ALAIN BENSOUSSAN
Juristendances Informatique et Libertés
n° 37 – Janv.- Fév. 2011

DISPOSITIFS D'ALERTE PROFESSIONNELLE : LA CNIL RÉVISE L'AUTORISATION UNIQUE AU-004 !

La délicate interprétation des dispositions de l'autorisation unique AU-004

L'enjeu

▪ Par **délibération du 14 octobre 2010** (1), la Cnil a redéfini le champ d'application de l'autorisation unique n°AU-004 relative aux dispositifs d'alerte professionnelle.

▪ Rappelons qu'à la suite de la **réglementation américaine Sarbanes-Oxley**, de nombreuses sociétés internationales opérant au sein de l'Union européenne ont instauré un système de collecte d'informations nominatives relatives à des comportements anormaux (« ***whistleblowing*** »).

- clarifier les dispositions de l'autorisation unique n°AU-004

- restreindre son champ d'application aux domaines comptable, financier, bancaire et de lutte contre la corruption.

▪ Considérant que de tels dispositifs constituent des **traitements relevant de** l'**article 25, I-4° de la loi du 6 janvier 1978** modifiée, donc soumis à autorisation, la Cnil a adopté, par délibération du 8 décembre 2005, l'autorisation unique n°AU-004 relative aux dispositifs d'alerte professionnelle visant notamment « *les domaines financier, comptable, bancaire et de lutte contre la corruption* ».

▪ A cet égard, l'**article 3** de l'autorisation unique du 8 décembre 2005 prévoyait 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* ». Une majorité d'entreprises pensait donc s'être mise en conformité en adhérant à l'autorisation unique intégrant les cas de **mise en jeu de l'intérêt vital de l'entreprise ou de l'intégrité physique ou morale de ses employés**, que les remontées puissent être faites de manière anonyme ou non.

(1) Cnil, Délibération 2010-369 du 14-10-2010
(2) Cass. soc. 8-12-2009 n°08-17191

Clarification et restriction du champ d'application de l'autorisation unique

Calendrier

▪ Par **arrêt du 8 décembre 2009** (2), 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 **doit se limiter aux seuls domaines comptable, financier et de lutte contre la corruption définis à l'article 1er** et que l'article 3 ne permet pas un élargissement de la finalité des dispositifs d'alerte.

▪ Par voie de conséquence, la Cnil, après avoir auditionné les principaux acteurs concernés par les dispositifs d'alerte (organisations syndicales, institutions publiques, groupes internationaux, etc.), a modifié l'autorisation unique. La **nouvelle rédaction de l'autorisation unique du 14 octobre 2010** clarifie l'article 3 et fait preuve d'une interprétation restrictive de l'arrêt de la Cour de cassation :

- en élargissant l'article 1er de l'autorisation unique à la loi américaine «Sarbanes-Oxley», à la loi japonaise « *Japanese SOX* » et aux traitements mis en œuvre pour lutter contre les pratiques anticoncurrentielles au sein de l'organisme concerné ;

- en supprimant du champ d'application de l'autorisation unique les faits mettant en jeu l'intérêt vital de l'entreprise ou l'intégrité physique ou morale de ses employés.

Les responsables de traitements disposent d'un délai de 6 mois, soit jusqu'au **8 juin 2011**, pour mettre en conformité leurs dispositifs d'alerte professionnelle à la réglementation Informatique et libertés.

▪ Les dispositifs exclus du champ d'application de la nouvelle autorisation, tels que ceux couvrant les domaines de la discrimination notamment, devront donc faire l'objet d'une **demande d'autorisation normale** auprès de la Cnil, complétée d'un dossier présentant les **fondamentaux techniques, juridiques et sécuritaires.**

CHLOE TORRES

LES FICHIERS COMMUNAUX DE CONSTATATION D'INFRACTIONS PENALES

Une procédure de déclaration simplifiée valant engagement de conformité

L'enjeu

- rappeler que les communes n'ont pas besoin d'une autorisation spécifique pour chacun des traitements relatifs à la recherche et la constatation d'infraction.

- sensibiliser les collectivités locales au respect des règles issues de la loi informatique et libertés.

(1) Circulaire n°IOCD1032722C du 15-12-2010.

▪ Le ministre de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration a publié une circulaire le **15 décembre 2010** (1) à l'intention des préfets de département pour leur rappeler les formalités auxquelles sont soumis les fichiers de constatation d'infractions pénales mis en œuvre par la police municipale.

▪ La mise en œuvre de traitements de données à caractère personnel par les services de police municipale obéit à un cadre juridique défini conjointement par les ministères de l'Intérieur, de la Justice et la Cnil, par l'**arrêté du 14 avril 2009** (RU-9).

