, d'authenticité et de disponibilité.

Étant donné qu'il doit être en mesure de démontrer le respect de ce principe, le gestionnaire des plaintes devra organiser des possibilités d'audit permettant de vérifier la manière avec laquelle les données sont traitées. Il devra ainsi disposer d'un *"audit trail"* permettant de montrer quelles sont les données à caractère personnel stockées, qui y a accédé, quand et comment. Les données ainsi stockées devront de plus être intègres, c'est-à-dire qu'il faudra être en mesure de démontrer que personne n'a pu y accéder pour les modifier.

Les transferts intragroupe et extra Union européenne doivent respecter les mêmes principes que ceux prévus dans l'Avis du Groupe 29 et la Décision d'Autorisation Unique, en ligne avec les articles 21 et 22 LVP. Nous renvoyons dès le lecteur aux sections pertinentes *supra*.

7. Droits de la personne mise en cause, de celle utilisant le système et des tiers[83]

7.1. Personne mise en cause

52. Dès qu'elle aura été mise au courant du signalement la concernant, la personne mise en cause pourra bénéficier des droits d'accès, de rectification et de suppression (si le traitement est interdit, excessif ou si les données ont été gardées trop longtemps) des données à caractère personnel traitées dans le cadre du dispositif d'alerte professionnelle, et ce en respect des articles 9 et suivants de la LVP.

7.2. Personne utilisant le système

53. La personne utilisant le système a quant à elle le droit d'être tenu informée de ce qu'il advient de sa plainte.

7.3. Principe d'interdiction d'accès aux données d'autrui

54. Ni la personne mise en cause, ni celle utilisant le système ne peuvent accéder aux données d'autrui, sauf accord de la personne concernée.

Ce principe connaît cependant deux exceptions:

– si la personne mise en cause est victime de signalements injustifiés, accusations calomnieuses ou faux témoignages, elle pourra alors accéder à toutes les données ayant trait à ces signalements;

– si, après enquête, la personne mise en cause a suspecté à tort des tiers ayant agi de mauvaise foi ou la personne ayant utilisé le système[84], cette dernière pourra alors accéder aux données personnelles stockées dans le système d'alerte.

8. Principe de déclaration préalable[85]

55. En application de l'article 17 LVP, préalablement à sa mise en œuvre, la société désirant implémenter un mécanisme de *whistleblowing* devra soumettre une déclaration auprès de la Commission de la Vie Privée. Ce n'est que lorsque cette obligation sera remplie que le système pourra effectivement être mis en œuvre. Il n'y a donc pas en Belgique de système d'autorisation unique. Il reviendra à la Commission de prendre contact avec la société si elle estime devoir obtenir des renseignements complémentaires ou si elle estime que la légalité du système n'est pas garantie.

La déclaration est requise même si les informations sont reprises dans un fichier manuel car la Recommandation instaure une présomption que la nature des informations traitées par un tel système d'alerte, fusse-t-il manuel, requiert *ipse facto* une telle déclaration (art. 19 LVP).

9. Rapport d'évaluation du système d'alerte

56. Des rapports d'évaluation du système peuvent bien entendu régulièrement être diligentés par les dirigeants de la société afin d'analyser la manière dont ce système fonctionne. Il faudra cependant s'assurer que ces rapports ne violent pas les droits des personnes ayant utilisé ou ayant été mises en cause par ce système. Ces rapports ne pourront donc pas être communiqués sous une forme permettant leur identification.

Il faudra de même mettre tous les moyens en œuvre afin d'éviter les cas d'identification indirecte. Néanmoins, ces cas d'identification indirecte ne pourront jamais être exclus car il est impossible d'éviter que certaines personnes soient identifiées, par exemple si un grand nombre de détails sont donnés dans le rapport quant à la nature des faits, ou si des problèmes organisationnels/structurels sont liés au signalement en cause.

82. Recommandation n° 1/2006 du 29 novembre 2006 de la Commission de la Vie Privée, p. 7.
83. Recommandation n° 1/2006 du 29 novembre 2006 de la Commission de la Vie Privée, p. 8.
84. En l'accusant à tort d'avoir participé aux pratiques abusives dénoncées.
85. Recommandation n° 1/2006 du 29 novembre 2006 de la Commission de la Vie Privée, p. 8.

§ 5. COMPATIBILITÉ ENTRE LES TEXTES EUROPÉENS ANALYSÉS ET LA LOI SOX

57. Il n'est pas certain que les efforts normatifs découlant de la position "Groupe 29" tels que décrits *supra* auront suffi à résoudre le conflit entre le SOX Act et les textes européens en matière de protection de la vie privée. Le président du Groupe 29 a bien adressé une lettre au président de la SEC afin de s'assurer que les systèmes répondant aux critères tels que fixés dans l'Avis seront bien déclarés compatibles avec le SOX Act mais à notre connaissance aucune réponse n'est encore parvenue.

