LAMY
REVUE

REVUE LAMY

Droit des Affaires

Loi Sapin II : l'arsenal répressif français et les défis de la modernité

Caroline BOYER, Emmanuel DAOUD, Kevin EL GOHARI, César GHRÉNASSIA, Clarisse LE CORRE et Solène SFOGGIA

125 | MENSUEL
AVRIL 2017

Wolters Kluwer

RLDA 6188

Réflexions pratiques sur la mise en œuvre du dispositif d'alerte professionnelle

Clarisse LE CORRE
Avocat au Barreau de Paris
Cabinet Vigo
Membre du réseau GESICA

L'adoption de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite « Sapin II », consacre l'émergence française d'une culture de l'alerte en entreprise. Certes, des mécanismes de signalement existaient déjà en droit français, qu'il s'agisse des obligations de dénonciation en matière pénale[1] ou des dispositifs spécifiques en matière de travail[2], de renseignement[3], de sécurité sanitaire[4], de santé et d'environnement[5].

Un tel éparpillement ayant conduit à dénoncer le manque de cohérence, le Conseil d'État avait souligné la nécessité d'une définition commune afin de renforcer l'efficacité des dispositifs sectoriels d'alerte[6]. C'est chose faite avec la loi *Sapin II*, qui définit le lanceur d'alerte comme « *une personne physique qui révèle ou signale, de manière désintéressée et de bonne foi, un crime ou un délit, une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice graves pour l'intérêt général, dont elle a eu personnellement connaissance* »[7] et institue un régime juridique général de protection des lanceurs d'alerte.

De manière plus spécifique, l'article 8 de la loi fait peser sur « *les personnes morales de droit public ou de droit privé d'au moins 50 salariés, les administrations de l'État, les communes de plus de 10 000 habitants ainsi que les établissements publics de coopération intercommunale à fiscalité propre dont elles sont membres, les départements et les régions* », l'obligation de mettre en œuvre « *des procédures appropriées de recueil des signalements émis par les membres de leur personnel ou par des collaborateurs extérieurs et occasionnels* », le même article définissant une procédure graduée d'alerte professionnelle.

La mise en œuvre du dispositif d'alerte par tous les organismes entrant dans le champ d'application de l'article 8 (pour les besoins du présent article, il sera fait référence aux « entreprises ») constitue un réel challenge : comment, en effet, concevoir le dispositif d'alerte professionnelle comme un avantage concurrentiel, et non comme un système de déstabilisation et de défiance vis-à-vis de l'entreprise ? Il s'agit de repenser la notion d'alerte en entreprise afin de mettre en œuvre, sur la base des dispositions de la loi *Sapin II* mais également de la culture de l'entreprise, un dispositif cohérent et opérationnel, témoin de la bonne santé de celle-ci.

I. – Définition du dispositif d'alerte professionnelle

A. – Rappel des prévisions de la loi Sapin II

Le dispositif d'alerte professionnelle défini par la loi *Sapin II* peut être présenté de manière synthétique, sous la forme du tableau suivant.

(1) C. pr. pén., art. 40-2 ; C. pén., art. 434-1 et 434-3.
(2) C. trav., art. L. 1152-2 et L. 1132-1 relatifs au signalement de faits de harcèlement moral et discrimination ; C. trav., art. L. 1161-1 issu de L. n° 2007-1598, 13 nov. 2007, relatif au signalement de faits de corruption.
(3) CSI, art. L. 855-3 issu de L. n° 2015-912, 24 juil. 2015.
(4) C. santé publ., art. L. 5312-4-2 issu de L. n° 2011-2012, 29 déc. 2011, relatif aux risques liés aux médicaments.
(5) L. n° 2013-316, 16 avr. 2013, relative à l'indépendance de l'expertise en matière de santé et d'environnement et à la protection des lanceurs d'alerte.
(6) CE, Le droit d'alerte : signaler, traiter, protéger, 25 févr. 2016.
(7) L. n° 2016-1691, 9 déc. 2016, art. 6.

