A COMPARATIVE STUDY OF THE IMPACT OF ELECTRONIC TECHNOLOGY ON WORKPLACE DISPUTES

Jean-Emmanuel Ray† and Jacques Rojot††

"An office at home and at home at the office." The new technologies of information and communication (NTIC)[1] blur the traditional borders separating work and home. If, traditionally, the "intellectual worker" was able to work anytime anywhere, carrying most of his tools in his brain, technological progress has extended this dubious privilege to more and more employees. From now on, when one wants to work, one can—but must one work if one can? All large French corporations use electronic mail, and have intranets and Internet connections. Even though only 32% of households in France have a personal computer and less than 25% are connected to the Internet,[2] with a total of around 10 million business and personal Internet subscribers,[3] the NTIC has moved out of the occupational area to impact personal and even family and social life.

Currently France has no specific statute covering at work use of electronic mail, intranets, or the Internet. However, instead of a legal void, this creates rather a legal traffic jam,[4] with several areas of the law (privacy, freedom of expression, mail status) applying concurrently. Moreover, the decline of the empire of industry and the rise of an economy of services has left the labor lawyer, whose expertise was based on the relationship of subordination, without that unifying concept thread.

Although the NTIC obviously are a source of freedom for subordinates to whom they grant temporal and geographical

† Professor of Labor Law, University of Paris 1, Panthéon-Sorbonne.
†† Professor of Industrial Relations, University of Paris 2, Panthéon-Assas.

1. Hereinafter, NTIC.

2. Even lower numbers have high speed connections. Only 240,000 French households are connected that way in contrast with 488,000 British and over one million Germans.

3. *See* http://www.internet.gouv.fr.

4. On these theoretical aspects, *see* J.E. Ray, *Le Droit du Travail à l'Epreuve des Nouvelles Technologies de l'Information et de la Communication*, *in* EDITIONS LIAISONS (2nd ed. 2001), *reprinted in* 4 DROIT SOCIAL 5 (Jan. 2002).

autonomy, the numerous system breakdowns notwithstanding, they are also the source of sometimes very heavy organizational intrusions. Thus, while 83% of French wage earners use the office phone for personal purposes and two-thirds use office faxes and e-mail to the same end, 76% receive work-related calls outside of working hours and 69% bring work back to their homes.[5] Accordingly, NTIC work can invade all levels of private life and even its spatial sacred temple, the home.

I. TELEWORKING AND OTHER ISSUES

From the situation of a manager taking some work home at night, to the situation of the full-time computer linked homeworker, telework covers an extraordinary variety of situations. IBM France, for instance, has created throughout Paris "neighborhood offices" equipped with secretarial services and all the necessary connections that allow the 1600 employees who take advantage of this opportunity to work there from a few hours, up to three days a week. These workers report to their manager, who must consent to the arrangement, and remain attached to their original job position and location. Other French corporations have created "pass through" offices, within their existing locations, to allow traveling employees to find a free and well-equipped office, when needed. In addition, "telecenters," such as the one in Villard-de-Lans employing 40 employees, are shared by several different corporations, each of which rents floors for their own establishments. Also, "tele-actors" or "tele-advisors" answer calls to hotlines, either during or outside usual working hours, sometimes on weekends or at night, and from the premises of the enterprise providing a related service, or from the office of a subcontractor or from a call center, located almost anywhere, including overseas. One should probably not consider as teleworkers the employees of small, geographically dispersed subcontractors providing services, such as secretarial, from a distance. Finally, the most frequent case is probably the one of "nomadic employees" such as consultants, salespersons, or maintenance employees, more and more home-based, without an office. However, in French Labor Law this type of work seldom alters the nature of the contract of employment because the link of subordination that constitutes the contract of employment[6] is the same whether one is

5. *Survey of 500 Employees*, LIAISONS SOCIALES 60 (Jan. 2001).

6. J. Rojot, *France*, *in* WORKPLACE JUSTICE: EMPLOYMENT OBLIGATIONS IN AN INTERNATIONAL PERSPECTIVE (H.N. Wheeler & J. Rojot eds., 1992).

connected to a database or to an intranet either from the employer's premises, one's home, or a customer's facilities. Therefore, ascertaining the "status of the teleworker" has little meaning, especially at a European level, because telework is now a well-entrenched modality of the organization of work in enterprises. It, however, raises interesting issues.

A. The French Worker Who Works at Home

Over a century ago, home working concerned a very large number of peasants who spent long winter days weaving, transforming, or assembling materials that entrepreneurs left and picked up in their home. This practice almost disappeared with industrialization, but now enjoys a new relevance with the NTICs. Modern telework, in the full sense of the word, most often conducted at home, now gives the employee who volunteers to work in that way considerable personal autonomy as well as a necessary degree of organizational autonomy. The conditions of subordination have nothing in common with those of a worker performing Taylorized tasks on a Fordian assembly line. What then is the real legal nature of the contract linking the teleworker with the principal for whom he performs work?

Although telework can appear under many different types of situations, the number of legal frameworks to fit it in is very limited. While, according to the 1996 ILO Convention 177, an employee can "choose" the status of self-employed performing independent work, French Labor Law applies the principle of reality. Regardless of the formal contract categorization, the relevant factor is the day-to-day behavior of the parties to the contract, whether voluntary or required. For instance the Cour de Cassation (Highest Judiciary Court) on November 23, 2000 decided that so-called independent commercial agents were employees because "under the actual conditions, the facts make it appear that they were working exclusively for one company, which put at their disposal offices, telephone and computers and to which they had to file weekly reports."

