ALAIN BENSOUSSAN
Juristendances Informatique et Libertés
n° 41 – Sept. – Oct. 2011

LE VOLET INFORMATIQUE ET LIBERTES DE L'ORDONNANCE DE TRANSPOSITION DU 3EME « PAQUET TELECOM »

Un texte protecteur de la vie privée et des données personnelles

▪ L'**ordonnance du 24 août 2011 transposant le 3ème « paquet télécom »** introduit une protection renforcée de la vie privée et des données personnelles se traduisant par diverses mesures modifiant les dispositions relatives aux «*cookies*», à la prospection directe et à la protection des données à caractère personnel.

▪ Rappelant le principe d'une **information claire et complète de l'internaute** sur l'installation des **cookies**, leur finalité et les moyens de les refuser, l'**article 37** de l'ordonnance subordonne l'accès aux informations déjà stockées dans l'équipement terminal ou l'inscription des informations dans cet équipement au **consentement préalable de l'abonné ou de la personne utilisatrice**.

▪ Ce consentement peut résulter de paramètres appropriés du dispositif de connexion ou de tout autre dispositif placé sous son contrôle. Ces dispositions sont inapplicables aux cookies dits « de navigation » ayant pour principale finalité de « *permettre ou faciliter la communication par voie électronique* », ainsi qu'aux cookies strictement nécessaires à la fourniture d'un service.

▪ La **prospection directe**, visée à l'**article 8** de l'ordonnance, est **interdite** lorsqu'elle est effectuée au moyen de systèmes automatisés d'appel et de communication, d'un télécopieur ou de courriers électroniques et qu'elle utilise les coordonnées d'une personne physique, abonné ou utilisateur, qui n'a pas exprimé préalablement son consentement.

▪ Enfin, l'**article L.121-15-1 du Code de la consommation** pose désormais l'obligation d'indiquer, dans toute publicité adressée par mél, une adresse ou un moyen électronique permettant au destinataire de faire cesser tout nouvel envoi.

Périmètre des obligations de notification du fournisseur de services

▪ L'**article 38** de l'ordonnance prévoit une **procédure spécifique de notification à la Cnil et à l'utilisateur** en cas de « *faille de sécurité* ».

▪ Cet article s'applique aux traitements de données mis en oeuvre dans le cadre de la fourniture de services de communications électroniques sur les réseaux ouverts au public, y compris ceux prenant en charge les dispositifs de collecte de données et d'identification.

▪ Il impose également au fournisseur de ces services d'informer l'intéressé lorsque la faille de sécurité porte **atteinte aux données personnelles ou à la vie privée d'un abonné ou d'une autre personne physique.** Toutefois, la **notification à l'intéressé** n'est plus nécessaire en cas de constatation par la Cnil de **mesures de protection appropriées** mises en oeuvre par le fournisseur pour rendre les données incompréhensibles à toute personne non autorisée. A défaut, la Commission peut mettre en demeure le fournisseur d'informer les intéressés après avoir examiné la gravité de la violation.

▪ Enfin, chacun de ces fournisseurs doit tenir à jour, à la disposition de la Cnil, un **inventaire des violations de données à caractère personnel**, de leur effet et des mesures adoptées pour y remédier.

Les enjeux

- renforcer la lutte contre les faits susceptibles de porter atteinte à la vie privée dans le domaine des communications électroniques

- sécuriser le traitement des données à caractère personnel

(1) Ordonnance du 26-8-2011 ; Rapport du 26-8-2011 ; Arcep, Avis n° 2011-0524 du 10-5-2011

L'essentiel

Les prestataires de services de communications électroniques sont désormais tenus de notifier sans délai à la Cnil toute violation de sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement.

CELINE AVIGNON

BIOMETRIE COMPORTEMENTALE : LA CNIL AUTORISE LA RECONNAISSANCE DE LA FRAPPE AU CLAVIER

Une application biométrique soumise à autorisation de la Cnil

▪ Par délibération en date du 23 juin 2011 (1), la Cnil a autorisé, pour la première fois, l'utilisation d'un dispositif biométrique de reconnaissance par frappe au clavier en vue de conforter l'authentification d'une personne et lui permettre l'accès à un **système d'information de démonstration**.