Auteur de l'alerte	Seules les personnes physiques peuvent procéder à une alerte. Sont concernés les salariés de l'entreprise mais également les « *collaborateurs extérieurs ou occasionnels* » – personnel intérimaire, stagiaires, prestataires de services, salariés d'entreprises sous-traitantes. Ainsi les personnes morales sont exclues du dispositif, précaution cohérente dès lors que le lanceur d'alerte doit avoir eu personnellement connaissance des faits reprochés, permettant ainsi de s'assurer de la réalité et de la fiabilité des faits relatés (E. Daoud et S. Sfoggia, Lanceurs d'alerte et entreprises : les enjeux de la loi *Sapin II*, AJ pénal 2017, p. 71).
Objet de l'alerte	Le champ d'application de l'alerte est vaste, celle-ci pouvant porter sur : • un crime ou un délit ; • une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement ; • une menace ou un préjudice grave pour l'intérêt général. Sont exclus du champ de l'alerte tous faits, informations ou documents, quel que soit leur forme ou leur support, couverts par le secret de la défense nationale, le secret médical et le secret de la relation avocat client. Le champ d'application du dispositif d'alerte et ses limites traduisent le devoir de divulgation avec les différents secrets professionnels, le principe de transparence n'excluant pas les secrets légitimes protégés (S. Schiller et M. Mosse, Secret des affaires et juristes d'entreprises, JCP E 2016, 1460).
Conditions de l'octroi du statut de lanceur d'alerte	L'émetteur du signalement doit : • avoir eu personnellement connaissance des faits reprochés ; • être de bonne foi ; • être désintéressé (ne retirer aucun avantage personnel de l'alerte ou de la menace d'une alerte) ; • procéder à une divulgation « *de manière nécessaire et proportionnée à la sauvegarde des intérêts en cause* » (opportunité de l'alerte). Les critères ainsi posés sont essentiels, en ce qu'ils conditionnent l'octroi du statut de lanceur d'alerte et le bénéfice de la protection y afférente – notamment l'irresponsabilité pénale visée au nouvel article 122-9 du code pénal issu de l'article 7 de la loi. Ces derniers font par ailleurs écho aux six critères dégagés par la jurisprudence de la CEDH (*défaut d'autres moyens à disposition du lanceur d'alerte pour procéder à la divulgation des faits dénoncés, intérêt public de la divulgation, vraisemblance des informations, intérêt général de la divulgation versus le préjudice causé par la divulgation aux personnes mises en cause, la bonne foi du lanceur d'alerte, proportionnalité de la sanction*) sur le fondement de la liberté d'expression consacrée à l'article 10 de la Convention, la Cour articulant le devoir de loyauté, de réserve et de discrétion dû à l'employeur, et l'intérêt général des révélations (CEDH, 12 févr. 2008, n° 14277/04, Guja c/ Moldavie ; CEDH, 19 févr. 2009, n° 4063/04, Marchenko c/ Ukraine ; CEDH, 8 janv. 2013, n° 40238/02, Bucur et Toma c/ Roumanie). Du reste, ces critères traduisent la volonté de clarifier et d'encadrer strictement la notion de lanceur d'alerte, souvent employée à tort pour désigner des réalités très différentes – « *tout dénonciateur n'est pas un lanceur d'alerte* » (S. Schiller et M. Mosse, Secret des affaires et juristes d'entreprises, JCP E 2016, 1460).
Procédure d'alerte	La procédure d'alerte prévue par la loi *Sapin II* est graduée : 1- Le lanceur d'alerte avertit son supérieur hiérarchique, direct ou indirect, l'employeur ou un référent désigné par celui-ci. 2- En l'absence de diligences de la personne destinataires de l'alerte, le lanceur d'alerte s'adresse à l'autorité judiciaire, à l'autorité administrative ou aux ordres professionnels. 3- En dernier ressort, à défaut de traitement dans un délai de trois mois, il peut rendre le signalement public. Toutefois, en cas de danger grave ou imminent ou en présence d'un risque de dommages irréversibles, le lanceur d'alerte peut porter directement le signalement à la connaissance des organismes mentionnés en deuxième phase, ou le rendre public. En tout état de cause, le lanceur d'alerte peut adresser son signalement au Défenseur des droits afin d'être orienté vers l'organisme approprié de recueil de l'alerte (loi organique n° 2016-1690 du 9 décembre 2016 relative à la compétence du Défenseur des droits pour l'orientation et la protection des lanceurs d'alerte). Dans sa décision n° 2016-741 DC du 8 décembre 2016, le Conseil constitutionnel apporte un éclairage important sur l'articulation des articles 6 (définition du lanceur d'alerte) et 8 (définition de la procédure d'alerte) de la loi *Sapin II*. Saisi de l'incohérence de ces deux articles, le Conseil relève en effet que « *le fait que le législateur ait retenu, à l'article 6, une définition plus générale du lanceur d'alerte, ne se limitant pas aux seules personnes employées par l'organisme faisant l'objet du signalement non plus qu'à ses collaborateurs, n'a pas pour effet de rendre les dispositions contestées inintelligibles. En effet, cette définition a vocation à s'appliquer non seulement au cas prévus par l'article 8, mais aussi, le cas échéant, à d'autres procédures d'alerte instaurées par le législateur, en dehors du cadre professionnel* ».

