ALAIN BENSOUSSAN
Juristendances Informatique et Libertés
n° 40 – Juillet – Août 2011

PREMIERE AUTORISATION DE MISE EN PLACE D'UN DISPOSITIF BIOMETRIQUE MULTIMODAL

Finalités des dispositifs de reconnaissance biométrique

▪ Par décision du 12 mai 2011, la Cnil a, pour la première fois, autorisé la mise en œuvre d'un dispositif biométrique multimodal reposant sur la reconnaissance combinée du réseau veineux des doigts de la main et des empreintes digitales et ayant pour finalité le **contrôle de l'accès aux locaux sur les lieux de travail** (1).

▪ La société Vauban Systems avait en effet saisi la Cnil, en application des dispositions de l'**article 25-I-8° de la loi Informatique et libertés**, lesquelles prévoient de soumettre à la Commission les traitements comportant des données biométriques nécessaires au contrôle de l'identité des personnes, préalablement à leur mise en œuvre.

▪ Pour mémoire, un dispositif biométrique vise à identifier une personne à partir de ses **caractéristiques physiques, biologiques, voire comportementales**. La donnée biométrique est une donnée produite par le corps humain, qui désigne une personne de façon certaine et permet de la tracer. A cet égard, le réseau veineux des doigts constitue une **biométrie plus sécurisante** que l'empreinte digitale, qui est moins fiable, car pouvant être reproduite à l'insu de la personne.

Synthèse analytique de la délibération rendue par la Cnil

▪ La Cnil a, tout d'abord, analysé le **mécanisme du dispositif** soumis à autorisation. Elle a relevé que celui-ci est composé d'un seul et même lecteur permettant de lire, de manière quasi-simultanée, le réseau veineux d'un doigt et l'empreinte digitale de ce même doigt. Ces deux informations sont enregistrées dans des gabarits stockés sur le terminal.

▪ Ainsi, une personne souhaitant accéder aux locaux de l'entreprise doit apposer son doigt sur le **lecteur biométrique** d'un boîtier. Une comparaison est alors réalisée entre l'empreinte digitale, le réseau veineux du doigt de la personne et les gabarits enregistrés dans la base de données du boîtier.

▪ La Commission en a déduit que la combinaison des deux techniques biométriques permettait une **identification efficace** (le réseau veineux permet de garantir que l'empreinte digitale est bien celle de la personne ayant apposé son doigt) **et rapide** de la personne. Dès lors, le **dispositif** est **adapté à la finalité de contrôle d'accès**.

▪ En outre, la Cnil a constaté que les **mesures de sécurité** étaient **satisfaisantes** et limitaient le **risque de dispersion des données biométriques** . Les données sont en effet stockées sur le terminal de lecture et non sur un serveur, seuls les gabarits du réseau veineux et de l'empreinte digitale sont conservés, les gabarits sont stockés sous un format propriétaire et chiffrés en utilisant des algorithmes cryptographiques réputés forts et les clés de chiffrement sont spécifiques à chaque terminal.

▪ Enfin, la Cnil a estimé que la **durée de conservation des données** n'excédait pas la durée nécessaire à la finalité du traitement, les données d'identification de la personne et les gabarits étant conservés le temps pendant lequel la personne est habilitée à pénétrer dans les locaux, tandis que l'historique des accès aux locaux est conservé pendant trois mois.

L'enjeu

Trouver un juste équilibre entre les impératifs de sécurité et de protection de la vie privée et des données à caractère personnel.

L'essentiel

Constatant que les mesures de sécurité présentées offrent des garanties satisfaisantes quant à la protection des données personnelles, la Cnil considère ce dispositif comme étant « adapté et proportionné à la finalité poursuivie ».

(1) Cnil, Délib. n° 2011-141 du 12-5-2011

ERIC BARBRY

VERS LA NOTIFICATION DES FAILLES DE SECURITE DES SYSTEMES D'INFORMATION

Responsabilité encourue pour défaut de sécurité informatique

▪ La recrudescence des attaques informatiques en 2011 a conduit le gouvernement à **accélérer la montée en puissance du dispositif national de sécurité et de défense des systèmes d'information** en adoptant un ensemble de mesures présentées en Conseil des ministres le 25 mai 2011 (1), comprenant notamment le renforcement des effectifs et des moyens mis à la disposition de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

▪ Si l'exploitation malveillante, par les hackers, de failles de sécurité est réprimée par la loi, l'existence d'une **faille de sécurité** n'est pas constitutive d'une faute en soi. Le défaut de sécurité n'est en effet condamnable que si l'intrusion non autorisée a effectivement porté préjudice à un tiers.

