Juristendances Informatique et libertés

Lettre électronique bimestrielle réalisée par ALAIN BENSOUSSAN - AVOCATS

n° 15 – mai / juin 2007

Annulation par le Conseil d'Etat de quatre délibérations de la Cnil !

Erreurs d'appréciation de la Cnil dans ses délibérations

‣ Les quatre sociétés requérantes, la SACEM, la SDRM, la SPPF et la SCPP voulaient mettre en place **un dispositif de surveillance** des internautes à partir d'une sélection d'adresses IP résultant de requêtes sur les réseaux Peer to Peer. Une fois identifiés, ceux qui mettaient gratuitement en ligne moins de 50 fichiers musicaux devaient recevoir un **message d'avertissement** leur signalant les conséquences juridiques des actes de contrefaçon. Pour les autres, elles envisageaient un **contrôle renforcé** avec une surveillance de **15 jours** des personnes concernées qui, une fois les preuves réunies, auraient pu faire l'objet de poursuites civiles ou pénales.

‣ La Cnil, dans ses délibérations du 18 octobre 2005[1], a refusé d'autoriser de tels traitements considérant qu'ils étaient **disproportionnés** au regard de la finalité poursuivie car ils aboutissaient à **une collecte massive de données** et pouvaient permettre la surveillance exhaustive et continue des réseaux d'échanges de fichiers.

‣ Le Conseil d'Etat a estimé dans son arrêt du 13 mai 2007 que la Cnil avait commis une erreur d'appréciation car compte tenu de **l'importance de la pratique des échanges de fichiers musicaux sur internet** et du nombre limité de **titres musicaux surveillés**, les traitements présentés étaient proportionnés. Le Conseil d'Etat a également estimé que la Cnil avait commis une erreur d'appréciation en considérant que les traitements envisagés reposaient uniquement sur des **critères quantitatifs**.

La Cnil n'est pas censurée sur l'envoi de messages pédagogiques

‣ Le Conseil d'Etat a toutefois considéré que les **envois de messages pédagogiques** étaient illégaux dans la mesure où ils ne relèvent pas des cas de figure où les fournisseurs d'accès à internet sont autorisés à conserver les **données de connexion** des internautes. Ce point ne pouvait toutefois justifier à lui seul les refus adoptés par la Cnil.

‣ Cette décision du Conseil d'Etat laisse ainsi la porte ouverte aux sociétés de droits d'auteur qui souhaiteraient mettre en œuvre de tels dispositifs de recherche et de constatation de contrefaçon sur internet.

L'essentiel

Le Conseil d'Etat, pour annuler les délibérations de la Cnil, a considéré qu'elle avait commis des erreurs d'appréciation en estimant que les traitements envisagés aboutissaient à une collecte massive de données et pouvaient permettre la surveillance exhaustive et continue des réseaux d'échange de fichiers. Concernant l'envoi de messages pédagogiques, le Conseil d'Etat considère toutefois que ces envois sont illégaux dans la mesure où ils ne relèvent pas des cas de figure où les fournisseurs d'accès à internet sont autorisés à conserver les données de connexion des internautes.

([1]) Délibérations n°2005-235 à 238 du 18 octobre 2005.

Aude Gerard
aude-gerard@alain-bensoussan.com
Olivier Proust
olivier-proust@alain-bensoussan.com

Impact sectoriel

La Cnil demande plus de transparence dans l'affaire Swift

Information de l'opinion et des pouvoirs publics sur l'évolution de l'affaire

L'essentiel

La Cnil suit l'évolution de l'affaire Swift pour s'assurer du respect des données à caractère personnel et bancaires transmises aux autorités américaines.

- Dans un communiqué publié le 13 juin 2007 sur son site internet, la Cnil réaffirme sa demande de transparence dans **l'affaire Swift**.

- Cette affaire a été révélée par la presse américaine le 23 juin 2006. Il s'agit de l'existence d'un **programme de surveillance** des transactions bancaires internationales mises en place par la CIA après les attentats du 11 septembre 2001, afin de lutter contre le financement du terrorisme.

- Cette surveillance permettrait de connaître le montant de la transaction, l'identité de l'expéditeur et du destinataire transitant par Swift, qui est le principal réseau international de messagerie utilisé dans le domaine bancaire.

- Dans un avis de novembre 2006, **le groupe de l'article 29** (groupe de coordination des autorités européennes de protection des données) avait jugé que la société Swift n'avait pas respecté les règles européennes de protection des données notamment en prêtant son concours à la mise en œuvre du programme de surveillance des données bancaires et financières par les autorités américaines.

- Le groupe a également jugé que les institutions financières avaient une part de responsabilité dans cette affaire.

- Suite à cet avis, les institutions européennes ont pris contact avec les **autorités américaines** pour négocier avec elles les conditions dans lesquelles les données extraites de la base de données Swift pourraient être traitées par ces dernières. Il semble que des **règles d'usage** en la matière pourraient être fixées par un échange de lettres.

- Par ailleurs, la société Swift a engagé une réflexion relative à la **refonte** de la structure globale de son réseau informatique, accueillie favorablement par la Cnil dans la mesure où elle permettrait une évolution vers une régionalisation du réseau de la société Swift.

- Enfin, la Cnil qui appelle à plus de **transparence** en la matière a pris contact avec les institutions françaises concernées ainsi qu'avec la fédération bancaire française et le groupement des utilisateurs de Swift en France pour suivre l'évolution de cette affaire.

