

# La lettre des technologies de l'information

## Protection des données personnelles et de la vie privée : bilan législatif et jurisprudentiel 2007 - juin 2008

Lors de la conférence de presse du 16 mai 2008, la Cnil a présenté son 28<sup>ème</sup> rapport d'activité pour l'année 2007. M. Alex Türk, président de la Cnil, a notamment émis le souhait que la protection des données figure désormais au préambule de la Constitution.

### DECRET N° 2007-451 DU 25 MARS 2007

Le décret du 25 mars 2007 modifie le décret n° 2005-1309 du 20 octobre 2005 pris en application de la loi Informatique et Libertés. Ce texte a renforcé la protection des individus en intégrant notamment un nouveau chapitre consacré aux modalités de mise en œuvre des obligations d'information qui pèsent sur le responsable du traitement. Ce texte précise désormais que les informations dont la communication est obligatoire, en application de l'article 32-I de la loi Informatique et Libertés (identité du responsable du traitement, finalité du traitement, etc.), doivent être directement portées à la connaissance des personnes auprès desquelles les données sont collectées, sur le support de la collecte ou, à défaut, sur un document préalablement porté à la connaissance des personnes concernées en caractères lisibles. En cas de collecte orale des données, ces informations doivent être lues à la personne concernée en lui indiquant qu'elle peut, sur simple demande, même exprimée oralement, les recevoir postérieurement par écrit. Le décret du 25 mars 2007 décrit également les modalités d'exercice de leurs droits par les personnes dont les données sont collectées (droit d'opposition, d'accès et de rectification). Le demandeur doit ainsi justifier de son identité et la réponse doit lui parvenir dans un délai de deux mois suivant la réception de la demande. L'intéressé doit pouvoir exercer son droit d'opposition avant la validation définitive de ses réponses et, en cas de collecte par voie orale, il doit être en mesure de l'exercer avant la fin de la collecte des données le concernant. Au titre du droit de rectification, il est prévu qu'en cas de transfert des données à un tiers, il doit être procédé sans délai à la rectification.

### REJET DE LA PREUVE COLLECTÉE AU MOYEN D'UN DISPOSITIF NON AUTORISÉ PAR LA CNIL

La collecte d'une adresse IP au moyen d'un dispositif non autorisé par la Cnil peut conduire à écarter la preuve produite. C'est sur ce fondement que dans son jugement du 6 septembre 2007, le tribunal correctionnel de Saint-Brieuc a prononcé la nullité du procès-verbal dans lequel avait été consignée l'adresse IP d'un internaute poursuivi par la Sacem pour avoir téléchargé et mis à disposition 150 000 fichiers musicaux et vidéo sur des réseaux P2P.

Cependant, il convient de noter que, par un arrêt du 23 mai 2007 le Conseil d'État a annulé la délibération de la Cnil qui n'avait pas autorisé la mise en place de dispositifs de recherche et de constatation de contrefaçons sur internet. La Haute juridiction a estimé que la Cnil avait commis une erreur d'appréciation en considérant que ces dispositifs ne remplissaient pas la condition de proportionnalité à raison de la finalité de ces traitements.

Par ailleurs, une ordonnance de référé du 20 décembre 2007 (TGI Paris) a rappelé que le constat et la collecte des adresses IP pour établir des infractions doivent être strictement réservés aux seules sociétés d'auteur visées à l'article L. 321-1 du Code de la propriété intellectuelle. Dans cette affaire, la société Techland,

éditeur du jeu vidéo « Call of Juarez » avait fait procéder par la société suisse Logistep – non visée par l'article L.321-1 précité – à la collecte des adresses IP d'internautes soupçonnés par elle de télécharger illicitement son logiciel.

