

# NEW TECHNOLOGIES AND EMPLOYMENT

TELEMONITORING AND CYBERSURVEILLANCE OF EMPLOYEES



**Jason BENIZRI**

June 2009

Since the turn of the century, there has clearly been a simplification as well as a multiplication of ways in which companies monitor and supervise employees: videos, badges, biometric devices, internet connection history, etc.

In parallel, employees have been given access to computer system tools to increase productivity and their degree of autonomy, and have generally been cautioned not to confuse working time and personal time when using these tools, which, being most often connected to the Internet, could lead to many distractions.

Nevertheless, what this large autonomy hides is the “ultra-subordination” generated solely from an employee’s use of a computer, cellular telephone or Internet access while at work. Computerization and automation have resulted in the unlimited traceability of employee’s acts and gestures and the disappearance of the right to turn a blind eye to such acts and gestures.

The risks associated with this true societal transformation are many: how can the collected data be used for monitoring employees? Has the right to monitor become an obligation to do so? What effect does the multiplication of monitoring methods have on employees?

## **1. The use of the collected data: procedures and safeguards**

Today, French law and case law delineate in an extremely strict manner how the data, stemming from systems used by companies to monitor employee activity, can be collected and processed.

Respect for the employee’s private life, which also holds true during working hours and at the place of work, naturally serves as a limit to investigations and surveillance, even though the computer or cellular telephone, for example, are the company’s property.

In any event, to render any evidence obtained by means of ICT (Information and Communication Technologies) enforceable, preliminary procedures must be respected.



### 1.1. The preliminary procedures

#### a. The principle of loyalty

The employment agreement is, first and foremost, a contract. The principle of loyalty therefore prevails. Evidence obtained through trickery is not considered admissible (concealed telephone recording, hidden cameras, etc.). Only methods of which employees have knowledge are enforceable.

Please note, however, that inadmissible means of obtaining evidence are first prohibited practices that may even be punished by law: for example, opening an employee's personal e-mail is not only inadmissible in court; it is also – and primarily – a violation of secrecy of correspondence, i.e. a criminal offense punishable by one year imprisonment and 45,000 Euros in fines (Art. 226-15 of the French Criminal Code).

Further, contractual loyalty requires the employer to first inform each employee individually of the existence of an information collection system concerning him personally. In other words, the employee must know whether he is being filmed, whether every move is closely monitored, etc. (Art. L.1222-4 of the French Labor Code).

#### b. The principle of collective information

In addition to informing each employee individually, the employer must inform the Works Council before any *“means used to monitor employee activity”* is implemented within the company (Art. L.2323-32 paragraph 3 of the French Labor Code).

This rule applies even if the system is not aimed at monitoring the employees themselves (but clients, for example). The employer is bound by this obligation to inform the Works Council once there is even a theoretical possibility that employees may be monitored.

When personal data is processed, the company must inform the CNIL (French Data Protection Agency) thereof and declare any collection and processing of information that has been carried out. The CNIL strictly controls the purpose of this automated processing and, in particular, tracks down the circumvention thereof (for example, GPS systems aimed at locating company cars cannot incidentally be used to track employees using these cars without their full knowledge).



## 1.2. The limits of use of collected data: distinction between “personal” and “professional”

Accessing an employee’s computer, reading his e-mails, opening his computer files, examining his Internet connection history or viewing his acts and gestures in a day comes very close to affecting certain of his individual liberties.

Article L.1121-1 of the French Labor Code states that *“No one may restrict the rights of individuals or individual and collective liberties if the means is not justified by the nature of the job to be performed or is not proportionate to the goal sought”*.

As specified by the Labor Chamber of the French Supreme Court, impairment of the rights of individuals is therefore possible if it is in the company’s interest and in moderation according to the case in question.

### a. Opening an employee’s e-mails or files

There is a presumption that, during working hours and at the place of work, an employee will use the ICT made available to him for professional reasons. Because it is not possible to prohibit occasional personal use of these tools, the employer must be able to easily identify what falls within the scope or not of an employee’s private life.

This is the reason why an e-mail or file labeled “personal” cannot be opened, unless there are exceptional risks or events, and unless the employee is present or his presence has been duly requested. French case law strictly interprets the notion of “exceptional risk or event”. For example, the discovery of erotic photographs on an employee’s hard drive is not considered such a risk or event (Cass. Soc. May 17, 2005).

As such, it is the employee himself who must first specify the personal nature of the e-mail or file by indicating, for example, “Personal” as the subject matter. Reading the subject line in an e-mail or the name of a file should also allow the reader to identify that said email or file is personal (for example, a file labeled “vacation photos” is clearly personal in nature).

Finally, as respect of one’s personal life does not signify impunity, courts may be requested to order the opening of or access to an employee’s personal e-mails or files if, in particular, he is strongly suspected of acts of unfair competition (Cass. Civ. II April 9, 2009 and Cass. Soc. June 10, 2008).



### b. *Monitoring activity*

Employees are sometimes highly tempted to use the tools made available to them for personal purposes, and occasionally in an abusive manner.

The implementation of an “Information Systems Charter” may prove very useful in defining early on the code of general conduct that employees must adopt with regard to their use of ICTs provided by the company. However, in principle, violation of such a charter is not sufficient to justify a disciplinary sanction.

This being said, may the employee complain if his employer does inspect, for example, his Internet connection history? Pursuant to case law, Internet connections made by an employee during his working hours are presumed to be professional in nature and therefore, the employer may investigate them outside his presence (Cass. Soc. July 9, 2008).

Nevertheless, it must be kept in mind that it is the abuse that is sanctioned, not the personal use itself. Personal use of a company’s ICTs, therefore, cannot serve as a pretext to make up for a lack of evidence against an employee the company would like to dismiss.

The same can be said for the inspection of an employee’s telephone bills. The French Supreme Court held that an employee cannot ignore the fact that he can be blamed for numerous personal calls, in particular to telephone dating services, made from the cellular telephone provided by the employer and generating significant extra costs (Cass. Soc. January 29, 2008).

## **2. Use of ICTs and societal transformation: the obligation to monitor and the role of the CHSCT (Health and Safety Committee)**

### **2.1. From the right to monitor to the obligation to monitor**

When an employer makes available to his employees a computer system tool, and especially an e-mail account that has, before the company’s logo, the name of the employee and the name of the company, it is important that an efficient system of control is implemented to prevent things from getting out of hand, thereby implicating the company (Cass. Soc. June 2, 2004, concerning an employee who had sent an anti-Semitic e-mail to an Israeli company from his professional e-mail account).



In fact, as abuse of one's position is very strictly defined, the employer may easily be found civilly liable for a harm caused to a third party by his employee (Cass. AP. February 25, 2000). The employer will be able to subsequently look to his employee for indemnification solely in the case of a *faute lourde* (gross misconduct) (Cass. Soc. May 6, 2009).

### 2.2. Towards systematic consultation of the CHSCT?

Employee surveillance and monitoring may result in a true modification of their behavior.

Even if what spontaneously comes to mind is a qualitative improvement in behavior, it must be noted that the employees will feel as if they have been placed under even more stress, which could have consequences on their working conditions.

As such, consultation of the CHSCT on certain contemplated systems to monitor employee activity should be considered as mandatory prior to any implementation, if they are likely to generate psychological pressure with repercussions on the working conditions (Cass. Soc. November 28, 2007).

It is therefore now preferable to first consider the consequences of using a monitoring system and strictly weigh the effects thereof against the goals sought.

Note, however, that making available ICTs should not veer towards a system of "permanent standby duty" in which consulting e-mails and Smartphones, which can be done at any time from any place (including during the holidays, vacations, weekends, etc.), will seriously affect the employees' private life and, potentially, their psychological balance.

Certain categories of employees must systematically be protected against these types of abuses, failing which, the employer might be liable for work-related accidents, psychological problems, or even in certain cases moral harassment. It appears that different services performed should imply different levels of interference in an employee's personal life.

[Click here to consult the e-newsletter](#)

You can also copy this link: [http://79.141.9.44/newsletter/index.php5?id\\_lettre=4507](http://79.141.9.44/newsletter/index.php5?id_lettre=4507)

---

Articles published in **Soulier's June 2009 e-newsletter**

**Competition & Antitrust:**

Abuse of a dominant position: record fine imposed upon Intel by the European Commission by **Stéphanie Yaviordios**

**Tax Law:**

French “*sociétés de personnes*”: a tax optimization instrument to be used wisely by **Philippe Drouillot**

**Moral Harassment:**

Criminalization of moral harassment: when subjectivity becomes presumption, how to defend employers by **Stéphanie Rébé and André Soulier**

**New Technologies and Employment:**

Telemonitoring and cybersurveillance of employees by **Jason Benizri**

**Labor & Employment:**

Continuing coverage under company-sponsored supplemental death and disability insurance plans for the unemployed: new obligations for companies as of July 1, 2009 by **Véronique Vincent**

**Business Immigration:**

Work permits for non-EU interns: conditions for issuance by **Sandra Vreedenburgh**

**International Perspective:**

An Overview of Foreign Direct Investment Law in China contribution authored by **Thomas Keenan**

---

Soulier's e-newsletters are available on our website  
[www.soulier-avocats.com](http://www.soulier-avocats.com)

E-mail  
[info@soulier-avocats.com](mailto:info@soulier-avocats.com)