Groupe de travail «ARTICLE 29» sur la protection des données

00195/06/FR

WP 117

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

Adopté le 1er février 2006

Le groupe de travail a été établi en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Son secrétariat est assuré par la Direction C (Justice civile, droits fondamentaux et citoyenneté) de la Direction générale Justice, liberté et sécurité de la Commission européenne, B-1049 Bruxelles, Belgique, bureau LX-46-01/43.

site Internet: http://europa.eu.int/comm/justice_home/fsj/privacy/index_fr.htm

SOMMAIRE

LE GROUPE DE PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

établi par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995[1],

Vu les articles 29 et 30, paragraphe 1, point c), et paragraphe 3, de cette directive,

Vu son règlement intérieur, et notamment ses articles 12 et 14,

A ADOPTÉ LE PRÉSENT AVIS:

I. INTRODUCTION

Le présent avis donne des orientations sur la façon dont les dispositifs internes d'alerte professionnelle des dysfonctionnements (ci-après «les dispositifs d'alerte professionnelle») peuvent être mis en oeuvre dans le respect des règles de protection des données instaurées par l'UE par le biais de la directive 95/46/CE[2].

Le nombre de questions soulevées par la mise en oeuvre des dispositifs d'alerte professionnelle en Europe en 2005, y compris du point de vue de la protection des données, montre que le développement de cette pratique dans tous les pays de l'UE peut poser des difficultés considérables. Ces difficultés sont en grande partie dues à des différences culturelles, elles-mêmes liées à des contextes sociaux et/ou historiques qui ne peuvent être ni contestés, ni méconnus.

Le groupe de travail sait que ces difficultés sont en partie liées à l'éventail des problèmes qui peuvent être signalés dans le cadre des mécanismes internes de dénonciation. Il sait également que ces mécanismes soulèvent des difficultés particulières dans certains pays de l'UE sous l'angle du droit du travail et que des travaux sont en cours sur ces questions, qui devront être approfondies. Le groupe de travail doit aussi tenir compte du fait que dans certains pays de l'UE, le fonctionnement des dispositifs d'alerte professionnelle est défini par la loi, tandis que dans la majorité des pays de l'UE, aucune législation ou réglementation spécifique n'existe en la matière.

En conséquence, le groupe de travail considère qu'il est prématuré à ce stade d'adopter un avis définitif sur la dénonciation des dysfonctionnements en général. En adoptant le présent avis, il a décidé de traiter des questions qui exigent d'urgence des orientations au niveau de l'UE. Par conséquent, pour les raisons mentionnées dans ce document, l'objet du présent avis est formellement limité à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière.

---

1 JO L 281 du 23.11.1995, p. 31, publié à l'adresse : http://europa.eu.int/comm/internal_market/privacy/law_en.htm

2 Conformément au mandat spécifique du groupe de travail, le présent document de travail ne traite pas des autres problèmes juridiques posés par les dispositifs d'alerte professionnelle, sous l'angle notamment du droit du travail et du droit pénal.

Le groupe de travail a adopté le présent avis étant entendu qu'il doit approfondir la question de savoir si les règles de protection des données de l'UE sont compatibles avec les mécanismes internes de dénonciation dans des domaines autres que ceux précédemment mentionnés, par exemple les ressources humaines, la santé et la sécurité des travailleurs, les dommages à l'environnement ou les menaces écologiques et la commission d'infractions. Il poursuivra donc son travail d'analyse dans les mois à venir pour déterminer si des orientations de l'UE sont aussi nécessaires sur ces points, auquel cas les principes énoncés dans le présent document pourraient être complétés ou adaptés dans un document ultérieur.

II. JUSTIFICATION DE LA LIMITATION DE L'OBJET DU PRESENT AVIS

En 2002, le Congrès américain a adopté la loi Sarbanes-Oxley («*Sarbanes-Oxley Act*» ou «SOX») à la suite de divers scandales financiers impliquant des entreprises.

Cette loi exige que les entreprises publiques américaines et leurs filiales dans l'UE, ainsi que les sociétés non américaines cotées à une bourse américaine, mettent en place, au sein de leur commission de vérification des comptes, des «procédures pour la réception, la conservation et le traitement des plaintes reçues par l'émetteur en ce qui concerne la comptabilité, les contrôles comptables internes ou les audits; ainsi que pour la communication confidentielle et anonyme par les employés de l'émetteur de préoccupations relatives à une comptabilité ou des audits douteux»[3]. En outre, l'article 806 de la loi SOX contient une disposition visant à garantir la protection des salariés de sociétés faisant appel public à l'épargne qui fournissent des preuves de fraude contre les représailles prises à leur égard parce qu'ils ont eu recours au système de notification[4]. La *Securities and Exchange Commission* (SEC) est l'autorité qui contrôle l'application de la loi SOX aux États-Unis.

Ces dispositions sont aussi contenues dans les règlements du Nasdaq[5] et de la bourse de New-York (NYSE)[6]. Si elles sont cotées au Nasdaq ou à la bourse de New York, les sociétés doivent certifier leurs comptes sur ces marchés tous les ans. Ce processus de certification implique que les sociétés sont en mesure d'affirmer qu'elles se conforment à un certain nombre de règles, y compris en matière de dénonciation des dysfonctionnements.

Les sociétés qui ne se conforment pas à ces obligations en matière de dénonciation des dysfonctionnements sont passibles de lourdes sanctions et peines infligées par le Nasdaq, la bourse de New York ou la SEC. Compte tenu des doutes qui planent quant à la compatibilité des dispositifs d'alerte professionnelle avec les règles de protection des données de l'UE, les sociétés concernées risquent, d'une part, de se voir infliger des sanctions par les autorités de protection des données de l'UE si elles ne se conforment pas aux règles européennes en la matière, et d'autre part, d'être sanctionnées par les autorités américaines si elles ne se conforment pas aux règles américaines.