### SANCTION POUR DÉFAUT DE DÉCLARATION D'UN TRAITEMENT

On rappellera que le défaut de déclaration constitue une infraction visée et sanctionnée par l'article 226-16 du Code pénal : « *Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 2° du I de l'article 45 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [injonction de cesser le traitement ou retrait d'autorisation] ».*

C'est précisément sur le fondement de cet article que la Cnil a condamné une société française, le 14 décembre 2006, à 30.000 euros d'amende pour manque de coopération et de transparence. Dans le cas d'espèce, la société avait été mise en demeure d'apporter des précisions sur un fichier international concernant 450 salariés. La Cnil a pu établir, à l'occasion d'un contrôle sur place, que la mise en œuvre de ce fichier n'avait pas été suspendue, comme cela lui avait été indiqué. Bien au contraire, il était régulièrement utilisé et mis à jour alors même que les garanties demandées relativement aux finalités du fichier, aux règles de transfert de ces données à l'étranger et aux mesures de sécurité n'avaient pas été communiquées.

C'est également à raison du non-respect des formalités préalables que la Ligue européenne de défense des victimes de notaires a été condamnée par la Cour d'appel de Bourges, suivant arrêt du 11 janvier 2007. Dans le cas d'espèce, non seulement l'association n'avait procédé à aucune déclaration préalable auprès de la Cnil, mais de plus, son site donnait accès à des listes nominatives de notaires, alors même que ceux-ci avaient exprimé leur refus de voir leur nom figurer sur ces listes. Les juges ont retenu que le dispositif constituait une liste noire qui s'apparentait à de la délation, occasionnant un préjudice aux notaires cités.

### SANCTION POUR COMMENTAIRES EXCESSIFS DANS LES FICHIERS DU PERSONNEL

La Cnil a condamné une société française, le 11 décembre 2007, à 40.000 euros d'amende en raison de commentaires subjectifs figurant dans le fichier de gestion des salariés. Elle précise, dans sa délibération, que s'il est admis que des traitements de données à caractère personnel puissent comporter des zones commentaires destinées à enregistrer des informations de gestion telles que des résumés d'entretiens ou des indicateurs de suivi

d'un dossier, ces mentions doivent être pertinentes, adéquates et non excessives au regard de la finalité du traitement. Le non-respect de cette obligation est susceptible d'entraîner l'application de l'article 226-18 du Code pénal.

### **OPPOSITION A L'EXERCICE DU DROIT D'ACCES A DES DONNEES A CARACTERE PERSONNEL**

En application de l'article 39, I, 4° de la loi informatique et libertés « *toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir [...] la communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que toute information disponible quant à l'origine de celles-ci* ». Le non-respect du droit d'accès par le responsable du traitement est sanctionné par une contravention de la 5<sup>ème</sup> classe (art. R. 625-10 du Code pénal) qui se prescrit par un délai d'un an.

La Chambre criminelle de la Cour de cassation (Cass. Crim, 6 mai 2008, arrêt n°2528), sous le visa de l'ancien article 34 de la loi, a apporté des précisions sur la contravention d'opposition à l'exercice du droit d'accès à des données à caractère personnel. En l'espèce, un opérateur de téléphonie mobile avait répondu à une demande de droit d'accès en adressant au demandeur des informations qui ne se présentaient pas sous une forme directement intelligible par le destinataire. Selon l'analyse de la Cour de cassation, l'opposition à l'exercice du droit d'accès est une infraction instantanée qui se consomme à la date d'envoi des informations incomplètes ou inintelligibles. Par conséquent, la Haute juridiction a confirmé l'arrêt de la Cour d'appel ayant jugé que les courriers ultérieurement adressés par l'opérateur afin de répondre à l'insistance de son client, courriers qui ne comportaient la communication d'aucune autre donnée que celles du premier envoi, ne pouvaient pas caractériser une réitération de l'infraction et faire courir à nouveau le délai de prescription. L'action du client (constitution de partie civile) était donc à ce titre prescrite, le délai d'un an ayant commencé à courir dès le premier envoi des informations inintelligibles par le responsable du traitement au titulaire du droit d'accès.

### **AUTORISATION UNIQUE POUR LES TRAITEMENTS DE PHARMACOVIGILANCE**

La pharmacovigilance, dont les règles sont harmonisées au plan communautaire, a pour objet la surveillance du risque d'effet indésirable résultant de l'utilisation des médicaments et produits à usage humain. Les exploitants de médicaments ont l'obligation de conserver des informations détaillées relatives à tous les effets indésirables survenus à l'intérieur ou à l'extérieur de la Communauté européenne, et susceptibles d'être dus à un médicament ou produit. L'échange international de ces données permet de partager toute nouvelle information relative à un potentiel effet indésirable d'un médicament, quel que soit le lieu de sa survenance.

