ALAIN BENSOUSSAN
Juristendances Informatique et Libertés
n° 32 – Mars – avril 2010

ALERTE PROFESSIONNELLE : LA CNIL VA RESTREINDRE L'AUTORISATION UNIQUE

Le périmètre de l'alerte professionnel doit être strictement limité

▪ Dans un arrêt du **8 décembre 2009** (1), la chambre sociale cour de cassation s'est prononcée sur le code de bonne conduite et le dispositif d'alerte professionnelle institués par un groupe international pour se conformer à la loi Sarbanes Oxley.

▪ L'un des principaux points en débat portait sur le **périmètre de l'alerte** professionnelle, qui pouvait s'appliquer en l'espèce, non seulement aux **manquements sérieux au code éthique** en matière comptable, financière ou de lutte contre la corruption, mais également en cas de **manquements graves** à ce code, mettant en jeu l'intérêt vital du groupe ou l'intégrité physique ou morale d'une personne, notamment en cas de divulgation d'informations strictement confidentielles, de discrimination, de **harcèlement moral ou sexuel**.

▪ La cour de cassation a considéré que la délibération de la Cnil du 8 décembre 2005 (2) portant autorisation unique des traitements automatisés de données à caractère personnel, mis en œuvre dans le cadre de dispositifs d'alerte professionnelle, ne s'applique qu'aux seuls systèmes qui répondent à une obligation législative ou réglementaire visant à l'établissement de procédures de contrôle interne dans les domaines financier, comptable, bancaire et de lutte contre la corruption (art. 1er).

▪ L'article 3 de la délibération de la Cnil précitée admet que le système d'alerte serve aussi à **signaler des faits mettant en jeu l'intérêt vital de l'entreprise** (conflits d'intérêts, atteintes grave à la santé publique...) ou l'intégrité physique ou morale de ses employés (harcèlement moral ou sexuel...).

La cour de cassation remet en cause la souplesse introduite par la Cnil

▪ Dans son arrêt du 8 décembre 2009, la cour de cassation a remis en cause cette souplesse introduite par la Cnil, en concluant au caractère illicite du dispositif d'alerte litigieux.

▪ Elle a en effet estimé qu'un dispositif d'alerte professionnelle faisant l'objet d'un engagement de conformité à l'autorisation unique n°4 doit se **limiter aux seuls domaines financier**, comptable, bancaire et de lutte contre la corruption.

▪ La chambre sociale considère qu'un dispositif d'alerte professionnelle faisant l'objet d'un engagement de conformité à l'autorisation unique « *ne peut avoir une autre finalité que celle définie à son article 1er, que les dispositions de l'article 3 n'ont pas pour objet de modifier* ».

▪ La Cour de cassation précise que cet article ne doit pas être interprété comme permettant un élargissement de la finalité des dispositifs d'alertes tels que prévus par l'autorisation unique.

▪ Compte tenu de cette décision, la Cnil a annoncé en janvier dernier qu'elle s'apprêtait à modifier l'autorisation unique (3).

Les enjeux

Pour être licite, un système d'alerte professionnelle mis en œuvre dans le cadre de l'autorisation unique n°4 doit se limiter aux seuls domaines financier, comptable, bancaire et de lutte contre la corruption.

(1) Cass. soc., 8 décembre 2009, pourvoi 08-17191.

(2) Norme d'autorisation unique n°AU-004 du 8 décembre 2005.

Le conseil

Les groupes concernés devront auditer leur dispositif d'alerte professionnel à la lumière de cet arrêt et réaliser, le cas échéant, une autorisation normale auprès de la Cnil.

(3) Cnil, Communiqué du 27 01 2010.

CHLOE TORRES

BIOMETRIE ALLEGEE A PROPOS DE LA RECONNAISSANCE DU RESEAU VEINEUX

La Cnil a assoupli les formalités

Les enjeux

▪ Vidéosurveillance, géolocalisation et biométrie font désormais partie de la panoplie sécuritaire des espaces privés ou publics. Aujourd'hui, l'accès à une salle d'examen ou un bloc opératoire peut ainsi être soumis à l'obligation de scanner le réseau veineux palmaire du candidat ou du personnel médical (1).

