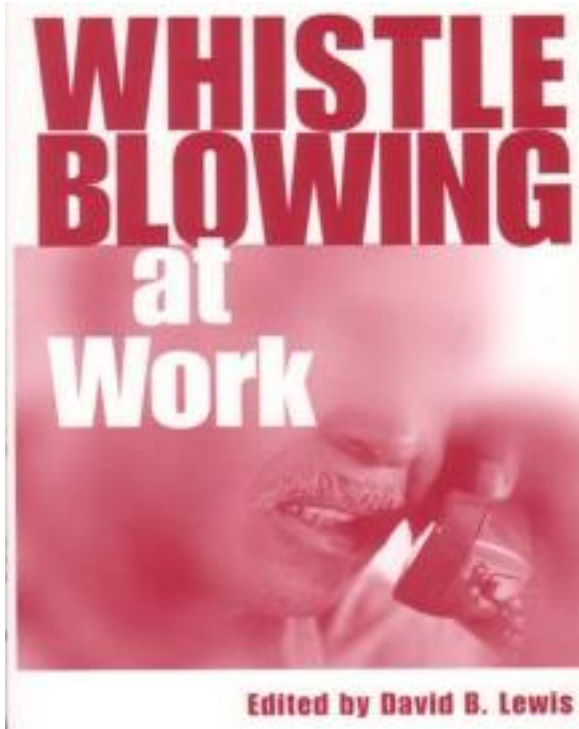




Commission nationale pour la protection des données

URL: <http://www.cnpd.lu/fr/dossiers/whistleblowing/index.html>

[Retour vers la page d'origine](#)



Le whistleblowing ou "déclenchement d'alerte" est un système de plus en plus employé par les entreprises afin d'enrayer les comportements frauduleux ou susceptible d'affecter sérieusement leur activité ou d'engager gravement leur responsabilité. Le système permet à des employés de signaler le comportement de leurs collègues de travail supposé contraire à la loi ou aux règles établies par l'entreprise.

En juillet 2002, suite aux scandales comptables et financiers que les Etats-Unis ont connu, avec la société Enron notamment, le Congrès américain a adopté la loi Sarbanes-Oxley, dite "SOX".

Cette loi impose en particulier aux sociétés américaines et étrangères cotées aux Etats-Unis (Nasdaq, NYSE, SEC), ainsi qu'à leurs filiales à l'étranger, de mettre en place un code d'éthique ou de conduite ainsi qu'un dispositif permettant aux salariés de rapporter anonymement les renseignements concernant des comportements contraires aux règles éthiques et les fraudes et malversations comptables et financières dont ils ont eu connaissance. Le système s'appuie généralement sur l'utilisation d'un numéro vert ou de l'intranet que les employés utilisent anonymement afin de dénoncer des pratiques qui leur semblent frauduleuses. Citons comme exemples, des employés qui dépensent des budgets inopinément, qui ne respectent pas les règles en matière d'appels d'offres ou, plus rarement, qui détournent des fonds.

- [Le groupe article 29 et la Commission Nationale pour la Protection des Données](#)
- [Les règles établies par le Groupe article 29 et les recommandations aux entreprises](#)
- [Principes de légitimité et de proportionnalité](#)
- [Protection du dénonciateur et anonymat](#)
- [Bénéfices de ces pratiques nouvelles et risques d'abus encourus](#)
- [Les recommandations à l'intention des entreprises](#)
- [Pour en savoir plus... \(liens et documents\)](#)

Le groupe article 29 et la Commission Nationale pour la Protection des Données

Le groupe de l'article 29, qui rassemble les représentants des vingt-cinq autorités européennes de protection des données, a trouvé urgent de prendre position sur la question de la licéité de ces dispositifs d'alerte au regard de la directive européenne 95/46/CE sur la protection des données. Il a ainsi chargé la délégation française, la Commission Nationale Informatique et Libertés (CNIL), conjointement avec le secrétariat du groupe, de rédiger un document de travail sur la question.

L'autorité de contrôle luxembourgeoise, la Commission Nationale pour la Protection des Données (CNPD), a participé à l'élaboration de cette orientation. La CNPD n'a pas encore eu à statuer formellement sur des questions liées au whistleblowing. En effet, contrairement à la loi française, la loi du 2 août 2002 ne confère pas à la Commission nationale de compétence d'autorisation en la matière : les entreprises basées au Luxembourg souhaitant installer un dispositif d'alerte professionnelle doivent effectuer une notification conformément aux articles 12 et 13 de la loi.

[↑ Haut de page](#)

Les règles établies par le Groupe article 29 et les recommandations aux entreprises

Le document adopté le 1er février 2006 statue sur les dispositifs d'alerte professionnelle dont le champ d'application se limite aux domaines bancaire, de la comptabilité, du contrôle interne des comptes, de l'audit, de la lutte contre la corruption et les infractions financières. A cette occasion, le groupe article 29 a abordé plusieurs aspects de la problématique dans son papier d'orientation.

