LARGEUR.COM

TECHNOPHILE

LUNDI 10 NOVEMBRE 2008

INFORMATIQUE

Surveillance des employés: psychose et parano des entreprises

Les entreprises invoquent la sécurité et l'espionnage industriel pour monitorer les activités online de leur personnel, souvent au mépris du respect de leur vie privée. Quelle est la meilleure politique? Enquête.

PAR LUDOVIC CHAPPEX

Les employés des grandes entreprises ont fini par s'y résoudre: plus un seul de leurs faits et gestes n'échappe désormais à l'œil circonspect de leur hiérarchie. Les méthodes de contrôle intrusives, qui se sont multipliées avec le développement des nouvelles technologies, laissent de moins en moins d'espace à la sphère privée. En pratique, le contenu des e-mails transmis ou reçus avec le matériel d'entreprise (ordinateurs fixes et portables, Blackberry, téléphones mobiles, etc.) peut être très facilement consulté par leur service informatique. Le même service pourra aussi savoir et enregistrer quels sites ont été consultés, et à quel moment, sans même avoir à ajouter de dispositif particulier dans l'ordinateur de l'usager. La plupart des employés savent aujourd'hui que ce type de contrôle liberticide est possible, mais dans quelle mesure est-il vraiment pratiqué par les entreprises?

Selon une étude de Forrester Consulting, 44% des grandes compagnies américaines emploient des gens dont la mission consiste à surveiller le contenu des emails professionnels sortants de l'entreprise; 48% déclarent réaliser des audits réguliers des contenus des messages. Justification? La peur que les employés délivrent des informations sensibles, un secret de fabrication ou encore des données relevant de la propriété intellectuelle.

Evidemment, il y a des effets collatéraux. Les entraves à l'autonomie et la liberté d'action des employés dépassent facilement les limites du cadre professionnel, par exemple lorsqu'une entreprise équipe ses véhicules de traceurs GPS afin de pouvoir les localiser 24 heures sur 24. Et, bien sûr, lorsqu'elle en vient à surveiller les sites consultés et les messages électroniques à l'insu des collaborateurs, au mépris du respect de la vie privée.

Dans les faits, beaucoup d'employeurs semblent se moquer des règles élémentaires de proportionnalité en matière de surveillance. Un tel flicage est-il pour autant illégal? «Les entreprises peuvent tirer profit d'une législation incertaine, répond Bertil Cottier, professeur de droit de la communication à l'Université de la Suisse italienne. Car les bases légales actuelles se contentent de définir des principes extrêmement généraux. La loi fédérale sur la protection des données (LPD), qui régit la collecte d'informations, reste très difficile à appliquer correctement. Par ailleurs, le préposé fédéral à la protection des données dispose comme seul pouvoir de fournir des recommandations. Pour se plaindre d'un abus, il faut donc passer par un juge qui, le plus souvent, n'a pas une connaissance optimale de ces questions.»

Le flou juridique est très néfaste dans ce domaine. «Je constate souvent avec étonnement que des entreprises, même de taille moyenne ou grande, ne disposent d'aucun règlement en matière de protection des données, observe à ce propos Gilles Monnier, avocat et professeur à la Faculté de droit et des sciences criminelles de Lausanne. Les sociétés sont pourtant tenues de s'organiser afin de réaliser dans les faits la protection des données personnelles. Il faut aussi souligner, en ce qui concerne notamment l'industrie, que la surveillance permanente de l'activité des employés est interdite, en vertu de l'art. 26 de l'Ordonnance 3 de la Loi sur le travail.»

Titulaire de la chaire Télécommunication et sécurité à HEC Lausanne, Solange Ghernaouti-Hélie dresse un bref état des lieux: «Il faut d'abord relever qu'Internet, avec toute sa palette d'outils de mise en relations de n'importe qui avec n'importe qui, n'importe où, n'importe quand, abolit non seulement les frontières temporelles et géographiques mais aussi celles qui existent entre vie professionnelle et vie privée, entre monde du travail et monde des loisirs. Il s'agit d'un phénomène dont les conséquences n'ont pas du tout été prises en considération et que l'on semble découvrir avec les problèmes potentiels générés par les utilisateurs de réseaux sociaux.»

La menace Facebook

Pour les entreprises, les réseaux sociaux de type Facebook entre dans la catégorie de menaces dite «d'ingénierie sociale»: par la tromperie ou des techniques de leurre, une personne malveillante peut par exemple amener un employé, approché amicalement, à livrer des paramètres de connexion (identification, login, mots de passe). Mais surtout, dans le contexte d'un réseau social, l'utilisateur fournit de son plein gré des informations qui, dès lors, ne lui appartiennent plus. Ce dernier n'a aucun contrôle quand à leur utilisation ultérieure par l'entreprise Facebook et par le public qui pourra y avoir accès. Pour cette raison, à la banque privée Pictet & Cie, par exemple, on se dit «préoccupé par les réseaux internet sociétaux», précisant qu'«une réflexion est en cours à ce sujet». Mais aucune directive ou interdiction n'a encore été formulée. Actuellement en Suisse, plus d'une centaine d'employés de Pictet s'affichent ouvertement comme tels sur Facebook. Ce type de réseau social n'effraie pas toutes les entreprises, au contraire: la plupart des multinationales (UBS, P&G, etc.) y possèdent des «Networks» officiels auxquels peuvent adhérer leurs employés.