Sanctions	Tout obstacle à la transmission d'un signalement est puni d'un an d'emprisonnement et de 15 000 euros d'amende. En cas de plainte pour diffamation à l'encontre d'un lanceur d'alerte, une amende civile de 30 000 euros est prévue pour toute constitution abusive de partie civile.
Protection du lanceur d'alerte	La protection du lanceur d'alerte se traduit par : • l'interdiction de toute forme de discrimination ou de sanction disciplinaire fondée sur l'exercice conforme aux prescriptions légales du droit d'alerte, que ce soit au stade du recrutement, de l'accès au stage ou à la formation professionnelle ou encore en matière de rémunération, formation, reclassement, affectation, qualification, classification, promotion professionnelle, mutation ou renouvellement de contrat ; • la possibilité de saisir le Conseil de prud'hommes en référé en cas de rupture du contrat de travail consécutive au signalement d'une alerte ; • un régime de preuve favorable : dès lors que le lanceur d'alerte sanctionné présente des éléments de fait permettant de présumer qu'il a lancé son alerte de bonne foi, il appartient au défendeur de prouver que sa décision est justifiée par des éléments objectifs étrangers au témoignage de l'intéressé. Par décision n° 2016-740 DC du 8 décembre 2016, le Conseil constitutionnel a censuré les dispositions de l'article 14 de la loi *Sapin II* qui attribuaient au Défenseur des droits la compétence d'apporter une aide financière ou un secours financier aux lanceurs d'alerte, aux motifs que cela ne pouvait relever de la mission confiée au Défenseur des droits par les dispositions du 1er alinéa de l'article 71-1 de la Constitution.
Garantie de confidentialité	Les procédures doivent garantir une stricte confidentialité de l'identité des auteurs du signalement, des personnes visées et des informations recueillies (art. 9). Les éléments de nature à identifier la personne mise en cause ne peuvent être divulgués, sauf à l'autorité judiciaire, une fois le caractère fondé de l'alerte. Le fait de divulguer les éléments confidentiels est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.

B. – Traduction concrète pour les entreprises

À partir des exigences dressées par la loi *Sapin II*, les opérateurs économiques vont devoir définir leur propre dispositif d'alerte, c'est-à-dire un dispositif qui satisfait les critères posés par la loi, mais qui correspond également à la culture, à la taille et à la structure de l'entreprise. Cette appropriation est indispensable pour garantir la cohérence et l'effectivité du dispositif.

