LA CYBERSURVEILLANCE SUR LES LIEUX DE TRAVAIL

RAPPORT PRESENTE PAR

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

PARTIE III : CONCLUSIONS

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

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 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 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.