

The internet rights Forum



www.foruminternet.org

FINAL REPORT

"WORKING RELATIONSHIPS AND INTERNET"

17 September 2002

Contact:

contact@foruminternet.org

CONTENTS

PART ONE – INFORMATION TECHNOLOGIES MODIFY RELATIONSHIPS AT WORK..... 7

I – Information technologies shake the traditional legal and organisational framework of work 7

A. The form of work is evolving 7

B. These evolutions raise various issues 8

1°. In relation to the subordinate relationship between an enterprise and the people it employs..... 8

2°. In relation to pay conditions 10

3°. In relation to working hours as a measure of the activity of the employee 11

II – Inter-penetration between the professional sphere and the personal sphere should be controlled 11

A. The employer and employee should agree precise rules for working from home..... 12

B. Mobile working should be controlled by defining genuine, continuous and effective time off 13

PART TWO – THE USE OF INTERNET BY EMPLOYEES IN THE WORK PLACE..... 16

I - Objective: define a clear and transparent framework that establishes the rules for the use of Internet within an enterprise 16

A. The Forum notes that employees expect to be able to use Internet for personal purposes..... 16

B. Employers cannot relinquish control of the use of the Internet by employees – including when this is for personal purposes..... 17

C. A need for clarification of the employees’ and employers’ approaches 18

II - General philosophy: a presumption of professional Internet use at work, with the possibility of reasonable and controlled personal use	18
A. The Forum considers that the Internet remains above all a tool that is made available to the employee for professional use	19
B. However, the Forum considers it is difficult to refuse in principle personal use of the Internet in the work place	19
III – Methods of monitoring personal use: fair, transparent and proportionate monitoring	20
A. Employees should distinguish professional documents from those they consider personal	20
1°. Employees should distinguish personal mail from professional mail	20
2°. Employees should distinguish personal files on the hard disk	22
3°. Employees have to undertake not to transform professional information into personal information.....	22
B. Fair and transparent methods of monitoring should be established	22
1°. Technical controls can always be carried out	22
2°. Employers may also monitor volume if necessary	22
3°. Monitoring the content of information should be limited	23
4°. Employers should remind employees of the need to protect their information and should inform them of the length of time data is kept.....	23
C. Network administrators should protect the confidentiality of personal data.....	24
IV – Legal instruments for putting these principles into action: an appendix to internal regulations and transparent information.....	25
A. The rules of Internet use should be defined in an appendix to the internal regulations	25
B. Employers should inform employees of how Internet use is monitored	26
C. Employers must respect the obligation to make a declaration to CNIL	26

PART THREE: THE CHALLENGE FOR INDUSTRIAL DIALOGUE	27
I - Observation: the employment code does not make provision for staff representatives to have access to an enterprise's networks	28
II – Position: staff representatives should be able to access intranets and e-mail systems	29
III – Methods of implementing access for staff representatives: a detailed agreement	30
A. Access to information technologies should be granted to all staff representatives with the same conditions relating to rights and duties.....	30
B. Some guiding principles should be provided for in the agreement defining the use of information technologies by staff representatives	31
1°. The agreement should be concluded for a set period of time	31
2°. Staff representatives should have complete freedom as to the content of the information sent, at the same time as being responsible for it	31
3°. The use of these tools should not hinder the normal functioning of the enterprise.....	32
4°. The intrinsic interactivity of these tools should be maintained	32
5°. The principle of employees' freedom of choice to accept or refuse messages from staff representatives should be safeguarded	32
6°. The confidentiality of exchanges between employees and staff representatives should be ensured	32
IV – Electronic consultation procedures should be gradually introduced	33
V – Far off horizons: modifying the employment code to become more technologically neutral	33

Today, the deployment of information technologies, and in particular Internet, in enterprises is well underway. It is widely reported by the media. However, the consequences of this phenomenon are not yet fully under control or properly understood. Employees and enterprises are still far from having completely accepted the potential these new tools offer. The fact remains that information technologies change not only day to day working conditions for employees but also the individual and group relationships forged within an enterprise.

Certainly, the problems raised are not entirely new: thus the question of personal use of the Internet for consulting sites or sending e-mails is only a repetition of questions raised when the telephone was installed or Minitel was developed. Nevertheless, information technologies represent a major technological break with earlier innovations because of their particularities: digitisation of data, traceability and storage of information, ease of remote access, network working methods, gearing down information etc. They cannot therefore be straightforwardly incorporated into an enterprise by transferring the patterns and practices relating to earlier technologies.

Of course, the impact of Internet on individual and collective freedoms within an enterprise has to be analysed with a view to the existing legal framework that applies to work and which, in particular, is based on the subordinate relationship between an employee or civil servant and his or her employer.

France is not the only country thinking about these questions: countries such as Spain, Germany and Great Britain are considering both the impact of Internet within enterprises and how the personal sphere can be recognised in the workplace. Belgium has even brought in legislation on the subject ⁽¹⁾.

The Internet Rights Forum wanted to make a contribution to this debate because for many employees the enterprise constitutes one of the best places for accessing new technologies and in particular Internet. In July 2001, the Forum therefore set up a working group entitled "*Relationships at work and the Internet*". The work of this group in part continues the thinking begun by the CNIL on monitoring employees, <http://www.cnil.fr>; it also links up with the thinking undertaken by employers and unions as well as linking up with the provisions made by the civil service.

The working group established by the Forum heard many well known qualified figures and brought together management and unions. It also collected the accounts and opinions of Internet surfers in two discussion forums organised in autumn 2001 and spring 2002. As a result, **the thinking and proposals attached to this recommendation are not simply the result of theoretical work but are the result of a process of consultation** that was finalised on 31 July 2002 by the Forum's guidance committee on the advice of all members of the Internet Rights Forum, i.e. around one hundred public and private enterprises, associations or public groupings, representing the full range of players involved in the Internet.

¹ - Belgium issued a royal decree dated 12 June 2002 relating to the protection of employees' private life concerning monitoring electronic communication data in networks.

A few preliminaries ...

Any consideration about the influence of information technologies on relationships at work has to take account of the huge diversity of organisations concerned. Firstly, although this report is based on an analysis of the private sector, a number of the considerations formulated apply to the public sector. Secondly, the problems encountered differ greatly depending on the size of the enterprise: SMEs are often only just beginning to introduce information technologies, whereas large enterprises can now look back on several years of experience of information technology practices. Finally, the problems encountered are significantly different depending on the type of activity carried out by the enterprise. Some enterprises, particularly in the "new economy" sector and indeed in the banking and finance sector, use information technologies very widely as they represent a natural medium for their businesses. They therefore offer a large number of their employees access to these tools, in particular to the Internet. On the other hand, in other enterprises such as industrial enterprises a large number of employees have in fact very limited access to these new tools.

Consequently, and given these differences in use, it is usually a question of not offering unique or too theoretical solutions. The Forum thinks that in such a context, **experimentation** on a case by case basis should be given preference and an **in-depth dialogue** should be undertaken between the different players in an enterprise in order to come to a consensus on the use of information technologies. Furthermore, **the Forum wanted to give preference to a pragmatic operational approach and, from the basis of an in-depth legal analysis, offer the players in an enterprise concrete tools for implementation.** These three methodological principles flow through the proposals that appear in the report.

In the first part, the Forum wanted to develop a future vision of the influence of information technologies on the definition of work. In the second part, the Forum wanted to respond to questions from employees and enterprises on monitoring the use of Internet in the workplace. Finally, in the third part, the Forum looked at the possibilities offered by information technologies in modernising and reviving the dialogue between management and unions.

All these recommendations are eagerly anticipated by the department for relationships at work within the Ministry of Social Affairs, Work and Solidarity. They will serve as the basis for discussions that the department would like to begin with employers and unions in the autumn.

PART ONE – INFORMATION TECHNOLOGIES MODIFY RELATIONSHIPS AT WORK

Information technologies influence the general evolution of work. The strategic challenge they represent for an enterprise is in addition highlighted by 78% of employees and 55% of enterprises ⁽²⁾. They are not the only issue, but they accompany or indeed increase the pace of the slow evolutions in enterprises' methods of functioning which should be analysed from the point of view of the existing legal and organisational framework. More specifically, they raise the issue of the inter-penetration of an employee's personal and professional spheres.

I – Information technologies shake the traditional legal and organisational framework of work

A. The form of work is evolving

Paid work is traditionally characterised by the subordinate relationship that exists between the employee and his or her employer. This authoritarian relationship has until now fitted into a strictly defined framework based on the place of work and working hours. However, information technologies are changing this traditional view of work in two main ways.

Firstly, the development of these tools within the enterprise is accompanied by changes in how it functions and by a movement away from the Taylor model.

The activity of many enterprises is increasingly orientated towards the production of an intangible capital connected to knowledge. In particular we are thinking of certain high tech enterprises. Work is no longer organised on the basis of a precise definition of tasks or of the mission to be achieved, but is based on mobilising knowledge in the production process. This evolution in demands gives workers more autonomy in how they organise their work, being increasingly less hemmed into a pyramidal and bureaucratic organisation. In return, the employer expects greater involvement in the enterprise, expecting workers to respond to the obligation to produce results and not only means.