Dans la mesure où les traitements de pharmacovigilance répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes catégories de destinataires, la Cnil a décidé d'adopter, le 10 janvier 2008, une décision unique d'autorisation. Aussi, sous réserve de satisfaire à l'ensemble des dispositions de l'autorisation, un simple engagement de conformité peut être adressé à la Cnil. Les traitements bénéficiant de l'autorisation unique sont ceux qui procèdent à la collecte, la conservation, l'analyse, le suivi, la documentation et la transmission des données relatives aux risques d'effets indésirables résultant de l'utilisation de médicaments et produits à usage humain. La gestion des contacts du laboratoire avec les professionnels de santé ayant signalé un effet indésirable, un mésusage, un surdosage ou un abus relève également de cette autorisation unique. Le texte de l'autorisation unique énumère les données à caractère personnel relatives aux personnes pouvant être traitées par le laboratoire dans le cadre de la pharmacovigilance en distinguant celles qui sont systématiquement collectées, comme l'identité par exemple (sous la forme exclusivement d'un numéro ou d'un code alphanumérique), et celles qui ne seront collectées que si elles s'avèrent nécessaires à l'appréciation de l'effet indésirable. Il s'agit de la vie professionnelle, de la consommation de tabac, d'alcool ou de drogues, des habitudes de vie et comportements, des modes de vie et de la vie sexuelle.

Sont également précisés par l'autorisation unique les différents destinataires des données collectées, les mesures de sécurité devant garantir la confidentialité des données et les modalités d'information des personnes concernées selon que la notification est faite par courrier ou par téléphone et par le patient lui-même ou par un professionnel de santé.

### **NUMÉRO DE SÉCURITÉ SOCIALE : UN IDENTIFIANT CONTROVERSÉ POUR LE DOSSIER MÉDICAL PERSONNEL**

La Cnil est réticente à ce que le numéro de sécurité sociale (NIR) soit utilisé dans le cadre du Dossier Médical Personnel (DMP) comme identifiant national. Le NIR est un numéro unique et pérenne (un seul numéro est attribué à chaque individu à sa naissance), certifié par l'Insee à partir des données d'état-civil transmises par les mairies. Il permet de déterminer le sexe, la date et le lieu de naissance. Comme il est susceptible d'être reconstitué à partir des éléments de l'état civil, il favorise la recherche et le tri des informations et rend plus aisées les interconnexions. Aussi, l'enregistrement du NIR est-il exclusivement autorisé pour les relations avec la sécurité sociale (employeurs, Assedic, Anpe, organismes d'assurance maladie obligatoires et complémentaires, professionnels de santé).

La Cnil considère que son utilisation, pour le DMP, ne pourrait pas se faire avec toutes les garanties de sécurité requises et qu'il pourrait en résulter une perte de confiance des patients. Aussi préconise-t-elle de recourir à un nouvel identifiant, unique à tous les dossiers patients, généré à partir du NIR, mais anonymisé. Sa création devra être autorisée par décret, après avis de la Cnil.

### **DONNÉES DE COMMUNICATIONS ÉLECTRONIQUES**

Les données de communications électroniques sont celles qui sont engendrées automatiquement par les communications effectuées *via* l'internet ou la téléphonie. Elles donnent des informations sur chaque message échangé : le nom, le prénom, le numéro de téléphone, l'adresse IP, etc.

La question de savoir s'il s'agit de données à caractère personnel a été débattue devant les juridictions, notamment par deux arrêts de la Cour d'appel (CA Paris, 13<sup>ème</sup> ch., sect. A, 15 mai 2007 (pourvoi n°06-01954) et CA Paris, 13<sup>ème</sup> ch., sect. B., 27 avril 2007 (pourvoi n°06-02334)). Dans le cas d'espèce, deux internautes étaient poursuivis pour avoir mis à disposition illicitement des fichiers musicaux sur un réseau P2P. Les procès-verbaux produits à titre de preuve avaient été écartés par les juges de première instance car ils avaient été établis par des agents de la SCPP sans l'autorisation préalable de la Cnil. Les juges d'appel n'ont pas retenu l'argument de l'utilisation non autorisée d'un traitement de données personnelles, provoquant un débat sur la qualification des adresses IP.