▪ La biométrie comportementale par frappe au clavier, qui repose sur l'analyse des intervalles de temps séparant les frappes successives des touches d'un clavier lors de la saisie par l'utilisateur de son identifiant et de son mot de passe, permet de **renforcer l'authentification des personnes** autorisées à accéder aux applications ou au système d'information d'une entreprise.

▪ Il est procédé, lors du contrôle d'accès, par comparaison du **gabarit de la frappe au clavier** lors de la tentative d'accès au dispositif par une personne avec le gabarit de sa frappe au clavier enregistré préalablement.

▪ Requérant l'enregistrement de données à caractère personnel, telles le nom, le prénom, le pseudonyme, le gabarit de la frappe au clavier et l'adresse IP, ce dispositif est soumis à autorisation de la Cnil, en vertu des dispositions de l'**article 25-I-8° de la loi Informatique et libertés**.

Périmètre de l'autorisation délivrée à la société JVL

▪ L'autorisation délivrée par la Cnil à la société JVL pour une **finalité strictement définie**, à savoir la démonstration à de potentiels clients du fonctionnement d'un dispositif biométrique de reconnaissance par frappe au clavier, est encadrée par des **règles de sécurité strictes** afin de garantir la confidentialité des données.

▪ Ainsi, seules les données des **personnes volontaires lors des démonstrations** feront l'objet d'un traitement informatisé, leur conservation étant exclue à l'issue de la démonstration.

▪ Les données des **salariés de la société JVL** en charge de la présentation du dispositif seront, quant à elles, supprimées dès lors qu'ils n'auront plus à effectuer la démonstration de ce dispositif biométrique, leurs adresses IP étant conservées pendant six mois à compter du jour de la connexion au dispositif.

▪ Une **note d'information** sera par ailleurs remise aux utilisateurs, lors de la collecte des données, précisant que les données biométriques recueillies seront utilisées **à seule fin de démonstration commerciale**.

▪ Enfin, des mesures de sécurité seront déployées par la société JVL afin de prévenir tout **risque de dispersion des données biométriques**, à savoir le chiffrement des gabarits biométriques des personnes, la mise à disposition des sociétés mettant en œuvre ce dispositif d'une clef de chiffrement personnelle, l'hébergement par JVL de la base de données comportant les gabarits biométriques chiffrés et enfin la vérification de l'absence, sur le poste informatique, de tout logiciel ou dispositif matériel permettant d'enregistrer puis de simuler les caractéristiques de la frappe clavier à l'insu de la personne.

▪ Constatant, au vu de ce qui précède, que le traitement soumis pour examen et en particulier, le recours à la constitution de bases de données biométriques, ne comporte pas de risques particuliers pour la protection des libertés et des droits fondamentaux des personnes, la Cnil a fait droit à la demande de la société JVL.

Les enjeux

Eu égard aux risques associés à l'utilisation de technologies biométriques, il importe que des garanties suffisantes soient apportées concernant notamment la protection de la vie privée, la confidentialité des données collectées et la fiabilité du système de reconnaissance utilisé.

L'essentiel

Est autorisée pour la première fois par la Cnil l'utilisation d'un dispositif biométrique de reconnaissance par frappe au clavier à des fins de démonstration auprès de clients potentiels.

(1) Cnil, Délib. n° 2011-183 du 23-6-2011

CHLOE TORRES

La collecte de données personnelles à des fins de marketing est-elle interdite ?

▪ **Non,** à condition toutefois que les **données** à caractère personnel collectées soient **adéquates, pertinentes et non excessives** par rapport aux finalités pour lesquelles elles sont enregistrées, ainsi qu'en dispose l'article 5 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, signée à Strasbourg le 28 janvier 1981 (1) et l'article 6 de la loi Informatique et libertés (2).

▪ Il est également précisé par ces textes que les données doivent être :

- collectées et traitées de manière loyale et licite ;

- enregistrées pour des finalités déterminées et légitimes et ne pas être utilisées de manière incompatible avec ces finalités ;

- exactes, complètes et si nécessaire mises à jour ;

- conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées et traitées.

