

Les traitements de données biométriques

Les décisions de la Cnil en matière de biométrie

Conseils

▸ La loi Informatique et libertés modifiée en août 2004 a introduit une nouveauté en soumettant au **régime strict d'autorisation** de la Commission nationale de l'informatique et des libertés (Cnil), la **biométrie sécuritaire**. Parallèlement, la Cnil a développé une doctrine applicable aux **différents usages** de la biométrie. Cette doctrine distingue les technologies dites « **sans trace** » et celles qui sont considérées comme **laissant des traces**.

▸ Une décision de la Cnil en date du **7 juin 2005** ⁽¹⁾ admet l'utilisation de techniques biométriques à titre commercial et de confort dès lors que **certaines conditions** de mise en oeuvre sont respectées. Cette décision porte sur un système de **carte de fidélité** comprenant la reconnaissance de l'empreinte digitale des titulaires de la carte afin de permettre aux personnes inscrites dans un programme de fidélité de bénéficier de services préférentiels. L'**empreinte digitale** est exclusivement stockée sur la carte de fidélité et il n'y a aucun caractère obligatoire.

- Etudier la finalité poursuivie par le traitement de données biométriques.

- Justifier le caractère proportionné du projet.

▸ Par ailleurs, la Cnil a autorisé dans une décision du **5 juillet 2005** ⁽²⁾ l'utilisation de la technique de la **reconnaissance du contour de la main** pour remplacer les **badges de contrôle** des horaires dans un collège.

(1) Echos des séances Cnil du 27/05/2005, <http://www.cnil.fr/index.php?id=1839>

(2) Séances des 21 juin et 5 juillet 2005, <http://www.cnil.fr/index.php?id=1853>

Un examen au cas par cas avant toute autorisation

▸ Bien que ces décisions ouvrent des **perspectives favorables** au développement de la biométrie à titre d'**usage non sécuritaire** et de confort, la Cnil examine au **cas par cas** chaque dossier afin de déterminer l'existence ou non d'un risque d'atteinte aux droits et libertés des personnes.

▸ Cette approche oblige la Cnil à apprécier chaque dispositif sous l'angle de la **proportionnalité**. L'application généralisée du régime d'autorisation alourdit considérablement les délais. L'**adoption prochaine d'une norme d'autorisation** (équivalent des normes simplifiées) devrait changer la donne.

Alain Bensoussan
alain-bensoussan@alain-bensoussan.com
Laurent Caron
laurent-caron@alain-bensoussan.com

Impact sectoriel

Les fichiers de clients et de prospects

La norme simplifiée n°48

▸ La Cnil vient de fournir de **nouveaux repères** en publiant la **norme simplifiée n° 48** relative à la gestion des fichiers de clients et de prospects ⁽¹⁾.

▸ Cette norme inclut la collecte de données par le biais d'**Internet** et la **prospection par voie électronique** et allège la déclaration des fichiers clients et de marketing.

▸ Elle **remplace trois normes simplifiées** : norme n° 11 relative à la gestion des clients actuels et potentiels, norme n° 17 concernant la gestion des fichiers de clientèle des entreprises dont l'objet social inclut la vente par correspondance et norme n° 25 concernant la gestion des fichiers de destinataires d'une publication périodique de presse.

L'enjeu

Vérifier la conformité des traitements de gestion de la relation client

(1) Norme simplifiée n° 48 du 7 juin 2005.

Une gestion plus simple des fichiers de clients et de prospects

▸ Applicable aux **organismes privés et publics**, la nouvelle norme couvre, de façon étendue, les traitements et fichiers relatifs à la gestion et à la prospection des clients, y compris dans le domaine de la **vente à distance** et des **services de communication au public en ligne** (internet, e-mailing, etc.).

▸ La norme n° 48 couvre les **opérations courantes**. D'une part, la gestion des clients : contrats, commandes, livraisons, factures, comptabilité et gestion d'un programme de fidélité. D'autre part, les **opérations relatives à la prospection**: constitution et gestion d'un fichier de prospects, sélection de clients, cession de fichiers, envoi de sollicitation, etc..

▸ La norme comporte **plusieurs limites** à son champ d'application. Ainsi, les traitements susceptibles d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat ou ceux qui reposent sur des interconnexions de fichiers (CRM, etc.) ne peuvent bénéficier de la norme simplifiée n° 48. De même, les **groupes internationaux** doivent prendre en compte le fait que les traitements comportant la transmission de données vers des pays tiers à l'Union européenne ne bénéficient pas de la simplification.

