LA CYBERSURVEILLANCE SUR LES LIEUX DE TRAVAIL

RAPPORT PRESENTE PAR

M. Hubert BOUCHET, vice-président délégué de la CNIL

Adopté par la Commission nationale de l'informatique et des libertés en séance plénière du 5 février 2002

Mis à jour à la suite de l'examen d'un rapport d'étape en séance plénière du 18 décembre 2003

Edition : mars 2004

Dans son rapport « Les libertés publiques et l'emploi »[1], le professeur Gérard Lyon-Caen rappelait que le débat sur la vie privée du salarié au sein de l'entreprise qui met en cause tout à la fois le lien de subordination qui caractérise le contrat de travail et la part irréductible de liberté des hommes et des femmes dans une société démocratique, n'était pas nouveau. Il soulignait cependant que le développement des moyens de contrôle technique lié aux nouvelles technologies nécessitait de le revisiter. *« La ligne de partage [entre lien de subordination et vie privée] ne saurait plus être tracée à la sortie des lieux de travail et à l'expiration de l'horaire. Tout est devenu plus complexe et plus flou »*. L'auteur du rapport évoquait un *« nouvel* espace police*, véritable ordre technologique qui n'a plus rien de commun avec l'ancienne subordination car le salarié n'est plus sous les ordres de quelqu'un. Il est surveillé par la machine, à la limite par lui-même, par tous et par personne »"*. S'agissant des messageries électroniques, le professeur Lyon-Caen annonçait : « *le strict respect des correspondances a vécu dans ce domaine ».* Nous étions en 1991...

La surveillance cantonnée par le droit

A la suite de ce rapport, la loi du 31 décembre 1992 a posé les jalons d'un droit « informatique et libertés » dans l'entreprise. Principe de proportionnalité (« *nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas proportionnées au but recherché* » - article L.120-2 du code du travail) ; consultation du comité d'entreprise lors de l'introduction de nouvelles technologies (article L.432-2 du code du travail) ; information préalable des salariés sur tout dispositif de collecte de données le concernant personnellement (article L.121-8).

Ces principes et droits font écho à la loi du 6 janvier 1978 qui impose que tout traitement de données personnelles soit déclaré à la CNIL, que les salariés soient informés de son existence, de ses finalités, de ses caractéristiques et qu'ils aient accès aux informations les concernant.

C'est sur la base de ces principes que, dès 1984, la Commission a établi, par le biais d'une recommandation qui devait trouver son prolongement dans une norme simplifiée, des règles d'usage des autocommutateurs téléphoniques qui permettent à l'employeur de connaître les numéros de téléphone appelés par un salarié depuis son poste[2].

Ces mêmes principes trouvent application en matière de vidéo-surveillance dans l'entreprise et la chambre sociale de la Cour de cassation donnera sa substance à ces principes : nul moyen de preuve ne peut être opposé par l'employeur aux salariés si le dispositif de contrôle a été mis en oeuvre à leur insu.

Mais jusqu'à présent, qu'il s'agisse d'autocommutateur téléphonique, de badges et de contrôle d'accès ou de vidéo-surveillance, la surveillance concernait principalement la présence ou la localisation physique de l'individu. En un mot, les technologies demeuraient encore à la périphérie du processus de travail.

[1] Rapport pour le ministre du travail, de l'emploi et de la formation professionnelle, décembre 1991, La Documentation française

[2] CNIL, 5ème rapport d'activité, p.109 et 15ème rapport d'activité, p.74, La Documentation française

Sans doute, le développement des écoutes téléphoniques dans le milieu du travail a-t-il signé un changement. La multiplication des services par téléphone et des centres d'appels a conduit les entreprises à surveiller la qualité du service, c'est-à-dire celle de la réponse apportée par le salarié. Sur ce point, la CNIL a développé un corpus de recommandations pratiques qui paraît être très largement respecté.

Cependant, avec l'émergence des nouvelles technologies de communication et tout particulièrement l'introduction d'internet dans l'entreprise, c'est une véritable migration des technologies de contrôle qui s'opère de la périphérie jusqu'au coeur du processus de travail proprement dit.

La cybersurveillance au coeur du processus de travail

Le recours de plus en plus systématique aux nouvelles technologies de réseau a des incidences considérables sur les rapports employés-employeurs.

