DELIBERATION N° 2011-73 DU 26 SEPTEMBRE 2011 PORTANT RECOMMANDATION SUR LES DISPOSITIFS D'ALERTE PROFESSIONNELLE MIS EN ŒUVRE SUR LE LIEU DE TRAVAIL

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales du Conseil de l'Europe ;

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 Recommandation du Conseil de l'Europe n° R (8 9) 2 du 19 janvier 1989 sur la protection des données à caractère personnel utilisées à des fins d'emploi ;

Vu la Loi n° 1.165 du 23 décembre 1993, modifiée, r elative à la protection des informations nominatives ;

Vu l'Ordonnance Souveraine n° 2.230 du 19 juin 2009 fixant les modalités d'application de la Loi n° 1.165 du 23 décembre 199 3, susvisée ;

Vu le Code civil ;

Vu le Code pénal ;

Vu la Délibération n° 2009-14 du 23 novembre 2009 p ortant recommandation sur les dispositifs d'alerte professionnelle.

LA COMMISSION DE CONTROLE DES INFORMATIONS NOMINATIVES,

Conformément à l'article 1er alinéa 1 de la loi n° 1.165 du 23 décembre 1993, les traitements automatisés ou non automatisés d'informations nominatives ne doivent pas porter atteinte aux libertés et droits fondamentaux consacrés par le titre III de la Constitution.

La Commission de Contrôle des Informations Nominatives, autorité administrative indépendante, a pour mission de veiller au respect de ces dispositions.

A ce titre, elle est notamment habilitée à formuler toutes recommandations entrant dans le cadre des missions qui lui sont conférées par la loi.

Par la présente délibération, la Commission souhaite préciser les grands principes de protection des informations nominatives applicables aux dispositifs d'alerte professionnelle (*Whistleblowing*) mis en œuvre par les personnes physiques ou morales de droit privé sur le lieu de travail, et ce afin d'orienter les demandeurs d'autorisation dans leurs démarches auprès d'elle.

A ce titre, la présente délibération annule et remplace la délibération n°2009-14 du 23 novembre 2009 portant recommandation sur les dispositifs d'alerte professionnelle.

I. Dispositions générales

Un dispositif d'alerte professionnelle permet à un individu de signaler tout problème survenant sur son lieu de travail, susceptible de mettre en jeu les intérêts ou la responsabilité de l'entreprise ou de l'organisme au sein duquel il travaille, et qui serait contraire à une législation, une réglementation ou aux règles internes de ladite entreprise ou organisme, dans un ou plusieurs domaine(s) déterminé(s).

Le fonctionnement de ce type de dispositif est variable : l'alerte peut être déclenchée par un appel téléphonique, un courriel ou par un courrier postal, traité au sein de l'entreprise ou organisme par un service dédié, ou en dehors de celui-ci par le biais d'un prestataire de service.

Il s'ensuit donc une collecte d'informations nominatives, afférentes tant à la personne ayant donné l'alerte, qu'à celle(s) visée(s) par l'alerte, et ce afin de permettre aux personnes en charge de leur traitement d'effectuer les vérifications nécessaires, et le cas échéant, de prendre toutes mesures utiles.

Ainsi, ces traitements « *portant sur des soupçons d'activités illicites [ou] des infractions* », ou encore « *mis en œuvre à des fins de surveillance* » au sens de l'article 11-1 de la loi n° 1.165, modifiée, sont s oumis à l'autorisation préalable de la Commission, dès lors que ceux-ci sont automatisés.

Cette procédure est applicable à l'ensemble des entreprises ou organismes du secteur privé, à savoir :

- les personnes physiques ou morales de droit privé, visées à l'article 6 de la loi n° 1.165, modifiée ;
- les organismes de droit privé investis d'une mission d'intérêt général ou concessionnaires d'un service public portés sur une liste établie par arrêté ministériel, telle que mentionnée à l'article 7 de ladite loi.