---

3 *Sarbanes-Oxley Act*, article 301, paragraphe 4.

4 L'article 406 de la loi Sarbanes-Oxley, et plus particulièrement les règlements édictés par les principaux opérateurs boursiers américains (NASDAQ, NYSE), disposent également que les sociétés cotées sur ces marchés adoptent des «codes de déontologie» assortis de mécanismes de mise en œuvre applicables aux directeurs et cadres supérieurs chargés des finances, en ce qui concerne les questions de comptabilité, d'information comptable et d'audit.

5 Règle 4350 (D)(3): «Responsabilités et pouvoirs de la commission de vérification des comptes»

6 New York Stock Exchange (NYSE), article 303A.06: «La commission de vérification des comptes»

L'applicabilité de certaines dispositions de la loi SOX aux filiales européennes de sociétés américaines et aux sociétés européennes cotées aux bourses américaines est actuellement examinée par la justice américaine[7]. Malgré cette relative incertitude quant à l'applicabilité de l'ensemble des dispositions de la loi SOX aux sociétés établies en Europe, les sociétés qui sont soumises à cette loi sur le fondement de dispositions extraterritoriales claires figurant dans ce texte souhaitent également être en mesure de se conformer aux dispositions spécifiques de celui-ci en ce qui concerne la dénonciation.

En raison du risque de sanctions qui pèse sur les sociétés de l'UE, le groupe de travail (GT29) a considéré qu'il était urgent de centrer principalement son analyse sur les dispositifs d'alerte professionnelle instaurés en vue du signalement d'éventuels manquements dans les domaines de la comptabilité, du contrôle comptable interne et de l'audit, comme le prévoit la loi Sarbanes-Oxley, ainsi que sur les questions connexes mentionnées ci-dessous. Ce faisant, le groupe de travail entend contribuer à renforcer la sécurité juridique des sociétés qui sont soumises tant aux règles de protection des données de l'UE qu'à la loi SOX.

III. ACCENT PARTICULIER MIS PAR LES REGLES DE PROTECTION DES DONNEES SUR LA PROTECTION DE LA PERSONNE MISE EN CAUSE DANS LE CADRE D'UNE PROCEDURE DE DENONCIATION DES DYSFONCTIONNEMENTS

Les dispositifs d'alerte professionnelle des dysfonctionnements internes sont généralement instaurés par souci de mettre en oeuvre les principes du bon gouvernement d'entreprise dans le fonctionnement quotidien des sociétés. La dénonciation des dysfonctionnements internes apparaît comme un mécanisme supplémentaire grâce auquel les salariés peuvent signaler toute faute par une procédure interne spécifique. Ce mécanisme complète les procédures d'information et de notification classiques de l'organisation, telles que les représentants du personnel, la voie hiérarchique, le personnel du contrôle de la qualité ou les auditeurs internes qui sont employés précisément pour signaler de telles fautes. La dénonciation des dysfonctionnements doit apparaître comme le complément, et non le substitut, de la gestion interne.

Le groupe de travail souligne que les dispositifs d'alerte professionnelle doivent être mis en oeuvre conformément aux règles de protection des données de l'UE. En fait, le fonctionnement de ces mécanismes repose dans la grande majorité des cas sur le traitement de données à caractère personnel (c'est-à-dire la collecte, l'enregistrement, le stockage, la diffusion et la destruction de données relatives à une personne identifiée ou identifiable), tant et si bien que les règles de protection des données sont d'application.

L'application de ces règles aura diverses conséquences sur l'instauration et la gestion des dispositifs d'alerte professionnelle. L'éventail de ces conséquences est décrit ci-dessous (voir section IV).

---

[7] La *U.S. Court of Appeals* (*1st Circuit*) a jugé le 5 janvier 2006 que les dispositions de la loi SOX sur la protection des «dénonciateurs» ne s'appliquent pas aux ressortissants étrangers travaillant en dehors des États-Unis pour des filiales étrangères de sociétés tenues de se conformer aux autres dispositions de cette loi.

Le groupe de travail note que si les réglementations et les orientations existantes relatives à la dénonciation des dysfonctionnements internes sont conçues pour protéger en particulier les personnes qui ont recours à la procédure de dénonciation (les «dénonciateurs»), elles ne font nulle mention spécifique de la protection de la personne mise en cause, notamment en ce qui concerne le traitement de ses données personnelles. Pourtant, même mis en cause, un individu doit jouir des droits que lui confère la directive 95/46/CE et des dispositions correspondantes de la législation nationale.

L'application des règles de protection des données de l'UE aux dispositifs d'alerte professionnelle implique qu'il faut accorder une attention particulière à la question de la protection de la personne mise en cause lors d'un signalement. À cet égard, le groupe de travail souligne que les dispositifs d'alerte professionnelle font courir un risque très grave de stigmatisation et de victimisation à cette personne au sein de son organisation. La personne sera exposée à ces risques avant même qu'elle ait connaissance de sa mise en cause et que les faits présumés aient fait l'objet d'une enquête pour déterminer s'ils sont établis.

Le groupe de travail est d'avis qu'une application correcte des règles de protection des données aux dispositifs d'alerte professionnelle contribuera à réduire ces risques. Il considère également que, loin d'empêcher ces mécanismes de fonctionner conformément à l'objectif qu'ils sont censés poursuivre, l'application de ces règles contribuera généralement au bon fonctionnement de ces mécanismes.

