



# **CYBER-SURVEILLANCE IN THE WORKPLACE**

A REPORT PRESENTED BY

Mr Hubert Bouchet, Delegate Vice-Chairman of the CNIL

Adopted by the Commission Nationale de l'Informatique et des Libertés (CNIL)  
during its session of February 5, 2002

Authors: Mrs Sandrine Mathon, Member of the Legal Department  
Mr Jean-Paul Macker, Officer in the Computer Expertise Department



## **GLOSSAIRE**

staff representatives : représentants du personnel

union representative : du syndicat

collective bargaining: negotiation collective

employment contract : contrat de travail

a decision dated x/xx/xxxx : un arrêt, un jugement du x./xx/xx :

at the computer age : a l'heure des nouvelles technologies

personal data : données nominatives

in-house privacy controller : le représentant informatique et libertés



<a href="#">Surveillance limited by law</a> .....	4
<a href="#">Cyber-surveillance at the heart of the work process</a> .....	5
<a href="#">The report for examination and public consultation adopted by the CNIL on March 8, 2001</a> .....	6
<a href="#">A concern shared at the European level</a> .....	7
<b><a href="#">I. General principles and implemented legal provisions</a></b> .....	<b>8</b>
<a href="#">. Prior information, a condition of transparency:</a> .....	8
<a href="#">. Collective bargaining:</a> .....	8
<a href="#">Proportionality:</a> .....	9
<b><a href="#">II. Encouraging collective bargaining and pedagogics</a></b> .....	<b>10</b>
<a href="#">. Prejudice No. 1: the personal computer, as such, placed at the disposal of the users in their workplace, is supposed to be protected by the Data Protection Act, and therefore, belongs to the area of the private life of the employee.</a> .....	10
<a href="#">. Prejudice No. 2: prior information for the employees is sufficient</a> .....	10
<b><a href="#">III. Conclusions</a></b> .....	<b>11</b>
<a href="#">1. Checking Internet connections</a> .....	11
<a href="#">2. E-mail monitoring</a> .....	11
<a href="#">3. Log files</a> .....	12
<a href="#">4. The role of network administrators</a> .....	13
<a href="#">5. The use of Information Technology by employee’s representative bodies</a> .....	13
<a href="#">6. A yearly Privacy Evaluation Statement</a> .....	13
<a href="#">7. Appointment of an in-house privacy controller</a> .....	14
<b><a href="#">APPENDIX</a></b> .....	<b>15</b>
<a href="#">Monitoring electronic communications</a> .....	15
<a href="#">Draft proposals:</a> .....	15
<a href="#">E.mail monitoring</a> .....	16
<a href="#">Draft proposal</a> .....	16
<a href="#">Daily record files and firewalls</a> .....	17
<a href="#">Annual Privacy evaluation statement</a> .....	17
<a href="#">Appointment of an in-house privacy controller</a> .....	18
<b><a href="#">GLOSSAIRE</a></b> .....	<b>2</b>



In his report entitled “Public liberties and employment”<sup>11</sup>, Professor Gérard Lyon-Caen recalled that the debate concerning the employee’s privacy within the company, which calls into question both the relationship of subordination characterising the contract of employment and the irreducible part played by the liberty of men and women in a democratic society, was no new issue. However, he stressed that the development of technical means of control, coupled to new technologies, has made it necessary to bring it up again. “*The dividing line (between the relationship of subordination and private life) can no longer be traced at the exit from the workplace and the end of working hours. Everything has become more complex and more blurred*”. The author of the report evoked “*a new policy area, a genuine technological order which has nothing in common with former systems of subordination, since the employee is no longer under the orders of someone. He is monitored by the machine, or at the most by himself, by everyone and by no-one*”. With regard to electronic mail, Professor Lyon-Caen announced : «*the strict respect of correspondence is out of date in this field*”. This was in 1991 ...

