LES GUIDES DE LA CNIL

GUIDE PRATIQUE POUR LES EMPLOYEURS

ÉDITION OCTOBRE 2005

COMMISSION NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS

Sommaire

ce guide est téléchargeable sur le site internet de la CNIL www.cnil.fr

Les entreprises et les administrations se sont largement ouvertes aux technologies de l'information et de la communication pour la gestion de leurs ressources humaines.

Des renseignements à caractère personnel concernant leurs employés font ainsi l'objet d'une exploitation informatique.

Ces informations, parce que leur traitement est susceptible de porter atteinte aux droits et libertés des employés sur leur lieu de travail, doivent être protégées.

La loi « informatique et libertés » du 6 janvier 1978, modifiée par la loi du 6 août 2004, a défini les principes à respecter lors de la collecte, du traitement et de la conservation de ces données. Elle prévoit également un certain nombre de droits pour les personnes dont les données ont été recueillies.

Le respect, par les employeurs publics ou privés, des règles de protection des données à caractère personnel est un facteur de transparence et de confiance à l'égard de leurs employés. Il est aussi un gage de sécurité juridique pour les responsables des ressources humaines.

Les 7 principes clés à respecter

1. Le principe de finalité

Les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage déterminé et légitime.

Par exemple, la mise en place d'un autocommutateur téléphonique ou d'un système de contrôle d'accès ne peut avoir pour objectif le contrôle des conversations téléphoniques ou des déplacements de salariés protégés. Tout détournement de finalité est passible de sanctions pénales.

De même, l'ensemble des objectifs poursuivis dans le cadre de l'informatisation doivent être clairement exprimés (pilotage de l'activité, contrôle des connexions Internet, détection des vols en cas de vidéosurveillance…).

2. Le principe de proportionnalité

Le traitement de données personnelles envisagé ne doit pas conduire à apporter aux droits et libertés des personnes de restrictions qui ne seraient pas proportionnées au but recherché (article L.120-2 du code du travail).

Par exemple, la mise sous vidéosurveillance permanente d'un poste de travail ne pourrait intervenir qu'en cas de risque particulier pour la sécurité de l'employé concerné.

De même, la mise en place d'une base de gabarits d'empreintes digitales ne peut se justifier que face à un fort impératif de sécurité et en l'absence de solutions alternatives moins intrusives.

3. Le principe de pertinence des données

Les données personnelles doivent être **adéquates, pertinentes et non excessives** au regard des objectifs poursuivis.

Par exemple, le recueil d'informations sur l'entourage familial, l'état de santé ou encore le numéro de sécurité sociale d'un candidat à un recrutement serait contraire au principe de pertinence des données. L'enregistrement de la situation matrimoniale ou familiale précise d'un employé ne peut se justifier que pour l'attribution d'avantages particuliers à cet employé et sa famille.

4. Les données ne peuvent être conservées dans un fichier de façon illimitée

Les informations ne peuvent être conservées de façon indéfinie dans les fichiers informatiques. Une **durée de conservation** doit être établie en fonction de la finalité de chaque fichier.

Par exemple : le temps de la présence de l'employé s'agissant de la gestion des carrières, cinq années pour la gestion de la paie, un mois pour les enregistrements de vidéosurveillance…

5. La sécurité des données doit être assurée

L'employeur, en tant que responsable du traitement, est astreint à une **obligation de sécurité** : il doit définir les mesures nécessaires pour garantir la confidentialité des données (sécurité des matériels, mots de passe individuels, habilitations d'accès définies en fonction des besoins réels de chaque intervenant…).

Ainsi, les données à caractère personnel ne peuvent être consultées que par les services habilités à y accéder en raison de leurs fonctions. Elles peuvent néanmoins être communiquées à des tiers autorisés en application de dispositions législatives particulières (inspection du travail, services fiscaux, services de police…).

6. Le principe de transparence

Lors de l'informatisation du service du personnel ou encore lorsque des données sont recueillies par exemple par voie de questionnaires, les employés concernés doivent être clairement informés des objectifs poursuivis, du caractère obligatoire ou facultatif de leurs réponses, des destinataires des données et des modalités d'exercice de leurs droits « informatique et libertés » (droit d'accès, de rectification et d'opposition).

Cette information peut être diffusée par tout moyen. Elle doit être portée sur les questionnaires établis par l'employeur.

Au-delà, l'employeur devra s'assurer du respect des procédures de consultation et d'information obligatoires des instances représentatives du personnel.

Enfin, l'employeur doit adresser une déclaration préalable à la CNIL sauf, pour les traitements les plus courants, en cas de désignation d'un « correspondant informatique et libertés » (cf. www.cnil.fr). Cette déclaration est ensuite communicable à toute personne qui en fait la demande.

7. Le respect des droits des employés ou des candidats à un emploi

Toute personne peut demander au détenteur d'un fichier de lui communiquer toutes les informations la concernant contenues dans ce fichier. Elle a également le droit de faire rectifier ou supprimer les informations erronées.

Toute personne a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant soient enregistrées dans un fichier informatique. Ainsi un employé peut s'opposer à figurer dans un fichier s'il avance des motifs légitimes (défaut manifeste de confidentialité, manque d'information sur les objectifs poursuivis…) que l'employeur doit apprécier. En revanche, un employé ne peut s'opposer au recueil de données nécessaires au respect d'une obligation légale (ex. : déclarations sociales obligatoires).

***

Il appartient à chacun de contribuer à la bonne application de ces principes protecteurs de la personne. La Commission nationale de l'informatique et des libertés, autorité administrative indépendante, est chargée de veiller au respect des dispositions de la loi du 6 janvier 1978 modifiée par la loi du 6 août 2004. A ce titre, elle a une triple mission d'information et de conseil, d'expertise et de veille technologique ainsi que de contrôle des fichiers. La CNIL dispose de pouvoirs particuliers pour faire respecter la loi : elle contrôle la mise en œuvre des fichiers informatiques qui doivent à cet effet être déclarés auprès d'elle ; elle peut également procéder à des vérifications sur place et sanctionner les manquements à la loi « informatique et libertés » (avertissements, sanctions pécuniaires, dénonciations au procureur de la République).

LE CORRESPONDANT : UN VECTEUR DE DIFFUSION DE LA CULTURE INFORMATIQUE ET LIBERTÉS

Introduit en 2004 à l'occasion de la refonte de la loi du 6 janvier 1978, le correspondant à la protection des données ou correspondant informatique et libertés est désormais un personnage incontournable dans le paysage de la protection des données à caractère personnel. Tous les responsables de traitement, qu'ils soient publics ou privés, qu'ils aient le statut d'associations, de collectivités locales ou de grandes administrations de l'Etat, qu'il s'agisse de PME-PMI ou d'entreprises multinationales, sont concernés.

La désignation d'un correspondant informatique et libertés, qui reste facultative, doit être notifiée à la CNIL selon les modalités prévues par le décret d'application de la loi. Elle entraîne un allégement non négligeable dans l'accomplissement des formalités déclaratives auprès de la CNIL, puisque seuls les traitements relevant d'un régime d'autorisation ou comportant des transferts de données en dehors de l'Union européenne continueront à faire l'objet de formalités préalables.

Toutefois, l'apport essentiel de la désignation d'un correspondant informatique et libertés consistera à fournir au responsable de traitement un interlocuteur spécialisé à même de le conseiller dans ses choix difficiles. La désignation du correspondant informatique et libertés n'entraîne aucune exonération de responsabilité civile ou pénale pour le responsable de traitement. Néanmoins, l'action du correspondant informatique et libertés a précisément pour objet de contribuer à une meilleure application de la loi et réduire d'autant le risque juridique.

En effet, les obligations du responsable de traitement ne se limiteront pas à l'accomplissement des formalités préalables, qui ne constituent en quelque sorte que la face émergée du système de protection des données à caractère personnel.

Le responsable de traitement est notamment tenu d'assurer le respect des droits des personnes (droits d'accès, droit de rectification et de radiation, droit d'opposition...) en leur fournissant une information suffisante sur les traitements mis en oeuvre. Il doit aussi veiller à la proportionnalité des traitements mis en oeuvre qui ne doivent porter qu'une atteinte limitée à la vie privée des personnes. Enfin, il doit assurer la sécurité et la confidentialité des données traitées et les informations traitées ne doivent pas être communiquées à des personnes n'ayant aucune raison de les connaître.

L'application pratique de ces obligations à l'exercice d'une activité professionnelle ne va pas de soi. Elle implique une réflexion sur l'usage qui sera fait des données, une définition des besoins tenant compte des droits garantis des personnes. Par ailleurs, les choix effectués en matière de systèmes d'informations doivent tenir compte de ces droits et obligations. En l'absence de correspondant, ces tâches s'ajoutent à celles découlant des formalités. Elles sont souvent négligées, alors qu'elles sont essentielles au regard de la protection des droits des personnes et que le responsable de traitement encourt des sanctions plus lourdes qu'en cas de manquement aux obligations liées à l'accomplissement des formalités préalables. Le temps libéré du fait de la dispense de déclaration pourra désormais être consacré à ce second volet.

