CYBER SURVEILLANCE SUR LES LIEUX DE TRAVAIL

11 / 02 / 2002

Fiches de synthèse

LA CYBERSURVEILLANCE SUR LES LIEUX DE TRAVAIL

Conclusions du rapport présenté par M. Hubert BOUCHET, vice-président délégué de la CNIL et adopté par la CNIL LE 5 février 2002

Le contrôle des connexions à Internet

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.

Les conditions d'usage peuvent être fixées par l'employeur et ne constituent pas, en soi, des atteintes à la vie privée des salariés ou agents publics.

Dispositifs de filtrage de sites non autorisés

Associés au pare-feu (contre les sites diffusant des produits à caractère pornographiques, pédophiles, incitation à la haine raciale, révisionnistes etc), ces dispositifs peuvent constituer une mesure de prévention dont il y a lieu d'informer les salariés ou agents publics.

Des prescriptions légitimes dictées par l'exigence de sécurité de l'entreprise

Des prescriptions, telles que l'interdiction de télécharger des logiciels, de se connecter à un forum ou d'utiliser le "chat"? , d'accéder à une boîte aux lettres personnelle par internet compte-tenu des risques de virus qu'un tel accès peut présenter, peuvent accompagner la possibilité offerte aux salariés ou agents publics de se connecter à Internet à des fins autres que professionnelles.

Contrôle a posteriori des données de connexion à Internet

Un tel contrôle, 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.*

Propositions 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. »

LA CYBERSURVEILLANCE SUR LES LIEUX DE TRAVAIL

Conclusions du rapport présenté par M. Hubert BOUCHET, vice-président délégué de la CNIL et adopté par la CNIL LE 5 février 2002

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.

> *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.

Les outils de contrôle

L'emploi d'outils de contrôle ou de sauvegarde doit être porté à la connaissance des salariés ainsi que la durée de conservation du message "sauvegardé".

Des exigences de sécurité, de prévention ou de contrôle de l'encombrement du réseau peuvent conduire 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.

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.

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

LA CYBERSURVEILLANCE SUR LES LIEUX DE TRAVAIL

Conclusions du rapport présenté par M. Hubert BOUCHET, vice-président délégué de la CNIL et adopté par la CNIL LE 5 février 2002

Les fichiers de journalisation

Les fichiers de journalisation des connexions permettent d'identifier et d'enregistrer toutes les connexions ou tentatives de connexion à un système automatisé d'informations.

Il n'ont pas pour vocation première le contrôle des utilisateurs.
Ils ont pour finalité de garantir une utilisation normale des ressources des systèmes d'information mais ils peuvent être associés à des traitements d'information qui revêtent un caractère sensible pour l'entreprise ou l'administration concernée.

Ils constituent une mesure de sécurité généralement préconisée par la CNIL.

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 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).*

En tant que tels, lorsqu'ils sont associés à un traitement automatisé d'informations nominative, ces fichiers de journalisation (proxis, caches, fire wall, …) n'ont pas à faire l'objet de déclaration auprès de la CNIL.

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, en revanche, doit être déclaré à la CNIL.

LA CYBERSURVEILLANCE SUR LES LIEUX DE TRAVAIL

Conclusions du rapport présenté par M. Hubert BOUCHET, vice-président délégué de la CNIL et adopté par la CNIL LE 5 février 2002

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.

"Prise de main à distance"

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 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.

Secret professionnel

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.

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

LA CYBERSURVEILLANCE SUR LES LIEUX DE TRAVAIL

Conclusions du rapport présenté par M. Hubert BOUCHET, vice-président délégué de la CNIL et adopté par la CNIL LE 5 février 2002

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.

LA CYBERSURVEILLANCE SUR LES LIEUX DE TRAVAIL

Conclusions du rapport présenté par M. Hubert BOUCHET, vice-président délégué de la CNIL et adopté par la CNIL LE 5 février 2002

Un bilan annuel "informatique et libertés"

Un bilan annuel "informatique et libertés" élaboré et présenté 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.

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 de ce bilan.

Désignation d'un délégué à la protection des données

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

> *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.*