IV. ANALYSE DE LA COMPATIBILITE DES DISPOSITIFS D'ALERTE PROFESSIONNELLE AVEC LES REGLES RELATIVES A LA PROTECTION DES DONNEES

L'application des règles de protection des données aux dispositifs d'alerte professionnelle implique l'examen des questions de la légitimation de ces mécanismes (1); de l'application des principes de qualité des données et de proportionnalité (2); de la diffusion d'informations claires et complètes sur ledit mécanisme (3); des droits de la personne mise en cause (4); de la sécurité du traitement des informations (5); de la gestion des mécanismes internes de dénonciation (6); des transferts internationaux de données (7); des obligations de notification et de vérification préalable (8).

1. Légitimation des dispositifs d'alerte professionnelle (article 7 de la directive 95/46/CE)

La légalité du mécanisme de dénonciation dépend de la légitimité du traitement des données à caractère personnel et de sa conformité avec l'une des justifications énoncées à l'article 7 de la directive relative à la protection des données.

Actuellement, deux justifications semblent être pertinentes dans ce contexte: l'établissement d'un mécanisme de dénonciation est nécessaire au respect d'une obligation légale (article 7(c)) ou à la réalisation d'un intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées (article 7, point (f))[8].

[8] Les entreprises doivent être conscientes du fait que dans certains États membres, le traitement des données relatives à des infractions pénales alléguées est soumis à d'autres conditions spécifiques concernant la légitimité de ce traitement (voir infra, section IV, 8).

i) Nécessité d'établir un mécanisme de dénonciation pour respecter une obligation légale à laquelle le responsable du traitement est soumis (article 7, point c))

L'établissement d'un mécanisme de signalement doit avoir pour objectif de remplir une obligation légale imposée par la législation communautaire ou celle des États membres, en particulier dans le but de mettre en place des procédures de contrôle interne dans des secteurs bien définis.

À l'heure actuelle, cette obligation existe dans la plupart des États membres de l'UE dans le secteur bancaire, par exemple lorsque les gouvernements décident de renforcer le contrôle interne, notamment en ce qui concerne les activités des sociétés de crédit et d'investissement.

Cette obligation légale de mettre en place des mécanismes de contrôle renforcés existe également dans le contexte de la lutte contre la corruption, notamment à la suite de la transposition en droit interne de la Convention sur la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales (convention de l'OCDE du 17 décembre 1997).

En revanche, une obligation imposée par une loi ou un règlement étrangers qui exigeraient l'établissement de systèmes de signalement ne saurait être qualifiée d'obligation légale légitimant le traitement des données dans l'UE. Toute autre interprétation permettrait à des législations étrangères de contourner les règles fixées par l'UE avec la directive 95/46/CE. En conséquence, les dispositions de la loi SOX relatives à la dénonciation ne sauraient être considérées comme légitimant ce traitement sur le fondement de l'article 7, point c).

Toutefois, dans certains États membres de l'UE, des dispositifs d'alerte professionnelle pourraient être nécessaires en vertu d'obligations juridiques découlant du droit national dans les mêmes domaines que ceux couverts par la loi SOX[9]. Dans d'autres pays de l'UE où ces obligations juridiques n'existent pas, le même résultat peut néanmoins être atteint sur le fondement de l'article 7, point f).

ii) Nécessité d'établir un mécanisme de dénonciation aux fins de la réalisation de l'intérêt légitime poursuivi par le responsable du traitement [article 7, point f)]

L'établissement de systèmes de signalement peut être jugé nécessaire à la réalisation d'un intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées [article 7, point f)]. Cette justification n'est acceptable qu' «à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée».

---

[9] Code néerlandais sur le gouvernement d'entreprise, 9.12.2003, section II, 1.6.

Projet espagnol de code unifié sur la gouvernance des sociétés cotées, chapitre IV, 67(1)d). Ce code doit encore être examiné par l'autorité espagnole compétente en matière de protection des données afin d'examiner les implications dans ce domaine.

Les principales organisations internationales, y compris l'UE[10] et l'OCDE[11], ont reconnu l'importance des principes relatifs au bon gouvernement d'entreprise pour garantir un bon fonctionnement des organisations. Les principes ou les orientations définis par ces organisations appellent au renforcement de la transparence, à l'adoption de pratiques de bonne gestion financière et comptable et donc à l'amélioration de la protection des parties intéressées et de la stabilité financière des marchés. Ces textes reconnaissent en particulier l'intérêt d'une organisation à mettre en place des procédures appropriées permettant aux employés de signaler au conseil d'administration ou à la commission de vérification des comptes toute irrégularité et pratique douteuse en matière de comptabilité ou de vérification des comptes. Ces procédures de signalement doivent prévoir toutes les modalités nécessaires à la proportionnalité et à l'indépendance de l'enquête sur les faits rapportés, ce qui suppose une procédure appropriée de sélection des personnes chargées de la gestion du mécanisme et un suivi adéquat.

Toutefois, ces règles et orientations mettent l'accent sur la protection des dénonciateurs et l'existence de garanties appropriées protégeant ceux-ci contre les représailles (mesures discriminatoires ou disciplinaires)[12].

