REVUE DES DIRECTEURS SÉCURITÉ D'ENTREPRISE 3
2010

Sécurité & Stratégie

DOSSIER : 2010-2020, UNE NOUVELLE DÉCENNIE DE MENACES ?

ENQUÊTE EDHEC – CDSE :
«Panorama 2008-2009 des crimes commis contre les entreprises»
Bertrand Monnet, Philippe Very & Olivier Hassid

L'ÉCOTERRORISME : vers une 5ème vague terroriste nord-américaine ?
Benoît Gagnon

RÉGLEMENTATION

La Cour de Cassation recadre le périmètre de l'alerte des systèmes d'alerte professionnelle

Emmanuel Daoud - *Avocat associé*
Emilie Bailly - *Avocat*
Cabinet VIGO

La Cour de Cassation recadre le périmètre de l'alerte des systèmes d'alerte professionnelle

Dans un arrêt du 8 décembre 2009[1], la Cour de cassation se prononce pour la première fois dans un litige lié à un *«dispositif d'alerte professionnelle»*, connu sous le nom de *whistleblowing*. En effet, la chambre sociale de la Cour de cassation a annulé un dispositif d'alerte professionnelle, jugé non conforme au dispositif juridique posé par la CNIL dans sa délibération du 8 décembre 2005. Ce faisant, la Cour de Cassation rappelle que le champ des sujets pouvant faire l'objet d'une alerte professionnelle est strictement limité afin que le recours à de tels dispositifs demeure exceptionnel. Une occasion de faire le point sur le régime juridique des dispositifs d'alerte professionnelle.

Définition

L'expression *whistleblowing*, qui signifie littéralement «donner un coup de sifflet», se traduit en français par l'expression «dispositif d'alerte professionnelle». Le *whistleblowing* institue une procédure d'alerte permettant aux salariés d'une entreprise de dénoncer aux autorités ayant le pouvoir d'y mettre fin, les pratiques illicites dont ils auraient eu connaissance dans le cadre de leur activité professionnelle. Le principe peut paraître simple : donner au salarié les moyens de s'exprimer de manière confidentielle et rassurante. La réalité est plus compliquée. Elle se confronte à de nombreuses difficultés légales, culturelles et morales.

Historique

L'institutionnalisation du *whistleblowing* dans les entreprises vient des États-Unis. Il a été rendu obligatoire par la loi du 31 juillet 2002 (Pub. L. No. 107-204, 116 Stat. 745) dite Sarbanes-Oxley Act, prise à la suite des scandales financiers suscités par les affaires Enron et Worldcom. Cette loi américaine impose, en effet, aux entreprises cotées en Bourse à New York, ainsi qu'à leurs filiales étrangères, de mettre en place un système de déclenchement d'alerte permettant aux salariés de dénoncer les fraudes et les malversations comptables ou financières dont ils auraient connaissance.

Certaines entreprises françaises cotées en Bourse aux Etats-Unis, ainsi que les filiales françaises de sociétés américaines se sont donc trouvées dans l'obligation de se conformer au Sarbanes-Oxley Act.

La finalité d'un tel dispositif d'alerte est louable, puisqu'il relève d'une démarche de prévention des risques de fraudes et des dérives comptables, en permettant aux salariés de dénoncer, sans crainte de représailles, des comportements frauduleux, dans le seul but d'améliorer les performances de l'entreprise.

> Plusieurs polémiques publiques autour de procédures d'alerte créées par des entreprises en France ont révélé des divergences profondes tant juridiques que culturelles opposant les Etats-Unis à la France.

Pour autant, l'adoption de tels dispositifs dans les entreprises françaises *«a reçu un accueil pour le moins mitigé et juridiquement mouvementé»*[2]. Plusieurs polémiques publiques autour de procédures d'alerte créées par des entreprises en France ont révélé des divergences profondes tant juridiques que culturelles opposant les Etats-Unis à la France.

