

INTERNET OU LA TOILE DE TOUS LES DANGERS...

Les courriers électroniques contenant des informations hautement stratégiques ou des informations délétères peuvent effectivement représenter une menace pour les Entreprises, un risque au demeurant connu depuis maintenant plusieurs années.

Nous sommes entrés depuis peu dans une nouvelle ère de risque majeur avec les **SOCIALS NETWORKERS**, autrement dit les « réseaux sociaux professionnels » tels que : **VIADEO – LINKEDIN – HUZZ** et consorts..

La création d'un annuaire professionnel en ligne est on ne peut plus légale. Cependant, c'est une révolution, bien plus qu'une évolution dans le monde du recrutement et de surcroît dans la quête d'informations.

On peut parer de vertus cette évolution radicale en considérant qu'elle facilite et accélère l'approche des bons profils, toutefois, à trop se réjouir, force est de constater que le phénomène joue dans les 2 sens.

En effet, ils sont de plus en plus nombreux à l'instar de **FACEBOOK**, à avoir leur profil en ligne sur les **VIADEO – LINKEDIN** et consorts.

De fait, pour un coût extrêmement modique, il devient enfantin d'approcher un Directeur du marketing, un Directeur commercial, un Directeur industriel, un Directeur du développement en lui faisant parfois miroiter quelques allouettes pour tenter de lui soustraire par la même occasion quelques informations.

Fort heureusement l'essentiel des approches ont un fond sincère. Néanmoins, le fait de savoir que très souvent et de plus en plus, vos meilleurs éléments sont en « vitrine », **devrait vous interpeller !**

Nous donnons 2 conseils :

1 – Vous êtes Patron de filiale ou de la société mère, mettez votre profil en ligne avec le nom patronymique de votre société. **C'est comme cela que vos collaborateurs sont chassés !**

2 – Insérer dans le contrat de travail « clause de confidentialité » un chapitre de mise en garde, au même titre que l'usage d'Internet et des courriers électroniques dans l'Entreprise.

HOMMES ET COMPÉTENCES

SÉCURITÉ | Blogs, réseaux sociaux, messagerie instantanée, e-mails...

Les communications électroniques génèrent de nouveaux risques dans les entreprises. Pour ne pas les subir, les employeurs doivent donc disposer de bons moyens pour contrôler et, au besoin, sanctionner les usages abusifs. ■ PAR MURIEL BEAUDOING

Gare aux échanges électroniques !

Productivité en berne

➤ **86 minutes**, c'est le temps moyen que passent quotidiennement les salariés sur Internet.

➤ **28 minutes** seulement à l'usage professionnel.

➤ **4 semaines de congés supplémentaires par an**, c'est en cumul le temps perdu à cause d'internet au bureau.

SOURCES : OLFFO, GARTNER GROUP

Ne pas surveiller les mails de ses salariés peut coûter cher. Dans ce domaine, le cas de la BNP fait école. Suite à une action en référé de la société WPO s'estimant victime d'un préjudice du fait d'un mail anonyme provenant d'un salarié de la BNP, la banque a été condamnée en 2005 pour responsabilité délictuelle, n'ayant pu identifier l'auteur du message pour des raisons techniques. Au-delà des risques judiciaires, le non-contrôle des communications électroniques pose des problèmes techniques, de sécurité et de productivité : encombrement de la bande passante, virus téléchargés via des pièces jointes ou du peer-to-peer (réseau de partage de fichiers entre internautes), dossiers stratégiques diffusés volontairement ou non à l'extérieur de l'entreprise... Pour se protéger, l'entreprise doit donc mettre en place des règles précises. Nos conseils pour ne pas se laisser déborder.

1 DÉFINIR DES RÈGLES DU JEU

Penser que vous pourrez empêcher totalement l'usage du web à des fins personnelles à vos salariés est une erreur. En revanche, vous pouvez encadrer cette pratique. C'est même

conseillé de préciser, dans une charte, les règles régissant l'utilisation des moyens de communications électroniques. Elle vous permettra de fixer les droits et les devoirs des salariés. Celle-ci devra respecter le code du travail, la loi informatique et libertés, avoir obtenu l'avis du CHSCT et des délégués du personnel. Annexée au règlement intérieur, elle prend une valeur juridique et contraignante. Eric Barbry, le directeur du pôle « Droit du numérique » du cabinet d'avocats Alain Bensoussan conseille, par ailleurs, de la compléter par d'autres outils : un livret technique expliquant comment l'appliquer, un guide d'utilisateur justifiant son intérêt, une charte spécifique pour les administrateurs systèmes et réseaux et un

guide présentant la manière dont est contrôlée l'activité des collaborateurs.