Au demeurant, de nombreuses entreprises disposent d'ores et déjà d'un dispositif d'alerte, lequel doit dès lors être adapté et mis en conformité avec les dispositions susvisées. Très souvent en effet, les dispositifs actuellement en vigueur sont trop restreints quant à leur champ d'application ou aux personnes pouvant effectuer un signalement, ou encore n'offrent pas suffisamment de garanties en termes de confidentialité et de protection. Notons que dans un tel cas de figure, il pourrait se poser la question de la création d'un second dispositif « Sapin II », en sus du dispositif existant. Cette possibilité, bien que parfois plus simple à mettre en œuvre, semble toutefois devoir être écartée, tant la multiplication des dispositifs d'alerte risque d'affaiblir leur lisibilité et leur bonne application par les utilisateurs potentiels de ces derniers.

Dans le cadre de la mise en conformité ou de la création de son dispositif d'alerte, l'entreprise est amenée à se positionner, en premier lieu, sur les modalités techniques de signalement (recueil de l'alerte via une messagerie électronique, une hotline, un formulaire en ligne sur un site sécurisé, etc.) et désigner le responsable de la réception et du traitement de l'alerte – par un prestataire externe ou en interne (interlocuteur unique ou équipe dédiée). L'élaboration du dispositif d'alerte suppose par ailleurs de définir les modalités de traitement de l'alerte, c'est-à-dire les étapes de la procédure de vérification et la durée de celle-ci, ainsi que les modalités de formalisation de la procédure de vérification (rédaction d'un rapport, etc.). À cet égard, l'entreprise doit trancher la question de la recevabilité et du traitement de l'alerte anonyme : le cas échéant, sous quelles conditions l'entreprise accepte de recueillir les alertes anonymes (par exemple en présence de faits détaillés et d'une gravité particulière) ? Une procédure de vérification spécifique est-elle prévue ? Enfin, il importe de définir les modes de contrôle du bon fonctionnement du dispositif (*reporting*, rapport annuel d'activité, etc.). Soulignons qu'une attention particulière doit être apportée au caractère national ou supranational du dispositif. Dès lors que la société concernée est également implantée à l'étranger, le dispositif d'alerte doit en effet tenir compte des législations locales, notamment en matière de protection des données personnelles. En définitive, l'ensemble de ces questions concrètes de mise en œuvre du dispositif *Sapin II* doivent être abordées à l'aune des particularités de l'entreprise concernée, afin de définir un dispositif d'alerte cohérent et opérationnel.

Outre la définition du dispositif d'alerte, la mise en œuvre effective de ce dernier suppose d'instaurer une dynamique interne, sous l'impulsion des dirigeants, visant à fédérer l'entreprise autour de la culture de la conformité et inciter à l'appropriation, à tous les niveaux de l'entreprise,

des outils de conformité tels que le dispositif d'alerte professionnelle. Pour cela, les utilisateurs potentiels du dispositif doivent bénéficier d'une information approfondie sur l'étendue du dispositif, portant sur la définition des personnes susceptibles de faire l'objet d'une alerte, l'identification de l'entité responsable du dispositif, les objectifs poursuivis, le champ d'application du dispositif, les garanties liées au statut de lanceur d'alerte et les critères d'octroi dudit statut, les obligations de confidentialité, les destinataires des alertes, le droit d'accès et de rectification des données traitées, les sanctions disciplinaires et judiciaires applicables en cas d'utilisation abusive du dispositif.

II. – Des incertitudes persistantes

De nombreuses interrogations demeurent quant à la mise en œuvre du dispositif d'alerte *Sapin II*, d'autant que si l'entrée en vigueur de la loi approche à grands pas, le décret d'application n'a, au jour de la publication du présent article, pas encore été adopté.

