Celui qui voulait surfer à l'insu de son employeur...

Rosier, Karen

Published in:
Bulletin social et juridique

Publication date:
2009

Document Version
le PDF de l'éditeur

Celui qui voulait surfer à l'insu de son employeur...

La Cour du travail d'Anvers a rendu, le 2 septembre 2008, un arrêt inédit[1] comportant une analyse détaillée des implications de l'application de la CCT n° 81[2]. Un contrôle opéré par le responsable du département ICT de l'entreprise avait mis en évidence une utilisation intensive de l'internet et de l'e-mail à des fins privées par un employé qui se révéla être, après individualisation des données, un autre membre du département ICT.

La Cour vérifie, de la mise en place du système contrôle jusqu'à sa mise en œuvre dans le cas d'espèce, si les conditions définies par la CCT ont été respectées. Deux points tranchés de la décision nous interpellent plus particulièrement.

Tout d'abord, la Cour se prononce sur le champ d'application de la CCT. En effet, les connexions internet mises en causes avaient été réalisées via une connexion réservée au serveur mail et non au moyen de la connexion internet à disposition du travailleur de sorte que l'employeur soutenait que la CCT ne s'appliquait pas. La Cour trouve appui sur l'article 2 de la CCT pour considérer que ce qui importe n'est pas la technologie utilisée mais le fait que le contrôle porte sur des communications réalisées dans le cadre ou, du moins, pendant la durée du travail.

Ensuite, la Cour se penche sur la problématique de la finalité des contrôles. On rappellera que la CCT n'autorise les contrôles que pour certaines finalités[3] et que si elle permet une individualisation immédiate des données pour identifier l'auteur du comportement problématique, elle exclut toutefois cette possibilité lorsque le contrôle vise à vérifier que les travailleurs respectent les consignes de l'employeur relatives à l'utilisation des outils de communication. Dans ce cas, l'employeur doit informer les travailleurs de l'existence de l'anomalie et les avertir qu'une individualisation des données de communication électroniques aura lieu si l'anomalie se répète[4]. Or ce qui était reproché en l'espèce au travailleur, c'est de ne pas avoir respecté le règlement IT en vigueur dans l'entreprise tandis qu'il n'était pas contesté qu'il avait été procédé lors du contrôle à une individualisation des données sans phase d'information préalable.

La Cour retient qu'en l'espèce, le contrôle poursuivait à la fois une finalité de contrôle du respect de ce règlement interne et une finalité de protection de la sécurité et du bon fonctionnement du système informatique de l'entreprise. À suivre la Cour, le simple fait que le contrôle vise au moins une finalité pour laquelle aucune phase d'alerte préalable n'est exigée autoriserait une identification immédiate du contrevenant, et ce nonobstant les conséquences que l'on pourrait tirer par la suite du constat d'une éventuelle violation des règles d'utilisation internes à l'entreprise dans le chef de la personne identifiée.

Notons encore que le travailleur faisait valoir que, sans en avoir averti son personnel, l'entreprise utilisait un système du contrôle dont une fonctionnalité permettait à tout moment une individualisation du contrôle de sorte qu'il était illusoire de penser que l'entreprise s'en prive, quelle que soit par ailleurs la finalité du contrôle. La Cour balaie l'argument en constatant notamment qu'à supposer même qu'il y ait eu une irrégularité dans la procédure de contrôle, celle-ci n'entacherait pas la fiabilité de la preuve ni ne priverait le travailleur d'un procès équitable. Elle entend ainsi faire application de la jurisprudence dite « Antigone » de l'arrêt de la Cour de cassation dans un litige social pour prendre en compte une preuve obtenue éventuellement de manière irrégulière[5].

KAREN ROSIER
Assistante à la faculté de Droit des FUNDP
Chercheuse au Centre de Recherches Informatique et Droit (Crid), FUNDP
Avocate au barreau de Namur

1 C. trav. Anvers (section de Hasselt), 2 septembre 2008, RG 2070230, Inédit.

2 CCT n°81 du 26 avril 2002 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau, rendu obligatoire par l'A.R. du 21 juin 2002, M.B., 29 juin 2002.

3 Définis à l'article 5, §1 de la CCT.

4 CCT n° 81, article 16.

5 Le Tribunal se fonde plus particulièrement sur l'arrêt du 10 mars 2008 (Cass., 10 mars 2008, RG n° S.07.0073.N, www.cass.be). Pour une autre application à un litige social, voy.: Trib. trav. Gand, 7e septembre 2008, R.G n° 175054/06, www.cass.be.