En effet, les Etats-Unis et la France ont une conception radicalement différente de la protection des données personnelles. En particulier, le souvenir très présent dans l'inconscient collectif français de l'Occupation allemande et de la collaboration active du gouvernement de Vichy a suscité bien des réserves. Pour autant, les dispositifs d'alerte professionnelle se sont développés en France, comme ailleurs. En effet, les entreprises sont partout confrontées à une exigence croissante de transparence, de meilleure gouvernance, de *compliance* et, à ce titre, ont de plus en plus besoin de compter sur la responsabilité et la loyauté de ceux qui les composent.

Les procédures d'alerte ne trouveront leur utilité que si elles sont perçues comme un moyen d'exercice de la responsabilité des salariés, et pas seulement un moyen de contrôle de tous par tous, que si elles sont conçues pour être au service non des intérêts des entreprises mais de l'intérêt public.

Comme l'a très justement noté Christelle Didier, «*les procédures d'alerte ne trouveront leur utilité que si elles sont perçues comme un moyen d'exercice de la responsabilité des salariés, et pas seulement un moyen de contrôle de tous par tous, que si elles sont conçues pour être au service non des intérêts des entreprises mais de l'intérêt public*»[3].

Les systèmes d'alerte professionnelle au regard du droit du travail français

En tant que tel, les dispositifs d'alerte professionnelle ne sont «*ni prévus, ni interdits par le code du travail*»[4]. Pour autant, une jurisprudence constante protège déjà les salariés qui dénoncent des pratiques douteuses constatées dans le cadre de leurs fonctions.
En effet, tout salarié doit pouvoir, au nom de sa liberté individuelle d'expression (article L2281-1 du Code du travail), relater tout fait qu'il estime préjudiciable à l'entreprise ou contraire à une règle de droit.

En effet, tout salarié doit pouvoir, au nom de sa liberté individuelle d'expression (article L2281-1 du Code du travail), relater tout fait qu'il estime préjudiciable à l'entreprise ou contraire à une de droit.

La Cour de cassation a ainsi jugé que le fait pour un salarié de porter à la connaissance de l'Inspecteur du travail des faits concernant l'entreprise et lui paraissant anormaux, qu'ils soient ou non susceptibles de qualification pénale, ne constituait pas en soi une faute (Cass. soc. 14 mars 2000, Bull. civ. V, n ° 104). De la même manière, la juridiction suprême a estimé que le fait pour un salarié de porter à la connaissance du procureur de la République des agissements de membres de l'entreprise de nature à caractériser des infractions pénales, ne constituent pas une faute, sauf si la dénonciation est mensongère ou que le salarié a agi de mauvaise foi. (Cass. soc. 12 juill. 2006, Bull. civ. V, n° 245).

En effet, toute personne, même salariée, est tenue d'apporter son concours à la justice (Cass. soc. 23 nov. 1994, Bull. civ. V, n° 308). En outre, un certain nombre de règles de droit français applicables au monde du travail sont proches des dispositifs d'alerte professionnelle. Il en va, notamment, ainsi de :

1 *Cass. Soc., 8 décembre 2009, n°08-17.191, La Fédération des travailleurs de la métallurgie (CGT) c/ La société Dassault systèmes, publié au Bulletin.*
2 *«Chartes d'éthique, alerte professionnelle et droit du travail, état des lieux et perspectives», rapport remis le 6 mars 2007 au ministre délégué à l'emploi, au travail et à l'insertion professionnelle des jeunes par Messieurs Antonmattei et Vivien; http://lesrapports.ladocumentationfrancaise.fr/BRP/074000335/0000.pdf*
3 *«L'alerte professionnelle en France : un outil problématique au cœur de la RSE», Christelle Didier, Docteure en sociologie, maître de conférences et chercheuse au Département d'éthique de l'Université catholique de Lille. http://clerse.univ-lille1.fr/spip/IMG/pdf/axe_2_didier.pdf*
4 *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.*

• **l'article L2313-2 du Code du travail** qui accorde au délégué du personnel qui constate l'existence d'une atteinte aux droits des personnes ou aux libertés individuelles dans l'entreprise *«qui ne serait pas justifiée par la nature de la tâche à accomplir ni proportionnée au but recherché»*, la faculté d'en saisir l'employeur ;