▪ Un traitement de données personnelles mis en œuvre à des fins de marketing doit donc, pour être licite, répondre aux conditions susvisées.

▪ Par ailleurs, il est interdit, en vertu des dispositions de l'article 8 de la loi Informatique et libertés de collecter ou de traiter des données à caractère personnel faisant apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci.

▪ Dans la mesure où la finalité du traitement l'exige pour certaines catégories de **données sensibles**, ne sont pas soumis à l'interdiction susvisée les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf dans le cas où la loi prévoit que l'interdiction ne peut pas être levée par le consentement de la personne concernée.

La collecte d'informations sur l'entourage familial d'un individu est-elle considérée comme excessive ?

▪ **Oui**, dans certains cas. Par exemple, la collecte d'informations auprès d'un mineur sur son entourage familial, le mode de vie de ses parents, leur statut professionnel est considéré comme excessive et déloyale par la Cnil.

▪ Toute personne procédant à la **collecte de données par un moyen frauduleux, déloyal ou illicite** est susceptible d'engager :

- sa r**esponsabilité civile délictuelle**, en application de l'article 1382 du Code civil (dommages et intérêts),

- sa responsabilité pénale, sur le fondement de l'article 226-18 du Code pénal et, dans ce cas, d'encourir le prononcé d'une **peine d'emprisonnement** de **cinq ans**, associée à une **peine d'amende de 300 000 euros**.

▪ Les personnes morales peuvent être déclarées responsables pénalement des infractions précédemment citées.

Références

(1) Conseil de l'Europe, Convention STE 108 du 28-1-1981

(2) Loi n° 78-17 du 6-1-1978 modifiée

Prochains événements

Informatique et libertés : impact du bilan d'activité de la Cnil sur les entreprises : 14 septembre 2011

▪ **Alain Bensoussan** animera, aux côtés de **Chloé Torres**, un petit-déjeuner débat portant sur le 31ème rapport d'activité publié par la Cnil pour l'année 2010.

▪ Dans le cadre de la présentation de son rapport annuel d'activité, la Cnil a mis en exergue les nombreux faits marquants de l'année écoulée, les contrôles diligentés, les sanctions prononcées, les actions envisagées en 2011, ainsi que les axes de réflexion retenus par la Commission.

▪ L'action de la Cnil pour l'année 2010 s'est concentrée principalement sur les thématiques suivantes :

- la protection de l'image sur internet : notamment grâce à des actions de sensibilisation et à l'ouverture de comptes sur les réseaux sociaux ;

- la labellisation : la Cnil se prépare à la délivrance des premiers labels Informatique et libertés ;

- la géolocalisation des véhicules : adoption, le 8 avril 2010, d'une recommandation relative à la mise en œuvre, par les compagnies d'assurance et les constructeurs automobiles, de dispositifs de géolocalisation embarqués dans les véhicules ;

- la communication politique à l'heure des nouvelles technologies : en raison des évolutions technologiques majeures survenues ces dernières années, la Commission intervient régulièrement auprès des politiques pour les informer des bonnes pratiques ;

- la mesure de la diversité : la Cnil est représentée au sein du Comité pour la mesure et l'évaluation de la diversité et des discriminations (COMEDD) ;

- le recrutement en ligne : la Commission souhaite encadrer l'utilisation des réseaux sociaux et sensibiliser l'ensemble des acteurs (futurs candidats et recruteurs) aux problématiques du recrutement sur internet.

▪ Nous vous proposons, au cours d'un petit-déjeuner débat, d'aborder les plans de mise en conformité qui s'imposent aux entreprises au vu du bilan d'activité de la Cnil.

Inscription gratuite sous réserve confirmation avant le 10 septembre 2011 par courrier électronique en indiquant vos coordonnées et le nombre de personnes qui assisteront au petit déjeuner débat à l'adresse suivante : invitation-conference@alain-bensoussan.com ou en faxant le bulletin d'inscription au 01 41 33 35 36.