In addition, enterprises are increasingly organised into networks, in relation both to their suppliers and their customers. Some firms even want to change the conditions of their work force in order to incorporate a networking approach, making the work force a service provider. This evolution changes how enterprises function, moving more towards a model that is decentralised into profit centres. They can even change the legal structure by outsourcing former activities to other entities with which they maintain a special or even exclusive relationship. Thus, the boundaries of the company gradually become more blurred as the network organisation develops.

In some enterprises, these two evolutions shatter the Taylor model, which is based on the division of work and a hierarchical organisation like a pyramid. New technologies accompany the phenomenon by facilitating reorganisation with an appropriate information system and with tools allowing mobility. This observation has of course to be put into perspective. There are

² - Source : Cegos, Paris Dauphine AIMS, June 2002.

areas within enterprises, including jobs using information technologies, that are not affected by this evolution and which continue to be characterised by a Taylorian approach. Telephone call centres are an example. Nonetheless, an increasing number of workers are affected by this evolution, which is characterised by an increase in autonomy and greater mobility for employees.

Secondly, new technologies change the framework of work by blurring the notions of workplace and working hours.

On one hand, new technologies facilitate the existence of a personal life in the office during working time. In fact, it has become easy to use Internet to correspond by e-mail with non-professional contacts or for consulting Internet sites for non-professional purposes. The phenomenon is not entirely new: the telephone and Minitel in enterprises produced the same effect. However, Internet increases the possibilities available to an employee and thus raises the question of limits or indeed of managing its use, something that we will be looking at in the second part of this report.

At the same time, these new tools facilitate the intrusion of professional life into the personal sphere. They allow work to be continued outside the company and therefore outside what has been traditionally considered working hours. Once again, the evolution is not entirely new. It has always been possible to take a business file home to work on in the evening or at the weekend. However, information technologies have extended these possibilities. The most obvious version of this evolution is teleworking in which the home becomes the workplace. However, in a more extensive way, information technologies favour the development of "mobile" working. It has become possible to get in touch with employees at any time and any place on their mobile telephones. Equally, employees are able to carry the office with them, working on laptop computers. They can even remotely consult any messages received at their business address by connecting to the enterprise's internal network, if an extranet has been put in place. Enterprises such as Vivendi in France or PeopleSoft in the United States have in addition taken the initiative of financing personal computer equipment for their employees, either completely or partly ⁽³⁾. It seems on this last point that British employees are among the best equipped in Europe with 8% having a laptop computer provided by their company ⁽⁴⁾.

B. These evolutions raise various issues

1°. In relation to the subordinate relationship between an enterprise and the people it employs

This relationship seems to have been shaken in two ways: on one hand in relation to the nature of employment, which is the traditional legal framework for employees and on the other hand, in relation to the emergence of a new model, the network company.

³ - In France, article 4 of the 2001 finance bill provides that employees benefiting from new computer equipment, software and service provision free or at special prices will not be taxed on this benefit up to the limit of 1525 € (10000 Frs) on condition that these operations are the result of an agreement with the enterprise or the group, concluded according to the modalities provided for in articles L. 442-10 and L. 442-11 of the employment code. This benefit is also exempt from social contribution subscriptions.

⁴ - Source: study by the British consultancy e-Mori quoted by the Journal du Net, 13 June 2001, <http://solutions.journaldunet.com/0106/010613peoplepc.shtml>

In fact, the development of the autonomy of employees firstly raises the issue of preserving employment. The press has covered the development of a category of autonomous professionals ⁽⁵⁾. The development of "solo workers" in the consultancy or computer sectors is the most tangible sign of this evolution ⁽⁶⁾.

The autonomy of these workers does not allow them to be considered as employees subject to a subordinate relationship. Their skills and expertise mean they are closer to the situation of independent workers but with special economic links to the enterprise. They seem to fall into a grey area between independence and employment ⁽⁷⁾.

Without doubt, the concept of employment is broadly interpreted by judges, regardless of any contract linking a worker to his or her employer. Judges therefore do not hesitate to re-define service contracts (fees) as work contracts. According to the Court of Appeal, "*the existence of a work relationship is not a question of the will of the parties nor of the denomination they have given to their agreements but a question of the actual conditions in which the activity of the worker is exercised*" ⁽⁸⁾. At the moment at which a contract is characterised by a legal subordinate relationship, that is by the power of the employer to give orders and directives, to monitor their execution and to sanction any failures in the subordinate, judges will redefine it as a work contract ⁽⁹⁾. The subordination criteria also allows workers who retain a large degree of autonomy in their work, but who are part of an organised service, to be defined ⁽¹⁰⁾.

Furthermore, chapter VII of the employment code brings a certain number of relatively heterogenous categories of professionals under the umbrella of a work contract. It sometimes imposes the definition of a work contract to the contract that links them to their employer, for example for commercial travellers ⁽¹¹⁾, or indeed presumes there is a work contract, for example for journalists ⁽¹²⁾. Nevertheless, as opposed to traditional employees, these categories in many cases do not benefit from every provision in the employment code.

However, for some commentators, although allowing differing situations to be taken into account providing proof of increasing autonomy for employees, the current framework of the employment code is inappropriate for dealing with the reality of this much vaunted grey area, which is sometimes called "para-subordination" ⁽¹³⁾. These autonomous professionals should therefore be the object of a special legal category, as is accepted in some European countries such as Germany and Italy, leaving a more important role for contracts in regulating relations between them and their employers.

In contrast to this position, some consider that the definition of employment is sufficiently flexible to cover this type of relationship with autonomous professionals that are economically answerable a single enterprise. They consider furthermore that a too fragmented view of employment does not offer the conditions for companies to really perform. In fact, to be efficient companies should set up a proper joint co-operation arrangement, particularly when their product is intangible. These players consider that this necessary co-operation would in

⁵ - Le Monde, 2 July 2002.

⁶ - A study by the Minister of Finances in September 2000 evaluated the increase in the number of enterprises composed of 0 to 1 person in the services to enterprises sector as being 25% between 1993 and 1998.

⁷ - Alain Supiot, "Les nouveaux visages de la subordination", Droit Social, February 2000, p. 131.

⁸ - Soc., 19 December 2000, Labbane, Bull. civ., V, no. 437, p. 337.

⁹ - Soc., 13 November 1996, Société Générale, Bull. civ., V, no. 386, p. 275.

¹⁰ - For example doctors in a clinic.

¹¹ - Article L. 751-1 of the employment code.

¹² - Article L. 761-2 of the employment code.

¹³ - Jacques Barthélémy, "Le professionnel parasubordonné", JCP 1996, I, 606.

many cases preclude limiting relations with intellectual workers to simple customer - supplier relations as that would adversely affect the performance of a company.

Apart from the issue of employees' increasing autonomy, the model of a large centralised integrated enterprise is giving way to the concept of a network of enterprises. Thus, employees, although legally linked to an enterprise, in fact find themselves dependent on the activity of the whole network. Some commentators have noted that the right to work does not sufficiently take the existence of these networks of enterprises into account for issues relating to health and safety or to sub-contracting ⁽¹⁴⁾. The question of contracts signed between employees and these new entities arises. It already implicitly appears in the continuation of work contracts during outsourcing operations and therefore during company reorganisations. For the time being and in spite of several initiatives ⁽¹⁵⁾, network enterprises have an economic identity, but no social identity. An employee is connected to an enterprise in the network, but not to the network itself. This legal constraint may inhibit employees' mobility within the network of enterprises. It may also be contrary to the economic reality of the network.

The Forum considers these to be crucial complex issues that go beyond the simple framework of information technologies, which in this area are only a catalyst for the evolutions taking place. In the next few years, economists, sociologists and lawyers will be driven to examining them in depth. The Forum is nonetheless convinced that this thinking should start with practice and in particular with the needs of enterprises and workers. **The authorities have to contribute to clarifying this debate through the work of bodies such as the State Planning Commission or the Economic and Social Council.**

2°. In relation to pay conditions

The question of the rights of salaried authors under private law raises some concerns. In fact today, in practical terms, a large number of work contracts for salaried authors make provision for writers to transfer their rights to works they have created during the period of the work contract to their employer. In the specific area of the press, service agreements have been signed in order to make provision for transferring rights to journalists' future work. These practices appear to have a legally precarious basis given the principle of prohibiting the overall transfer of future works as provided for in article L. 131-1 of the intellectual property code.

The commission on the rights of salaried writers in private law, responsible to the council for literary and artistic property (CSPLA), looked into this question but was unable to bring the different parties to a mutually acceptable solution. In 1998, in its report entitled "Internet and digital networks", the Council of State tackled the question and suggested a regime for payment of employees inspired by that anticipated for patents (art. L. 611-7 of the intellectual property code).