• l'**article L. 1161-1 du code du travail** qui, sans désigner explicitement le dispositif d'alerte éthique, a instauré une protection des salariés qui dénoncent, de bonne foi, soit à leur employeur, soit aux autorités judiciaires ou administratives, des faits de corruption dont ils auraient eu connaissance dans l'exercice de leurs fonctions ;

• des **articles L.561-1, L.562-1 à L.562-10 et L.564-1 à L.564-6 du code monétaire et financier** qui instaurent pour certains corps de métiers dont l'activité est liée au maniement de fonds dans la lutte contre le blanchiment d'argent la déclaration de sommes ou d'opérations soupçonnées d'être d'origine illicite.

Ainsi, le fait pour un salarié d'alerter sur des faits graves qui concernent le fonctionnement de son entreprise n'est ni moralement, ni juridiquement condamnable. Toutefois, si les dispositifs d'alerte professionelle ne sont pas encadrés par un dispositif juridique propre, ils n'échappent pas pour autant au droit. Au contraire, *«ils se trouvent au cœur d'une interpénétration complexe de différents champs juridiques (droit du travail, droit pénal des affaires, loi «informatique et libertés», etc...)»*[5]. Ainsi, en France, les dispositifs d'alerte professionnelle sont licites, à condition toutefois de respecter les dispositions du code du travail et de la loi Informatique et Libertés.

Les systèmes d'alerte professionnelle au regard du droit du travail

Avant de mettre en place un dispositif d'alerte professionnelle au sein d'une entreprise, la direction doit :

• informer préalablement les salariés : l'article L1222-4 du code du travail dispose qu'aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance;

• consulter préalablement le comité d'entreprise : l'article L2323-32 du code du travail prévoit, en effet, que le comité d'entreprise doit être informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés. A défaut, l'employeur s'expose à des poursuites pour délit d'entrave (article L.2328-1 du code du travail);

Les dispositifs d'alerte professionnelle entrent dans le champ d'application de la loi Informatique et Liberté en ce qu'ils consistent en un traitement automatisé des données ou informations à caractère personnel.

• enfin, certaines entreprises ont cru devoir solliciter l'avis du CHSCT (Comité d'Hygiène, de Sécurité et des Conditions de Travail) sur le dispositif d'alerte professionnelle qu'elles envisageaient d'installer, ce qui à notre sens ne relève pas nécessairement de ses missions. En effet, selon l'article L.4612-8 du Code du Travail, le CHSCT doit être consulté par l'employeur avant toute décision d'aménagement important modifiant les conditions de santé et de sécurité ou les conditions de travail, et notamment avant toute transformation importante des conditions des postes de travail découlant de la modification de l'outillage, d'un changement de produit ou de l'organisation du travail, avant toute modification des cadences et des normes de productivité liées ou non à la rémunération du travail. *(cf. TGI Nanterre, réf., 27 décembre 2006, n°2006/02550, Dupont de Nemours).*

[5] *Circulaire DGT n° 2008/22 du 19 novembre 2008 relative aux chartes éthiques, dispositifs d'alerte professionnelle et au règlement intérieur ; voir le lien suivant : http://www.travail-solidarite.gouv.fr/publications/picts/bo/30122008/TRE_20080012_0110_0004.pdf*

Les systèmes d'alerte professionnelle au regard de la loi «Informatique et Libertés»

Les dispositifs d'alerte professionnelle entrent dans le champ d'application de la loi Informatique et Liberté en ce qu'ils consistent en un traitement automatisé des données ou informations à caractère personnel.
Dans un premier temps, la CNIL a refusé d'autoriser les dispositifs d'alerte professionnelle qu'elle qualifiait de «*systèmes organisés de délation professionnelle*»[6]. Elle estimait que «*les dispositifs présentés étaient disproportionnés au regard des objectifs poursuivis et des risques de dénonciations calomnieuses et de stigmatisation des employés objets d'une alerte éthique*».

La CNIL a également adopté, le 8 décembre 2005, une décision d'autorisation unique de traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle, conformes aux orientations retenues par elle.