L'importance de la tâche peut laisser sceptique nombre de responsables de traitement et de correspondant informatique et libertés. Toutefois, si le correspondant informatique et libertés peut avoir vocation à devenir un expert en matière de protection des données à caractère personnel, il est avant-tout la personne pouvant répondre aux besoins spécifiques du responsable de traitement, disposant de la liberté d'action et de l'autorité indispensable à la préconisation de solutions organisationnelles ou technologiques qui pourraient ne pas recueillir immédiatement l'assentiment de la direction ou des services concernés. Cette configuration n'est pas destinée à faire du correspondant informatique et libertés un « électron libre », mais à assurer qu'il exerce son jugement en dehors de toute pression et présente ses conclusions au responsable de traitement sans parti pris.

La désignation d'un correspondant informatique et libertés ne saurait donc s'analyser comme une simple mesure d'allégement des formalités, mais comme un outil privilégié de diffusion de la culture informatique et libertés au sein des organismes traitant des données à caractère personnel.

RECOMMANDATION RELATIVE À LA COLLECTE ET AU TRAITEMENT D'INFORMATIONS NOMINATIVES LORS D'OPÉRATIONS DE RECRUTEMENT

La délibération n° 02-017 du 21 mars 2002 abroge et remplace la précédente recommandation n° 85-044 du 15 octobre 1985.

On entend par opérations de recrutement, tout recrutement opéré par un intermédiaire choisi par un employeur afin de l'assister dans le choix d'une personne extérieure pour un poste à pourvoir, ainsi que tout recrutement opéré directement par un employeur partie prenante dans le choix d'une personne extérieure pour un poste à pourvoir.

Sur la nature des informations collectées relatives à la vie privée :

L'article L 121-6 du code du travail dispose que "Les informations demandées sous quelque forme que ce soit, au candidat à un emploi ne peuvent avoir comme finalité que d'apprécier sa capacité à occuper l'emploi proposé ou ses aptitudes professionnelles. Les informations doivent présenter un lien direct est nécessaire avec l'emploi proposé ou avec l'évaluation des aptitudes professionnelles. Le candidat à un emploi (...) est tenu d'y répondre de bonne foi."

Aussi, la Commission estime-t-elle que, de manière générale, la collecte des informations suivantes **n'est pas conforme à ces dispositions légales,** sauf cas particuliers justifiés par la nature très spécifique du poste à pourvoir ou, le cas échéant des règles en vigueur dans le pays étranger concerné par le poste :

- date d'entrée en France ;
- date de naturalisation ;
- modalités d'acquisition de la nationalité française ;
- nationalité d'origine ;
- numéros d'immatriculation ou d'affiliation aux régimes de sécurité sociale ;
- détail de la situation militaire : sous la fome "objecteur de conscience, ajourné, réformé, motifs d'exemption ou de réformation, arme, grade" ;
- adresse précédente ;
- entourage familial du candidat (nom, prénom, nationalité, profession et employeur du conjoint ainsi que nom, prénom, nationalité, profession, employeur, des parents, des beaux-parents, des frères et sœurs et des enfants)
- état de santé, taille, poids, vue ;
- conditions de logement (propriétaire ou locataire);
- vie associative ;
- domiciliation bancaire, emprunts souscrits.

Sur la collecte des informations :

En application des dispositions de l'article 6 de la loi du 6 janvier 1978 modifiée, la collecte de données, par tout moyen frauduleux, déloyal ou illicite est interdite.

En conséquence, serait contraire aux dispositions de cet article, l'utilisation d'annonces qui ne correspondrait pas à un poste à pourvoir, mais aurait pour seul objet de constituer un fichier de candidatures.

Constituerait de même une manœuvre déloyale, le fait, par une personne chargée du recrutement, de porter à la connaissance d'un employeur la candidature de l'un de ses salariés sans l'accord exprès de celui-ci.

La collecte de références auprès de l'environnement professionnel du candidat (supérieurs hiérarchiques, collègues, maîtres de stages, clients fournisseurs …) n'est pas contraire aux dispositions de la loi du 6 janvier 1978 dès lors qu'elle n'est pas faite à l'insu du candidat. En revanche, la collecte du nom et de l'adresse de références personnelles aux fins de diligenter une enquête dite "de moralité" serait excessive et contraire à la loi.

En application de l'article 8 de la loi du 6 janvier 1978 et de l'article 6 de la convention 108 du Conseil de l'Europe, il est interdit de collecter et de conserver, sauf accord exprès du candidat, des données nominatives qui, directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales, les informations relatives à la santé ou à la vie sexuelle des personnes. L'accord exprès exigé par la loi qui doit être recueilli par écrit ne saurait, à lui seul, justifier la collecte de telles données si ces dernières sont dépourvues de lien direct et nécessaire avec l'emploi proposé. Aussi de telles informations ne peuvent-elles être collectées, sous réserve des interdictions légales, que lorsqu'elles sont justifiées par la spécificité du poste à pourvoir.

Sur l'information des personnes concernées :

En application de l'article 38 de la loi du 6 janvier 1978, toute personne a le droit de s'opposer, pour des raisons légitimes, à ce que des informations nominatives la concernant fassent l'objet d'un traitement.

En application des dispositions de l'article 32 de la loi du 6 janvier 1978 les personnes auprès desquelles sont recueillies des informations nominatives doivent être informées :

- du caractère obligatoire ou facultatif des réponses ;
- des conséquences à leur égard d'un défaut de réponse ;
- des personnes physiques ou morales destinataires des informations ;
- de l'existence d'un droit d'accès et de rectification.

Lorsque de telles informations sont recueillies par voie de questionnaires, ceux-ci doivent porter mention de ces prescriptions.

Il résulte en outre de l'article 10 de la directive 95-46 du 24 octobre 1995 que le candidat doit également être informé de l'identité du responsable du traitement ainsi que les finalités du traitement auquel les données sont destinées.

La Commission recommande en conséquence que :

- les personnes chargées du recrutement prennent toutes les dispositions nécessaires pour informer le candidat, dans un délai raisonnable, de l'issue donnée à sa candidature, de la durée de conservation des informations le concernant ainsi que de la possibilité de demander la restitution ou la destruction de ces informations.
- les personnes, dont les coordonnées sont enregistrées dans un fichier de candidats potentiels utilisé dans le cadre d'une activité par approche directe, soient informées des dispositions de l'article 27 de la loi du 6 janvier 1978, au plus tard lors du premier contact. Lorsque l'identité de l'employeur n'a pas été précisée lors de l'offre de poste, l'accord du candidat doit être recueilli préalablement à la transmission des informations nominatives à cet employeur. Dans le cas de collecte d'informations nominatives par le biais de connexions à distance, la CNIL recommande que le candidat à l'emploi soit informé de la forme, nominative ou non, sous laquelle les informations le concernant seront éventuellement diffusées en ligne ou transmises aux employeurs. Le candidat doit également être préalablement informé de toute éventuelle cession d'informations à d'autres organismes chargés de recrutement et être en mesure de s'y opposer.

Les informations collectées ne peuvent être utilisées que pour la proposition d'emploi à l'exclusion de toute autre finalité, notamment de prospection commerciale.

L'article L 121-7 du code du travail prescrit que "le candidat à un emploi est expressément informé, préalablement à leur mise en oeuvre, des méthodes et techniques d'aide au recrutement utilisées à son égard. (...) Les résultats obtenus doivent rester confidentiels. Les méthodes et techniques d'aide au recrutement ou d'évaluation des salariés et des candidats à un emploi doivent être pertinentes au regard de la finalité poursuivie."

La Commission recommande que l'information concernant les méthodes d'aide au recrutement employées soit dispensée préalablement par écrit sous une forme individuelle ou collective.

Sur le droit d'accès et de rectification :

En application des articles 39 et suivants, de la loi du 6 janvier 1978, et L 121-7 du code du travail tout candidat peut obtenir communication des informations le concernant.

En application de de la loi du 6 janvier 1978, en cas de contestation portant sur l'exactitude des informations, la charge de la preuve incombe au service auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les informations contestées ont été communiquées par la personne concernée ou avec son accord.

La Commission recommande en conséquence que tout candidat soit clairement informé des modalités d'exercice du droit d'accès et puisse obtenir sur sa demande toutes les informations le concernant y compris les résultats des analyses et des tests ou évaluations professionnelles éventuellement pratiqués.

Le droit d'accès s'applique aux informations collectées directement auprès du candidat, aux informations éventuellement collectées auprès de tiers ainsi qu'aux informations issues des méthodes et techniques d'aide au recrutement.

La Commission recommande que la communication des informations contenues dans la fiche du candidat soit effectuée par écrit, la communication des résultats des tests ou évaluations devant être faite par tout moyen approprié au regard de la nature de l'outil utilisé.

Sur la durée de conservation :

En application de l'article 36 de la loi du 6 janvier 1978, sauf dispositions législatives contraires, les informations ne doivent pas être conservées sous une forme nominative au-delà de la durée prévue à la déclaration, à moins que leur conservation ne soit autorisée par la Commission.

La Commission recommande que le candidat ayant fait l'objet d'une procédure de recrutement, que cette dernière ait abouti ou non, soit informé de la durée pendant laquelle les informations le concernant seront conservées et du droit dont il dispose d'en demander, à tout moment, la suppression. En tout état de cause, la durée de conservation des informations ne devrait pas excéder deux ans après le dernier contact avec la personne concernée.

Ces recommandations sont applicables quelle que soit la forme sous laquelle les informations relatives aux candidats sont conservées, qu'il s'agisse de traitements automatisés d'informations nominatives ou de fichiers manuels ou mécanographiques.

