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 dans sa séance du 5 février 2002

Rédacteurs : Mme Sandrine MATHON, attachée à la direction juridique
M. Jean-Paul MACKER, chargé de mission à la direction de l'expertise informatique

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*" - art L 120-2 du code du travail) ; consultation du comité d'entreprise lors de l'introduction de nouvelles technologies (art L 432-2 du code du travail) ; information préalable des salariés sur tout dispositif de collecte de données le concernant personnellement (art 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.

Sans doute, le développement des écoutes téléphoniques dans le milieu du travail a-t-il signé un

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

[2] *cf. 5 ème rapport d'activité de la CNIL, 15 ème rapport d'activité, p 74.*

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 réseau, 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 de nature différente que les 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 d'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, accessibles depuis le site de la CNIL. 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.

A ce jour, le groupe européen des commissaires à la protection des données, institué par l'article 29 de la directive du 24 octobre 1995, a inscrit ce thème dans son programme de travail et rendra public un avis qui devrait témoigner de la forte convergence de vues entre autorités de protection des données des Etats membres de l'Union européenne.

*

A l'issue de ce premier travail d'approfondissement et de consultation, il revenait 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

. 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".*

Le décret du 28 mai 1982 relatif aux comités techniques paritaires des trois fonctions publiques prévoit pour sa part que ces comités *"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".*

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 mises 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.

. 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 récemment 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 - affaire N. c/Allemagne du 23 novembre 1992 et H. C/Royaume-Uni du 27 mai 1997.

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…).

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.

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.

PARTIE III : CONCLUSIONS

1. Le contrôle des connexions à 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. Un usage raisonnable, non susceptible d'amoindrir les conditions d'accès professionnel au réseau ne mettant pas en cause la productivité paraît 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'entreprise, 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, de façon globale, par service ou par utilisateur ou un contrôle statistique des sites les plus visités devrait dans la plupart des cas être suffisant sans qu'il soit nécessaire de procéder à un contrôle nominatif individualisé des sites accédés.

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

Lorsque l'entreprise ou l'administration met en place un dispositif de contrôle individuel poste par poste du fonctionnement de la messagerie, le traitement automatisé d'informations nominatives ainsi mis en œuvre doit être déclaré à la CNIL. 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. 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. Il 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 lorsqu'ils sont associés à un traitement automatisé d'informations nominatives n'ont pas, en tant que tels, à faire l'objet des formalités préalables auprès de la CNIL.

Afin de garantir ou de renforcer l'obligation de sécurité, 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 destiné à contrôler l'activité des utilisateurs, doit être déclarée à la CNIL.

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

Une durée de conservation de l'ordre de 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 (Cour de cassation – chambre sociale n° 98-43.485 du 18 juillet 2000).

4. Le rôle des administrateurs de réseaux

Les administrateurs qui doivent veiller à assurer le fonctionnement normal et la sécurité des réseaux et systèmes sont conduits par leurs fonctions même à avoir accès à l'ensemble des informations relatives aux utilisateurs (messagerie, connexions au 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 encadrée de logiciels de télémaintenance qui permettent de détecter et réparer les pannes à distance ou à 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 les mesures de sécurité nécessaires à la protection des données soient mises en œuvre.

Toutefois, 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, tenus au secret professionnel, 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.

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

Les entreprises et administrations devraient négocier les conditions dans lesquelles la messagerie de l'entreprise peut être utilisée par les instances représentatives du personnel ou pour l'exercice d'un mandat syndical.

Lorsque les instances représentatives du personnel disposent d'un compte de messagerie dédié, des mesures de sécurité particulières devraient être définies ou mises en œuvre afin d'assurer la confidentialité des informations échangées.

Les modalités d'utilisation des technologies de l'information et de la communication de l'entreprise par les représentants syndicaux pour exercer leur mandat devraient également être précisées.

6. 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.

7. 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
sur ces questions.

Afin de servir d'outil pédagogique, la Commission souhaite annexer au présent rapport les réponses aux questions qui lui sont le plus fréquemment posées.