Toutefois, après des consultations avec ses homologues européens et les autorités américaines, et afin de permettre la mise en conformité de certaines entreprises françaises concernées avec le Sarbanes-Oxley Act, la CNIL a défini, le 10 novembre 2005, les conditions que doivent remplir les dispositifs d'alerte professionnelle pour être conformes à la loi Informatique et Libertés[7].
Ainsi, le dispositif d'alerte professionnelle «à la française» ne peut avoir qu'un caractère complémentaire, être facultatif et avoir un champ restreint. La CNIL a également adopté, le 8 décembre 2005[8], une décision d'autorisation unique de traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle, conformes aux orientations retenues par elle. La décision d'autorisation unique a mis en place une procédure d'autorisation simplifiée pour les dispositifs d'alerte professionnelle et a fixé les conditions que les entreprises doivent respecter afin de pouvoir en bénéficier.

Grâce à la décision d'autorisation unique, les entreprises ont simplement à adresser à la CNIL un engagement de conformité à la décision. Elles reçoivent le récépissé de leur déclaration par retour de courrier et peuvent alors mettre en œuvre leur dispositif.

La procédure d'autorisation simplifiée

En effet, la procédure d'autorisation nécessite le dépôt d'un dossier complet qui doit être examiné en séance plénière de la Commission dans les deux mois de son dépôt, à condition de ne pas nécessiter un complément d'information. Grâce à la décision d'autorisation unique, les entreprises ont simplement à adresser à la CNIL un engagement de conformité à la décision. Elles reçoivent le récépissé de leur déclaration par retour de courrier et peuvent alors mettre en œuvre leur dispositif. Il s'agit d'une procédure purement déclarative sur laquelle la CNIL n'opère pas de contrôle avant de délivrer récépissé.

Les règles posées par la CNIL pour bénéficier de la procédure simplifiée en matière de dispositifs d'alerte professionnelle

La décision d'autorisation unique prévoit notamment que le dispositif d'alerte professionnelle ne devra couvrir que «*les domaines financier, comptable, bancaire et de la lutte contre la corruption*» (article 1). Au-delà de ce cadre très précis, et encadré par la CNIL, tout dispositif d'alerte professionnelle à visée

[6] *Délibération n°2005-110 du 26 mai 2005 relative à une demande d'autorisation de McDonald's France pour la mise en œuvre d'un dispositif d'intégrité professionnelle. Délibération n°2005-111 du 26 mai 2005 relative à une demande d'autorisation de la Compagnie européenne d'accumulateurs pour la mise en œuvre d'un dispositif de «ligne éthique».*

[7] *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.*

[8] *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».*

générale - qui porterait, par exemple, sur le respect du règlement intérieur ou de la loi - doit être étudié au cas par cas par la CNIL.

La décision d'autorisation unique prévoit également que l'émetteur de l'alerte professionnelle doit s'identifier mais son identité est traitée de façon confidentielle par l'organisation chargée de la gestion des alertes.

Toutefois, selon la CNIL, *«l'article 3 de l'autorisation unique permet également la prise en compte, dans le dispositif d'alerte, de faits ne relevant pas du champ du dispositif compte tenu de leur particulière gravité. Celle-ci est appréciée au cas par cas par l'organisation chargée de la gestion des alertes. Au sens de l'autorisation unique, sont considérés comme graves les faits mettant en jeu l'intérêt vital de l'entreprise ou l'intégrité physique ou morale de ses employés. Exemples : mise en danger d'un autre employé, harcèlement moral, harcèlement sexuel, discriminations, délit d'initié, conflit d'intérêts, atteinte grave à l'environnement ou à la santé publique, divulgation d'un secret de fabrique, risque grave pour la sécurité informatique de l'entreprise...»*[9]. La décision d'autorisation unique prévoit également que l'émetteur de l'alerte professionnelle doit s'identifier mais son identité est traitée de façon confidentielle par l'organisation chargée de la gestion des alertes (article 2). Seules les personnes spécialement chargées du recueil ou du traitement des alertes profesionnelles peuvent être destinataires de tout ou partie des données à caractère personnel enregistrées dans la mesure où ces données sont nécessaires à l'accomplissement de leurs missions (article 4). Les données recueillies ne doivent pas être conservées plus de deux mois après la clôture des opérations de vérification, si l'alerte n'est pas suivie d'une procédure disciplinaire ou judiciaire (article 6).