Three legal statuses are possible for the teleworker from home:

- In the vast majority of cases he is and remains simply a regular wage earner, under Labor Law as applicable to all wage earners characterized by a link of subordination. This is the case notwithstanding contractual provisions to the contrary (for instance categorizing him as a "free-lance" worker, if the actual conditions of

performance of his tasks show a legal link of subordination to an employer. This is the case, for example, when an insurance company teleworker must be permanently connected on the company's server. He is then paid by the hour, in agreement with the criteria set up by the collective agreement for the insurance sector.

- He could be considered a "home worker" in the meaning of Section L. 721-1 of the Labor Code, enacted in 1957, which applies to work for one or several enterprises for a fixed sum set in advance if materials or equipment are owned by the worker. Although enacted to cover the case of women working at home sewing dresses and rag dolls, it conceivably could be extended to Internet or extranet home telework. However, Section 721-6 of the Labor Code provides that all legal, administrative, and contractual provisions applying to regular wage earners apply to the case of such home workers, as well as relevant collective agreements, unless there is express exclusion for the latter.[7]
- He can be considered as self-employed if, despite conditions of work close to those of a home worker, he remains free to select his customers (which would be employers for a home worker), acceptance or refusal of orders, make his own decisions on prices and delivery dates, and generally carry the risks of the undertaking.

Multi-activity is possible, where, for instance, a worker performs wage earning work for a given firm, under a labor contract, and is a self-employed independent contractor under a commercial contract with another firm. However, the law does not permit dual status with the same firm.

Employers, for flexibility as well as for cost reasons, given the restrictive law of dismissal as well as the current heavy wage-based social security contributions, generally would prefer to deal with self-employed contractors rather than with wage earning employees. However, courts quickly recategorize a commercial contract into a contract of employment, in face of the relevant elements of subordination, with the appropriate penalties. For instance, this would be the case if a single principal several times a day, through e-

7. Cour de Cassation C.S., No. 2276 D (May 6, 1998).

mails or telephone calls at times fixed by him, controls the performance of work for the needs of his own customers.

B. Limits on Requiring Employees to Work at Home

The High Court decision Abrams/Sté Zurich Assurances of October 2, 2001[8] rejected the action of an enterprise that decided to close its offices and invite its employees to adequately equip their homes in order to handle professional calls and maintain their files. The High Court based its decision not only on the contract of employment's obligations, but also on Section L. 120-2 of the Labor Code (which forbids interference with freedoms), Section 12 of the Universal Declaration of Human Rights (which forbids arbitrary interference into private life, family, home, and correspondence), and Section 9 of the Civil Code (which protects privacy). The High Court viewed the imposed modification of the contract of employment as improper since the employee had no choice regarding whether to work at home and transfer his files and working tools there. It also was observed that the arrangement provided no additional compensation for the removal from private use of a room of the employee's home,[9] and the problematic issues of insurance, professional occupancy, and the like.

Besides its legitimacy, the Abrams/Sté Zurich Assurances decision is analytically sound. It is impossible for an employee, when hired, to anticipate the need for a contractual provision insuring that he will not one day be transferred to his own home! Such a modification of the contract and such a drastic disruption of privacy and family life obviously require the employee's consent, as it would also be the case for a reversal of the situation—assigning to an office an employee working from home base—as the High Court decided on February 28, 2001.

These decisions, of course, do not forbid telework, as long as both parties expressly agree, either at the time of hiring, or later. If agreed, the decisions indicate that a provision for reversibility would be wise inasmuch as there may later be changes the worker's personal life. Accordingly, the Euro TUC and the FIET (International Union of Employees, Technical and Managerial Staff) advocate inclusion of a

8. *See* J.E. Ray, *La légitime censure des télé-travaux forcés*, 12 DROIT SOCIAL 1039 (2001).

9. In continental Europe, at least in large cities, town planning generally provides for apartment buildings, which demand less space than a house, and thereby makes it impossible to build an additional room.

"right to reinstatement" in collective agreements implementing telework.

C. Special Issues

The contract of employment for telework of course falls under the provisions of the (voluminous) Labor Code and the applicable collective agreements. This raises five, apparently insolvable, questions.

1. Telework and Control of the Labor Inspectorate

French Law is territorial in application. However, how can a Labor Inspector check the safety of an employee connected, but located half a world away? Even if they are located on the national territory, will the Inspector have the time and the will to visit the hundreds (thousands?) of teleworkers in his area of responsibility? Even if he could (and would), will he actually gain access to their private homes? As the ILO Convention of 1996 on work at home recognizes, this important question raises huge technical and legal problems. However, except for safety and health controls over the workplace, the NTIC allow inspections regarding working time and wages to take place at the employer's premises, with a possible telephone check with the employee.

2. Health and Safety

In fact, cases of occupational injuries for teleworkers at home remain few and far between—less than a dozen cases are annually reported in France. Besides, the rules of the Labor Code remain valid, even if, in practice, they must be adapted to the situation. The enterprise must specially inform the teleworker of the existing risks of a general nature and additionally of those that are specific to the situation. The worker may have to face these alone, such as, for instance, an electrical fire in his equipment and the availability of a fire extinguisher or the risk of electrocuting a curious pet. A safety specialist, and possibly an ergonomist, must make a preliminary visit to check the reliability of the electrical circuitry and the compliance with safety regulations of the whole set-up, probably more demanding than at the usual worksite because of the possible presence of children, and there must be a yearly check. The teleworker, like any other worker, is subject to a physical examination, at the time of hiring and annually from then on.

