Juristendances Informatique et libertés

Lettre électronique bimestrielle réalisée par ALAIN BENSOUSSAN - AVOCATS

n° 21 – mai / juin 2008

Les flux transfrontières de données personnelles

De la centralisation intra-groupe à la délocalisation de centres d'appel

Les enjeux

Concilier la liberté de circulation des données et la protection des personnes dont les données à caractère personnel sont transférées.

▸ La loi Informatique et libertés impose une **réglementation stricte** pour l'exportation des données à caractère personnel hors Union européenne dans les pays n'ayant pas une protection suffisante (1).

▸ Or, il existe de nombreuses situations susceptibles de générer des **transferts internationaux** de données et dont il faut tenir compte lors de la déclaration de traitement et surtout, de son exploitation.

▸ Des entreprises françaises qui communiquent avec des partenaires, des sociétés **filiales** ou mères ou qui ont des activités situées **hors de l'Union européenne** sont des situations dans lesquelles se produiront des transferts internationaux de données à caractère personnel.

▸ De même, la centralisation intra-groupe de la base de données de gestion des commandes, de la comptabilité clients, ou de la gestion des ressources humaines d'un **groupe multinational**, ou encore la délocalisation de centres d'appel constituent autant de situations qui entraîneront des transferts de données à caractère personnel hors des frontières communautaires.

(1) Pour une étude, cf. « Informatique et libertés », éd. Francis Lefebvre 2008.

Cas ne nécessitant pas d'autorisation de la Cnil

Les règles

Tout transfert vers un pays extérieur à la Communauté européenne est interdit si ce pays n'assure pas un niveau de protection suffisant, sauf dérogations définies de manière restrictive, à l'article 69 de la loi de 1978 modifiée.

▸ La Commission européenne a établi une **liste des pays** accordant une protection adéquate. Il s'agit des vingt-cinq pays de l'Union européenne, des pays membres de l'Espace Economique Européen (2), des pays ayant fait l'objet d'une reconnaissance de protection adéquate (3). En ce qui concerne les Etats-Unis, un accord au titre du **Safe Harbor**, a été négocié.

▸ La Cnil n'a pas à autoriser les transferts vers les pays dont la protection est jugée adéquate. Cette situation est gérée lors des formalités déclaratives.

▸ Pour les **pays tiers** n'ayant pas une protection suffisante, l'opération de transfert n'est possible que si elle entre dans les **dérogations** définies de manière restrictive à l'article 69 de la loi de 1978, à défaut de quoi, une **autorisation de la Cnil** est nécessaire. Elle s'obtient en encadrant le flux d'échanges par une **convention de flux transfrontières** ou des **règles internes**.

▸ Les **règles internes** (codes de bonne conduite, chartes) constituent pour les groupes de sociétés une **alternative à la convention de flux**. Adoptées de manière unilatérale par la direction du groupe, elles évitent de conclure autant de contrats qu'il existe de transferts de données en son sein.

(2) Islande, Liechtenstein, Norvège.
(3) Argentine, Canada, Guernesey, Ile de Man, Suisse, entreprises US adhérentes au Safe Harbor.

Chloé Torres
chloe-torres@alain-bensoussan.com

Impact sectoriel

Vidéosurveillance : la Cnil prône une redéfinition du cadre juridique

Dualité des régimes juridiques applicables

Aux termes d'une note sur les difficultés d'application des règles relatives à la vidéosurveillance adressée à Madame Michèle Alliot-Marie, Ministre de l'intérieur (1), la Cnil a souhaité attirer l'attention du gouvernement sur les **risques d'une multiplication des caméras de surveillance** sans une clarification de leur régime juridique.

La Cnil souligne le nombre croissant de demandes de conseil et de **plaintes du public** et des professionnels du fait de leur incompréhension des règles applicables.

En effet, les systèmes de vidéosurveillance peuvent relever de **deux régimes distincts** :

- la loi n°95-73 du 21 janvier 1995 (dite **loi Pasqua**) soumettant les systèmes de vidéosurveillance visionnant les lieux ouverts au public à une autorisation préfectorale :
- la **loi Informatique et libertés** réglementant les systèmes de vidéosurveillance installés dans un lieu non ouvert au public ou implantés dans des lieux publics lorsqu'ils sont couplés ou intégrés à un traitement de données à caractère personnel.

Face à cette dualité des régimes juridiques applicables, la Cnil se propose d'encadrer et d'accompagner le développement de la vidéosurveillance.

Le développement des systèmes de vidéosurveillance numérique

Actuellement, l'installation d'un système de vidéosurveillance numérique, dans la mesure où il constitue un **traitement automatisé de données à caractère personnel**, relève des dispositions de la loi du 6 janvier 1978 modifiée en 2004, et nécessite l'accomplissement de **formalités préalables** auprès de la CNIL.

Que le lieu soit ouvert au public ou non (entrepôts, réserves, bureaux fermés au public) :

- un **système numérique** enregistrant des images sur un support informatisé doit faire l'objet d'une déclaration auprès de la CNIL ;
- l'utilisation d'une **technique biométrique couplée** à un système de vidéosurveillance nécessite l'autorisation de la Cnil (art. 25-8° et 27).

Seuls les systèmes de vidéosurveillance « **analogiques** » (enregistrant sur bande magnétique) mis en oeuvre dans des **lieux ouverts au public** relèvent uniquement de la compétence du **Préfet**, au titre de la loi Pasqua. Cette dernière doit être revue au regard des évolutions que connaît la vidéosurveillance vers le tout numérique.