Sur la prohibition des profils automatiques :

En application du deuxième alinéa de l'article 10 de la loi du 6 janvier 1978, aucune décision de sélection de candidature impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement informatisé donnant une définition du profil ou de la personnalité du candidat. Dès lors, une candidature ne saurait être exclue sur le seul fondement de méthodes et techniques automatisées d'aide au recrutement et doit faire l'objet d'une appréciation humaine.

La Commission recommande à ce titre que les outils d'évaluation automatisés à distance excluant toute appréciation humaine sur la candidature soient proscrits.

En application de l'article 3 de la loi du 6 janvier 1978 tout candidat a le droit d'être informé des raisonnements utilisés dans les traitements automatisés d'aide à la sélection de candidatures.

Sur les formalités préalables à l'automatisation :

En application de l'article 22 de la loi du 6 janvier 1978, les traitements automatisés d'informations nominatives effectués par les personnes chargées du recrutement doivent, préalablement à leur mise en oeuvre, faire l'objet, sauf désignation d'un correspondant informatique et libertés, d'une déclaration auprès de la Commission nationale de l'informatique et des libertés, l'omission de ces formalités préalables étant passible des sanctions prévues aux articles 226-16 à 226-24 du code pénal.

Sur les mesures de sécurité et de confidentialité :

En application de l'article 34 de la loi du 6 janvier 1978 et L 121-7 du code du travail les personnes chargées du recrutement sont tenues de s'engager vis-à-vis des candidats à prendre toutes précautions utiles afin de préserver la sécurité et la confidentialité des informations, quels que soient les tests, méthodes ou techniques utilisées. Cette obligation de confidentialité s'oppose à ce que des tiers à la procédure de recrutement puissent en avoir directement ou indirectement connaissance.

Une interdiction générale et absolue de toute utilisation d'internet à des fins autres que professionnelles ne paraît pas réaliste dans une société de l'information et de la communication, et semble de plus disproportionnée au regard des textes applicables et de leur interprétation par la jurisprudence. Un usage raisonnable, non susceptible d'amoindrir les conditions d'accès professionnel au réseau ne mettant pas en cause la productivité est généralement et socialement admis par la plupart des entreprises ou administrations.

Aucune disposition légale n'interdit évidemment à l'employeur d'en fixer les conditions et limites, lesquelles ne constituent pas, en soi, des atteintes à la vie privée des salariés ou agents publics.

À ce titre, la mise en place de dispositifs de filtrage de sites non autorisés (sites diffusant des produits à caractère pornographiques, pédophiles, incitation à la haine raciale, révisionnistes, etc.), associés au pare-feu peut constituer une mesure de prévention dont il y a lieu d'informer les salariés ou agents publics.

De même, la possibilité pour les salariés ou agents publics de se connecter à internet à des fins autres que professionnelles peut s'accompagner de prescriptions légitimes dictées par l'exigence de sécurité de l'organisme, telles que l'interdiction de télécharger des logiciels, l'interdiction de se connecter à un forum ou d'utiliser le "chat", l'interdiction d'accéder à une boîte aux lettres personnelle par internet compte tenu des risques de virus qu'un tel accès est susceptible de présenter.

Un contrôle a posteriori des données de connexion à internet, restitué de façon globale, par exemple au niveau de l'organisme ou d'un service déterminé, devrait dans la plupart des cas être suffisant sans qu'il soit nécessaire de procéder à un contrôle individualisé des sites visités par un employé déterminé.

Les modalités d'un tel contrôle de l'usage d'internet doivent, conformément à l'article L.432-2-1 du code du travail, faire l'objet d'une consultation du comité d'entreprise ou, dans la fonction publique, du comité technique paritaire ou de toute instance équivalente et d'une information des utilisateurs, y compris lorsque le contrôle est dépourvu d'un caractère directement nominatif.

Lorsque l'entreprise ou l'administration met en place un dispositif de contrôle individuel destiné à produire, poste par poste, un relevé des durées de connexion ou des sites visités, le traitement automatisé d'informations nominatives ainsi mis en œuvre doit être déclaré à la CNIL (sauf désignation d'un correspondant informatique et libertés).

La durée pendant laquelle les relevés ainsi établis sont conservés doit être précisée. Une durée de conservation de l'ordre de six mois devrait être suffisante, dans la plupart des cas, pour dissuader tout usage abusif d'internet. Le dossier de déclaration doit en outre comporter l'indication et la date à laquelle les instances représentatives du personnel ont été consultées sur de tels dispositifs.

LE CONTROLE DE L'USAGE DE LA MESSAGERIE ÉLECTRONIQUE

L'utilisation de la messagerie électronique professionnelle pour envoyer ou recevoir, dans des proportions raisonnables, un message à caractère personnel correspond à un usage généralement et socialement admis. D'ailleurs, compte tenu des termes de l'arrêt de la chambre sociale de la Cour de cassation en date du 2 octobre 2001 une interdiction ne permettrait pas à l'employeur de prendre connaissance dans des conditions régulières du contenu de celles des correspondances qui relèveraient de la vie privée des personnes.

Il doit être généralement considéré qu'un message envoyé ou reçu depuis le poste du travail mis à disposition par l'entreprise ou l'administration revêt un caractère professionnel, sauf indication manifeste dans l'objet du message ou dans le nom du répertoire où il pourrait avoir été archivé par son destinataire qui lui conférerait alors le caractère et la nature d'une correspondance privée protégée par le secret des correspondances.

Des décisions de justice postérieures à l'arrêt de la Cour de cassation du 2 octobre 2001 ont précisé la « marge de manœuvre » de l'employeur en matière de contrôle de la messagerie professionnelle de ses employés.

Il a ainsi été jugé que constitue une violation du secret des correspondances privées la lecture par l'employeur d'un message qui, bien que ne comportant pas expressément dans son objet la mention « personnel », est classé automatiquement dans un dossier qualifié de « personnel » et fait référence dans son objet aux vacances, avec une formulation et une orthographe familières. Avant d'accéder à un courriel, l'employeur doit donc vérifier que l'objet du message ne lui confère pas un caractère manifestement personnel.

Une solution identique a été retenue lorsque l'employeur, pour établir que le salarié a créé une société concurrente, se fonde sur le seul contenu des messages qu'il a découverts en se faisant remettre par un huissier l'ordinateur portable du salarié et en examinant l'ensemble du disque dur sans satisfaire à la demande préalable de restitution de ses fichiers personnels émise par ce dernier.

Des exigences de sécurité, de prévention ou de contrôle de l'encombrement du réseau peuvent conduire les entreprises ou les administrations à mettre en place des outils de mesure de la fréquence ou de la taille des fichiers transmis en pièce jointe au message électronique ou encore des outils d'archivage des messages échangés. Dans cette dernière hypothèse, le message électronique bien qu'étant effacé du poste de l'émetteur et du poste du récepteur sera néanmoins conservé. L'emploi de tels outils de contrôle ou de sauvegarde doit être porté à la connaissance des salariés ainsi que la durée de conservation du message "sauvegardé".

Lorsque l'entreprise ou l'administration met en place un dispositif de contrôle individuel poste par poste du fonctionnement de la messagerie, le traitement automatisé d'informations nominatives ainsi mis en œuvre doit être déclaré à la CNIL (sauf désignation d'un correspondant informatique et libertés). La durée pendant laquelle les messages sont conservés doit être précisée. Le dossier de déclaration doit en outre comporter l'indication et la date à laquelle les instances représentatives du personnel ont été consultées sur de tels dispositifs.

Les administrateurs qui doivent veiller à assurer le fonctionnement normal et la sécurité des réseaux et systèmes sont conduits par leurs fonctions mêmes à avoir accès à l'ensemble des informations relatives aux utilisateurs (messagerie, connexions à internet, fichiers "logs" ou de journalisation, etc.) y compris celles qui sont enregistrées sur le disque dur du poste de travail. Un tel accès n'est contraire à aucune disposition de la loi du 6 janvier 1978.

De même, l'utilisation, par les administrateurs informatiques, de logiciels de télémaintenance qui permettent de détecter et de réparer les pannes à distance ou de prendre le contrôle, à distance, du poste de travail d'un salarié ("prise de main à distance") ne soulève aucune difficulté particulière au regard de la loi du 6 janvier 1978 à condition que certaines précautions minimales en termes d'information des employés et de sécurité aient été prises. (cf. page 14 : L'utilisation des logiciels de prise de main à distance).

En tout état de cause, l'accès aux données enregistrées par les employés dans leur environnement informatique - qui sont parfois de nature personnelle - ne peut être justifié que dans les cas où le bon fonctionnement des systèmes informatiques ne pourrait être assuré par d'autres moyens moins intrusifs.

De plus, aucune exploitation à des fins autres que celles liées au bon fonctionnement et à la sécurité des applications des informations dont les administrateurs de réseaux et systèmes peuvent avoir connaissance dans l'exercice de leurs fonctions ne saurait être opérée, d'initiative ou sur ordre hiérarchique.

De même, les administrateurs de réseaux et systèmes, généralement tenus au secret professionnel ou à une obligation de discrétion professionnelle, ne doivent pas divulguer des informations qu'ils auraient été amenés à connaître dans le cadre de leurs fonctions, et en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs et ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt de l'entreprise. Ils ne sauraient non plus être contraints de le faire, sauf disposition législative particulière en ce sens.

L'obligation de confidentialité pesant sur les administrateurs informatiques devrait ainsi être clairement rappelée dans leur contrat, ainsi que - lorsque celle-ci est mise en œuvre - dans la charte d'utilisation des outils informatiques annexée au règlement intérieur de l'entreprise ou de l'administration.