Section 411-1 of the Labor Code regulating occupational injuries does not make any distinction regarding the place where the injury occurred. It is an occupational injury, with the resulting employee benefit of 100% coverage of health expenses from the social security system, if it is work related or occurred at the opportunity of work performance, wherever situated. Thus, a high court decision of 2001[10] ruled that an employee on a traveling assignment teleworking from his car or hotel room is considered at work during the entire time of his assignment, whether the injury occurs during work performance or an act of everyday life, unless the employer proves that the employee had interrupted his assignment for personal reasons. Of course, regarding work at home, the work-related character of the injury is more difficult to prove, unless there are fixed times of connection with the server.

3. Wages of the Teleworker at Home

The home teleworker is legally covered by the minimum wage. Collective agreements' provisions apply to wherever the employees perform their work in France.[11] If a given amount of work cannot be performed within the contractually allotted time, wage increases for overtime, and possibly Sunday work, holiday work, or night work are due, as for regular employees. In addition, caselaw[12] provides that although such modifications are permitted for occasional short periods, unless the contract has provisions to the contrary, significant or long term modification of the normal work week can only be made by mutual agreement.

4. Work-related Expenses

Work-related expenses of an employee must be paid by the employer and reimbursed when necessary. However, by contract, the parties can arrange for the employer to pay a lump sum to cover expenses, provided that the result does not reduce earnings below the minimum legal hourly wage.[13] Nor can the employee be required to participate in the risks and expenses of the enterprise. Because this applies to the homeworker, as proposed by the Eurocommerce convention, it is the best to avoid misunderstandings by allocating

10. Cour de Cassation, Chambre Sociale, No. 9920.603 (July 19, 2001).
11. Cour de Cassation, Chambre Sociale, No. 2276D (May 8, 1998).
12. Cour de Cassation, Chambre Sociale, No. 4074 (Oct. 10, 2001).
13. Cour de Cassation, Chambre Sociale, No. 1, F. Guillon/Médicale de France IARD (Jan. 9, 2001).

expenses in advance, in the contract of employment, regarding the equipment to be used, its replacement, and the operating expenses. The arrangement then becomes an element of the contract of employment and any modifications must satisfy the normal requirements for such changes.

5. Working Time

Telework has challenged the basic premise that the employer must pay for the time the employee is at the work site. Employment, such as design work, can take place outside the premises of the enterprise and, of course, a teleworker can be at the work site without actually working.

European Law and High Court decisions have extended the legal definition of working time.[14] It has now been broadened to encompass "the time during which the employee is at the disposal of the employer, without being able to spend his time to his own occupations." Moreover, the High Court warned enterprises using NTICs to externalize the work of managerial staff, in an effort to cope with the 35 hours law, that the status of manager, by itself, does not exclude the payment of overtime. In addition, if the employer claims it was not informed of the overtime payment work, lower courts must check that it was not imposed on the employee, either implicitly by the nature or the quantity of the work required, or performed at the request or with the implicit consent of the employer.[15] Thus, a former influential justice from the High Court's social chambers wrote that "private life of the employees must be protected, against their will sometimes, against an excessive overflow from their professional life. . . . The right to a normal family life, established by the Council of State in its Gisti decision of 8 December 1978 applied originally to the Law applicable to foreigners; but this rule has the scope to apply to all."[16]

There are now four possible situations. First, since the adoption of a 35 hour work week law, a day lump time amount excluding time accounting, and thus overtime, may apply to "autonomous"[17]

14. Always a tricky issue in French law. *See*, *e.g.*, J. Rojot, *France*, *in* R. BLANPAIN, E. KOHLER AND J. ROJOT, LEGAL AND CONTRACTUAL LIMITATIONS TO WORKING TIME IN THE EUROPEAN UNION (1996).

15. Cour de Cassation, Chambre Sociale, JS UIMM 2001 16 (Apr. 19, 2000)

16. P. Waquet, *En Marge de la loi Aubry: Travail Effectif et Vie Personnelle du Salarié*, 12 DROIT SOCIAL 963, 967 (1998).

17. *See* J.E. Ray, *Le temps de travail des cadres: Acte IV, Scène 2*, 3 DROIT SOCIAL 244 (2001).

managerial staff, under conditions specified in a collective agreement and individual contract.[18] This is well suited to the case of telework at home. For non-managerial staff, a yearly lump time, as allowed by section L. 212-15-3-II of the Labor Code, applies to traveling employees on "nomadic" assignments, but not to teleworkers working exclusively from their homes. Second, if telework requires constant connection to a server or a data bank, that connection can be computed, from both sides, as working time. Third, most telework tasks can be the object of a lump time estimate of the duration needed for performance of each task. It is then possible to multiply by the number of times the task is performed. This, however, solves the legal problem of the duration of work, not the ones of the enforcement of daily and weekly rests and breaks for work on-screen. However, control software can be adopted to control the times and duration of the use of the computer, of which the employee must be individually informed and the Works Council collectively informed. Fourth, for complex work, a system similar to the one applicable to managers has to be adopted, which must, however, also comply with the rules of maximum working time.

Thus, theoretically, NTIC allows the rules on rest and work time to be applied. Realistically, however, teleworkers have different working schedules than those at headquarters and it could be counterproductive to apply, for instance, the prohibition of night work, if the individual employee prefers to enjoy his afternoon of leisure and then work after 9 p.m.