This question should be resolved with the adaptation of the 22 May 2001 directive on the harmonisation of some aspects of copyright and related rights in the information society.

¹⁴ - Alain Supiot, *Ibid.*

¹⁵ - Such as employers' groupings allowing employees linked to these groupings by a work contract to be made available to their members, as in article L. 127-1 of the employment code.

3°. In relation to working hours as a measure of the activity of the employee

The Taylor economy is based on a precise assessment of the productive performance of a physical worker in manufacturing or in a factory. However, how can the production of an intellectual worker be measured? How can the part provided by the individual be distinguished in what is increasingly a joint production? How can it be ensured that an individual efficiently uses his or her skills in the service of the enterprise? Guaranteeing production levels is much more difficult when the product is chiefly intangible.

In this context, the criterion of hours of work often appears inadequate for measuring an employee's contribution to production. Thus, hours worked can no longer be the only measure for a salary. The salary could for example be earned for reaching an objective, or even for supplying a service within a set time, at the same time as giving the employee a great deal of freedom to organise themselves. In this respect, this evolution is revealed by the recent creation of the category of autonomous executives⁽¹⁶⁾ and of day rates in the 19 January 2000 law relating to the reduction in working hours.

Nevertheless, jurisprudence has established a number of principles. Thus, although it has been accepted that an employer has the right to define unilaterally the content of the objectives, these have to be realistic⁽¹⁷⁾. These objectives also have to be appropriate to the hours worked by the employee and should not encourage him or her to exceed the maximum working hours, nor should they encroach on time off. In addition, a simple lack of results in relation to the objectives set is not in itself cause for cancelling the work contract⁽¹⁸⁾. Judges have to assess whether the poor results are the result of professional inadequacy or of an error that can be imputed to the employee⁽¹⁹⁾, while taking the market situation into account.

These evolutions go hand in hand with the issue of workload. This question is essential for the performance of companies that have to successfully mobilise their employees while making the workload acceptable to them. It may call into question the actual definition of how production is organised.

The Forum considers that the definition of the workload should be subject to wide ranging discussions within the company, not only between the management and unions but also with employees at all levels in the enterprise. In fact, the reality of the workload can often only be appreciated at a very decentralised level.

II – Inter-penetration of the professional sphere and the personal sphere must be controlled

Information technologies blur the boundaries between private and professional life. This inter-penetration responds partly to a desire for flexibility that not only the enterprise wants but also some employees. Thus, an employee may want to work at home for a certain period in his or her professional life (when there are young children for example). An employee may also use information technology in order to be mobile, thus gaining some flexibility in organisation. An

¹⁶ - Article L. 212-15-3 of the employment code.

¹⁷ - Cass. Soc., 22 May 2001, Société Expertises Galtié c/ M. Farrouilh, Bull. civ., V, n° 180, p. 142.

¹⁸ - Cass. Soc., 3 February 1999, Société Dilux, Bull. civ., V, n° 56, p. 42.

¹⁹ - Cass. Soc., 3 April 2001, M. Grandemange c/ Société Point Provence Comasud, Bull. civ., V, n° 117, p. 91.

employee is able to decide to leave earlier and finish off his or her work at home or on the journey.

The Forum considers that the inter-penetration facilitated by new technologies is not bad in itself but that it should be controlled to protect both the company and the employee against abuses.

It is useful to distinguish two scenarios: working from home and mobile working. In the first case, it is a question of making the home the usual place of work of an employee, either exclusively or partially (for example an employee working two days a week from the company premises and three days a week from home). In the second case, the usual place of work is the company premises, but an employee decides to continue his or her work outside the enterprise from time to time.

A. The employer and employee should agree precise rules for working from home

In principle, the work relationship should exist in a predetermined place decided upon by the employer. It may be the company premises or an annexe. In any event, the place of work should be distinguished from an employee's home (²⁰).

However, this distinction does not prohibit provision being made in the work contract for an employee's home to be his or her usual place of work. On the other hand, when working from home has not initially been provided for in the work contract, the employer may not unilaterally impose such a change on an employee's living conditions. As the Court of Appeal stated in its Abram ruling on 2 October 2001, the employee "*is required neither to accept working from home nor to install files and the instruments of work there*".

Working from home must therefore be voluntary. Furthermore, enterprises that operate remote working recognise that for the operation to be really successful the employee has to do so voluntarily. The management of an employee has also to be in favour of this type of organisation.

On the basis of this observation, **the Forum considers that implementing working from home should be accompanied by three essential safeguards:**

- A number of elements have to be clearly defined among which are the hours and control of work, insurance and special arrangements in the home, responsibility for professional expenses etc;
- it is also advisable to make provision for a period at the end of which the employee may exercise a "right to return" to the company premises;
- finally, provision should be made for some link between the employee and the collective life of the company by establishing times and places for the employee to meet with his or her work community.

²⁰ - In articles L. 721-1 and following, the employment code in addition provides for the existence of a special status for those working from home. However, this old status has been rarely applied and is no longer applicable to the situation of employees working on Internet.

These principles have been recognised in the framework agreement on teleworking signed on 16 July 2002 at a European level between employers' representatives, UNICE/UEAPME and the CEEP, and the European Trades Union Confederation (ETUC) for employees.

These elements should appear in an amendment to the work contract.

B. Mobile working should be controlled by defining genuine, continuous and effective time off

Mobile working allows work to be continued outside the enterprise. It creates a degree of porosity between professional and private life that is not without risk for either the employee or the enterprise.

For the employee, the inter-penetration of professional and private life should not result in these two spheres becoming confused. An individual's personal equilibrium requires a border being established between work and time off. An employee cannot be in a work situation 24 hours a day, 7 days a week without being able to "switch off" from his or her professional environment. The mobile phone, a new instrument of constraint, which allows an employee to be contacted at any time or place, is in this respect what is sometimes called "an electronic leash". The welfare lobby as a whole does not accept too great a permeability between public and private spaces. To ensure employees have a well balanced life, the sphere of the family and personal life has to be protected. This should be separate from the professional sphere where employees use their skills.

It is also in the interests of the enterprise to differentiate between private life and professional life. Companies run a variety of risks by feigning ignorance of this separation. It may appear less attractive to recruit employees that aspire to a balance between their professional lives and personal lives. Companies also run risks in the event of a dispute with an employee. In fact, an employee may oppose the employer by bringing to light an infringement of the law, work being required outside the work place and working hours. Information technologies then represent a powerful weapon in the hands of employees. They allow them to retain evidence of the time spent on a laptop computer or indeed the time connected to the enterprise's extranet... The employer may therefore find themselves with heavy sentences for non payment of additional hours, or even be exposed to criminal proceedings for non declaration of work⁽²¹⁾.

This observation of an inter-penetration of professional and private life has led a good number of observers to raise the possibility of putting a genuine right to switch off in place.

The Forum notes that the legal framework embodies this right to switch off by introducing the right to time off.

Employers have to take account of the legal framework of work, particularly the provisions relating to 11 consecutive hours a day time off⁽²²⁾ and 35 hours time off a

²¹ - Offence under articles L. 324-9 and L. 324-10 of the employment code.

²² - Article L. 220-1 of the employment code introduces for all employees the right to 11 consecutive hours time off every day. Although the text authorises exceptions to this rule, it is only limited and in very specific situations. The texts make provision for two types of exceptions to this rule: " [...] A convention or a wide-ranging collective agreement may be exempt from the previous paragraph under the conditions established by decree, particularly for activities that are characterised by the necessity to ensure continuity of service or by the necessity for intermittent periods of work. This decree also makes provision for the conditions under which there may be exemptions to the

week (²³). During this time off, the employee may not be in a work situation or on call (²⁴). These provisions guarantee employees a period of time during which they may freely go about their business (²⁵). In a ruling dated 10 July 2002, the Court of Appeal considered that time off "*presupposes that, except for exceptional circumstances, the employee is totally free directly or indirectly from having to undertake any work for his or her employer, even if only potentially or occasionally*". An employee can therefore rely on these legal safeguards to ensure he or she is able to benefit from a genuine right to switch off, thus safeguarding the personal sphere.

Nevertheless, information technologies may be used to reduce this time off. An employee may be reached at any time by mobile phone. They may also decide to transfer their professional e-mails to their homes. The concentration of techniques will make this evolution increasingly inescapable, particularly when employees are able to read their professional messages on their mobile phones. This intrusion into the personal sphere is often spontaneous on the part of both the employer and employees' colleagues. The employee may in fact be the one creating the confusion.

The Forum considers that internal discussions should be initiated within companies in order to ensure that this right to switch off is effectively applied by establishing clear regulations.

Appropriation of these tools by the work community will no doubt reduce the most obvious excesses. Nevertheless, there should be a debate to create awareness of the need to establish collective regulations in order to prevent excessive overlap of the professional sphere into the personal sphere.

This discussion returns to that relating to defining the overall work load, which as we have already seen should completely objectively be able to be dealt with during working hours in order to avoid any continuation into time off.