Faille ou défaut de sécurité : ce qui (v)a changé (er) : 5 octobre 2011

▪ **Alain Bensoussan**, **Eric Barbry**, **Céline Avignon** animeront un petit-déjeuner débat consacré à la nouvelle obligation de notification des failles de sécurité introduite par l'Ordonnance du 24 août 2011 de transposition du nouveau « Paquet télécom »

▪ S'agissant de la protection de la vie privée et des données personnelles dans le cadre des services de communications électroniques, l'ordonnance complète la loi relative à l'informatique, aux fichiers et aux libertés par de nouvelles obligations figurant à l'article 34 bis.

▪ Cet article est une véritable révolution juridique qui s'applique à « toute violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques ».

▪ Quelles sont les personnes soumises à ces nouvelles obligations ? Qu'est ce qu'une violation de sécurité : une faille ou un défaut ? Comment informer la Cnil et notifier les clients ? Quelles sont les « mesures de protection appropriées » qui permettent d'éviter une notification client ?

▪ Nous vous proposons, à l'occasion d'un petit-déjeuner, de faire le point sur ces nouvelles dispositions.

▪ **Inscription gratuite** sous réserve de confirmation avant le 1er octobre 2011 par courrier électronique en indiquant vos coordonnées et le nombre de personnes qui assisteront au petit déjeuner débat à l'adresse suivante : invitation-conference@alain-bensoussan.com ou en faxant le bulletin d'inscription au 01 41 33 35 36.

Bioéthique : la loi est parue au Journal officiel

Sources

▪ La loi bioéthique, parue au Journal officiel du 8 juillet 2011, est venue actualiser les textes en vigueur, dans le respect des principes fondamentaux de la bioéthique, énoncés dans la Déclaration universelle sur la bioéthique et les droits de l'homme, adoptée en octobre 2005 par la Conférence générale de l'Unesco (1).
▪ La présente loi autorise également, en son article premier, la ratification de la Convention sur les droits de l'homme et la biomédecine, qui avait été signée en Espagne, à Oviedo, le 4 avril 1997.

(1) Loi 2011-814 du 7-7-2011 ; Unesco, Déclaration universelle du 10-2005

Signature électronique : une validité reconnue en matière pénale

▪ Un arrêté du 21 juin 2011 est venu préciser les conditions de validité de la signature électronique ou numérique en matière pénale (2).
▪ Ce texte, qui introduit de nouvelles dispositions dans le Code de procédure pénale concernant la signature électronique, la signature numérique et l'archivage, s'applique aux systèmes de traitements automatisés de type MINOS, WINOMP, PV électronique et Contrôle automatisé.

(2) Arrêté du 21-6-2011

Registre national des crédits : le rapport du Comité de préfiguration

▪ Le Comité de préfiguration du registre national des crédits aux particuliers, institué par l'article 49 de la loi n° 2010-737 du 1er juillet 2010 portant réforme du crédit à la consommation, a rendu public son rapport, à l'issu de travaux auxquels a participé la Cnil de septembre 2010 en juin 2011 (3).
▪ Il s'agissait pour le Comité de préciser les caractéristiques que devrait présenter un registre national des crédits aux particuliers pour répondre au double objectif fixé par la loi : contribuer à la prévention du surendettement et faciliter l'examen par le prêteur de la solvabilité de l'emprunteur.

(3) Comité de préfiguration, rapport du 7-2011

Numérique : publication d'un rapport de l'Assemblée nationale

▪ Constituée en avril 2010 sous l'impulsion de la commission des Lois et de la commission des Affaires culturelles, la mission d'information de l'Assemblée nationale sur les droits de l'individu dans la révolution numérique a publié, le 22 juin 2011, les résultats de ses travaux (4), après avoir procédé à l'audition de l'ensemble des acteurs du monde numérique, dont la Cnil, le 19 mai 2010.
▪ Aux termes de ce rapport, 54 orientations ont été formulées par les rapporteurs Patrick Bloche et Patrice Verchère, concernant notamment la protection de la vie privée et des données personnelles.

(4) Doc. AN n° 3560 du 22-6-2011

Directeur de la publication : Alain Bensoussan
Rédigée par les avocats et juristes de ALAIN BENSOUSSAN SELAS
Animée par Chloé Torres, Céline Avignon, Stéphanie Le Bris et Isabelle Pottier, avocats
Diffusée uniquement par voie électronique
ISSN 1634-071X
Abonnement à : paris@alain-bensoussan.com