La Commission relève en outre que la mise en place de tels systèmes comprend un certain nombre de dangers qui leur sont inhérents, et notamment :

- le risque de mise en place d'un système organisé de délation professionnelle ou de dénonciation calomnieuse, notamment en cas d'anonymat de la personne dénonciatrice ;
- le risque de disproportion entre le dispositif mis en place et les objectifs poursuivis par l'entreprise ou organisme ;
- la déloyauté de la collecte et du traitement des données nominatives d'une personne n'ayant pas les moyens de s'y opposer ou de se défendre.

Au vu de ces éléments, et en l'absence de dispositions légales ou réglementaires encadrant ce type de traitements automatisés ou non automatisés d'informations nominatives, la Commission estime nécessaire de retenir les principes fondamentaux ci-après exposés, afin de s'assurer de la conformité des dispositifs d'alerte professionnelle avec les dispositions de la loi n° 1.165 du 23 décembre 1993, modifiée, relative à la protection des informations nominatives.

II. Légitimité et finalités du traitement relatif à un dispositif d'alerte professionnelle

La Commission considère que tout traitement automatisé ou non automatisé d'informations nominatives afférent à un dispositif d'alerte professionnelle est licite et justifié, conformément aux dispositions des articles 10-1 et 10-2 de la loi n° 1.165, modifiée, dès lors qu'il est mis en œuvre aux seules fins de :

- répondre à une obligation législative ou réglementaire de droit monégasque visant à l'établissement de procédures de contrôle interne dans les domaines financier, comptable, bancaire et de lutte contre la corruption ; ou
- permettre la réalisation d'un intérêt légitime poursuivi par le responsable de traitement ou son représentant, à la condition de ne pas méconnaître les libertés et droits fondamentaux des personnes concernées.

Sont ainsi justifiés les traitements d'alerte professionnelle mis en œuvre dans les domaines :

- comptable et d'audit, notamment par les entreprises ou organismes concernés par la section 301(4) de la loi américaine dite « *Sarbanes-Oxley* » du 31 juillet 2002, ou par la loi japonaise « *Financial Instrument and Exchange Act* » dite « *Japanese SOX* » du 6 juin 2006 ;
- de lutte contre les pratiques anticoncurrentielles.

III. Catégories d'informations traitées

Conformément au principe de qualité des informations nominatives, la Commission estime que seules les catégories d'informations suivantes peuvent être traitées :

- identité, fonctions et coordonnées de l'émetteur de l'alerte ;
- identité, fonctions et coordonnées du/ des personne(s) faisant l'objet de l'alerte ;
- identité, fonctions et coordonnées des personnes intervenant dans le recueil et/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.

La Commission rappelle par ailleurs que les faits recueillis doivent être strictement limités aux domaines concernés par le dispositif d'alerte.

Elle souligne que la prise en compte de l'alerte professionnelle ne doit s'appuyer 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. Ainsi, les formulations utilisées pour décrire la nature des faits signalés doivent impérativement faire apparaître leur caractère présumé.

IV. Traitement de l'identité de l'émetteur de l'alerte

Face aux risques de délation professionnelle ou de dénonciation calomnieuse, la Commission demande à ce que l'émetteur de l'alerte professionnelle s'identifie.

Son identité doit ensuite être traitée de façon confidentielle, afin qu'il ne subisse aucun préjudice quelconque du fait de sa démarche.

Par dérogation à ce principe, et à titre exceptionnel, la Commission admet que l'alerte d'une personne souhaitant rester anonyme puisse être recueillie aux conditions cumulatives suivantes :

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

  Cet examen doit prendre en compte l'ensemble des principes établis dans le cadre de la présente délibération, et notamment : le domaine concerné par l'alerte, l'objectivité des éléments fournis, la possibilité de vérification de ces éléments sans porter préjudice aux individus visés par l'alerte, etc. ; et

- l'entreprise ou organisme ne doit à aucun moment inciter les utilisateurs potentiels du dispositif à témoigner de manière anonyme. A cet égard, toute publicité concernant l'existence du dispositif doit en tenir compte, et ce dernier

doit être conçu de façon à ce que les utilisateurs soient amenés à s'identifier lors de la procédure d'alerte.