Progressivement, l'information dont disposent les entreprises est numérisée, quelle que soit la nature de cette information. Dès lors qu'elle est informatisée et susceptible d'accès par internet ou intranet, des risques d'accès indus à cette information sont réels. Pour l'entreprise, les nouvelles technologies de l'information et de la communication vont naturellement poser des problèmes nouveaux en matière de sécurité dès lors que se trouvent externalisées des informations sur toute la vie de l'entreprise, ses fichiers de personnels, la gestion des commandes, ses secrets de fabrique, etc. Pour les salariés, la différence de nature entre les TIC et tout ce qui précède réside en la capacité nouvelle de la technologie de conserver toutes les traces laissées par la personne connectée.

Ainsi, la technique pose de façon nouvelle des questions qui avaient été réglées dans un contexte ancien. Un message électronique que le salarié a cru supprimer peut avoir été sauvegardé sur un serveur de messagerie ou sur un support magnétique de sauvegarde. Et ce salarié serait trompé si nul ne lui avait exposé que le message qu'il avait reçu de son épouse pour lui rappeler de ne pas oublier de faire une course avant de rentrer à son domicile, et qu'il avait aussitôt effacé de sa messagerie, avait été conservé à son insu.

L'équilibre est délicat à trouver.

L'ouverture de l'entreprise sur le monde, grâce à internet, et l'utilisation des réseaux d'information, la rendent plus vulnérable à des attaques informatiques venues de l'extérieur. La mise en place de mesures de sécurité constitue à cet égard une nécessité pour éviter les intrusions et pour protéger des documents confidentiels, des secrets de fabrique, ou encore les fichiers de l'entreprise. Or, ces mesures de sécurité auront précisément pour objet de conserver trace des flux d'informations, directement ou indirectement nominatives, afin de mieux prévenir les risques et de repérer l'origine des problèmes.

Par ailleurs, ces technologies qui sont tout à la fois, ergonomiques, faciles d'emploi et parfois ludiques, peuvent conduire les entreprises à veiller à ce que leurs salariés n'en fassent pas un usage abusif, sans lien avec leur activité professionnelle. Ce contrôle de productivité du « cyber-travailleur » s'exercera d'autant plus que toute architecture en réseau a pour effet d'éloigner géographiquement le salarié de sa hiérarchie.

L'évolution aura été constante.

D'abord, le contremaître, personne repérable, chargé de contrôler la présence physique du salarié sur son lieu de travail et en activité.

Puis, les « contremaîtres électroniques » chargés du contrôle de la présence physique : les badges d'accès.

S'ouvre désormais l'ère du « contremaître virtuel » pouvant tout exploiter sans que le salarié en ait toujours parfaitement conscience et permettant, le cas échéant, au-delà des légitimes contrôles de sécurité et de productivité des salariés, d'établir le profil professionnel, intellectuel ou psychologique du salarié « virtuel ».

Des « chartes d'information » au statut imprécis et au contenu variable

Des entreprises de plus en plus nombreuses adoptent des « chartes d'information » précisant les mesures de sécurité à prendre et les usages que les salariés peuvent faire des nouveaux outils informatiques mis à leur disposition.

La Commission en soutient l'initiative lorsque ces « chartes » ou « guides des bons usages » se fixent pour objectif d'assurer une parfaite information des utilisateurs, de sensibiliser les salariés ou les agents publics aux exigences de sécurité, d'appeler leur attention sur certains comportements de nature à porter atteinte à l'intérêt collectif de l'entreprise ou de l'administration.

Cependant, de telles « chartes », au statut juridique mal défini, peuvent manquer à l'objectif qu'elles s'assignent lorsque, sans souci de pédagogie, elles cumulent les prohibitions de toutes sortes y compris celles des usages généralement et socialement admis de la messagerie et du internet à des fins privées. En outre, dans certains cas, elles permettent mal de distinguer entre ce qui relève des obligations auxquelles est légalement tenu l'employeur de ce qui relève de la négociation collective ou encore du domaine de la discipline. Enfin, sous l'influence sans doute des entreprises américaines, les employeurs soumettent individuellement aux salariés des engagements écrits équivalant à une abdication complète de leurs droits.

