# *Whistleblowing : quand un rapport propose d'élargir le domaine de l'alerte professionnelle, la CNIL siffle le hors-jeu*

*Anne Carlevaris*
*Diplômée IEP Paris (OI 2002)*

*Email : carlevarisanne@yahoo.fr*

*Brad Spitz*
*Docteur en Droit*
*Avocat au barreau de Paris*
*Chargé d'enseignement à l'Université de Paris 1 (Panthéon-Sorbonne)*

*Email : brad@bradspitz.com*

Le Ministre délégué à l'emploi, au travail et à l'insertion professionnelle des jeunes, a commandé un rapport[1] destiné à dresser un bilan des relations entre droit du travail, chartes d'éthique et systèmes d'alerte professionnelle (ci-après le « Rapport »). Le Rapport, qui lui a été remis le 7 mars 2007, propose des voies d'évolution possibles, notamment la rédaction d'une loi.

Actuellement, la France ne dispose pas de texte législatif sur les « alertes professionnelles ». Cette expression fait référence au terme anglais *whistleblowing*, souvent indifféremment traduit en français, peut-être à tort, par « alerte professionnelle », « alerte éthique » ou encore « ligne éthique ». La *Commission Nationale de l'Informatique et des Libertés* (CNIL) définit le dispositif d'alerte professionnelle comme « *un 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* »[2]. La CNIL a admis le principe de l'alerte professionnelle, mais en restreignant son champ à des domaines précis : comptabilité, contrôle des comptes, domaine bancaire, corruption[3] ; l'objectif était de permettre aux sociétés françaises de se conformer à la fois aux exigences de la loi américaine *Sarbanes-Oxley*[4], qui impose la mise en place de systèmes de « *whistleblowing* », et aux dispositions de la loi française « Informatique et Libertés »[5].

Le Rapport propose d'introduire dans le Code du travail des règles spécifiques permettant aux entreprises de mettre en place des dispositifs organisant la possibilité de signaler non seulement des actes contraires aux dispositifs législatifs ou réglementaires et des atteintes aux droits des personnes et à la santé des salariés, mais également des actes contraires à des règles d'origine éthique ou professionnelle. Le Rapport prend ainsi acte du rôle économique des chartes d'éthiques, véritables « *instruments de gestion économique* »[6]. Le Rapport considère en effet que l'éthique d'entreprise est « *devenue une source affichée de règles comportementales de l'entreprise et dans l'entreprise qui contribue à sa réussite économique* »[7], permettant de « *fédérer les hommes et les femmes de l'entreprise autour de certaines valeurs qui déterminent des comportements* »[8]. L'objectif n'est plus de permettre aux sociétés françaises de se conformer aux dispositions de la loi *Sarbanes-Oxley*, mais

[1] *Chartes d'éthique, alerte professionnelle et droit du travail français : état des lieux et perspective*, Rapport établi par Paul-Henri Antonmattei et Philippe Vivien et remis à Gérard Larcher, Ministre délégué à l'emploi, au travail et à l'insertion professionnelle des jeunes.
[2] Délibération n° 2005-305 du 8 décembre 2005 portant autorisation unique de traitements de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle (décision d'autorisation unique n° AU-004).
[3] *Ibid*.
[4] *Public Company Accounting Reform and Investor Protection Act*, 2002. Cette loi a été adoptée suite aux scandales des affaires *Enron* et *Worldcom*.
[5] Loi du 6 janvier 1978, modifiée par la 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.
[6] Rapport, précité, paragraphe n° 50.
[7] Rapport, précité, paragraphe n° 3 et 4.
[8] Rapport, précité, paragraphe n° 4.

bien plus largement de leur permettre de mettre en place des systèmes d'alerte éthique, tels que, par exemple, celui qui avait été présenté par la société *McDonald's France* à la CNIL en 2005[9]. Le dispositif en cause s'inscrivait dans le cadre du « code d'éthique » du groupe international *McDonald's*, et incitait les collaborateurs des filiales françaises du groupe à alerter la société mère américaine sur les comportements supposés contraires aux règles légales françaises, mais aussi au code d'éthique du groupe. La CNIL n'a pas autorisé la mise en œuvre du dispositif d'intégrité professionnelle, parce qu'un tel dispositif risquait de « *conduire à un système organisé de délation professionnelle* ».