Annexe au rapport

Ce document a vocation à fournir des réponses aux questions les plus fréquemment posées à la CNIL sur l'équilibre du contrôle par l'employeur de l'usage des technologies de l'information et de la communication. Il ne constitue pas un modèle de charte de sécurité des ressources informatiques qu'il appartient aux administrations et entreprises de déterminer librement en fonction des exigences de sécurité qui leurs sont propres.

Les règles d'utilisation d'internet

Il appartient au responsable de l'organisation de déterminer les règles d'usage d'internet.

> *Proposition de rédaction* :
>
> *"Seuls ont vocation à être consultés les sites internet présentant un lien direct et nécessaire avec l'activité professionnelle, sous réserve que la durée de connexion n'excède pas un délai raisonnable et présente une utilité au regard des fonctions exercées ou des missions à mener.*
>
> *"Une consultation ponctuelle et dans des limites raisonnables du web, pour un motif personnel, des sites internet dont le contenu n'est pas contraire à l'ordre public et aux bonnes mœurs et ne mettant pas en cause l'intérêt et la réputation de l'organisation est tolérée".*

Lorsqu'un mécanisme de filtrage de certains sites à contenu particulier ou illégal (pornographie, pédophilie, racisme, incitation à la haine raciale, révisionnisme, …) est mis en place, il doit être portée à la connaissance des utilisateurs.

L'entreprise ou l'administration peut poser d'autres conditions d'usage d'internet parmi lesquelles les plus fréquentes sont : l'interdiction de développer son propre site internet, l'accès à des sites de jeux, la connexion à internet via un modem, la participation à des conversations en ligne, la participation à des forum (y compris professionnels), la diffusion d'informations concernant l'entreprise, etc. Ces conditions d'usage doivent être portées à la connaissances des utilisateurs.

Des modalités de contrôle de l'usage d'internet par les utilisateurs peuvent être mises en place. Les contrôles les plus usuels peuvent consister à établir les statistiques relatives aux durées de connexion de façon globale ou service par service. Un autre mode de contrôle peut consister à recenser les sites les plus visités dans l'entreprise ou l'administration.

Les dispositions législatives et réglementaires prévoient que le comité d'entreprise ou le comité technique paritaire ou toute instance équivalente doit être informé et consulté préalablement sur les règles d'usage et les modalités de contrôle. Ces règles d'usage et modalités de contrôle, une fois arrêtées, doivent être portées à la connaissance du salarié ou l'agent public.

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. Le dossier de déclaration doit en outre comporter l'indication et la date à laquelle les instances représentatives du personnel ont été consultées sur de tels dispositifs.

Les règles d'utilisation de la messagerie

Il appartient au responsable de l'organisation de déterminer les règles d'usage de la messagerie.

> *Proposition de rédaction* :
>
> *"Un usage raisonnable dans le cadre des nécessités de la vie courante et familiale est toléré, à condition que l'utilisation du courrier électronique n'affecte pas le trafic normal des messages professionnels."*

Des exigences de sécurité particulières peuvent conduire l'entreprise ou l'administration à mettre en place un dispositif d'analyse des messages au regard d'une liste de "mots clés". Dans cette hypothèse particulière, le risque de détournement du dispositif peut légitimement conduire l'entreprise à ne pas révéler les "mots clés" aux utilisateurs.

L'entreprise ou l'administration peut mettre en place, dans un souci de sécurité de l'organisation ou de contrôle de l'encombrement du réseau un dispositif de limitation du volume ou de la taille des messages échangés ou du type des pièces jointes.

Ces mêmes exigences de sécurité juridique ou technique peuvent également conduire l'entreprise ou l'administration à conserver une copie de sauvegarde des messages échangés. Dans cette hypothèse, les utilisateurs doivent être informés que les messages qu'ils ont reçus ou envoyés seront conservés sur le dispositif de sauvegarde, y compris dans le cas où l'utilisateur les aurait supprimés de son poste de travail. La durée pendant laquelle les messages seront conservés dans le dispositif de sauvegarde doit être précisée.