Ainsi, certaines des chartes dont la CNIL a eu à connaître prévoient que l'ensemble des données de connexions qui peuvent révéler à l'administrateur du système, ou au chef de service, ou au directeur de personnel, l'usage qui est fait de l'outil (les sites qui ont été consultés, les messages qui ont été adressés) sont conservées pendant des durées très longues et font l'objet d'analyses individualisées.

De la même façon, les salariés se trouvent le plus souvent contraints par ces chartes à n'utiliser le courrier électronique qu'à des fins exclusivement professionnelles, certaines sociétés, notamment des filiales de groupes américains, précisant même que tout message électronique envoyé par un salarié doit être considéré comme un « enregistrement permanent, écrit, pouvant à tout moment être contrôlé et inspecté » (sic).

Cette manière de procéder réalise à coup sûr l'obligation d'information préalable. Mais en se dispensant de la consultation du comité d'entreprise ou des délégués du personnel, elle peut méconnaître les dispositions du code de travail. Enfin, certaines des dispositions qu'elles peuvent parfois comporter ne sont pas opposables au juge auquel revient, en dernière instance, le soin d'exercer le contrôle de proportionnalité au regard du respect de la vie privée consacré par l'article 9 du code civil.

Cependant, les salariés demeurent encore largement ignorants des possibilités de traçage, notamment par accumulation et recoupement de traces multiples, que les nouvelles technologies offrent à l'employeur et, de fait, l'équilibre nécessaire entre contrôle légitime exercé par l'entreprise et respect des droits des salariés ne paraît pas assuré dans bien des cas.

Le rapport d'étude et de consultation publique adopté par la CNIL le 8 mars 2001

Cet état des lieux a conduit la CNIL à entreprendre une étude d'ensemble de ces questions dans le souci de suggérer aux entreprises et aux salariés utilisateurs l'adoption d'une règle du jeu équilibrée, comme les autorités de protection des données l'ont fait lors de l'apparition des précédentes technologies : badges, autocommutateurs, vidéosurveillance, etc.

Après avoir consulté des experts informatiques et tout particulièrement des experts en réseaux, ainsi que les organisations syndicales des salariés (CGT, CFDT, FO, CFTC et CGC) et patronales (MEDEF et CGPME), la CNIL a élaboré un rapport d'étude soumis à consultation publique autour des quatre questions dont elle était le plus fréquemment saisie.

1. En quoi les technologies en réseau seraient-elles d'une nature différente de celle des précédents outils mis en place dans les entreprises ?

2. Quelle est la part de la vie privée et des libertés individuelles garantie aux salariés qui sont liés à l'employeur par un contrat de travail qui est d'abord lien de subordination ?

3. Quel usage à des fins privées d'outils mis à la disposition des salariés par leur employeur est-il admis ?

4. Y a-t-il des limites au contrôle et à la surveillance que les employeurs peuvent exercer sur les salariés ?

Toutes ces questions ne relèvent évidemment pas de la seule compétence de la Commission nationale de l'informatique et des libertés. Mais, imbriquées les unes aux autres, elles constituent naturellement, prises ensemble, un champ de préoccupations communes aux employeurs et aux salariés à l'heure de la société de l'information.

La CNIL a souhaité, dans ce rapport d'étude et de consultation, offrir divers éclairages que son expertise autorisait : aspects techniques, rappel du droit, panorama jurisprudentiel, étude des pratiques comparées et, au titre des questions encore à débattre, quelques recommandations pratiques.

Ce premier rapport qui a notamment été mis en ligne sur le site www.cnil.fr a rencontré un large écho et suscité diverses contributions de la part de groupes professionnels, de représentants syndicaux ou de particuliers. C'est ainsi qu'il a notamment été décidé que les conclusions envisagées pourraient s'appliquer non seulement aux entreprises mais également aux administrations.

Une préoccupation partagée au niveau européen…

Parallèlement aux premières orientations ainsi esquissées par la CNIL, plusieurs de ses homologues européens adoptaient des recommandations en la matière. Tel était notamment le cas des commissaires à la protection des données britannique, belge et néerlandais.