La raison de cette absence de réaction est peut être à chercher dans les différences les plus fondamentales entre les deux positions. Voici donc pourquoi, selon nous, les *"ethical lines SOX"* pourraient ne pas être acceptées en Europe.

I. Le champ d'application du mécanisme d'alerte professionnelle

58. Alors que de nombreuses entreprises américaines ont interprété le SOX Act, et plus spécialement sa Section 806, comme justifiant les mécanismes d'alerte professionnelle qui visent non seulement les dysfonctionnements liés aux domaines financiers mais aussi, par exemple, en matière de droit du travail, de santé et de sécurité publique, la position du G29 et de la CNIL est par contre pour l'instant plus restrictive.

L'Avis du G29 et la Déclaration d'Autorisation Unique ne visent en effet que les faits liés aux risques sérieux encourus par la compagnie dans les champs comptables, d'audit financier, de la corruption ou encore bancaire (soit le champ d'application originel du SOX Act tel que prévu dans la Section 301). Pour ce qui est de la France, des *whistleblowing lines* mises en place suite à l'interprétation limitative du SOX Act pourront donc bénéficier de l'autorisation unique de la CNIL alors que ceux ayant un champ d'application plus étendu ne pourront être mis en place que moyennant l'autorisation préalable de la CNIL faisant suite à une analyse approfondie de sa légalité.

En Belgique, par contre, ce genre de limitation n'est pas d'application. La Recommandation ne limite en effet pas son champ d'application aux domaines financiers de sorte que des mécanismes d'alerte à l'étendue plus large pourraient être admis pour autant qu'ils répondent aux conditions fixées dans la Recommandation de la Commission de la Vie Privée.

II. Caractère spécial de l'organe recevant les signalements

59. Alors que les textes européens requièrent que la cellule chargée de gérer ces signalements soit indépendante dans l'organisation et soit située dans un département spécifique, le SOX Act ne requiert quant à lui pas de mettre en place une telle organisation de la même manière qu'il ne contient aucune disposition quant aux caractéristiques d'indépendance que doit présenter le gestionnaire des plaintes. Il précise même au contraire que le *whistleblower* ne peut fournir ses informations qu'à une série limitée de personnes (tout superviseur ou toute personne travaillant pour l'employeur qui a autorité pour enquêter, découvrir ou stopper le méfait; auprès d'une agence chargée de l'application des lois et régulations fédérales; à un membre du Congrés ou un de ses comités).

III. Caractère anonyme des signalements

60. Alors que le SOX Act requiert la mise en place d'au minimum un système de *whistleblowing* permettant de préserver l'anonymat de la personne faisant usage dudit système, la position européenne est par contre de recommander que les compagnies découragent l'utilisation de tels systèmes anonymes, ou de tout le moins s'abstiennent de promouvoir l'existence de cette possibilité de signalements anonymes.

IV. Caractère facultatif de l'usage du système d'alerte

61. Beaucoup de codes de conduite estampillés SOX requièrent de reporter les dysfonctionnements sous peine de sanction. Cette exigence est en contradiction avec les dispositions des textes européens qui stipulent quant à eux l'utilisation volontaire du mécanisme. La solution la plus évidente pour ces sociétés serait de désormais distinguer leur code de conduite de la procédure de *whistleblowing*, sans créer de lien entre l'un et l'autre.

V. Non-applicabilité du SOX Act aux employés non américains en Europe

62. Une cour d'appel américaine a récemment décidé[86] que les dispositions du SOX Act relatives au *whistleblowing*

86. *Carnero/Boston Scientific Corp.*, 433 F.3d 1 (1st Cir., 5 janvier 2006).

ne s'étendaient pas aux citoyens non américains travaillant en dehors des États-Unis pour des filiales étrangères de compagnies soumises au SOX Act. Ce jugement réduit donc le champ d'application *rationae personae* du SOX Act mais introduit une limitation non connue des normes européennes qui ne font quant à elles aucune distinction quant à la nationalité de la personne utilisant le système.

VI. Transfert de données vers le siège central américain

63. Selon le SOX Act, il revient au comité d'audit de mettre en place le système d'alerte professionnelle. C'est donc à ce comité que seront communiqués les cas les plus sérieux de manquements financiers reportés via le système. Or, ces comités d'audit, pour les sociétés américaines, sont presque exclusivement localisés sur territoire américain. Il appartiendra dès lors pour ces sociétés de respecter les règles européennes en matière de transfert de données à caractère personnel vers des pays situés hors de l'Union européenne.