6. Duty of Non-Competition

The teleworker often uses high performance equipment, provided by the employer, has access to confidential data, and Web access to potential competitors that he might be tempted use in improper ways. In a case involving unfair competition by a teleworker to the benefit of a consulting firm set up by the spouse, the High Court[19] found that there had been a "heavy" offense by the employee, [20] with the result that immediate dismissal was justified and damages were owed by the guilty employee. The decision is unusual, for generally the High Court, rather naively, would only assess responsibility based on the spouse's wrongful competition.

18. Then, it is a change in the individual contract of employment that the employee may reject.

19. Cour de Cassation, Chambre Sociale, JS UIMM 2001 74 (Nov. 14, 2001).

20. On the gradation of offenses and its consequences, *see* J. Rojot, *supra* note 6.

7. Provision for Exclusive Services

Freedom of work is guaranteed by the preamble to the Constitution and by section L. 120-2 of the Labor Code. A Provision for exclusive services runs against it and is valid only if it is absolutely necessary to the protection of the legitimate interests of the enterprise and if it is proportioned to its goal. The High Court has applied to such a situation the same rule as for the covenant of non-competition (which applies after the contract of employment has ended, in contrast with the duty of non-competition, which applies during the contract). Such a provision is, therefore,[21] void for a part-time contract of employment.

However, the issue remains open for full-time employees. Although both salaried work and self-employed work must remain possible for the employee, the legitimacy of other work will be determined, case by case, and often will rest in practice on the affect of such work on the duty of non-competition.

8. Professional Use of the Equipment

Although there are no Court decisions, it is obvious that the homeworker must be able to use the provided equipment in the same way as his colleagues on the enterprise premises, but without the support at home of a manager, a maintenance crew, and a fire department. In the same way, conversely, he must take all provisions to secure the equipment against theft or hazards, particularly confidential files in his care (as provided by section 10 and 11 of the EU level Eurocommerce Agreement). For its part, the enterprise must suspend and and/or change access codes, safeguards, and the like. As an example, the Worldwide Renault Company charter for the correct use of computer, numerical, and electronic resources specifically lists the safety operating provisions to be observed. Additionally, if justified by the interests of the enterprise to protect the confidential nature of the data, disks, memories, and the like, the employer can require that the equipment be used only by the employee to the exclusion of family and friends. For example, as a precaution, the France Telecom charter prohibits a teleworker from transmitting to anyone his personal home address, electronic, or otherwise. For the purpose of control of contacts, every data transmission, notably, but not only with customers, must be

21. Cour de Cassation, Chambre Sociale (July 11, 2000).

transmitted through the enterprise that forwards calls and data transmission.

9. Obedience to the Rules of Computer Use Law

Rules regarding the piracy of software and the Act on Computer Science and Freedom must be observed, to avoid the joint civil and criminal responsibility of the teleworker and of the enterprise. Section 16 of the Eurocommerce Agreement, for instance, mandates that the employee commits himself not to use the means at his disposal for unlawful or illicit activities on the Internet.

Of course, telework can be a wonderful method of preventing employee violations of the rules prohibiting lucrative work during paid breaks for sickness or child bearing. A provision prohibiting such misuse can be included in the employment contract, even if, operationally, enforcement is difficult.

D. Work at Home and Remote Control of the Employee—The Right to Rest and Privacy in the 21st Century

The most ordinary cellular phone constitutes an electronic leash, especially if paid by the enterprise, and calls or e-mails at home during rest periods appear more acceptable than 20 years ago. Legally, such a call raises no obligation for the employee, but, in practice, most employees will feel compelled, if not flattered, to answer and comply with a phone or mail request for information.

1. On-call Status ("Astreinte")

Section L. 212-4b of the Labor Code defines "on-call" status for an employee as a period of time during which the employee, without being at the immediate and permanent disposal of the employer, is under the obligation to remain either at home or nearby, in order to be able to proceed to carry out work for the employer, such work being considered as effective working time. The statute enacting this provision follows the earlier decisions of the High Court and clarifies the difficult question of the legal nature of the time spent "on-call." According to the High Court applying EU Law, the *summa divisio*, which separates time spent working from all the rest, which is precisely resting time,[22] is not applicable here: time spent on-call is

22. Cour de Cassation, Chambre Sociale, 999 DROIT SOCIAL 730 (May 4, 1999).

neither work nor rest.[23] If being on-call does not allow the employee to perform his personal activities, then it is work. However, as noted by the Court of Appeals of Paris,[24] most employees "on-call" by cellular phone do not have to remain at their homes or nearby. Thus, this first attempt at definition is practically obsolete. The employee on-call, through the modern means of communication, remains at the disposal of the employer wherever he is (in the enterprise or nearby, in a place put at his disposal) and work performance does not depend on the number of operations effectively carried out during a period, but is characterized by the permanent character of the availability of the employee at the disposal of the employer and deprived of his freedom to move.

2. On-call at Home by Cellular Phone: Availability in European Law

The Court of Justice of the European Communities on October 3, 2000 held that physicians "on-call," not compelled to be present on hospital premises but able to be reached and respond if needed, could manage their time with less constraints and use their time for their own interests and, as such, were not at work. It added that only the time linked to the effective provision of care could be considered working time. The first proposition is in conformity with French Law; however, the second is not. Time not spent effectively at work is not compulsorily rest time, such as, for instance travel time. Real rest time must not be interrupted by being "on-call" nor by calls for the provision of information or advice.[25]

3. The Right to Effective Rest

In France, an Act of January 19, 2000 has enacted the EU directive of 1993[26] into sections L. 220-1 and L. 221-4 of the Labor Code, which respectively provide that, on the one hand, "Every employee benefits from a daily rest of a minimal duration of 11 consecutive hours" and, on the other, that "The weekly rest must have a minimal duration of 24 consecutive hours to which must be added the consecutive hours of daily rest provided for at section L. 220-1"

23. *See* P. Waquet, *Le temps de repos*, 3 DROIT SOCIAL 288 (2000).