### **Surveillance limited by law**

Following that report, the law of 31<sup>st</sup> December 1992 set the markers for a “Data Processing and Liberties” Act within companies : the principle of proportionality (“no-one may introduce restrictions to personal rights and individual and collective liberties that are out of proportion to the result sought” - Art. L 120-2 of the Labour Code ); consultations with the Works Committee when new technologies are introduced ( Art. L 432-2 ); prior information given to employees (Art. L 121-8 ).

These principles and rights are echoed in the law dated 6<sup>th</sup> January 1978 which lays down that all processing of personal data must be notified to the CNIL, that employees must be informed of its existence and characteristics and that they must have access to information concerning them.

It is on the basis of these principles that, as early as 1984, the Commission established, through a recommendation which was to lead to a simplified standard, rules for the use of automatic telephone switchboards which enable the employer to find out the telephone numbers dialled by an employee on his telephone.<sup>22</sup>

These same principles are applied with regard to video-surveillance within the company and the Social Chamber of the *Cour of Cassation* (the French Supreme Court) was to give substance to these principles: no means of evidence may be used by the employer against employees if the means of control was installed without their knowledge.

However, up to now, whether it is a matter of automatic telephone switchboards, badges and access controls or video-surveillance, the surveillance mainly concerned the presence or physical location of the individual. In a word, the technologies were still on the periphery of the working process.

Undoubtedly, the development of telephone monitoring in the workplace signalled a change. The increase in the number of telephone services and call-centres led companies to monitor the quality of service, i.e. that of the response provided by the employee. On this point, the CNIL has developed a body of practical recommendations, which appears to be widely respected.

However, with the emergence of IT and in particular the introduction of the Internet into companies, a genuine migration of the technologies has occurred, from the periphery to the very centre of the work

---

<sup>1</sup> *Report to the Minister of Labour, Employment and Professional Training, December 1991, La Documentation Française.*

<sup>2</sup> *cf. 5<sup>th</sup> activity report by the CNIL, 15<sup>th</sup> activity report, p. 74.*



process as such.

## **Cyber-surveillance at the heart of the work process**

The increasingly systematic recourse to new network technologies has a considerable effect on employer/employee relationships.

More and more, the information available to companies is digitalised, whatever its nature. From the moment that it is computerised and likely to be accessed by the Internet or Intranet, the risk of undue access to this information is real. For the company, the new information and communication technologies will naturally cause new problems with regard to the security of staff files, the management of orders, manufacturing secrets, etc. For employees, the difference in nature between IT and all that went before lies in the new capacity of technology to preserve all the traces left by the person who uses it.

In this way, technology raises again questions which had been settled in a former context. An electronic mail, which the employee thinks he has deleted, may have been saved on a message service server or on a magnetic backup medium. And this employee would be deceived if nobody had told him that the message he received from his spouse to remind him not to forget to do some shopping before returning home, and that he had immediately deleted from his e-mail, had been stored without his knowledge.

The balance is difficult to establish.

The expanding of the company's horizon, through the Internet, and the use of information networks, make companies more vulnerable to external computer attacks. The setting up of security measures constitutes, in this respect, an essential requirement to avoid intrusion and to protect confidential documents, manufacturing secrets or simply the company files. However, the very aims of these security measures are to keep traces of information flows, which are directly or indirectly identified by name, in order better to avoid risks more efficiently and identify the origin of problems.

Moreover, these technologies which are simultaneously ergonomic, easy to use and sometimes playful, may induce companies into making sure that their employees do not abuse their use for purposes which are not related with their professional activity. The implementation of such productivity checks of the "cyber-worker" will be all the more frequent that any network architecture has the effect of geographically separating employees from their hierarchical superiors.

The change has occurred at a steady rate. First of all, we had the foreman, an identifiable person who is responsible for checking the physical presence and activity of the employee in the workplace. Then, we had "electronic foremen" responsible for checking physical presence : access badges. The era of the "virtual foreman" is now dawning. In this era everything can be done outside of the employee full awareness and which, if necessary, enables a professional, intellectual or psychological profile of the "virtual employee" to be established beyond the legitimate checks of employees' security and productivity

An increasing number of companies are adopting "privacy policies" or "information charters"<sup>1</sup> setting out the security measures to be taken and the use that employees may make of the new computer tools made available to them. An examination of these privacy policies, which are very rarely negotiated with staff representatives or their unions, reveals a patent imbalance between the prerogatives of the employer and the rights of employees.

