CNIL

Délibération n°2010-369 du 14 octobre 2010 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 professionnelle

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

Vu le décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifié par le décret n°2007-451 du 25 mars 2007 ;

Vu la délibération n°2005-305 de la Commission nationale de l'informatique et des libertés du 8 décembre 2005 ;

Vu le document d'orientation relatif aux dispositifs d'alerte professionnelle adopté par la Commission le 10 novembre 2005;

Après avoir entendu M. Emmanuel de GIVRY, commissaire, en son rapport, et Mme Elisabeth ROLIN, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

La Commission a adopté le 8 décembre 2005 une délibération portant autorisation unique (AU-004) de traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle (« whistleblowing »).

Par un arrêt n°2524 du 8 décembre 2009, la chambre sociale de la Cour de cassation a mis en lumière les difficultés d'interprétation de certaines dispositions de l'autorisation unique n°AU-004, en particulier ses articles 1er et 3.

En effet, l'article 3 de l'autorisation unique n°AU-004 du 8 décembre 2005 prévoit que « *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* ».

A cette occasion, la Cour de cassation a rappelé que la mise en œuvre d'un dispositif d'alerte professionnelle, faisant l'objet d'un engagement de conformité à l'autorisation unique, devait se limiter aux seuls domaines comptables, financiers, et de lutte contre la corruption définis à l'article 1er et que l'article 3 ne devait pas être interprété comme permettant un élargissement de la finalité des dispositifs d'alertes tels que prévus par l'autorisation unique.

Dans ce contexte, il est apparu nécessaire à la Commission de clarifier son autorisation unique, les organismes aspirant légitimement à une plus grande sécurité juridique. Préalablement, elle a mené de nouvelles auditions des principaux acteurs concernés par les dispositifs d'alerte pour déterminer dans quelle mesure il y a lieu de modifier les termes de l'autorisation unique.

Par ailleurs, depuis 2005 la Commission a eu l'occasion d'autoriser à de nombreuses reprises, dans le cadre du régime d'autorisation spécifique, des dispositifs d'alerte élargis aux pratiques anticoncurrentielles, ainsi que ceux fondés sur la loi japonaise dite « Japanese SOX ». La Commission a souhaité prendre en compte ces évolutions dans l'autorisation unique en modifiant son champ d'application en ce sens.

Décide :

Article 1er

Le dernier alinéa de l'article 1er relatif aux finalités du traitement est rédigé comme suit :

« Conformément à l'article 7-5° de la loi du 6 janvier 1978 modifiée, entrent également dans le champ de la présente décision :

- les traitements mis en œuvre dans les domaines précités par les entreprises concernées par la section 301(4) de la loi américaine dite «Sarbanes-Oxley» du 31 juillet 2002, ainsi que par la loi japonaise « Financial Instrument and exchange Act » du 6 juin 2006 dite « Japanese SOX ».
- les traitements mis en œuvre pour lutter contre les pratiques anticoncurrentielles au sein de l'organisme concerné ».

Article 2

La phrase suivante de l'article 3 est supprimée : « *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* ».

Article 3

Les deux premiers alinéas de l'article 6 sont ainsi rédigés :

« 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.

Lorsque l'alerte n'est pas suivie d'une procédure disciplinaire ou judiciaire, les données relatives à cette alerte 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 ».

Article 4

L'article 12 est ainsi rédigé :

« Article 12. Dispositions transitoires

Les responsables de traitements de données à caractère personnel dont la mise en œuvre est régulièrement intervenue avant la publication de la délibération n°2010-369 du 14 octobre 2010 et qui ne respectent pas strictement les conditions fixées aux articles 1er et 3 de l'autorisation unique modifiée, disposent d'un délai de 6 mois, à compter de la publication de la délibération n°2010-369, pour mettre leurs traitements en conformité ».

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

Le président

Alex Türk