LES GUIDES DE LA CNIL

GUIDE
POUR LES EMPLOYEURS ET LES SALARIÉS

Édition 2008

CNIL
Commission Nationale de l'Informatique et des Libertés

Sommaire

Ce guide est téléchargeable sur le site Internet de la CNIL : www.cnil.fr

Avant-propos

Les entreprises et les administrations recourent de façon croissante aux moyens informatiques pour gérer leurs ressources humaines. L'ensemble du secteur des RH est concerné : recrutement, gestion des carrières et des compétences, le suivi du temps de travail, etc..

Simultanément, les dispositifs de contrôle des salariés liés aux nouvelles technologies se multiplient : vidéosurveillance, cybersurveillance, applications biométriques, géolocalisation, etc..

Ces applications enregistrent de nombreuses informations à caractère personnel sur les salariés. La loi Informatique et Libertés fixe un cadre à la collecte et au traitement de ces données afin de les protéger, dans la mesure où leur divulgation ou leur mauvaise utilisation est susceptible de porter atteinte aux droits et libertés des personnes, ou à leur vie privée.

Le respect, par les entreprises et administrations des règles de protection des données à caractère personnel est un facteur de transparence et de confiance à l'égard des salariés. C'est aussi un gage de sécurité juridique pour les employeurs qui sont responsables de ces traitements informatiques et de la sécurité des données personnelles qu'ils contiennent. Ils peuvent ainsi voir leur responsabilité, notamment pénale, engagée en cas de non-respect des dispositions de la loi.

C'est pourquoi notre commission, chargée de veiller au respect de ces principes, souhaite informer les salariés des droits dont ils disposent, ainsi que les employeurs, en les conseillant sur les mesures à adopter pour se conformer à la loi.

Ce guide a pour vocation de leur donner les clés pour bien utiliser ces outils et les fichiers mis en œuvre en matière de gestion des ressources humaines.

C'est aussi le but du « correspondant informatique et libertés », interlocuteur privilégié de la CNIL dont la désignation permet, au-delà de l'exonération de déclaration, d'intégrer pleinement la problématique de la protection des données personnelles.

Alex TÜRK
Président de la CNIL

I – Les 5 principes clés à respecter

La loi « Informatique et Libertés » du 6 janvier 1978 modifiée par la loi du 6 août 2004 est applicable dès lors qu'il existe un traitement automatisé ou un fichier manuel (c'est-à-dire un fichier informatique ou un fichier « papier ») contenant des informations relatives à des personnes physiques.

Elle définit les principes à respecter lors de la collecte, du traitement et de la conservation de ces données et garantit un certain nombre de droits pour les personnes.

1. Le principe de finalité

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

- *la mise en place d'un autocommutateur téléphonique ou d'un dispositif de localisation par GPS (géolocalisation) ne peut avoir pour objectif le contrôle des conversations téléphoniques ou des déplacements de salariés protégés.*

- *Le fichier du personnel et l'adresse électronique des employés ne peut être utilisé à des fins de propagande politique. Les informations enregistrées par un logiciel conçu pour la réservation de billets de transports et déclaré comme tel ne peuvent être utilisées par un employeur pour contrôler l'activité de ses salariés (Cour d'appel de Paris, ch. Soc., 31 mai 1995).*

Tout détournement de finalité est passible de sanctions pénales.

Les objectifs poursuivis par la mise en place d'une application informatique doivent donc être au préalable clairement définis (gestion des recrutements, sécurité du réseau informatique, contrôle du temps de travail, etc.).

2. Le principe de proportionnalité et de pertinence des données

Seules doivent être traitées les informations **pertinentes et nécessaires** 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 n'est pas pertinent. L'enregistrement de la situation familiale précise d'un salarié ne peut se justifier que pour l'attribution d'avantages sociaux particuliers au salarié ou à sa famille.

En outre, comme le rappelle le code du travail, la mise en place d'un dispositif de contrôle des salariés ne doit pas conduire à apporter aux droits et libertés des personnes de restrictions qui ne seraient pas **proportionnées** au but recherché et justifiées par l'intérêt légitime de l'entreprise (article L1121-1 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 et dûment avéré pour la sécurité du salarié concerné (voir fiche n° 8). De même, la mise en place, pour contrôler l'accès à des locaux d'une base d'empreintes digitales ne peut se justifier que face à un fort impératif de sécurité et en l'absence de solutions alternatives moins intrusives (voir fiche n° 12).

3. Le principe d'une durée limitée de conservation des données

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

Par exemple : le temps de la présence du salarié s'agissant d'une application de gestion des carrières, cinq ans pour un fichier de paie, deux ans après le dernier contact avec le candidat à un emploi pour un fichier de recrutement, un mois pour les enregistrements de vidéosurveillance…

4. Le principe de sécurité et de confidentialité des données

L'employeur, en tant que responsable du traitement, est astreint à une **obligation de sécurité** : il doit prendre les mesures nécessaires pour garantir la confidentialité des données et éviter leur divulgation à des tiers non autorisés.

