Cybersurveillance des salariés : ce qu'il faut savoir

© 2013 Les Echos Publishing

L'utilisation d'internet par les salariés : quels risques pour les employeurs ?

Virus, fichier indésirable, diffamation, injure, perte de productivité… les risques induits par la navigation non maîtrisée sur internet sont potentiellement nombreux.

La navigation sur internet par les salariés peut faire peser sur le fonctionnement de l'entreprise des risques de nature technique, juridique, mais aussi économique.

Risques techniques

Premier danger : l'exposition à des virus ou à des fichiers indésirables susceptibles d'endommager les postes de travail de l'entreprise et le réseau qui leur est, éventuellement, associé. Bien sûr, ce risque n'est pas spécifique à l'usage privé d'internet par les salariés, mais cette utilisation est incontestablement un facteur susceptible de l'aggraver.

Pour y remédier, l'employeur doit alors généralement faire appel à des outils de contrôle des messageries électroniques et des connexions internet. Grâce à ces outils, un administrateur réseau ou, plus généralement, un informaticien doit pouvoir prendre connaissance des données de connexion et identifier les situations potentiellement dangereuses nécessitant une politique de sécurité particulière (logiciels « pare-feu », anti-virus, filtrage de sites non autorisés, etc.).

Risques juridiques

L'utilisation à titre personnel des moyens informatiques de l'entreprise peut également avoir des répercussions juridiques sur l'employeur. Ainsi, en créant ou en alimentant un blog ou un site Internet, en participant à un réseau social ou un forum de discussion, un salarié peut éventuellement injurier ou diffamer des individus enclins, en retour, à assigner son employeur en justice.

En effet, le Code civil (article 1384, alinéa 5) prévoit que les commettants peuvent être reconnus responsables du dommage causé par leurs préposés dans l'exercice de leurs fonctions.

Une règle que la Cour de cassation interprète d'ailleurs de manière extensive considérant que, dès lors qu'un employeur fournit à un salarié les moyens de commettre un dommage, ce dernier est réputé avoir agi dans l'exercice de ses fonctions (Cassation civile 2e ch., 19 juin 2003, n° 00-22626).

La mise en cause d'un employeur par le biais des activités internet de ses salariés, même à des fins privées, est donc tout à fait envisageable, comme le prouve un arrêt de la Cour d'appel d'Aix-en-Provence du 13 mars 2006. Par cette décision, les magistrats ont en effet retenu la responsabilité civile d'une société de télécommunication vis-à-vis d'une entreprise autoroutière en raison des critiques injurieuses proférées sur

internet par un de ses salariés.

Risques économiques

Avec la généralisation de l'accès haut débit à Internet, difficile de nier que les salariés peuvent s'adonner à un nombre d'activités personnelles nettement plus diverses et intéressantes que lorsqu'elles ne disposaient encore seulement que d'un téléphone et d'un minitel. Toutefois, peut-on réellement affirmer que la productivité gagnée par l'usage professionnel des Nouvelles technologies de l'information et de la communication (NTIC) se réduit à mesure que les salariés peuvent utiliser internet à des fins privées ? Difficile à établir avec certitude. Pour l'heure, notons que rares sont les entreprises qui interdisent tout usage personnel d'internet à leurs salariés, autrement que pour des raisons de sécurité (interdiction concernant certains personnels de grandes banques, par exemple).

Une telle prohibition qui entrerait d'ailleurs en contradiction avec le principe énoncé par le Code du travail selon lequel toute restriction aux droits des personnes et aux libertés individuelles et collectives doit être proportionnée au but recherché.

Illustration : la Cour d'appel de Bordeaux a ainsi invalidé, le 15 janvier 2013, le licenciement d'une salariée employée à temps partiel (30 heures par semaine) à qui son employeur reprochait d'avoir utilisé internet pour des besoins personnels à raison d'un peu plus d'une heure par semaine, et ce en méconnaissance du règlement intérieur qui prévoyait que « tout usage ou consultation de sites internet sans rapport avec l'exercice professionnel pourra entraîner des sanctions disciplinaires ».