V. Information des personnes concernées

- ***Information de l'utilisateur potentiel du dispositif***

Conformément à l'article 14 de la loi n° 1.165, modifiée, et nonobstant l'information collective prévue par les conventions collectives professionnelles, la Commission demande à ce que l'utilisateur potentiel du dispositif soit clairement et individuellement informé :

- de l'identité du responsable du dispositif et le cas échéant de celle de son représentant à Monaco ;
- de la finalité du traitement et les domaines concernés par le dispositif ;
- du caractère facultatif du dispositif, et partant, de l'existence d'autres voies de recours hiérarchiques classiques ;
- de l'absence de conséquence ou sanction du fait de la non-utilisation du dispositif ;
- de l'identité des destinataires ou catégories de destinataires des alertes ;
- de l'existence de droits d'accès, d'opposition, de rectification et de suppression relativement aux informations le concernant.

Par ailleurs, la Commission demande à ce que l'utilisateur du dispositif soit également informé que l'utilisation abusive du dispositif peut l'exposer à des sanctions disciplinaires et à des poursuites judiciaires, mais qu'à l'inverse, l'utilisation de bonne foi du dispositif, si les faits ne donnent lieu à aucune suite, ne l'exposera à aucune sanction.

- ***Information de la personne visée par l'alerte***

Conformément aux articles 13 et 14 de la loi n° 1.165, modifiée, la Commission demande à ce que la personne faisant l'objet d'une alerte en soit informée dès l'enregistrement, informatisé ou non, des données la concernant, afin de lui permettre de s'opposer pour des raisons légitimes au traitement de ces dernières.

Lorsque des mesures conservatoires sont nécessaires, notamment pour prévenir la destruction de preuves relatives à l'alerte, l'information de la personne n'intervient qu'après l'adoption desdites mesures. Cette information, réalisée selon des modalités permettant de s'assurer de sa bonne délivrance à la personne concernée, précise, notamment, le nom de l'entité responsable du dispositif, les faits reprochés, les éventuels destinataires de l'alerte ainsi que les modalités d'exercice de ses droits d'accès, d'opposition, de rectification et de suppression.

VI. Respect des droits d'accès, de rectification et de suppression

Conformément aux articles 13, 15 et 16 de la loi n° 1.165 du 23 décembre 1993, modifiée, la Commission rappelle que le responsable de traitement est tenu de garantir à toute personne identifiée dans le cadre du dispositif d'alerte professionnelle le droit d'accéder aux données la concernant et d'en demander, si elles sont inexactes, incomplètes, équivoques, périmées, ou illicites, la rectification ou la suppression.

Elle souligne également que la personne qui fait l'objet d'une alerte ne saurait, sur le fondement de son droit d'accès, obtenir communication d'informations concernant l'identité de l'émetteur de l'alerte.

VII. Personnes ayant accès aux informations et destinataires

- ***Service interne à l'entreprise ou organisme, ou au groupe***

Vu les principes posés à l'article 10-1 de la loi n° 1.165, modifiée, et afin de garantir la confidentialité des informations collectées, la Commission considère que les personnes ayant accès aux informations sont, sous réserve d'externalisation du service, celles spécialement chargées du recueil ou du traitement des alertes au sein de l'entreprise ou organisme concerné.

Elle rappelle que conformément à l'article 17-1 de la loi n° 1.165, modifiée, le responsable de traitement est tenu de définir nominativement la liste de ces personnes, habilitées à avoir aux accès aux informations dans le stricte cadre de l'accomplissement de leurs missions.

En outre, la Commission relève que les données traitées peuvent également être communiquées aux personnes spécialement chargées de la gestion des alertes au sein du groupe de sociétés auquel appartient l'entreprise ou organisme concerné, dès lors que cette communication est nécessaire à la vérification de l'alerte ou résulte de l'organisation même du groupe.