Le groupe de coordination des autorités de contrôle européennes s'est tout d'abord penchée sur le rôle limité que les entreprises peuvent attribuer à un tel dispositif d'alerte et sur les circonstances susceptibles d'en faire un traitement de données à caractère personnel déloyal, car opéré à l'insu des personnes concernées et visant l'instauration d'un climat de suspicion et de délation généralisé au moyen du whistleblowing. Celui-ci doit être perçu comme mécanisme additionnel et subsidiaire pour rapporter des dysfonctionnements internes via un support spécifique et non en tant que dispositif se substituant au management interne de la société. Les dispositifs d'alerte professionnelle ne doivent pas remplacer les auditeurs internes ou le contrôle de qualité du personnel.

[↑ Haut de page](#)

Principes de légitimité et de proportionnalité

Le groupe article 29 a également rappelé l'importance du respect des grands principes de la protection des données personnelles dans le cadre du recours au whistleblowing. Il en ressort que la mise en place d'un dispositif d'alerte professionnelle doit se faire conformément à une obligation légale spécifique ou à un intérêt légitime conforme aux droits et libertés fondamentaux. Ainsi, le principe de légitimité des dispositifs est défini dans l'article 7 de la directive 95/46/CE et les principes de qualité et de proportionnalité des données dans l'article 6 de cette même directive. Il découle de cet article 6 que les finalités des dispositifs d'alerte professionnelle doivent être spécifiées, explicites et légitimes. Le groupe article 29 juge fondamental la balance des intérêts entre proportionnalité, subsidiarité et fiabilité des faits dénoncés.

Le critère de proportionnalité renvoie également à la question de la limitation possible du nombre de personnes chargées de rapporter les dysfonctionnements. Le groupe article 29 s'inquiète en effet du sérieux des personnes qui en ont la charge. De même, la limitation du nombre de personnes pouvant être incriminées a été soulevée. L'autorité de contrôle européenne a décidé d'en laisser la compétence aux chargés de protection et aux autorités nationales compétentes. Le respect du principe de proportionnalité implique encore que les dispositifs définissent à l'avance le type d'informations qui peuvent être dénoncées.

[↑ Haut de page](#)

Protection du dénonciateur et anonymat

La protection du dénonciateur est un autre thème abordé dans la prise en position. Selon cette dernière, la sécurité de la personne qui utilise le dispositif d'alerte doit être assurée contre d'éventuelles représailles. Le groupe article 29 note qu'il existe des protections pour le rapporteur mais pas pour l'accusé. La personne accusée encoure ainsi un risque accru de stigmatisation de la part des autres collègues.

Concernant l'anonymat, le groupe article 29 précise que seules les dénonciations identifiées doivent être communiquées par « whistleblowing », par opposition à des dénonciations anonymes. Celles-ci peuvent en effet s'avérer calomnieuses et poser un certain nombre de contraintes : Difficultés de poser des questions aux autres employés dans le cadre d'une enquête, représailles infondées et risques de développer une véritable culture de dénonciations calomnieuses. Il se peut que le dénonciateur n'ait pas la disposition psychologique pour remplir un rapport de dénonciation mais le groupe article 29 estime que les dénonciations au sein des entreprises sont inévitables et qu'il est dès lors préférable qu'elles soient faites via des dispositifs prévus à cet effet. Par ailleurs, le dénonciateur doit être informé du fait qu'il n'encoure aucune sanction ce faisant et que sa dénonciation restera confidentielle tout au long du processus. Si malgré tout, il désire rester anonyme, le dispositif doit prendre sa plainte en compte mais l'entreprise doit éviter que de la publicité encourageant les dénonciations anonymes soit faite.

[↑ Haut de page](#)

Bénéfices de ces pratiques nouvelles et risques d'abus encourus

La mise en place de systèmes d'alerte professionnelle comprend un certain nombre de dangers et notamment :

- le risque de mise en place d'un système organisé de délation professionnelle notamment du fait de l'anonymat de la personne dénonciatrice ;
- la disproportion entre les dispositifs et les objectifs poursuivis ;
- la déloyauté de la collecte et du traitement des données pour la personne n'ayant pas les moyens de s'opposer et de se défendre.

[↑ Haut de page](#)

Les recommandations à l'intention des entreprises

En outre, les organismes de protection de données doivent préconiser quatre règles principales pour faire face à ces contraintes :

- La nécessité de restreindre le dispositif d'alerte au domaine comptable, du contrôle des comptes, bancaire et de la lutte contre la corruption ;
- Le fait de décourager les dénonciations anonymes en assurant, dans la mesure du possible, l'identification des auteurs d'alerte;
- La mise en place d'une organisation spécifique pour recueillir et traiter les alertes. La ou les personnes chargées du dispositif d'alerte doivent être formées et astreintes à une obligation de confidentialité quant aux données dont elles prennent connaissance ;
- L'information de la personne concernée dès que les preuves ont été préservées, afin de lui permettre d'exercer ses droits d'opposition, d'accès et de rectification.

Dernière mise à jour de cette page le 30-06-2006.
Copyright Commission nationale pour la protection des données

[Retour vers la page d'origine](#)