Le plus sûr est donc de permettre aux salariés de faire un usage raisonnable d'internet au bureau, à l'instar de ce qui existe déjà le plus souvent à propos de l'utilisation

personnelle du téléphone au bureau. Cet usage raisonnable pourra alors être consigné dans une charte spécifique ou par une adjonction au règlement intérieur.

Réglementer l’accès personnel à internet et à la messagerie électronique, comment procéder ?

La réglementation de l’accès des salariés aux moyens de communication numérique nécessite de suivre une procédure particulière.

Quelles que soient les motivations de l’employeur, la réglementation de l’accès personnel à internet et à une messagerie électronique doit faire l’objet d’une information des salariés la plus claire possible. En effet, opposer unilatéralement aux salariés une liste d’interdictions sans prendre le soin de leur préciser les raisons d’être de ces interdictions risque de créer dans l’entreprise un climat de défiance.

Les règles d’usage d’internet à des fins personnelles

Dès lors que le principe d’un usage personnel d’internet au bureau est admis par l’employeur, il lui faut toutefois rappeler que cet usage personnel est nécessairement limité.

Pourra ainsi notamment faire l’objet d’une interdiction :

– la consultation de sites internet répréhensibles ;

– la création ou l’alimentation de sites ou de blogs personnels ;

– la participation à certains types de forum ou à certains « chat » ;

– le téléchargement de fichiers illicites ou de logiciels.

L’employeur pourra également préciser que cet usage devra avoir lieu en principe pendant les temps de pause et non durant les plages horaires de travail.

De la même manière, l’usage du courrier électronique pourra aussi être réglementé afin de permettre au salarié de recevoir ou d’envoyer des messages destinés à résoudre certains problèmes de la vie courante (garde d’enfants, formalités administratives urgentes, etc.), de préférence en dehors des heures de travail effectif.

La procédure à suivre

Pour réglementer l’usage de d’internet à des fins personnelles, deux voies s’offrent à l’employeur. Il peut choisir d’ajouter au règlement intérieur une ou plusieurs clauses relatives à l’utilisation des NTIC dans l’entreprise ou préférer rédiger une charte internet spécifique.

Rappel : un règlement intérieur est obligatoire dans les entreprises ou établissements où sont employés habituellement au moins 20 salariés. Les autres entreprises peuvent choisir d’en établir un, à la condition toutefois de suivre la procédure prévue par le Code du travail.

Mais quelle que soit la solution retenue (charte internet ou ajouts au règlement intérieur), il est indispensable de suivre la procédure relative à l’établissement d’un règlement intérieur. À défaut, les prescriptions en matière d’usage des NTIC dans l’entreprise pourraient être considérées par les juges comme inopposables aux salariés.

Rappel : l’élaboration du règlement intérieur se déroule en plusieurs étapes :
– l’employeur rédige un projet de règlement intérieur ;
– il le soumet ensuite pour avis aux représentants du personnel s’il en existe dans l’entreprise (comité d’entreprise ou, à défaut, délégués du personnel, ainsi que, pour les matières relevant de sa compétence, CHSCT) ;
– l’employeur peut alors librement décider d’amender ou non son projet pour tenir compte des éventuelles observations des représentants du personnel ;
– l’employeur transmet deux exemplaires du règlement intérieur – accompagnés, le cas échéant, de l’avis des représentants du personnel – à l’inspecteur du travail, qui peut en vérifier le contenu et exiger la modification ou la suppression de dispositions qu’il estime illicites. Par ailleurs, un exemplaire est déposé au secrétariat-greffe du conseil de prud’hommes ;
– l’employeur procède, enfin, à l’affichage du règlement intérieur, à un endroit de l’entreprise accessible à l’ensemble des salariés. Le règlement intérieur doit à ce moment indiquer la date à laquelle il entre en vigueur, cette date devant être postérieure d’un mois à la date d’accomplissement des formalités de dépôt et de publicité.

Mettre en place des outils de cybersurveillance, quelles précautions prendre ?

Dans le cadre de la surveillance de la navigation des salariés sur la toile, l’employeur doit respecter certaines règles.