Les FAQ juristendances

Le responsable des lieux doit-il être informé des contrôles sur place de la Cnil ?

Non, lorsque la Cnil effectue un contrôle sur place, elle peut informer au plus tard au début du contrôle le responsable des lieux de l'objet des vérifications qu'elle compte entreprendre, ainsi que de l'identité et de la qualité des personnes chargées du contrôle. Lorsque le responsable du traitement n'est pas présent sur les lieux du contrôle, ces informations sont portées à sa connaissance dans les 8 jours suivants le contrôle. Le contrôle ne peut être effectué qu'entre 6 heures et 21 heures. C'est le procureur de la République dans le ressort territorial duquel doit avoir lieu la visite ou la vérification qui est informé préalablement par écrit du contrôle sur place. Ce dernier est informé au plus tard 24 heures avant la date à laquelle doit avoir lieu le contrôle sur place. Cet avis précise la date, l'heure, le lieu et l'objet du contrôle.

Est-il nécessaire d'informer les personnes sur les flux transfrontières de données les concernant ?

Oui, le décret du 20 octobre 2005 a été modifié par le décret du 25 mars 2007 (1), notamment sur l'obligation d'informer les personnes concernées sur le transfert de données. Ainsi, le responsable du traitement doit communiquer à la personne auprès de laquelle des données à caractère personnel sont recueillies les informations suivantes :

- le ou les pays d'établissement du destinataire des données dans les cas où ce ou ces pays sont déterminés lors de la collecte des données ;
- la nature des données transférées ;
- la finalité du transfert envisagé ;
- la ou les catégories de destinataires des données ;
- le niveau de protection offert par le ou les pays tiers.

Sur ce dernier point, la mention d'information doit préciser si le ou les pays tiers destinataires des données figure dans la liste des décisions de la Commission européenne considérée comme ayant un niveau de protection suffisant, et doit mentionner la décision de la Commission européenne qui autorise ce transfert. Enfin, si les données sont transférées vers un état hors Union européenne qui n'assure pas un niveau de protection suffisant au sens de l'article 68 de la loi Informatique et libertés, la mention légale d'information doit préciser l'exception prévue à l'article 69 de cette même loi qui permet ce transfert ou la décision de la Cnil qui autorise ce transfert. Le non-respect de ces dispositions relatives à l'information des personnes peut faire l'objet de sanctions pénales (2).

Sources

(1) Décret n° 2007-451 du 25 mars 2007 et délibération n° 2006-218 du 28 septembre 2006

(2) art. R.625-10 du Code pénal.

www.cnil.fr

Actualité

Sources

La Cnil rappelle sa préoccupation sur les dispositifs biométriques

La Cnil vient de rappeler sa vigilance en matière de **biométrie** afin de préserver les **libertés** de chaque individu. Ce communiqué fait suite à un avis rendu public le 31 mai 2007 du **Comité Consultatif National d'Ethique pour les sciences de la vie et de la santé** qui s'inquiétait sur la biométrie.

La Cnil rappelle ainsi que l'utilisation de ces dispositifs est subordonnée à l'information individuelle des personnes concernées et à son autorisation préalable. Elle examine chaque dispositif en prenant en compte **les caractéristiques de la biométrie** utilisée et les **risques** qu'elles comportent pour les libertés individuelles et la protection des données personnelles.

Elle n'autorise l'enregistrement des empreintes digitales dans une base centralisée que si cette technologie se justifie par un **fort impératif de sécurité**. Le Président de la Cnil a souligné que le nombre de dossiers en matière de dispositifs biométriques a considérablement augmenté et a exprimé sa préoccupation compte tenu de l'insuffisance des moyens qui lui sont attribués pour contrôler l'émergence de tels moyens de technologie.

Communiqué 01/06/2007
www.cnil.fr

Traitement des données bancaires par les hôtels

La Cnil rappelle les règles encadrant le traitement des données bancaires des clients et le respect par un hôtel de ses obligations en matière de gestion d'un fichier client. Elle insiste sur la nécessité **d'effacer** les données bancaires une fois la transaction réalisée afin d'éviter l'utilisation frauduleuse des numéros de carte bancaire. Les hôtels doivent par ailleurs prendre des **mesures** garantissant la **sécurité** et la **confidentialité** des informations, notamment protéger **l'accès** aux fichiers clients par un mot de passe et chiffrer les données bancaires stockées. Enfin, les clients doivent être **informés** sur les conditions de traitement de leurs données et des droits qui leur sont reconnus par la loi.

Brève 29/05/2007
www.cnil.fr

Lutte contre le blanchiment : modification de l'autorisation unique

L'autorisation unique n°AU-003 du 1er décembre 2005 ([1]) consacrée au traitement de données personnelles relatives à la **lutte contre le blanchiment et le financement du terrorisme** ne prévoyait pas la possibilité de partager les informations au sein des groupes bancaires. Depuis l'entrée en vigueur du décret du 26 juin 2006, les personnes désignées au sein des organismes financiers pour occuper la fonction de correspondant **Tracfin** peuvent se transmettre les informations sur leur clientèle relatives à l'existence et aux suites des **déclarations de soupçon** adressées au service Tracfin.

([1])Modifiée par la délibération n°2007-060 du 25 avril 2007.

Brève 28/05/2007
www.cnil.fr

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