A. – La protection des données personnelles

Le recueil et la gestion de l'alerte professionnelle implique nécessairement la collecte et le traitement de données personnelles. Qu'en est-il, dès lors des implications du dispositif *Sapin II* en matière de protection des données personnelles ? Cette incertitude tient principalement au fait que la CNIL ne s'est pas encore prononcée sur le dispositif *Sapin II*. Rappelons qu'en mai 2005, la CNIL avait refusé d'autoriser les dispositifs de « lignes éthiques » qui lui avaient été notifiés par la Compagnie européenne d'accumulateurs et McDonald's, considérant que « *la mise en oeuvre par un employeur d'un dispositif destiné à organiser auprès de ses employés le recueil, quelle qu'en soit la forme, de données personnelles concernant des faits contraires aux règles de l'entreprise ou à la loi imputables à leurs collègues de travail, en ce qu'il pourrait conduire à un système organisé de délation professionnelle, ne peut qu'appeler de sa part une réserve de principe au regard de la loi du 6 janvier 1978 modifiée, et en particulier de son article 1er. En ce sens, la Commission observe que la possibilité de réaliser une* "alerte éthique" *de façon anonyme ne pourrait que renforcer le risque de dénonciation calomnieuse* »[8].

La CNIL a par la suite fait évoluer sa position en adoptant une autorisation unique le 8 décembre 2005 modifiée le 30 janvier 2014[9], afin d'encadrer la mise en place des dispositifs d'alerte et de simplifier les formalités administratives. Depuis lors, tous les systèmes d'alerte professionnelle satisfaisant les critères visés par l'autorisation sont dispensés de la procédure d'autorisation individuelle et doivent seulement faire l'objet d'une déclaration de conformité auprès de la CNIL.

L'autorisation unique n° AU-004 apparaît toutefois inadaptée aujourd'hui pour encadrer le dispositif *Sapin II*, dès lors que son champ est plus restreint. La CNIL indique en effet qu'« *un dispositif d'alerte doit être limité dans son champ. Les dispositifs à portée générale et indifférenciée (tels que ceux destinés à garantir à la fois le respect des règles légales, du règlement intérieur et des règles internes de conduite professionnelle) soulèvent une difficulté de principe au regard de la loi* "informatique et libertés" *eu égard aux risques de mise en cause abusive ou disproportionnée de l'intégrité professionnelle voire personnelle des employés concernés* »[10].

En conséquence, les dispositifs entrant dans le champ de l'autorisation unique sont ceux cantonnés aux domaines suivants : (i) financier, comptable, bancaire et de la lutte contre la corruption ; (ii) pratiques anticoncurrentielles ; (iii) lutte contre les discriminations et le harcèlement au travail ; (iv) santé, hygiène et sécurité au travail ; et (v) protection de l'environnement. Or, on l'a vu précédemment, le champ du dispositif d'alerte *Sapin II* est nettement plus large, de telle sorte qu'en l'état (et sauf nouvel amendement de l'autorisation unique par la CNIL), l'entreprise mettant en œuvre un dispositif d'alerte conforme à *Sapin II* devra suivre la procédure classique d'autorisation individuelle du dispositif auprès de la CNIL, laquelle appréciera la légitimité des finalités poursuivies et la proportionnalité du dispositif d'alerte envisagé. La CNIL a indiqué examiner actuellement les implications du dispositif d'alerte mis en œuvre en application de la loi *Sapin II* et devrait se prononcer dans les mois à venir, ce qui tarde cependant à se faire connaître, compte tenu du calendrier d'entrée en vigueur des nouvelles dispositions.

En tout état de cause, les dispositifs d'alerte doivent dès à présent intégrer les problématiques afférentes à la protection des données personnelles :

- Quelles sont les données collectées lors du signalement, et comment sont-elles consignées (rédaction d'une fiche d'alerte, d'un rapport, etc.) ?
- Quelles sont les données collectées lors de la procédure de vérification, et comment sont-elles consignées (rédaction d'un rapport d'enquête, recueil de tous documents probants, etc.) ?

(8) 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 relative à une demande d'autorisation de la Compagnie européenne d'accumulateurs pour la mise en œuvre d'un dispositif de « ligne éthique ».

(9) Délibération n° 2014-042 du 30 janvier 2014 modifiant l'autorisation unique n° 2005-305 du 8 décembre 2005 n° AU-004 relative aux traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte.