En effet, l'objectif de garantie de la sécurité financière sur les marchés financiers internationaux et notamment de prévention de la fraude et de la commission de fautes dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit et de l'information comptable, ainsi que de la lutte contre la corruption, la criminalité bancaire et financière ou les délits d'initiés, apparaît comme un intérêt légitime de l'employeur justifiant le traitement des données à caractère personnel par le biais de dispositifs d'alerte professionnelle dans ces domaines. Une entreprise publique, en particulier cotée sur les marchés financiers, a particulièrement intérêt à veiller à ce que les signalements de prétendues manipulations comptables ou de fautes dans la vérification des comptes - actes qui peuvent avoir une incidence sur les comptes de la société et affecter les intérêts légitimes des parties intéressées dans la stabilité financière de l'entreprise - soient effectivement transmis au conseil d'administration en vue d'un suivi adéquat.

Dans ce contexte, la loi américaine Sarbanes-Oxley peut être considérée comme une initiative adoptée pour veiller à la stabilité des marchés financiers et à la protection des intérêts légitimes des parties intéressées, puisqu'elle fixe des règles qui garantissent le bon gouvernement d'entreprise.

Pour l'ensemble de ces raisons, le groupe de travail considère 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.

Toutefois, l'article 7, point f), exige de maintenir un juste équilibre entre l'intérêt légitime poursuivi lors du traitement des données à caractère personnel et la protection des doits

---

[10] Communauté européenne: 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 (JO L 52 du 25.2.2005, p. 51).

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

[12] Voir, par exemple, la loi britannique sur la divulgation dans l'intérêt général de 1998 (*Public Interest Disclosure Act*).

fondamentaux des personnes concernées. Cet équilibre fondé sur le critère de l'intérêt légitime devrait prendre en considération les questions de proportionnalité, de subsidiarité et de gravité des infractions alléguées qui peuvent être notifiées, ainsi que les conséquences pour les personnes concernées. Pour maintenir cet équilibre fondé sur le critère de l'intérêt, les garanties appropriées devront également être mises en place. En particulier, l'article 14 de la directive 95/46/CE prévoit que, lorsque le traitement des données se fonde sur l'article 7, point f), la personne concernée a le droit de s'opposer à tout moment, pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet d'un traitement. Ces aspects sont développés ci-dessous.

2. Application des principes de qualité des données et de proportionnalité (article 6 de la directive sur la protection des données)

Aux termes de la directive 95/46/CE, les données à caractère personnel doivent être traitées loyalement et licitement;[13] elles doivent être collectées pour des finalités déterminées, explicites et légitimes[14] et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. En outre, les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement[15]. Combinées entre elles, ces règles sont parfois désignées comme constituant le «principe de proportionnalité». Enfin, des mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes soient effacées ou rectifiées[16]. L'application de ces règles essentielles en matière de protection des données comporte un certain nombre de conséquences quant à la façon dont les signalements peuvent être faits par les employés d'une organisation et être traités par celle-ci. Ces conséquences sont examinées ci-dessous.

i) Limitation possible du nombre de personnes autorisées à signaler des irrégularités ou fautes présumées par le biais de dispositifs d'alerte professionnelle

En application du principe de proportionnalité, le groupe de travail recommande que la société responsable du mécanisme de dénonciation examine attentivement s'il est opportun de limiter le nombre de personnes en droit de signaler de prétendues fautes par l'usage du mécanisme de dénonciation, notamment à la lumière de la gravité des manquements allégués. Le groupe de travail reconnaît néanmoins que les catégories de personnel énumérées peuvent parfois inclure l'ensemble des employés dans certains des domaines couverts par le présent avis.

Le groupe de travail est conscient du caractère déterminant des circonstances de chaque cas. Ainsi, il n'entend pas dicter de règles sur ce point et laisse le soin aux responsables du traitement des données, après vérification éventuelle par les autorités compétentes, de déterminer si ces restrictions sont opportunes dans les circonstances particulières auxquelles ils sont confrontés.

---

13 Article 6, paragraphe 1, point a), de la directive 95/46/CE
14 Article 6, paragraphe 1, point b), de la directive 95/46/CE
15 Article 6, paragraphe 1, point c), de la directive 95/46/CE
16 Article 6, paragraphe 1, point d), de la directive 95/46/CE

ii) Limitation possible du nombre de personnes susceptibles d'être mises en cause par le biais d'un mécanisme de dénonciation

En application du principe de proportionnalité, le groupe de travail recommande que la société mettant en place un mécanisme de dénonciation examine attentivement s'il est opportun de limiter le nombre de personnes susceptibles d'être mises en cause dans le cadre de ce mécanisme, notamment à la lumière de la gravité des infractions alléguées. Le groupe de travail reconnaît néanmoins que les catégories de personnel énumérées peuvent parfois inclure l'ensemble des employés dans certains des domaines couverts par le présent avis.

Le groupe de travail est conscient du caractère déterminant des circonstances de chaque cas. Ainsi, il n'entend pas dicter de règles sur ce point et laisse le soin aux responsables du traitement des données, après vérification éventuelle par les autorités compétentes, de déterminer si ces restrictions sont opportunes dans les circonstances particulières auxquelles ils sont confrontés.

iii) Préférence accordée aux signalements confidentiels dont l'auteur est identifié par rapport aux signalements anonymes

La question de savoir si les dispositifs d'alerte professionnelle doivent permettre de faire des signalements anonymes plutôt qu'ouverts (c'est-à-dire avec identification de l'auteur mais en respectant en tout cas la confidentialité) mérite une attention particulière.