---

<sup>1</sup> privacy policies



The Commission supports such initiatives when the objective of the “charters” or “good practice guides” is to ensure complete information for the users, to make the private or public employees aware of security needs, and to call their attention to certain types of behaviours which might be harmful to the collective interests of the company or the administration.

However, such privacy policies, of uncertain legal status, may miss the objective aimed at when, without pedagogical concerns, all kinds of prohibitions are accumulated, including the generally and socially allowed private use of e-mail and Internet services. Furthermore, some privacy policies do not distinguish legal obligations of the employer from collective negotiation, or even discipline. Finally, no doubt influenced by American companies, employers submit to each employee written engagements for signature, a total abdication of the employee’s rights.

Therefore, some of the privacy policies notified to the CNIL provide for individual analysis and long time storage for any connection data, while the latter may reveal to the system administrator, the departmental head, or the staff manager, the use being made of the tool (the sites consulted, the messages sent).

In the same way, employees are most often required by these privacy policies to use the electronic mail only for professional purposes and some, particularly subsidiaries of American groups, even state that any electronic message sent by an employee must be considered as a “permanent, written record which may at any time be checked and inspected” (sic).

This way of proceeding puts definitely in practice the prior information rule. But in sparing the consultation with the works committee or the employees’ representatives, it may disregard the provisions of the Labour Code. Finally, some provisions implemented by those policies can be wiped out by the judge who, in the last instance, is entrusted with exercising the control of proportionality in the respect of privacy as laid down in Article 9 of the Civil Code.

However, employees still remain largely ignorant of the possibilities of tracing, offered to employers by the new technologies, particularly by accumulating and cross-checking multiple traces and, thus, the necessary balance between the legitimate controls exercised by the company and the employees’ rights does not appear to be ensured in only too many cases.

### **The report for examination and public consultation adopted by the CNIL on March 8, 2001**

This inventory has led the CNIL to undertake a study of all these questions with a view to suggesting to companies and user employees the adoption of a balanced set of rules, like data protection authorities did when former technologies, badges, automatic switchboards and video-surveillance, etc., appeared.

After having consulted computer experts, and particularly network experts, as well as union organisations of employees (CGT, CFDT, FO, CFTC and CGC) and of employers (MEDEF and CGPME), the CNIL drew up a study report submitted to public consultation around the four most frequently asked questions.

- ❑ To what extent do the network technologies differ in nature from the previous tools installed within companies ?
- ❑ To what extent are privacy and individual liberties guaranteed to employees who are linked to their employer by an employment contract, which is primarily a subordinate relationship?



- ❑ How far is the private use of tools made available to employees by their employer allowable?
- ❑ Are there limits to employee monitoring?

All these questions are obviously not within the sole competence of the National Data Processing and Liberties Commission. However, they overlap each other and, taken together, form a natural area of preoccupations, common to both employers and employees, at the emerging times of the information society.

By means of this examination and consultation report, the CNIL wished to offer enlightenment within its areas of expertise: technical aspects, a reminder of the law, overview of case law, a comparative practices study and, with regard to some questions still left to discuss, a few practical recommendations.

This first report, which has been placed on-line on the [www.cnil.fr](http://www.cnil.fr) site, has been very well received and has given rise to various contributions from professional groups, trade-unions representatives, or individuals, all of which accessible on the site. It is for this reason that it has been decided more particularly, that the envisaged conclusions might apply, not only to companies, but also to administrations.

### **A concern shared at the European level**

In parallel to the first trends thus outlined by the CNIL, several of its European opposite numbers voted recommendations in this matter. This, in particular, was the case of the British, Belgian and Dutch Data Protection Commissioners.

To date, the European group of Data Protection Commissioners, founded by Article 29 of the Directive of October 24, 1995, has listed this subject in its work program and will publish a notice, which should demonstrate the complete convergence of opinion between Data Protection Authorities of the Member States of the European Union.