▪ Concernant les **fichiers de données à caractère personnel**, toutefois, une faute de sécurité peut être induite de la seule existence d'une faille de sécurité.

▪ Il résulte en effet des dispositions de l'article 34 de la loi Informatique et libertés que « *le* ***responsable du traitement*** *est tenu de* ***prendre toutes précautions utiles****, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* ».

▪ Ainsi, toute personne susceptible de détenir des données à caractère personnel est astreinte à une **obligation de sécurité** (obligation de moyens « *renforcée* »).

Périmètre juridique de l'obligation de notification à la Cnil

▪ Pour satisfaire à cette obligation, il incombe au détenteur de données personnelles de démontrer qu'il a agi conformément aux **règles de l'art**, selon les plus **hauts niveaux de sécurité** et en liaison avec les **risques anticipés**.

▪ Il ne pourra être exonéré de toute responsabilité que s'il parvient à démontrer qu'en l'état actuel des technologies, il lui était impossible de prendre des mesures complémentaires. Cette preuve s'avèrera, en pratique, très difficile à rapporter.

▪ En conséquence, il est conseillé aux personnes gérant des données à caractère personnel d'instaurer une **politique de sécurité du SI** attestant de la volonté de l'entreprise de mettre en oeuvre tous les moyens au regard de l'état de l'art..

▪ Un **projet d'ordonnance** (2), transposant la directive « Paquet télécoms », prévoit d'instaurer une procédure spécifique en cas de violation de la sécurité, en vue de renforcer la protection des données personnelles. Son adoption emportera modification des dispositions du II de l'article 32 de la **loi Informatique et libertés**.

▪ Toute **violation de données personnelles** constatée par un fournisseur de service de communications électroniques devra ainsi faire l'objet d'une notification à la Cnil précisant les mesures proposées ou prises pour y remédier.

▪ La notification à l'abonné ou au particulier concerné sera facultative si la Cnil a, d'une part, validé les **mesures de protection technologiques** mises en oeuvre par le fournisseur pour remédier à la violation et d'autre part, constaté que ces mesures sont effectivement appliquées aux données concernées.

▪ Aux termes de la loi n° 2011-302 du 22 mars 2011, le Gouvernement dispose de six mois pour adopter cette ordonnance, soit jusqu'au **21 septembre 2011**.

▪ Il s'agira d'une véritable révolution juridique…

Les conseils

- rédaction d'un livret de contrôle du SI adressé à toutes les directions métier et d'un code de la sécurité reprenant l'ensemble des obligations au regard de l'état de l'art ;

- mise en œuvre d'une politique de sensibilisation de l'ensemble du personnel, d'une politique d'audit de la sécurité et de tests d'intrusion.

La consultation publique

Le 22 juin 2011, les dispositions réglementaires contenues dans le projet d'ordonnance ont été soumises à consultation publique et transmises pour avis au Conseil national du numérique. Les commentaires sur ces dispositions peuvent être adressés à la DGCIS jusqu'au 20 juillet 2011.

(1) Communication du 25-5-2011

(2) Projet d'ordonnance

ALAIN BENSOUSSAN

Les dispositifs biométriques en entreprise sont–ils légaux ?

▪ **Oui** les entreprises peuvent décider de l'implantation d'un dispositif biométrique, sous réserve de requérir l'autorisation préalable de la Cnil (1).

▪ La Commission a simplifié les **formalités déclaratives** s'agissant des dispositifs biométriques suivants :

- reconnaissance du contour de la main ayant pour finalités le contrôle d'accès, ainsi que la gestion des horaires et de la restauration sur les lieux de travail (2) ;

- reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée, destiné à contrôler l'accès aux locaux sur les lieux de travail (3) ;

- reconnaissance du réseau veineux des doigts de la main ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail (4).

- reconnaissance de l'empreinte digitale ayant pour finalité le contrôle de l'accès aux postes informatiques portables professionnels (5).

▪ Lorsqu'une entreprise entend mettre en œuvre un dispositif biométrique relevant de l'une de ces autorisations uniques, il lui suffit de transmettre à la Cnil une **déclaration simplifiée**, par laquelle l'entreprise s'engage à se conformer aux conditions posées par l'autorisation.

▪ Cet **engagement de conformité** peut être effectué en ligne, sur le site de la Cnil. La Commission peut, à tout moment, diligenter un contrôle sur place en vue de vérifier la réalité de cet engagement.