L'anonymat n'est peut-être pas une bonne solution, que ce soit pour le dénonciateur ou l'organisation, pour un certain nombre de raisons:

- l'anonymat ne fait pas obstacle à ce que d'autres réussissent à deviner l'identité de la personne qui a soulevé le problème;
- il est plus difficile d'enquêter sur le problème si on ne peut pas poser de questions complémentaires;
- il est plus facile de protéger le dénonciateur contre les représailles, en particulier si cette protection est prévue par la loi[17], si les problèmes sont soulevés ouvertement;
- les signalements anonymes peuvent conduire à une focalisation sur le dénonciateur, en soupçonnant peut-être chez lui une intention malveillante;
- l'organisation risque de développer une culture de signalements anonymes malveillants;
- le climat social dans l'organisation peut se détériorer si les employés savent que des signalements anonymes les concernant peuvent être faits par le biais de ce mécanisme à tout moment.

Sous l'angle des règles relatives à la protection des données, les signalements anonymes soulèvent un problème spécifique en rapport avec la condition essentielle que les données à caractère personnel ne peuvent être collectées que loyalement. En règle générale, le groupe de travail considère que seuls les signalements dont l'auteur est identifié peuvent être communiqués par le biais des dispositifs d'alerte professionnelle pour respecter cette exigence.

---

[17] Par exemple, en vertu du *UK Public Interest Disclosure Act*.

Toutefois, le groupe de travail est conscient du fait que certains dénonciateurs peuvent ne pas toujours être en mesure de faire des signalements en s'identifiant ou peuvent ne pas y être disposés psychologiquement. Il sait également que les plaintes anonymes sont une réalité dans les sociétés, même et particulièrement en l'absence de dispositifs d'alerte professionnelle confidentiels organisés, et que cette réalité ne peut être ignorée. Le groupe de travail considère donc que la prise de mesures à partir de signalements anonymes est possible dans le cadre de dispositifs d'alerte professionnelle, mais que cela doit rester une exception et se faire dans les conditions énoncées ci-dessous.

Le groupe de travail considère que les dispositifs d'alerte professionnelle devraient être conçus de manière à ne pas encourager la perception des signalements anonymes comme étant la règle habituelle. En particulier, les sociétés ne doivent pas promouvoir la possibilité de faire des signalements anonymes par le biais de ce mécanisme. Au contraire, puisque les dispositifs d'alerte professionnelle doivent permettre de garder l'identité du dénonciateur confidentielle, une personne qui entend faire un signalement dans ce cadre doit savoir qu'elle ne subira pas de préjudice en raison de son action. C'est pourquoi il convient d'informer le dénonciateur, dès qu'il a recours au mécanisme, que son identité restera confidentielle à tous les stades du processus et en particulier ne sera pas divulguée à des tiers, que ce soit à la personne mise en cause ou à la hiérarchie de l'employé. Si, malgré ces informations, la personne ayant recours au mécanisme veut toujours rester anonyme, son signalement sera accepté dans le système. Il est également nécessaire d'informer les dénonciateurs qu'il peut être nécessaire de divulguer leur identité aux personnes intéressées participant à une autre enquête ou procédure judiciaire engagée ultérieurement à la suite de l'enquête menée dans le cadre du mécanisme de dénonciation.

Les signalements anonymes doivent être traités avec une précaution particulière. Il peut être nécessaire, par exemple, que le premier destinataire du signalement se penche sur son admissibilité et l'opportunité de sa diffusion dans le cadre du mécanisme. Il pourrait également être utile d'examiner s'il convient d'enquêter sur les signalements anonymes et de les traiter plus rapidement que les plaintes confidentielles en raison du risque d'abus. Cette précaution spéciale ne signifie toutefois pas que les signalements anonymes doivent être traités sans examiner attentivement tous les faits en cause – au contraire, leur traitement doit être identique à celui des notifications ouvertes.

iv) Proportionnalité et exactitude des données collectées et traitées

Aux termes de l'article 6, paragraphe 1, points b) et c), de la directive relative à la protection des données, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes et doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement.

L'objectif du système de signalement étant de garantir le bon gouvernement d'entreprise, les données collectées et traitées par le biais d'un mécanisme de dénonciation doivent se limiter aux faits ayant un rapport avec cette finalité. Les sociétés qui mettent en place de tels systèmes doivent clairement définir le type d'informations à divulguer par ce biais, en limitant celles-ci aux domaines de la comptabilité, des contrôles comptables internes, de l'audit ou de la criminalité bancaire et financière et de la lutte contre la corruption. Il est admis que dans certains pays, la loi peut expressément prévoir d'appliquer les

dispositifs d'alerte professionnelle à d'autres catégories de dysfonctionnements graves qu'il faut peut-être porter au grand jour dans l'intérêt général[18], mais ces mécanismes ne relèvent pas du champ d'application du présent avis; ils peuvent en effet ne pas être appliqués dans d'autres pays. Les données à caractère personnel traitées dans le cadre de ce mécanisme doivent se limiter aux données strictement et objectivement nécessaires pour vérifier les allégations faites. En outre, les plaintes doivent être séparées des autres données à caractère personnel.

Lorsque les faits signalés dans le cadre d'un mécanisme de dénonciation ne se rapportent pas aux domaines couverts par celui-ci, ils peuvent être communiqués aux employés compétents de la société ou de l'organisation si les intérêts vitaux de la personne concernée par ces données ou l'intégrité morale d'employés sont en jeu, ou s'il existe, en vertu du droit national, une obligation légale de communiquer ces informations aux pouvoirs publics ou aux autorités de poursuites compétentes.

v) Respect des durées strictement limitées de conservation des données

La directive 95/46/CE dispose que les données à caractère personnel traitées sont conservées 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 est essentiel pour garantir le respect du principe de proportionnalité du traitement des données à caractère personnel.

