Image not found or type unknown

La surveillance de l'outil informatique (2/2)

publié le **30/12/2013**, vu **3476 fois**, Auteur : Adrien LANCIAUX

Suite et fin de l'article relatif à la surveillance de l'outil informatique. Il est cette fois consacré au contrôle de l'utilisation de l'ordinateur.

La surveillance de l'utilisation de l'ordinateur

Deux grandes problématiques sont posées par la surveillance de l'utilisation de l'ordinateur. D'une part la nécessité de protéger le système informatique et la sécurité de l'entreprise. Cette mission revient la plus part du temps à l'administrateur réseau (A) qui se trouve dans une position délicate. D'autre part, l'outil informatique dont dispose le salarié est souvent mis à sa disposition par l'employeur (B). Pour ce dernier il est donc légitime d'attendre que cet outil soit mis au profit de l'activité professionnelle, et non au service des occupations privées. Pour autant, toutes les formes de surveillance ne sont pas permises

A. La position délicate de l'administrateur réseau

En matière de cyber surveillance, les administrateurs réseaux occupent un rôle central. Ces derniers sont chargés de la sécurité informatique de l'entreprise. A ce titre, ils peuvent par le biais des moyens dont ils disposent accéder à des informations personnelles des salariés. Afin d'illustrer cette problématique, il convient de faire référence à un arrêt rendu par la chambre sociale de la Cour de cassation le 17 juin 2009. En l'espèce, un employeur soupçonnait dix-sept salariés d'avoir eu connaissance de données confidentielles (l'entreprise en question était classée Seveso). Il demande alors à l'administrateur réseau de surveiller leurs postes de travail, et de lui transmettre les informations obtenues. La Cour de cassation s'est demandée si les messages *« qualifiés de personnels ou pouvant, de par leur classement, être considérés comme tels avaient été ouverts dans le seul cadre de la mission confiée à l'administrateur réseaux ou s'ils l'avaient été par l'employeur*[1] *»*. Pour Sandrine Maillard, ce raisonnement sous-tend le fait que *« si l'employeur ne peut pas accéder aux messages qualifiés de personnel ou pouvant, de par leur classement, être considérés comme tel, l'administrateur réseaux qui est tenu d'une obligation de confidentialité peut ouvrir ces messages personnels dans le cadre de sa mission de sécurité des réseaux informatiques*[2] *»*. En raison de son obligation de sécurité, l'administrateur ne peut en aucun cas transférer les messages « personnels » à l'employeur quand bien même il lui demanderait. La possibilité d'ouvrir les messages des salariés s'inscrit uniquement dans le cadre de ses missions. Autrement dit, cela doit être justifié par un impératif de sécurité. Toutefois, si *« la préoccupation de la sécurité du réseau [justifie] que les administrateurs de systèmes et de réseaux fassent usage de leurs positions et des possibilités techniques dont ils [disposent] pour mener les investigations et prendre les mesures que cette sécurité [impose], la divulgation du contenu des messages (...) ne [relève] pas de ces objectifs*[3] *».* En outre, l'administrateur se doit de garantir la sécurité du système, et prendre les mesures qui s'imposent. Ce dernier peut alors se trouver dans une situation délicate. Car s'il doit détecter et sécuriser la faille, les moyens dont il dispose peuvent se trouver limiter. Il peut par exemple décider de restreindre l'accès au web des salariés concernés, mais *« s'agit-il d'une mesure de sécurité relevant du pouvoir de l'administrateur réseaux ou d'une mesure disciplinaire relevant du pouvoir de l'employeur ?*[4] *».* D'un autre côté, les informations qu'il peut communiquer à l'employeur sont limitées. A noter également que s'il vient à ouvrir des messages personnels sans raison, il risque des poursuites pénales au titre de la violation du secret des correspondances

[5]. En tout état de cause, l'administrateur réseau ne pourra sanctionner des utilisations abusives, ce pouvoir étant exclusivement réservé à l'employeur.

B. **L'employeur et la surveillance de l'utilisation de l'ordinateur**

Si l'employeur à toute la légitimité pour exiger une utilisation professionnelle de l'ordinateur, les moyens dont il dispose pour s'en assurer ne sont pas illimités. Ainsi, proportionnalité des moyens et loyauté sont à nouveau exigés. On peut comprendre qu'un employeur puisse être tenté de mettre en place des logiciels espions sur les postes informatiques des salariés afin de s'assurer qu'ils sont bien entrain de travailler. A titre d'exemple, on peut citer les "keyloggers". Ces logiciels sont des dispositifs de surveillance qui se lancent automatiquement à chaque démarrage du poste informatique, et ce à l'insu de son utilisateur. Ce type de dispositif doit faire l'objet d'une information préalable des IRP au titre de l'article L.2323-32 du Code du travail, et d'une information individuelle des salariés concernés[6]. De tels dispositifs doivent être déclarés auprès de la CNIL, pour laquelle ces derniers ne peuvent se justifier que pour de forts impératifs de sécurité. A défaut, les preuves obtenues par l'employeur seraient irrecevables dans un litige l'opposant à un salarié. En outre, depuis la loi d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011, la CNIL a rappelé que le fait d'utiliser des *« dispositifs de captation de données informatiques à l'insu des personnes concernées »* est puni de 5 ans d'emprisonnement et de 300 000 euros d'amendes[7].

Si l'employeur ne peut contrôler par n'importe quel moyen l'utilisation qui est faîte de l'ordinateur, il peut être légitime à le faire en raison des abus susceptibles d'être commis. S'il est déconseillé d'interdire totalement l'utilisation à titre personnel de l'outil professionnel - au risque de voir cette décision condamnée pour non-respect du principe de proportionnalité[8] -il semble important, au vu des nombreuses tentations que suscite le web, d'en limiter l'accès. Cela pourra ainsi éviter à certains de se voir licencier pour faute grave. En effet, il est acquis que l'utilisation personnelle et abusive d'internet à partir de l'ordinateur professionnel est un cas de licenciement pour faute grave [9]. Cette sanction trouve son fondement dans la violation des obligations contractuelles du salarié. Ainsi, dans un arrêt du 18 mars 2009 la Cour de cassation a considéré qu'un salarié pouvait être licencié pour faute car il avait usé de la connexion internet de l'entreprise à des fins non professionnelles pour une durée d'environ 41 heures sur un mois[10].

1 Cass. soc., 17 juin 2009, n° 08-40.274, FS P+B, Sté Sanofi Chimie c/ M. Guzzi et a. : JurisData n° 2009-048669

2 S. MAILLARD « L'administrateur réseaux peut ouvrir les messages personnels des salariés dans le cadre de sa mission » *La Semaine Juridique Edition Générale n° 39, 21 Septembre 2009, 263*

3CA Paris, 11e ch., sect. A, 17 déc. 2001 : JurisData n° 2001-166690 ; JCP G 2002, II, 10087, note M. Vivant et J. Devèze

4S.MAILLARD *(op-cit)*

5Art. 226-15 du Code pénal

6Art. L.1222-4 du Code du travail

725 févr. 2013 « Keylogger : des dispositifs de cybersurveillance particulièrement intrusifs - CNIL - Commission nationale de l'informatique et des libertés » **www.cnil.fr/la-cnil/actualite/article/article/keylogger** des-dispositifs-de-cybersurveillance-particulierement-intrusifs/ 2/2

8Art. L.1221-1 du Code du travail

9Cass. soc., 9 juill. 2008, n° 06- 45.800

10Cass. soc., 18 mars 2009, n° 07-44.247 : JurisData n° 2009-048024