Le : 25/11/2010

Commission Nationale de l'Informatique et des Libertés

Délibération n°2005-305 du 08 décembre 2005
Délibération portant autorisation unique de traitements automatisés de données à caractère personnel mis en oeuvre dans le cadre de dispositifs d'alerte professionnelle.

NOR: CNIX0508957X

La Commission nationale de l'informatique et des libertés,

Vu la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques a l'égard du traitement de données a caractère personnel et la libre circulation de ces données ;

Vu 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 relative a la protection des personnes physiques à l'égard des traitements de données a caractère personnel, et notamment son article 25 I 4° et II ;

Vu le document d'orientation relatif aux dispositifs d'alerte professionnelle adopté par la Commission le 10 novembre 2005, annexé à la présente décision ;

Après avoir entendu M. Alex Türk, président, en son rapport, et Mme Pascale Compagnie, commissaire du Gouvernement, en ses observations,

Un dispositif d'alerte professionnelle est 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.

Constate que les dispositifs d'alerte professionnelle ("whistleblowing") mis en oeuvre sur les lieux de travail peuvent prendre la forme de traitements automatisés de données à caractère personnel susceptibles, du fait de leur portée, d'exclure des personnes du bénéfice de leur contrat de travail en l'absence de toute disposition législative ou réglementaire.

Dès lors, de tels dispositifs constituent des traitements relevant de l'article 25-I 4° de la loi du 6 janvier 1978 modifiée et doivent, à ce titre, être autorisés par la CNIL.

En vertu de l'article 25-II de la loi du 6 janvier 1978 modifiée, la Commission peut adopter une décision unique d'autorisation pour des traitements répondant notamment aux mêmes finalités, portant sur des catégories de données et des catégories de destinataires identiques.

Le responsable de traitement mettant en oeuvre un dispositif d'alerte professionnelle dans le respect des dispositions de cette décision unique adresse à la Commission un engagement de conformité à la présente autorisation.

Décide que les responsables de traitement qui adressent à la Commission une déclaration comportant un engagement de conformité pour leurs traitements de données à caractère personnel répondant aux conditions fixées par la présente décision unique sont autorisés à mettre en oeuvre ces traitements.

Article 1. Finalités du traitement

Seuls peuvent faire l'objet d'un engagement de conformité par référence à la présente décision unique les traitements mis en oeuvre par les organismes publics ou privés dans le cadre d'un dispositif d'alerte professionnelle répondant à une obligation législative ou réglementaire de droit français visant à l'établissement de procédures de contrôle interne dans les domaines financier, comptable, bancaire et de la lutte contre la corruption.

Conformément à l'article 7-5° de la loi du 6 janvier 1978 modifiée, les traitements mis en oeuvre dans les domaines comptable et d'audit par les entreprises concernées par la section 301(4) de la loi américaine dite "Sarbanes-Oxley" de juillet 2002 entrent également dans le champ de la présente décision.

Article 2. Traitement de l'identité de l'émetteur de l'alerte

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.

Cette organisation ne peut recueillir, par exception, l'alerte d'une personne qui souhaite rester anonyme qu'aux conditions suivantes :

- le traitement de cette alerte doit s'entourer de précautions particulières, telles qu'un examen préalable, par son premier destinataire, de l'opportunité de sa diffusion dans le cadre du dispositif,

- l'organisme n'incite pas les personnes ayant vocation à utiliser le dispositif à le faire de manière anonyme et la publicité faite sur l'existence du dispositif en tient compte. Au contraire, la procédure est conçue de façon à ce que les employés s'identifient auprès de l'organisation chargée de la gestion des alertes.

Article 3. Catégories de données à caractère personnel enregistrées

Seules les catégories de données suivantes peuvent être traitées :

- identité, fonctions et coordonnées de l'émetteur de l'alerte professionnelle ;

- identité, fonctions et coordonnées des personnes faisant l'objet d'une alerte ;

- identité, fonctions et coordonnées des personnes intervenant dans le recueil ou dans le traitement de l'alerte ;

- faits signalés ;

- éléments recueillis dans le cadre de la vérification des faits signalés ;

- compte rendu des opérations de vérification ;

- suites données à l'alerte.