L'entreprise ou l'administration peut établir d'autres prescriptions. Elle doit en informer les utilisateurs. Tel doit notamment être le cas lorsque l'usage, depuis l'entreprise, des services d'un site web spécialisé messagerie est interdit par l'organisation.

Selon la Chambre sociale de la Cour de cassation 2 octobre 2001 :
"Le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; que celle-ci implique en particulier le secret des correspondances ; que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et 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."

Il doit être généralement considéré qu'un message envoyé ou reçu depuis le poste de travail mis à la disposition par l'entreprise ou l'administration revêt un caractère professionnel. Il ne peut en être autrement qu'en cas d'indication manifeste dans l'objet du message de son caractère personnel ou dans l'hypothèse d'un archivage dans un répertoire clairement identifié comme étant personnel.

Compte tenu des termes de l'arrêt de la Chambre sociale de la Cour de cassation, il convient de considérer que les administrateurs de réseaux et systèmes qui sont conduits par leurs fonctions à avoir accès à l'ensemble des informations relatives aux utilisateurs, y compris celle enregistrées sur

le disque dur du poste de travail, ne sauraient être contraints de divulguer des informations qu'ils auraient été amenés à connaître dans le cadre de leurs fonctions lorsque ces dernières 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 la sécurité, ni les intérêts de l'entreprise.

La CNIL estime que les modalités de contrôles de l'usage d'une messagerie d'entreprise ne relèvent pas, en tant que telles, des dispositions de la loi du 6 janvier 1978, dés lors qu'il ne s'agit pas d'un contrôle individuel poste par poste. Elles doivent en revanche être soumises aux instances représentatives du personnel et faire l'objet, une fois l'avis de ces instances recueilli, d'une information auprès des utilisateurs.

Les fichiers de journalisation et les pare-feu

Un système de journalisation est destiné à assurer la sécurité et le bon fonctionnement d'un système ou d'une application informatique. Il n'a pas pour vocation première le contrôle des utilisateurs.

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

Le pare-feu assure la protection de l'entreprise à l'égard des intrusions ou attaques informatiques. Il vérifie à cette fin tout le trafic entrant et sortant de l'entreprise, aussi bien local que distant.

Il n'a pas pour objet de réaliser une surveillance de l'activité des salariés ou agents publics mais doit permettre, en cas d'attaques informatiques, d'en identifier l'origine et d'en prévenir les effets.

En tant que tels, les serveurs (proxys, cache,…) qui permettent d'optimiser le temps de connexion en mémorisant les pages web consultées, ainsi que les serveurs ayant la fonction de pare-feu (fire wall), destinés à protéger les applications informatiques de l'entreprise des attaques extérieures, n'ont pas à faire l'objet de formalités préalables auprès de la CNIL. Ils doivent faire l'objet d'une information des utilisateurs.

Seuls les administrateurs ont accès aux informations enregistrées. Aucune exploitation à des fins autres que celles liées au bon fonctionnement et à la sécurité des systèmes d'informations n'est opérée.

Pour la CNIL, un fichier de journalisation n'a pas à être déclaré à la CNIL de façon autonome lorsqu'il est associé à un traitement automatisé d'informations nominatives dont il a pour fonction d'assurer la sécurité. Il doit en être fait mention dans le dossier de déclaration du traitement principal dont il constitue 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 destinée à contrôler l'activité des utilisateurs doit faire l'objet des formalités préalables auprès de la CNIL.

La durée pendant laquelle les données de connexion sont conservées doit être précisée. La CNIL estime qu'une durée de l'ordre de six mois n'est pas excessive.

Bilan annuel "informatique et libertés"

La CNIL suggère qu'un bilan "informatique et libertés" soit présenté au comité d'entreprise ou au comité technique paritaire à l'occasion de la discussion du bilan social. Ce bilan inclurait les principes et mesures de sécurité qui conduisent à conserver traces de l'activité des utilisateurs ou de l'usage qu'ils font des technologies de l'information et de la communication.

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 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 en charge 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 sur ces questions, ce délégué pourrait devenir un « correspondant informatique et libertés » dans l'entreprise.