Par ailleurs, des mesures de sécurité spécifiques doivent être mises en œuvre, la circulation des informations devant être limitée (article 7). L'entreprise doit informer préalablement les salariés sur l'utilisation et les objectifs du dispositif d'alerte, ensuite le salarié faisant l'objet d'une alerte professionnelle doit être informé après que l'entreprise a recueilli les éléments de preuve (articles 8 et 9). Enfin, tout salarié identifié dans le dispositif d'alerte dispose des droits d'accès aux données le concernant, et aussi de rectification ou de suppression, si elles sont inexactes, incomplètes, équivoques ou périmées, sans qu'il soit possible d'obtenir l'identité de l'émetteur de l'alerte (article 10).

Les données recueillies ne doivent pas être conservées plus de deux mois après la clôture des opérations de vérification, si l'alerte n'est pas suivie d'une procédure disciplinaire ou judiciaire.

Si le dispositif d'alerte professionnelle envisagé sort du cadre fixé par la décision d'autorisation unique, l'entreprise doit déposer un dossier individuel d'autorisation qui fera l'objet d'un examen approfondi par la CNIL. A titre d'exemple, c'est en suivant cette procédure contraignante que, le 22 novembre 2007 deux entreprises concurrentes ont été autorisées à instaurer des dispositifs d'alerte professionnelle permettant à leurs salariés de signaler des infractions au droit de la concurrence, domaine exclu du champ d'application de la délibération du 8 décembre 2005[10].

L'arrêt de la Chambre sociale du 8 décembre 2009

Dans l'affaire qui a donné lieu à l'arrêt du 8 décembre dernier, les juges de la Cour de cassation devaient vérifier si le dispositif

[9] *Voir le site internet de la CNIL : http://www.cnil.fr/nc/dossiers/travail/que-dit-la-cnil-sur/faq-sur-les-dispositifs-dalerte-professionnelle/*

[10] *CNIL, Délibération du 22 novembre 2007 ; Conseil de la concurrence, Décision n°07-D-21 du 26 juin 2007 relative à des pratiques mises en œuvre dans le secteur de la location-entretien du linge. A cette occasion, la CNIL a indiqué que « si le champ d'application de ces procédure d'alerte avait été initialement restreint aux infractions préjudiciables au patrimoine de l'entreprise, afin d'éviter tout risque d'atteinte aux droits des salariés, il n'y avait aucune objection de principe à ce que les infractions au droit de la concurrence soient également visées, les entreprises devant néanmoins déposer un dossier individuel d'autorisation auprès de la Commission ».*

d'alerte mis en place par la société Dassault Systèmes respectait les obligations posées par la loi du 6 janvier 1978 et la délibération du 8 décembre 2005. Le système mis en place visait à recueillir les dénonciations des salariés sur tout *«manquement sérieux aux principes décrits par le «Code of Business Conduct» en matière comptable, financière ou de lutte contre la corruption», mais aussi «en cas de manquements graves aux autres principes énoncés dans ledit code lorsqu'est mis en jeu l'intérêt vital du groupe DS ou l'intégrité morale ou physique d'une personne (notamment en cas d'atteinte aux droits de la propriété intellectuelle, de divulgation d'informations strictement confidentielles, de conflits d'intérêts, de délit d'initié, de discrimination, de harcèlement moral ou sexuel)»*.

La protection des droits de propriété intellectuelle, de la confidentialité, des intérêts de l'entreprise et du marché boursier, des victimes de discrimination ainsi que de harcèlement moral ou sexuel peut être assuré par d'autres moyens qu'un dispositif d'alerte.