Le groupe européen des commissaires à la protection des données, institué par l'article 29 de la directive du 24 octobre 1995, a notamment adopté, le 29 mai 2002, un avis sur la « surveillance des communications électroniques » sur le lieu de travail[3]. Cet avis, inspiré des travaux de la CNIL, témoigne de la forte convergence de vues entre autorités de protection des données des Etats membres de l'Union européenne.

… mais également au niveau national

La CNIL a pu constater au travers de récentes décisions de justice la recherche, par les juridictions, d'un équilibre entre les intérêts légitimes des employeurs et des employés.

Cette recherche d'équilibre se retrouve dans les décisions rendues en matière de contrôle des messages électroniques et des accès à Internet, d'accès des représentants du personnel et des syndicats aux messageries et espaces Intranet de l'entreprise, ou encore d'accès des employeurs aux données informatiques nécessaires à la poursuite de l'activité de l'organisme en cas d'absence d'un employé gestionnaire de ces données. A cet égard, la CNIL constate avec intérêt que certaines de ces décisions se réfèrent explicitement à ses recommandations[4].

Par ailleurs, le Forum des droits sur l'internet, organisme de réflexion associant des acteurs publics et privés du réseau, a rejoint les positions d'équilibre développées par la CNIL dans son rapport « relations du travail et internet » du 17 septembre 2002[5].

Le suivi des recommandations de la CNIL par les acteurs publics et privés

La CNIL, quotidiennement saisie de questions relatives à la « cybersurveillance », suit avec attention la mise en œuvre de ses recommandations en ce domaine. Ainsi est-elle amenée régulièrement à intervenir pour conseiller, à leur demande, les entreprises et les administrations dans la définition de leur « charte informatique ».

[3] disponible sur www.europa.eu.int/comm/privacy
[4] voir notamment : Cour d'appel de Versailles, 6è chambre sociale, 18 mars 2003, arrêt n°481
[5] disponible sur www.foruminternet.org

Elle a également conduit, au cours des années 2002 et 2003, plusieurs missions de vérification du suivi de ses recommandations en se déplaçant auprès d'entités tant publiques que privées.

***

Sur la base de ce travail d'information, de concertation et de vérifications sur place entrepris depuis 2001, il revient à la CNIL, pour ce qui la concerne, et compte tenu des nombreuses demandes de conseil, plaintes ou demandes de renseignements dont elle est saisie dans le cadre de ses missions, de faire part des éclaircissements et des conclusions qui suivent.

I. Principes généraux et dispositions législatives applicables

. La proportionnalité :

« Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas proportionnées au but recherché ».

Ce principe désormais codifié sous l'article L.120-2 du code du travail a été appliqué tant par les juridictions administratives que par les juridictions judiciaires, à l'occasion notamment des contentieux portant sur la régularité des règlements intérieurs. Les juridictions exercent un contrôle a posteriori des restrictions que l'employeur peut légalement apporter aux droits des personnes et aux libertés individuelles, la jurisprudence dessinant ainsi les contours d'une part sans doute résiduelle mais irréductible de liberté personnelle et de vie privée sur le lieu du travail.

« Le salarié a droit, même au temps et au lieu de travail, au respect de sa vie privée ; celle-ci implique en particulier le secret de ses correspondances ; l'employeur ne peut dès lors, sans violation de cette liberté fondamentale, prendre connaissance des messages personnels émis par le salarié ou reçus par lui grâce à un outil informatique mis à sa disposition pour son travail, et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur. » C'est ce qu'a affirmé la Chambre sociale de la Cour de cassation dans un arrêt du 2 octobre 2001.

Le principe de protection de l'intimité de la vie privée du salarié sur son lieu de travail n'est pas nouveau et a été affirmé à des nombreuses reprises, notamment par la Cour européenne des droits de l'Homme qui a fait application de l'article 8 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales (« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ») dans les domaines relevant de la vie professionnelle[6].

Ce principe est cependant d'une application plus délicate à l'heure des nouvelles technologies. En effet, le phénomène de convergence ne permet plus de distinguer nettement ce qui relèverait de la vie professionnelle et ce qui ressortirait à l'intimité de la vie privée : le disque dur de l'ordinateur est également « bavard » dans un domaine que dans l'autre ; le message électronique envoyé ou reçu dans les mêmes conditions techniques qu'il soit d'ordre professionnel ou personnel ; la consultation de sites internet s'opère à l'identique quelle que soit la nature du site et le motif de la connexion.