Les faits recueillis sont strictement limités aux domaines concernés par le dispositif d'alerte. Des faits qui ne se rapportent pas à ces domaines peuvent toutefois être communiqués aux personnes compétentes de l'organisme concerné lorsque l'intérêt vital de cet organisme ou l'intégrité physique ou morale de ses employés est en jeu.

La prise en compte de l'alerte professionnelle ne s'appuie que sur des données formulées de manière objective, en rapport direct avec le champ du dispositif d'alerte et strictement nécessaires à la vérification des faits allégués. Les formulations utilisées pour décrire la nature des faits signalés font apparaître leur caractère présumé.

Article 4. Destinataires des données à caractère personnel

Les personnes spécialement chargées, au sein de l'organisme concerné, du recueil ou du traitement des alertes professionnelles ne sont destinataires de tout ou partie des données visées à l'article 3 que dans la mesure où ces données sont nécessaires à l'accomplissement de leurs missions.

Ces données peuvent être communiquées aux personnes spécialement chargées de la gestion des alertes professionnelles au sein du groupe de sociétés auquel appartient l'organisme concerné si cette communication est nécessaire à la vérification de l'alerte ou résulte de l'organisation du groupe.

S'il est fait recours à un prestataire de service pour recueillir ou traiter les alertes, les personnes spécialement chargées de ces missions au sein de l'organisme prestataire de service n'accèdent à tout ou partie des données visées à l'article 3 que dans la limite de leurs attributions respectives. Le prestataire de service éventuellement désigné pour gérer tout ou partie de ce dispositif s'engage notamment, par voie contractuelle, à ne pas utiliser les données à des fins détournées, à assurer leur confidentialité, à respecter la durée de conservation limitée des données et à procéder à la destruction ou à la restitution de tous les supports manuels ou informatisés de données à caractère personnel au terme de sa prestation.

Dans tous les cas, les personnes chargées du recueil et du traitement des alertes professionnelles sont en nombre limité, spécialement formées et astreintes à une obligation renforcée de confidentialité contractuellement définie.

Article 5. Transferts de données à caractère personnel hors de l'Union européenne

Le présent article s'applique dans les cas où les communications de données envisagées à l'article 4 concernent un transfert vers une personne morale établie dans un pays non membre de l'Union européenne n'accordant pas une protection suffisante au sens de

l’article 68 de la loi du 6 janvier 1978 modifiée.

Dans ces cas, ces communications de données à caractère personnel doivent s’opérer conformément aux dispositions spécifiques de la loi du 6 janvier 1978 modifiée relatives aux transferts internationaux de données, et notamment son article 69, alinéa 8.

Il est satisfait à ces dispositions lorsque la personne morale au sein de laquelle travaille le destinataire des données a adhéré au Safe Harbor, dans la mesure où la société américaine concernée a expressément fait le choix d’inclure les données de ressources humaines dans le champ de cette adhésion.

II est également satisfait à ces dispositions lorsque le destinataire a conclu un contrat de transfert basé sur les clauses contractuelles types émises par la Commission européenne dans ses décisions du 15 juin 2001 ou du 27 décembre 2004, ou lorsque le groupe auquel appartiennent les entités concernés ont adopté des règles internes dont la CNIL a préalablement reconnu qu’elles garantissent un niveau de protection suffisant de la vie privée et des droits fondamentaux des personnes. S’il est satisfait à ces conditions, et si le traitement dont le transfert est issu est par ailleurs conforme à l’ensemble des autres dispositions de la présente délibération, la présente délibération porte également autorisation du transfert envisagé en application de l’article 69, alinéa 8, de la loi du 6 janvier 1978 modifiée.

Article 6. Durée de conservation des données à caractère personnel

Les données relatives à une alerte considérée, dès son recueil par le responsable du traitement, comme n’entrant pas dans le champ du dispositif sont détruites ou archivées sans délai, sous réserve de l’application de l’avant-dernier alinéa de l’article 3.

Les données relatives à une alerte ayant fait l’objet d’une vérification sont détruites ou archivées par l’organisation chargée de la gestion des alertes dans un délai de deux mois à compter de la clôture des opérations de vérification lorsque l’alerte n’est pas suivie d’une procédure disciplinaire ou judiciaire.