However, it should also result in developing rules for the "proper" use of information technologies.

Thus, clear conditions have to be established for re-routing e-mails or for remote access to the enterprise's network. It is also necessary to define rules for the proper use of mobile phones. These should ensure that the facilities offered by modern methods of communication do not result in an invasion of an employee's personal sphere. The regulations may use technical restrictions limiting the use of these tools outside working hours (for example by restricting access to extranet outside working hours) in the best interests of the two parties to the contract.

provisions in the first paragraph if there is not a wide-ranging collective convention or agreement, and in the case of urgent work because of accident or the threat of accident or exceptional additional business".

²³ - Which come from the 24 hours time off as provided for in article L. 221-4 and time off of 11 hours in article L. 220-1.

²⁴ - In accordance with article L. 212-4 bis of the employment code, on call is a period during which the employee, without being permanently and immediately available to the employer is obliged to remain at home or close-by in order to be able to undertake work for the enterprise. Regularly the Appeal Court has ruled that periods on call constitute neither effective work nor time off (Cass. soc., 4 May 1999, Bull. civ., V, n° 187, p. 137).

²⁵ - Ph. Waquet, "Le temps de repos", Droit Social 2000, p. 288.

The Forum considers that these proper uses of information technologies should be formalised in codes of conduct established by the employer in conjunction with staff representation institutions.

PART TWO– THE USE OF INTERNET BY EMPLOYEES IN THE WORK PLACE

An increasingly large number of employees are connected to Internet at their place of work. It is estimated that 20% of French employees have access to Internet at work ⁽²⁶⁾. The enterprise is therefore an ideal place for accessing and using these new technologies. Today there is a certain lack of clarity in the rights and duties of different players in relation to the use of these technologies. If new technologies are to become a permanent and day to day part of the life of companies, it will be necessary to define a framework for use in which they can develop, respecting the interests of both employees and employers.

I – Objective: define a clear and transparent framework that establishes the rules for the use of Internet within an enterprise

A. The Forum notes that employees expect to be able to use Internet for personal purposes

Information technologies and in particular the Internet, allow employees to easily and discreetly accomplish a number of day to day activities. From their work stations and during their working hours they can therefore book a train ticket, make contacts with the administration or communicate by e-mail with a friend. Without doubt, these possibilities existed before with the telephone and Minitel. Nonetheless, with Internet the possibilities are far greater. After the discovery phase, employees are tempted to use the tool made available by the employer for non professional purposes.

Many employees with an Internet connection consider that the employer should accept personal use. It is furthermore often a compensation for the inter-penetration of professional and personal life. If their employers can encroach on their personal life, for example by supplying them with laptop computers so they can be mobile or by reaching them on their mobile phone, it seems logical for them to be able to use Internet for personal purposes in the work place.

Some go as far as considering that it is a right that the employer should respect. For these employees, the enterprise should allow a personal sphere to exist in the office and should give all employees access to information technologies.

Without going that far, most employees consider that the employer should not be able to access information received, sent or held as a result of personal Internet use. In fact, they consider that it would constitute an encroachment into their private life, which is protected by article 9 of the civil code and by the stipulations in article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. Both Court of Appeal and the European Court of Human Rights jurisprudence upholds this in relations between employees and employers. A particularly sensitive question arises for many employees: the question of

²⁶ - Ipsos study carried out for "Nouvel Hebdo" 8 February 2002.

opening electronic mail that some consider is covered by the confidentiality of correspondence, under article 226-15 of the penal code (²⁷).

From this viewpoint, it is impossible to ignore the particularities of Internet, which does not allow an employee to wipe out any personal actions from the network. In fact, digital information is easily stored. It can easily be traced by the employer. What is more, it is in the very nature of these new tools to monitor trails left by employees, giving rise to fears of cyber-surveillance, which is more insidious but more efficient than the old methods employers used to check up on employees.

B. Employers cannot relinquish control of the use of the Internet by employees – including when this is for personal purposes

Given their responsibility for managing the enterprise, employers have to be particularly vigilant in relation to the risks for the enterprise arising out of the use of Internet.

Internet use can undermine the integrity of enterprises' information systems, which have become essential to their economic activity.

The security of networks may be endangered by data coming into the enterprise either via e-mails or in downloaded files. Similarly, the enterprise has to ensure that its networks do not become overloaded with the associated risk of slowing or paralysing their activity, for example by downloading too voluminous files or by sending attachments that are excessively large. Personal use may endanger the enterprise's networks.

Furthermore, employers highlight the possibility of Internet use damaging the enterprise.

An enterprise may be responsible for illegal or incorrect use of the Internet in the work place. In fact, civilly, as the principal for its employees, the employer is responsible for any offences committed by them when using Internet during working hours, on the basis of article 1384 paragraph 5 of the civil code. Of course, the employer may be exonerated if an employee acted outside the functions for which he or she was employed, without authorisation and for purposes outside his or her remit. Nevertheless, enquiries may be made into the extent of the company's responsibility. It is necessary therefore to be vigilant. (²⁸).

²⁷ - Article 226-15 of the penal code makes provision for "The act, committed in bad faith, of opening, removing, delaying, or withholding correspondence, whether or not at its destination and addressed to a third party, or of fraudulently reading it, is punishable by one year's imprisonment and 45000 € fine. The same sentences applies to the act, committed in bad faith, of intercepting, diverting, using or divulging correspondence sent, transmitted or received via telecommunications or of installing apparatus designed to carry out such interceptions."

²⁸ - Enterprises' criminal responsibility appears more difficult to engage. In fact, article 120-2 of the new penal code makes provision for a legal entity being responsible for infractions committed on their behalf and by their representatives. In addition, an enterprise's criminal responsibility cannot be engaged unless it is expressly provided for by a special provision for the infraction under consideration. The risk for the enterprise of their criminal responsibility being engaged in relation to an illegal act committed by an employee outside their functions during personal use of Internet, would appear therefore to be low.

In addition, the employer may quite legitimately not want to see consultation of licentious sites developing or see dubious messages being sent from the work place. The employer may want to prevent the situation getting out of hand, if only to avoid the possible negative consequences on the company image.

Employers may want to prevent any disloyal employee using Internet to communicate with the competition, endangering company secrets, for example by e-mailing the customer file.

Lastly, **some employers would like to control Internet use in order to monitor employees' productivity.** Of course, monitoring an employee's activity is in the first place the responsibility of his or her direct line manager; if an employee spends an excessive amount of time visiting web sites or sending e-mails, his or her superior should note that his or her productivity is not optimal. Nonetheless, the difficulty in some cases of measuring activity complicates the task. Some employers want to accompany this managerial monitoring with controlling Internet use to prevent abusive use developing, which has no relationship to the professional activity.

C. A need for clarification of the employees' and employers' approaches

We see that employers' approaches and employees' approaches to the use of new technologies are not in theory always the same. In practice however, a consensus usually prevails: most employers can only note employees' personal use of Internet. These practices have already been observed in relation to the use of the telephone in enterprises. Similarly, employers have neither the means nor the desire to monitor the use every employee makes of Internet. They merely want to be able to prevent any abuse. Finally, nearly all employees are conscious that the office is actually still a place of work.

Consequently, many players consider that a tacit, unwritten arrangement between employees and employers is sufficient. Such a solution nevertheless poses various problems. It does not define what is allowed and what is prohibited. It leaves uncertainties that make it more difficult for employers to take action in the event of a problem. After all, if no rules have been established, what checks can be undertaken and more especially, what measures can be taken should there be excessive or improper use? More over, it leaves the door open for speculation on employers' real motives. How can employees be sure that they are not being systematically checked on by the employer when they send personal messages?

Given the supposition that we do want the new technologies to be deployed in enterprises and that we want them to become commonplace tools and given the supposition that enterprises want to build trust, this type of response is no longer acceptable. The framework for use must be clarified and the rights and duties of the respective players should be precisely defined in terms of their Internet use.

II – General philosophy: a presumption of professional Internet use at work, with the possibility of reasonable and controlled personal use.

A. The Forum considers that the Internet remains above all a tool that is made available to the employee for professional use

Personal use cannot be considered an employee's right. Nothing requires the employer to supply Internet access to employees for personal use. In fact, access is first and foremost dependent on an employee's economic activity. If access is not professionally necessary, the company has no obligation to provide it. Similarly, in the case of abuse, nothing prohibits the enterprise depriving the dishonest employee of access to Internet.

Some enterprises have decided to put interactive terminals in place that allow their employees to consult web sites or messages during their breaks. Such initiatives are obviously very positive. For all that, they remain the choice of individual enterprises and not an obligation.

B. However, the Forum considers it is difficult to refuse in principle personal use of the Internet in the work place

Such a ban would not seem to be illegal in principle. The Forum considers that internal regulations covering it would not be unlawful whilst Internet in the work place remains a tool the employer has made available to the employee for purely professional purposes.