▪ En application de la loi Informatique et libertés modifiée en 2004, les dispositifs de reconnaissance biométrique sont pour la plupart, soumis à une **autorisation préalable de la Cnil**.

▪ Or, la Cnil vient d'**alléger** les formalités d'autorisation pour la mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main, privilégiant ainsi les dispositifs d'identification **sans contact** (2).

▪ Encore faut-il que cette technique ne soit affectée qu'au **contrôle d'accès** des locaux sur le lieu de travail. La société qui souhaite s'équiper d'un tel dispositif dans le respect des dispositions de la décision unique n°AU-019 doit adresser à la Cnil un **engagement de conformité**.

▪ La biométrie regroupe les techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales.

▪ Ces données sont ainsi considérées comme des **données à caractère personnel**, permettant d'identifier une personne de manière irrévocable. Or, tous les traitements comportant des données biométriques doivent faire l'objet d'une autorisation préalable de la Cnil.

Distinguer les autorisations délivrées par la CNIL selon qu'il s'agisse d'un dispositif à empreinte digitale ou d'une identification effectuée par le réseau veineux.

(1) Délib. 2009-360 du 18-06-2009 et 2009-174 du 26-03-2009.

(2) Délib. 2009-316 du 07-05-2009.

Adresser à la Cnil un engagement de conformité

Les conseils

▪ Parmi les données biométriques utilisées aujourd'hui, la Cnil considère l'empreinte digitale comme une donnée à risque dont la diffusion, non maîtrisée ou accidentelle, peut avoir des **conséquences irrémédiables** pour les personnes.

▪ Contrairement à tout autre identifiant (code, mot de passe), l'empreinte digitale ne peut être modifiée une fois collectée, ce qui impose d'en limiter l'usage pour éviter une usurpation d'identité presque « parfaite ».

▪ Cette "**biométrie à trace**" est donc particulièrement **encadrée** par la Cnil qui, l'an dernier, a refusé d'autoriser plusieurs dispositifs ne pouvant justifier d'un fort impératif de sécurité. Pour la Cnil, confier ses données biométriques à un tiers doit répondre à une nécessité exceptionnelle, et être entourée de garanties sérieuses.

▪ Cette technologie doit tout d'abord présenter certaines **caractéristiques techniques** (chiffrage de l'enregistrement du gabarit veineux ou possibilité d'associer d'autres données d'identification - nom, prénom, photographie - au gabarit du réseau veineux du doigt).

▪ La **durée de conservation** des données doit être fixée (de 3 mois à 5 ans selon les cas). Le responsable du traitement doit également prendre « *toutes les précautions utiles pour préserver la sécurité et la confidentialité des données traitées, et notamment pour empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance* » (3).

▪ Enfin, l'**information des employés** et des instances représentatives du personnel doit être effectuée avant la mise en œuvre effective du dispositif biométrique sous peine d'une peine pouvant atteindre **300 000 euros d'amende** et 5 ans de prison.

La Cnil précise que le gabarit veineux doit être enregistré dans la mémoire du lecteur biométrique ou sur un support individuel sécurisé qui reste en possession de la personne qui doit être authentifiée.

(3) Art 34 loi du 06-01-1978 modifiée.

EMMANUEL WALLE

La mise en œuvre d'un dispositif d'alerte professionnelle (« whistleblowing ») doit-il faire l'objet de formalités préalables auprès de la Cnil ?

Source

▪ **Oui** Dès lors qu'ils constituent des traitements automatisés de données à caractère personnel susceptibles, du fait de leur portée, d'exclure des personnes du bénéfice de leur contrat de travail en l'absence de toute disposition législative ou réglementaire (1), les dispositifs d'alertes professionnelles sur les lieux de travail doivent faire l'objet d'une **autorisation de la Cnil**.

(1) Art. 25-I loi du 8 janvier 1978 modifiée.

Un régime d'**autorisation unique** a été mis en œuvre par la Cnil en décembre 2005 (2). Le responsable de traitement mettant en oeuvre un dispositif d'alerte professionnelle dans le respect des dispositions de cette décision unique doit adresser à la commission un **engagement de conformité** à l'autorisation unique 004. La Cnil décide que les responsables de traitement qui lui adressent une déclaration comportant un engagement de conformité à la décision unique sont autorisés à mettre en oeuvre ces traitements.