\*

At the end of this first work of deepening and consulting, taking into account the numerous requests for advice, complaints, or requests for information received in the framework of its missions, the CNIL felt it due to share the explanations and the conclusions that follow.



## **I. General principles and implemented legal provisions**

### **. Prior information, a condition of transparency:**

The obligation of prior information is a result of Article L 121-8 of the Labour Code (« No information concerning an employee or a candidate for employment personally may be collected by a means that has not previously been communicated to the employee or the candidate for employment»).

The obligation of transparency inspired the Data Protection and Liberties Act of January 6, 1978, which submits all automatic processing of personal data to a notification to the CNIL prior to implementation, forbids the collection of data by fraudulent, unfair or illicit means, and imposes the obligation to inform the persons concerned, in particular about the addresses to whom the data are to be disclosed , and about the department where right of access and rectification is to be exercised.

Whether it is a result of the provisions of the Labour Code or of the Act of January 6, 1978, prior information, a condition of fairness in data collection, is therefore a necessary condition. It is not sufficient.

### **.Collective bargaining:**

Article L 432-2 of the Labour Code provides that« the Works Committee must be informed and consulted prior to any important project introducing new technologies, when these are likely to affect [...] the employees' working conditions» and specifies that« when the employer plans to implement important and rapid mutations» the plan of adaptation must be submitted« for information and consultation» to the Works Committee, who must be« informed regularly and consulted at intervals» on the implementation of the plan.

Moreover, Article L 432-2 provides that the Works Committee must be« informed and consulted, prior to any decision of implementation in the company, about the means and techniques allowing the control of employees' activities».

The Decree dated May 28, 1982 concerning the Equal Representation Technical Committees of the three Civil Services provides that the committees should have« knowledge of [...] questions and draft texts concerning», in particular« programs of modernisation of working methods and techniques and the effect of these on the situation of the employees».

These texts clearly show that informing the employees of the private or public sector individually does not exempt the persons in charge from the institutionally organized, phase of collective bargaining with the elected staff representatives.

In view of these texts, when the CNIL is requested for advice or is notified a an automatic processing of personal data for employee monitoring purposes, checking that these consultations have been first carried out is the condition of reliability of the draft data processing notified to the Commission.



## **Proportionality:**

« No-one may introduce restrictions to personal rights and to individual and collective liberties that are out of proportion to the result sought».

This principle, now codified in Article L 120-2 of the Labour Code, has been applied both by administrative and legal jurisdictions, particularly in cases of litigation relative to the regularity of internal rules. The Courts control with hindsight the restrictions, the employer may legally place on people's rights and individual liberties, the case law, thus, outlines a, no doubt residual but irreducible, part of personal liberty and privacy in the workplace.

« The employee has the right, even during working hours and at his workplace, to the respect of his privacy; this includes in particular the confidentiality of his correspondence; the employer cannot, without infringing this fundamental liberty, examine the personal messages sent or received by the employee on a computer tool placed at his disposal for work, and this even in the case of the employer having prohibited a non-professional use of the computer». This was recently confirmed by the Social Chamber of the Court of Appeals in a decision dated October 2, 2001.

The principle of protection of the employee's privacy at his workplace is not new and has been stated on numerous occasions, in particular the European Court of Human Rights has had the opportunity to quote Article 8 of the European Convention on preserving Human Rights and fundamental liberties (« Everybody is entitled to the respect of his private and family life, his home and his correspondence») in fields relating to professional life - N. v/ Germany dated November 23, 1992 Case and H. v/United Kingdom dated May 27, 1997 Case.

This principle is, however, more difficult to implement in the computer age. In fact, the convergence phenomenon no longer allows a clear distinction between that which concerns professional life from private life: the computer's hard disc is equally talkative in either case; the electronic message is sent or received in identical technical conditions, whether of a professional or a personal nature, consultations of Internet sites are identical, whatever the nature of the site and the motive for connection.

By nature, the computer can record everything done on the machine, as its memory capacity is an essential element of its performances. It constitutes a veritable« black box» of the digital activities of the user (texts, images, messages sent and received, hidden memory recording the Internet pages consulted in order to optimize the download time and avoid congesting the network, etc.).

As a general rule, be it for ensuring smooth functioning of the computer department, computer security of the company, or user comfort, these« traces» are intrinsically linked to the availability of such technology. Therefore, it is not their existence, but their processing for purposes other than technical, which must be in proportion to the result sought.



## II. Encouraging collective bargaining and pedagogics

Given the evolutionary character of the techniques and the case law surrounding these subjects, it seems suitable to train organisations and users in the various measures of security, of consultation and of communication to adopt. Numerous companies or administrations are already up to it. It is, however, necessary to fight against two received ideas.

**. Prejudice No. 1: the personal computer, as such, placed at the disposal of the users in their workplace, is supposed to be protected by the Data Protection Act, and therefore, belongs to the area of the private life of the employee.**

It is nothing of the sort. A computer placed at the disposal of an employee of the private or public sector, within the framework of working relationships, is the property of the company or the administration and may only subsidiary contain information of a private nature.

It may be protected by a password or a login, but this measure of security is designed to avoid malevolent or abusive uses by a third party; it is not aimed to transform the company computer into a private computer.

Therefore, the company requirements and the necessary respect for the employees' privacy must be conciliated through the collective bargaining and training of the users in computer security.

**. Prejudice No. 2: prior information for the employees is sufficient**

Numerous companies imagine that prior information for the employees is sufficient to avoid any problems and to authorise the use of all means of monitoring. Concerned about guaranteeing against any hazard, they may sometimes be tempted to notify to the CNIL their total security plan.

Such a way of proceeding is not sufficient if the end results are badly defined or badly understood.

It could, mistakenly, make the users believe that they would be subject to the constant monitoring of the company, when, in fact, in many cases, the measures taken are restricted to ensuring the security of the system or its applications, and not an individual or nominative control of their activity.

It may make the employer believe that notifying the CNIL the whole of its security system would authorise it to infringe on what is left of the respect of privacy and individual liberty of the employee in the workplace, whereas, finally, it is up to the administrative or legal jurisdictions to appreciate its regularity and its proportionality, given the de facto and de jure circumstances of the case.



### **III. Conclusions**

#### **1. Checking Internet connections**

A general and absolute prohibition of any use of the Internet for other than professional purposes does not seem realistic in a society of information and communication. A reasonable use, not likely to lessen the conditions of professional access to the network, and not endangering productivity, appears to be generally and socially admitted by most companies or administrations.

No legal provision obviously prohibits employers from determining the conditions and limits, which as such do not constitute attempts on the employees' privacy.

In this respect, the implementation of filtering tools against non-authorized sites, in association with firewalls (sites distributing products of a pornographic, pedophilic, racial hate inciting, or revisionist content, etc. ) may constitute measures of prevention, which would necessitate informing the private or public sector employees.

In the same manner, the possibility for the employee of the private or public sector to connect himself to the Internet for other than professional purposes may be accompanied by legitimate restrictions, dictated by the need for security within the workplace, such as, the interdiction of downloading software, the interdiction of connection to a discussion forum, or of using a « chat room », the interdiction of accessing a personal mail-box via the Internet, considering the virus risks that such an access may present.

A global « a posteriori » control of Internet connection data, by department or by user, or a statistical control of the most visited sites, should in most cases be sufficient without it being necessary to carry out an individualised, personal control of the accessed sites.

The modalities of such a control of Internet use should, according to Article L 432-2-1 of the Labour Code, be subject to a consultation with the Works Committee, or, in the Civil Service, the Equal Representation Technical Committee, or any other equivalent organism, or to a diffusion of information for users, including when the control is not of a directly nominative nature.