Par exemple : chaque salarié doit disposer d'un mot de passe individuel régulièrement changé. Les droits d'accès aux données doivent être précisément définis en fonction des besoins réels de chaque personne (lecture, écriture, suppression). Il peut également être utile de prévoir un mécanisme de verrouillage systématique des postes informatiques au-delà d'une courte période de veille.

Ainsi, les données à caractère personnel ne doivent être consultées que par les personnes habilitées à y accéder en raison de leurs fonctions.

Par exemple : les personnes habilitées du service des ressources humaines s'agissant de la gestion de la paie, les administrateurs réseaux s'agissant des données de connexion à internet.

Les données peuvent néanmoins être communiquées à des tiers autorisés à en connaître en application de dispositions législatives particulières (Inspections du travail, services fiscaux, services de police…).

5. Le principe du respect des droits des personnes

> Information des personnes

Lors de l'informatisation de leurs données, les salariés concernés ou les candidats à un emploi 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 au titre de la loi « Informatique et Libertés » (droit d'accès, de rectification et d'opposition).

Cette information peut être diffusée par tout moyen approprié : panneaux d'affichage ; page « protection des données » ou « informatique et libertés » sur l'intranet de l'entreprise.

En outre, lorsque les données sont recueillies par voie de questionnaires, papier ou informatisé, ceux-ci doivent comporter cette information.

Au-delà, l'employeur doit 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 ».

> Droits d'accès et de rectification

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.

Par exemple : un salarié peut accéder à son dossier professionnel (voir fiche n° 3).

> Droit d'opposition

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, sauf si celui-ci résulte d'une obligation légale ou réglementaire (ex. : déclarations sociales obligatoires, tenue du registre du personnel).

Par exemple : une personne peut dans certaines conditions s'opposer à la mise en ligne de ses coordonnées professionnelles ou de sa photographie (voir fiche n° 2).

II – Les missions de la CNIL

La Commission nationale de l'informatique et des libertés, autorité administrative indépendante est chargée d'assurer le respect des dispositions de la loi du 6 janvier 1978 modifiée par la loi du 6 août 2004.

1. Le rôle de conseil et d'information

La CNIL conseille et renseigne les personnes et les organismes qui envisagent de mettre en œuvre des fichiers informatiques, que ce soit par téléphone, par courrier ou par ses publications. Elle s'est dotée d'un service d'orientation et de renseignement afin d'apporter une réponse rapide aux requêtes des particuliers comme des professionnels sur l'application de la loi.

2. Le contrôle de la conformité des fichiers à la loi

La CNIL vérifie, lors de l'instruction des déclarations de fichiers qui lui sont adressées, que les caractéristiques des traitements concernés sont bien conformes à la loi et autorise la mise en œuvre des traitements qui, aux termes de la loi, nécessitent une attention particulière du fait de leur contenu ou de leur finalité. Elle peut simplifier les formalités déclaratives, voire exonérer de déclaration certains fichiers.

La CNIL reçoit les plaintes concernant le non-respect de la loi.

La CNIL dispose d'un pouvoir de contrôle qui permet à ses membres et ses agents d'accéder à tous les locaux professionnels. Sur place, ses membres et agents peuvent demander communication de tout document nécessaire et en prendre copie, recueillir tout renseignement utile et accéder aux programmes informatiques et aux données.

3. Le pouvoir de sanction

Au titre de son pouvoir de sanction, la CNIL peut notamment :

- adresser des avertissements et des mises en demeure de faire cesser un manquement à la loi ;
- prononcer une injonction de cesser le traitement ou un retrait de l'autorisation et, en cas d'urgence, décider l'interruption du traitement ou le verrouillage des données ;
- prononcer des sanctions pécuniaires pouvant aller jusqu'à 300 000 € en cas de réitération ;
- dénoncer au parquet les infractions à la loi dont elle a connaissance.

III – Le correspondant (CIL) : un vecteur de diffusion de la culture informatique et libertés

Institué 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 (CIL) est un acteur et un relais incontournable de la culture « informatique et libertés ».

Le correspondant doit, si possible, être un employé du responsable de traitement (correspondant interne), car connaissant mieux, a priori, l'activité et le fonctionnement interne de son entreprise ou de son administration, il est à même de veiller en temps réel à la bonne application des règles et des conditions de mise en œuvre des traitements. Mais il est aussi possible de désigner un correspondant n'appartenant pas à l'organisme (correspondant externe).