(2) Décision d'autorisation unique n° AU-004, délib. n° 2005-305 du 8 décembre 2005.

La durée de conservation des données issues des alertes traitées est-elle limitée ?

▪ **Oui** Les données relatives aux alertes ayant nécessité une vérification ne doivent pas être conservées au delà de **deux mois** à compter de la clôture des opérations de vérification, sauf engagement d'une procédure disciplinaire ou de poursuites judiciaires à l'encontre de la personne mise en cause ou de l'auteur d'une alerte abusive (3).

(3) Cnil, Document d'orientation du 10 novembre 2005.

Les données relatives à une alerte jugée infondée par l'entité responsable des alertes doivent être détruites sans délai.

L'alerte peut-elle être communiquée à une autre société du groupe ?

▪ **Oui** si elle est nécessaire à la vérification de l'alerte ou résulte de l'organisation du groupe (organisations transversales de gestion de telles alertes par des « ethics officers »).

Le **groupe de l'article 29** (groupe des autorités européennes de protection des données personnelles) précise que le fait qu'une communication soit nécessaire à la vérification de l'alerte dépendra notamment « *de la nature et de la gravité* » des faits rapportés.

Tel sera le cas, par exemple, si l'alerte met en cause un collaborateur d'une autre personne morale du groupe, un membre de haut niveau ou un organe de direction de l'entreprise concernée ;

(4) Avis du G29 du 1er février 2006.

Tel sera également le cas si les faits rapportés sont d'une **gravité** telle que, s'ils étaient fondés, ils pourraient avoir des conséquences sur la société-mère du groupe, d'autres sociétés du groupe, voire le groupe dans son ensemble (scandale financier, etc.) (4).

Autorisation des d'éthylotests anti-démarrage dans les véhicules

Source

▪ La Cnil **autorise** la mise en place d'éthylotests anti-démarrage (EAD) dans les véhicules affectés au transport de personnes (1).

▪ Les éthylotests anti-démarrage dont sont équipés, à titre préventif, les véhicules des entreprises de transport permettent le **traitement automatisé de données** relatives à leur fonctionnement, au taux d'alcoolémie des conducteurs et au démarrage des véhicules. Ils sont donc soumis à autorisation préalable de la Cnil.

▪ Cette dernière vient de décider d'une autorisation unique pour ce type de traitements.

(1) Autorisation unique n° AU-026 du 28-01-2010, JO du 26-02-2010.

Proposition de loi sur le respect de la vie privée

▪ La commission des lois a procédé à l'examen du rapport de M. Christian Cointat et du texte proposé par la commission pour la proposition de loi tendant à mieux garantir le droit à la vie privée à l'heure du numérique à travers notamment l'instauration d'un **droit à l'oubli numérique** (2).

▪ Le texte sera examiné en séance publique le mardi **23 mars 2010**.

(2) Communiqué du Sénat du 24 février 2010.

Informatique et libertés : transfert de données hors UE

▪ Décision de la Commission du **5 février 2010** relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil (3).

(3) Décision 2010/87/UE, JOUE (L) 39 du 12 février 2010.

Alertes professionnelles : la Cnil va restreindre l'autorisation unique

▪ Tenant compte de la décision rendue le 8 décembre 2009 par la Cour de cassation (4), la **CNIL** a annoncé, le **27 janvier 2010**, qu'elle s'apprêtait à modifier le régime d'autorisation unique.

▪ Cette procédure devrait donc être expressément limitée aux dispositifs d'alerte correspondant à une obligation législative ou réglementaire de droit français visant à l'établissement de procédures de contrôle interne dans les domaines financier, comptable, bancaire et de lutte contre la corruption. Dès l'instant où il débordera de ces domaines, le système d'alerte ne pourra être mis en œuvre qu'après **autorisation préalable de la CNIL** (5).

(4) Cf. sur notre site.

(5) Cnil, Communiqué du 27 01 2010

Directeur de la publication : Bensoussan Alain
Rédigée par les avocats et juristes de ALAIN BENSOUSSAN SELAS
Animée par Chloé Torres et Isabelle Pottier, avocat
Diffusée uniquement par voie électronique
ISSN 1634-0698
Abonnement à : paris@alain-bensoussan.com