ACTUALITES DES ALERTES PROFESSIONNELLES : LE MUR DE L'ATLANTIQUE EST FRANCHI !

Les alertes professionnelles sont apparus et se sont développées aux Etats unis sous l'effet conjugué du barème de peines fédérales (Sentencing Federal Guidelines) de 1991 qui invitait les juges américains à tenir compte de la qualité et de l'efficacité de la « politique éthique » de l'entreprise dans la fixation des peines et des dispositions de la Loi Sarbane Oxley (SOX).

Les entreprises et l'administration française ont initialement accueilli assez fraichement l'arrivée de ces dispositifs d'alertes professionnelles. Ce qui peut aisément se comprendre tant il paraissait inconcevable de vouloir transposer littéralement un outil qui provient d'une culture anglo-saxonne dans un système qui, culturellement, n'est pas prêt à le recevoir.

Toutefois et contrairement à ce que l'on a pu lire dans les journaux il y a quelques années, les alertes éthiques ont finalement, non seulement franchi l'atlantique, mais elles se sont aussi durablement installées dans le paysage culturel et juridique français à telle enseigne que la CNIL, autrefois plutôt réfractaire à ces dispositifs, a décidé d'élargir le champ d'application de 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 professionnelle et de faire preuve de davantage de souplesse à l'égard des alertes anonymes.

1. ELARGISSEMENT DU CHAMP D'APPLICATION DE DE L'AU-004

Tout traitement informatisé de données (dispositifs d'alerte professionnelle inclus) mis en place au sein d'une entreprise doit être soumis au contrôle de la CNIL par voie de déclaration ou d'autorisation selon le cas. Se soustraire à cette formalité, même par négligence, est passible de sanctions pénales *(5 ans*

d'emprisonnement et 300.000 € d'amende : Article 226-16 du Code pénal).

Devant le développement des alertes professionnelles et consciente de la nécessité de simplifier les formalités, la CNIL a adopté par délibération n°2005-305 du 8 décembre 2005 une autorisation unique de traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle. Jusqu'à la récente délibération du 30 janvier 2014, les entreprises pouvaient ainsi, en vertu de cette autorisation unique, se contenter de déclarer leur traitement dès lors que l'alerte professionnelle respectait les conditions décrites dans cette autorisation et en particulier :
- recueillir uniquement des signalements de faits graves de nature comptable ou financière, de lutte contre la corruption ou encore relatifs à des manquements au droit de la concurrence,
- informer les utilisateurs sur l'objet du traitement, l'identité du responsable du traitement, et lorsqu'ils ont fait l'objet d'une alerte,
- conserver les données que le temps nécessaire à la procédure,
- satisfaire aux conditions de transfert hors Union Européenne, en cas de transmission à des tiers en dehors du territoire européen.

Toutefois, entre 2011 et 2013, la Commission a été amenée à traiter près d'une soixantaine de demandes d'autorisations spécifiques relatives à des domaines n'entrant pas dans le champ d'application de l'AU-004 et ne pouvant dès lors entrer dans le cadre du régime des formalités simplifiées. C'est dans ce contexte que la CNIL a décidé d'étendre l'Autorisation Unique aux domaines de la lutte contre les discriminations et du harcèlement, de la santé, de l'hygiène et de la sécurité au travail, ainsi que de la protection de l'environnement. En outre, la CNIL a étendu les fondements juridiques pouvant justifier la mise en place d'une alerte professionnelle puisqu'il n'est plus nécessaire de « répondre à une obligation législative ou réglementaire », mais de répondre « à une obligation légale ou à un intérêt légitime de l'entreprise».

Depuis une délibération du 30 janvier 2014 (n°2014-042), il est dorénavant prévu que peuvent bénéficier d'un engagement de conformité, les organismes mettant en œuvre des traitements automatisés de données à caractère personnel ayant pour finalité le signalement d'alertes dans les domaines suivants, et ce, dès que la mise en œuvre de ces traitements répond à une obligation légale ou à un intérêt légitime de l'entreprise dans ces domaines :
- financier, comptable, bancaire et de la lutte contre la corruption ;
- pratiques anticoncurrentielles ;
- lutte contre les discriminations et le harcèlement au travail ;
- santé, hygiène et sécurité au travail ;
- protection de l'environnement.

Des lors que le dispositif porte sur les points évoqués ci-dessus, une simple déclaration suffit. Les dispositifs d'alerte portant sur d'autres domaines doivent faire l'objet d'une autorisation.

2. ANONYMAT

Les dispositifs d'alerte éthique doivent être conçus par les entreprises uniquement comme un moyen complémentaire par rapport aux autres modes d'alerte existants

(intervention des représentants du personnel, du commissaire aux comptes, d'une autorité publique....). L'utilisation du dispositif d'alerte doit donc demeurer facultative, le salarié devant en effet pouvoir, s'il souhaite alerter sur des dysfonctionnements qu'il constate, s'adresser aux institutions existantes dans leur domaine respectif (délégués du personnel, délégué syndical notamment).

La question des alertes anonymes est en revanche une question épineuse. La CNIL a finalement estimé que « le recueil de ces alertes doit nécessairement être toléré » mais encadré.

Le lanceur d'alerte doit en principe s'identifier. En effet, aux termes de la délibération CNIL (n° 2014-042) en date du 30 janvier 2014, est consacré le principe selon lequel l'auteur de la dénonciation doit s'identifier et ne pas être incité à rester anonyme de sorte que pour être accueilli dans l'ordre juridique français un dispositif d'alerte doit :

- en principe prévoir que les auteurs d'alertes mettant en cause des comportements attribués à des personnes désignées doivent s'identifier afin d'assurer leur protection contre d'éventuelles représailles et d'éviter des dérapages vers la délation et la dénonciation calomnieuse.
- ne prévoir la possibilité pour la personne usant de ce droit d'alerte de conserver l'anonymat que dans des situations bien précises :

i. la gravité des faits mentionnés est établie et les éléments factuels sont suffisamment détaillés ;
ii. le traitement de cette alerte doit être entouré de précautions particulières, telles qu'un examen préalable, par son premier destinataire, de l'opportunité de sa diffusion dans le cadre du dispositif.

Il convient par ailleurs d'indiquer que le recours excessif ou injustifié à l'anonymat est un des éléments retenus par certaines juridictions pour suspendre l'application d'un dispositif d'alerte litigieux (*TGI Caen 5 novembre 2009 n° 09-287 ; TGI Libourne 15 septembre 2005 n° 05-143*).

Ces changements importants montrent l'acceptation croissante de ces dispositifs d'alerte par notre système juridique. Et cela ne fait que commencer !

Mohamed OULKHOUIR,
Chassany Watrelot & Associés

Chassany Watrelot & Associés
AVOCATS - DROIT SOCIAL