Pour s'acquitter de sa tâche, quel que soit son statut, le correspondant « informatique et libertés » doit disposer de la liberté d'action et des moyens qui lui permettront de recommander des solutions organisationnelles ou techniques adaptées. Il doit pouvoir exercer pleinement ses missions, en dehors de toute pression, et jouer son rôle auprès du responsable de traitement.

Le CIL – Quelques informations pratiques

Pourquoi désigner un CIL ? : Sa désignation, qui est facultative, exonère de déclaration la plupart des fichiers. Il contribue à une meilleure application de la loi.

Quels avantages pour l'organisme ? : Le CIL est un acteur de la sécurité juridique au sein de l'organisme. Son action peut prendre plusieurs formes : le conseil, la recommandation, la sensibilisation, la médiation et l'alerte en cas de disfonctionnement.

Comment désigner un CIL ? : C'est simple, il suffit de remplir le formulaire téléchargeable sur le site internet de la CNIL.

Comment le CIL pourrait-il/elle être formé(e) ? : La CNIL propose des ateliers d'information gratuits, généralistes et thématiques, animés par ses propres experts.

Quelle relation avec la CNIL ? : La CNIL a mis en place un service spécifique pour garantir au CIL une réponse rapide et de qualité. Il s'agit d'un guichet unique pour toutes les questions juridiques ou les éclairages liés à l'exercice de la fonction.

D'autres avantages ? : Le CIL est un interlocuteur privilégié de la CNIL. Ses demandes sont donc traitées en priorité. Il fait partie du réseau des CIL animés par la CNIL. Il participe à la réflexion liée à l'évolution de la fonction, à la création d'outils de travail, des textes juridiques…

Fiche n° 1 – les opérations de recrutement

1. Quelles sont les données qui peuvent être collectées ?

Les informations demandées sous quelque forme que ce soit, au candidat à un emploi ont pour finalité d'apprécier sa capacité à occuper l'emploi proposé. Elles doivent présenter un lien direct et nécessaire avec l'emploi proposé ou avec l'évaluation des aptitudes professionnelles du candidat.

La collecte des informations suivantes n'est pas pertinente, sauf cas particuliers justifiés par la nature très spécifique du poste à pourvoir ou par une obligation légale :

- 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 forme « 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.

Enfin, il est interdit de collecter et de conserver des données personnelles qui, directement ou indirectement, font apparaître les **origines raciales** ou **ethniques**, 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 que, dans certains cas, lorsqu'elles sont dûment justifiées par la spécificité du poste à pourvoir.

Le recueil de références auprès de l'environnement professionnel du candidat (supérieurs hiérarchiques, collègues, maîtres de stages, clients, fournisseurs…) est permis dès lors que le candidat en a été préalablement informé.

Attention

Les « zones commentaires » destinées à enregistrer des informations de gestion, telles des résumés d'entretien, doivent, comme toute donnée à caractère personnel enregistrée dans un traitement être pertinentes, adéquates et non excessives au regard de la finalité du traitement. La CNIL veille au respect de ces principes. Il faut avoir à l'esprit en rédigeant ces zones commentaires que la personne concernée peut y avoir accès à tout moment. Ainsi, à la suite d'un contrôle sur place effectué par une délégation de la CNIL en décembre 2006, il a été constaté que des commentaires particulièrement subjectifs, relatifs aux personnes ayant déjà été employées par une société mais qui n'ont pas donné satisfaction, figuraient dans le traitement de gestion des salariés qu'elle avait mis en œuvre. Ainsi, ont pu être relevés des commentaires tels que *« trop chiante », « problèmes d'hygiène (odeurs) », « personne sans dents et qui boit »*. Conformément aux articles 45 et suivants de la loi du 6 janvier 1978 modifiée, la formation contentieuse de la CNIL a prononcé, le 11 décembre 2007, une sanction pécuniaire d'un montant de 40 000 euros à l'encontre de cette société, compte tenu de la gravité des manquements constatés *(Délibération n° 2007-374 du 11 décembre 2007).*

2. L'information des candidats

Lors de la collecte des données, les candidats doivent être informés :

- de l'identité du responsable du traitement (ex : cabinet de recrutement X ; service des ressources humaines de la société Y) ;
- des finalités du traitement (ex : gestion des candidatures) ;
- du caractère obligatoire ou facultatif des réponses, (ex : le recueil d'informations sur les loisirs est facultatif) ;
- des conséquences à leur égard d'un défaut de réponse ;
- des personnes physiques ou morales destinataires des informations (ex : autres cabinets de recrutements) ;
- des conditions d'exercice de leur droit d'accès et de rectification ainsi que de leur droit d'opposition (ex : indication du service auprès duquel ces droits peuvent être exercés).

Attention

Lorsque des informations sur un candidat sont recueillies par voie de questionnaires papier ou de formulaires en ligne, ceux-ci doivent porter mention de ces prescriptions de façon claire et lisible (voir modèle proposé en annexe).