▪ Cet arrêté élabore des procédures de **déclaration « simplifiées »** et définit les règles de fonctionnement des fichiers mis en œuvre par les communes dès lors qu'ils ont pour objet la recherche et la constatation des infractions pénales.

▪ Ces fichiers correspondent notamment à la constitution de **mains courantes** destinées à enregistrer les interventions d'agents verbalisateurs, de fichiers relatifs aux **listings de contraventions** ou encore à l'élaboration et au suivi de procès verbaux.

Le ministre rappelle les obligations des maires

Les perspectives

▪ Dans la circulaire prise en application de l'arrêté, le ministre rappelle que leur mise en œuvre peut être constitutive d'**atteintes aux libertés individuelles** et publiques.

▪ Les élus et responsables locaux doivent en prendre conscience car leur **responsabilité juridique**, y compris pénale, peut être engagée.

▪ La circulaire a donc un double objectif, celui de préciser que les communes n'ont pas besoin d'une autorisation spécifique pour chacun des traitements relatifs à la recherche et la constatation d'infraction et de sensibiliser les collectivités locales au respect des règles issues de la loi informatique et libertés du 6 janvier 1978.

Le directeur des libertés publiques et des affaires juridiques Laurent Touvet signataire de la circulaire, demande à ce que lui soient rapportées toutes difficultés rencontrées dans la mise en oeuvre des instructions évoquées.

▪ Rappelons que **la Cnil peut contrôler une collectivité locale** au même titre que n'importe quel organisme, public ou privé. Le secteur public (administrations d'État et collectivités locales) fait d'ailleurs partie, pour la deuxième année consécutive, du programme annuel de contrôle de la Cnil et a représenté en 2009, plus de 10 % des procédures engagées par la formation restreinte (commission des sanctions).

▪ Les contrôles réalisés ont montré que de **nombreuses collectivités ne respectaient pas certaines règles** de base de la loi informatique et libertés :

- catégories d'informations pouvant être recueillies,
- durée de conservation,
- sécurité des données, etc.

▪ C'est pourquoi la circulaire rappelle la disposition de l'article 12 de son arrêté d'application qui prévoit que la mise en oeuvre par les communes de ce type de traitements demeure subordonnée à l'envoi préalable d'un « **engagement de conformité** » aux prescriptions de l'arrêté du 14 avril 2009.

EMMANUEL WALLE

La mise en œuvre de la nouvelle autorisation unique AU-004 suppose-t-elle l'accomplissement de certaines formalités ?

L'essentiel

▪ **Non**, il n'est aucunement nécessaire de procéder à une nouvelle déclaration de conformité à l'autorisation unique n°AU-004 si le périmètre du dispositif d'alerte professionnelle instauré au sein de l'organisme concerné respecte le nouveau champ d'application de l'autorisation unique, tel que défini par la Cnil par délibération en date du 14 octobre 2010 (1).

(1) Autorisation unique AU-004 modifiée par la délibération 2010-369 du 14-10- 2010

▪ Les organismes ayant déjà adressé à la Cnil un engagement de conformité à l'AU-004 et qui ne respecteraient pas strictement les conditions posées à l'article 1er de l'autorisation unique modifiée, bénéficient d'un délai de six mois pour se conformer à la réglementation Informatique et libertés.

▪ Les dispositifs non conformes à l'autorisation unique, en particulier les dispositifs applicables en matière de propriété intellectuelle ou de discrimination, doivent faire l'objet d'une demande d'autorisation spécifique. Les dossiers feront l'objet d'un examen individuel par la Commission, en vue « *d'encadrer ces nouveaux mécanismes de remontées d'alertes afin de garantir les droits et libertés des personnes concernées, conformément à la loi Informatique et libertés*».

Il n'est pas nécessaire de procéder à une nouvelle déclaration de conformité à l'AU-004 si le périmètre du dispositif d'alerte professionnelle respecte le nouveau champ défini par la CNIL.

Le champ d'application de l'autorisation unique a-t-il été modifié ?

▪ **Oui**, la Cnil a modifié les dispositions de l'article 3 de l'autorisation unique afin d'exclure du champ d'application de l'AU-004 les traitements réalisés sur la base d'un dispositif dénonçant des comportements susceptibles de mettre en jeu l'intérêt vital de l'entreprise ou l'intégrité physique ou morale de ses employés.

▪ En vertu de l'article 1er de l'autorisation unique modifiée, seuls peuvent désormais faire l'objet d'un engagement de conformité les traitements mis en œuvre dans le cadre d'un dispositif signalant des manquements graves en rapport avec les domaines comptable, financier, bancaire et de lutte contre la corruption, les traitements réalisés pour lutter contre les pratiques anticoncurrentielles au sein de l'organisme concerné, ainsi que ceux relevant de la loi américaine dite « Sarbanes-Oxley » ou de la loi japonaise dite « Japanese SOX ».