A la présentation du Rapport, la CNIL, gardienne de la vie privée et des libertés individuelles, s'est empressée de rappeler, dans un communiqué, les règles qu'elle a posées en la matière, en précisant notamment que le dispositif d'alerte doit garder un champ spécifique restreint[10].

**1. Les règles posées par la CNIL en matière de dispositifs d'alerte professionnelle : un champ restreint**

Les dispositifs d'alerte professionnelle, qui conduisent à des traitements de données personnelles, tombent sous le coup de la loi « Informatique et libertés ». Bien que dans un premier temps hostile à tout dispositif de cette nature, car jugé contraire aux dispositions de la loi « Informatique et Libertés » du 6 janvier 1978, la CNIL a dû faire évoluer ses positions pour répondre à des difficultés nouvelles. Conformément au principe d'extraterritorialité, les entreprises françaises et les filiales françaises de sociétés américaines côtées à la bourses de New York ont eu à se conformer à la loi *Sarbanes-Oxley* du 30 juillet 2002[11], notamment en mettant en place des systèmes d'alerte professionnelle. Ces entreprises se sont donc retrouvées dans une situation délicate : devoir mettre en place des procédures d'alertes en France, alors que la CNIL était réservée à leur encontre[12].

Par la suite, la CNIL a défini, dans un document d'orientation du 10 novembre 2005[13], les conditions de conformité des dispositifs d'alerte professionnelle. Dans un souci de simplification des procédures, la CNIL a ensuite adopté, sur la base de ce document, une décision d'autorisation unique fixant les conditions que les entreprises doivent respecter afin de pouvoir bénéficier d'une simplification des procédures à accomplir[14].

Le dispositif de l'alerte est restreint à un champ spécifique : les alertes professionnelles ne peuvent concerner que le domaine comptable, le contrôle des comptes, le domaine bancaire et celui de la lutte contre la corruption. Ce champ peut être exceptionnellement élargi dans le cas où l'intérêt vital de l'entreprise ou l'intégrité physique ou morale des salariés est en jeu. Résumant la position qu'elle a retenue dans sa Délibération du 8 décembre 2005, notamment aux articles 1 et 3, la CNIL a rappelé dans son communiqué que le champ du dispositif d'alerte est « *aujourd'hui défini comme celui du domaine comptable, du contrôle des comptes, bancaire et de la lutte contre la corruption (des alertes pouvant être exceptionnellement recueillies et traitées si elles s'avèrent concerner l'intérêt vital de l'entreprise ou l'intégrité physique ou morale des salariés)* »[15].

Les entreprises souhaitant mettre en place ce type de dispositifs doivent en outre porter un certain nombre d'éléments d'information à la connaissance de leurs employés. La CNIL a également indiqué que ces dispositifs ne devaient pas encourager les dénonciations anonymes[16]. L'émetteur de l'alerte

[9] Délibération n° 2005-110 du 26 mai 2005.

[10] « La CNIL rappelle les règles pour les dispositifs d'alerte professionnelle », Communiqué de la CNIL du 8 mars 2007, Site internet de la CNIL, http://www.cnil.fr .

[11] *Sarbanes-Oxley Act*, ratifié le 30 juillet 2002. En vertu de la loi *Sarbanes-Oxley*, les Présidents des entreprises cotées aux Etats-Unis doivent certifier leurs comptes auprès de l'organisme de régulation des marchés financiers américains (la *Securities and Exchanges Commission* -SEC).

[12] V. notamment Délibérations 2005-110 et 205-111 du 26 mai 2005.

[13] 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 « Informatique et Libertés ».

[14] Délibération n° 2005-305 du 8 décembre 2005 portant autorisation unique de traitements de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle (décision d'autorisation unique n° AU-004).

[15] Communiqué du 8 mars 2007, Site internet de la CNIL, http://www.cnil.fr.

[16] Elle se différencie en cela de la loi *Sarbanes-Oxley*, qui à sa section 301 indique que « *(le) comité chargé de la réception et du traitement des plaintes concernant la présentation des comptes et l'audit (…) doit garantir*

devra être identifiable, mais son identité ne sera pas révélée à la personne mise en cause[17]. La personne concernée devra être informée dès que les preuves auront été préservées.