L'enjeu

Le développement des dispositifs de vidéo-surveillance rend nécessaire une clarification du cadre juridique applicable pour éviter toute dérive et garantir le respect des droits individuels.

(1) Cnil, www.cnil.fr

Les conseils

La mise en œuvre d'un système de vidéosurveillance nécessite :

- le respect des formalités préalables auprès de la Cnil ;

- l'information des personnes par voie d'affichage ;

- la consultation des instances représentatives du personnel (IRP) au titre de l'introduction d'une nouvelle technologie.

Les FAQ juristendances

Remarques

Quels sont les droits reconnus aux personnes physiques ?

Les droits des personnes sur leurs données sont renforcés par la loi Informatique et libertés modifiée. Les responsables de traitement ont l'obligation de délivrer une **information détaillée** sur les conditions d'utilisation des données que la collecte soit directe ou indirecte. La loi précise le **droit d'accès** et à **rectification** des données à caractère personnel par les intéressés. Elle maintient le **droit d'opposition** et précise qu'il est discrétionnaire et sans frais lorsque les données sont utilisées à des fins de prospection, notamment commerciale (1).

(1) L. du 6-1-1978 modifiée, art. 32, 38, 39 et 40.

Qu'est ce que le droit à l'information ?

Toute personne a le droit de savoir si elle est fichée et dans quels fichiers elle est recensée. Le droit à l'information sur ses propres données à caractère personnel vise aussi bien la collecte des informations que leur utilisation.

Toute personne qui met en œuvre un fichier ou un traitement contenant des données à caractère personnel doit informer les personnes fichées, sauf si elle l'a été au préalable, de :

- l'identité du responsable du traitement ;
- l'objectif de la collecte d'informations ;
- le caractère obligatoire ou facultatif des réponses ;
- les conséquences de l'absence de réponse ;
- les destinataires des informations ;
- les droits reconnus à la personne ;
- les éventuels transferts de données vers un pays hors de l'Union européenne (2)

Un décret institue des **contraventions de police** à l'encontre de quiconque aura recueilli ou fait recueillir des données à caractère personnel, oralement ou par voie de questionnaire, sans avoir au préalable informé la personne interrogée (Décr. 2005-1309 du 20-10-2005 art. 90, *JO* du 22-10-2005).

Lorsque les données à caractère personnel sont recueillies **par voie de questionnaires ou formulaires**, ceux-ci doivent porter mention de l'identité du responsable de traitement, de la finalité du traitement, du caractère obligatoire ou facultatif des réponses et des droits d'accès, de rectification et d'opposition.

En cas de **collecte indirecte** des données à caractère personnel (via des cookies), toute personne utilisatrice des réseaux de communications électroniques doit être informée de la finalité de cette collecte et des moyens de s'y opposer dès l'enregistrement de ses données ou lors de leur première communication. De plus, les personnes doivent être informées de l'emploi éventuel de témoins de connexion (cookies, variables de session…) et de la récupération d'informations sur la configuration de leurs ordinateurs (systèmes d'exploitation, navigateurs…).

(2) L. du 6-1-1978 modifiée, art. 32 I.

Actualité

La Cnil délibère sur la prévention et à la gestion des impayés

Sources

▸ La Cnil a adopté une **décision d'autorisation unique** relative aux traitements automatisés de données à caractère personnel mis en œuvre par les **commerçants** relatifs à la prévention et la gestion des impayés par chèque bancaire, qui s'engagent à respecter les conditions figurant dans le tableau joint en annexe de sa délibération du **10 avril 2008**.

(1) Délib. n° 2008-097 du 10 avril 2008, www.cnil.fr

Données collectées par les moteurs de recherche

▸ Le groupe des **27 Cnil européennes** vient d'adopter à l'unanimité un avis (2) précisant que les données personnelles enregistrées par les moteurs de recherche, doivent être **effacées au plus tard au bout de 6 mois**.

▸ De nouvelles discussions devront s'engager avec les moteurs de recherche afin de déterminer comment mettre en œuvre l'ensemble de ces mesures pour éviter l'explosion des plaintes.

(2) Document de travail WP 148 du groupe de travail «Article 29» adopté, le 4 avril 2008 http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_fr.htm

Correspondant Informatique et Libertés : la Cnil créée un logo

▸ La CNIL innove en créant un **logo** qu'elle met à disposition des sociétés ayant désigné un Correspondant Informatique et Libertés (CIL).

▸ Ce logo permet aux entreprises d'**afficher sur l'ensemble de leurs supports** leur politique de transparence et de conformité informatique et libertés.

▸ Un précieux outil qui peut être utilisé comme facteur de différentiation.

Consécration de l'autorité judiciaire de la Cnil par le Conseil d'état

▸ Dans un arrêt du **19 février 2008**, le Conseil d'Etat a qualifié la Cnil de « **juridiction** » au sens de l'article 6-1 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales (3).

(3) CE, 19 février 2008, Ord. référé n°311974, http://www.alain-bensoussan.com/Documents/250389.doc

La CNIL condamne les commentaires douteux sur les salariés

▸ La CNIL a infligé une amende de **40.000 euros** à la société Service Innovation Groupe France (SIG) en raison de commentaires subjectifs figurant dans le fichier des salariés (4).

(4) Délib. n° 2007-374 du 11 décembre 2007, www.cnil.fr

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