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 sont conservées par l’organisation chargée de la gestion des alertes jusqu’au terme de la procédure.

Les données faisant l’objet de mesures d’archivage sont conservées, dans le cadre d’un système d’information distinct à accès restreint, pour une durée n’excédant pas les délais de procédures contentieuses.

Article 7. Mesures de sécurité

Le responsable des traitements prend toutes précautions utiles pour préserver la sécurité des données tant à l’occasion de leur recueil que de leur communication ou de leur conservation.

En particulier, les accès aux traitements de données s’effectuent par un identifiant et un mot de passe individuels, régulièrement renouvelés, ou par tout autre moyen d’authentification. Ces accès sont enregistrés et leur régularité est contrôlée.

L’identité de l’émetteur d’une alerte est traitée de façon confidentielle afin que celui-ci ne subisse aucun préjudice du fait de sa démarche.

Article 8. Information des utilisateurs potentiels du dispositif

Une information claire et complète des utilisateurs potentiels du dispositif d’alerte est réalisée.

Au delà de l’information collective et individuelle prévue par le Code du travail, et conformément à l’article 32 de la loi du 6 janvier 1978 modifiée, cette information précise notamment l’identification de l’entité responsable du dispositif, les objectifs poursuivis et les domaines concernés par les alertes, le caractère facultatif du dispositif, l’absence de conséquence à l’égard des employés de la non-utilisation de ce dispositif, les destinataires des alertes, les éventuels transferts de données à caractère personnel à destination d’un Etat non membre de la Communauté européenne, ainsi que l’existence d’un droit d’accès et de rectification au bénéfice des personnes identifiées dans le cadre de ce dispositif.

Il est clairement indiqué que l’utilisation abusive du dispositif peut exposer son auteur à des sanctions disciplinaires ainsi qu’à des poursuites judiciaires mais qu’à l’inverse, l’utilisation de bonne foi du dispositif, même si les faits s’avèrent par la suite inexacts ou ne donnent lieu à aucune suite, n’exposera son auteur à aucune sanction disciplinaire.

Article 9. Information de la personne faisant l’objet d’une alerte professionnelle

La personne qui fait l’objet d’une alerte est, conformément aux articles 6 et 32 de loi du 6 janvier 1978, informée par le responsable du dispositif dès l’enregistrement, informatisé ou non, de données la concernant afin de lui permettre de s’opposer au traitement de ces données.

Lorsque des mesures conservatoires sont nécessaires, notamment pour prévenir la destruction de preuves relatives à l’alerte, l’information de cette personne intervient après l’adoption de ces mesures.

Cette information, qui est réalisée selon des modalités permettant de s’assurer de sa bonne délivrance à la personne concernée, précise notamment l’entité responsable du dispositif, les faits qui sont reprochés, les services éventuellement destinataires de l’alerte ainsi que les modalités d’exercice de ses droits d’accès et de rectification. Si elle n’en a pas bénéficié auparavant, la personne reçoit également une information conforme à l’article 8 de la présente décision.

Article 10. Respect des droits d’accès et de rectification

Conformément aux articles 39 et 40 de la loi du 6 janvier 1978 modifiée, le responsable du dispositif d’alerte garantit à toute personne identifiée dans le dispositif d’alerte professionnelle le droit d’accéder aux données la concernant et d’en demander, si elles sont inexactes, incomplètes, équivoques ou périmées, la rectification ou la suppression.

La personne qui fait l’objet d’une 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.

Article 11

Tout dispositif d'alerte professionnelle prévoyant la mise en oeuvre de traitement de données à caractère personnel ne répondant pas aux dispositions précédentes doit faire l'objet d'une demande d'autorisation auprès de la Commission dans les formes prescrites par les articles 25-I 4° et 30 de la loi du 6 janvier 1978 modifiée.

Article 12

La présente délibération sera publiée au Journal officiel de la République française.

Le président, Alex TURK.

ANNEXE

Document d'orientation adopté par la Commission le 10 novembre 2005 pour la mise en oeuvre 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.