Les juges de première instance avaient jugé ce champ d'application *«trop vaste»* dès lors qu'il était étendu à des situations non prévues par la délibération de la CNIL du 8 décembre 2005. En effet, *«la protection des droits de propriété intellectuelle, de la confidentialité, des intérêts de l'entreprise et du marché boursier, des victimes de discrimination ainsi que de harcèlement moral ou sexuel peut être assuré par d'autres moyens qu'un dispositif d'alerte»*, dès lors, selon le Tribunal, *«l'extension du dispositif d'alerte à de tels faits apparaît disproportionnée par rapport aux objectifs poursuivis»*[11]. Dans ces conditions, la société ne pouvait se prévaloir du régime simplifié prévu par cette délibération et devait recueillir l'autorisation de la CNIL selon le droit commun.

Les dispositifs d'alerte professionnelle devraient concerner tous les actes «contraires aux obligations législatives, aux droits des personnes et à la santé des salariés», ou «à des règles d'origine éthique ou professionnelle susceptibles de nuire gravement au fonctionnement de l'entreprise».

Le Tribunal de grande instance de Nanterre avait donc annulé le dispositif d'alerte professionnelle mis en cause. Mais le 17 avril 2008, la Cour d'appel de Versailles a infirmé cette décision, estimant que le dispositif mis en place par la société Dassault Systèmes était conforme au régime simplifié d'autorisation unique défini par la CNIL dans sa délibération du 8 décembre 2005[12]. La Cour d'appel rappelait, en effet, que l'article 3 de la délibération de la CNIL du 8 décembre 2005 prévoyait expressément que des faits concernant d'autres domaines que les matières comptable, financière et de lutte contre la corruption pouvaient faire l'objet de dénonciation lorsque l'intérêt vital de la société ou l'intégrité physique ou morale de ses employés était en jeu. Or, le dispositif mis en cause reprenait les termes de l'article 3 la délibération de la CNIL du 8 décembre 2005 en permettant aux salariés de dénoncer tous faits de nature à *«mettre en jeu l'intérêt vital du groupe DS ou l'intégrité morale ou physique d'une personne»*. Selon la Cour d'appel, il ne pouvait donc être reproché à la société de ne pas avoir sollicité l'autorisation de la CNIL. Cette décision s'inscrivait à l'évidence dans l'élargissement du champ des systèmes d'alerte professionnelle, préconisé par le rapport de Messieurs Paul-Henri Antonmattei et Philippe Vivien sur les chartes d'éthique, l'alerte professionnelle et le droit du travail français[13]. En effet, selon ces auteurs, les dispositifs d'alerte professionnelle devraient concerner tous les actes *«contraires aux*

[11] *TGI de Nanterre, 19 octobre 2007, n° 06/06450, Dassault Systeme.*
[12] *CA Versailles, 17 avril 2008, Dassault Systeme.*

obligations législatives, aux droits des personnes et à la santé des salariés», ou «*à des règles d'origine éthique ou professionnelle susceptibles de nuire gravement au fonctionnement de l'entreprise*». Cependant, cette interprétation extensive de la délibération de la CNIL du 8 décembre 2005 a été sanctionnée par la Cour de cassation qui, dans sa décision du 8 décembre dernier, a affirmé que l'autorisation unique prévue par la CNIL ne peut s'appliquer qu'à des dispositifs visant à l'établissement de procédures de contrôle interne dans les domaines financier, comptable, bancaire et de lutte contre la corruption à l'exclusion de tout autre.

Un dispositif d'alerte professionnelle ne peut en aucune manière concerner d'autres domaines que les domaines financier, comptable, bancaire et de lutte contre la corruption, à moins d'avoir fait l'objet d'une autorisation préalable individuelle par la CNIL.