Par nature, l'ordinateur peut enregistrer tout ce qui a été fait sur la machine, sa capacité de mémoire constituant un élément essentiel de ses performances. Il constitue une véritable « boîte noire » des activités numériques de l'utilisateur (textes, images, messages envoyés et reçus, mémoire cache enregistrant les pages internet consultées afin d'optimiser le temps de chargement et d'éviter l'engorgement du réseau…).

[6] affaires N. c/Allemagne du 23 novembre 1992 et H. c/Royaume-Uni du 27 mai 1997

De manière plus générale, qu'il s'agisse d'assurer le bon fonctionnement du service informatique, la sécurité numérique de l'entreprise ou le confort de l'usager, ces « traces » sont intrinsèquement liées à la mise à disposition d'une telle technologie. Aussi n'est-ce pas leur existence mais leur traitement à des fins autres que techniques qui doit être proportionné au but recherché.

. L'information préalable, condition de la transparence :

L'obligation d'information préalable résulte de l'article L.121-8 du code du travail (« *Aucune information concernant personnellement un salarié ou un candidat à un emploi ne peut être collectée par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié ou du candidat à l'emploi »).*

L'obligation de transparence inspire la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés qui soumet tout traitement automatisé d'informations nominatives à déclaration préalable auprès de la CNIL, interdit que les données soient collectées par un moyen frauduleux, déloyal ou illicite et impose une obligation d'information des personnes concernées notamment sur les destinataires des données et le lieu où s'exerce le droit d'accès et de rectification.

Qu'elle résulte des dispositions du code du travail ou de la loi du 6 janvier 1978, l'information préalable, condition de la loyauté de la collecte des données, est donc une condition nécessaire. Elle n'est pas suffisante.

. La discussion collective :

L'article L.432-2 du code du travail dispose que « *le comité d'entreprise est informé et consulté préalablement à tout projet important d'introduction de nouvelles technologies, lorsque celles-ci sont susceptibles d'avoir des conséquences sur [...] les conditions de travail du personnel »* et précise que *« lorsque l'employeur envisage de mettre en oeuvre des mutations technologiques importantes et rapides »* le plan d'adaptation doit être transmis *« pour information et consultation »* au comité d'entreprise, lequel doit être « *régulièrement informé et périodiquement consulté »* sur la mise en oeuvre de ce plan.

Par ailleurs, l'article L.432-2-1 prescrit que le comité d'entreprise doit être *« informé et consulté, préalablement à la décision de mise en oeuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés ».*

Les textes applicables aux trois fonctions publiques[7] prévoient pour leur part que les comités techniques paritaires *« connaissent [...] des questions et des projets de textes relatifs »*, notamment *« aux programmes de modernisation des méthodes et techniques du travail et à leur incidence sur la situation du personnel ».*

[7] articles 15 de la loi n°84-16 du 11 janvier 1984 et 12 du décret n°82-452 du 28 mai 1982 (fonction publique de l'Etat), article 33 de la loi n°84-53 du 26 janvier 1984 (fonction publique territoriale), article 24 de la loi n°86-33 du 9 janvier 1986 (fonction publique hospitalière)

Il résulte clairement de ces textes qu'une information individuelle des salariés ou agents publics ne saurait dispenser les responsables concernés de l'étape de la discussion collective, institutionnellement organisée, avec les représentants élus du personnel.

Compte tenu de ces textes, la CNIL vérifie, lorsqu'elle est saisie d'une demande d'avis ou d'une déclaration relative à un traitement automatisé d'informations nominatives mis en oeuvre à des fins de contrôle, que ces consultations ont été effectuées préalablement à sa saisine, condition de régularité du projet de traitement déclaré à la Commission.

II. Privilégier la discussion collective et la pédagogie

Compte tenu du caractère évolutif des techniques et de la jurisprudence qui se dégage sur ces sujets, il convient de former les organisations et les utilisateurs sur les mesures de sécurité, de consultation ou d'information à prendre. De nombreuses entreprises ou administrations le font déjà. Il y a lieu cependant de lutter contre deux idées fausses.