L'article 8 de la Délibération sur l'autorisation unique protège également le salarié auteur de l'alerte puisque le « délateur » de bonne foi ne peut encourir de sanctions. En effet, si l'émetteur de l'alerte peut encourir des sanctions disciplinaires, voire judiciaires, en cas d'utilisation abusive du système, l'émetteur de bonne foi est en revanche à l'abri de telles sanctions, même si les faits dénoncés ne se sont par la suite pas révélés exacts.

**2. Les propositions du Rapport : élargissement du domaine de l'alerte professionnelle**

Le Rapport propose en premier lieu une définition de l'alerte beaucoup plus large que celle retenue par la CNIL. Ses auteurs considèrent en effet que ce n'est pas la source du manquement qu'il convient de prendre en considération pour déterminer le domaine des alertes, mais les conséquences du manquement sur le fonctionnement de l'entreprise, et en concluent que « *les actes contraires à des règles d'origine éthique ou déontologique peuvent être concernés dès lors qu'ils entraînent cet effet préjudiciable* »[18].

Le Rapport donne alors la définition suivante aux alertes professionnelles :

« *Un dispositif d'alerte professionnelle est un ensemble de règles organisant la possibilité pour un salarié ou toute autre personne exerçant une activité dans une entreprise de signaler au chef d'entreprise ou à d'autres personnes désignées à cet effet :*

- ***des actes contraires** à des dispositions législatives ou réglementaires, **aux dispositions des conventions et accords collectifs de travail applicables à l'entreprise ou à des règles d'origine éthique ou professionnelles**, qui nuisent gravement au fonctionnement de l'entreprise*
- *des atteintes aux droits des personnes et aux libertés individuelles qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché*
- *des atteintes à la santé physique et mentale des salariés* »[19].

Une telle définition élargirait considérablement le champ des alertes professionnelles et permettrait aux entreprises de mettre en œuvre des dispositifs de dénonciation des actes contraires aux chartes éthiques.

On peut toutefois se demander s'il est véritablement envisageable d'étendre ainsi le domaine de l'alerte professionnelle, notamment au regard du droit communautaire et plus particulièrement de la directive 95/46/CE 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. Comme le rappelle le *Groupe de travail « Article 29 »* sur la protection des données[20], dans un avis sur les dispositifs d'alerte professionnelle[21] adopté le 1er février 2006, la légalité d'un 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 précitée, deux justifications pouvant être pertinentes dans le contexte de l'alerte professionnelle : (i) l'établissement

*l'anonymat des collaborateurs qui signalent des défaillances (…)* » (« *COMPLAINTS – Each audit committee shall establish procedures for – (…) the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters.* »).

[17] Notons que ces précautions constituent des aménagements aux dispositions de la loi « Informatique et libertés » et plus précisément au principe du droit d'accès et de rectification d'une personne aux données la concernant (articles 39 et 40 de la Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004).

[18] Rapport, précité, paragraphe n° 42 (en gras dans le texte).

[19] Rapport, précité, paragraphe n° 49, souligné par nous.

[20] 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.

[21] 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.

d'un dispositif d'alerte nécessaire au respect d'une obligation légale (article 7(c)), ou (ii) la réalisation d'un intérêt légitime (article 7(f)). Aux termes de cet article, « *Les Etats membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si :* […] *c) il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ou* […] *f) il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement* ». La Cour de Justice des Communautés européennes a eu l'occasion de rappeler que tout traitement de données à caractère personnel doit être conforme à l'un des principes énumérés à cet article, et a précisé que ces dispositions sont directement applicables et peuvent donc être invoqués devant les juridictions nationales pour écarter des règles de droit interne contraires[22].

Or, d'une part, la possibilité donnée aux entreprises de mettre en œuvre des dispositifs de dénonciation des actes contraires aux chartes éthiques, telle qu'envisagée par le Rapport, dépasse le cadre de l'article 7 c) de la directive, dans la mesure où les systèmes de recueil de données pourraient concerner non seulement des faits contraires à la législation communautaire ou française, mais également des faits contraires aux règles de l'entreprise.

D'autre part, s'agissant de la justification de l'article 7 f), le *Groupe Article 29* définit restrictivement l'intérêt légitime de l'entreprise en précisant que 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 la lutte contre la corruption, la criminalité bancaire et financière, apparaît comme un intérêt légitime de l'entreprise pouvant justifier le dispositif d'alerte professionnelle[23].