La SSII Raynet, filiale du sous-traitant automobile A Raymond, fait ainsi signer aux salariés du groupe une charte internet. « Notre système est surtout basé sur la confiance, sachant qu'une utilisation personnelle est possible durant les pauses » note Marie-Thérèse King, la directrice des systèmes d'information.

En revanche, à la Caisse d'Épargne Rhône-Alpes, les règles sont strictes. « Au départ, nous avons interdit aux salariés de communiquer par mail avec les clients pour éviter tout risque de litige commercial en cas de défaillance technique », indique Philippe Brunier, le directeur de la sécurité.

LES ERREURS À ÉVITER

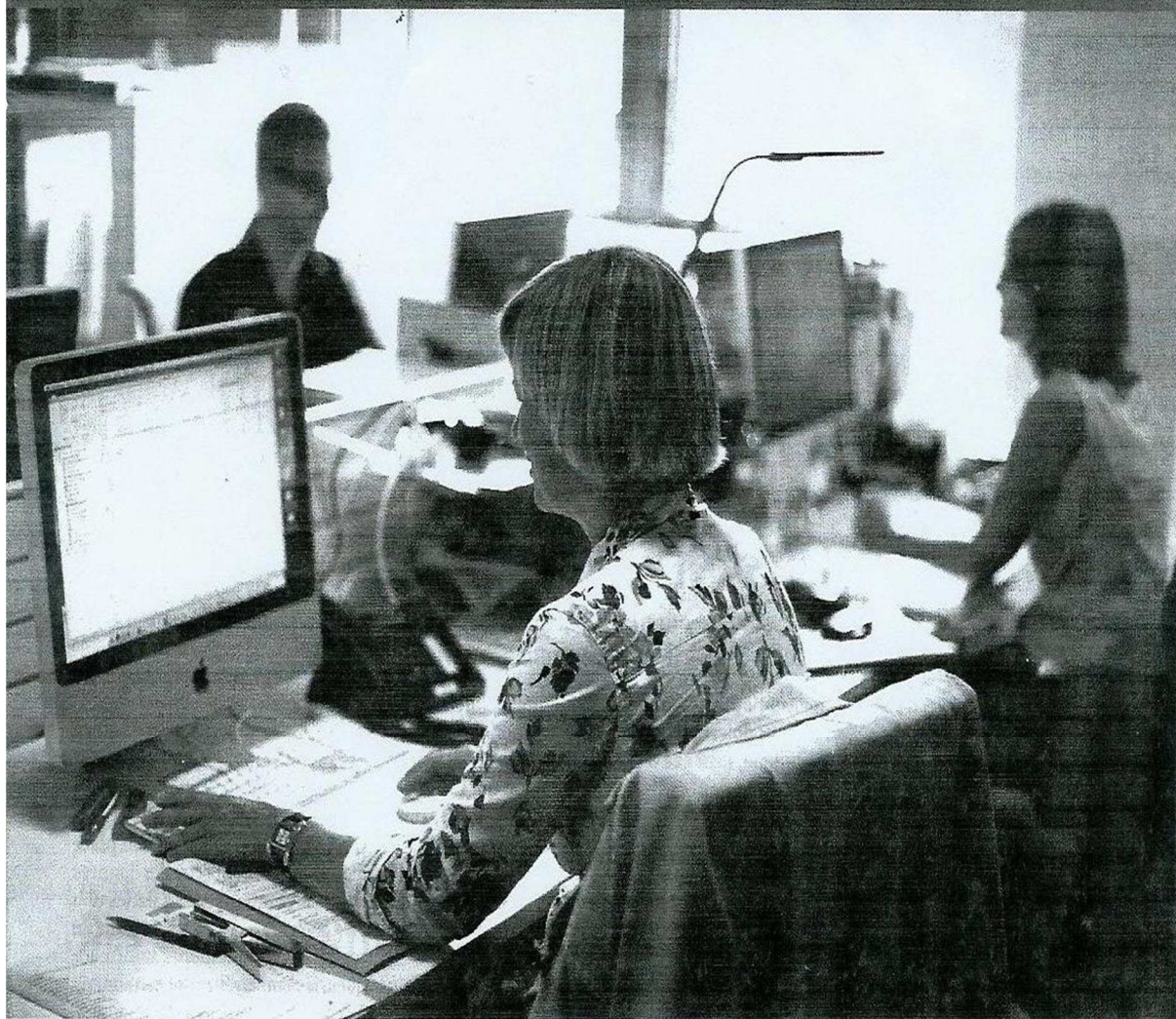
FAIRE L'IMPASSE SUR LA CNIL. Oublier de déclarer son système de surveillance auprès de la Commission nationale de l'informatique et des libertés (Cnil) peut poser des problèmes lors des conflits avec les salariés. L'omission risque de fragiliser la preuve, voire de se retourner contre l'employeur.