VII. Divers

64. Notons encore que le SOX Act ne prévoit pas de droit d'accès ou de rectification pour la personne mise en cause par un signalement comme il ne prévoit pas non plus de délai maximum pendant lequel les données à caractère personnel relatives à un signalement peuvent être stockées. Enfin, la position Groupe 29 requiert d'avertir immédiatement (sauf exceptions) la personne mise en cause par l'alerte, exigence non requise par le SOX Act. Cette information immédiate pourrait même être en contradiction avec le SOX Act si elle compromet de manière significative l'environnement de contrôle de la société.

§ 6. *Whistleblowing* ET GOUVERNEMENT D'ENTREPRISE (*corporate governance*)

65. L'introduction de système d'alerte professionnelle n'est pas que le propre de textes émanant des autorités de protection de la vie privée. La tendance actuelle de favoriser au sein des entreprises un *corporate governance* transparent et efficace permettant de gérer au mieux la société en évitant tout dérapage immoral a ainsi amené divers régulateurs à inclure dans leur texte une provision prévoyant la mise en œuvre d'un mécanisme de *whistleblowing* par les entités régulées.

66. Ainsi, en Belgique, la Commission Bancaire, Financière et des Assurances est-elle en train de travailler sur un avant-projet de circulaire relative à la bonne gouvernance des établissements de crédit, entreprises d'assurance et autres institutions financières[87] qui comprend une disposition selon laquelle l'institution peut développer des procédures qui permettent de rapporter des plaintes directement ou indirectement (médiateur, compliance, audit interne) au niveau de la direction sans passer par les canaux hiérarchiques normaux.

Elle ajoute que les personnes ayant émis un signalement de bonne foi seront protégées contre toute mesure disciplinaire, et termine en précisant que les signalements communiqués doivent être effectivement analysés et que des mesures adéquates doivent être prises pour redresser toute irrégularité. Ces mécanismes ne peuvent cependant, précise l'avant-projet de circulaire, être mis en œuvre que moyennant le respect de la réglementation relative à la protection de la vie privée. Une fois adoptée, cette circulaire pourrait selon nous constituer une obligation réglementaire justifiant la mise en œuvre d'un système d'alerte professionnelle au sens de la loi vie privée.

67. Le *Committee of European Banking Supervisors* a quant à lui émis une série de lignes directrices[88] que les établissements de crédits sont supposés respecter et qui doivent être appliquées par les autorités de supervision en matière de gouvernance interne. Selon le CEBS, il revient au management de mettre en place des procédures d'alerte appropriées afin de permettre aux employés de communiquer leurs inquiétudes face à des questions de gouvernance interne significatives et légitimes.

Les procédures mises en place doivent (i) assurer la confidentialité de la personne ayant soulevé ses inquiétudes, (ii) être subsidiaires par rapport aux lignes de reporting classiques, (iii) être mises à disposition des employés de manière écrite.

De manière assez étrange, le CEBS continue en précisant que les informations relevantes reçues au moyen de cette procédure d'alerte doivent être mises à la disposition de l'organe de management, allant ainsi en contradiction avec le principe de confidentialité qu'il avait pourtant énoncé auparavant.

Enfin, le CEBS recommande aux états membres d'aussi permettre aux employés de communiquer leurs inquiétudes, non

87. Avant-projet de circulaire relative aux attentes prudentielles de la CBFA au sujet de la bonne gouvernance des institutions financières, disponible à l'adresse suivante: http://www.cbfa.be/fr/consultations/lop/pdf/corporategovernance_04-2006.pdf.

88. Guidelines on the Application of the Supervisory Review Process under Pillar 2 (CP03 revised), 25 janvier 2006, disponibles à l'adresse suivante: http://www.c-ebs.org/pdfs/GL03.pdf.

seulement au travers de la procédure d'alerte, mais aussi aux autorités de supervision. Aucune clarté n'est cependant apportée quant à la question de savoir ce qu'il faut exactement leur communiquer, ni quand, et enfin, ni par quel moyen?

CONCLUSION: DIX CONSEILS AFIN DE METTRE EN PLACE UN SYSTÈME DE *whistleblowing.*

68. Au-delà des incertitudes planant quant aux réactions de la SEC vis-à-vis de la position européenne en matière de système d'alerte professionnelle, dix principes de base[89] sont à respecter par toute entreprise désirant implémenter un tel mécanisme en France ou en Belgique.

