Juristendances Informatique et libertés

Lettre électronique bimestrielle réalisée par ALAIN BENSOUSSAN - AVOCATS

n° 07 – janv. / fév. 2005

Hébergement de données de santé : le nouveau régime issu du décret du 4 janvier 2006

Les professions visées par ces nouvelles mesures

Le décret du 4 janvier 2006 fixe le cadre juridique applicable aux **hébergeurs de données de santé** à caractère personnel (1).

Le Code de la santé publique permet en effet aux **professionnels de santé** ou aux **établissements de santé** de « *déposer des données de santé à caractère personnel, recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins, auprès de personnes physiques ou morales agréées à cet effet* » (2).

Les conditions d'agrément des hébergeurs

L'hébergeur devra notamment définir et mettre en œuvre une **politique de confidentialité** et de sécurité permettant d'assurer le respect des droits des personnes concernées par les données hébergées, la **sécurité de l'accès** aux informations et la **pérennité des données** hébergées.

La prestation d'hébergement devra faire l'objet d'un **contrat** entre l'hébergeur et son client (établissement de santé, médecins…) comportant **neuf clauses obligatoires** parmi lesquelles : une clause mentionnant les **indicateurs de qualité** et de performance permettant la vérification du niveau de qualité de service annoncé et la périodicité de leur mesure, une clause décrivant les **prestations réalisées**, une autre relative aux **obligations de l'hébergeur** à l'égard de la personne à l'origine du dépôt des données de santé à caractère personnel, en cas de modifications ou d'évolutions techniques introduites par lui, une autre relative à **l'information** sur les conditions de recours à d'éventuels prestataires techniques externes et les engagements de l'hébergeur pour que soit assuré un niveau équivalent de garantie au regard des obligations pesant sur l'activité d'hébergement, et enfin une clause traitant de l'information sur les **garanties permettant de couvrir toute défaillance** éventuelle de l'hébergeur.

L'agrément est délivré aux hébergeurs de données de santé pour **trois ans renouvelables** et le ministre de la santé peut procéder au retrait ou à la suspension de l'agrément dans certaines conditions.

L'essentiel

Ces nouvelles dispositions induiront :

- le déploiement de process nouveaux et la mise en place d'un schéma directeur visant à se conformer aux dispositions de la loi «Informatique et libertés».
- l'adaptation des contrats d'hébergement existants.
- l'établissement d'un dossier d'agrément en bonne et due forme.

(1) Décret n° 2006-6, *JO* du 5 janvier 2006.
(2) Cf. «*Informatique, Télécoms, internet*», Ed. Fr. Lefebvre 2004.

Alain Bensoussan
alain-bensoussan@alain-bensoussan.com
Chloé Torres
chloe-torres@alain-bensoussan.com

Impact sectoriel

La Cnil a réalisé un audit des principaux sites internet de banque en ligne

Un bilan plutôt positif…

Au cours du **premier semestre 2005**, la Cnil a procédé à une série de contrôles dans le secteur de la banque en ligne. Ce contrôle a été effectué à partir de grilles d'audit soumises aux responsables de **dix sites internet bancaires**.

Cette opération a permis d'**évaluer** la qualité de la **confidentialité** et de la **sécurité** des sites bancaires et de mettre en évidence leurs éventuelles faiblesses, pointées par la Cnil. Fort de ces constats, la Cnil établit une liste des **7 bonnes pratiques à adopter** notamment :

- la vérification de l'orthographe de l'adresse du site,
- la prohibition de tout accès aux comptes à partir d'un cybercafé,
- l'interdiction formelle de cliquer sur un lien reçu par email (phishing).

Une nouvelle forme d'action de la Cnil

Un tel audit représente une **nouvelle forme de l'action de la Cnil**, dans le cadre de sa mission de contrôle et d'information.

Si la portée de cet audit est incertaine d'un point de vue strictement juridique, cette action démontre une volonté apparente de la Cnil de contrôler certains traitements, tout en limitant son intervention à un aspect **plus pédagogique** que coercitif.

Bien que les résultats de cet **audit** soient **anonymisés**, cette démarche révèle une évolution dans l'action de la Cnil et son implication dans toutes ses missions.

Cela doit par conséquent **alerter** les **responsables de traitement** sur deux risques émergents :

- D'une part, dans le contexte actuel de renforcement des pouvoirs de la Cnil, de tels audits constituent très certainement un préalable à une phase de contrôles assortie de sanctions.

- D'autre part, ces audits donnent une **importante publicité aux pratiques** des responsables de traitement et à leurs éventuelles lacunes ; cette tendance de la Cnil à l'information du public est donc source de risques pour l'image d'entreprises dont les traitements ne seraient pas conformes à la loi.

L'enjeu

Vérifier le respect des dispositions de la loi «Informatique et Libertés» concernant la sécurité et à la prospection commerciale de la banque en ligne.

(1) disponible sur le site www.cnil.fr/

Les conseils

Augmenter le niveau de confidentialité et de sécurité par:

- des mises en garde sécuritaires lors de chaque connexion ;

- l'envoi des mots de passe en LRAR ;

- des transactions sécurisées « https » dès l'échange des identifiant et mot de passe.

Les FAQ juristendances

Sources

Peut-on exiger que soient modifiées certaines informations contenues dans un fichier ?

Oui, une personne peut exiger que soient rectifiées, complétées, clarifiées, mises à jour, verrouillées ou effacées les informations inexactes, incomplètes, équivoques, périmées ou illégalement enregistrées la concernant [1].

(1) Loi n°78-17 de la loi du 6 janvier 1978 modifiée, art. 40.