La Commission nationale de l'informatique et des libertés constate le développement récent en France de dispositifs permettant à des employés de signaler le comportement de leurs collègues de travail supposé contraire à la loi ou aux règles établies par l'entreprise.

Ces dispositifs "d'alerte professionnelle" ("whistleblowing") ne sont ni prévus, ni interdits par le code du travail. Quand ils s'appuient sur le traitement de données à caractère personnel c'est-à-dire la collecte, l'enregistrement, la conservation et la diffusion d'informations relatives à une personne physique identifiée ou identifiable, ils sont soumis à la loi du 6 janvier 1978 modifiée, que le traitement soit réalisé sur support informatique ou sur support papier. Lorsqu'ils sont automatisés, ils doivent faire l'objet d'une autorisation de la CNIL, en application de l'article 25-4° de cette loi du fait qu'ils sont susceptibles d'exclure des personnes du bénéfice d'un droit ou de leur contrat de travail en l'absence de toute disposition législative ou réglementaire spécifique.

La CNIL a refusé en mai 2005 d'autoriser deux systèmes spécifiques de "lignes éthiques" relevant de cette démarche d'alerte professionnelle. Pour autant elle n'a pas d'opposition de principe à de tels dispositifs dès lors que les droits des personnes mises en cause directement ou indirectement dans une alerte sont garantis au regard des règles relatives à la protection des données personnelles. En effet, ces personnes, en plus des droits de la défense qui leur sont assurés par la législation du travail en cas d'engagement d'une procédure disciplinaire, disposent de droits particuliers qui leur sont reconnus par la loi "informatique et libertés" ou la directive européenne 95/46/CE du 24 octobre 1995 quand des informations les concernant font l'objet d'un traitement : droit à ce que ces informations soient recueillies de manière loyale, droit à être informé du traitement de ces informations, droit de s'opposer à ce traitement si un motif légitime peut être invoqué, droit de rectifier ou de faire supprimer les informations inexactes, incomplètes, équivoques ou périmées.

Afin de contribuer à la mise en oeuvre de dispositifs d'alerte respectueux des principes définis par la loi et la directive, la CNIL préconise l'adoption par les entreprises des règles suivantes qui ne portent que sur l'application de ces textes, à l'exclusion des questions pour lesquelles la CNIL n'a pas de compétence, en particulier celles relatives à la législation du travail.

1) Portée du dispositif d'alerte : un caractère complémentaire, un champ restreint, un usage facultatif

Le fonctionnement normal d'une organisation implique que les alertes relatives à un dysfonctionnement, dans quelque domaine que ce soit, remontent jusqu'aux dirigeants par la voie hiérarchique ou par des modes ouverts d'alerte tels que l'intervention des représentants du personnel ou, en matière de contrôle des comptes, les rapports des commissaires aux comptes. Dans la législation française, la protection et l'indépendance des uns et des autres sont du reste particulièrement assurées.

La mise en place d'un dispositif d'alerte peut être justifiée par l'hypothèse que ces canaux d'information pourraient ne pas fonctionner dans certaines circonstances. Toutefois, un tel dispositif ne saurait être conçu, par les entreprises, comme un mode normal de signalement des dysfonctionnements de l'entreprise, à part égale avec les modes de signalement gérés par des personnes dont les fonctions ou les attributions consistent précisément à repérer et traiter de tels dysfonctionnements. En ce sens, les dispositifs d'alerte doivent être conçus comme uniquement complémentaires par rapport aux autres modes d'alerte dans l'entreprise.

Afin de tenir compte de ce caractère intrinsèquement complémentaire, 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 en effet 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.

A cet égard, il résulte de l'article 7 de la loi du 6 janvier 1978 modifiée que les dispositifs d'alerte ne peuvent être considérés comme légitimes que du fait de l'existence d'une obligation légale (législative ou réglementaire) imposant la mise en place de tels dispositifs (article 7-1°), ou du fait de l'intérêt légitime du responsable de traitement, dès lors que celuici est établi, et "sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée" (article 7-5°).