Les données à caractère personnel traitées dans le cadre d'un mécanisme de dénonciation devraient être supprimées rapidement, et généralement dans un délai de deux mois à compter de l'aboutissement de l'enquête sur les faits signalés.

Ces délais varient 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. En pareil cas, les données à caractère personnel devraient être conservées jusqu'au terme de ces procédures et jusqu'à l'expiration du délai de recours. Ces durées de conservation seront déterminées par la loi de chaque État membre.

Les données à caractère personnel en rapport avec des signalements que l'autorité chargée du traitement juge non fondés devraient être supprimées dans les plus brefs délais.

En outre, toute réglementation nationale concernant l'archivage des données dans la société reste d'application. Ces réglementations peuvent notamment prévoir l'accès aux données conservées dans ces archives et préciser les conditions de cet accès, les catégories de personnes qui peuvent avoir accès à ces fichiers, ainsi que toute autre règle pertinente en matière de sécurité.

3. Diffusion d'informations claires et complètes sur le mécanisme (article 10 de la directive relative à la protection des données)

L'exigence d'informations claires et complètes sur le mécanisme oblige le responsable du traitement des données à fournir aux personnes concernées des informations sur l'existence, la finalité et le fonctionnement du mécanisme, les destinataires des

[18] Voir, par exemple, la loi britannique sur la divulgation dans l'intérêt général de 1998 (*Public Interest Disclosure Act*).

signalements et les droits d'accès, de rectification et de suppression conférés aux personnes mises en cause.

Les responsables du traitement des données devraient également fournir des informations sur le fait que l'identité du dénonciateur restera confidentielle pendant tout le processus et que tout abus du système peut aboutir à l'adoption de mesures à l'encontre de l'auteur de cet abus. D'autre part, les utilisateurs du système peuvent également être informés qu'ils ne feront l'objet d'aucune sanction s'ils ont recours au mécanisme en toute bonne foi.

4. Droits de la personne mise en cause

Le cadre juridique de la directive 95/46/CE met en particulier l'accent sur la protection des données à caractère personnel de la personne concernée. En conséquence, du point de vue de la protection des données, les dispositifs d'alerte professionnelle devraient être axés sur les droits de la personne concernée, sans préjudice des droits du dénonciateur. Un équilibre des intérêts devrait être établi entre les droits des parties concernées, y compris les besoins légitimes de la société en matière d'enquête.

i) Droits d'information

L'article 11 de la directive 95/46/CE exige d'informer les personnes lorsque leurs données personnelles sont collectées auprès d'un tiers et non directement auprès d'elles.

La personne mise en cause dans le signalement du dénonciateur est informée par la personne chargée du mécanisme dans les plus brefs délais après l'enregistrement des données la concernant. En vertu de l'article 14, elle a également le droit de s'opposer au traitement de ses données si la légitimité du traitement se fonde sur l'article 7, point f). Ce droit d'opposition ne peut toutefois être exercé que pour des raisons prépondérantes et légitimes tenant à sa situation particulière.

En particulier, l'employé faisant l'objet du signalement doit être informé 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.

Toutefois, lorsqu'il y a un risque sérieux que cette notification compromette la capacité de la société d'enquêter efficacement sur les faits allégués ou de collecter les preuves nécessaires, l'information de la personne mise en cause peut être retardée aussi longtemps que ce risque existe. Cette exception à la règle de l'article 11 vise à sauvegarder les preuves en empêchant leur destruction ou leur modification par la personne mise en cause. Elle doit s'appliquer de manière restrictive, au cas par cas, et doit tenir compte des intérêts plus larges qui sont en jeu.

Le mécanisme de dénonciation doit prévoir les mesures nécessaires pour garantir que les informations divulguées ne seront pas détruites.

ii) Droits d'accès, de rectification et d'effacement des données

L'article 12 de la directive 95/46/CE donne à la personne concernée la possibilité d'avoir accès aux données enregistrées la concernant afin de vérifier leur exactitude et les rectifier si elles sont erronées, incomplètes ou ne sont pas à jour (droits d'accès et de rectification). En conséquence, l'établissement d'un système de signalement doit garantir

le respect du droit d'accès et du droit de rectification des données incorrectes, incomplètes ou non à jour.

Toutefois, l'exercice de ces droits peut être restreint afin d'assurer la protection des droits et des libertés d'autres personnes impliquées dans le système. Cette restriction devrait s'appliquer au cas par cas.

En aucun cas la personne mise en cause dans un signalement ne saurait obtenir du système des informations sur l'identité du dénonciateur en invoquant son droit d'accès, sauf si le dénonciateur fait une fausse déclaration à des fins malveillantes. Dans tous les autres cas, la confidentialité de l'identité du dénonciateur doit toujours être garantie.

En outre, les personnes concernées ont le droit de rectifier ou d'effacer leurs données lorsque le traitement de celles-ci n'est pas conforme aux dispositions de la directive, en raison notamment de la nature incomplète ou inexacte des données [article 12, point b)].

5. Sécurité des opérations de traitement (article 17 de la directive 95/46/CE)

i) Mesures concrètes de sécurité

Conformément à l'article 17 de la directive 95/46/CE, la société ou l'organisation responsable du mécanisme de dénonciation met en oeuvre les mesures techniques et d'organisation appropriées pour protéger les données collectées, diffusées ou conservées. L'objectif est de protéger ces données contre la destruction accidentelle ou illicite, la perte accidentelle, la diffusion ou l'accès non autorisés.

Les signalements peuvent être collectés par tout moyen de traitement des données, électronique ou non. Ces moyens devraient être réservés au système de dénonciation afin de prévenir tout écart par rapport à sa finalité initiale et renforcer la confidentialité des données.