24. Cour de Paris, Da Silva/EDF-GDF Pyramides, No. 98/31017 (Nov. 3, 2000).

25. P. Waquet, *Le pouvoir de direction et les libertés des salariés*, 12 DROIT SOCIAL 1051, 1053 (2000).

26. F. Favennec-Hery, *Le temps de repos: une nouvelle approche de la durée du travail*, 12 REVUE DE JURISPRUDENCE SOCIALE 819 (1999).

(35 hours all together). Additionally, the preamble of the Constitution establishes the right to "rest and leisure" as does the Universal Declaration of Human Rights of December 10, 1948.[27] Of course, the NTIC makes it all the easier for the enterprise to encroach on this rest time.

4. A Right to Disconnection[28] and the Respect of Privacy in the 21st Century

The French High Court has become extremely strict regarding the observance of rest time, considered as an essential element of personal and family life. It is a time during which the contract of employment is suspended and all employer interference is *a priori* illegitimate. For instance, it was held that during a sick leave, an employee does not have to answer a telephone call from her employer.[29] However, the duty of loyalty remains and a traveling saleswoman on sick leave cannot refuse to return to the employer a customer's file in her possession.[30]

However, it is to be feared that, in fact, beyond the reach of the law, workaholism combines with the practical and convenient aspects of electronic leashes and increasingly adds stress and constraints to managers, sometimes accepted not unwillingly, even if not enthusiastically. In this case, it is up to their unions to negotiate changes, perhaps using the model adopted in Nordic countries.

E. The Present Work of the European Union

The EU Commission is not indifferent to telework, far from it. In 1996, two reports respecting such work were required from each Member State, respectively on Labor Law[31] and Social Security.[32] This activity is much welcomed, for, obviously, the issue typically transcends borders. Each year, the Commission publishes a report on the issue. E-work in 2000: Status Report on the New Ways to Work in the Information Society, for instance, indicates that, at the present rate, France will be way behind in 2005[33] with 4.8% of the Labor force

27. Waquet, *supra* note 23, at 288.

28. J.E. Ray, *Le Droit à la Déconnexion, Droit à la Vie Privée du XXI Siècle*, 11 DROIT Social 9 (2002).

29. Cour de Cassation, Chambre Sociale (June 14, 1999).

30. Cour de Cassation, Chambre Sociale, No. 98-46.345, LS 706 du 26 février 2001 (Feb. 8, 2001).

31. J. E. Ray, *reprinted in* 4 DROIT SOCIAL 351 (1996).

32. Authored by J.J. Dupeyroux (unpublished report) (on file with author).

33. Bruxelles (Sept. 2000).

teleworking (against 2.9% today) as compared with an average above 10% for six out of the ten countries studied.[34] The program decided upon for the Commission at the Lisbon Summit includes, within the modernization and improvement of the conditions of work, two closely related issues: "The Economically Dependant Teleworker" and "Telework."

The UNICE offered the Euro TUC to open a voluntary negotiation, excluding a binding agreement, on the issue of telework, on March 8, 2001. TUC declined, insisting on a binding regulation. The Commission, favorable to these discussions, encouraged renewed efforts between the parties, which began on November 15, 2001. The Euro TUC has adopted a balanced view of telework, recognizing its benefits and dangers for employees. At the sectoral level, the dialogue has ended in agreements, on April 26, 2001 between Uni-Europa and Eurocommerce, in the commerce sector[35] and on February 7, 2001, in the telecommunications sector.[36] However, the European Commission Web site devoted to this effort[37] cautions against excessive hopes for rapid transformation into general models from pilot projects which are geared to the best fit employees.

II. RESPONSIBILITY FOR HIGH TECHNOLOGY WORK TOOLS

A. Criminal Offenses Linked to NTIC

The NTIC gave birth to a new category of offenses unknown twenty years ago and now included in the new Penal Code, enacted in 1994. After initial hesitations, repression of such offenses is now treated as a serious matter.[38] It is also to be noted that, if, in principle only, the author of the crime is criminally responsible, in many cases now (such as plagiarism of software or breach of automatic data transmission systems), the criminal responsibility of the morally responsible party (company, association, works council) can also be involved if the crime was perpetrated by one of its legal representatives.

34. 29.4% in Finland (16.8% today), 25.2% in the Netherlands (14.5% today), 12.6% in Germany (6% today), and 11.7% in the United Kingdom (7.6% today).

35. *Available at* http://www.eurocommerce.be.

36. The French situation is reported on the Web site of the French Society for Telework, *available at* http:// www.aftt.org.

37. *Available at* http://www.telework-mirti.org.

38. However, fines as well as jail terms indicated below are maximum.

1. Breach of Automatic Data Transmission Systems

Section 323-1 of the new Penal Code provides punishment of a year in prison and a fine of 100,000 FF for unauthorized accessing or maintaining all or part of a system of automatic data processing. Alteration of the system or modification or suppression of data increases the penalties to two years and 200,000 FF, regardless of whether the alteration, modification, or suppression was voluntary. Section 323-2 of the new Penal Code punishes, with three years imprisonment and a 300,000 FF fine, the hindering or falsifying of the functioning of such a system. In applying this text to an employee who inundated his former employer's system with unwanted e-mails and files, the Court of Lyon imposed a suspended sentence of eight months in jail, a fine of 20,000 FF and damages of 200,000 FF. The new employer was not held liable for civil damages, because the employee acted outside of his job functions.[39]

Fraudulent data entry, suppression, or modification is punished by Section 323-1 of the new Penal Code with three years in prison and a fine of 300,000 FF. Section 323-7 of the new Penal Code imposes the same penalties for the simple attempt, without success, of the above mentioned actions. And, Section 323-1 of the new Penal Code imposes the same penalties, or of the highest penalty applicable, for participation in a group established to attempt any of the above offenses.