. Première idée fausse : l'ordinateur personnel mis à la disposition des utilisateurs sur leur lieu de travail serait, en tant que tel, protégé par la loi « informatique et libertés » et relèverait de la vie privée du salarié

Il n'en est rien. Un ordinateur mis à la disposition d'un salarié ou d'un agent public dans le cadre de la relation de travail est la propriété de l'entreprise ou de l'administration et ne peut comporter que subsidiairement des informations relevant de l'intimité de la vie privée.

Il peut être protégé par un mot de passe et un login, mais cette mesure de sécurité est destinée à éviter les utilisations malveillantes ou abusives par un tiers ; elle n'a pas pour objet de transformer l'ordinateur de l'entreprise en un ordinateur à usage privé.

Aussi les impératifs de l'entreprise et le nécessaire respect de la vie privée des salariés doivent-ils être conciliés, grâce à la discussion collective et à la formation des utilisateurs à la sécurité informatique.

. Deuxième idée fausse : une information préalable des personnels suffirait

De nombreuses entreprises imaginent qu'une information préalable des salariés suffirait à se prémunir de tout problème et à autoriser l'emploi de tous les modes de surveillance et de contrôle. Dans le souci de se garantir contre tout aléa, elles peuvent quelque fois être tentées de déclarer à la CNIL leur schéma de sécurité d'ensemble.

Une telle manière de procéder n'est pas suffisante dès lors que les finalités seraient mal définies ou mal comprises.

Elle peut nourrir, à tort, le sentiment des utilisateurs qu'ils se trouveraient sous un contrôle constant de l'organisation alors que les mesures prises, dans bien des cas, se bornent à assurer la sécurité du système ou celles des applications et non pas un contrôle individuel ou nominatif de leur activité.

Elle peut conforter l'entreprise ou l'administration dans l'idée qu'une déclaration à la CNIL de l'ensemble de son système de sécurité l'autoriserait à porter des atteintes à ce que commande le respect de l'intimité de la vie privée et de la liberté personnelle résiduelle du salarié sur son lieu de travail, alors qu'il appartient, en dernière instance, aux juridictions administratives ou judiciaires d'en apprécier la régularité et, compte tenu des circonstances de fait ou de droit de l'espèce, la proportionnalité.

III. Conclusions

A. Un équilibre doit être recherché dans la mise en œuvre des dispositifs de « cybersurveillance »

1. Le contrôle de l'usage d'internet

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.

A ce titre, la mise en place de dispositifs de filtrage de sites non autorisés, associés au pare-feu (sites diffusant des produits à caractère pornographiques, pédophiles, incitation à la haine raciale, révisionnistes, etc.) 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.

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.

2. Le contrôle de l'usage de la messagerie

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[8]. 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[9].

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".

[8] Cour d'appel de Toulouse, 4è chambre sociale, 6 février 2003 (affaire n°02-02519)
[9] Cour d'appel de Versailles, 2 avril 2003 (affaire n°02-00293)

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. 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.

3. Le rôle des administrateurs informatiques

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. point 5 : *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[10] 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.

[10] Dans un arrêt du 17 décembre 2001, la Cour d'appel de Paris a ainsi relevé que, de manière générale, « la préoccupation de la sécurité du réseau justifie que les administrateurs fassent usage de leur position et des possibilités techniques dont ils disposaient pour mener les investigations et prendre les mesures que cette sécurité imposait », mais elle a considéré dans cette affaire que « la divulgation du contenu des messages, et notamment du dernier qui concernait le conflit latent dont le laboratoire était le cadre, ne relevait pas de ces objectifs » (affaire n°00-07565)

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. Au-delà de cette mention, il serait certainement très utile qu'une réflexion soit engagée sur la reconnaissance d'un secret professionnel attaché à cette fonction particulière.

4. L'utilisation des technologies de l'information et de la communication par les instances représentatives du personnel et les syndicats

Les entreprises et administrations devraient négocier les conditions dans lesquelles la messagerie de l'entreprise et les adresses électroniques des employés peuvent être utilisées par les instances représentatives du personnel ou pour l'exercice d'un mandat syndical. L'article L.412-8 du code du travail devrait être prochainement modifié en ce sens[11].

Cette négociation devrait en particulier aborder les modalités selon lesquelles des employés peuvent s'opposer à recevoir des messages électroniques émanant des instances représentatives du personnel ou des syndicats, et définir les mesures de sécurité propres à garantir la confidentialité des échanges.