«Sur Facebook, les employés d'une entreprise pourraient critiquer les conditions de travail, se plaindre de phénomènes de corruption ou de passe-droit, note à ce propos Solange Ghernaouti-Hélie. On peut imaginer des retombées négatives en terme d'image.» Ajoutons que les employés, de par leur comportement, leurs photographies privées (par exemple pendant des fêtes arrosées) et, au sens large, leur activisme plus ou moins exubérant sur le réseau, sont susceptibles de nuire à la réputation de sérieux, voire de discrétion, de leur employeur. Mais ces mêmes dérives potentielles existent ailleurs online (si l'employé anime un blog ou un site personnel par exemple) et, dans une certaine mesure, aussi dans le monde réel. Alors, jusqu'où l'entreprise paranoïaque doit-elle réglementer le comportement privé de ses employés?

De l'avis des experts de la sécurité, les préoccupations des entreprises n'ont rien d'illégitimes. L'espionnage industriel, le vol d'informations, l'atteinte à l'image ou la malveillance de certains employés représentent autant de menaces bien réelles. Selon une enquête* de Pricewaterhousecoopers, 37% des entreprises suisses se disent avoir été victimes de délits économiques. Or, la moitié des auteurs de ces délits appartient au management même des entreprises concernées!

Une autre étude, menée par l'institut de Criminologie et de droit pénal de l'Université de Lausanne (ICDP) auprès d'entreprises du canton de Genève, aboutit à des résultats similaires: sur les 543 entreprises (commerces et institutions financières) interrogées, 35% ont été victimes de délits économiques commis par leurs employés au cours des quatre dernières années. Un chiffre spectaculaire. Dans plus de 60% des cas, l'acte est répété au moins cinq fois avant que l'auteur soit appréhendé. Pas surprenant, donc, si les entreprises se montrent outrageusement suspicieuses. Reste à mettre en place la bonne stratégie...

Selon l'étude de l'ICDP, le risque est deux fois moins important lorsque les entreprises optent pour une gestion transparente de la surveillance, et une attitude reconnaissante envers les employés, plutôt que pour des contrôles systématiques effectués en catimini. «Les entreprises qui adoptent un code de conduite formel subissent nettement moins de délits économiques», approuve Rolf Schatzmann, consultant en sécurité informatique, associé de Pricewaterhousecoopers.

Dans leur dernier rapport sur la sûreté de l'information**, les experts de la Confédération soulignent d'ailleurs que les mesures techniques, à elles seules, protègent toujours moins contre les cyberattaques. D'où l'importance croissante, suggèrent-ils, de créer un climat de confiance, d'informer et de sensibiliser le personnel à ce sujet. «Les entreprises sont à la merci de leurs employés, résume Nicolas Giannakopoulos, fondateur de l'Observatoire du crime organisé à Genève. Un salarié en colère peut causer beaucoup de tort.» Autrement dit, les entreprises devraient éviter à tout prix d'instaurer un régime de défiance, préjudiciable aux performances à long terme.

Les atteintes les plus grossières à la sphère privée seraient davantage le fait de petites et moyennes entreprises; la majorité des grandes firmes ont intégré la notion de gouvernance en matière de

sécurité, lorsqu'elles ne sous-traitent pas carrément une partie de cette gestion à des sociétés de consulting spécialisées. Un juge d'instruction genevois, qui souhaite rester anonyme, livre cet exemple parlant: «J'ai traité cet été du cas d'une PME active dans l'informatique dont le patron avait installé des mouchards sur tous les ordinateurs. C'est seulement lors du transfert d'activité à une autre société que la nouvelle direction s'est aperçue de cette situation. L'ancien patron pouvait contrôler l'ensemble de l'activité et de la correspondance, y compris privée, de ses employés.»

Un cas de figure qui n'étonne guère Olivier Ribaux, ancien analyste criminel à la police cantonale vaudoise, aujourd'hui professeur associé à l'Ecole des Sciences criminelles de l'Université de Lausanne: «Par rapport au cadre légal extrêmement rigoureux imposé à la police pour ses investigations, les entreprises disposent d'une grosse marge de manœuvre. Il est difficile de savoir quelle surveillance elles exercent réellement sur leurs employés.»

Combien d'entreprises respectent les prescriptions légales? Combien savent réellement comment se comporter en matière de surveillance, quelle stratégie adopter? Savent-elles seulement combien de personnes, cadres et informaticiens, ont accès aux données personnelles? Ces questions sont-elles seulement évoquées et débattues en leur sein? Difficile de le dire car beaucoup de sociétés, comme par réflexe conditionné, se réfugient dans le mutisme sitôt qu'on les interpelle sur ce thème. La plupart des entreprises contactées (de Logitech à Omega, en passant par Hublot), ne souhaitent pas se prononcer sur le sujet. Swisscom et UBS répondent, mais sans donner trop de détails.

Il existe de rares exceptions, comme la Banque Cantonale vaudoise, qui s'exprime avec la plus grande clarté sur son dispositif: «Nous avons nommé un responsable de la sécurité directement rattaché à un directeur général de la banque. Ce dernier décide, avec la validation du département des ressources humaines et du département compliance, de tout ce qui est lié à des enquêtes sur des collaborateurs. Ce contrôle dit 'Six Yeux' est nécessaire pour s'assurer du respect de la Loi sur la protection des données (LPD) pour tous les aspects de contrôles ou de surveillance», explique Paul Coudret, conseiller économique à la BCV. La banque rappelle une évidence qui semble parfois oubliée: c'est le facteur humain, impossible à maîtriser, qui constitue «le maillon faible de la sécurité», et qui représente donc «une des préoccupations majeures du top management».

Internet ou pas, un employé sera toujours potentiellement une menace. Aux entreprises de limiter les frustrations, les risques et les abus. Notamment en adoptant une politique claire et transparente en matière de surveillance électronique.

---
* Etude PwC «Economic Crime Survey 2007»
** Sûreté de l'information: situation en Suisse et sur le plan international. Rapport semestriel 2007 (juillet à décembre). Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI.

Une version de cet article est parue dans le magazine économique suisse Bilan.