(10) Document d'orientation adopté par la CNIL 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.

- Quelles sont les modalités et la durée de conservation des données ?
- Quelle est la personne désignée responsable de ces traitements de données personnelles ?
- Quelle est la personne responsable des démarches auprès de la CNIL en vue de l'autorisation du traitement ?

Bien que l'autorisation unique n° AU-004 ne semble pas, en l'état, s'appliquer aux dispositifs d'alerte *Sapin II*, lesquels sortent du cadre défini par l'autorisation, celle-ci apporte des indications concrètes et pertinentes auxquelles il est intéressant de se référer lors de l'élaboration du dispositif. C'est le cas notamment de la nature des données traitées dans le cadre de l'alerte, lesquelles devraient se limiter à (i) l'identité, les fonctions et coordonnées de l'émetteur de l'alerte professionnelle, des personnes faisant l'objet de l'alerte et des personnes intervenant dans le recueil ou dans le traitement de celle-ci ; (ii) les faits signalés, formulés de manière objective, (iii) les éléments recueillis dans le cadre de la vérification des faits signalés ; (iv) le compte rendu des opérations de vérification ; et (v) les suites données à l'alerte[11]. C'est le cas également de la durée de conservation des données : celles-ci devraient être détruites ou archivées, lorsque l'alerte n'est pas suivie d'une procédure disciplinaire ou judiciaire, dans un délai de deux mois à compter de la clôture des opérations de vérification (les données faisant l'objet de mesures d'archivage devant être conservées, dans le cadre d'un système d'information distinct à accès restreint, pour une durée n'excédant pas les délais de procédures contentieuses). *A contrario*, lorsqu'une procédure disciplinaire ou des poursuites judiciaires sont engagées à l'encontre de la personne mise en cause ou de l'auteur d'une alerte abusive, les données relatives à l'alerte devraient être conservées jusqu'au terme de la procédure[12].

En dernier lieu, l'application du droit des données personnelles au dispositif *Sapin II* conduit nécessairement à souligner l'importance de la sécurisation du dispositif d'alerte, à tous les stades de la procédure – recueil de l'alerte, traitement, communication et conservation. L'entreprise doit ainsi veiller à ce que les mesures adéquates soient prises pour prévenir tout détournement et utilisation frauduleuse des données recueillies lors d'un signalement et de la procédure de vérification subséquente. À titre d'exemple, le mode de recueil de l'alerte (hotline, messagerie électronique, espace internet) doit être spécialement dédié à l'alerte professionnelle et faire l'objet de mesures de sécurité particulière, ce qui implique par ailleurs d'identifier clairement le responsable de la sécurité en la matière.

(11) Autorisation unique n° AU-004, art. 3.
(12) Autorisation unique n° AU-004, art. 6.

B. – Protection des lanceurs d'alerte et préservation des intérêts de l'entreprise : un équilibre délicat

Conformément à l'article 9 de la loi *Sapin II*, les dispositifs d'alerte professionnelle doivent garantir la confidentialité de l'identité des auteurs du signalement, des personnes visées et des informations recueillies. Les éléments de nature à identifier le lanceur d'alerte ne peuvent être divulgués, sauf à l'autorité judiciaire, qu'avec le consentement de celui-ci, tandis que les éléments de nature à identifier la personne objet de l'alerte ne peuvent être divulgués, sauf à l'autorité judiciaire, qu'une fois établi le caractère fondé de celle-ci. Cette garantie de confidentialité protège les lanceurs d'alerte, d'une part, afin d'éviter tout risque de représailles ou de pression, mais également les personnes mises en cause, au nom du respect de la présomption d'innocence. À cet égard, la fausse affaire d'espionnage industriel Renault en 2011 a marqué les esprits quant à l'effet boule de neige d'une dénonciation anonyme reprise sans vérification du bien-fondé des allégations, et les conséquences dramatiques pour les personnes visées à tort.