1. Réaliser une analyse approfondie afin d'obtenir une délimitation claire et précise du champ d'application du système d'alerte ainsi que des matières pouvant être sujettes à signalement. Cette analyse est à conserver afin de pouvoir fournir, si nécessaire, un justificatif de l'étendue du système.

Comme préalablement mentionné, si il est préférable de se limiter aux domaines financiers, comptables, d'audit et de blanchiment en France (afin de bénéficier de l'autorisation unique), il semble qu'une telle limitation ne soit pas d'application en Belgique pour autant que les mécanismes d'alerte professionnelle proposés soient légitimes au sens de la loi sur la protection de la vie privée.

2. Rédiger une *policy* à faire approuver par l'organe de management contenant une description du champ d'application du système, des catégories de personnes pouvant utiliser ou être mises en cause par le système, de la procédure à suivre pour signaler un soupçon légitime de dysfonctionnement, de la confidentialité assurée quant à l'identité de la personne faisant usage du système, des droits d'accès et de rectification de la personne concernée par le signalement, du caractère supplétif et complémentaire du système. Si nécessaire, il faudra consulter les syndicats préalablement à l'adoption de ce document introduisant un mécanisme de contrôle des travailleurs[90].

3. S'assurer que ce mécanisme n'est pas le seul outil permettant de remonter des signalements suspects dans ces domaines. Il faudra de même mentionner clairement dans la *policy* précitée le caractère facultatif de l'utilisation de ce système et préconiser l'identification des personnes émettant des alertes.

4. En France, il sera nécessaire de documenter comment l'accès au mécanisme d'alerte professionnelle a été limité à certaines catégories de personnes. Etablir un lien entre les personnes visées et leur place dans l'organigramme pourrait être envisagé. Pareille condition ne se retrouve par contre pas dans la Recommandation de la Commission de la Vie Privée.

5. Mettre en place un mécanisme automatique de notification immédiate de la personne mise en cause dès qu'un signalement a été introduit qui la concerne et l'informer par le même canal qu'elle dispose d'un droit d'accès, de rectification et de suppression si cela s'avère nécessaire.

6. S'assurer que tous les signalements émis dans le domaine financier aboutissent *in fine* aux personnes en charge de la cellule responsable de la gestion des systèmes d'alerte, et ce qu'elles aient été introduites via les mécanismes de *whistleblowing* ou via un autre canal. De surcroît, il sera nécessaire de placer cette cellule de manière indépendante au sein de l'organigramme, par exemple comme rapportant de manière directe à l'administrateur délégué ou bien dans le département *compliance*.

Il sera de même utile de rédiger un "job description" précis et de prévoir un training spécifique pour les gestionnaires de plaintes afin de s'assurer qu'ils respecteront les obligations qui leur sont imposées par les textes français et belge (soit entre autre vérifier que les conditions de confidentialité et de sécurité sont respectées, que le contenu des signalements est pertinent, adéquat et non excessif…) et de faire en sorte que chaque personne travaillant au sein de ce département signe un *Non-Disclosure Agreement* spécifique.

7. Inclure dans les spécifications du système d'alerte les mesures techniques et de sécurité nécessaires en vue de mener les enquêtes et de traiter les données à caractère personnel de la manière la plus diligente possible, c'est-à-dire transparente, adéquate, effective et efficace. Ainsi, il faudra s'assurer que les caractéristiques techniques du système d'alerte permettent d'assurer la *"CIA"*, soit la *confidentiality*, l'*integrity* et l'*availability*, des données stockées. Enfin, il faudra prévoir, documenter et implémenter des règles de rétention des informations strictes en ligne avec les exigences fixées par les autorités nationales.

8. L'opportunité de sous-traiter cette fonction d'enquête à des fins d'indépendance et d'impartialité peut être envisagée mais en garantissant toutefois que le prestataire choisi respectera lui aussi les conditions s'imposant normalement à l'entreprise. La rédaction d'un

89. Le respect de ces principes de base ne remplace aucunement le respect de l'ensemble des dispositions reprises dans les divers textes analysés.

90. En droit français, une telle consultation est prévue par l'art. L 432, 2, 1 § 3 du Code de travail.

contrat standard reprenant l'ensemble des obligations reprises dans l'Autorisation Unique ou dans la Recommandation peut être à cet égard utile.

9. Établir au niveau du groupe des règles claires en matière de communication des informations contenues dans les signalements à d'autres entreprises du même groupe ou encore en matière de communication de ces informations à une entité localisée dans un pays hors de l'Union européenne.

10. Enfin, avant de mettre en place un mécanisme d'alerte professionnelle, il faudra respecter les procédures d'autorisation unique, d'analyse traditionnelle ou encore de notification préalable prévues par les autorités de vie privée relevantes.