When the company or the administration implements individual monitoring measures, for the purpose of producing a workstation-by-workstation statement of the connection times or the visited sites, the processing of personal data thus organized, must be notified to the CNIL. The duration of storage of such established statements must be specified. Duration of storage of about 6 months should in most cases be sufficient to dissuade from any abusive use of the Internet. The notification file should, furthermore, refer to and date the accurate consultation of the employee's representative organisms.

#### **2. E-mail monitoring**

The use of one's professional e-mail to send or receive, within reasonable limits, a message of a personal nature corresponds to a generally and socially accepted use. Moreover, given the terms of the decision of the Social Chamber of the Court of Appeals dated October 3, 2001 (Nikon case), a general ban would not



allow the employer in normal circumstances to examine the contents of any correspondence of a personal nature.

It should be generally considered that a message sent or received on a workstation owned by the employer is of a professional nature, excepting specific indication given in the subject heading or in the name of the directory where it may have been filed by its recipient which could, thus, give it the character and nature of private correspondence, protected by the confidentiality of correspondence.

Requirements of security, of prevention, or control of congestion of the network may lead companies or administrations to implement tools for measuring the frequency or the size of files sent attached to an e-mail, or even tools for archiving the exchanged messages. In this latter hypothesis, even after having been deleted from the workstation of the sender and the workstation of the receiver, the e-mail will nonetheless be stored. The use of such control or backup tools should be communicated to the employees, as should the duration of storage of the « safeguarded » message.

When the company or the administration implements a measure of individual workstation-by-workstation control of the functioning of the e-mail, the automatic processing of personal data thus implemented must be notified to the CNIL. The duration of storage of the messages must be specified. The notification file must refer to and date the accurate consultation of the employee's representative organisms.

### **3. Log files**

Daily log files of traffic aimed at identifying and recording all the connections or attempts to connect to an automated information system are a measure of security, generally recommended by the CNIL in a concern for ensuring the security and confidentiality of personal data, which must neither be accessible by non-authorized third parties, nor used for purposes other than those that justify their processing. They are not destined primarily for checking on users.

The purpose of these daily log files, which may also be associated with processing of data that are not of any nominative nature, but that may be of a sensitive nature, to the company or the administration concerned, is to guarantee a normal use of information system resources and, if necessary, to identify any use contrary to the rules of confidentiality and security of data defined by the company.

When these daily log files are associated with automatic processing of personal data they are not, as such, subject to prior notification to the CNIL.

In order to guarantee or to reinforce the need for security, they should be communicated to the CNIL as one of the measures of the security surrounding the functioning of the principal processing to which they are a corollary.

On the other hand, the implementation of software for analysing the various journals (applications and systems), which would allow the collection of individual information, workstation by workstation, aimed at controlling the activity of the users, must be notified to the CNIL.

In any case, users must be informed of the implementation of daily record systems and of the duration of storage of any traffic data allowing the workstation or the connected user to be identified. This information, which fulfills the legal obligation to which is held the processor, it allows preventing all risk, and participates in the requirement of fairness in the company or the administration.



Duration of storage of about 6 months does not appear excessive considering the purpose of daily record files.

No provision of the January 6, 1978 Act deprives the controller of the possibility of confronting an employee of the private or public sector, who has not respected the conditions of access or use, with the information recorded in the daily record files associated with automatic personal data processing (Court of Appeals, Social Chamber N° 98-43.485 of July 18, 2000).

#### **4. The role of network administrators**

Administrators who are responsible for ensuring the regular functioning and the security of networks and systems are led by their very functions to access to all user information (e-mail, Internet connections,» logs» or daily record files, etc.) including that which is recorded on the workstation hard disc. Such access is not contrary to any provision of the January 6, 1978 Act.

In the same manner, the controlled use of remote maintenance softwares, which allow remote detection and repair of breakdowns, or, at a distance, taking control of an employee's workstation (« remote handling») presents no particular difficulty with regard to the January 6, 1978 Act, so long as the security measures necessary for data protection are set .

However, system and network administrators should not exploit information to which they have access due to their functions, for purposes other than those linked to the good functioning and the security of applications – and this either on personal initiative or by order of the hierarchy.