> *L'entreprise doit ainsi veiller à ce que les mesures adéquates soient prises pour prévenir tout détournement et utilisation frauduleuse des données recueillies lors d'un signalement et de la procédure de vérification subséquente.*

La mise en œuvre concrète de cette garantie de confidentialité n'est pas aisée, surtout lorsque l'on tente de parvenir au juste équilibre, conciliant l'exigence de protection des personnes physiques concernées (lanceurs d'alerte et mis en cause) et la préservation des intérêts de l'entreprise.

À l'évidence, le signalement de faits d'une gravité particulière impose d'agir vite, afin de faire cesser tout trouble éventuel ou de prévenir la survenance d'un dommage (mais aussi d'éviter que les faits ne soient révélés dans l'intervalle, par voie de presse notamment, avec de lourdes conséquences sur le plan réputationnel). Le signalement rend parfois nécessaire la mise en œuvre de mesures conservatoires, d'autant que les procédures de vérification des faits allégués peuvent, lorsque ces derniers sont complexes, être relativement longues.

En d'autres termes, la préservation des intérêts de l'entreprise peut justifier qu'une remontée d'information soit effectuée par le service dédié de recueil et traitement de

l'alerte professionnelle vis-à-vis de la direction de l'entreprise, afin que soient prises les mesures d'urgence adéquates. Il semble en effet totalement déconnecté de la réalité des entreprises de prétendre, au nom de cet impératif de confidentialité, laisser à une unité spécialisée et indépendante le soin de vérifier les signalements effectués, sans avertir d'aucune manière la direction en cas de faits d'une particulière gravité, et ce jusqu'à être en mesure de déterminer la véracité des allégations. Du reste, l'efficacité du dispositif d'alerte repose également sur la capacité de l'entreprise à réagir de manière rapide et mesurée face aux faits révélés.

Se pose alors la question de l'usage et de la diffusion des informations recueillies dans le cadre du dispositif d'alerte – *reporting* fonctionnel ou matriciel, rapport d'activité auprès de la maison mère située à l'étranger, information des instances représentatives du personnel et/ou des salariés, etc. Le sujet est sensible et appelle à la prudence, puisque la divulgation des éléments confidentiels définis par la loi (identité des auteurs du signalement, des personnes visées par celui-ci et des informations recueillies par l'ensemble des destinataires du signalement) est punie de deux ans d'emprisonnement et de 30 000 euros d'amende.

Plusieurs cas de figure peuvent être distingués :

- Il peut tout d'abord apparaître nécessaire, suite à une alerte professionnelle et après première vérification du caractère fondé de celle-ci, d'en informer les dirigeants afin notamment de prendre les mesures conservatoires qui s'imposent, dans l'attente de l'issue de la procédure de vérification. Cette communication doit viser des personnes restreintes, elles-mêmes soumises à une obligation de confidentialité.

- Dans l'hypothèse de la révélation de faits d'une particulière gravité, l'entreprise peut également être amenée à effectuer une communication auprès de tiers tels que les instances représentatives du personnel, pour évoquer les faits révélés et l'existence d'une enquête interne. Cette communication doit être mesurée et ne divulguer aucune information de nature à identifier l'auteur de l'alerte et le(les) personne(s) visée(s) par cette dernière. De la même manière, les données recueillies par le dispositif d'alerte peuvent être communiquées au sein du groupe « *si cette communication est nécessaire aux besoins de l'enquête et résulte de l'organisation du groupe. Une telle communication sera considérée comme nécessaire aux besoins de l'enquête par exemple si l'alerte met en cause un collaborateur d'une autre personne morale du groupe, un membre de haut niveau ou un organe de direction de l'entreprise concernée. Dans ce cas, les données ne doivent être transmises, dans un cadre confidentiel et sécurisé, qu'à l'organisation compétente de la personne morale destinataire apportant des garanties équivalentes dans la gestion des alertes professionnelles* »[13].