Le Rapport propose ensuite la possibilité de mettre en place des dispositifs d'alerte par des conventions ou accords collectifs de branche ou de groupe, ou par décision du chef d'entreprise, ces conventions, accords ou décision devant fixer les éléments suivants :

> *« - les actes qui peuvent être signalés dans le cadre du dispositif*
> *- Les personnes susceptibles d'utiliser le dispositif*
> *- Les personnes dont les actes sont susceptibles d'être signalés*
> *- Les modalités de recueil et de traitement des actes signalés*
> *- Le nom ou la qualité des personnes intervenant dans le recueil ou le traitement de l'alerte.*
> *- Les modalités d'information de ou des personnes mises en cause.*
> *- Le caractère anonyme et/ou confidentiel de l'alerte.* »

Une certaine liberté serait ainsi laissée à l'entreprise pour fixer des éléments importants du dispositif d'alerte. Le Rapport semble notamment indiquer que l'entreprise pourrait décider de l'instauration de l'anonymat[24]. De même, alors que la CNIL, dans sa Délibération du 8 décembre 2005, a aménagé le droit d'information de la personne concernée de manière pragmatique mais très stricte, en prévoyant que la personne doit être informée dès que les preuves sont préservées[25], le Rapport semble proposer que l'entreprise puisse fixer elle-même les modalités d'information de la personne mise en cause. Si tel était le cas, on s'éloignerait de manière assez caractérisée des dispositions prévues par la CNIL[26].

---

[22] CJCE, affaires jointes C-465/00, C-138/01 et C-139/01 du 20 mai 2003, *Rechnungshof contre Osterreichischer Rundfunk e.a. et Christa Neukomm et Joseph Lauermann contre Osterreichischer Rundfunk*, spéc. paragraphe 101.

[23] Avis précité p. 9. Il est vrai que le *Groupe de l'Article 29* a également indiqué que les principes énoncés dans son avis allaient être complétés afin de vérifier si les mécanismes internes de dénonciation pouvaient être compatibles avec les règles de protection des données de l'Union européenne dans d'autres domaines. Ces domaines, qui feront l'objet d'un prochain avis, seront toutefois également spécifiques et un but légitime devra également être poursuivi ; les exemples cités sont les ressources humaines, la santé et la sécurité des travailleurs, l'environnement, les menaces écologiques et la commission d'infractions.

[24] Le Rapport précise à cet égard que « *Même si, à l'instar de la CNIL, nous considérons qu'il est préférable de connaître l'identité de l'émetteur tout en la traitant de manière confidentielle, possibilité doit être laissée dans certaines situations d'instaurer l'anonymat* ».

[25] Ce qu'elle a d'ailleurs rappelé dans son communiqué du 8 mars 2007, http://www.cnil.fr .

[26] Notons toutefois que le Rapport propose une protection de l'émetteur proche de celle prévue par les règles de la CNIL, puisqu'il prévoit qu'« *Aucun salarié ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire, directe ou indirecte,* […] *pour avoir utilisé de bonne foi un dispositif d'alerte professionnelle* ».

**Conclusion**

Les propositions émises par le Rapport élargissent considérablement le domaine de l'alerte professionnelle, justifiant ainsi la réaction rapide de la CNIL. Cette autorité de protection, qui doit être consultée sur tout projet de loi ou de décret relatif à la protection des personnes à l'égard des traitements automatisés[27], remplit parfaitement son rôle en précisant dans un communiqué les règles qu'elle a déjà posées en la matière. Il est intéressant à cet égard de souligner que l'avis du *Groupe Article 29* du 1er février 2006[28] reprend les grands principes issus du document d'orientation et de la Délibération de 2005 de la CNIL[29].

Si les auteurs du Rapport ne préconisent pas une intervention législative rapide sur cette question, souhaitant principalement nourrir le débat[30], la CNIL a selon nous raison de marquer son opposition à l'élargissement proposé ; permettre aux entreprises de mettre en place des systèmes de délation s'étendant aux violations des chartes d'éthique des entreprises, avec par conséquent un domaine potentiellement très large, constitue un danger réel pour les libertés individuelles que la CNIL est chargée de protéger.

[27] La CNIL propose également au Gouvernement les mesures législatives ou réglementaires d'adaptation de la protection des libertés à l'évolution des procédés et techniques informatiques (article 11, 4°, a et b de la loi n°78-17 du 6 janvier 1978).
[28] Avis précité.
[29] Cf. *supra.*
[30] Rapport précité, spéc. paragraphe n° 50.