La CNIL recommande que les personnes chargées du recrutement prennent toutes les dispositions nécessaires pour informer le candidat, dans un délai raisonnable :

- des suites données à sa candidature;
- de la durée de conservation des informations le concernant ainsi que de la possibilité d'en demander la restitution ou la destruction;
- de toute éventuelle cession d'informations avec d'autres organismes de recrutement et de la possibilité de s'y opposer;
- 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 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.

Lorsque l'identité de l'employeur n'a pas été précisée lors de l'offre de poste, il est recommandé que l'accord du candidat soit recueilli préalablement à la transmission de son CV à cet employeur.

Dans le cas de sites de recrutements en ligne, 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.

3. Comment exercer ses droits ?

Tout candidat ou employé doit pouvoir obtenir sur demande et dans un délai raisonnable toutes les informations le concernant y compris les résultats des analyses et des tests (psychologiques, graphologiques...) 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 peut être faite par tout moyen approprié au regard de la nature de l'outil utilisé.

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.

4. Combien de temps peut-on conserver les données relatives à un candidat ?

La CNIL recommande que la durée de conservation des informations (sur support informatique et papier) n'excède pas **deux ans** après le dernier contact avec la personne concernée.

5. Comment déclarer ?

Les applications de gestion du recrutement doivent, préalablement à leur mise en œuvre, faire l'objet d'une déclaration normale, sauf désignation d'un correspondant informatique et libertés (dispense de déclaration).

Fiche n° 2 – les annuaires du personnel

La constitution d'un annuaire du personnel sur support informatisé comportant l'identité des salariés, leur fonction, leurs coordonnées professionnelles et le cas échéant leur photographie, constitue un traitement de données personnelles soumis aux dispositions de la loi du 6 janvier 1978 modifiée en 2004.

Les annuaires du personnel ne doivent pas être utilisés à des fins commerciales ou politiques.

Distinction annuaire interne/annuaire « externe »

Annuaire interne : annuaire accessible aux seuls membres du personnel, diffusé sur intranet ou sur format papier.

Annuaire « externe » : annuaires accessibles à d'autres personnes que le personnel de l'organisme (ex : annuaire publié sur internet).

1. La nécessité d'informer les intéressés

L'employeur doit informer ses salariés, préalablement à la mise en place d'un annuaire, de leurs droits d'accès, de rectification et d'opposition. Cette information s'effectue par la remise d'un document écrit ou par voie électronique (voir modèle proposé en annexe).

La diffusion sur internet de données à caractère personnel (ex : nom, prénom, coordonnées professionnelles, etc.) rend ces informations accessibles à quiconque, sans que l'intéressé puisse réellement maîtriser leur utilisation. Par conséquent, le salarié doit pouvoir s'opposer simplement et à tout moment à une telle diffusion.

La CNIL recommande que la diffusion de la photographie soit subordonnée à l'accord préalable de l'employé en particulier lorsque cette photographie est destinée à être publiée ou mise en ligne sur internet.

2. Comment déclarer ?

Les annuaires professionnels internes doivent faire l'objet d'une déclaration de conformité en référence à la norme n° 46 relative à la gestion des personnels des organismes publics et privés, sauf si un Correspondant informatique et libertés a été désigné au sein de l'organisme (dispense de déclaration).

Les annuaires autres que les annuaires internes doivent faire l'objet d'une déclaration normale préalablement à leur mise en œuvre, sauf si un Correspondant informatique et libertés a été désigné au sein de l'organisme (dispense de déclaration).

Fiche n° 3 – l'accès au dossier professionnel

Tout salarié ou ancien salarié justifiant de son identité a le droit d'accéder à son dossier professionnel auprès du service du personnel.

1. Un droit d'accès à quelles données ?

L'intéressé peut obtenir communication de l'ensemble des données le concernant, qu'elles soient conservées sur support informatique ou dans un dossier papier.

Par exemple, il a le droit d'accéder aux données relatives :
- à son recrutement;
- à son historique de carrière;
- à sa rémunération;
- à l'évaluation de ses compétences professionnelles (entretiens annuels d'évaluation, notation);
- à son dossier disciplinaire, etc.

2. Limites au droit d'accès

Le salarié ou ancien salarié n'a pas le droit d'accéder :

- aux données concernant la situation personnelle d'un tiers, notamment d'un autre salarié;
- aux données prévisionnelles de carrière (potentiel de carrière, classement), sauf si ces données ont été prises en compte pour décider de son augmentation de salaire, de sa promotion, de son affectation, etc. Un salarié doit ainsi pouvoir accéder à l'ensemble des données de gestion des ressources humaines qui ont servi à prendre une décision à son égard.

L'employeur a le droit de s'opposer aux demandes manifestement abusives. En cas de contestation, il doit démontrer que la demande du salarié est abusive.