- S'agissant de l'évaluation du dispositif d'alerte professionnelle, l'entreprise peut communiquer aux entités chargées de cette mission au sein de son groupe toutes les informations statistiques utiles à leur mission (telles que les données relatives aux typologies d'alertes reçues et aux mesures correctives prises), ces informations ne devant toutefois en aucun cas permettre l'identification des personnes concernées par les alertes.

À travers ces différents exemples concrets, l'on perçoit combien la définition préalable de la procédure d'alerte est importante, de manière à prévoir et formaliser ces différentes possibilités d'utilisation et de diffusion de l'information, et combien il est nécessaire d'en informer les utilisateurs potentiels.

La conciliation des intérêts en présence amène également à s'interroger sur l'information de la personne mise en cause par l'alerte, s'agissant tant de l'étendue que du moment de l'information. D'une part, la préservation des intérêts de l'entreprise incite à différer le plus possible dans le temps cette information, afin de prendre les mesures conservatoires qui s'imposent. D'autre part, le droit des données personnelles implique de garantir un droit d'accès et de rectification des données aux personnes concernées, en premier lieu les personnes mises en cause par l'alerte. Rappelons que c'est le défaut d'information qui avait conduit la CNIL à refuser d'autoriser deux dispositifs d'alerte en mai 2005, relevant que « les *employés objets d'un signalement ne seraient, par définition, pas informés dès l'enregistrement de données mettant en cause leur intégrité professionnelle ou de citoyen, et n'auraient donc pas les moyens de s'opposer à ce traitement de données les concernant* ».

Ici encore, et dans le prolongement des développements précédents relatifs à la protection des données personnelles[14], l'autorisation unique n° AU-004 comporte des préconisations utiles, dès lors qu'il est prévu que la personne objet de l'alerte soit informée par le responsable du dispositif dès l'enregistrement de données la concernant, l'information devant préciser : l'entité responsable du dispositif, les faits reprochés, les services éventuellement destinataires de l'alerte ainsi que les modalités d'exercice de ses droits d'accès et de rectification[15]. Deux limitations de bon sens sont toutefois instituées par la CNIL à ce droit d'information. D'une part, l'information de la personne objet de l'alerte peut intervenir après l'adoption des mesures conservatoires nécessaires notamment

(13) Document d'orientation adopté par la CNIL 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.

(14) voir *supra*, II.A.

(15) Autorisation unique n° AU-004, art. 9.

pour prévenir la destruction de preuves relatives à l'alerte, d'autre part la personne objet de l'alerte ne peut en aucun cas obtenir communication du responsable du traitement, sur le fondement de son droit d'accès, des informations concernant l'identité de l'émetteur de l'alerte[16].

*

L'alerte a longtemps été perçue comme un moyen d'instrumentalisation et de déstabilisation de l'entreprise. Il s'agit désormais de l'intégrer à nos pratiques et d'en faire un nouvel outil de compétitivité. La mise en œuvre d'un dispositif d'alerte impose aux acteurs concernés de repenser le sens et la pertinence de l'alerte en entreprise et d'aller au-delà de la mise en conformité juridique. Car la question dépasse le dispositif d'alerte professionnelle, qui n'a d'ailleurs pas vocation à se substituer aux canaux traditionnels de la remontée de l'information (via les supérieurs hiérarchiques, représentants du personnel, commissaires aux comptes, etc.), canaux dont les dysfonctionnements ont rendu nécessaires la création d'une procédure spécifique de signalement et la protection des lanceurs d'alerte. En cela, la mise en conformité aux dispositions de la loi *Sapin II* donne à l'entreprise l'occasion d'interroger ses pratiques, son appréciation du rapport transparence/ secret, ainsi que sa capacité à fédérer autour de l'éthique. Une telle dynamique conduit à autonomiser les salariés, favoriser leur esprit critique et les rendre « alertes » au bon fonctionnement de l'entreprise, chacun s'associant à la trajectoire, à l'efficacité et aux progrès de celle-ci. ■

(16) Autorisation unique n° AU-004, art 9 et 10.