Une définition plus claire et plus rigoureuse du champ d'application de l'autorisation unique.

Les données exclues du dispositif peuvent-elles faire l'objet d'un traitement informatique ?

▪ **Non**, les données relatives à une alerte considérée, dès son recueil par le responsable du traitement, comme exclues du champ d'application du dispositif ne peuvent en aucune façon être exploitées. L'autorisation unique modifiée prévoit, à l'article 6, que ces données sont détruites ou archivées sans délai.

▪ Lorsque l'alerte n'est suivie d'aucune procédure disciplinaire ou judiciaire, les données relatives à cette alerte sont détruites ou archivées par le service en charge de la gestion des alertes dans un délai de deux mois à compter de la clôture des opérations de vérification.

▪ 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 le service en charge de la gestion des alertes jusqu'au terme de la procédure.

▪ Les données archivées sont conservées via un système d'information distinct d'accès restreint pour une durée n'excédant pas les délais de procédures.

Les organismes qui ont déjà fait une déclaration de conformité à l'AU-004 et qui ne respecteraient pas strictement les conditions fixées à l'article 1er de l'autorisation unique modifiée, disposent d'un délai de 6 mois pour mettre leurs traitements en conformité.

Sécurité publique : un magistrat référent est institué !

▪ Un décret du **13 décembre 2010** (1) est venu modifier le décret du 16 octobre 2009 portant création d'un traitement de données à caractère personnel relatif à la prévention des atteintes à la sécurité publique.
▪ Saisie pour avis, la Cnil a considéré que la modification envisagée « *vise à **renforcer les garanties offertes aux mineurs** en créant un référent national chargé de veiller au respect de ce droit* » (2).
▪ Membre du Conseil d'Etat, ce référent, assisté d'adjoints issus du corps des tribunaux administratifs et des cours administratives d'appel, bénéficiera de prérogatives complémentaires de celles de la Cnil, dans la mesure où il « *exercera une activité consultative au bénéfice de l'administration et non une activité de contrôle extérieur et indépendant* ».

(1) Décret 2010-1540 du 13-12-2010.

(2) Cnil, Délib. 2010-029 du 04-02-2010.

Justice : création d'un portail accessible au grand public

▪ Le ministère de la justice et des libertés est autorisé, par arrêté du **8 décembre 2010** (3), à créer un traitement automatisé de données à caractère personnel mis en oeuvre dans le cadre du portail www.teleservices.justice.gouv.fr, dénommé « *Portail d'accès grand public à la justice* ».
▪ Ce portail, en accès sur le site internet www.vos-droits.justice.gouv.fr, a pour objet de mettre à la disposition des usagers un ensemble de services qui permet de **dématérialiser les échanges** de divers actes d'administration judiciaire entre le public et les juridictions compétentes et leur greffe, et les greffes des établissements pénitentiaires.

(3) Arrêté du 08-12-02010.

E-santé : la Cnil autorise le lancement du dossier médical personnel

▪ La Cnil a annoncé, par un communiqué de presse du **14 décembre 2010** (4), qu'elle autorisait les applications informatiques nécessaires à la première phase de généralisation du Dossier Médical Personnel (DMP).
▪ Destiné à permettre le regroupement et le partage entre professionnels et établissements de santé des informations jugées utiles à la coordination des soins, il devrait être **progressivement déployé sur l'ensemble de la France** sous la responsabilité de l'Agence des Systèmes d'Information Partagés de Santé (ASIP Santé).

(4) Cnil, communiqué du 14-12-2010.

Réseaux sociaux : consultez le profil de la Cnil en ligne…

▪ Un communiqué de la Cnil du **16 décembre 2010** (5) précise que la Commission dispose désormais d'un profil sur les réseaux participatifs Viadeo et LinkedIn, après avoir ouvert un compte sur Facebook et Twitter.
▪ La Commission entend ainsi « *informer les membres de ces réseaux professionnels sur le métier de **correspondant informatique et libertés (Cil)** et l'intérêt qu'il représente pour les entreprises et les administrations* ».

(5) Cnil, communiqué du 16-12-2010.

Directeur de la publication : Alain Bensoussan
Rédigée par les avocats et juristes de ALAIN BENSOUSSAN SELAS
Animée par Chloé Torres et Isabelle Pottier, avocats
Diffusée uniquement par voie électronique
ISSN 1634-071X
Abonnement à : paris@alain-bensoussan.com