Tout système de surveillance est par principe interdit par la loi. Sauf exceptions.

Jusqu'où peut-on surveiller ses employés?

PAR CAMILLE ANDRES **Pour une entreprise, il est aujourd'hui facile techniquement de tracer les actions électroniques de ses collaborateurs. Mais juridiquement, ce contrôle est très encadré. Comment éviter vols et fuites?**

TOUS LES vendredis soir a lieu, en Suisse, une migration invisible: des millions de kilooctets de données que des employés s'envoient chez eux pour finir leurs dossiers et projets en retard. Que celui qui n'a jamais finalisé une présentation depuis son salon leur jette la première pierre.

La fuite de données est aujourd'hui un challenge pour toutes les organisations et pose de vraies questions de sécurité. Techniquement, faire sortir une information stratégique est aujourd'hui très facile. «Malgré toutes les protections du monde, faire une photo d'un écran via un smartphone est possible, tout comme le fait de noter des noms de clients clés sur un simple bout de papier», remarque Sylvain Métille, avocat à l'étude HDC, et enseignant à l'Université de Lausanne ainsi qu'à l'Institut de management des technologies et de la télécommunication de Fribourg. La démocratisation des ordinateurs et smartphones personnels et l'incitation des entreprises d'apporter son propre appareil au travail ne font qu'augmenter les risques.

LA DERNIÈRE TENDANCE? DES LOGICIELS ESPIONS COMME SPECTOR360 QUI PREND ET TRANSMET À INTERVALLES RÉGULIERS DES CAPTURES D'ÉCRAN

Identifier les informations stratégiques

Mais le vrai problème, c'est que peu d'entreprises, notamment parmi les PME, savent identifier quelles données sont stratégiques, et comment gérer leur flux permanent. «Aujourd'hui, il revient moins cher de stocker et conserver ses données que de les trier et de les éliminer», note Lennig Pedron, directrice des ressources humaines et communication dans la cybersécurité pour SecuLabs, lors d'une conférence de l'Association suisse en veille stratégique et intelligence économique (ASVIE), début octobre.

A l'heure de la digitalisation et du big data, des informations clients ou même des archives offrent une solide valeur ajoutée. Quoi qu'il en soit, insiste l'experte, «chaque entreprise est responsable des données qu'elle stocke». Qu'il s'agisse d'informations concernant les salariés ou ses propres clients, à l'entreprise d'éviter les fuites, notamment. Une exigence forte et contraignante – imposée par la loi sur la protection des données. Pour y faire face, le premier conseil que donnent les spécialistes en sécurité est donc d'identifier le «patrimoine informationnel» de l'entreprise: quelles sont les informations dont dispose la structure, où sont-elles stockées et qui y a accès. Le but étant évidemment de le limiter aux personnes qui en ont réellement besoin: les process R&D ne concernent a priori pas le service comptable.

Bannir la culture du secret

Pour autant, pas question de laisser des zones d'ombre s'installer. «Toute politique de protection des données doit être connue, planifiée, communiquée... pour que les employés y adhèrent. Il faut éviter que s'installe un tabou», assure Lennig Pedron.

PHOTO: COLORBLINDIGETTY

Le souci n'est pas le travail à distance, selon Sylvain Métille: «Venir au travail avec son ordinateur privé est bien plus dangereux que de travailler depuis son salon connecté à un serveur sécurisé.»

C'est justement dans les cas où un flou existe sur la classification de l'information, son accès, les sanctions encourues que surviennent les dérapages pour les employés, surveillés ou... sollicités par leur direction pour des demandes de surveillance en réalité illégales. «Les services IT sont très preneurs de conseils pour éviter de sortir du cadre légal lors d'investigations techniques ou de requêtes de la hiérarchie», signale Michael Chochois, expert dans le domaine de cybersécurité.

Dernière tendance en date? L'utilisation de logiciels espions, à l'instar de Spector360, vendu comme un outil de «surveillance des employés». Il prend et transmet à intervalles réguliers des captures d'écran. «Le marketing de SpectorSoft qui fabrique cet outil est très bon: certains ne se rendent pas compte qu'en réalité cette technologie peut aller à l'encontre de la loi suisse», remarque Lennig Pedron. Car si l'outil peut permettre de vérifier que l'employé n'envoie pas des contenus stratégiques ailleurs, il peut facilement être aussi utilisé pour surveiller qu'il n'aille pas faire du shopping en ligne durant ses heures de travail. Au Tessin, un cas s'est présenté: même si un tel logiciel a pu prouver qu'un fonctionnaire n'effectuait pas son travail, il a été réintégré à son poste et son salaire lui a été reversé. Le motif? «Le Tribunal fédéral a estimé que les preuves étaient illégales. Il y avait d'autres moyens pour s'enquérir du fait que les tâches étaient ou non effectuées», explique Sylvain Métille.

Adapter les moyens aux objectifs

Si faire fuiter des informations est un jeu d'enfant, mettre en place une surveillance électronique en entreprise ne s'improvise pas (lire ci-dessous). Elle est possible et acceptée pour des raisons économiques et stratégiques. «La sécurité des données, la présence de fichiers sensibles peuvent justifier la mise en place d'une surveillance: caméra pour vérifier les accès, logiciel de contrôle électronique...», reconnaît Sylvain Métille. Mais l'employeur devra toujours prouver que cette solution a été expliquée à l'employé, qu'elle est indispensable, proportionnée, et constitue sa seule possibilité de contrôle. Installer une caméra, d'accord, mais celle-ci devra filmer le clavier, le coffre-fort ou le tiroir-caisse, pas l'employé. Idem pour une balise GPS: elle est acceptable tant qu'elle se limite à vérifier qu'un trajet prévu est effectué et non si elle permet de suivre un chauffeur de taxi à la trace.

Dans tous les cas, Sylvain Métille conseille de mettre en place un règlement des ressources informatiques, qui prévoit les conditions de surveillance et de sanction, et anticipe les procédures en cas de licenciement. Ce dernier peut être établi par un «service RH, de sécurité informatique ou de contrôle interne», voire même par un groupe de travail réunissant les personnes intéressées par le sujet. Car c'est souvent dans les moments de litiges que l'entreprise se retrouve face à une fuite de données. «La meilleure façon d'éviter ces situations, c'est de s'assurer que tous les employés se sentent bien dans l'entreprise et n'aient pas intérêt à lui causer du tort», résume le juriste. ■

QUE DIT LE DROIT?

LÉGISLATION Texte central sur le sujet, l'article 26 de l'ordonnance 3 relative à la Loi sur le travail interdit tout système de surveillance par principe. Le texte admet des exceptions, précisées par la jurisprudence: la surveillance ne doit pas être un but en soi, elle doit être effectuée de bonne foi, justifiée, proportionnée, c'est-à-dire limitée au strict nécessaire et ne poser aucun danger pour la santé ou la liberté du travailleur, qui doit en être informé. Par ailleurs, elle doit respecter la loi sur la protection des données. Une surveillance mise en place sans information équivaut à de l'espionnage et tombe sous le coup du Code pénal (articles 179ss), y compris sur le lieu de travail.
Informations: www.edoeb.admin.ch et https://ntdroit.wordpress.com