ESPIONNER SES SALARIÉS. Surveiller les communications électroniques de salariés sans les informer est un délit puni par la loi informatique et libertés. Mieux vaut donc jouer la transparence en leur détaillant les activités surveillées, les données collectées,

la durée de leur conservation et les moyens d'y accéder.

SORTIR L'ARTILLERIE LOURDE.

Mettre en place des dispositifs de contrôle disproportionnés par rapport à l'objectif poursuivi est une erreur. Le système doit être adapté aux risques avérés. ■



Depuis, ces règles ont été assouplies. Un commercial peut communiquer son adresse mail à un client mais, dans le cadre d'un contrat, seule la signature a une valeur juridique. De leur côté, les salariés de STMicroelectronics, soumis à une charte annexée au règlement intérieur, suivent régulièrement des séances de sensibilisation et de formation sur la sécurité et la bonne utilisation des moyens informatiques.

2 IMPOSER UN CONTRÔLE

Pour contrôler le temps passé par ses salariés sur le net, les sites fréquentés ou les caractéristiques des mails adressés à l'extérieur, l'entreprise peut mettre en place des logiciels de filtrage et de surveillance. « Mieux vaut commencer par les

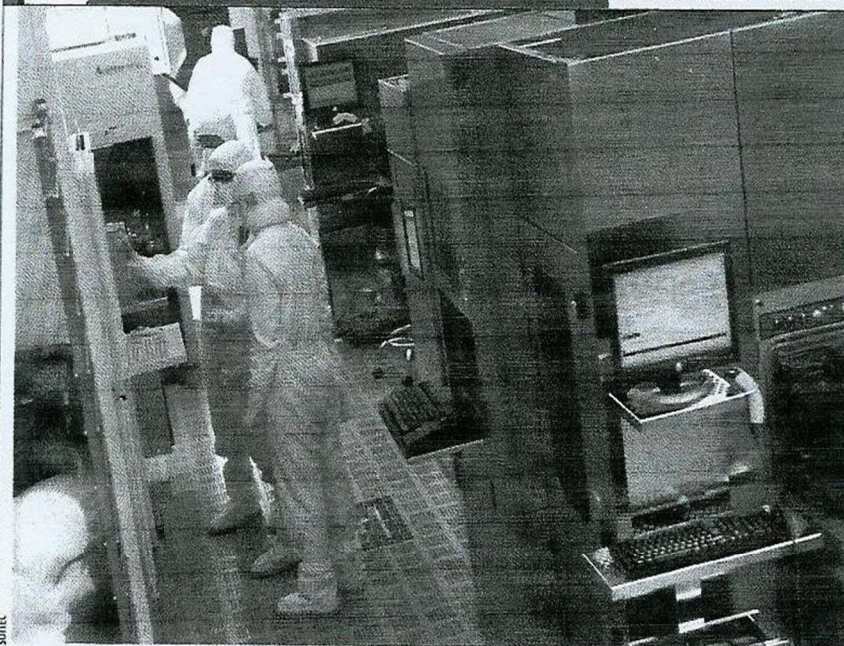
contenus clairement immoraux, puis durcir le filtrage au fil du temps », conseille Alexandre Souillé, le président d'Olféo, un éditeur de logiciels de sécurité pour la maîtrise d'internet. À chaque entreprise sa stratégie. « Nous ne filtrons ni les mails ni les sites et les salariés peuvent utiliser de la messagerie instantanée pour communiquer entre les différentes plates-formes, indique Philippe Lornet, le directeur technique de la SSII Genitech. Mais nous veillons à ce que la bande passante ne se réduise pas trop ; sinon, nous intervenons. »

Chez le spécialiste de la simulation, Corys, les salariés ont accès à leur messagerie personnelle, avec une surveillance globale des flux entrants et sortants. « Il y a une certaine tolé-

Essentiel. La mise en place dans l'entreprise d'outils visant à collecter des données sur l'usage d'internet des salariés doit obligatoirement être déclarée à la Cnil.

rance. Cela étant, chaque connexion est clairement identifiée et les chefs de projet veillent au rendement de leurs équipes », précise Stéphane Grumel, le responsable du support informatique. Pour transmettre des données confidentielles, les salariés doivent, par ailleurs, utiliser leur mail professionnel avec un système de cryptage ou des tunnels VPN sécurisés. « Nous avons également bloqué les applications de VoIP, type Skype, et interdit la copie des mails sur des boîtes personnelles pour la confidentialité des données. »

STMicroelectronics bloque, pour sa part, les sites à risques ou nécessitant des ressources importantes grâce à un filtrage par mots clés. Un salarié peut toutefois faire une demande d'autorisation pour



SOITEC INTERDIT L'USAGE DES WEBMAILS



Laurent Maumet, le directeur des systèmes d'information, bloque les webmails par crainte d'éventuels virus.