5. 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 ».

[11] article 52 du projet de loi relatif à la formation professionnelle tout au long de la vie et au dialogue social, voté dans les mêmes termes par l'Assemblée nationale et le Sénat : « 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. »

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.

6. Les fichiers de journalisation

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 déclaré 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 6 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[12].

7. Accès aux données informatiques en cas d'absence d'un employé

L'obligation de loyauté impose à l'employé absent de son poste de travail en raison d'un congé ou d'un « arrêt maladie » à communiquer à l'employeur qui en fait la demande tout document nécessaire à la poursuite de l'activité de l'entreprise[13].

Récemment appliquée dans le domaine des technologies de l'information et de la communication, cette jurisprudence impose au salarié de communiquer son mot de passe ou les fichiers en sa possession lorsque le bon fonctionnement de son entreprise dépend des données détenues par cet employé[14].

C'est pourquoi les modalités d'accès de l'employeur aux données stockées sur l'environnement informatique d'un employé absent (messagerie, fichiers, supports de stockage) devraient être préalablement définies en concertation et diffusées auprès de l'ensemble des employés susceptibles d'être concernés.

Il importe notamment que ces modalités prévoient qu'un tel accès ne pourra avoir lieu que dans le cas où il s'avèrerait nécessaire à la poursuite de l'activité de l'organisme public ou privé, et que l'employé concerné sera informé de cet accès réalisé en son absence.

Enfin, compte tenu des termes de l'arrêt de la Cour de cassation du 2 octobre 2001 reconnaissant à l'employé un droit au respect de sa vie privée au temps et lieu de travail, il importe également que cet accès soit réalisé dans des conditions propres à garantir ce droit, et notamment le respect du secret des correspondances électroniques.

[12] Cour de cassation, chambre sociale, arrêt n° 98-43.485 du 18 juillet 2000
[13] Voir notamment : Cour de cassation, chambre sociale, 6 février 2001 (n°98-46345)
[14] Voir notamment : Cour de cassation, chambre sociale, 18 mars 2003 (n°01-41343)

B. Trois propositions pour une meilleure prise en compte des principes « informatique et libertés » sur les lieux de travail

1. La réalisation d'un bilan annuel « informatique et libertés »

Les mesures de sécurité qui conduisent à conserver trace de l'activité des utilisateurs ou de l'usage qu'ils font des technologies de l'information et de la communication ou qui reposent sur la mise en oeuvre de traitements automatisés d'informations directement ou indirectement nominatives devraient faire l'objet d'un bilan annuel « informatique et libertés » à l'occasion de la discussion du bilan social soumis au comité d'entreprise ou au comité technique paritaire ou à toute autre instance équivalente.

2. La désignation d'un délégué à la protection des données

Les entreprises ou les administrations pourraient désigner, dès lors que leurs effectifs et leur mode d'organisation le justifieraient et le leur permettraient, en concertation avec les instances représentatives du personnel, un « délégué à la protection des données et à l'usage des nouvelles technologies dans l'entreprise ».

Ce délégué pourrait être plus particulièrement chargé des questions relevant des mesures de sécurité, du droit d'accès et de la protection des données personnelles sur le lieu de travail.

Interlocuteur des responsables de l'entreprise ou de l'administration ainsi que des instances représentatives du personnel et des salariés ou agents publics, ce délégué pourrait devenir un « correspondant informatique et libertés » dans l'entreprise ou l'administration sur ces questions, fonction qui devrait bientôt faire l'objet d'une définition légale dans le cadre de la réforme de la loi « informatique et libertés » en cours d'examen par le Parlement[15].

3. Le renforcement de la formation des employeurs et des employés

Les entreprises ou les administrations, ainsi que les organisations syndicales d'employeurs et d'employés, pourraient encourager les formations liées aux nouvelles technologies et à la protection des données personnelles au bénéfice de l'ensemble des salariés et des agents publics dans le cadre des droits à formation prévus par le code du travail[16] et les textes relatifs à la fonction publique[17].

[15] article 22 du projet de loi adopté par le Sénat le 1er avril 2003
[16] article L.451-1 et suivants, article L.931-1 et suivants du code du travail
[17] notamment : articles 21 et 22 de la loi n°83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires