

# CYBER-SURVEILLANCE IN COMPANIES: A SENSIBLE BALANCE BETWEEN EMPLOYEES AND EMPLOYERS INTERESTS

New technologies offer to companies tools of surveillance and optimisation of the productivity of employees. However, their efficiency is conditioned by the respect of a balance between rights and individual liberties of the employees on the one hand and prerogatives and interest of the employer on the other hand.

Companies make means of communication and telecommunication available for their employees: it is a factor of productivity and risks. It is therefore necessary for a firm to take adequate measures in order to ensure that its employees will reasonably use information technology. It is as well necessary that companies can sanction employees' faults committed through these means.

## ► Setting up cyber-surveillance's tools

It is now accepted that employees can use IT tools of a firm for personal use. However such a use must interfere neither with the normal functioning of the firm, nor to its productivity<sup>1</sup>. In any case, companies would not be allowed to limit access to Internet and to e-mails only for professional purposes<sup>2</sup>. It is therefore necessary to ensure that use of IT tools provided to employees does not interfere with the interest of companies and does not interfere with its image [e.g. downloads of illegal protected content, connection to websites which content is in contravention with public order, spamming, etc...]. Cyber-surveillance intervenes therefore through diverse proceedings, such as control of the mail exchanges, daily Internet connection, tracking of the connections, filtration of messages, and more recently biometry or even geolocalisation.

Since such procedures allow collection of personal information, Article L121-8 of the French Labour Code, following the dispo-

sition of data Data Processing, Files and Liberties Act of January 6<sup>th</sup>, 1978, imposes to inform the employee of such a procedure. The IT Charter (equivalent of IT Guidelines), to be annexed to the internal regulations<sup>3</sup>, enables to ensure this information process. The purpose of this Charter will be to present and draw the boundaries of the use of the IT means provided by companies<sup>4</sup>. The Labour Code imposes the employer to inform and consult the firm Comity before setting up tools and technique to control the employees' activity in companies. With regards to IT in firm, collective consultation has to be the rule.

## ► A possible hold in check

The use of cyber-surveillance's tools can result in a breach of rights and individual liberties of the employees and especially of their right to privacy<sup>5</sup>. Setting up such tools must therefore be framed by some bulwark. When tools for collection of and treatment of personal data are used, employers have to respect the disposition of the Data Processing, Files and Liberties Act in addition to the Code of the Labour Code. Violation of one of these dispositions can result in a breach of procedure and all burden of proof can be seen as invalid. It has been decided by the Cour de cassation<sup>6</sup> (French Supreme Court) that an employee cannot be sanctioned if he refuses to comply with the automated system which controls the entries and exits of em-

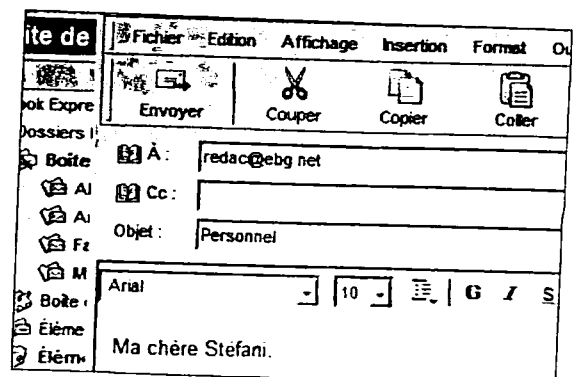
ployees, but which has not been declared to CNIL as provided by the Data Processing, Files and Liberties Act, even if this employee has been dully informed. One can therefore understand the importance of the respect of legal disposition directly or indirectly applicable to settings of cyber-surveillance.

