WHAT CYBERSURVEILLANCE IN THE WORKPLACE

As part of the exercise of their professional activity, employees have a computer which, most often, is connected to the Internet and has an e-mail address. electronic warehouse.

The employer generally tolerates the use of different IT tools for purposes other than professional ones. In any case, this use must remain reasonable. sound and not affect the smooth running of the business.

What are the interests involved?

The **employee** has the right to respect for his private life at his place of work. Respect for private life includes, in particular, the secrecy of correspondence. But the employee must execute terminate his employment contract and also has a duty of loyalty to his employer: it must not prejudice the proper functioning of the company.

The **employer** has the right to protect his property: confidential data must not be divulged or communicated, his computer system must be able to function. work normally (avoid viruses, saturation or engorgement phenomena, etc.).

Obligation to inform employees about the use of IT tools

The employer must inform the limits and the use for personal ends that he tolerates of IT tools as well as the systems put in place and the methods of control of these tools: it must thus say if it authorizes employees to use an electronic messaging system and / or to surf the Internet and / or to create and have personal files. nels.

Without being exhaustive, it may be the following information:

- the use of these tools for private purposes (periods and durations of use, how information is stored on the hard drive, etc.);
- the reasons and objectives of the control, the nature of the data collected, scope and circumstances of the controls, the recipients of the data;
- the implementation of tools blocking websites and / or chain messages or files that are too large;
- the method of collection and use of surveillance data;
- who is authorized to use the surveillance data and under what circumstances;
- the retention period of the data resulting from the surveillance;
- the decisions that can be taken by the employer during an inspection;
- the role of employee representatives in the implementation of the monitoring policy;
- the terms and conditions of employees' right of access to their data.

For the sake of transparency and loyalty in labor relations, the National Commission recommends that the employer adopt a charter, internal regulations or any other document relating to the use of IT tools as well as to the control methods.

When and how can the employer control IT tools?

Even in the event of a total ban on the use of IT tools for private purposes, the employer does not have the right to continuously monitor the use, with some exceptions. legal.

Whatever the IT tool, monitoring must always be **graduated** ("progressive Kontrollverdichtung"): the employer must first carry out monitoring ad hoc during which employees are not identified. If clues and suspicions are detected, then the employer can intensify his surveillance and carry out analyzes individualized where employees are identified.

Controlling email usage

The employer must respect the secrecy of correspondence:

Any incoming or outgoing e-mail from a workstation made available by the employer is presumed to be received or sent within the framework of the professional relationship, that is, the recipient or sender is deemed to be the employer.

But, this is a simple presumption: the message may have the character of a private correspondence.

In this case, the employer cannot open the personal e-mails of his employees, under penalty of violating the secrecy of correspondence, which constitutes a criminal Offence. Case law also holds that this prohibition on reading private messages applies even in the event that the employer has prohibited a use non-professional computer tools.The principle of the secrecy of correspondence can however be lifted in the context of a criminal investigation or by a decision of justice.

Control of professional messages:

Anything that is not identified as "personal" is deemed to be professional, so that the employer can access it.

The latter can quite get traffic and logging data like volume, frequency, size, format of their attachments. This information is controlled without identifying the person concerned.

In the event that irregularities are observed, he can in a second phase proceed to the identification of the persons concerned and check the content of the emails. professionals.

Recommendations on the use of messaging:

- Distinguish between private and business emails
  To prevent the employer from undermining the confidentiality of personal messages, the National Commission proposes:
  - the installation of a double mailbox separating personal messages and professional messages;
  - archiving personal messages in a folder called "personal";
  - employees indicate the private and personal nature in the subject of messages and encourage their correspondents to do the same.
- Can the employer have access to the messaging system in the event of the employee's absence to ensure business continuity?
  After having informed the employees and the representative bodies, it is suggested to:
  - set up an automatic out-of-office response to the sender with an indication of the people to contact in the event of an emergency;
  - designate a substitute who has a personalized access right to his colleague's mailbox: he can read and process professional messages, but he cannot not read messages identified as personal;
  - forward all incoming messages to an alternate.

Each employee must know the identity of his substitute.

- In the event of the employee's final departure, it is recommended that:
  - the employee who leaves the company transfers all current professional documents to a predefined person (for example, his supervisor);
  - he certifies having given his employer all professional documents;
  - he can copy e-mail messages and other documents of a private nature to a private medium and then delete them from the company's servers;
  - the employer undertakes to block all computer accounts and to erase the employee's mailbox (es) upon departure;
  - people who send a message to the blocked address are automatically notified of the deletion of the email address and are given an address alternative.

Control of internet usage

Internet access is provided for professional reasons.

The employer can set the conditions and limits for using the internet for private purposes. He must clearly inform employees in advance of the systems and the control methods.

He cannot individually supervise an employee without first having carried out overall and non-personal supervision. So he can make a list addresses of sites consulted globally over a certain period, without identifying the authors of the consultations. If he has any clues about prejudiced internet use target for the company by spotting an abnormally long duration of Internet consultation or the mention of addresses of suspicious sites, he can then take the necessary measures. appropriate control measures and then pass in a second stage to individualized supervision.

The National Commission recommends the implementation of preventive means of protection taking into account the risks of viruses presented by this access, such as, for example, filtering of unauthorized sites, the prohibition of software downloads or the prohibition to connect to discussion forums ("chat").

Control of computer media and log files

In general, all documents and files created by an employee are supposed to be of a professional nature. But the employee can, within reasonable limits, create documents or files that it identifies as personal, by virtue of the principle of privacy in the workplace.

The monitoring of computer media and log files should not be done in the form of individualized analysis but should be graded in pace and the scope of the data checked.

Regarding files or documents identified as private, the employer cannot access them without the presence of the employee concerned. The latter must have the possibility right to oppose the opening of a private file and must be informed of this possibility at the time of the control.

The National Commission therefore recommends that the employer take measures to ensure that the company's electronic documents are accessible. during the employee's absence without it being necessary to open the employee's "personal" files.

Finally, it is recommended that at the end of his employment, the employee is entitled to obtain a copy of the documents kept in his private file and that he has the possibility of deleting his personal files, if applicable, in the presence of a representative of the employer.

Last update 05/09/2019

National Commission
for data protection

15, Boulevard du Jazz
L-4370 Belvaux

Phone. : (+352) 26 10 60 -1