Nul ne conteste la faculté reconnue à un employeur de contrôler l’activité de ses salariés pendant leur temps de travail. Mais dès lors qu’il met en place un dispositif de

contrôle de leur activité, il est soumis à une procédure astreignante. Toutefois, lorsque ces outils de contrôle n'ont vocation que d'assurer la sécurité informatique de l'entreprise, les formalités sont allégées.

Les outils destinés à contrôler l'activité des salariés

En vertu du Code du travail, l'introduction dans l'entreprise de tout système de contrôle de l'activité des salariés doit d'abord faire l'objet d'une information et d'une consultation du comité d'entreprise, lorsqu'il en existe un. Peu importe, à cet égard, que le système de contrôle serve également à d'autres usages (assurer la sécurité du système informatique ou la formation d'opérateurs de téléphonie, par exemple).

Important : la loi exige l'information et la consultation du comité d'entreprise. L'employeur ne peut donc se borner à informer les membres du CE, mais doit solliciter leur avis exprès sur le dispositif qu'il envisage de mettre en place.

La preuve d'un agissement répréhensible obtenue grâce à un système de contrôle mis en place sans consultation du comité d'entreprise est considéré par les tribunaux comme irrecevable. Cette absence de consultation est, par ailleurs, passible d'une condamnation pénale pour délit d'entrave.

À noter : s'il n'existe pas de comité d'entreprise, le ou les délégués du personnel peuvent toutefois agir en justice pour faire cesser toute atteinte aux droits et aux libertés individuelles des salariés, occasionnée en particulier par un système de contrôle informatique.

De plus, le Code du travail prévoyant que « aucune information concernant personnellement un salarié […] ne peut être collectée par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié », un employeur ne

peut donc logiquement mettre en place un système de cybersurveillance sans informer préalablement les salariés concernés de son existence et de ses modalités.

Enfin, dès lors que les outils de cybersurveillance entraînent un traitement de données à caractère personnel (ce qui sera généralement le cas pour que le contrôle soit effectif) une déclaration de ce traitement à la Cnil devra être effectuée.

À savoir : les entreprises peuvent être dispensées de cette déclaration si elles prennent le soin de nommer un correspondant Informatique et Libertés dans les conditions requises par la loi.

Les outils destinés à assurer la sécurité informatique

Les administrateurs informatiques, dont le rôle est d'assurer le fonctionnement normal et la sécurité des réseaux et systèmes informatiques de l'entreprise, ont accès régulièrement à des informations relatives à l'activité des salariés (messagerie, connexion à internet, fichiers archivés sur le réseau ou le disque dur, etc.).

Étant amenés à traiter des informations personnelles, ils sont soumis à une obligation de confidentialité qui pourra être consignée dans le contrat de travail, le règlement intérieur ou dans une charte d'utilisation des outils informatiques annexée à ce règlement.

Pour réaliser leurs missions, ces administrateurs-réseaux utilisent généralement des outils tels que des logiciels de maintenance, de prise en main à distance ou encore des fichiers de journalisation.

Précision : les fichiers de journalisation recensent et enregistrent toutes les connexions ou les tentatives de connexion à internet des utilisateurs.

Tant que ces outils ne sont pas utilisés pour collecter des informations individuelles, poste par poste, dans le but de contrôler l'activité des utilisateurs, une déclaration à la Cnil n'est en principe pas obligatoire.

Attention : lorsque les fichiers de journalisation sont associés à un traitement automatisé d'informations nominatives afin de garantir ou de renforcer le niveau de sécurité de ce dernier, ils doivent cependant être portés à la connaissance de la Cnil en même temps que la déclaration du traitement automatisé d'informations nominatives.

En revanche, même s'il n'existe aucune volonté patronale de contrôler l'activité des salariés, dès lors que l'usage de ces outils informatiques entraîne la collecte d'informations concernant personnellement un salarié, le Code du travail impose à l'employeur d'informer tout salarié susceptible d'être concerné de son projet d'introduire un dispositif entraînant une collecte d'informations personnelles.

En pratique : pour éviter toute difficulté, cette information doit être réalisée par écrit auprès de chaque salarié.

© 2013 Les Echos Publishing