Cette légitimité est acquise en vertu de l'article 7-1° de la loi du 6 janvier 1978 quand des dispositifs d'alerte sont mis en oeuvre à seule fin de répondre à une obligation législative ou réglementaire de droit français visant à l'établissement de procédures de contrôle interne dans des domaines précisément définis. Une telle obligation résulte clairement, par exemple, des dispositions relatives au contrôle interne des établissements de crédit et des entreprises d'investissement (arrêté du 31 mars 2005 modifiant le règlement du Comité de la réglementation bancaire et financière n° 97-02 du 21 février 1997).

En revanche, il ne semble pas que le simple fait de l'existence d'une disposition légale

étrangère en vertu de laquelle un dispositif d'alerte serait mis en place permette de légitimer un traitement de données personnelles au sens de l'article 7-1°. Tel est le cas des dispositions de la Section 301(4) de la loi Sarbanes-Oxley qui prévoient que les employés d'une entreprise doivent pouvoir faire état au comité d'audit de leurs inquiétudes quant à une comptabilité ou un audit douteux en étant assurés de bénéficier de garanties de confidentialité et d'anonymat.

Il est cependant impossible, dans ce cas, d'ignorer l'intérêt légitime, au sens de l'article 7-5° de la loi du 6 janvier 1978, que les sociétés françaises cotées aux Etats-Unis ou les sociétés françaises filiales de sociétés cotées aux Etats-Unis, tenues de certifier leurs comptes auprès des autorités boursières américaines, ont à mettre en place des procédures d'alerte quant à des dysfonctionnements supposés en matière comptable et de contrôle des comptes. A l'évidence, la remontée jusqu'au conseil d'administration d'informations relatives, par exemple, à des suspicions de manipulations comptables pouvant avoir un impact sur les résultats financiers de l'entreprise est une préoccupation essentielle pour les entreprises faisant appel public à l'épargne.

Loin de se limiter aux Etats-Unis, des initiatives en la matière ont également été prises en Europe (cf. notamment la récente recommandation de la Commission européenne du 15 février 2005 concernant le rôle des administrateurs non exécutifs et des membres de conseil de surveillance des sociétés cotées et les comités du conseil d'administration et de surveillance), qui poursuivent le même objectif de renforcement de la sécurité des marchés financiers que la loi Sarbanes-Oxley. Ces différents textes caractérisent manifestement, au sens de l'article 7-5° de la loi du 6 janvier 1978, l'intérêt légitime de l'entreprise à mettre en place des dispositifs d'alerte dans les domaines qu'ils couvrent, et, dans ce contexte, ceux-ci doivent donc être considérés comme acceptables.

Pour les mêmes raisons, sont légitimes les dispositifs d'alerte qui visent à lutter contre la corruption, par exemple celle d'agents publics étrangers dans les transactions commerciales internationales (convention OCDE du 17 décembre 1997, ratifiée par la loi n° 99-424 du 27 mai 1999).

Les dispositifs d'alerte limités au champ ainsi défini bénéficieront d'une autorisation unique de la CNIL, sous réserve du respect des autres règles recommandées par elle. En revanche, pour les dispositifs ne se fondant pas sur des obligations législatives ou réglementaires de contrôle interne dans les domaines financier, comptable, bancaire et de la lutte contre la corruption, la CNIL conduira une analyse au cas par cas, dans le cadre de ses pouvoirs d'autorisation, de la légitimité des finalités poursuivies et de la proportionnalité du dispositif d'alerte envisagé.

Afin de prévenir un usage détourné du dispositif d'alerte pour dénoncer des faits sans rapport avec les domaines définis a priori, le responsable de ce dispositif doit clairement indiquer qu'il est strictement réservé à de tels domaines et doit s'interdire d'exploiter les alertes qui y sont étrangères, sauf si l'intérêt vital de l'entreprise, l'intégrité physique ou morale de ses employés est en jeu.