En effet, la chambre sociale de la Cour de cassation a jugé qu'«*un dispositif d'alerte professionnelle faisant l'objet d'un engagement de conformité à l'autorisation unique ne peut avoir une autre finalité que celle définie à son article 1er et que les dispositions de l'article 3 n'ont pas pour objet de modifier*». Autrement dit, un dispositif d'alerte professionnelle ne peut en aucune manière concerner d'autres domaines que les domaines financier, comptable, bancaire et de lutte contre la corruption, à moins d'avoir fait l'objet d'une autorisation préalable individuelle par la CNIL (par opposition à la procédure simplifiée mise en place par décision d'autorisation unique du 8 décembre 2005). Or, en l'espèce, le dispositif mis en place par Dassault Systèmes avait un objet plus large puisqu'il prévoyait la possibilité de dénoncer des manquements graves, de nature à mettre en jeu l'intérêt vital de la société ou l'intégrité morale ou physique d'une personne notamment dans les domaines de la propriété intellectuelle, de divulgation d'informations strictement confidentielles, de conflit d'intérêts, de délit d'initié, de discrimination, de harcèlement moral ou sexuel.

Il convient toutefois de souligner que la Cour de cassation ne pose aucune objection de principe à ce que d'autres infractions que celles relatives aux domaines précités soient également visées dans un dispositif d'alerte.

Enfin la chambre sociale a jugé que le dispositif d'alerte professionnelle de la société Dassault Systèmes n'était pas conforme aux obligations posées par la loi informatique et liberté du 6 janvier 1978, dès lors qu'il n'assurait pas l'information des personnes concernées par une dénonciation et ne leur rappelait pas davantage leur droit d'accès et de rectification. Ainsi, pour être licites, les dispositifs d'alerte professionnelle doivent garder un champ spécifique restreint aux domaines comptable, financier, bancaire et à la lutte contre la corruption. Il convient toutefois de souligner que la Cour de cassation ne pose aucune objection de principe à ce que d'autres infractions que celles relatives aux domaines précités soient également visées dans un dispositif d'alerte. Dans un tel cas, les entreprises doivent simplement obtenir une autorisation préalable de la CNIL, en suivant la procédure traditionnelle d'autorisation (par opposition à la procédure simplifiée mise en place par décision d'autorisation unique du 8 décembre 2005).

Pour conclure

Les interrogations sur la licéité de principe des dispositifs d'alerte professionnelle en France, datent du refus par la CNIL de délivrer deux autorisations relatives à deux de ces dispositifs, en mai 2005. Depuis la délibération de la CNIL du 8 décembre 2005, la question est réglée : les dispositifs d'alerte professionnelle sont

[13] *Rapport du 6 mars 2007, préc., http://lesrapports.ladocumentationfrancaise.fr/BRP/074000335/0000.pdf*

parfaitement licites à condition de se conformer au cadre posé par la CNIL. En effet, le champ d'application des dispositifs d'alerte professionnelle doit rester limité afin d'éviter d'éventuelles dénonciations calomnieuses, mais aussi pour ne pas être dénaturé en un *«système organisé de délation professionnelle»*[14].

En effet, le champ d'application des dispositifs d'alerte professionnelle doit rester limité afin d'éviter d'éventuelles dénonciations calomnieuses, mais aussi pour ne pas être dénaturé en un «système organisé de délation professionnelle».

A ce titre, la Cour de cassation a confirmé que le juge judiciaire a le pouvoir d'apprécier la licéité d'un dispositif d'alerte professionnel ayant fait l'objet d'une déclaration à la CNIL, en vérifiant si le champ d'application dudit dispositif ne dépasse pas le cadre posé par la délibération du 8 décembre 2005 et plus généralement s'il ne contrevient pas à la loi du 6 janvier 1978. En France, le dispositif d'alerte professionnelle est - et doit donc rester - un mécanisme complémentaire de recueil d'informations. En effet, d'autres voies existent pour signaler des faits répréhensibles au sein de l'entreprise : les comités d'entreprise, les délégués du personnel, les syndicats, mais aussi les commissaires aux comptes, les procédures spécifiques de lutte contre le blanchiment et l'inspection du travail permettent, ainsi, de signaler des dysfonctionnements au-delà des domaines comptable, financier et de lutte contre la corruption, auxquels se limitent les dispositifs d'alerte. ▨

Emmanuel Daoud - *Avocat associé*
Emilie Bailly - *Avocat*
Cabinet VIGO

[14] *TGI de Nanterre, 19 octobre 2007, préc.*