L'UTILISATION DES LOGICIELS DE PRISE DE MAIN À DISTANCE

Il existe sur le marché de nombreux logiciels conçus pour aider les administrateurs informatiques dans l'accomplissement de leurs missions. Ces outils peuvent notamment permettre aux gestionnaires techniques d'accéder à distance à l'ensemble des données de n'importe quel poste de travail informatisé.

Or, la CNIL constate parfois que ces outils de télémaintenance ou de prise de main à distance sont aujourd'hui également utilisés à des fins de contrôle, par l'employeur, de l'activité de ses employés sur leur poste informatique. Il doit être considéré qu'une telle utilisation n'est ni conforme au principe de proportionnalité, ni respectueux du principe de finalité posé par la loi « informatique et libertés ».

Dans l'hypothèse d'un recours à ces outils à des fins de maintenance informatique par un administrateur technique, leur utilisation devrait s'entourer de précautions afin de garantir la transparence dans leur emploi et la confidentialité des données auxquelles le gestionnaire technique accédera par ce moyen, dans la stricte limite de ses besoins.

Devraient notamment figurer au titre de ces précautions l'information préalable et le recueil de l'accord de l'utilisateur pour « donner la main » à l'administrateur informatique avant l'intervention sur son poste (à titre d'illustration, l'accord peut être donné par simple validation d'un message d'information apparaissant sur son écran), la traçabilité des opérations de maintenance (par exemple, par la tenue d'un registre des interventions), ainsi que la précision dans les contrats des personnes assurant la maintenance - notamment en cas de recours à des prestataires extérieurs - de leur obligation de n'accéder qu'aux données informatiques nécessaires à l'accomplissement de leurs missions et d'en assurer la confidentialité.

L'utilisation de ces logiciels à des fins strictes de maintenance informatique n'est pas soumise à déclaration auprès de la CNIL.

LES FICHIERS DE JOURNALISATION DES CONNEXIONS INFORMATIQUES

Les fichiers de journalisation des connexions destinés à identifier et enregistrer toutes les connexions ou tentatives de connexion à un système automatisé d'informations constituent une mesure de sécurité, généralement préconisée par la CNIL dans le souci que soient assurées la sécurité et la confidentialité des données à caractère personnel, lesquelles ne doivent pas être accessibles à des tiers non autorisés ni utilisées à des fins étrangères à celles qui justifient leur traitement. Ils n'ont pas pour vocation première le contrôle des utilisateurs.

La finalité de ces fichiers de journalisation, qui peuvent également être associés à des traitements d'information dépourvus de tout caractère nominatif mais revêtent un caractère sensible pour l'entreprise ou l'administration concernée, consiste à garantir une utilisation normale des ressources des systèmes d'information et, le cas échéant, à identifier les usages contraires aux règles de confidentialité ou de sécurité des données définies par l'entreprise.

Ces fichiers de journalisation n'ont pas, en tant que tels, à faire l'objet des formalités préalables auprès de la CNIL. Lorsqu'ils sont associés à un traitement automatisé d'informations nominatives afin de garantir ou de renforcer le niveau de sécurité de ce dernier, ils doivent être portés à la connaissance de la CNIL au titre des mesures de sécurités entourant le fonctionnement du traitement principal dont ils sont le corollaire.

En revanche, la mise en œuvre d'un logiciel d'analyse des différents journaux (applicatifs et systèmes) permettant de collecter des informations individuelles poste par poste pour contrôler l'activité des utilisateurs doit être déclarée à la CNIL.

Dans tous les cas de figure, les utilisateurs doivent être informés de la mise en place des systèmes de journalisation et de la durée pendant laquelle les données de connexion permettant d'identifier le poste ou l'utilisateur s'étant connecté sont conservées ou sauvegardés. Cette information, qui réalise l'obligation légale à laquelle est tenu le responsable du traitement, est de nature à prévenir tout risque et participe de l'exigence de loyauté dans l'entreprise ou l'administration.

Une durée de conservation de l'ordre de six mois ne paraît pas excessive au regard de la finalité des fichiers de journalisation.

Aucune disposition de la loi du 6 janvier 1978 ne prive le responsable de l'entreprise de la possibilité d'opposer les informations enregistrées dans les fichiers de journalisation associés à un traitement automatisé d'informations nominatives à un salarié ou un agent public qui n'en n'aurait pas respecté les conditions d'accès ou d'usage.

LA VIDEOSURVEILLANCE SUR LES LIEUX DE TRAVAIL : QUELLES GARANTIES APPORTER ?

Les systèmes actuels de vidéosurveillance se caractérisent notamment par l'utilisation de technologies numériques, le recours à la miniaturisation, la facilité de branchement et d'utilisation, ainsi que la possibilité de visualiser des images sur divers supports « nomades ». L'installation sur un lieu de travail juridiquement qualifié de « privé » d'un système de vidéosurveillance captant et conservant les images sur un support numérique constitue un traitement automatisé d'informations nominatives soumis à la loi du 6 janvier 1978. La CNIL se trouve donc aujourd'hui, de fait, dans la plupart des cas compétente en cas de vidéosurveillance sur les lieux de travail.

Une réflexion préalable indispensable

Les systèmes de vidéosurveillance peuvent porter atteinte aux libertés individuelles (par exemple, à la liberté d'aller et venir). Dès lors, **une réflexion préalable** à la décision d'utiliser un système de vidéosurveillance, comportant notamment **une analyse précise des risques** devrait être menée de façon à identifier les solutions alternatives permettant d'atteindre l'objectif poursuivi sans recourir à ce moyen (une sécurisation des accès aux moyens de badges magnétiques peut par exemple constituer la réponse efficace et adaptée à un objectif particulier de sécurisation).

Cette **démarche préalable indispensable** devrait ainsi permettre la mise en lumière, au cas par cas, des enjeux spécifiques **et des risques particuliers liés au contexte propre à chaque lieu de travail.**

Le nécessaire respect du principe de proportionnalité

La mise en œuvre d'un système de vidéosurveillance des employés doit nécessairement **respecter le principe de proportionnalité.** Elle doit donc s'effectuer de façon **adéquate, pertinente, non excessive et strictement nécessaire à l'objectif poursuivi** (article L.120-2 du code du travail).

Si le déploiement de tels dispositifs sur un lieu de travail répond généralement à un objectif sécuritaire (contrôle des accès aux locaux, surveillance de zones de travail à risques), **il ne peut avoir pour objectif la mise sous surveillance spécifique d'un employé déterminé ou d'un groupe particulier d'employés.**

Le nombre, l'emplacement, l'orientation, les fonctionnalités et les périodes de fonctionnement des caméras, ou la nature des tâches accomplies par les personnes devant être soumises à la vidéosurveillance, sont autant d'éléments devant notamment entrer en ligne de compte lors de l'évaluation du caractère proportionné du système.

Il convient de rappeler que **l'article 226-1 du code pénal** prévoit une peine d'un an d'emprisonnement et de 45000 € d'amende au fait de volontairement porter atteinte à l'intimité de la vie privée d'autrui « en fixant, enregistrant ou

transmettant, sans le consentement de celle-ci, l'image d'un personne se trouvant dans un lieu privé ».

En outre, en cas d'installation d'un système de vidéosurveillance à l'insu des employés, la responsabilité civile de l'employeur pourrait être recherchée sur la base de l'obligation générale d'exécution loyale du contrat de travail à laquelle l'un comme l'autre sont tenus.

Exemples de systèmes de vidéosurveillance susceptibles de présenter un caractère illégal :

- Un système qui serait installé dans un lieu susceptible de porter atteinte à l'intimité de la vie privée des employés (vestiaires, douches, toilettes)
- Un système qui aboutirait à placer une personne ou un groupe déterminé de personnes, sauf justification spécifique particulière, sous la surveillance constante et permanente de caméras
- Un système qui serait installé à l'insu des employés ou de façon non visible (caméra miniaturisée)
- Un système qui serait installé de façon à enregistrer de façon spécifique les allées et venues des personnes se rendant dans un local syndical

L'obligation d'information : pas de surveillance à l'insu des personnes

En application de la loi du 6 janvier 1978, les personnes concernées (employés ou visiteurs) doivent être informées, au moyen d'un panneau d'information réalisé à cet effet, de l'existence du dispositif, des destinataires des images, ainsi que des modalités concrètes d'exercice de leur droit d'accès aux enregistrements visuels les concernant (art. 39 de la loi du 6 janvier 1978).

Conformément aux dispositions du code du travail (article L. 432-2-1), ainsi qu'aux textes relatifs aux trois fonctions publiques (lois n°84-16 du 11 janvier 1984, n°84-53 du 26 janvier 1984 et n°86-33 du 9 janvier 1986), les instances représentatives du personnel doivent être consultées avant toute mise en oeuvre d'un système de vidéosurveillance et précisément informées des fonctionnalités envisagées.

Sur un plan individuel, l'article L.121-8 du code du travail prévoit qu'aucune information concernant directement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance.

Une visualisation des images restreinte aux seuls destinataires habilités

Les images enregistrées ne peuvent être visionnées que par les seules personnes dûment habilitées à cet effet, dans le cadre de leurs attributions respectives (par exemple : le responsable de la sécurité de l'organisme). Ces personnes devraient être particulièrement formées ou avoir été sensibilisées aux règles encadrant la mise en oeuvre d'un système de vidéosurveillance.