Plus généralement, l'utilisation par les personnels d'un dispositif d'alerte légitimement mis en oeuvre ne peut revêtir qu'un caractère non obligatoire. En ce sens, le ministère de l'emploi, du travail et de l'insertion professionnelle des jeunes a souligné, dans une lettre adressée à la CNIL, que "l'utilisation des dispositifs d'alerte ne doit pas faire l'objet d'une

obligation mais d’une simple incitation. (...) Rendre obligatoire la dénonciation revient donc en réalité à transférer sur les salariés la charge de l’employeur en matière de respect du règlement intérieur. On peut également estimer que l’obligation de dénonciation serait contraire à l’article L120-2 du code du travail en tant que sujétion non proportionnée à l’objectif à atteindre”.

2) Une définition des catégories de personnes concernées par le dispositif d’alerte

Conformément au principe de proportionnalité, les catégories de personnels susceptibles de faire l’objet d’une alerte devraient être précisément définies en référence aux motifs légitimant la mise en oeuvre du dispositif d’alerte.

Cette définition relève de la compétence du chef d’entreprise à qui il appartient, dans le respect des procédures prévues en droit du travail, de fixer les limites de la procédure.

3) Un traitement restrictif des alertes anonymes

La possibilité de réaliser une alerte de façon anonyme ne peut que renforcer le risque de dénonciation calomnieuse. A l’inverse, l’identification de l’émetteur de l’alerte ne peut que contribuer à responsabiliser les utilisateurs du dispositif et ainsi à limiter un tel risque. En effet, l’alerte identifiée présente plusieurs avantages et permet :

- d’éviter des dérapages vers la délation et la dénonciation calomnieuse ;

- d’organiser la protection de l’auteur de l’alerte contre d’éventuelles représailles ;

- d’assurer un meilleur traitement de l’alerte en ouvrant la possibilité de demander à son auteur des précisions complémentaires.

La protection de l’émetteur de l’alerte est une exigence consubstantielle à un dispositif d’alerte.

La CNIL n’a pas à se prononcer sur les moyens de l’assurer sauf sur un point qui résulte clairement de la loi “informatique et libertés” : l’identité de l’émetteur doit être traitée de façon confidentielle afin que celui ne subisse aucun préjudice du fait de sa démarche. En particulier, cette identité ne peut être communiquée à la personne mise en cause sur le fondement du droit d’accès prévu par l’article 39 de cette loi.

Cependant, l’existence d’alertes anonymes, même et surtout en l’absence de systèmes organisés d’alerte confidentielle, est une réalité. Il est également difficile pour les responsables d’une organisation d’ignorer ce type d’alerte, quand bien même ils n’y seraient pas favorables par principe.

Le traitement de telles alertes doit s’entourer de précautions particulières, notamment un examen préalable, par leur premier destinataire, de l’opportunité de leur diffusion dans le cadre du dispositif. En tout état de cause, l’organisation ne doit pas inciter les personnes ayant vocation à utiliser le dispositif à le faire de manière anonyme et la publicité faite sur l’existence du dispositif doit en tenir compte. Au contraire, la procédure doit être conçue de manière à ce que les employés s’identifient à chaque communication d’informations par la procédure d’alerte et soumettent des informations relatives à des faits plutôt qu’à des

personnes.

4) La diffusion d’une information claire et complète sur le dispositif d’alerte

Une information claire et complète des utilisateurs potentiels du dispositif d’alerte doit être réalisée par tout moyen approprié.

Au delà de l’information collective et individuelle prévue par le code du travail, et conformément à l’article 32 de la loi du 6 janvier 1978 modifiée, cette information doit notamment préciser l’identification de l’entité responsable du dispositif, les objectifs poursuivis et le domaine concerné par les alertes, le caractère facultatif du dispositif, l’absence de conséquence à l’égard des employés de la non-utilisation de ce dispositif, les destinataires des alertes, ainsi que l’existence d’un droit d’accès et de rectification au bénéfice des personnes identifiées dans le cadre de ce dispositif.

Il doit enfin être clairement indiqué que l’utilisation abusive du dispositif peut exposer son auteur à des sanctions disciplinaires ainsi qu’à des poursuites judiciaires, mais qu’à l’inverse, l’utilisation de bonne foi du dispositif, même si les faits s’avèrent par la suite inexacts ou ne donnent lieu à aucune suite, ne peut exposer son auteur à des sanctions.

5) Un recueil des alertes par des moyens dédiés

Le recueil des alertes peut reposer sur tous moyens, informatisés ou non, de traitement des données.