La cession d'une base de données personnelles est-elle possible ?

Oui, si elle a été initialement déclarée à la Cnil. Dans le cas contraire, il est obligatoire de soumettre la nouvelle finalité à la Cnil. L'identité du nouveau destinataire de la base de données doit être communiquée aux personnes fichées, lesquelles pourront éventuellement mettre en œuvre leur droit d'opposition.

A défaut, la **responsabilité** du producteur pourrait se trouver engagée, ce qui peut être de nature à constituer un obstacle à la cession.

Les blogs doivent-ils être déclarées auprès de la Cnil ?

Non, depuis une recommandation de la Cnil du 22 novembre 2005. La Cnil a précisé les règles applicables aux blogs et a décidé de les **dispenser** de déclaration.

(2) Norme d'exonération n° 6, *JO* du 17/12/2005.

Parallèlement à cette dispense, la Cnil a lourdement insisté sur le fait que les règles de la loi de 1978 s'appliquent aux blogs diffusant ou collectant des données à caractère personnel [2].

Existe-t-il une procédure simplifiée de déclaration pour les recherches biomédicales ?

Oui, la CNIL a mis en place une procédure simplifiée de déclaration en homologuant une méthodologie de référence pour les traitements de données personnelles mis en œuvre dans le cadre des recherches biomédicales traduisant ainsi, dans le secteur de la recherche, la volonté de simplifier les formalités pour des applications conduites dans le cadre d'exigences législatives et réglementaires strictes.

Un seul engagement de conformité, adressé directement à la CNIL, est suffisant dès lors que le traitement mis en œuvre est conforme à la méthodologie de référence.

Actualité

Sources

La Cnil simplifie la déclaration des dispositifs de whistleblowing

- La Cnil fixe les conditions de mise en œuvre des **dispositifs d'alertes** et de **dénonciation** «(whistleblowing) au sein des entreprises.
- La procédure d'**autorisation unique** n'est ouverte qu'aux dispositifs considérés comme légitimes par la Cnil, c'est-à-dire ceux répondant à une **obligation légale d'ordre public économique**, national ou international.
- La Norme précise aussi certaines exigences en terme de proportionnalité et de **transparence du dispositif**, ainsi qu'en matière de protection des personnes [(1)].
- La mise en conformité avec la norme implique de mettre en place des **processus de sécurisation** juridique des dispositifs (structures dédiées au traitement des alertes, respect des droits de personnes…).
- L'adoption par la Cnil d'une norme d'autorisation unique laisse entrevoir la perspective de **contrôles a posteriori**, susceptibles de mettre en jeu la **responsabilité pénale** des responsables de traitements.

(1) Norme d'autorisation unique n°AU-004 du 08/12/2006 disponible sur le site de la Cnil.

La Cnil commente la loi « antiterrorisme »

- La Cnil revient sur la **loi du 23 janvier 2006** relative à la lutte contre le terrorisme [(2)]. Seules certaines de ses propositions ont été prises en compte.
- Elle devrait de nouveau **être saisie pour avis** lors de l'élaboration des décrets d'applications et faire des **préconisations** sur les finalités des traitements, la nature des données traitées, leurs durées de conservation et la sécurité.

(2) Cnil, Echos des séances du 16/02/2006 http://www.cnil.fr/

La protection des données sur le passeport européen

- Les Etats membres de l'Union européenne ont deux obligations : intégrer dans les documents d'identité, la **photographie** faciale numérisée et les **empreintes digitales** [(3)].
- Le **G29** [(4)] préconise d'attendre le rapport du projet européen **ETIB** (Ethique des Technologies d'Identification Biométrique) avant de se lancer.

(3) Règlement CE n°2252/2004 http://www.cnil.fr/

(4) Groupe des autorités européennes de protection des données.

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

Flash : Deuxièmes assises des Correspondants Informatique et libertés

Désigné par le responsable du traitement, le correspondant Informatique et Libertés permet à ce même responsable de bénéficier d'un régime juridique allégé. Cette innovation majeure, issue de la directive communautaire 95/46/CE, a fait l'objet d'un décret en Conseil d'Etat du 20 octobre 2005.

En tant que co-fondateur de l'Association française des correspondants à la protection des données à caractère personnel (AFCDP), le cabinet Alain Bensoussan a le plaisir de vous annoncer la tenue des deuxièmes assises des correspondants Informatique et libertés.

Mardi 28 février 2006 se tiendront les deuxièmes Assises des Correspondants Informatique et Libertés qui se dérouleront de 9h à 12h30, dans les locaux de l'Institut Catholique de Paris - Salle des Actes - 21 rue d'Assas - 75006 Paris.

Au cours de la matinée, Alex Türk, Président de la CNIL, Christoph Klug, Directeur Général de GDD (Association allemande pour la Protection et la Sécurité des Données), Ludovic Denis, Président de l'AFCDP, Maître Alain Bensoussan et Alain Borghesi, Vice-Présidents de l'AFCDP, se succéderont pour aborder les dimensions stratégiques et juridiques de la loi d'août 2004 et du décret d'octobre 2005, mais aussi les aspects plus concrets liés au statut, aux missions ou à la formation des Correspondants.

Pour les membres de l'AFCDP, le déjeuner sera suivi de l'Assemblée Générale de l'association de 14h30 à 17h.

Programme prévisionnel disponible sur : http://www.afcdp.org/pages/rub_eve_assises2006.htm
Bulletin d'inscription sur http://www.afcdp.org/pdf/Bulletin-inscription-AFCDP2006.pdf