3. Comment s'exerce le droit d'accès ?

Le droit d'accès peut s'exercer soit sur place, soit par écrit, avec un justificatif d'identité.

L'employeur doit répondre immédiatement si la demande est effectuée sur place, ou dans un délai maximal de 2 mois si la demande est écrite (ou s'il est impossible de répondre immédiatement à la demande sur place). Son éventuel refus doit être écrit, motivé et doit mentionner les voies et délais de recours.

Une copie des données est délivrée à l'intéressé à sa demande. Le simple coût de la copie peut éventuellement lui être réclamé.

Les codes, sigles et abréviations figurant dans les documents communiqués doivent être expliqués, si nécessaire à l'aide d'un lexique.

Fiche n° 4 – la gestion des œuvres sociales et culturelles

Qu'il s'agisse de la gestion des subventions, des bourses, des primes de crèches, des chèques cadeaux, des activités de voyages, sport ou loisirs, les traitements informatisés mis en œuvre par les comités d'entreprise (CE) ou d'établissement, ainsi que par les comités centraux d'entreprises, les comités de groupe, les comités interentreprises ou les délégués du personnel, enregistrent des données personnelles sur les salariés et doivent à ce titre se conformer à la loi informatique et libertés.
Ces informations doivent être limitées à celles qui sont strictement nécessaires au CE pour exercer ses fonctions légales.

Par exemple : 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).

1. Information des salariés

Les salariés doivent être préalablement informés par le CE, et le cas échéant l'employeur, 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 (voir modèles proposés en annexe).

Par exemple : affichage d'une note d'information dans les locaux, remise d'un document à l'employé, mentions apparentes sur le questionnaire.

2. Droit d'opposition

- Tout salarié a le droit de s'opposer à ce que le CE soit rendu destinataire de données le concernant par l'employeur. 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;

  Par exemple : application du tarif le plus élevé ou exclusion du bénéfice d'une prestation.

- Lorsque les données sont utilisées à des fins d'offres promotionnelles les personnes concernées sont informées qu'elles peuvent s'y opposer sans frais et sans justification. L'envoi d'offres promotionnelles par voie électronique est subordonné au recueil du consentement préalable des personnes concernées.

3. Comment déclarer ?

Les traitements de gestion sociale ou culturelle les plus courants sont dispensés de déclaration. Pour bénéficier de cette dispense, les traitements envisagés doivent être conformes à la dispense de déclaration n°10 en date du 17 octobre 2006 (disponible sur www.cnil.fr).

Dans tous les autres cas, le CE doit adresser à la CNIL une déclaration normale.

4. Droits de mise à jour ou de suppression des données

S'il constate la présence de données erronées ou interdites (ex. : appréciations subjectives, opinions politiques, sanctions amnistiées…), le salarié ou ancien salarié a le droit de demander la mise à jour ou la suppression de ces données.

Si ces données ont été transmises à des tiers (à d'autres entreprises du groupe par exemple), l'employeur doit demander à ces tiers leur mise à jour ou leur suppression.

L'intéressé peut demander à l'employeur de justifier, sans frais, qu'il a bien pris en compte ses demandes de rectification ou de suppression des données. Il peut également obtenir le remboursement des frais de copie que l'employeur lui a éventuellement réclamés.

5. Que faire en cas de difficulté ?

Il est possible d'alerter le correspondant informatique et libertés (CIL) qui a pu être désigné par l'employeur ou de saisir la CNIL d'une plainte. Une plainte pénale peut également être déposée auprès du Procureur de la République ou des services de police ou de gendarmerie.

Fiche n° 5 – les transferts internationaux de données

1. De quoi s'agit-il ?

Constitue un transfert de données vers un pays tiers toute communication ou copie de données par l'intermédiaire d'un réseau, ou d'un support à un autre, quel que soit le type de ce support, dans la mesure où ces données ont vocation à faire l'objet d'un traitement dans le pays destinataire.

Par exemple : sont considérés comme des transferts internationaux de données :

- *la centralisation dans un pays étranger de la base de données de gestion des ressources humaines ;*
- *le transfert vers un prestataire étranger aux fins de saisie informatique des dossiers du personnel ;*
- *l'hébergement de données à caractère personnel dans un pays étranger.*

2. Pourquoi encadrer les transferts de données à caractère personnel vers des pays n'appartenant pas à l'Union européenne ?

Les personnes bénéficiant d'une protection de leurs données en France par la loi « Informatique et Libertés » doivent continuer à en bénéficier lorsque leurs données quittent le territoire français pour faire l'objet d'un traitement en dehors de l'Union européenne.