Chez Soitec, les salariés peuvent utiliser leur messagerie professionnelle à des fins personnelles, mais ils doivent en faire un usage raisonnable. L'entreprise de microélectronique, installée à Bernin en Isère, a adopté, il y a quelques années, une charte de sécurité de l'information qui cadre notamment l'usage d'internet et de la messagerie. «Tous les webmails, type Yahoo ou Gmail, sont inaccessibles, afin d'éviter le contournement des règles de sécurité de la messagerie interne et de se prémunir d'éventuelles contaminations virales», explique Laurent Maumet, le directeur des systèmes d'information. Ecrire «privé» dans l'objet des mails envoyés et placer ceux reçus dans un dossier dédié les dotent d'un caractère personnel. Tous les autres sont considérés comme professionnels et l'entreprise est susceptible d'en prendre connaissance. Pour l'heure, les salariés peuvent accéder aux réseaux sociaux comme Twitter, Facebook ou LinkedIn. «Ces sites ne sont pas filtrés, même si nous nous interrogeons aujourd'hui sur leur intérêt», confie Laurent Maumet. En revanche, le chat sur MSN ou Gtalk est impossible, ayant peu d'utilité pour le travail. «D'autant que nous avons déployé cette année une solution de messagerie instantanée interne à Soitec, avec l'outil MOCS de Microsoft.»

► Suite de la page 45 accéder, par exemple, à des sites de jeux en ligne s'il développe des applications de téléphonie mobile. Dans les banques, les contrôles sont plus importants. Les salariés n'ont pas accès aux réseaux sociaux, aux forums de discussion et à leur messagerie personnelle. «Nous avons mis en place des solutions techniques proches du contrôle parental, avec des listes noires pour les sites contraires à la morale ou sans rapport avec l'activité de l'entre-

prise», indique Philippe Brunier de la Caisse d'Epargne Rhône-Alpes. Un tableau de bord mensuel fait apparaître les dix personnes ayant le plus surfé et téléchargé, mais les abus sont rares. «En cas de problème, nous rappelons à l'ordre le salarié. S'il récidivait, cela pourrait aller jusqu'au licenciement pour faute professionnelle.» Plusieurs profils ont par ailleurs été définis, un commercial n'ayant pas les mêmes besoins qu'un professionnel de la publicité.

3 DOSER SON EFFORT

Sortir l'artillerie lourde ne servira à rien ! Le contrôle réalisé par l'employeur est strictement encadré par la loi et les moyens mis en œuvre doivent être proportionnels à l'objectif visé. Une entreprise dans un secteur stratégique très concurrentiel fera ainsi plus facilement accepter une cybersurveillance étroite du fait des enjeux. Si tous les mails envoyés depuis le lieu de travail sont présumés professionnels et sont donc a priori consultables par l'employeur, lorsqu'ils comportent un objet «personnel» ou sont classés dans des dossiers portant le même intitulé, le secret de la correspondance privée s'applique. «Pour éviter les situations litigieuses, mieux vaut donc avoir fixé des règles très claires dans sa charte informatique pour différencier les mails professionnels et privés, précise Paul Ebest, le chef du service des affaires juridiques de la Commission nationale de l'informatique et des libertés (Cnil). Pour ce qui est des communications des organisations syndicales, nous préconisons un accès propre non surveillé, avec une ligne dédiée.»

Quoi qu'il en soit, la mise en place d'outils visant à collecter des données sur l'usage internet des salariés doit être déclarée à la Cnil. Pour tenir un registre des traitements informatiques, les employeurs ont tout intérêt à désigner un correspondant informatique et libertés, relais entre la Commission et l'entreprise. En outre, l'installation de logiciels de contrôle ne peut se faire sans une information préalable des salariés et sans l'avis du comité d'entreprise. En cas de suspicion, l'employeur peut procéder, en présence du salarié et sous contrôle d'huissier, à une sauvegarde de la messagerie sur un support fiable et durable. Seul un juge pourra alors autoriser la levée du secret des correspondances. Toute preuve recueillie autrement serait irrecevable et exposerait l'employeur à des poursuites pour violation du secret des correspondances et non-respect de la vie privée.

Ces précautions prises, tout abus peut être puni. Un salarié a ainsi été licencié par son entreprise pour avoir envoyé avec sa boîte professionnelle, 157 mails à caractère privé.