Ces moyens doivent être dédiés au dispositif d’alerte afin d’écarter tout risque de détournement de finalité et de renforcer la confidentialité des données.

6) Des données d’alerte pertinentes, adéquates et non excessives

Le support permettant la prise en compte de l’alerte professionnelle ne doit comporter que des données formulées de manière objective, en rapport direct avec le champ du dispositif d’alerte et strictement nécessaires à la vérification des faits allégués.

Les formulations utilisées pour décrire la nature des faits signalés doivent faire apparaître leur caractère présumé.

7) Une gestion interne des alertes réservée à des spécialistes, dans un cadre confidentiel

Le recueil et le traitement des alertes professionnelles doivent être confiés à une organisation spécifique mise en place au sein de l’entreprise concernée pour traiter ces questions. Les personnes chargées de traiter les alertes doivent être en nombre limité, spécialement formées et astreintes à une obligation renforcée de confidentialité contractuellement définie.

La confidentialité des données à caractère personnel doit être garantie tant à l’occasion de leur recueil que de leur communication ou de leur conservation.

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.

Si une telle communication s’avère nécessaire, et ce vers une personne morale établie dans un pays non membre de l’Union européenne n’accordant pas une protection adéquate au sens de la directive 95/46/CE du 24 octobre 1995, il doit être fait application des dispositions spécifiques de la loi du 6 janvier 1978 modifiée relatives aux transferts internationaux de données (encadrement juridique particulier et information des personnes concernées sur le fait que les données seront transférées vers un tel pays).

Enfin, dans l’hypothèse où il serait envisagé d’avoir recours à un prestataire pour gérer le dispositif d’alerte, celui-ci doit s’engager contractuellement à ne pas utiliser les données à des fins détournées, à assurer leur confidentialité, et à respecter la durée de conservation limitée des données. L’entreprise concernée restera en tout état de cause responsable des traitements que le prestataire effectuera pour son compte.

8) La possibilité de rapports d’évaluation du dispositif

Dans le cadre de l’évaluation du dispositif d’alerte professionnelle, l’entreprise responsable 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 doivent en aucun cas permettre l’identification directe ou indirecte des personnes concernées par les alertes.

9) Une conservation limitée des données à caractère personnel

Les données relatives à une alerte jugée infondée par l’entité responsable des alertes doivent être détruites sans délai.

Les données relatives aux alertes ayant nécessité une vérification ne doivent pas être conservées au delà de deux mois à compter de la clôture des opérations de vérification, sauf engagement d’une procédure disciplinaire ou de poursuites judiciaires à l’encontre de la personne mise en cause ou de l’auteur d’une alerte abusive.

10) Une information précise de la personne mise en cause

Conformément aux articles 6 et 32 de loi du 6 janvier 1978 modifiée l’information de la personne identifiée visée par une alerte doit être par principe réalisée par le responsable du dispositif dès l’enregistrement, informatisé ou non, des données la concernant afin de lui permettre de s’opposer sans délai au traitement de ces données.

Toutefois, l’information de la personne mise en cause ne saurait intervenir avant l’adoption de mesures conservatoires lorsque celles-ci s’avèrent indispensables, notamment pour

prévenir la destruction de preuves nécessaires au traitement de l’alerte.

Cette information est réalisée selon des modalités permettant de s’assurer de sa bonne délivrance à la personne concernée.

Elle doit notamment préciser au salarié mis en cause l’entité responsable du dispositif, les faits qui lui sont reprochés, les services éventuellement destinataires de l’alerte ainsi que les modalités d’exercice de ses droits d’accès et de rectification.

11) Le respect des droits d’accès et de rectification

Conformément aux articles 39 et 40 de la loi du 6 janvier 1978 modifiée toute personne identifiée dans le dispositif d’alerte professionnelle peut accéder aux données la concernant et en demander, le cas échéant, la rectification ou la suppression.

Elle ne peut en aucun cas obtenir communication, sur le fondement de son droit d’accès, des informations concernant des tiers, telles que l’identité de l’émetteur de l’alerte.

Nature de la délibération: Autorisation unique