Les conseils

- Analyser la finalité et la sensibilité des traitements

- Porter une attention particulière aux flux de données transfrontaliers

Les FAQ juristendances

Sources

Peut-on sous-traiter la réalisation de traitements de données ?

▸ **Oui**, la loi Informatique et libertés ⁽¹⁾ précise cependant que l'opération de traitement ne peut se faire que sur **instruction du responsable** du traitement.

▸ Le sous-traitant doit présenter des **garanties suffisantes** pour assurer la mise en œuvre des mesures de sécurité et de confidentialité.

▸ Le responsable du traitement doit **établir un contrat** avec le sous-traitant.

(1) Loi n°78-17 de la loi du 6 janvier 1978 modifiée, art. 35.

Doit-on permettre à la personne concernée d'accéder à toutes les informations contenues dans un fichier ?

▸ **Oui**, la loi Informatique et libertés ⁽²⁾ précise que la personne concernée doit se voir communiquer les données qui la concerne ainsi que toute information disponible quant à leur origine.

▸ Une **copie des données** doit être délivrée à la demande de la personne concernée.

▸ Le responsable du traitement peut néanmoins s'opposer aux **demandes manifestement abusives** notamment lorsque celles-ci sont trop nombreuses, répétitives ou systématiques.

(2) Loi n°78-17 de la loi du 6 janvier 1978 modifiée, art. 39.

Quelles sont les formalités préalables à accomplir auprès de la Cnil pour réaliser des transferts internationaux de données ?

▸ Les transferts de données à caractère personnel **hors de l'Union européenne** obéissent à un **régime strict** dans la loi Informatique et libertés ⁽³⁾.

▸ Le transfert de données doit dans tous les cas, faire l'objet d'une **autorisation de la Cnil** quelles que soient les formalités concernées (déclaration simplifiée, déclaration ordinaire...).

▸ Un cadre général de transfert des données à caractère personnel peut être mis en place à travers la notion de **règles internes**. Cette solution dispense l'entreprise de formalités au cas par cas.

(3) Loi n°78-17 de la loi du 6 janvier 1978 modifiée, art. 68 à 70.

Actualité

La Cnil s'oppose à des systèmes de dénonciation ausein d'entreprises

▸ La Cnil a adopté deux **décisions de refus** le 26 mai 2005 concernant pour l'un, la mise en œuvre du **dispositif d'intégrité** professionnelle présenté par la société McDonald's France ⁽¹⁾, pour l'autre, la mise en œuvre du dispositif de « **ligne éthique** » présenté par la Compagnie européenne d'accumulateurs ⁽²⁾.

▸ La Cnil estime que de tels dispositifs sont, dans leur principe même, contraires à la loi « informatique et libertés » parce qu'ils pourraient conduire à un système organisé de **délation professionnelle**.

Sources

(1) Cnil, délib. n°2005- 110.

(2) Cnil, délib. n°2005- 111.

Une norme simplifiée pour la téléphonie fixe et mobile

▸ La Cnil a adopté le 3 février 2005 une nouvelle **norme simplifiée n° 47** relative à l'utilisation de services de téléphonie fixe et mobile sur les lieux de travail ⁽³⁾.

▸ La nouvelle norme s'applique notamment aux données issues de la mise en place d'un **autocommutateur téléphonique**.

(3) Cnil délib. n°2005- 019 publiée au *JO* n°50 du 1^{er} mars 2005.

Un guide pratique sur les transferts de données hors UE

▸ La Cnil a publié en **mai 2005**, un guide pratique sur les transferts de données vers les pays n'appartenant pas à l'Union européenne. Présenté sous la forme de **douze questions-réponses**, ce guide répond de façon détaillée aux principales questions qui se posent en matière de **flux transfrontaliers de données** à caractère personnel ⁽⁴⁾.

(4) Disponible sur le site de la Cnil, <http://www.cnil.fr/>

Un document sur les technologies RFID

▸ Le groupe dit « article 29 » ⁽⁵⁾ a fait un état des lieux des usages de la technologie de **radio-identification** (RFId) et des principes à respecter. Cela permet de connaître le **processus de conformité** à prendre en compte.

(5) Groupe consultatif des autorités des Etats membres de l'UE en charge de la protection des données.

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