Juristendances Informatique et libertés

Lettre électronique bimestrielle réalisée par ALAIN BENSOUSSAN - AVOCATS

n° 14 – mars / avril 2007

Un nouveau décret modifiant le décret d'application de la loi Informatique et libertés

L'essentiel

- Un **décret** a été adopté le 25 mars 2007 **modifiant** celui du 20 octobre 2005 pris pour l'**application de la loi du 6 janvier 1978** relative à l'informatique, aux fichiers et aux libertés

- Outre des mesures destinées à **améliorer le dispositif existant**, ce décret a introduit deux séries de dispositifs : l'un relatif aux **obligations incombant au responsable** de traitement et aux droits des personnes ; l'autre portant sur le **transfert de données** à caractère personnel vers les Etats n'appartenant pas à la Communauté européenne.

- S'agissant de la première série de dispositions, le décret du 25 mars 2007 précise d'une part, le contenu et les modalités de l'**obligation d'information** incombant au responsable du traitement en distinguant selon que la **collecte** des informations est effectuée **par écrit**, **oralement** ou par **voie électronique**.

- Ce même texte précise d'autre part, les conditions dans lesquelles les personnes peuvent exercer les droits que leur reconnaît la loi Informatique et libertés : **droit d'opposition**, droit **d'accès direct**, droit **de rectification**.

- Dans tous les cas, la personne concernée devra être en mesure de justifier de son **identité** par la photocopie d'un titre d'identité portant la signature du titulaire, lorsque la demande est effectuée par écrit ou par tout autre moyen, lorsqu'elle est présentée sur place. Le responsable du traitement doit **répondre** à la demande **dans les deux** mois suivants sa réception, le silence gardé valant décision de refus.

- S'agissant de la seconde série de dispositions relatives au **transfert de données** vers des pays tiers à l'Union européenne, le texte définit les formalités préalables incombant au responsable de traitement envisageant un tel transfert de données en distinguant selon que le **niveau de protection** est suffisant ou non et selon que le transfert requiert ou un non une décision ou un **avis de la Cnil**.

- Le texte précise l'obligation pour la Cnil d'**informer** les responsables de traitement, le public et **les autorités européennes**.

L'attention doit être attirée sur l'importance que revêt ce décret notamment par l'impact qu'il peut avoir sur les conditions devant être respectées lors de la collecte des informations auprès des personnes concernées et dans le cadre des formalités préalables à réaliser en cas de transfert de données à caractère personnel hors Union européenne.

(1) Décret n° 2007-451 du 25/03/2007, *JO* du 28/03/2007.

Chloé Torres
chloe-torres@alain-bensoussan.com

Impact sectoriel

La Cnil use de son pouvoir de sanction pécuniaire à l'égard des entreprises « récalcitrantes »

Une condamnation à 30 000 € pour manque de coopération

L'essentiel

Les responsables de traitement doivent particulièrement veiller au contenu de leurs déclarations et doivent impérativement répondre à toutes les demandes de la Cnil, sous peine de sanction particulièrement sévère

Un traitement de données à caractère personnel a été déclaré à la Cnil par la **société Tyco Healthcare France** en septembre 2004.

Considérant qu'il lui manquait des éléments indispensables à l'**instruction du dossier**, la Cnil a adressé plusieurs courriers au déclarant, lui demandant notamment de **décrire les finalités** précises du traitement, de préciser les cas d'envois de données à l'étranger, de donner les **lieux d'implantation des serveurs**, d'indiquer les **mesures de sécurité** assurant la confidentialité des données et de préciser la **durée de conservation** des données.

La société n'ayant pas répondu aux demandes de la Cnil, cette dernière lui a adressé une **mise en demeure** (1) la sommant de **répondre aux demandes**.

En réponse à cette mise en demeure, le responsable du traitement a écrit à la Cnil et indiqué que le traitement avait été suspendu. Suite à cette réponse, la Cnil a effectué un **contrôle sur place** et constaté que le traitement n'était pas suspendu et qu'il était utilisé en dépit des nombreuses incertitudes relevées par la Cnil.

Aussi, la Cnil a considéré que la société n'avait « *pas pris la mesure de la gravité des manquements qui lui étaient reprochés concernant son manque de coopération et de transparence* » et a prononcé à son encontre une **sanction pécuniaire de 30 000€** sur le fondement des articles 45 et suivants de la loi informatique et libertés (2).

Cette sanction de la Cnil est intéressante à plusieurs égards. Tout d'abord, elle confirme la **tendance de la Cnil** a user de ses pouvoirs et sanctionner lourdement tout obstacle à son action.

Ensuite, cela révèle une certaine **prise d'autonomie** de la Cnil qui choisit de prononcer elle même une sanction, plutôt que de s'en remettre au parquet sur le fondement d'un éventuel délit d'entrave à l'action de la Commission.