However, **an absolute ban is difficult to apply legally**, as ignoring it cannot automatically be penalised if the employee were to decide, despite the ban, to use Internet for personal purposes.

In the first place, in accordance with article L. 122-43 of the employment code any penalty has to be in proportion to the offence committed. The principle of proportionality prohibits any penalty if an employee's use is reasonable. It would be difficult for an employer to sack an employee for an innocuous message exchanged with a husband or wife. The penalty would be considered disproportionate in relation to the offence.

In the second place, it would still be difficult for the employer to provide proof of prohibited personal use. In its Nikon decree on 2 October 2001⁽²⁹⁾, which we will return to, the Court of Appeal considered that, even if there is an absolute ban on personal use, the employer may not read personal messages sent or received by the employee via a computerised tool made available for work purposes. Protection of the confidentiality of correspondence will in practice prevent employers providing proof that the ban was ignored.

Furthermore, an absolute ban would appear socially difficult to accept. It is out of step with employees' current practices and in particular future practices. When equipment with Internet access is installed, personal use nearly always follows and furthermore enters into the realms of the process appropriating technology. The ban is therefore ignored and loses credibility. It is in addition, contrary to the employer's desire for employees to be independent and responsible.

²⁹ - Soc., 2 October 2001, Nikon France SA c/ M. Onof, Bull. civ., V, n° 291, p. 233.

Enterprises should therefore accept personal use of the Internet by employees that have access to it. However, this personal use should remain reasonable. The employer then has a basis for monitoring use.

III – Methods of monitoring personal use: fair, transparent and proportionate monitoring.

Monitoring of personal use by employers' should not encroach on the employees' fundamental freedoms, which also apply in the work place. It therefore has to be carried out in accordance with the requirement for proportionality and justification covered by article L. 120-2 in the employment code. It states that "*Nothing which is not justified by the nature of the task to be accomplished nor proportionate to the aim may restrict individual or collective rights and freedoms*". Furthermore, it should be carried out fairly and transparently in order to establish the conditions for trust between employers and employees.

The Forum considers that three essential conditions should underpin monitoring in order for it to be carried out effectively.

A. Employees should distinguish professional documents from those they consider personal

In the work place, employees are first and foremost considered to be in a professional environment. Thus, if they have an electronic mailbox or a computer it is also first and foremost in their capacity as an economic agent of the enterprise. Thus, nearly all e-mails sent to or by an employee are professional e-mails relating to his or her activity. Similarly, nearly all files stored on the hard disk are files relating to the enterprise. Employees then only use the tools made available to them by the enterprise on behalf of the enterprise. It is usual for the enterprise to be able to access all messages or files concerning its activity in the framework of, for example, an absence caused by illness or because of a reduction in working hours.

On the other hand, if employees want to protect information they consider personal, they should distinguish it from professional information which can be read by the employer and which is not covered by the confidentiality of correspondence.

1°. Employees should distinguish personal mail from professional mail

The confidentiality of correspondence is a public freedom covered by articles 226-15 and 432-9 of the penal code (³⁰). It is also covered by article 8 of the European Convention of Human Rights as a part of personal life. It stipulates that "*any person has the right to respect for his or her private life and family, for his or her home and correspondence*".

³⁰ - This article 432-9 of the penal code prevents any act by a person with public authority or responsible for a public service to order, commit or facilitate, excepting those cases provided for by the law, the interception or diversion of correspondence sent, transmitted or received by telecommunications, and prevents their content being used or divulged.

For a very long time, French judges have recognised employees' rights to confidentiality of correspondence (³¹). An employer opening, with malicious intent, an envelope addressed to an employee is committing a criminal offence (³²). It has been adjudged that electronic mail is comparable to the correspondence protected by the criminal code (³³). As previously mentioned, in its Nikon ruling the Court of Appeal also considered that an employer cannot, without violating the confidentiality of correspondence, read personal messages sent or received by an employee.

However, the majority of electronic mail sent or received by employees is in fact addressed to the enterprise for which they work. Furthermore, criminal jurisprudence considers that when correspondence is addressed to a member of an organisation showing their name and membership of that organisation, without any indication on the envelope that the correspondence is of a personal nature and that the content of this correspondence has been addressed to the individual in their capacity as a member of the organisation, the latter being the true recipient, there is no infringement of the confidentiality of correspondence (³⁴).

The Forum considers this interpretation of confidentiality of correspondence should apply to electronic mail received or sent by an employee in an enterprise, whether by Internet or by the enterprise's internal e-mail system.

In the absence of any other indication, an electronic message should be considered a professional message and not a personal one. The enterprise should therefore have access to these, if only to reply to e-mails received during an employee's absence. Consequently, employees should ensure that personal e-mails are distinguished from professional ones.

This distinction can be made in two ways:

- an employee may decide to send and receive personal mails in a personal mailbox hosted on a server outside the e-mail system. An employer would then in principle have access to all messages in the professional mailbox;
- an employee may indicate "personal" in the reference line of their message. They are then showing that they want the message to be considered as personal correspondence, protected by the confidentiality of correspondence, which presupposes that the employer may not read the contents.

Nonetheless, if a message is addressed to an employee without the mention "personal" in the reference line and the content of this is in fact personal and therefore protected, it is the network administrator's responsibility to read it and if necessary reclassify it as a personal message.

The Forum considers however, that encryption does not appear to be a realistic solution for ensuring the confidentiality of employees' personal messages.

³¹ - See, Paris Court of Appeal 17 June 1938, Mas and Association de la Critique Dramatique c/ de Rovera et Signorino, Dalloz Hebdomadaire, p. 520.

³² - Crim., 18 July 1973, Bull. Crim. No. 336.

³³ - Paris Court of Appeal 17 December 2001, confirming the Paris magistrates court decision of 2 November 2000.

³⁴ - Crim., 16 January 1992.

Firstly, there is little chance of an employer letting encrypted messages that may carry viruses into the network. Secondly, the limitations of encryption would not in any event guarantee the inviolability of the message. Nothing would prevent a message being decoded if the encryption were not very powerful. The solution therefore does not lie in the use of technology. It lies primarily in establishing the reciprocal trust of employers and employees.

2°. Employees should distinguish personal files on the hard disk

In relation to the hard disk, the distinction between the personal sphere and the professional sphere may be made by creating a directory labelled "personal" on an employee's hard disk. This could contain files the employee considers personal.

3°. Employees have to undertake not to transform professional information into personal information

The distinction between personal and professional files and messages allows the confidentiality of personal life of the employee to be protected in the work place. Nevertheless, employees must undertake not to qualify professional information as personal information. This obligation should be mentioned in the internal regulations. It results from the principle according to which "*the work contract is executed in good faith*"⁽³⁵⁾.

B. Fair and transparent methods of monitoring should be established

Trust comes by establishing clear rules on the use of Internet. However, it also requires employers indicating what monitoring methods will be used to ensure these rules are respected.

1°. Technical monitoring may always be carried out

Technical monitoring is part of the normal functioning of the enterprise's information system: it should, with the appropriate software, be able to monitor and if necessary reject attachments to messages or downloaded files that may contain computer viruses. It should also be able to prevent too voluminous files being downloaded (for example videos). This monitoring, which is indispensable for the security of the enterprise, does not monitor the content of the information. It is "blind" monitoring that does not encroach on employees' private lives.

2°. Employers may also monitor volume if necessary

This may be carried out in relation to Internet site visits: the number of pages consulted, overall connection time etc. It may also be carried out in relation to e-mails, with an employer having access to the number of messages sent or received as well as the size and nature of the attachments.

³⁵ - Article L. 120-4 of the employment code inserted by the law of 17 January 2002.

No doubt such monitoring cannot be systematically carried on in relation to all employees, if not only because of the size of the task it would represent. However nonetheless, it is legal and may be legitimate if it is a question of detecting abuse, such as excessive connection time. It may also monitor whether the designation "personal" is used advisedly. Thus, sending a large file of customers would be detected by this monitoring of volume even if the e-mail has been designated personal... Similarly, the directory "personal" on the hard disk may be the object of a volume check (number of files held, size of these files, nature of the files).

3°. Monitoring the content of information should be limited

Given the principles outline above, the employer cannot access e-mails designated as personal or re-classified as such by the administrator or access files in the personal space on the hard disk. In principle, the employer can only access information of a professional nature.

Such measures may nevertheless be moderated. Thus, it may be necessary to make provision for employers to have access to personal messages or files in exceptional situations, for example if a criminal act has taken place. In this case, it is likely that the principle of proportionality covered by article L. 120-2 of the employment code would not go unrecognised.

The Forum nonetheless considers that putting such an exceptional procedure in place should be controlled. It should firstly be precisely described in an appendix to the internal regulations relating to the use of Internet. It should also make provision for specific safeguards for the employee. Thus, disclosure by the network administrator of information requested by the employer may only take place after the employee has been informed about the check and that the check has been carried out in the presence of a third party, for example a staff representative.

In relation to visiting **web sites**, the Forum considers that employers should be able to install **filtering software** that would allow most problems the enterprise may encounter to be dealt with, for example in relation to visits to detrimental or improper web sites or network overloading caused by excessively large video files (for example 2 Mo). However, representative institutions should be informed of the filtering methods (categories of filters put in place, list of key words).

4°. Employers should remind employees of the need to protect their information and should inform them of the length of time data is kept

Respecting the confidentiality of personal data lies in using passwords. The enterprise should make provision for their use so that employees can protect their personal information. In fact, there should be safeguards to ensure that employees are not able to access information concerning their colleagues if they are not authorised to do so. To illustrate, an employee responsible for drawing up pay slips should not be able to access the employee assessment file if not authorised to do so.

Furthermore, the enterprise should inform employees of the length of time connection data collected during monitoring is kept. **The Forum agrees with the recommendation issued by CNIL that connection data should be kept for a maximum of 6 months** ⁽³⁶⁾.

C. Network administrators should protect the confidentiality of personal data

Network administrators have an administrator password allowing them to access file servers, web servers and e-mail servers. Potentially they are able to read all data received, sent or created by employees.

The Paris Court of Appeal, in a ruling on 17 December 2001, stated that it "*it is part of the function of a network administrator to ensure the normal functioning and security of the network*" which implies they have access to all the data in the network in order to be able to resolve technical problems or ensure the security of the system. However, network administrators may not use the content of the information they come across in this way when disclosure would infringe the confidentiality of correspondence. This obligation may, as we have seen, require the administrators to re-classify messages as personal if they see such is the case.

Above and beyond this secrecy, network administrators should ensure they do not disclose personal information to anyone in the enterprise, including line management and colleagues, concerning an employee that they may have learned about in the framework of their job. Other than the content of messages marked "personal", confidentiality should also be extended to the content of files that the employee may have stored in the personal space on the computer.

The Forum considers network administrators' obligation to maintain confidentiality should be included in an appendix to internal regulations relating to information technologies in order to ensure complete transparency. Thus, employees will be aware of the extent of the protection accorded to the content of data that they consider personal.

Moreover, **the Forum thinks that in addition to this, it is necessary to give network administrators the cover of proper professional secrecy in law.**

This secrecy should not only cover confidentiality of correspondence but all the employees' personal data, such as for example their files. It would fall within the remit of the network administrator and not to a designated named person. It would also explicitly make it a criminal

³⁶ Article 29 of the law on day to day security of 12 November 2001 requires telecommunications operators to delete or make connection data anonymous with two exceptions connected to the requirements of invoicing and the requirements relating to criminal investigations. However, although this point deserves to be explicitly confirmed by the texts, enterprises cannot easily be considered as telecommunications operators within the meaning of the provisions of this law. In fact, they have independent networks that they open up to their employees and not to the public. They would not therefore be subject to the obligation to delete or make connection data anonymous. These national provisions should be brought closer to the stipulations in the cyber-crime convention of 23 November 2001 <http://conventions.coe.int/Treaty/FR/Treaties/Html/185.htm> that requires states to adopt the necessary measures to allow computer data to be conserved.

offence for the employee's line manager or the network administrator's line manager to ask the network administrator to violate professional secrecy.

IV – Legal instruments for putting these principles into action: an appendix to internal regulations and transparent information

A. The rules for Internet use should be defined in an appendix to the internal regulations

Most enterprises with Internet access have adopted charters defining the rules of use that should be respected by employees.

The content of these charters varies greatly. Some are only general reminders of instructions about caution and proper use of technologies. Others, however, impose obligations that may be subject to sanctions. Similarly, the status of charters differs from enterprise to enterprise. Some take the form of an appendix to internal regulations, others are merely documents that are brought to the attention of employees. Some enterprises require employees to subscribe to text whereas others are content to bring the stipulations of the charter to their attention.

The importance of the charters is incontestable: they often allow an initial clarification of the rules that apply in an enterprise; they also encourage internal discussions with staff representatives and employees that reconcile the different points of view. In this respect, they play an eminently positive role in ensuring employers and employees take the problems connected to information technology on board.

Nevertheless, if charters have not been drawn up in accordance with internal regulations, the essential instructions they contain cannot lead to disciplinary sanctions. In fact, documents containing general and permanent instructions in the field of health, safety and discipline are considered adjuncts to the internal regulations that should be adopted in the same way.⁽³⁷⁾ To be applicable, the provisions in the charter, supposing they are not limited to purely technical regulations or etiquette, should therefore be adopted according to the procedure for the internal regulations. They should be submitted to the works council for their opinion, or failing that to the staff representatives as well as, if necessary to the health and safety committee. They should also be publicised and should be forwarded to the factory inspector⁽³⁸⁾. If the rules are modified the same procedure should be followed.

The Forum recommends that the principles outlined above should be incorporated into an appendix to the internal regulations, after prior consultation with staff representation institutions, or indeed after negotiations if the partners so wish.

³⁷ - In accordance with article L. 122-39 of the employment code.

³⁸ - Article L. 122-36 of the employment code.

B. Employers should inform employees of how Internet use is monitored

Generally speaking, the introduction of information technologies to an enterprise should give rise to information and consultation with the works council in accordance with article L. 432-2 of the employment code. Too often, enterprises seem to be ignorant of this obligation.

More specifically, article L. 432-2-1, paragraph 3, of the same code states that "*The workers council is informed and consulted about the means or techniques allowing the monitoring of employees activity, prior to introducing them in the enterprise*".

If the works council has not been consulted, the proof obtained by the surveillance measures will be considered illegal in employment law and may not be used in the event of a dispute with an employee (³⁹).

Furthermore, it is also necessary to inform employees on the methods of monitoring. This obligation of transparency results from article L. 121-8 of the employment code that states that no information concerning an employee or an applicant for employment personally may be collected by a mechanism that has not previously been brought to the attention of the employee or applicant for employment. Again, a mechanism for monitoring that has not been brought to an employee's attention may not be used in the event of problems (⁴⁰).

Generally, the Forum considers that drawing up rules for the use of Internet in the work place should provide the opportunity for in depth discussions with employees and staff representatives.

Only this dialogue will establish trust between employees and employers and move towards a consensus on the rules for Internet use in the work place and in working hours.

C. Employers must respect the obligation to make a declaration to the CNIL

In accordance with the law of 6 January 1978, nominative automatic information processing should be declared to the CNIL. If this formality is not respected, it is penalised by a prison term of 3 years and a fine of 45,000 euros (⁴¹).

In addition, in employment law, the absence of a declaration to CNIL would prevent employers using the data obtained by the monitoring system in the event of a dispute with the employee, such proof being considered illegal (⁴²).

³⁹ - Soc., 15 May 2001, Aymard c/ Cabinet Regimbeau, Bull. civ., V, n° 168, p. 132.

⁴⁰ - Soc., 20 November 1991, Néocel, Bull. civ., V, n° 519, p. 323. In criminal matters, however, such proof would be admissible.

⁴¹ - Criminal code, article 226-16.

⁴² - CA Paris, 7 March 1997, Société Suisse d'Assurances Générales.

PART THREE: THE CHALLENGE IN TERMS OF SOCIAL DIALOGUE

If information technologies profoundly modify the ways in which work and relations between employers and employees are organised, they also appear to be transforming the methods of social dialogue in enterprises. Of course, it is an illusion to believe they could replace staff representatives' traditional communication and action methods. Direct physical contact between employees and their representatives continues to be indispensable. Furthermore, today, consulting the staff representation institution pages, and in particular trades union pages, on intranets continues to be of little importance if the figures put forward by some enterprises that have signed agreements in this field are to be believed. However, information technologies may turn out to be a useful and valuable addition to the traditional channels. They may in some cases, allow staff representation institutions to reach employees with whom direct contact is difficult because of geographic distance, for example when an employee works from home or is on a different timetable. They may also encourage greater closeness and better follow up of the relationship between staff representatives and employees. By their very nature therefore they may be able to revive and enrich social dialogue in an enterprise.

This evolution is not limited to trades union organisations. It also concerns other staff representation institutions such as staff delegates, health and safety committees and works councils. In this last case, the use of information technologies already seems to be a given, if only for informing employees about cultural or sporting events...

Today, the phenomenon is limited: while being conscious of the possibilities offered by intranets and e-mail systems for reviving the methods of communication with employees, management and trades unions are still acquiring these tools. These technologies are recent and some staff representatives are poorly prepared, or indeed trained, for using them to carry out their functions. In the absence of clarity about the use that may be made of these tools, employers appear to view their use by staff institutions with some circumspection. As a result, there are only some twenty agreements with enterprises.

Nonetheless, this problem is a major issue for the future of enterprises. In organisations that are built around information systems, the dialogue between management and trades unions has to adapt to technological changes; these may even in some cases revive it. Management and trades unions are gradually becoming aware of how important it is. Thus, access to information technologies by trades union organisations was one of the points raised in the joint position on ways and means of increasing collective negotiation of 16 July 2001, signed between management and trades unions, referring this issue back to branch negotiations (www.medef.fr/refondation/refhtm/ref05-negociation-collective.htm). Similarly, the question was enlarged upon in the ministry's recommendations of 19 June 2001 relating to the civil service for a ministerial charter on the use of information and communication technologies by trades union organisations in the civil service (www.fonction-publique.gouv.fr/reforme/admelec/syndicats2.htm).

In this context, the Internet Rights Forum intends to highlight a number of points to guide thinking on the use of information technologies to revive the dialogue between management and trades unions and to allow negotiated industrial modernisation.

I - Observation: the employment code does not make provision for staff representatives to have access to an enterprise's networks

In a number of articles, the employment code provides for certain information from staff representatives to be displayed. Article L. 412-8 of the employment code thus makes provision for "*trades union communications being freely displayed on notice boards reserved for this use*". Similarly, staff representation institutions also have the possibility of displaying certain information (⁴³). Article L. 412-8 also provides that the "*trades union publications or handouts may be freely distributed to company workers on its premises at the beginning and end of working hours.*"

It is debatable whether article L. 412-8 of the employment code applies to digital media.

In relation to what constitutes a notice board, article L. 412-8 does not in principle seem to exclude electronic display of trades union information on a page on an enterprise intranet site. However, the question becomes more complicated if account is taken of the possibility of links to external sites. Would it still fall within the concept of displaying trades union communications?

For e-mails, jurisprudence has sometimes made parallels between old and new methods of communication, considering that access by staff representatives to the company e-mail system is possible. Thus, a trades union could communicate by electronic mail insofar as it does not affect the functioning of the network, that only employees receive messages and that handouts are read outside working hours (⁴⁴). In other cases, jurisprudence likens the new tools to the traditional channels provided for in the enterprise's contractual provisions. Thus the Rouen court considered that the possibility provided for in the contractual provisions for trades union sections to distribute circulars and trades union magazines within the enterprise using the internal mail mechanisms would allow handouts to be distributed by e-mail (⁴⁵). However, it is difficult to put sending e-handouts into the legal framework of the beginning and end of work.

In any event, other more interactive forms of communication, such as discussion forums organised by trades union organisations on the enterprise intranet site, do not appear to be covered by the current article L. 412-8 of the employment code. These cannot be considered

⁴³ - Article L. 424-2 of the code thus provides for staff delegates being able to display information that they are required to make known to the staff in obligatory locations designated for trades union information and at the doors into the place of work.

⁴⁴ - Nanterre court 25 June 1990.

⁴⁵ - Rouen court 6 September 2001, Caisse d'épargne de Normandie c/ CGT CEHN and Couralet.

similar to displaying trades union information or distributing handouts. It is also difficult to see how they could be included in the framework of the monthly meeting that trades union sections are able to organise for their members outside working hours on the enterprise's premises (⁴⁶).

Given these uncertainties, the Forum observes that staff representatives cannot demand access to an enterprise's network on the basis of the current provisions in the employment code.

In reality, given the current state of the texts, an employer has to offer the means of passing on information to staff representatives. Once their obligations have been fulfilled, in the vast majority of cases with a wooden notice board or distributing paper handouts, the employer is not legally required to give staff representatives access to their e-mail system.

It is also true that a straightforward comparison of the different modalities of information and communication appears to be problematic. Going from a paper medium (display on a wooden notice board or distributing handouts) to a digital medium gives rise to very different uses and more than anything presupposes the use of an enterprise's essential infrastructure. In addition, in nearly all enterprises, all employees do not have access to the intranet or e-mail system. These differences prevent a straightforward substitution of old information and communication methods for new.

II – Position: staff representatives should be able to access intranets and e-mail systems

Today, it seems natural to give staff representatives access to the enterprise's infrastructures. Of course, such access **can only be envisaged on condition that these networks exist and are widely used by employees in the enterprise.** In this respect, we can only emphasise once more the wide variation in situations in enterprises in relation to the development of information technologies. These differences prohibit any attempt to impose uniform solutions on all companies. We understand that small companies cannot put an intranet or an e-mail system in place purely to develop the dialogue between trades unions and management. Staff representation institutions can only have access if these tools exist.

When the tools do exist, a refusal in principle to authorise access by staff representatives to communication tools used as a matter of course in the enterprise appears to be incompatible with a desire to promote active discussions between management and trades unions. It is also difficult to explain this refusal to employees that use these tools every day and that the employer wants to act responsibly. The danger in a refusal on principle is that it could be interpreted as a symptom of poor relations between management and trades unions. It would also be a sign of a lack of awareness of the importance of information technologies for developing the company, as in this field, social change appears to be indissociable from economic development.

Furthermore such a decision risks being counterproductive. In fact, on Internet staff representatives can easily find the resources refused to them within the enterprise. Thus, it is technically not very complicated to send e-mails to employees via an external server. Similarly, trades unions may be tempted to create an Internet site including information on the enterprise

⁴⁶ - Article L. 412-10 of the employment code.

and reproducing hand-outs ⁽⁴⁷⁾. In this situation, these sites escape employment law and are subject only to common law. The employer of course is not short of ways of dealing with any potential problems. They may put pressure on the site hoster or use the limits provided by the laws relating to defamation or copyright on brands or logos. However, even if the enterprise wins in legal proceedings, the danger is that their image is significantly dented by such a dispute. In this respect, there is the example of the jeboycottedanone web site. The enterprise certainly won its case in the courts, but given the effects on its image, the result appeared to be a Pyrrhic victory...

The Forum considers therefore that staff representation institutions should have access to information technologies provided by the enterprise to communicate between themselves and with employees.

However, and as previously mentioned, trades union information via information technologies can currently only be an addition to information distributed by traditional channels such as wooden notice boards and paper handouts. In nearly all enterprises, since many employees do not have access to these tools, new technologies cannot replace traditional communication methods.

III – Methods of implementing access for staff representatives: a detailed agreement

While there is still no provision for it in the employment code, access by staff representation institutions to intranet and the e-mail system will have to be covered by signed agreements. Such agreements appear to be a suitable instrument that will be able to take the range of situations found in enterprises into account. They will allow **industrial modernisation negotiated between the players**. These agreements should fulfil a variety of principles:

A. Access to information technologies should be granted to all staff representatives with the same conditions relating to rights and duties

Jurisprudence lays down that access by staff representatives should respect the principle of equality between trades unions.

The court in Versailles considered that an employer cannot unilaterally reserve access to the company's computerised tools to a single trades union and refuse it to others. Access to these resources for one particular trades union would constitute a privilege and would ignore the principle of trades union pluralism ⁽⁴⁸⁾. This appears to apply to the use of electronic communication resources.

Furthermore, when a collective agreement has been signed with certain trades unions on accessing information technologies, a non-signatory trades union may also ask to benefit from it. In effect, the Court of Appeal considers that the provisions in an agreement or collective convention that improves the exercise of trades union rights are fully applicable to all

⁴⁷ - See for example the CGT Pizza Hut site (<http://cgt.pizzahut.free.fr>).

⁴⁸ - Versailles court, 20 November 1998, Bull c/ FGMM-CFDT.

representative trades unions, without any discrimination between those that have signed or subscribed and those that have not (⁴⁹).

To ensure the rules of the game are respected, some enterprises have chosen not to sign a collective agreement but to sign bilateral agreements with each trades union organisation subjecting access to the enterprise's information technologies to certain rules. However, in a decision on 31 May 2002 the court in Nanterre considered that it is illegal to refuse certain trades unions access to the enterprise's communication tools, even if it is based on the trades union organisation's refusal to comply with the rules laid down in the bilateral agreement. (⁵⁰).

This obligation should not, however, mean that non-signatory trades unions are free from the rules of use applying to information technologies and the guiding principles set for signatory trades unions. The principle of non-discrimination between trades union organisations laid down in the Cegelec judgement cannot result in some trades unions benefiting from the agreement without respecting the commitments that ensure proper functioning of the information system. If the stipulations in the agreement benefit all trades union organisations, the rules laid down should also apply to them all. Jurisprudence previously cited of the Nanterre court took this view, judging that the charter applies in its totality to any beneficiary, whether or not that beneficiary is a signatory.

B. Some guiding principles should be provided for in the agreement defining the use of information technologies by staff representatives

1°. The agreement should be concluded for a set period of time

Technological evolutions are very fluid. Given these changes, it would appear preferable to provide for a time limited agreement that would allow any necessary modifications and adjustments in the future.

2°. Staff representatives should have complete freedom as to the content of the information sent, at the same time as being responsible for it

It is not up to the employer to control the content of the information provided. It is the responsibility of the staff representative to take full and complete responsibility for the content of any information distributed.

This responsibility presupposes that staff representation institutions provide themselves with the necessary organisation to do so. It would thus be desirable for them to set up a procedure for approving information before it is put on line or sent by e-mail. Similarly, a designated person within the institution should be responsible for the quality of the information put on an intranet site. Finally, a moderator should be provided to chair trades union forums on intranet. These organisational requirements should be included in order to determine the tools that should be covered by the agreement.