▪ Si le dispositif envisagé n'est pas strictement conforme à l'une de ces autorisations uniques sus-mentionnées, une **demande d'autorisation** devra être déposée auprès de la Commission

La Cnil peut-elle refuser d'autoriser l'installation de tels dispositifs ?

▪ **Oui**, la demande d'autorisation est susceptible d'être rejetée par la Cnil, dès lors que le dispositif soumis à autorisation ne répond pas aux critères établis. La délivrance de l'autorisation est en effet subordonnée au respect de **4 principes directeurs**, fixés par la Commission. La Commission apprécie la **finalité**, la **proportionnalité**, la **fiabilité** et la **sécurité** du dispositif.

▪ Ainsi que le souligne la Commission (6), aux termes d'une communication publiée en 2007, elle se prononce « *en l'état actuel de la technologie* ».

Les salariés doivent-ils être informés ?

▪ **Oui**, les personnes concernées par le dispositif biométrique doivent être informées individuellement des conditions de son fonctionnement, ainsi que des raisons de son implantation.

▪ L'information doit porter sur la finalité du dispositif, les destinataires ou catégories de destinataires des données et les modalités d'exercice des droits d'accès aux données et de rectification. Saisie d'une demande d'autorisation, la Cnil s'assure invariablement de **l'information des salariés** concernés, ainsi que de la **consultation des instances représentatives du personnel**.

Références

(1) en application des dispositions de l'article 25 de la loi Informatique et libertés,

(2) Cnil, Délib. n°2006-101 du 27-4-2006

(3) Cnil, Délib. n°2006-102 du 27-4- 2006

(4) Cnil, Délib. N°2009-316 du 7-5-2009

(5) Cnil, Délib. N°2011-074 du 10-3-2011

(6) Communication Cnil 2007.

Il est conseillé :

- d'adresser aux salariés concernés une note d'information ;
- de communiquer à la Cnil les résultats de la consultation des organes représentatifs du personnel.

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 31eme 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 induites 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.

Identité numérique : adoption de la proposition de loi par le Sénat

Sources

▪ La proposition de loi relative à la protection de l'identité a été adoptée en première lecture, le 31 mai 2011, par le Sénat.
▪ La principale finalité de ce texte est l'instauration d'un titre d'identité biométrique, ainsi que d'un fichier central national correspondant. Ce titre sera doté d'un composant électronique sécurisé, intégrant des données biométriques, destiné à faciliter la mise en œuvre de nouveaux services, tels que l'authentification à distance ou encore la signature électronique.

(1) Doc. Sénat n° 126 du 31-5-2011

Conséquences de la révolution numérique sur les droits de l'individu

▪ Un rapport d'information, réalisé en conclusion des travaux entrepris par la mission d'information commune sur les droits de l'individu dans la révolution numérique de l'Assemblée nationale, a été présenté par Messieurs Patrick Bloche et Patrice Verchère le 22 juin 2011 (2).
▪ Ayant procédé à 45 auditions en vue de préciser les opportunités et les risques que représentent le développement des nouvelles technologies de l'information et de la communication pour la garantie des droits individuels, la mission d'information a souhaité, par le présent rapport, fixer 54 orientations pour l'avenir.

(2) Doc. AN n° 3560 du 22-6-2011

CEPD : publication du rapport annuel d'activité 2010

▪ Le 15 juin 2011, Messieurs Peter Hustinx, Contrôleur européen de la protection des données (CEPD), et Giovanni Buttarelli, Contrôleur adjoint, ont présenté à la presse leur rapport d'activité pour l'année écoulée.
▪ Intervenant au terme de 6 années d'activité du CEPD en qualité d'Autorité de surveillance indépendante, ce rapport s'inscrit, selon Peter Hustinx, « *dans la nécessité d'intensifier les efforts pour assurer une protection plus efficace de la vie privée et des données personnelles dans un monde en mutation qui est de plus en plus global, dominé par Internet et dépendant des technologies de l'information dans tous les domaines* »

(3) Rapport d'activité pour l'année 2010

La protection des données personnelles et de la vie privée au cœur du G8

▪ La protection des données personnelles et de la vie privée figure au cœur des préoccupations des Etats du G8, ainsi qu'en témoigne la déclaration finale adoptée par les chefs d'Etats et de gouvernement réunis à Deauville les 26 et 27 mai derniers.
▪ Estimant que la protection des données personnelles est « *un enjeu pour toutes les parties prenantes* », les membres du G8 en appellent à la « *définition d'approches communes tenant compte des cadres juridiques nationaux, qui soient fondées sur les droits de l'homme et protègent les données à caractère personnel, tout en permettant les transferts légitimes de données* ».

(4) Déclaration du 26/27-5-2011

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