La Cnil, préoccupée par la position de la Cour d'appel de Paris, a demandé au garde des Sceaux d'examiner la possibilité d'intenter un pourvoi en cassation dans l'intérêt de la loi contre les deux arrêts précités.

Le Conseil d'Etat a également été saisi, à l'initiative de plusieurs organismes de télécommunications, d'un recours en annulation pour excès de pouvoir du décret du 24 mars 2006 relatif à la conservation des données des communications électroniques. Selon eux, les dispositions de ce décret sont contraires à l'alinéa 2 de l'article L. 34-1 V du Code des postes et communications électroniques, lequel interdit la conservation de données relatives au contenu des communications. Le Conseil d'Etat a rejeté cette requête dans son arrêt du 7 août 2007 (CE, 2<sup>ème</sup> et 7<sup>ème</sup> sous-sections réunies, 7 août 2007 (requête n° 293774)) et rappelle que l'alinéa 1<sup>er</sup> du V de cet article précise que, parmi les catégories de données à conserver, figurent celles portant sur l'identification des personnes utilisatrices du service.

Les dispositions du décret du 24 mars 2006 pourraient être prochainement étendues. Le gouvernement a en effet exprimé la volonté de clarifier ces dispositions afin de les rendre applicables à l'ensemble des acteurs de l'Internet et non plus aux seuls opérateurs de communications électroniques. Seraient ainsi concernés les bornes d'accès Wi-Fi, les éditeurs de messagerie électronique, les points d'accès dans les lieux publics...

Parallèlement, un projet de décret d'application de l'article 6-II de la loi pour la confiance dans l'économie numérique (LCEN) a été

rendu public. Il a vocation à préciser les conditions dans lesquelles les hébergeurs et les fournisseurs d'accès à Internet doivent détenir et conserver les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont ils sont prestataires. Devraient ainsi être conservées pendant un an des données telles que : l'identifiant de la connexion à l'origine de la communication, l'identifiant attribué par le système d'information au contenu, l'objet de l'opération de création, le type de protocole ou de réseau utilisé, les date et heure de l'opération de création, les pseudonymes utilisés...

## VOTE ÉLECTRONIQUE

Le décret n° 2007-602 du 25 avril 2007 (JORF n°99 du 27 avril 2007, p. 7492) confirme la possibilité de recourir au vote électronique pour les élections des délégués du personnel et des représentants du personnel au comité d'entreprise. Celles-ci doivent être organisées dans le respect des dispositions techniques de mise en œuvre et des garanties fixées par l'arrêté du 25 avril 2007 (JORF n°99 du 27 avril 2007, p. 7494). Le décret pose les principales règles suivantes : le bulletin secret sous enveloppe reste possible sous réserve que cette faculté n'ait pas été exclue par un accord d'entreprise ou par un accord de groupe ; le chef d'entreprise choisit le prestataire en charge de la conception et de la mise en place du système de vote électronique ; le traitement « *fichier des électeurs* », établi à partir des listes électorales, a pour finalité de délivrer à chaque électeur un moyen d'authentification, d'identifier les électeurs ayant pris part au vote et d'éditer les listes d'émargement ; les listes sont enregistrées sur un support distinct de celui de l'urne électronique, scellé, non réinscriptible, rendant son contenu inaltérable et probant ; le fichier dénommé « *contenu de l'urne électronique* » recense les votes exprimés par voie électronique ; les données de ce fichier sont chiffrées et ne doivent pas comporter de lien permettant l'identification des électeurs, afin de garantir la confidentialité du vote.

## VIDÉOSURVEILLANCE ET SÉCURITÉ

Deux régimes juridiques coexistent pour encadrer les conditions dans lesquelles peut être installé un système de vidéosurveillance, dans les lieux publics comme dans les lieux privés. Outre la loi du 21 janvier 1995, qui soumet à autorisation préfectorale les dispositifs installés dans les lieux ouverts au public, la loi informatique et libertés a également vocation à s'appliquer. C'est en effet le cas lorsque « *les enregistrements visuels de vidéosurveillance (...) sont utilisés dans des traitements automatisés ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques (...)* » (Loi n°95-73 du 21 janvier 1995, art. 10-I). De même, le décret d'application n°96-926 du 17 octobre 1996 indique dans son article 5 que lorsque les enregistrements visuels de vidéosurveillance sont utilisés pour la constitution d'un fichier nominatif, la demande du pétitionnaire doit être adressée à la Cnil.