⁴⁹ - Cass. soc., 29 May 2001, Union Nationale des Syndicats CGT Cegelec c/ Société CEGELEC, Bull. civ., V, n° 185, p146.

⁵⁰ - Nanterre court, 31 May 2002, Fédération des Travailleurs de la Métallurgie CGT c/ SA Renault.

3°- The use of these tools should not hinder the normal functioning of the enterprise

Non-negotiable technical rules may be laid down to ensure the security of the enterprise network. Security requirements can often be dealt with by a joint security mechanism. Thus, the enterprise may want to limit the size of attachments to e-mails from staff representatives so that network functioning is not disrupted. However, specific rules could also be considered: it may therefore be possible to restrict mass mailings to particular times in order to avoid saturating the enterprise's internal network, for example during the night using an automatic e-mail system.

The agreement may also provide for **limiting the number of mass mailings to all employees in order to avoid the risk of repetitive mailings (or spam) of e-handouts**. Trades unions are certainly not interested in duplicating messages and thus perhaps arousing the irritation of employees. There may nevertheless be a great temptation to send a lot of mass mailings at tense periods, either at the approach of professional elections, or perhaps during a trades union dispute.

4°- The intrinsic interactivity of these tools should be maintained.

Implementing essential security rules should not provide a pretext for removing the inherent interactivity of these tools. Thus, banning of links outside intranet pages for security reasons may be admissible in the experimental stage, but rapidly appears out of step with enterprise's practices when they retain wide Internet access. Employers' fears about the time spent by employees consulting trades union sites may often be behind these explanations. Such doubts are understandable but do not justify making new electronic communication tools simple passive vectors for distributing information; that would be to deny their essential characteristics. Interactivity should therefore be authorised for staff representation institutions, given that employers can always monitor the time spent by employees using the previously outlined monitoring methods.

5°. The principle of employees' freedom of choice to accept or refuse messages from staff representatives should be safeguarded

In fact, employees have the right to refuse to receive trades union information from staff representatives. Solutions must therefore be found. Firstly, the origin of the message should be identified in the reference line by indicating whether it is a trades union message. A system for removing the subscription of an employee from the staff representation mailing list should also be provided for.

6°. The confidentiality of exchanges between employees and staff representatives should be ensured

Employers should not be able to read messages sent by employees to their representatives or indeed between the staff representatives themselves. Similarly, employers should not be able

to trace the number of visits made by an employee to the trades union pages of the intranet site.

This obligation should constitute part of the obligation to maintain confidentiality applying to network administrators, in accordance with professional secrecy as described earlier.

IV – Electronic consultation procedures should gradually be introduced

Today, classic employee consultation procedures may seem clumsy and expensive. In fact, organising consultations requires major and complex logistics in terms of intranet. Furthermore, mobile employees or multiple sites complicate the task of organising these procedures for those responsible for human resources.

The potential of information technologies could usefully facilitate employee consultations. It is advisable to note in relation to company functioning that the public authorities have specified the conditions for using information technologies for voting at shareholders' annual general meetings in the 3 May 2002 decree on enforcement of the law of 15 May 2001 relating to new economic regulations. It has also been adjudged that an association may be authorised to convene, hold and carry out deliberations by Internet under the control of a legal official⁽⁵¹⁾.

Nevertheless, in the current state of the law, there is no provision for electronic voting in professional elections, the methods for which are strictly set in the provisions of articles L. 423-13 and L. 433-9 of the employment code⁽⁵²⁾. However, whilst respecting the principles of fairness and equality, nothing prevents electronic ballots in non-obligatory consultation procedures. Indeed, some enterprises are experimenting in this field.⁽⁵³⁾

The Forum is in favour of the principle of electronic voting within enterprises if the technical conditions are able to guarantee the confidentiality and fairness of the ballot.

The confidentiality and fairness of the ballot should be guaranteed so that electoral operations are carried out in a climate of trust. If these guarantees are provided, in particular by implementing suitable technical systems, the Forum considers that electronic voting for professional elections could be organised. It is up to the legislature to look into this question further.

V – Far off horizons: modifying the employment code to become more technologically neutral.

It has already been mentioned that the employment code does not clearly take into account use of information technologies by staff representatives to communicate with employees. Agreements on this point are developing but practices are still uncertain. It is still too soon to look back at the experiments underway and at any difficulties that may arise in the use of

⁵¹ - Tribunal de commerce de Paris, 10 October 2001, Dalloz 2002, p. 1669.

⁵² - These articles lay down that « *L'élection a lieu au scrutin secret sous enveloppe* ». The caselaw has clearly forbidden the remote vote, Soc., 20 Oct. 1999 : Bull. civ. V, no. 390.

⁵³ - Like Liberty Surf on the 35 hour week.

these new tools. Added to these limitations is the great variety of situations in enterprises in relation to the introduction of new technologies.

The Forum considers therefore that at this stage modifying employment legislation to more explicitly take account of the use of these new tools by staff representatives would be premature, or even counterproductive. An introductory and experimental phase for agreements is necessary in the framework of branch collective agreements provided for in the common position issued on 16 July 2001.

Nevertheless, the Forum considers that in the medium term, any legislative changes should be based on the results of these experiments.

Two scenarios are possible in principle.

It would be possible to introduce special provisions into the employment code relating to the use of companies' computer tools. Thus just as notice boards and the distribution of handouts are provided for in the employment code, rules relating to the use of intranet and the company e-mail system could be defined.

The other solution would be to make provision for greater technological neutrality so that the rules are not set according to the medium used (paper, digital format) but according to use. The experimental period that is beginning should provide the opportunity to delimit these uses more effectively. However, we can already see that communications from staff representatives have different purposes. Thus we see the information for employees from staff representatives and interactive communication between trades unions and employees. Similarly, we can distinguish information that is available for employees to find and that brought to their attention, which is the equivalent of push/pull.

The Forum believes the second solution of technological neutrality should serve as the basis for future deliberations. It would mean that employment legislation is more appropriate, avoiding imposing a framework that would be likely to become obsolete as technological advances are made.

COMPOSITION OF THE WORKING GROUP

Antoine Cristau, Doctor of law, course director at Paris I University and the institute of political studies in Paris

Jean-Michel Dusuzeau, Information technology director representative at the SME development bank

Eric Godard, Director of information systems, Siemens

Yves Lasfargue, Researcher and consultant

Antoine Lyon-Caen, Professor at Paris X University, President of the French employment law association

Jean-Pierre Quignaux, Member of the Forum's guidance committee, UNAF

Jean-Emmanuel Ray, Professor of employment law at Paris I University

Maurice Ronai, Project leader for society and information technologies at the State Planning Commission

Jean-Christophe Sciberras, Director of industrial relations, Renault

Laurent Setton, Head of service in the department of employment at the Ministry of Employment and Solidarity

Hélène Tissandier, Lecturer in employment law

Philippe Waquet, Most senior advisor to the Court of Appeal

Isabelle Falque-Pierrotin, President of the Internet Rights Forum guidance committee

Study reporters: **Mathieu Hérondart**, Council of State official and **Marie-Françoise Le Tallec**, Internet Rights Forum representative

LIST OF PEOPLE APPEARING BEFORE THE WORKING GROUP
--

The following people appeared before the working group:

Verveine Angeli, Delegate SUD-PTT

Jacques Barthélémy, Emeritus barrister

Christine Baudoin, Barrister, at Courtot, Lemetais and associates

Arnaud Belleil, Consultant advisor Cecurity.com, course director at IEP in Paris

Hubert Bouchet, Vice President of CNIL, Secretary General UCI-FO

Jean-Paul Bouchet, Deputy Secretary General of CFDT-cadres

Bernard Boudin, Industrial relations advisor, HR group BNP Paribas

Karine Boullier, Director of Studies, enterprise and personnel

Dominique de Calan, Deputy leader of the metallurgical and mining industries union

Patricia Chapuis, Secretary General SUD-PTT

Jean-Denis Combrexelle, Director of industrial relations at the Ministry of Employment and Solidarity

Alain Foret, Vice President of the young directors' centre

Jean-Marc Icard, National Secretary CFE-CGC

Alain d'Iribarne, Director of research, economy and employment sociology laboratory, CNRS

Gilles Jolivet, Queen's Counsel, Baker & McKenzie

Pierre-David Labani, Confederal Secretary CFDT

Bernard Massas, Secretary General UCAPLAST - CGPME

Philippe Masson, National Secretary UGICT-CGT

Denis Meis, Director of industrial relations, France Telecom

Ariane Mole, Barrister, Bensoussan and associates

Florence Richard, Barrister, cabinet Barthélémy

Michel Sursingéas, Delegate CFTC

Dominique Tellier, Director of industrial relations MEDEF

Alexandre Tessier, Director, French association of private enterprises

Martine Zuber, Development manager, FCC-CFDT