Une durée de conservation des images limitée

Dans la mesure où, en cas d'incident, la visualisation des images s'effectue généralement rapidement, la durée de conservation des images enregistrées à l'aide d'un dispositif de vidéosurveillance ne devrait pas excéder quelques jours. Cette durée ne peut en tout état de cause s'étendre au delà d'un mois.

La nécessité d'accomplir certaines formalités préalables

Un système de vidéosurveillance numérique mis en place sur un lieu de travail ne peut être installé que s'il a préalablement fait l'objet d'une déclaration effectuée auprès de la CNIL.

Le dossier de déclaration auprès de la CNIL devra comporter un descriptif précisant notamment :

- les raisons rendant nécessaires la mise en place du système ; à cet égard, il est utile de joindre au dossier un plan de situation faisant apparaître l'angle d'orientation et le champ des caméras ;
- les modalités selon lesquelles les personnes sont informées de l'existence du système, de l'identification du service ou de la personne auprès duquel s'exerce le droit d'accès aux images enregistrées ;
- le descriptif technique du système de vidéosurveillance utilisé ainsi que les mesures de sécurité prévues afin d'assurer notamment la confidentialité des données traitées ;
- l'identification précise des destinataires (internes ou éventuellement externes) des images ; la durée maximale de conservation des images enregistrées.

En cas de mise en œuvre dans un lieu de travail pouvant être juridiquement qualifié de lieu « public » ou « ouvert au public », la CNIL est compétente, selon la nouvelle rédaction de l'article 10 de la loi n°95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, lorsque les enregistrements visuels « sont utilisés dans des traitements automatisés ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques » (tel est, par exemple, le cas de systèmes comportant la possibilité d'effectuer un rapprochement avec d'autres fichiers). De tels systèmes sont alors soumis à déclaration auprès de la CNIL (NB : dispense de déclaration en cas de désignation d'un correspondant informatique et libertés).

En dehors de ces cas, une autorisation préalable doit être obtenue auprès de la préfecture du lieu d'installation compétente.

Les systèmes de vidéosurveillance relèveraient toutefois, dès lors que serait utilisé un procédé informatique de reconnaissance faciale, de la procédure d'autorisation ou de la procédure de demande d'avis prévues par les articles 25 et 27 de la loi du 6 janvier 1978 modifiée pour la mise en œuvre de traitements de données biométriques.

L'UTILISATION DU TÉLÉPHONE AU TRAVAIL : QUELLES GARANTIES ?

L'utilisation d'un service de téléphonie par les employés peut conduire l'employeur à mettre en œuvre un traitement automatisé de données à caractère personnel : ces données peuvent être directement issues de l'autocommutateur, ressaisies à partir des factures papier envoyées par l'opérateur, transférées par voie électronique par l'opérateur ou encore accessibles à l'organisme par l'intermédiaire du site web de l'opérateur.

Le traitement de ces données doit s'effectuer dans le respect de la loi "informatique et libertés" et des dispositions légales applicables aux employés.

Fonctionnalités des autocommutateurs

Les autocommutateurs sont des standards téléphoniques permettant d'orienter l'ensemble des numéros de téléphone appelants et des numéros appelés. Au-delà de cette fonction première d'orientation des appels, ces appareils permettent l'enregistrement des numéros de téléphone sortants, et constituent ainsi des traitements automatisés de données personnelles au sens de la loi « informatique et libertés ».

Ils peuvent également servir à la comptabilisation statistique des flux entrants et sortants au niveau de l'organisation, d'un service ou d'un poste particulier. Reliés à des logiciels « de taxation », ils peuvent permettre d'imputer et de contrôler par service ou par poste les dépenses téléphoniques de l'organisation.

De tels dispositifs sont également susceptibles d'être utilisés afin d'identifier les communications téléphoniques qui relèveraient d'un usage non professionnel.

Enfin, les autocommutateurs comportent des fonctionnalités permettant des transferts d'appel, des conférences entre plusieurs interlocuteurs ou encore d'interrompre une conversation en cours pour signaler un appel d'un tiers.

Mise à disposition de lignes mobiles

Dans le cadre de leur activité professionnelle, certains employés peuvent être dotés d'un téléphone portable.

Une partie fixe du coût des communications peut être prise en charge par l'employeur, l'employé prenant à sa charge les éventuels dépassements. Dans ce cas, l'employeur n'a pas à connaître le détail des services utilisés par l'employé.

L'employeur peut choisir de prendre en charge l'intégralité des coûts des services de téléphonie utilisés, ce qui peut le conduire à connaître le détail des services utilisés.

Quelles garanties apporter ?

La possibilité d'un usage personnel du téléphone est reconnue à condition qu'une telle utilisation demeure raisonnable et ne soit pas préjudiciable à l'employeur.

Il est ainsi légitime qu'un employeur s'assure du caractère non abusif de cette utilisation. Ce contrôle doit toutefois s'opérer dans des conditions propres à

garantir le respect de la vie privée et des libertés des personnels sur leur lieu de travail.

• Contenu et destinataires des relevés individuels

Les supérieurs hiérarchiques ne doivent accéder aux relevés individuels des numéros de téléphone appelés ou des services de téléphonie utilisés que de façon exceptionnelle, par exemple en cas d'utilisation manifestement anormale de ces services au regard de leur utilisation moyenne constatée au sein de l'entreprise ou de l'organisme.

De plus, lorsque de tels relevés sont établis, les quatre derniers chiffres de ces numéros doivent être occultés.

Bien entendu, un employé doit avoir la possibilité d'accéder aux numéros de téléphone complets qu'il a composés, en particulier lorsqu'il lui est demandé le remboursement du coût des communications téléphoniques présumées personnelles.

• Conservation limitée des données enregistrées

La durée de conservation des données relatives à l'utilisation des services de téléphonie ne doit pas excéder un an.

• Dispositif « d'entrée en tiers »

Sauf exceptions dûment motivées par l'employeur, la fonctionnalité « d'entrée en tiers » dans une conversation téléphonique offerte par certains autocommutateurs ne doit pas être activée compte tenu des risques de surveillance ou d'interception discrète des conversations téléphoniques des personnels qui y sont attachés.

En cas de mise en œuvre justifiée, il est indispensable que l'ensemble des interlocuteurs soit clairement informé de cette fonctionnalité et de ses bénéficiaires par un dispositif d'alerte visuelle et sonore permanent.

• Préservation des droits des salariés protégés

Toute utilisation des informations issues de l'utilisation des services de téléphonie pour un contrôle des appels émis et reçus par les représentants du personnel et les représentants syndicaux dans le cadre de leur mandat est interdite.

La Cour de cassation a estimé, dans un arrêt du 6 avril 2004, que pour l'accomplissement de leur mission légale et la préservation de la confidentialité qui s'y attache, les salariés investis d'un mandat électif ou syndical dans l'entreprise doivent pouvoir disposer d'un matériel excluant l'interception de leurs communications téléphoniques et l'identification de leurs correspondants.

Ces employés doivent ainsi disposer d'une ligne téléphonique non connectée à l'autocommutateur ou ne pouvant donner lieu à la production d'une facturation détaillée.

ECOUTE ET ENREGISTREMENT DES CONVERSATIONS TÉLÉPHONIQUES SUR LE LIEU DE TRAVAIL

L'écoute ou l'enregistrement de conversations téléphoniques des employés sur le lieu de travail sont généralement interdits compte tenu des risques d'atteinte aux libertés et à la vie privée des salariés ou des agents publics concernés.

Aucune écoute permanente ou aucun enregistrement permanent des conversations des personnels d'une entreprise ou d'une administration ne peuvent être mis en œuvre, sauf législation ou réglementation particulière l'imposant (par exemple, pour le passage d'ordres dans les salles de marchés).

Une écoute ou un enregistrement ponctuels des conversations téléphoniques ne sont possibles que dans des cas limités et dûment justifiés (par exemple, pour la formation du personnel en vue de l'amélioration de l'accueil téléphonique) et selon des modalités strictement encadrées.

Un interdit pénal

Il doit être rappelé que l'article 226-15 du code pénal incrimine 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 (un an d'emprisonnement, 45.000 € d'amende).

De même l'article 432-9 du code pénal incrimine le fait, pour une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, de d'ordonner, de commettre, ou de faciliter, hors les cas prévus par la loi, l'interception ou le détournement des correspondances émises, transmises ou reçues par la voie des télécommunications, l'utilisation ou la divulgation de leur contenu (trois ans d'emprisonnement, 45.000 € d'amende).

Le respect du principe de proportionnalité : pas d'écoute téléphonique sans démonstration de la nécessité absolue d'y recourir

L'écoute ou l'enregistrement des conversations téléphoniques ne peuvent être réalisés qu'en cas de nécessité reconnue et doivent être proportionnés aux objectifs poursuivis (par exemple, un enregistrement pour des besoins de formation ne pourra être réalisé que sur une brève période et en aucun cas de manière permanente).

En l'absence d'une telle nécessité, une solution alternative devra être recherchée pour atteindre les objectifs poursuivis (par exemple : plutôt qu'enregistrer toutes les conversations avec la clientèle à des fins de constitution de preuves matérielles pour faire face à un éventuel contentieux, demander une confirmation écrite du client, notamment par voie électronique).