Ainsi, comme tout traitement de données à caractère personnel, la vidéosurveillance est assujettie aux formalités de déclaration préalable auprès de la Cnil, en précisant les raisons de la mise en place d'un tel dispositif, le descriptif technique des mesures de sécurité ainsi que les modalités d'identification des destinataires des images et le plan de situation des caméras avec l'angle d'orientation choisi et le champ de couverture. S'il s'agit d'un procédé biométrique de reconnaissance faciale, une procédure d'autorisation ou de demande d'avis, au sens des articles 25 et 27 de la loi, doit être mise en œuvre. Plus généralement, le dispositif doit respecter deux principes fondamentaux : la transparence et la proportionnalité.

A l'heure où de nouveaux développements de la vidéosurveillance sont envisagés au nom de la sécurité des citoyens, la Cnil dénonce d'importants risques d'atteinte à la vie privée et préconise un renforcement de ses pouvoirs dans ce secteur. Dans une note rendue publique le 8 avril 2008, elle revendique le contrôle de tous les systèmes de vidéosurveillance, quel que soit leur lieu d'implantation.

## CYBERSURVEILLANCE

**Consultation de sites pornographiques.** La consultation de sites pornographiques par un employé sur son lieu et pendant ses heures de travail est susceptible de conduire cet employé au licenciement, comme l'illustre un arrêt du 10 octobre 2007<sup>1</sup> de la chambre sociale de la Cour de cassation (rejet du pourvoi CA Montpellier, 17 mai 2006).

**Courriel personnel à titre de preuve.** Un arrêt de la Cour de cassation, en date du 6 juin 2007 (Cass., ch. soc., 6 juin 2007 - pourvoi n° 05-43996 -, rejet du pourvoi contre CA Aix-en-Provence, 18<sup>ème</sup> ch., 7 juin 2005) a approuvé un arrêt de la Cour d'appel qui, relevant le caractère privé du courrier électronique adressé par l'employé à l'un des ses collègues de travail, en a déduit que cet élément de la vie personnelle de l'intéressé ne pouvait constituer un motif de licenciement.

**Récusation des moyens de preuve pour manquement aux règles Cnil.** Un arrêt de la chambre sociale de la Cour de cassation en date du 29 janvier 2008 (pourvoi n°06-45279) a admis que les relevés d'appels téléphoniques produits par l'employeur pouvaient justifier le licenciement de l'employé pour utilisation abusive de son téléphone professionnel. Ces relevés établissaient que l'employé avait téléphoné, depuis son poste de travail, à des messageries de rencontre entre adultes, totalisant 63 heures entre juillet 2002 et janvier 2003. Le salarié a vainement tenté de se prévaloir de l'irrecevabilité de la preuve produite, arguant qu'il n'avait pas été informé du procédé de contrôle. Mais la Haute juridiction considère que la simple vérification des relevés de la durée, du coût et des numéros des appels téléphoniques passés à partir de chaque poste édités au moyen de l'autocommutateur téléphonique de l'entreprise ne constitue pas un procédé de surveillance illicite pour ne pas avoir été préalablement porté à la connaissance du salarié. On notera que la question de la conformité à la loi informatique et libertés de la collecte de données personnelles des employés au travers des relevés téléphoniques n'a pas été soulevée en l'espèce.

**Admission des moyens de preuve.** Un arrêt de la Cour d'appel de Montpellier du 17 mai 2006 a admis que les faits révélés à l'occasion de l'intervention de l'entreprise gestionnaire du système informatique de l'établissement appelée par le salarié qui se plaignait de la présence d'un virus informatique sur son poste de travail, avaient été licitement portés à la connaissance de l'employeur. Les juges ont validé la procédure de licenciement, considérant que le salarié, en consultant à plusieurs reprises des sites pornographiques, avait failli à ses obligations d'enseignant et d'éducateur « *de conserver la dignité inhérente à sa fonction et de respecter le caractère propre de l'établissement* », figurant à la convention collective des professeurs du secondaire de l'enseignement privé. La chambre sociale de la Cour de cassation, dans un arrêt du 10 octobre 2007 (rejet du pourvoi CA Montpellier, 17 mai 2006) a confirmé cette analyse.