2. Breach to the Rights of the Person by Means of Data Files or Computer Processing

Proceeding or having somebody proceed, even by neglect, to automatically process nominative information, without having complied with the compulsory legal formalities, is punished under Section 226-16 of the new Penal Code by three years in prison and a fine of 5,000,000 FF. Section 226-17 of the new Penal Code punishes, with three years in prison and a fine of 5,000,000 FF, proceeding or having somebody proceed to automatically process nominative information without taking all due care to protect the security of such information including preventing their being transformed, damaged, or communicated to unauthorized third parties. Section 226-18 of the new Penal Code punishes, with three years in prison and a fine of 5,000,000 FF, collecting through illicit, fraudulent, or unfair means, or

39. *Available at* http://www.legtalis.net/jnet/actualité (Mar. 2001).

processing data regarding a person against his will, when his opposition is based on legitimate reasons. Section 226-19 of the new Penal Code punishes, with three years in prison and a fine of 5,000,000 FF, storage of data regarding, directly or indirectly, a person's racial origins, political, religious, or philosophical opinions, union membership or morals, without the express agreement of the person concerned. Section 226-22 of the new Penal Code punishes, with one year in prison and a fine of 100,000 FF, the collecting or revealing to a third party, without special legitimate qualifications, nominative data whose disclosure could undermine public esteem or the intimacy of a person's private life.

3. Attacks Against the Person

Section 226-1 of the new Penal Code punishes, with one year in prison and a fine of 100,000 FF, breaches of privacy including recording and transmitting without consent, through whatever means, the image of a person in a private place, or attempts to do so. The French Code of Intellectual Property and the Law of Industrial Property also protect an author's royalties for unlicensed use of software and punish unlawful copying with two years in jail and a fine of 1,000,000 FF.

B. Liability of the Enterprise

1. Civil Liability

An enterprise is responsible for the damages caused by an employee who causes harm or a wrong to somebody else while acting on behalf of the enterprise, through an Internet or intranet or otherwise. However, this does not apply if the employee acted outside the frame of his duties without authorization and for purposes unrelated to the employment.[40] Nevertheless, the High Court has interpreted this exception very narrowly. If the conduct occurs during working time and using the enterprise's computer[41] the employee will be held to have found in his employment the opportunity and the means to commit his offense[42] even if the use is contrary to the enterprise's regulations.

40. Doctrine of the abuse of functions; with variable conceptions from the High Court.
41. This also may apply to home teleworkers.
42. Cass. Crim. (June 23, 1988).

2. Criminal Liability of the Enterprise

Since 1994, corporate entities (as "moral persons") can be held criminally liable for the offenses committed by their representative organs in the cases foreseen by the new penal code, such as discrimination, procuring, and computer use.

C. Liability of the Employee

1. Civil Liability of the Employee

In the situation of a "heavy" offense (a very grave offense involving the employee's willful intention to harm the employer) an employee cannot only be legitimately terminated, but can also be held liable for the damages resulting from his offense. Willingness to harm is the criteria for employee liability in all other cases; absent willfulness, the employee escapes liability for the consequences of his offense toward his employer even if the damage is severe. In the same way, a third party may not hold an employee liable for damages caused by an employee who was acting within the scope of his duties under the orders of his employer.[43] (However, he may still be criminally responsible for his conduct.)

2. Criminal Liability of the Employee

Whether or not he acts under employer instructions, the employee has to answer to all his penal (criminal and misdemeanors) offenses, whether they are committed from home or his office. Such is the case of insulting or defamatory e-mails in which the injury is to the particular victim alone, not to society as a whole. Hence, the limited nature of the publicity will restrict the consequences of such acts when on intranets.

III. ELECTRONIC MONITORING OF PERFORMANCE AND COMMUNICATIONS

The debate respecting this sub-topic is framed by two propositions. On the one hand, section L. 120-2 of the Labor Code imposes a narrow frame of authority over an employee for the employer, or even a collective agreement, by establishing: "None can

43. *See* Assemblée Pléniére de la Cour de Cassation, D. 2000, IR 85 (Feb. 25, 2000), in which an employee unlawfully jammed the Web site of a competitor under his employer's instructions.

bring to the individual and collective freedoms and the rights of the person restrictions that would not be justified by the nature of the task to be performed nor proportional to the goal to be reached." On the other hand, the employer has the right and the duty (because of his possible liability as a principal) to control the employee's professional activity, as well as the duty to safeguard the security of his network of data processing and transmission.