Textes de référence :

- l'article L.120-2 du code du travail dispose que « Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions

qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché » ;

- la loi du 6 janvier 1978 modifiée précise en son article 6 que les données personnelles (en l'occurrence, les échanges téléphoniques des employés) doivent être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ».

L'obligation d'information : pas d'écoute téléphonique à l'insu des personnels et de leurs interlocuteurs

Outre les dispositions du code du travail et des textes relatifs aux trois fonctions publiques, concernant la consultation ou l'information des instances représentatives du personnel et des salariés, sur un plan individuel, les personnels, mais également leurs interlocuteurs, doivent être informés des objectifs poursuivis par la mise en place du dispositif d'écoute, des destinataires des enregistrements et de leur droit d'accès à ces enregistrements.

Les employés doivent être également informés, préalablement à la mise en place du dispositif, des conséquences individuelles qui pourront en résulter, et des périodes pendant lesquelles leurs conversations seront écoutées ou enregistrées. A cet effet, un dispositif d'alerte visuelle et/ou sonore en temps réel doit être mis en œuvre.

L'information des interlocuteurs doit être réalisée par la diffusion d'un message au début de l'appel, ainsi que par l'insertion d'une mention particulière dans le document contractuel ou d'information relatif au service téléphonique.

La nécessité d'une déclaration préalable

Un dispositif d'écoute ou d'enregistrement des conversations téléphoniques ne peut être installé que s'il a préalablement fait l'objet d'une déclaration normale auprès de la CNIL si le dispositif d'écoute ou d'enregistrement repose sur des moyens numériques.

A cet égard, le dossier présenté à la CNIL doit notamment apporter toutes précisions utiles sur les finalités poursuivies et la proportionnalité du dispositif d'écoute au regard de ces finalités, l'information et la consultation des instances représentatives du personnel, l'information des personnels, la durée de conservation des enregistrements et les mesures prises pour assurer leur confidentialité.

NB : en cas de désignation d'un correspondant informatique et libertés, aucune déclaration ne doit être réalisée.

De nombreux services reposant sur le suivi des véhicules se sont développés, nécessitant que la CNIL s'assure qu'ils ne portent pas atteinte à la liberté d'aller et venir et à la vie privée.

L'offre de services reposant sur la technologie GSM/GPS n'a cessé de croître et de se diversifier ainsi qu'en témoigne le nombre croissant des dossiers reçus à ce sujet par la CNIL.

Les systèmes de géolocalisation GSM/GPS reposent sur un même schéma : une demande d'information est adressée par le biais du réseau GSM ; le récepteur GPS à bord du véhicule calcule en temps réel la position de ce dernier et renvoie l'information par le réseau GSM central, qui affiche alors la situation sur une carte routière.

Certaines applications visent les particuliers alors que d'autres sont destinées aux employeurs afin d'assurer la localisation de leurs salariés lorsqu'ils utilisent des véhicules professionnels. Dans les deux cas, le risque d'atteinte à la liberté d'aller et de venir et à la vie privée existe, les dispositifs envisagés permettant de connaître avec précision les itinéraires des conducteurs des véhicules. En revanche, la problématique diffère selon qu'il s'agit de salariés ou non.

D'une manière générale, la mise en œuvre de tels dispositifs nécessite de s'assurer que les modalités d'information des personnes concernées sont satisfaisantes, de déterminer une durée de conservation des données pertinente par rapport à la finalité du traitement et de strictement limiter l'accès aux données de géolocalisation aux personnes habilitées en raison de leurs fonctions.

Les sociétés abonnées aux services GSM/GPS disposent d'un accès direct aux données de géolocalisation en se connectant via internet aux serveurs du prestataire de service. L'information de base, celle relative au trajet effectué, peut être associée à des informations relatives au temps d'arrêt, à l'heure de départ et d'arrivée et à la vitesse des véhicules.

Ce type de services doit notamment être apprécié à la lumière de l'article L120-2 du Code du travail qui dispose que « nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature des tâches à accomplir ni proportionnées au but recherché ».

La CNIL considère que la mise sous surveillance permanente des déplacements des salariés est disproportionnée lorsque la tâche à accomplir ne réside pas dans le déplacement lui-même mais dans la réalisation d'une prestation pouvant faire elle-même l'objet d'une vérification.

Du reste, un arrêt du 26 novembre 2002 de la Chambre sociale de la Cour de Cassation faisant application de cet article juge qu'une filature organisée par l'employeur pour contrôler et surveiller l'activité d'un salarié constitue un moyen de preuve illicite, sans faire de distinction selon que le salarié a été ou non informé de l'existence d'un tel contrôle. Or, la surveillance systématique des déplacements des salariés via la mise en œuvre d'un dispositif GPS/GSM pourrait être assimilée par les juridictions compétentes à une filature électronique et constituer ainsi une atteinte à la vie privée de ces derniers, susceptible de ne pouvoir être justifiée, eu égard à son caractère disproportionné, par les intérêts légitimes de l'employeur.

Sur le lieu de travail, les badges électroniques (cartes magnétiques ou à puce) servent notamment au contrôle des accès aux locaux, à la gestion des temps de travail, ainsi qu'à la gestion de la restauration d'entreprise.

Ces différents types de dispositifs, qui comportent des données permettant l'identification des employés, sont soumis à la loi « informatique et libertés » et, ainsi que la Cour de cassation l'a rappelé dans son arrêt du 6 avril 2004, doivent être préalablement déclarés auprès de la CNIL.

Quels enjeux, quelles garanties prévoir ?

Chaque passage au niveau d'un lecteur de badge permet la lecture et l'enregistrement de données relatives à son détenteur. Ces enregistrements favorisent la « traçabilité » des déplacements de la personne concernée. Ils pourraient notamment conduire à la surveillance des allées et venues des représentants du personnel et des délégués syndicaux. Le dispositif pourrait également leur interdire abusivement l'accès à certains locaux.

Par ailleurs, les enregistrements réalisés seraient susceptibles de permettre à l'employeur d'accéder au détail des consommations de ses personnels au sein du restaurant d'entreprise ou du restaurant administratif.

Des garanties particulières doivent donc être apportées par l'employeur pour éviter de tels détournements de finalité (Voir délibération n°2002-001 du 8 janvier 2002).

Les personnels et leurs représentants doivent être également parfaitement informés, préalablement à la mise en œuvre du système de badges, des objectifs poursuivis, des services destinataires des données les concernant, et de leur droit d'accès et de rectification à ces données.

Comment déclarer auprès de la CNIL ?

Si le dispositif envisagé respecte en tout point le cadre fixé par la norme simplifiée n°42, l'employeur privé ou public peut réaliser une déclaration simplifiée (NB : il est dispensé de déclaration s'il a mis en place un correspondant informatique et libertés).

Dans le cas contraire - notamment en cas de recours à des dispositifs biométriques -, des formalités de déclaration particulières devront être accomplies auprès de la CNIL.

UTILISATION DE BADGES SUR LE LIEU DE TRAVAIL

La CNIL reste défavorable à la création de bases de données d'empreintes digitales en l'absence d'un impératif de sécurité incontestable.

La Commission considère que les empreintes digitales, à la différence d'autres données biométriques, laissent des traces qui peuvent être exploitées pour l'identification des personnes et que dès lors toute base de données d'empreintes digitales est susceptible d'être utilisée à des fins étrangères à sa finalité première. Seul un impératif de sécurité incontestable peut justifier la constitution de telles bases.

À l'inverse, elle estime que si le gabarit de l'empreinte digitale est uniquement stocké dans un support personnel (carte à puce…), le dispositif ne pose pas de difficultés au regard de la loi « informatique et libertés ». Il en est de même pour les dispositifs recourant aux biométries qui ne laissent pas de traces telles que la reconnaissance du contour de la main ou de l'iris.

Elle a ainsi rendu un avis favorable à la mise en oeuvre d'un contrôle d'accès aux zones réservées de sûreté d'aéroports reposant sur un système de reconnaissance de l'empreinte digitale car sa proposition de conservation du gabarit biométrique sur une carte d'accès individuelle (et non dans une base de données centralisée ou sur un lecteur biométrique) avait été suivie.

Elle a en revanche délivré un avis défavorable à la mise en place, par un centre hospitalier, d'un dispositif de reconnaissance de l'empreinte digitale utilisé pour le contrôle des temps de travail dans la mesure où les données biométriques étaient stockées non pas sur un support individuel mais dans un lecteur biométrique sur lequel l'employé n'a aucune maîtrise.

La reconnaissance du contour de la main : une technique biométrique qui ne laisse pas de traces

La CNIL a autorisé plusieurs dispositifs reposant sur l'utilisation de la technique biométrique de reconnaissance du contour de la main pour des usages variés : entrée dans des locaux sécurisés, accès à une cantine scolaire mais aussi contrôle des horaires des employés d'une mairie. Dans tous ces cas elle a considéré que dans la mesure où le dispositif recourt à une biométrie qui ne laisse pas de traces, ce qui est le cas de la reconnaissance du contour de la main, il ne pose pas de difficultés au regard de la loi informatique et libertés.

Les dispositifs de traitements de données biométriques sont, depuis la loi du 6 août 2004 modifiant la loi informatique et libertés, soumis à autorisation de la CNIL.

Deux sociétés privées ont présenté chacune à la CNIL un dispositif biométrique de reconnaissance du contour de la main afin de contrôler l'accès de leurs personnels à certains locaux, des zones de stockage de produits de valeur dans un cas, la salle d'hébergement informatique dans l'autre cas.