Ces mesures de sécurité doivent être proportionnées aux finalités de l'enquête sur les problèmes soulevés, conformément aux règles de sécurité fixées dans les différents États membres.

Lorsque le mécanisme de dénonciation est mis en oeuvre par un fournisseur de services externe, le responsable du traitement des données doit conclure un contrat de conformité et, notamment, prendre toutes les mesures appropriées pour garantir la sécurité des informations traitées pendant tout le processus.

ii) Confidentialité des signalements faits dans le cadre de dispositifs d'alerte professionnelle

La confidentialité des signalements est une nécessité absolue pour respecter l'obligation de sécurité des opérations de traitement prévue par la directive 95/46/CE.

Pour respecter la finalité du mécanisme de dénonciation et encourager l'utilisation de ce système ainsi que le signalement de faits derrière lesquels peuvent se cacher des fautes ou des actes illicites de la société, il est essentiel que l'auteur du signalement soit suffisamment protégé, en garantissant la confidentialité du signalement et en empêchant les tiers de connaître son identité.

Les sociétés mettant en place des dispositifs d'alerte professionnelle doivent adopter des mesures appropriées visant à garantir que l'identité des dénonciateurs reste confidentielle et ne soit pas divulguée à la personne mise en cause au cours de l'enquête. Toutefois, s'il s'avère qu'un signalement est infondé et que le dénonciateur a fait une fausse déclaration par malveillance, la personne mise en cause pourra vouloir agir en diffamation, auquel cas l'identité des dénonciateurs devra éventuellement lui être révélée si le droit national le permet. Les législations et les principes de droit nationaux relatifs à la dénonciation des dysfonctionnements en matière de gouvernement d'entreprise prévoient aussi que le dénonciateur ayant eu recours au système est protégé contre les représailles telles que les mesures disciplinaires ou discriminatoires prises par la société ou l'organisation.

La confidentialité des données à caractère personnel doit être garantie lorsque celles-ci sont collectées, divulguées ou stockées.

6. Gestion des dispositifs d'alerte professionnelle des dysfonctionnements

Dans les dispositifs d'alerte professionnelle, la façon dont les signalements sont collectés et traités mérite une attention particulière. Si le groupe de travail donne la préférence à la gestion interne du système, il reconnaît néanmoins que les sociétés ont la faculté d'utiliser les services de fournisseurs externes à qui elles sous-traitent une partie de cette gestion, principalement la collecte des signalements. Ces fournisseurs externes doivent être liés par une obligation de confidentialité stricte et s'engager à respecter les principes relatifs à la protection des données. Quel que soit le système mis en place par la société, celle-ci doit se conformer notamment aux articles 16 et 17 de la directive.

i) Organisation interne spécifique de la gestion des dispositifs d'alerte professionnelle

Une organisation spécifique doit être mise en place au sein de la société ou du groupe en rapport avec le traitement des signalements et la conduite des enquêtes.

Cette organisation doit comprendre des personnes spécialement qualifiées et chargées de cette tâche, dont le nombre sera limité et qui seront liées contractuellement par des obligations particulières de confidentialité.

Ce mécanisme de dénonciation doit être strictement distinct des autres services de la société, tels que la direction des ressources humaines.

Il garantit, s'il y a lieu, que les informations collectées et traitées sont exclusivement transmises aux personnes spécifiquement chargées, au sein de la société ou du groupe dont la société fait partie, de l'enquête ou de l'adoption des mesures nécessaires dans le cadre du contrôle des faits signalés. Les personnes qui reçoivent ces informations veillent à ce que les informations reçues soient traitées confidentiellement et respectent les mesures de sécurité.

ii) Possibilité d'utiliser des fournisseurs de services externes

Lorsque des sociétés ou groupes de sociétés ont recours à des fournisseurs de services externes pour sous-traiter une partie de la gestion du mécanisme de dénonciation, ils restent néanmoins responsables des opérations de traitement qui en résultent, étant donné que ces fournisseurs ne sont chargés que du «sous-traitement» au sens de la directive 95/46/CE.

Ces fournisseurs externes peuvent être des sociétés gérant des centres d'appel ou des sociétés ou cabinets d'avocats spécialisés dans la collecte de signalements et effectuant parfois eux-mêmes une partie des enquêtes nécessaires.

Ces fournisseurs externes doivent également se conformer aux principes de la directive 95/46/CE. Ils veillent, en vertu d'un contrat conclu avec la société pour laquelle le mécanisme est géré, à collecter et traiter les informations conformément aux principes de cette directive, et à traiter les informations pour les seules finalités déterminées pour lesquelles elles ont été collectées. En particulier, ils respectent les obligations strictes de confidentialité et ne communiquent les informations traitées qu'à des personnes désignées dans la société ou l'organisation responsable de l'enquête ou de l'adoption des mesures nécessaires dans le cadre du contrôle des faits signalés. Ils se conforment également aux délais de conservation des données qui lient le responsable du traitement. La société qui a recours à ces mécanismes, en sa qualité de responsable du traitement des données, est tenue de vérifier régulièrement le respect des principes de la directive par les fournisseurs externes.

iii) Principe d'enquête dans l'UE pour les sociétés de l'UE et exceptions

La nature et la structure des groupes multinationaux impliquent que les faits et les conclusions tirées des signalements peuvent devoir être partagés au sein du groupe dans son ensemble, y compris en dehors de l'UE.