A. The Two Main Principles

1. Principle of Loyalty

Section L. 121-8 of the Labor Code, which embodies one of the most important provisions in the Act of December 31, 1992, provides that, "No information concerning personally an employee can be collected through a device of which he has not beforehand been made knowledgeable. The works council is informed and consulted before a decision to implement the means and techniques allowing a control of the activities of the employee." If he has not been informed beforehand, the courts deem the gathered information invalid and illicit as proof. If the works council has not been consulted, it is characterized as the criminal offense of hindering the council's functioning. This encompasses not only software for the control of productivity or for connecting to the Internet, but all techniques, even unsophisticated and computerless methods, and even those producing information as an indirect consequence of a system not designed for control purposes.[44]

2. Principle of Proportionality

Section L. 121-7 of the Labor Code embodies a second principle: "The methods and techniques of appraisal of the employees must be relevant to the goal to be reached." Certainly, the enterprise is not a public place where anyone can act however he wishes. The employer can limit or forbid certain acts or behavior, under the dual conditions of the above text that must be applied case-by-case. For instance, in most establishments, it would be unlawful for an employer to blanketly forbid all talk that is unrelated to work performance or permit changing rooms to be searched at any time. However,

44. Court of Paris (May 31, 1995), in which the absence of a railway employee was made evident through the reservation system; A. Mole, *Jusqu'où ira le droit à l'information*, GAZETTE DU PALAIS 193 (Jan. 23, 1997).

enterprises working for the Defense Department or in Currency Exchanges can be expected to regulate conduct more rigorously than in more usual lines of business. For example, a permanent, broad control of e-mails is legitimate in one case, but not in the other.

With regard to computer use, the High Court very carefully monitors the mutual respect that must prevail in employment relations, even in matters such as locating software viruses or remote repair of a hard disk. "If the employer has the right to control and monitor the activities of his employees during working time, any recording, for whatever reason, without their knowledge, of image or words is an illicit mode of proof."[45]

3. Joint Application of the Principles of Loyalty and Proportionality on the Matter of Nominative Information: the Act on Computer Science and Freedom

As early as January 6, 1978, France adopted a statute called "Act on Computer Science and Freedom," which inspired the European Directive of November 23, 1995,[46] which, in turn, requires some modifications in French Law.[47] Section 1 of this founding Act states, not without some pomposity, that: "computer science must be in the service of each citizen. It must not undermine either human identity, human rights, privacy or individual and public freedoms."

Section 3 states that "every person has a right to know and to challenge information and thought processes used in data processing with which results he can be confronted." The National Commission on Computer Science and Freedom[48] (CNIL) regularly publishes recommendations on sensitive topics. These are guidelines based on gathered good practices rather than compulsory legal texts.[49]

B. The Dangerous Collision of Different Areas of the Law

Civil law, labor law, computer law, and penal law, which recently discovered computers, apply here, with high risks for enterprises.

45. Cour de Cassation, Chambre Sociale, 1 DROIT SOCIAL 28 (1992).

46. Directive 95/46 aims to insure the protection of freedom and fundamental rights of physical persons on the matter of personal data, JOCE (Nov. 23, 1995).

47. Proposal for an Act introduced in Parliament on June 2001.

48. Besides professional judges, high ranking civil servants, politicians, employers, and unionists also sit on it. The present President is H. Bouchet, Secretary General of the National Union of Cadres and Engineers Force Ouvriére. *See* http://www.cnil.fr.

49. In March 2000, it published a general report regarding the use by employees of the "information highways."

1. The Right to Privacy at the Office, and in the At-home Office

Many international texts, such as the European Convention of Human Rights or the more recent Charter of Fundamental Rights of Nice adopted on December 7, 2000, recognize that private life is an aspect of personal life. And, as observed by the High Court,[50] section 9 of the Civil Code provides that: "everyone has a right to the respect of his privacy. The Judge may, besides redress and compensation of the damages suffered, order all provisions . . . able to prevent or to end any attack on the intimacy of the private life." The guilty party is not confined to the employer, as for instances in cases of vengeful e-mails sent as copy by a disappointed lover, or in the course of a union matter, related e-mail also settling a personal account ("instead of watching us, Mrs. X. . . . would be better inspired to watch over her husband"). The question has been raised as to whether an enterprise could argue that a non-work-related use of intranet e-mail is an offense against shop rules,[51] and thus not protected by the intimacy of private life.[52]

The new Penal Code gives a strong emphasis to the privacy of personal life. Its section 226-1 punishes by a maximum of a year in jail and a fine of €50,000[53] those who "through any process voluntarily tap, record or transmit, without the consent of their author, words uttered privately or confidentially." Section 226-7 holds penally liable the guilty legal entities and, thus, enterprises themselves. A number of companies require the employee to agree in principle to possible monitoring controls and provide management with a signed document to that end. Nevertheless, even if it is the wish of the enterprise to monitor business communications, can it maintain that professional life is totally separated from private life? Where is the border in an e-mail sent to a colleague and friend on the other side of the world mixing office news and technical information?

50. Discussed by J.E. Ray, *Surf au Bureau et Droit du Travail*, LIAISONS SOCIALES, Jan. 2001, at 58.

51. Regarding the "charters" of use, see below.

52. On the issue, *see* J.E. Ray & J. Rojot, *Worker Privacy in Europe*, 17 COMP. LAB. L.J. 61 (1995).

53. In French law, the penalties mentioned by the Penal Code are the maximum charges. The breaches of the law considered here fall into a category unknown in U.S. law. This category lies between felonies and misdemeanors, the "delits." They are tried by the "Tribunal Correctionnel," where journalists specializing in such news are often present. Thus, the media gives considerable attention to small cases. (Big Brother paranoia and moral harassment are presently in fashion.)