Un collège a opté pour un système biométrique de reconnaissance de la géométrie de la main afin de gérer les accès des élèves et du personnel au service de restauration scolaire de l'établissement. Les personnes ne désirant pas utiliser ce système sont dotées d'une carte à code barre.

Une mairie a souhaité remplacer le dispositif de contrôle des horaires par badge afin de remédier aux pertes et oublis des badges. Le dispositif vise à enregistrer les dates et heures d'entrée et de sortie des employés pour la gestion de leur temps de travail dans le contexte de la mise en place des horaires variables.

Ces dispositifs reposent sur la mise en œuvre de lecteurs biométriques du contour de la main qui contiennent une base de données comportant les gabarits biométriques et les codes d'accès. Lors de chaque passage, la reconnaissance du contour de la main s'opère après saisie sur le clavier du lecteur d'un code personnel, en plaçant la main sur un appareil de capture de l'image géométrique de la main. Aucune image ou photo de la main n'est conservée. Seule une clé biométrique (chaîne de caractères), résultat du traitement des mesures par un algorithme, est associée à l'identité de la personne.

La CNIL (séances des 21 juin et 5 juillet 2005) a considéré que dans la mesure où ces dispositifs recourent à une biométrie qui ne laisse pas de traces, ils ne posent pas de difficultés au regard de la loi du 6 janvier 1978 modifiée en août 2004.

En effet, le contour de la main, à la différence des empreintes digitales notamment, fait partie des données biométriques qui ne laissent pas de traces susceptibles d'être utilisées à des fins étrangères à la finalité recherchée par le responsable du traitement. Par conséquent, dans tous ces cas, compte tenu des caractéristiques des dispositifs présentés et en l'état actuel des connaissances sur la technologie utilisée, la mise en œuvre d'un traitement reposant sur la reconnaissance du contour de la main apparaît adaptée et proportionnée à la finalité assignée au dispositif.

L'UTILISATION PAR LES ORGANISATIONS SYNDICALES DE L'INTRANET ET DE LA MESSAGERIE ÉLECTRONIQUE DE L'ENTREPRISE

L'article L. 412-8 modifié du Code du travail officialise la possibilité pour les organisations syndicales d'utiliser l'intranet et la messagerie électronique de leur employeur par voie d'accord d'entreprise.

La loi n°2004-391 du 4 mai 2004 relative à la formation professionnelle tout au long de la vie et au dialogue social insère à l'article L 412-8 du Code du travail un alinéa ainsi rédigé :

« Un accord d'entreprise peut autoriser la mise à disposition des publications et tracts de nature syndicale, soit sur un site syndical mis en place sur l'intranet de l'entreprise, soit par diffusion sur la messagerie électronique de l'entreprise. Dans ce dernier cas, cette diffusion doit être compatible avec les exigences de bon fonctionnement du réseau informatique de l'entreprise et ne pas entraver l'accomplissement du travail. L'accord d'entreprise définit les modalités de cette mise à disposition ou de ce mode de diffusion, en précisant notamment les conditions d'accès des organisations syndicales et les règles techniques visant à préserver la liberté de choix des salariés d'accepter ou de refuser un message. »

Ces dispositions rejoignent les recommandations formulées par la CNIL dès mars 2001 dans son rapport sur la « cybersurveillance des salariés dans l'entreprise » concernant la définition des conditions internes d'utilisation des moyens informatiques par la négociation interne.

Certaines règles et principes peuvent ainsi être utilement rappelés :

La nécessité d'une négociation préalable

L'accès par les organisations syndicales à l'intranet et à la messagerie électronique de l'entreprise ne peut être considéré comme légitime que si sa mise en œuvre résulte d'une négociation, désormais rendue obligatoire par la loi.

Le respect du principe de finalité

Si la diffusion d'informations syndicales par voie électronique peut ainsi être autorisée par accord d'entreprise, les adresses de messagerie électronique des salariés ne peuvent être utilisées dans le cadre de celui-ci par les organisations syndicales ou par l'employeur pour d'autres raisons que la mise à disposition de publications et tracts de nature syndicale.

Le respect des droits d'information et d'opposition préalable

Les salariés doivent être clairement et préalablement informés de cette utilisation afin de pouvoir manifester leur accord ou leur opposition à l'envoi de tout message syndical sur leur messagerie professionnelle.

L'accord conclu doit donc préciser les modalités selon lesquelles les employés peuvent s'opposer à recevoir des messages électroniques émanant d'organisations syndicales. En tout état de cause, ce droit ainsi que ses modalités d'exercice devraient être systématiquement rappelés dans tout message ultérieur afin que les salariés puissent, à tout moment, manifester leur volonté de s'opposer à la réception de messages syndicaux.

Il apparaît par ailleurs utile de prévoir que l'indication du caractère syndical du message soit systématiquement mentionnée en objet du message électronique adressé, de façon à informer clairement les employés quant à l'origine et à la nature du message.

Assurer la confidentialité des échanges avec les organisations syndicales

L'accord conclu devrait également rappeler l'obligation de confidentialité à laquelle employeurs et organisations syndicales sont tenus. En particulier, toute mesure de sécurité devrait être prise afin d'assurer la confidentialité des échanges électroniques éventuels des salariés avec les organisations syndicales.

Afin d'éviter toute possibilité d'utilisation détournée, l'employeur ne devrait pas pouvoir exercer de contrôle sur les listes de diffusion ainsi constituées. En effet, celles-ci sont susceptibles de révéler l'opinion favorable d'un salarié à l'égard d'une organisation, voire son appartenance à un syndicat déterminé, sur la base du choix opéré par ce salarié quant à son acceptation ou son refus de recevoir des messages à caractère syndical.

Enfin, le texte nouveau ne concerne pas l'accès par les instances représentatives du personnel (membres du comité d'entreprise, du CHSCT, de comités techniques paritaires, délégués du personnel) aux moyens informatiques de l'entreprise. Conformément, à ses précédentes recommandations, la CNIL considère qu'un tel accès devrait être reconnu et organisé selon les mêmes modalités.

ENREGISTREMENT ET UTILISATION DU NUMÉRO DE SÉCURITÉ SOCIALE DANS LES TRAITEMENTS DE DONNÉES RELATIFS À LA PAIE ET À LA GESTION DU PERSONNEL

L'enregistrement du numéro de sécurité sociale dans les fichiers de paie et de gestion du personnel n'est autorisé que pour :

- l'établissement des bulletins de paie et des différentes déclarations sociales obligatoires (décret n° 91-1404 du 27 décembre 1991, articles R.115-1 et R.115-2 du code de la sécurité sociale) ;
- la tenue des comptes d'épargne salariale (article L.444-5 du code du travail).

Les états produits et les documents édités ne peuvent donc porter mention de ce numéro que dans le cadre des opérations précitées.

Cette règle s'applique même dans le cas de logiciels intégrés de gestion et de paie qui doivent être paramétrés pour limiter l'utilisation du numéro de sécurité sociale aux seules opérations précédemment décrites.

En particulier, le numéro de sécurité sociale ne fait pas partie de la liste des informations qui doivent figurer dans le registre unique du personnel, fixée par les articles L.620-3 et R. 620-3 du code du travail, et ne doit donc pas être enregistré dans ce cadre.

Le numéro de sécurité sociale d'un employé ne peut donc pas être utilisé comme numéro de matricule unique pour l'identifier dans tous les fichiers de gestion des ressources humaines de son entreprise ou de son administration.

GESTION DES ŒUVRES SOCIALES PAR LE COMITÉ D'ENTREPRISE

Les comités d'entreprise ou d'autres organismes ayant, dans le secteur public, un objet similaire, sont amenés à mettre en œuvre des fichiers informatisés afin de faciliter la gestion des œuvres sociales qui leur est confiée. De ce fait, le comité d'entreprise est amené à traiter des données à caractère personnel relatives aux salariés et à leur famille, voire à des salariés retraités.

Dans tous les cas, la mise en œuvre d'un fichier informatique par le CE doit respecter les conditions suivantes :

1. Information préalable

Que le CE soit amené à demander au service du personnel de son entreprise des renseignements concernant le personnel ou qu'il recueille ces renseignements en diffusant un questionnaire directement auprès des salariés, ces derniers doivent dans tous les cas être préalablement informés de la transmission, de l'objectif poursuivi, des destinataires des données, ainsi que de l'identité de la personne ou du service auquel ils peuvent s'adresser pour exercer leurs droits d'accès, de rectification et d'opposition.

L'affichage d'une note d'information dans les locaux ou la remise d'un document à l'employé peuvent constituer des mesures d'information adaptées. En cas de questionnaire, celui-ci doit obligatoirement comporter les mentions précisées au paragraphe précédent.

2. Droit d'opposition

Tout salarié a le droit de s'opposer à ce que le CE soit rendu destinataire de données le concernant. La transmission de ces données au CE ne peut être que facultative, le salarié devant être clairement informé des conséquences d'un éventuel refus de sa part (à titre d'exemple : application du tarif le plus élevé ou exclusion du bénéfice d'une prestation).

Si un salarié exprime son opposition (auprès de la direction du personnel ou directement auprès de son employeur), les données le concernant ne doivent pas être transmises au CE. Si l'opposition est exprimée postérieurement à la transmission de ces informations, le CE doit en être informé afin de supprimer les données le concernant.

3. Pertinence des données

Les données transmises doivent être limitées à celles qui sont strictement nécessaires au CE pour exercer ses fonctions légales.