3. Quelles sont les principales obligations à respecter ?

> Finalité

Tout transfert de données vers l'étranger doit avoir une finalité déterminée, explicite et légitime : le responsable de traitement établi en France doit pouvoir expliquer pourquoi le transfert a lieu (ex : transfert d'information à destination de la maison mère, hébergement des données à l'étranger, externalisation de certains services…) et s'être assuré que ces raisons sont compatibles avec les exigences de la loi française (ex : sécurité des données, durée de conservation limitée des données…).

Les données transférées ne doivent pas être traitées ultérieurement de manière incompatible avec cette finalité.

> Pertinence des données

Les données transférées doivent être adéquates, pertinentes et non excessives au regard de la ou des finalités pour lesquelles elles sont transférées.

Concernant cette dernière obligation, la CNIL constate fréquemment que des sociétés multinationales envisagent d'opérer des transferts concernant l'intégralité du personnel de sociétés françaises dans le cadre de la centralisation des bases de données « ressources humaines » de leur groupe.
Ces transferts ne devraient pas porter sur la totalité ou la quasi-totalité des informations nominatives relatives aux salariés. En particulier le numéro de sécurité sociale, ou les données touchant à des aspects de la vie privée des employés (ex : détails sur la situation familiale, coordonnées bancaires) paraissent a priori ne devoir relever que d'une gestion locale.

> Information des salariés
Outre les dispositions législatives concernant la consultation des instances représentatives du personnel, les salariés doivent être informés, préalablement des transferts de données envisagés à destination d'un pays non membre de l'Union européenne.

Cette information doit être rédigée en français. Elle doit préciser :

- le ou les pays d'établissement du destinataire des données;
- la nature des données transférées, (ex : identité, salaire, CV…);
- la finalité du transfert envisagé, (ex : hébergement des données par une société étrangère, centralisation des données par la société mère à des fins statistiques…);
- la ou les catégories de destinataires des données (ex : le service informatique, personnes habilités du service ressource humaines…).

Voir modèle proposé en annexe

4. Comment déclarer les transferts internationaux de données ?

Lorsque le transfert de données concerne un pays de l'Union européenne, il n'a pas à être autorisé par la CNIL.

En cas de transfert de données en dehors de l'Union européenne, l'employeur doit le préciser sur le formulaire de déclaration et remplir une annexe « transfert ».

Il doit ainsi joindre au dossier les garanties de protection des données y afférentes : existence de clauses contractuelles types issues des directives européennes, ou de règles internes d'entreprises (BCR), adhésion au *safe harbor*.

Le transfert doit ensuite faire l'objet d'une autorisation par la CNIL, sauf dans certains cas bien spécifiques (par exemple, entreprise destinataire adhérente au *safe harbor*).

Fiche n° 6 – contrôle de l'utilisation d'internet et de la messagerie

Pour l'exercice de leur activité professionnelle, les salariés ont à leur disposition un poste de travail informatique qui peut être connecté à internet et doté d'une messagerie électronique. L'utilisation, sur les lieux de travail, de ces outils informatiques à des fins autres que professionnelles est généralement tolérée. Elle doit rester raisonnable et ne doit pas affecter la sécurité des réseaux ou la productivité de l'entreprise ou de l'administration concernée.

1. Le contrôle de l'utilisation d'internet

L'employeur peut fixer les conditions et limites de l'utilisation d'internet, lesquelles ne constituent pas, en soi, des atteintes à la vie privée des salariés.

Par exemple : L'employeur peut mettre en place des dispositifs de filtrage de sites non autorisés (sites à caractère pornographique, pédophile, d'incitation à la haine raciale, révisionnistes, etc.). Il peut également fixer des limites 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, etc.

> Nécessité d'informer les salariés

Les salariés doivent être informés des dispositifs mis en place et des modalités de contrôle de l'utilisation d'internet :

- Le comité d'entreprise doit avoir été consulté et informé (article L2323-32 du code du travail);
- Les salariés doivent être informés, notamment de la finalité du dispositif de contrôle et de la durée pendant laquelle les données de connexion sont conservées.

Une durée de conservation de l'ordre de **six mois** est suffisante, dans la plupart des cas, pour dissuader tout usage abusif d'internet.

Si des procédures disciplinaires sont susceptibles d'être engagées sur la base de ces fichiers, les salariés doivent en être explicitement informés (par exemple au moyen d'une charte).

> Comment déclarer ?

Lorsque l'entreprise ou l'administration met en place un **dispositif de contrôle individuel des salariés destiné à produire un relevé des connexions ou des sites visités, poste par poste,** le traitement ainsi mis en œuvre doit être déclaré à la CNIL (déclaration normale) sauf si un correspondant informatique et libertés a été désigné, auquel cas aucune déclaration n'est nécessaire.

Par exemple : logiciel de contrôle de l'utilisation d'internet permettant d'analyser les données de connexion de chaque salarié ou de calculer le temps passé sur internet par un salarié déterminé.