**Principe de l'inviolabilité des correspondances privées.** Toute violation de ce principe constitue l'infraction visée et réprimée par l'article 226-15 du Code pénal : « *le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45.000 euros d'amende. Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions* ».

Ce principe est applicable aux salariés de l'entreprise comme en témoigne la condamnation prononcée par le jugement du 1<sup>er</sup> juin 2007 du tribunal de grande instance de Paris. Dans cette affaire, deux dirigeants d'une société de gestion de patrimoine privé ont découvert qu'ils faisaient l'objet d'une surveillance électronique. L'enquête judiciaire a permis d'établir qu'un ancien consultant informatique de cette société avait conservé, bien après son départ, les codes lui permettant d'accéder aux messageries électroniques du directeur général et du directeur des ressources humaines. La perquisition effectuée chez lui a permis de constater des traces de connexions aux messageries concer-

<sup>1</sup> Cass., ch. Soc., 10 oct. 2007, rejet du pourvoi CA Montpellier, 17 mai 2006, disponible sur le site [www.legalis.net](http://www.legalis.net)

nées. Il a déclaré avoir transmis ces codes à son frère, ancien salarié de cette société, travaillant actuellement pour son concurrent, pour surveiller le rachat éventuel de cette société par son employeur. Comme l'ont rappelé les juges, le simple fait de consulter les courriers électroniques de tiers en utilisant leurs codes d'accès constitue un accès frauduleux à un système informatique et une atteinte au secret des correspondances en violation de l'article 226-15 du Code pénal.

**Ouverture des fichiers personnels.** La chambre sociale de la Cour de cassation, dans un arrêt en date du 17 mai 2005 ouvre une possibilité pour l'employeur d'avoir accès aux fichiers personnels d'un salarié. Cette règle a été précisée par un arrêt du 23 mai 2007 qui précise que « *le juge peut, à la demande de l'employeur, autoriser un huissier à accéder aux données contenues dans l'ordinateur mis à la disposition du salarié et à prendre connaissance, pour en enregistrer la teneur, de messages électroniques émis et reçus par le salarié, dès lors que cette mesure d'instruction procède d'un intérêt légitime et qu'elle est nécessaire à la protection des droits de la partie qui la sollicite* ».

**Contrôle d'accès biométrique.** On observe un développement important des dispositifs biométriques ayant pour objet le contrôle des accès sur le lieu du travail ou à des systèmes d'information. Leur mise en œuvre est subordonnée à une autorisation délivrée par la Cnil. Celle-ci précise, dans un guide rendu public le 28 décembre 2007<sup>2</sup>, ses principaux critères d'appréciation ainsi que les risques auxquels s'exposent les entreprises qui y ont recours et les droits des employés. Pour l'essentiel, le dispositif doit répondre à un « *fort impératif de sécurité* ». Par ailleurs, la finalité du dispositif doit être limitée au contrôle de l'accès à une zone bien définie pour un nombre déterminé de personnes (1<sup>er</sup> critère). A raison des risques associés pour la protection des données à caractère personnel, le dispositif doit être « *proportionné* », c'est-à-dire adapté à la finalité qu'il poursuit (2<sup>ème</sup> critère). Des garanties doivent être prises pour que l'authentification et/ou l'identification ne provoquent pas la divulgation des données (3<sup>ème</sup> critère). Enfin, les personnes concernées doivent être informées (4<sup>ème</sup> critère).

La Cnil a ainsi autorisé, le 13 septembre 2007, la mise en œuvre d'un traitement automatisé de données à caractère personnel reposant sur un procédé de reconnaissance vocale. Ce dispositif qui vise à permettre de générer et de réinitialiser automatiquement les mots de passe d'accès au système d'information de l'entreprise, repose sur la reconnaissance du gabarit de l'empreinte de la voix des employés.