Si l'on tient compte du principe de proportionnalité, la nature et la gravité de l'infraction alléguée doivent en principe déterminer à quel niveau, et donc dans quel pays, le signalement doit être examiné. En règle générale, le groupe de travail estime que les groupes doivent traiter 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.

Le groupe de travail admet toutefois certaines exceptions à cette règle.

Les données reçues dans le cadre du mécanisme de dénonciation peuvent être communiquées au sein du groupe si cette communication est nécessaire aux fins de l'enquête (en fonction de la nature ou de la gravité des fautes signalées) ou découle de la composition du groupe. Cette communication sera considérée comme nécessaire pour les besoins de l'enquête, par exemple si le signalement met en cause un partenaire d'une autre société du groupe, un cadre supérieur ou un directeur de la société concernée. Dans ce cas, ce n'est qu'en respectant les conditions de confidentialité et de sécurité que les données doivent être communiquées à l'organisation compétente de la personne morale destinataire, laquelle fournit les mêmes garanties en ce qui concerne la gestion des signalements par ce mécanisme que l'organisation chargée du traitement de ces signalements dans la société de l'UE.

7. Transferts vers les pays tiers

Les articles 25 et 26 de la directive 95/46/CE sont d'application lorsque les données à caractère personnel sont transférées vers un pays tiers. L'application des dispositions des articles 25 et 26 sera pertinente, notamment lorsque la société sous-traite une partie de la gestion du mécanisme de dénonciation à un fournisseur tiers établi en dehors de l'UE ou lorsque les données collectées dans le cadre des signalements sont diffusées à l'intérieur du groupe et transmises ainsi à des sociétés en dehors de l'UE.

Ces transferts sont particulièrement susceptibles de se produire dans le cas de filiales de sociétés de pays tiers établies dans l'UE.

Lorsque le pays tiers vers lequel les données sont envoyées ne garantit pas un niveau de protection suffisant, comme l'exige l'article 25 de la directive 95/46/CE, les données peuvent être transférées pour les raisons suivantes:

[1] si le destinataire des données à caractère personnel est une entité établie aux États-Unis qui a adhéré aux principes de la «sphère de sécurité» (*Safe Harbor*);

[2] si le destinataire a passé un contrat de transfert avec la société de l'UE transférant les données, en vertu duquel celle-ci apporte les garanties nécessaires, par exemple sur la base des clauses contractuelles standard publiées par la Commission européenne dans ses décisions des 15 juin 2001 ou 27 décembre 2004;

[3] si le destinataire dispose d'un ensemble de règles contraignantes internes à l'entreprise qui ont été dûment approuvées par les autorités compétentes en matière de protection des données.

8. Respect des obligations de notification

En application des articles 18 à 20 de la directive sur la protection des données, les sociétés qui mettent en place des dispositifs d'alerte professionnelle doivent se conformer aux obligations de notification aux autorités nationales de protection des données ou à l'obligation de vérification préalable par ces autorités.

Dans les États membres prévoyant cette procédure, les opérations de traitement pourraient être soumises à la vérification préalable de l'autorité nationale de protection des données, dans la mesure où ces opérations sont susceptibles de faire peser un risque particulier sur les droits et libertés des personnes concernées. Cela pourrait être le cas lorsque le droit national permet le traitement des données concernant de prétendues infractions pénales par des personnes morales privées à certaines conditions, par exemple avec vérification préalable par l'autorité de contrôle nationale compétente. Cela pourrait également être le cas lorsque l'autorité nationale considère que les opérations de traitement peuvent retirer aux personnes signalées un droit ou un bénéfice ou les exclure d'un contrat. La réponse à la question de savoir si ces opérations sont soumises à l'obligation de vérification préalable dépend de la législation nationale et de la pratique de l'autorité nationale de protection des données.

V – CONCLUSIONS

Le groupe de travail reconnaît que les dispositifs d'alerte professionnelle peuvent être utiles pour permettre à une société ou à une organisation de contrôler le respect des règles et des dispositions qu'elle a instaurées en matière de gouvernement d'entreprise, en particulier 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 et du droit pénal. Ces mécanismes peuvent permettre à une société de mettre dûment en oeuvre les principes de bon gouvernement d'entreprise et de détecter les faits qui auraient une incidence sur sa situation.

Le groupe de travail souligne que l'établissement de 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, qui fait l'objet du présent avis, doit être conforme aux principes de protection des données à caractère personnel, inscrits dans la directive 95/46/CE. Il considère que la conformité avec ces principes permet aux sociétés et aux dispositifs d'alerte professionnelle de garantir le bon fonctionnement de ces derniers. En effet, il est essentiel que dans la mise en oeuvre d'un mécanisme de dénonciation, le droit fondamental à la protection des données à caractère personnel, concernant tant le dénonciateur que la personne mise en cause, soit garanti d'un bout à l'autre du processus.

Le groupe de travail souligne que les principes de protection des données inscrits dans la directive 95/46/CE doivent être intégralement appliqués aux dispositifs d'alerte professionnelle, notamment en ce qui concerne les droits de la personne mise en cause à l'information, à l'accès au système, à la rectification et à l'effacement des données. Toutefois, compte tenu des différents intérêts en jeu, le groupe de travail reconnaît que l'exercice de ces droits peut être restreint dans des cas très spécifiques, afin de maintenir un juste équilibre entre le droit au respect de la vie privée et les intérêts poursuivis dans le cadre de la mise en oeuvre du mécanisme. Ces restrictions doivent toutefois être appliquées limitativement, dans la mesure où elles sont nécessaires pour atteindre les objectifs du mécanisme.

Fait à Bruxelles, le 1er février 2006

Par le groupe de travail

Le Président
Peter Schaar