Lorsque l'entreprise ou l'administration met en place un dispositif qui ne permet pas de contrôler individuellement l'activité des salariés, ce dispositif peut faire l'objet d'une déclaration de conformité en référence à la norme simplifiée n° 46 (gestion des personnels des organismes publics et privés).

Par exemple : logiciel permettant seulement de réaliser des statistiques sur l'utilisation d'internet au niveau de l'ensemble des salariés de l'entreprise ou au niveau d'un service déterminé.

2. Le contrôle de l'utilisation de la messagerie

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 contrôle de la messagerie.

Par exemple : outils de mesure de la fréquence, de la taille, des messages électroniques ; outils d'analyse des pièces jointes (détection des virus, filtres « anti-spam » destinés à réduire les messages non-sollicités, etc.).

> Nécessité d'informer les salariés
Les dispositifs de contrôle de la messagerie doivent 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 individuelle des salariés.

Ils doivent notamment être informés, de la finalité du dispositif et de la durée pendant laquelle les données de connexion sont conservées ou sauvegardées.
En cas d'archivage automatique des messages électroniques, ils doivent en outre être informés des modalités de l'archivage, de la durée de conservation des messages, et des modalités d'exercice de leur droit d'accès.

> Comment déclarer ?
La messagerie professionnelle doit faire l'objet d'une déclaration de conformité en référence à la norme n° 46 (gestion des personnels des organismes publics et privés).

Si un **dispositif de contrôle individuel de la messagerie** est mis en place, il doit être déclaré à la CNIL (déclaration normale), sauf désignation d'un correspondant informatique et libertés.

Par exemple : logiciel d'analyse du contenu des messages électroniques entrant ou sortants destinés au contrôle de l'activité des salariés.

3. L'accès au poste informatique ou à la messagerie

> L'employeur doit respecter le secret des correspondances privées
Une communication électronique émise ou reçue par un employé peut avoir le caractère d'une correspondance privée. La violation du secret des correspondances est une infraction pénalement sanctionnée par les articles L.226-15 (pour le secteur privé) et L.432-9 (pour le secteur public) du Code pénal.

La Cour de cassation a affirmé, dans un arrêt du 2 octobre 2001 (arrêt « Nikon »), qu'un employeur ne saurait prendre connaissance de messages personnels d'un employé sans porter atteinte à la vie privée de celui-ci (article 9 du code civil) et au principe du secret des correspondances (article 226-15 du code pénal), quand bien même une utilisation à des fins privées aurait été proscrite par l'employeur.

Pour autant, le principe du secret des correspondances connaît des limites dans la sphère professionnelle. Il peut également être levé dans le cadre d'une instruction pénale ou par une décision de justice.

> Tout ce qui n'est pas identifié comme « personnel » est réputé être professionnel de sorte que l'employeur peut y accéder librement
La Cour de cassation considère qu'un message envoyé ou reçu depuis le poste de travail mis à disposition par l'employeur revêt un caractère professionnel, sauf s'il est identifié comme étant « personnel », dans l'objet du message par exemple (Cour de cassation, 30 mai 2007).

Il appartient à l'employé d'identifier les messages qui sont personnels. À défaut d'une telle identification, les messages sont présumés être professionnels.

La nature personnelle d'un message peut figurer dans l'objet du message ou dans le nom du répertoire dans lequel il est stocké.

La CNIL recommande de porter à la connaissance des salariés (par exemple dans une charte) le principe retenu pour différencier les e-mails professionnels des e-mails personnels (qualification par l'objet, création d'un répertoire spécifique dédié au contenu privé, etc.).

> Le cas des fichiers et des répertoires créés par un employé
Il a été jugé que les fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel (Cour de cassation, 18 octobre 2006).

Tout fichier qui n'est pas identifié comme « personnel » est réputé être professionnel de sorte que l'employeur peut y accéder hors la présence du salarié.

En revanche, si un fichier est identifié comme étant personnel, l'employeur ne peut y avoir accès « qu'en présence du salarié ou si celui-ci a été dûment appelé, ou en cas de risque ou événement particulier ».

Par exemple : il a été jugé que la découverte de photos érotiques dans le tiroir d'un salarié ne constituait pas un risque ou un événement particulier justifiant que l'employeur accède au répertoire intitulé « perso » hors la présence du salarié ou sans que celui-ci en soit informé.

> L'employé doit exécuter son contrat de travail de bonne foi
L'employé ne doit pas transformer des messages de nature professionnelle en correspondance « privée ».

Par exemple : Un employé ne doit pas communiquer des documents confidentiels à un concurrent en identifiant ses messages comme étant « personnels ». Une telle identification serait contraire au principe de bonne foi prévu à l'article L1222-1 du Code du travail.
La Cour de cassation a ainsi admis, après avoir constaté que l'employeur avait des motifs légitimes de suspecter des actes de concurrence déloyale, qu'un employeur puisse être autorisé par le juge à mandater un huissier de justice pour prendre connaissance et enregistrer des messages électroniques échangés entre le salarié et deux personnes étrangères à l'entreprise (Cour de cassation, 23 mai 2007).