Ainsi, le CE peut être amené à demander la fourniture de la copie de l'avis d'imposition des ouvrants-droit afin de procéder au calcul de la contribution de chacun en fonction de ses ressources. En revanche, le CE ne peut exiger la production de la déclaration de revenus, qui comporte des informations relevant de la vie privée des intéressés (Cour de Cassation, chambre civile, arrêt du 29 mai 1984, n°82-12.232).

4. Obligation d'assurer la confidentialité et obligation de déclaration préalable

Les données communiquées au CE ne peuvent être utilisées que dans le cadre de ses attributions. Il a également l'obligation d'assurer la sécurité et la confidentialité des données qu'il détient (article 34 d0e la loi informatique et libertés).

Si le CE met en place un fichier informatisé, pour son propre compte, il doit adresser à la CNIL une déclaration normale (formulaire disponible sur www.cnil.fr, rubrique déclarer, mode d'emploi), sauf désignation d'un correspondant informatique et libertés.

DOIS-JE DÉCLARER MON FICHIER À LA CNIL ? COMMENT ?

FINALITE DU FICHIER	FORMALITES DECLARATIVES
• Paie • Déclarations fiscales et sociales obligatoires (déclarations aux organismes de protection sociale, de retraite et de prévoyance, DADS, DUE, travailleurs handicapés...), y compris celles réalisées à partir de www.net-entreprises.fr • Tenue des registres obligatoires (registre unique du personnel...) • Tenue des comptes individuels relatifs à l'intéressement et à la participation • Statistiques non nominatives liées à l'activité salariée dans l'entreprise	AUCUNE
Comptabilité générale	AUCUNE
• Gestion des contrôles d'accès aux locaux, • Gestion des horaires, • Gestion de la restauration d'entreprise	DECLARATION SIMPLIFIEE Si désignation d'un correspondant informatique et libertés : AUCUNE
Fichiers courants de gestion des ressources humaines : • gestion administrative (dossiers professionnels, annuaires, élections professionnelles, convocations) • mise à disposition d'outils informatiques (suivi et maintenance, annuaires informatiques, messagerie électronique, Intranet) • organisation du travail (agenda professionnel, gestion des tâches) • gestion des carrières (évaluation, validation des acquis, mobilité…) • gestion de la formation	DECLARATION SIMPLIFIEE Si désignation d'un correspondant informatique et libertés : AUCUNE
Mise en œuvre de services de téléphonie fixe et mobile sur les lieux de travail Gestion des communications (annuaire interne, gestion des dotations, messagerie téléphonique interne, maîtrise des dépenses liées à l'utilisation des services de téléphonie …)	DECLARATION SIMPLIFIEE Si désignation d'un correspondant informatique et libertés : AUCUNE
Tout autre traitement automatisé, dès lors qu'il n'est pas conforme aux normes élaborées par la CNIL, notamment : • Traitements informatiques permettant un contrôle de l'activité professionnelle des salariés (vidéosurveillance, surveillance des connexions internet ou de la messagerie électronique, géolocalisation) • Traitements de recrutement (base de données de CV ou de candidats) • Fichiers médicaux gérés par la médecine du travail • Fichiers du service social • Fichiers détenus par les Comités d'entreprise aux fins de gestion des œuvres sociales • Traitements comportant un transfert de données vers un pays tiers à l'Union européenne	DÉCLARATION NORMALE Si désignation d'un correspondant informatique et libertés : AUCUNE
Dispositifs biométriques	AUTORISATION

CONDITIONS PARTICULIERES

Respecter la dispense n°1 (employeurs publics) ou la dispense n° 2 (employeurs privés).

Exclusion des transferts de données vers un pays tiers à l'Union Européenne.

Respecter les termes de la délibération n°80-34 du 21 octobre 1980.

Respecter la norme simplifiée n° 42. Cette norme ne concerne pas les traitements recourant à un procédé de reconnaissance biométrique, qui sont soumis à une procédure d'autorisation.

Respecter la norme simplifiée n° 46.
Cette norme exclut notamment :

- les traitements permettant le contrôle individuel de l'activité des employés
- les dispositifs ayant pour objet l'établissement du profil psychologique des employés
- les transferts de données vers un pays tiers à l'union européenne.

Respecter la norme simplifiée n°47
Cette norme exclut expressément :

- les finalités relatives à l'écoute ou à l'enregistrement de conversations téléphoniques
- la localisation d'un employé à partir de son téléphone portable.

Utiliser le formulaire de déclaration normale (téléchargeable sur le site de la cnil www.cnil.fr, rubrique déclarer, mode d'emploi).
Joindre un descriptif du fichier ou du traitement informatisé, établi à l'aide des modèles d'annexes proposés ou sur papier libre.
Pour les fichiers de recrutement : respecter la recommandation n°02-017 du 21 mars 2002.

Un système recourant, par exemple, à un procédé de reconnaissance des empreintes digitales ne peut être mis en œuvre sans l'autorisation préalable de la CNIL.

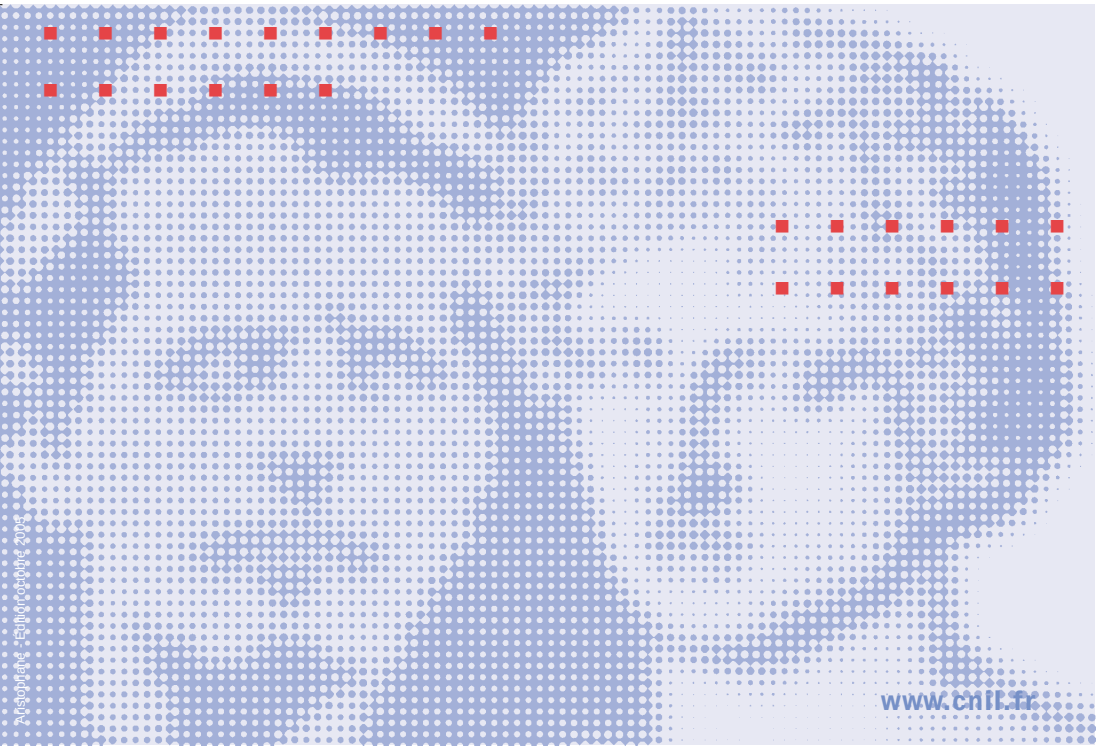
Dans tous les cas, la déclaration doit être effectuée avant la mise en œuvre du traitement. Cette mise en œuvre ne peut intervenir qu'à réception du récépissé de déclaration (pour les déclarations simplifiées et normales) ou de l'autorisation de la CNIL (pour les demandes d'autorisation).

Droit à l'information

Conformément aux dispositions du code du travail (article L.432-2-1) et aux textes relatifs aux trois fonctions publiques (lois n°84-16 du 11 janvier 1984, n°84-53 du 26 janvier 1984 et n°86-33 du 9 janvier 1986), les instances représentatives du personnel doivent être consultées et précisément informées des fonctionnalités envisagées dans le cas de mise en œuvre de traitements qui ont une incidence sur le personnel.
De plus, l'article L.121-8 du code du travail prévoit qu'aucune information concernant directement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance.
Les employés doivent, dans tous les cas de figure, être informés individuellement de l'existence des traitements contenant des données personnelles les concernant par note, affichage, publication dans le journal interne, courrier électronique ...
En application de la loi du 6 janvier 1978 modifiée, les personnels concernés doivent être informés de la ou des finalité(s) et fonctionnalités précises de chaque traitement automatisé mis en oeuvre par l'employeur, des conséquences individuelles qui pourront en résulter (par exemple un contrôle), des destinataires des données enregistrées et de leur droit d'accès , d'opposition et de rectification à ces données.
A cet égard, le dossier de déclaration présenté à la CNIL devra comprendre les modalités de consultation des instances représentatives du personnel et celles relatives à l'information individuelle des salariés.
Enfin, la déclaration préalable est accessible à toute personne qui en ferait la demande auprès de la CNIL.

Besoin d'information sur les règles applicables, les missions de la CNIL, les déclarations, le correspondant informatique et libertés... ?

www.cnil.fr



Artophane - Edition octobre 2005