Also, network and systems administrators are bound by their duty of professional secrecy. Consequently, they may not disclose information which they come to know because of their functions, in particular when information is covered by the secret of correspondence, when it concerns the users' privacy, and when it does not endanger either the functioning of the applications, their security, or the interests of the company. Neither could they be forced to do so, with the exception of particular legislative provisions in this sense.

#### **5. The use of Information Technology by employee's representative bodies**

Companies and administrations must negotiate the conditions in which the company's email service may be used by employee's representative organisms, or in the exercise of a union mandate.

When the employee's representative bodies avail of their own e-mail account, particular measures of security must be defined or implemented, in order to ensure the confidentiality of the information exchanged.

The conditions of use of the company's IT services by union representatives in the exercise of their mandate must also be specified.

#### **6. A yearly Privacy Evaluation Statement**

The security measures, which lead either to storing trace of user activity or of the use made of information and communication technologies, or which are based on the implementation of the automatic processing of directly or indirectly personal data, should be subject to an annual privacy evaluation statement on the



occasion of the discussion of the social evaluation statement submitted to the works committee, or the Equal Representation Technical Committee, or any other equivalent organism.

## **7. Appointment of an in-house privacy controller**

When their manpower and type of organisation justify and allow it, companies or administrations could, together with the employee's representative bodies, appoint a representative for data protection and the use of new technologies in the company. This representative could more particularly be in charge of security aspects, right of access, personal data protection in the workplace. As an interface between the manager of the company or the head of the administration, the personnel representative organisms, and the employees of the private or public sector, this representative could become the in-house "privacy controller".

As a pedagogical tool, the Commission wishes to append to this report its responses to the most frequently asked questions.



## **APPENDIX**

This document is dedicated to answer to the most frequently asked questions on the proportionality of the employees' monitoring while using information and communication technologies. It does not aim at a modeling security policies, whose implementation belongs to administrations and companies in accordance with their own appropriated and freely determined security standards.

### **Monitoring electronic communications**

It belongs to the managing staff or head of the organisation to define the rules for the use of the Internet.

#### **Draft proposals:**

“Only the Internet sites presenting a direct and essential link with the professional activity should be consulted, subject to the condition that the connection does not exceed a reasonable length of time and that it presents a certain usefulness with regard to the functions exercised or the missions to accomplish.

An occasional consultation on the Web, within reasonable limits, for personal reasons, of the Internet sites whose contents are not contrary to public order and to morality, and which do not question the interests and the reputation of the organisation, is accepted”.

When a filtering tool targeting certain sites of a particular or illegal content (pornography, pedophilia, racism, incitation to racial hate, revisionism, etc.) is implemented it must be brought to the knowledge of the users.

The company or the administration may impose other conditions for the use of the Internet, among which the most frequent are: prohibiting the establishment of one's own Internet site, the access to games sites, the connection to the Internet via a modem, the participation in on-line discussions, the participation in discussion forums (including professional forums), the diffusion of information concerning the company, etc. These rules must be brought to the knowledge of the users.

The legal and statutory measures provide that the Works Committee or the Equal Representation Technical Committee or any other equivalent organism must be previously informed and consulted with on the rules and standards of conduct and the form of monitoring. Once agreed on, these rules must be brought to the knowledge of the employees of the private or public sector.

When the company or the administration implements monitoring designed to produce, workstation by workstation, a statement of the duration of connection or of the sites visited, the automatic processing of such personal data must be notified to the CNIL. Duration of storage of such statements must be specified. The notification file must, furthermore, refer to and date the consultation of the employees representative organisms on such measures.



## **E.mail monitoring**

It belongs to the manager or head of the organisation to define standards e.mail monitoring.

## **Draft proposal**

“A reasonable use in the framework of the requirements of daily and family life is allowed, on condition that the use of the electronic mail does not affect the normal traffic of professional messages.”

Special security requirements may lead the company or administration to implement a messages analysis tool based on a list of» key words». In this particular hypothesis, the risk of the system being diverted may legitimately lead the company not to reveal the» key words» to the users.

