Élu meilleur site internet de magazine 2008
L'Expansion.com
Le décryptage instantané de l'économie

Chronique juridique

Contrôler sans espionner ses collaborateurs

Laëtitia Boncourt, avocate, cabinet Alain Bensoussan - 10/06/2008 15:02 - L'Expansion.com

EN PLUS

- Les risques du pot au bureau
- Licenciement : savoir négocier sa transaction
- Préparer son kit départ pour l'étranger
- Comment débloquer sa participation ?
- Comment monétiser ses RTT ?

Quels sont les outils dont je dispose pour contrôler mes collaborateurs ?

Les nouvelles technologies vous permettent de surveiller l'activité de vos salariés. Par exemple, les autocommutateurs qui servent à vérifier la durée et le coût des appels par poste permettent indirectement de quantifier la productivité de vos salariés. De même, les systèmes de badge qui sont utilisés pour contrôler l'accès aux locaux, permettent en même temps de savoir à quelle heure le salarié arrive au travail, à quelle heure il en part et quels sont ses mouvements dans la journée. Grâce à la géolocalisation, vous pouvez repérer le véhicule de dépannage le plus proche d'une demande client, mais également surveiller les déplacements de vos salariés itinérants. Enfin, les journaux de connexion permettent de "tracer" les connexions à internet et d'identifier quels sont les sites consultés, par qui, et pendant combien de temps.

Comment éviter que mes collaborateurs ne se sentent espionnés ?

D'un côté, le principe est que vous ne pouvez pas totalement interdire l'usage privé des outils informatiques que vous mettez à disposition de vos salariés dans le cadre de leur activité professionnelle. Par exemple, vous ne pouvez pas empêcher vos collaborateurs d'utiliser leur messagerie électronique professionnelle pour transmettre, de façon épisodique, quelques mails, d'un format usuel, à des amis ou de la famille.

De l'autre côté, certains comportements de vos salariés peuvent mettre en danger la sécurité de votre réseau informatique (par exemple, intrusion de virus à partir de fichiers personnels) ou encore risquent d'engager votre responsabilité (par exemple, propos racistes tenus sur un blog pendant le temps de travail, à l'aide de l'ordinateur que vous mettez à disposition du salarié, auteur des propos). Vous avez donc le droit –et même le devoir !- de surveiller ce que font vos salariés à l'aide des outils informatiques que vous leur fournissez.

L'enjeu est d'effectuer les contrôles dans le cadre de la « cyberconfiance », c'est-à-dire en toute transparence, de façon objective (quand des indices vous font penser qu'un problème se pose) et proportionnée. Vous devez donc prévenir, avant de les mettre en place, vos collaborateurs, individuellement, et les représentants du personnel, sur le plan collectif, de l'existence de tel ou tel dispositif que vous allez installer pour surveiller leur activité. Il faut aussi que vos contrôles ne soient pas abusifs, vous devez respecter une certaine proportionnalité entre la mesure de contrôle et le but poursuivi.

Quelles sont mes obligations ?

Avant d'introduire des dispositifs de contrôle d'activité, vous devez avoir mené une réflexion avec les représentants du personnel. En outre, vous devez avoir informé chacun de vos salariés. Enfin, dans le cadre des contrôles que vous ferez en votre qualité de manager, vous pouvez avoir l'occasion de prendre connaissance de données à caractère personnel. Il s'agit de traitement automatisé portant sur des données qui permettent d'identifier la personne du salarié qui a été surveillé. Vous devez donc accomplir des formalités auprès de la Commission

nationale de l'informatique et des libertés (Cnil).

Quelles sont mes risques en cas d'abus ?

Si vous ne respectez pas les règles imposées pour mettre en place des dispositifs de surveillance, vous ne pourrez pas vous servir des preuves recueillies à partir de ces dispositifs. Donc vous ne pourrez pas vous référez à ces preuves pour licencier un salarié pris en faute grâce à ce dispositif. En effet, si le salarié en question vous attaquait en justice prétendant qu'il ne savait pas qu'il était surveillé, il obtiendrait que les preuves ne soient pas examinées par les tribunaux. Or, faute de telles preuves, le licenciement serait abusif et vous devriez indemniser votre collaborateur. En outre, vous ne pourriez plus utiliser le dispositif jusqu'à ce que vous ayez complètement régularisé vos obligations.

Quelle est la parade juridique pour instaurer un contrôle objectif ?

Vous pouvez fixer des règles de contrôle, définir en quelque sorte les "règles du jeu" concernant l'utilisation des outils informatiques, dans une charte d'utilisation des systèmes d'information. Ce document peut prévoir des sanctions contre vos salariés qui ne le respecteraient pas, au même titre que le règlement intérieur. Il ne s'agit pas de tout interdire mais d'expliquer aux salariés qui, par exemple, reçoivent des fichiers personnels lourds (en raison du format) qu'ils mettent en danger la sécurité du réseau informatique. La charte a pour but d'éviter les abus, de les identifier et de prévenir le salarié qu'il pourra être sanctionné s'il ne respecte pas les règles d'utilisation.

SALAIRES

Calculez ce que vous devriez gagner
et estimez votre augmentation 2008 avec notre simulateur exclusif

JEUNES DIPLÔMÉS

Palmarès des écoles
Les salaires d'embauche école par école et nos conseils pour votre premier job

BIEN-ÊTRE

Luttez contre le stress
Tests, conseils et vidéos pour retrouver la sérénité au bureau

HIGH-TECH

Tout savoir sur la nouvelle économie
Les start-ups, les produits, les enjeux des nouvelles technologies