## ► How to maximise its cyber-surveillance tools?

Cyber-surveillance tools are not considered as lawful due to the only fact that employees have been informed of



**It is now accepted that employees can use IT tools of a firm for personal use**





DR

their settings and that the firm Comity has been duly consulted. Indeed, the risk of privacy violation of employees means that cyber-surveillance means must not be disproportionate. Law imposes such an obligation as it states that: "No one may introduce restriction to personal rights and individual and collective liberties that are out of proportion to the result sought."<sup>1</sup> This requirement of proportionality applies to the selection of cyber-surveillance tools, as well as to the conditions of their setting. The most outstanding example is the surveillance of the mails received and sent by employees from its professional e-mail box.

The main foundation of e-mail surveillance is security of the firm network on the one hand (especially due to the multiplication of viruses and Trojan Horses using e-mails), and on the other hand the prevention of any divulgation sensible and confidential information, as well as the analyse of the efficiency of the employees work. Since employees can use the professional e-mails for personal purposes, to what extend can the network administrator - or the head of the firm - can act on an infected e-mail or on an e-mail containing illegal content? Case law of the *Cour de cassation* does not solve directly this question. However, since the Nikon case it is clearly established that the employer cannot be aware of the personal e-mails contents sent or received by the employee through its professional e-mail box. Indeed, employee benefit from a right to privacy which implies the secret of its correspondences.

► **Some borders remain blurred...**

One can still wonder how to distinguish between a personal message and a professional message... While the Forum des Droits de l'Internet considers that mails where the heading contains the word 'Personal' are personal e-mails<sup>2</sup>, the Court of Appeal of Bordeaux states that the principle stated by the Nikon case, has qualified as personal messages, messages sent or received by an employee from the address of its firm solely because this e-mail address was available only from the computer of this employee<sup>3</sup>

and individualized messages were therefore sent and received only from this e-mail address. Let's hope that case law will quickly determine a more flexible criteria.

In the meantime, the network administrator plays a role of fundamental importance since he can have access to the whole range of information stocked in the computers of the firm, included those information which regard Internet connection and e-mails exchanges. It has to be noted that the network administrator might have to respect professional secrecy. Cnil considers that the network administrator cannot disclose information to which he has an access and especially those information which relate to privacy or of secrecy of correspondences<sup>4</sup>. However, the principle of the professional secrecy of the network administrator is not clearly established. The engagement of this professional remains the best protection of computing system of the firm.

HR have to come back to cyber-surveillance because of the evolution of the regulation with regards to this issue. The law dated 4 August, 2004, which modifies the Data Processing, Files and Liberties Act states that companies can designate a correspondent to the protection of database and can therefore benefit from a simplification of their obligations of declaration. Acting as a kind of "local take over" from CNIL, this correspondent could simplify a lot the HR task and more generally the management of the firm, especially with regards to cyber-surveillance. ■

<sup>1</sup> Report of the French Data Protection Authority (CNIL) - "Cyber-surveillance sur les lieux de travail" - March 2004.

<sup>2</sup> Cour d'appel de Versailles, March 18<sup>e</sup>, 2003.

<sup>3</sup> Article L122-34 of the Labour Code, internal regulation determines the conditions of application of the rules dealing with security and discipline.

<sup>4</sup> Article L432-2-1 of the Labour Code.

<sup>5</sup> Article 9 of the Civil Code.

<sup>6</sup> Cour de cassation, chambre sociale, April 6<sup>e</sup>, 2004.

<sup>7</sup> Article L 120-2 du Labour Code.

<sup>8</sup> Cour de cassation, Chambre sociale, October 2<sup>e</sup>, 2001.

<sup>9</sup> Forum des Droits de l'Internet, Report "Relations de travail et Internet", September 17<sup>e</sup>, 2002 ([http://www.forum-internet.org/telechargement/documents/rapp-rti-20020917\\_en.html](http://www.forum-internet.org/telechargement/documents/rapp-rti-20020917_en.html)).

<sup>10</sup> Cour d'appel de Bordeaux, July 1<sup>e</sup>, 2003

<sup>11</sup> Report of the French Data Protection Authority (CNIL), op.cit. 1.



**Julie Jacob & Benjamin Jacob**