> L'employé est-il tenu de communiquer ses mots de passe ?
Si un employé est absent, l'employeur peut lui demander de communiquer son mot de passe lorsque les informations détenues par cet employé sont nécessaires à la poursuite de l'activité de l'entreprise (Cour de cassation, 18 mars 2003). L'employeur ne doit pas accéder au contenu personnel de l'intéressé.

La CNIL recommande que les modalités d'accès de l'employeur aux données stockées sur l'environnement informatique d'un employé absent soient préalablement définies en concertation et diffusées auprès de l'ensemble des salariés susceptibles d'être concernés (via une charte par exemple).

> Comment organiser la fermeture du compte utilisateur lors du départ de l'employé ?
Les modalités de fermeture du compte sont à prévoir dans la charte informatique. Il est recommandé à l'employeur d'avertir le salarié de la date de fermeture de son compte afin que ce dernier puisse vider son espace privé.

> Que faire en cas de difficulté ?
En cas de contestation, il appartient aux juridictions compétentes d'apprécier la régularité et la proportionnalité de l'accès par l'employeur au poste informatique ou à la messagerie de l'employé.

Fiche n° 7 – les administrateurs réseau

Les administrateurs ont pour mission d'assurer le fonctionnement normal et la sécurité des réseaux et systèmes. Ils sont conduits par leurs fonctions même à avoir accès à des informations personnelles relatives aux utilisateurs (messagerie, historique des sites visités, fichiers « logs » ou de journalisation, etc.) y compris celles qui sont enregistrées sur le disque dur du poste de travail (fichiers temporaires, cookies…).

> Accès aux données personnelles des utilisateurs

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 même, les administrateurs de réseaux et systèmes 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 doit ainsi être clairement rappelée dans leur contrat, ainsi que 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

Les logiciels de prise de main à distance peuvent notamment permettre aux gestionnaires techniques d'accéder à distance à l'ensemble des données de n'importe quel poste de travail, à des fins de maintenance informatique.

Or, la CNIL constate parfois que ces outils de télémaintenance ou de prise de main à distance sont également utilisés à des fins de contrôle, par l'employeur, de l'activité de ses employés sur leur poste informatique. Une telle utilisation n'est ni conforme au principe de proportionnalité, ni respectueuse 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 doit 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.

Doivent 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.

Fiche n° 8 – la vidéosurveillance sur les lieux de travail

L'état actuel du droit se caractérise par la concurrence de deux régimes juridiques applicables : celui de la loi « informatique et libertés » du 6 janvier 1978 modifiée en 2004 et celui de l'article 10 de la loi du 21 janvier 1995 modifiée d'orientation et de programmation pour la sécurité (autorisation préfectorale).

Ceci explique le caractère complexe du régime juridique applicable en matière de vidéosurveillance.

Pour savoir quelle formalité préalable est nécessaire, il convient d'abord de déterminer si le dispositif de vidéosurveillance concerne un lieu public (ou ouvert au public) ou un lieu privé (ou non ouvert au public).

Distinction lieu public/lieu privé

• **lieu public ou ouvert au public :** tout lieu du secteur public ou du secteur privé où le public peut accéder. ***Exemple : le guichet d'une mairie ou un supermarché.***

• **lieu privé (lieu non ouvert au public) :** tout lieu du secteur public ou du secteur privé où le public ne peut pas accéder. ***Exemple : la chaîne de montage d'une entreprise automobile, le parking réservé au personnel d'une entreprise, un entrepôt ou des bureaux fermés au public***

Le régime juridique est clair dans deux cas :

- **Premier cas** : seule une autorisation préfectorale est nécessaire, quand le dispositif de vidéosurveillance est installé dans un lieu public ou ouvert au public et qu'aucune image n'est enregistrée ni conservée dans des traitements informatisés ou des fichiers structurés qui permettent d'identifier des personnes physiques ;
- **Deuxième cas** : seule une déclaration auprès de la CNIL est nécessaire, quand le dispositif est installé dans un lieu privé ou non ouvert au public et que les images sont enregistrées ou conservées dans des traitements informatisés ou des fichiers structurés qui permettent d'identifier des personnes physiques.

Le régime juridique n'est pas clair et pose problème lorsque le dispositif de vidéosurveillance est installé dans un lieu mixte (lieu ouvert au public qui comporte également des zones privées, par exemple un supermarché) et les images enregistrées dans un fichier ou traitées informatiquement. Dans cette hypothèses une déclaration auprès de la CNIL est nécessaire. Se pose toutefois la question du cumul avec la loi de 1995 (autorisation préfectorale).