In a concern for security of the organisation or for control of network congestion, the company or administration may implement a system for limiting the volume or size of the messages exchanged or of the files attached.

These same requirements for legal or technical security may also lead the company or administration to store a backup copy of the messages exchanged. In this hypothesis, the users must be informed that the messages they have received or sent will be stored in the backup system, notwithstanding that the user having deleted them from his workstation. The duration of storage of the messages in the backup system must be specified.

The company or administration may establish other regulations. These must be communicated to the users. This must, in particular, be the case when the use of services, from the company premises, of a specialised e-mail Website is prohibited by the organisation.

Quoting a decision of the Social Chamber of the Appeals Court dated October 2, 2001:

« The employee has the right, even during working hours and at his place of work, to the respect of his privacy; this includes in particular the confidentiality of his correspondence; the employer cannot, without infringing this fundamental liberty, examine the personal messages sent or received by the employee on a computer tool placed at his disposal for his work, and this even in the case of the employer having prohibited a non-professional use of the computer».

It must be generally considered that a message sent or received by the workstation made available by the company or the administration is of a professional nature. It cannot be otherwise, except in the case of specific reference in the message heading to its personal character or if it has been filed in a directory clearly identified as being personal.

According to the above decision it can be considered that network and systems managers, whose functions lead them to have access to all the users' data, including that registered on the hard disc of the workstation, cannot be forced to disclose any information which has come to their knowledge due to their function, when this information is covered by the confidentiality of correspondence, or comes under user privacy, and does not endanger either the smooth functioning of the applications, or the security, or the interests of the company.



The CNIL considers, that the modalities of e-mail monitoring do not, as such, come under the provisions of the January 6, 1978 Act as long as it does not concern an individual control, workstation by workstation. They must, however, be submitted to the employee's representative organisms and, once the opinion of these organisms has been collected, be communicated to the users.

### **Daily record files and firewalls**

A method of daily record keeping is designed to ensure security and the smooth functioning of a system or of a computer application. Monitoring is not its primary function.

No provision of January 6, 1978 Act prevents the processor from confronting an employee of the private or public sector, who has not respected the rules and standards of conduct, with the information recorded in the daily record files.

Firewalls ensures the protection of the company with regard to computer intrusions or attacks. In order to achieve this it checks all the company's incoming and outgoing traffic, both local and remote.

Its objective is not to carry out a monitoring, but in case of computer attacks, to be in a position to identify their origin and to prevent the effects.

As such, the servers (proxy, cache, etc.) which allow optimising the connection time by memorising the Web pages consulted, as well as the servers with a firewall function, designed to protect the company's computer applications from outside attacks, are not subject to prior notification to the CNIL. Users must be informed of their existence .

Administrators alone have access to the recorded information. No exploitation is made for purposes other than those linked to the smooth functioning and the security of the information systems.

The CNIL considers that a daily record file does not need to be notified to the CNIL as long as it is associated with an automatic processing of personal data, and its function is to ensure security. Nevertheless, its existence must be mentioned in the notification file of the main processing to which it is a corollary.

On the other hand, the implementation of a software of analysis of the different journals (applications and systems) which allow collection of personal data, workstation by workstation, designed to control user activity must be subject to prior notification to the CNIL.

Duration of storage of traffic data must be specified. The CNIL considers that duration of about six months is not excessive.

### **Annual Privacy evaluation statement**

The CNIL proposes that a privacy evaluation statement be presented to the Works Committee or the Equal Representation Technical Committee on the occasion of the discussion of the annual statement of



accounts. The statement would include the principles and measures of security, which lead to storing traces of user activity, or of the use made of information and communication technologies.

### **Appointment of an in-house privacy controller**

When their manpower and type of organisation allows it, the companies or administrations could, in concert with the employees representative organisms, appoint an in-house “privacy controller”. This representative could, more particularly, be charged with questions of security, of right of access, and of personal data protection in the workplace. As an interface between the manager of the company or the head of the administration, the personnel representative organisms, and the employees of the private or public sector, this representative could become the in-house»privacy controller».