Enfin, cette décision démontre, s'il en était besoin, que la Cnil opère un **contrôle minutieux des traitements** qui lui sont simplement déclarés et pas uniquement des traitements soumis au régime d'autorisation.

(1) Délib. du 10 mai 2006.
(2) Délb. n°2006-281 du 14/12/2006.

Les FAQ juristendances

Sources

Les salariés peuvent-ils consulter leurs données d'évaluation ?

Oui Les données d'évaluation professionnelle des salariés sont généralement considérées par les responsables des ressources humaines comme des **informations sensibles** et, dès lors, confidentielles. Cette confidentialité est parfois opposée au salarié qui souhaite accéder à son dossier en invoquant la loi informatique et libertés.

Lors de sa séance plénière du **8 mars 2007**, la CNIL a ainsi examiné des plaintes dirigées à l'encontre d'une grande entreprise internationale pour refus de communication à ses cadres de leur "classement" et de leur "potentiel de carrière" précis (1).

(1) Cnil, En Bref, du 13/04/2007, www.cnil.fr

La Commission a considéré que les valeurs de "**classement annuel**" ("ranking ") et de "**potentiel**" sont des données communicables au salarié concerné dès lors qu'elles ont été prises en compte pour décider de son **augmentation de salaire**, de sa promotion, de son affectation, etc.

La CNIL réaffirme donc le principe selon lequel un employé doit pouvoir accéder à des **données de gestion des ressources humaines** qui ont servi, à prendre une décision à son égard.

Une autorisation de la Cnil est-elle obligatoire pour la biométrie ?

Oui Tous les traitements comportant des **données biométriques** doivent faire l'objet d'une autorisation préalable de la CNIL. D'une manière générale, la CNIL n'autorise que les dispositifs où l'empreinte digitale est **enregistrée** exclusivement sur un **support individuel** (carte à puce, clé USB), et non dans une base centralisée.

La CNIL a adopté le **27 avril 2006** (2) **trois autorisations uniques** en matière de biométrie. Elle encadre ainsi les modalités d'utilisation et simplifie les formalités déclaratives de certains dispositifs biométriques :

(2) Délib. n°2006-101, 102, 103 du 27 avril 2006, www.cnil.fr

- le contour de la main pour le contrôle d'accès, la gestion des horaires et de la restauration sur les lieux de travail ;
- l'empreinte digitale exclusivement enregistrée sur un support individuel pour le contrôle de l'accès aux locaux sur les lieux de travail ; - le contour de la main pour l'accès au restaurant scolaire.

Actualité

Sources

Traitement des infractions dans les transports

Le 11 janvier 2007, la Cnil a adopté une **autorisation unique** qui permet aux sociétés de transports publics mettant en œuvre des fichiers de **suivi de contravention**, de déclarer leur traitement en conformité à la norme d'autorisation unique (1).

Le traitement ainsi mis en œuvre permet d'assurer le **suivi des procès-verbaux** émis par les agents habilités à constater les infractions dans les transports publics de voyageurs. La Cnil exige que les destinataires de ce fichier soient limitativement déterminés. La conformité à la norme d'autorisation implique de respecter un délai de conservation restreint

(1 Délib. n° 2007-002 du 11/01/2007.

Expérimentation de lecture automatisée des plaques d'immatriculation

En application de l'article 8 de la loi du 23 janvier 2006 relative à la **lutte contre le terrorisme**, le ministère de l'Intérieur a soumis à l'**avis de la Cnil** un projet d'arrêté relatif à une expérimentation de deux ans de LAPI. Grâce à des **caméras vidéos** installées sur six **véhicules de police**.

Ce dispositif permettra de capter et de stocker une image de la plaque d'immatriculation et de prendre la photographie des occupants des véhicules. En cas d'alerte, les policiers pourront accéder aux images pour contrôler le numéro d'immatriculation ainsi que les informations figurant dans le fichier des véhicules volés et signalés. L'arrêté relatif à une expérimentation de deux ans de LAPI a été publié au Journal officiel le **3 mars 2007** suite à l'avis rendu par la Cnil le **8 février 2007**.

(2) Cnil, Echos des séances du 15/03/2007.

·

Chartes d'éthique et systèmes d'alerte professionnelle

Le rapport sur les dispositifs d'alerte professionnelle (« **whistleblowing** ») vient d'être rendu public (3).

Les auteurs concluent qu'il n'est **pas urgent de légiférer**. Il semble toutefois nécessaire de **s'entendre sur une définition unique** de la notion de dispositif d'alerte professionnelle, de préciser les conditions dans lesquelles il doit être mis en place et de formaliser une protection de celui qui l'aurait, de bonne foi, utilisé.

(3) http://www.alain-bensoussan.com/pages/1087/

Directeur de la publication : Bensoussan Alain
Rédigée et animée par Chloé Torres, Virginie Bensoussan-Brulé, Aude Gérard et Isabelle Pottier
Diffusée uniquement par voie électronique
ISSN (en cours)
Abonnement à : avocats@alain-bensoussan.com