En tout état de cause, la Commission rappelle qu'eu égard à la sensibilité des données traitées, l'ensemble des personnes susvisées est astreint à une obligation de confidentialité stricte. A cet effet, le responsable de traitement devra envisager toutes mesures utiles, y compris l'externalisation du service si nécessaire, aux fins de garantir le respect de la confidentialité des données.

- ***Externalisation du service auprès d'un prestataire***

S'il est fait recours à un prestataire de service pour le recueil et le traitement des alertes, la Commission rappelle que les employés spécialement chargés de ces missions ne doivent accéder à tout ou partie des données visées au point III que dans la limite de leurs attributions respectives.

Elle demande à ce que le prestataire de service désigné s'engage, par voie contractuelle, à :

- déterminer nominativement la liste des personnes autorisées à avoir accès au traitement et aux données y contenues, conformément aux dispositions de l'article 17-1 de la loi n° 1.165, modifiée ;
- ne pas utiliser les informations à des fins détournées ;
- assurer leur confidentialité ;
- 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 d'informations nominatives au terme de sa prestation.

En outre, eu égard à la sensibilité des données traitées, la Commission demande à ce que les personnes chargées du recueil et du traitement des alertes, qui devront être en nombre limité, soient spécialement formées et astreintes à une obligation renforcée de confidentialité contractuellement définie.

VIII. Transferts de données à caractère personnel hors pays disposant d'un niveau de protection adéquate

La Commission rappelle que dans les cas où les communications d'informations envisagées au point VII de la présente délibération impliquent un transfert d'informations nominatives vers un pays ne disposant pas d'un niveau de protection adéquate au sens de l'article 20 de la loi n° 1.165, modifiée, lesdites communications devront s'opérer conformément aux dispositions spécifiques de la loi dont s'agit, et notamment son article 20-1 alinéa 2.

IX. Mesures de sécurité et de confidentialité

La Commission demande à ce que le responsable de traitement prenne toutes précautions utiles pour préserver la sécurité des données, tant à l'occasion de leur collecte que de leur traitement ou de leur communication, en application des dispositions des articles 17 et 17-1 de la loi n° 1 .165, modifiée.

A ce titre, elle exige que les accès au traitement s'opèrent par le biais d'un identifiant et d'un mot de passe individuels, régulièrement renouvelés, ou par tout autre moyen d'authentification. En outre, lesdits accès devront faire l'objet d'une journalisation aux fins de contrôle par les personnes habilitées à cet effet.

Ces moyens techniques sont sans incidence sur la nécessité du responsable de traitement de sensibiliser son personnel au respect de la confidentialité des données, et plus généralement, à la législation relative à la protection des informations nominatives.

X. Durée de conservation

La Commission demande à ce que soient détruites sans délai les informations relatives à une alerte, considérée dès son recueil comme n'entrant pas dans le champ du dispositif tel que défini au point II de la présente délibération.

Par ailleurs, elle considère que lorsque l'alerte n'est pas suivie d'une procédure disciplinaire ou judiciaire, les informations y afférentes doivent être détruites dans un délai de deux mois à compter de la clôture des opérations de vérification.

Enfin, lorsqu'une procédure disciplinaire ou judiciaire est engagée à l'encontre de la personne mise en cause ou de l'auteur d'une alerte abusive, la Commission rappelle que les informations relatives à l'alerte pourront être conservées jusqu'au terme de la procédure.

APRES EN AVOIR DELIBERE :

Rappelle que :

- d'une manière générale, les traitements automatisés ou non automatisés d'informations nominatives afférents à des dispositifs d'alerte professionnelle doivent respecter les principes de la loi n° 1.165, modifiée, tels qu'interprétés par la présente délibération ;

- les traitements automatisés d'alerte professionnelle sont soumis à l'autorisation de la Commission de Contrôle des Informations Nominatives, en application de l'article 11-1 de la loi n° 1.165, modifiée ; seuls ceux respectant les termes de la présente délibération donneront lieu à une autorisation de mise en œuvre ;

- la délibération n° 2009-14 du 23 novembre 2009 portant recommandation sur les dispositifs d'alerte professionnelle est annulée.

Le Président,

Michel Sosso