La Cnil a également autorisé, le 8 novembre 2007 par cinq délibérations (n°2007-335 à 339) la mise en œuvre de plusieurs dispositifs reposant sur la reconnaissance du réseau veineux du doigt de la main et ayant pour objet le contrôle de l'accès aux locaux ou à des systèmes d'information.

**Dispositifs d'alerte professionnelle.** La loi américaine Sarbanes-Oxley (juillet 2002) impose aux sociétés cotées aux Etats-Unis et à leurs filiales étrangères de procurer à leurs employés un dispositif de whistleblowing (dénommé, en français, « *alerte professionnelle* » ou encore « *alerte éthique* ») qui doit permettre de dénoncer les délits financiers dont ils ont connaissance.

Il n'existe pas de loi française sur ces dispositifs mais elle pourrait bien voir le jour, cette voie étant préconisée par un rapport remis le 7 mars 2007 au Ministre délégué à l'emploi, au travail et à l'insertion professionnelle des jeunes. En effet, ce rapport dénommé « *Charte d'éthique, alerte professionnelle et droit du travail français : état des lieux et perspectives* » préconise plu-

sieurs voies pour renforcer la sécurité juridique des chartes d'éthique et pour encadrer un système d'alerte professionnelle. Il propose notamment d'introduire dans le Code du travail des règles spécifiques pour permettre aux entreprises de mettre en place des dispositifs organisant la possibilité de signaler, non seulement des actes contraires aux dispositifs législatifs ou réglementaires et des atteintes aux droits des personnes et à la santé des salariés, mais également des actes contraires à des règles d'origine éthique ou professionnelle.

Pour l'heure, c'est la Cnil qui encadre les conditions de mise en œuvre de ces dispositifs qu'elle définit comme des « *systèmes mis à la disposition des employés d'un organisme public ou privé pour les inciter, en complément des modes normaux d'alerte sur les dysfonctionnements de l'organisme, à signaler à leur employeur des comportements qu'ils estiment contraires aux règles applicables et pour organiser la vérification de l'alerte ainsi recueillie au sein de l'organisme concerné* ».

#### Articles 2007 :

26 janvier - Le Monde Informatique : **Géolocalisation : la Cnil encadre les traitements de données**

8 février - JDnet : **Correspondant Informatique et Liberté : une innovation majeure**

27 avril - Le Monde Informatique : **Archivage : les règles préconisées par la Cnil**

15 mai - JDNet : **Dispositifs d'alerte professionnelle : la voie de la législation**

24 mai - JDNet : **Prospection sur Internet : quelles règles faut-il respecter ?**

21 juin - JDNet : **Données à caractère personnel des employés : règles et contraintes**

29 juin - Le Monde Informatique : **Correspondant Informatique et Liberté : indépendance requise**

23 juillet - www.cio-online.com : **Données à caractère personnel des employés : règles et contraintes**

4 septembre - JDNet : **Quelle sanction pour les abus commis par les salariés dans l'utilisation du système d'information de l'entreprise ?**

Novembre - JDNet : **Le dispositif légal de la vidéosurveillance dans les lieux publics**

5 novembre - www.cio-online.com : **Les formalités déclaratives pour les fichiers de données personnelles**

19 novembre - www.cio-online.com : **Qui doit et comment doit-on remplir les formalités applicables aux traitements de données personnelles ?**

#### Articles 2008 :

4 janvier - JDNet : **La vidéosurveillance dans l'entreprise**

7 janvier - CIO : **Transfert à l'étranger des données à caractère personnel**

4 février - CIO : **Contrôle Cnil : quelles mesures et sanctions en cas d'infraction à la loi informatique et liberté ?**

13 mars - Le Quotidien du Médecin n° 8331 du 13 mars 2008 : **L'utilisation de la biométrie dans les hôpitaux**

24 mars - CIO : **Collecte des données à caractère personnel sur les sites web : les obligations à respecter**

25 mars - JDNet : **L'externalisation et la délocalisation face à la Cnil : le parcours du combattant**

Avril - Revue Lamy droit de l'immatériel n°37 : **La Cnil, un obstacle aux transferts de données hors Union européenne ?**

<sup>2</sup> <http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/Communication-biometrie.pdf>