2. The Secrecy of Correspondence

Correspondence is protected by the Act of July 10, 1991. Section 226-15 of the Penal Code punishes by a maximum jail term of one year and a fine of €50,000. "The fact perpetrated in bad faith to open, suppress, delay or divert correspondence, whether delivered or not, or to fraudulently read them." It remains to find out what exactly is a "correspondence," the intention of the law expressly being aimed at mail—sealed envelopes carried in mailbags. The criminal Chamber or the High Court had decided that the secrecy of correspondence did not apply to occupational mail addressed as such (for instance Mr. A, marketing manager of Company B). A business Internet/intranet e-mail would thus not be covered by it, but this exclusion would not cover a personal Internet that inadvertently arrived at the office. The 17th Chamber of the Tribunal Correctional of Paris[54] has decided that, indeed, the sending of electronic mail from person to person constitutes private correspondence. The term correspondence applies to any written relationship existing between two identifiable persons, whether it concerns letters, messages of closed or opened envelope. The law protects this relationship since the contents that it carries are aimed exclusively by a named person to another equally individualized person, as contrasted with messages placed at the disposal of the public. In one particular case, a female student in a University research laboratory in physics had complained of harassment by e-mail. The director of the laboratory, the system engineer, and the Webmaster had opened and monitored the mailbox of a suspected visiting doctoral student whose volume of e-mail was abnormally high. They discovered that 90% of his e-mails were of a private nature as well as derogatory to the laboratory. Expelled on these grounds, the student sued in criminal court. The decision vindicated him and sentenced the director of the laboratory, the system engineer, and the Webmaster to fines between 5,000 FF and 10,000 FF, as well as to 10,000 FF damages. This decision makes little of the risks of piracy for a research lab working on sensitive matters and is probably not transferable to the private sector. In that case, public employees were involved, and bad faith is not required as it is generally in section 226-15 of the Penal Code, quoted above.

The Court of Appeals of Paris took the concern in account and, in a balanced decision on December 17, 2001, noted that "the concern

54. Al Baho/Virieux et a., affaire n+ 97.522311; *see also*, L. Rapp, *Point de vue*, D. III (Nov. 23, 2000).

for network security justifies that network administrators make use of the technical possibilities at their disposal to carry out investigations and take the necessary safety provisions, in the same way as the postal service must react to a suspicious package. However, the disclosure of the contents of the messages does not fulfill this goal." It, therefore, gives the network administrators a special status by allowing them to monitor the communications, but upon becoming aware of the contents of a personal message, prohibits them from disclosing the contents.

3. The Nikon Case of October 2, 2001 and the Ban on Reading Personal E-mails or Files[55]

Faced with the suspicious behavior of an employee, his employer, upon opening the hard disk of his computer and reading files labeled "personal" and "fax," discovered that he was running his own commercial activity from work in competition with the employer. It terminated him for a "grave" offense. The High Court voided the dismissal for the reason that "the employee has the right, even at the work place and during work time, to the respect of the intimacy of his privacy. It implies, in particular, the respect of the secrecy of his correspondence. The employer cannot, without violating that freedom, read personal e-mails sent or received by the employee."

This absolute ban seems excessive and does not take into account the vital interests of the firm. On the matter of telephone calls, for instance, the High Court holds that if employees in sensitive positions for the interests of the firm (for instance, traders in a brokerage firm) have been duly warned that their telephone calls could be listened to, the internal wiretaps constitute a valid mode of proof. This apparently does not apply here. Also, the division between personal and professional e-mails and files seems inadequate. First, as discussed above (III, B, 1) the two often intermesh. Second, it is often by reading the e-mail that one discovers if it is one or the other. However, while in the past the employee was unlikely to open a file labeled "personal" on his hard disk for fear of attracting attention, under the inspiration of this Court decision, this might become the rage as a means of insulating the misuse of the transmission system. Conversely some mistrustful employees use technical professional file labels for very personal files in order to better hide them. For

55. For an extended treatment of the question, *see* J.E. Ray, *Courrier Privé et Courriel Personnel*, 11 DROIT SOCIAL 915 (2001); *see also,* special issue *Droit du Travail et Nouvelles Formes de Subordination*, 1 DROIT SOCIAL (2002).

instance, to satisfy the request of a customer, during the vacation of a young intern, a supervisor opened a file with a relevant label and found a detailed, somewhat technical, description and appraisal of the sexual performances, together with grades and comments, of a large number of his male office colleagues. If, by manipulation or mistake, such files are spread around the office, or worse outside, the civil liability of the employee, and the enterprise, might be involved. Third, the inviolability of personal files might cause some employees to hide there unlawful data such as pedophiliac pictures. This raises even more complicated liability issues, from alleging the complicity of the enterprise for not having prevented such activities, to its exoneration if it is forbidden to it to exert any control.

As it stands, the consequences of this High Court decision are puzzling. First, it might simply be unenforceable, at least for incoming e-mails. Routinely, and for good reasons dealing with hackers and/or industrial spying, firms use firewalls scanning all types of connections into their systems. This automated control carried out by a "computerized tool" is an indirect way of reading personal e-mails, and thus forbidden. It is unlikely that this vital protection can be surrendered without considerable damage. Will a Parliament Act be necessary to counter the catastrophic consequences of the High Court Nikon case?

Second, although the enterprise might restrict the number of employees given the tools to access intranet and Internet, however, as such access becomes more and more generalized, it will become a casual working tool and it will be impractical, if not downright impossible, for efficiency reasons to deprive access to most employees.

Third, charters of use of the Internet, also generalized in large firms, if they adopt a permanent, general, and blanket provision forbidding personal use are, at this point, invalid in France, because of the principle of proportionality discussed above. The Nikon case has indeed "opened the debate."

C. Punishment for Abusive or Illicit Use

Employees can be disciplined, including dismissal, for violating rules of use that are lawful (i.e., as discussed above, are not of a blanket and permanent nature), so long as the prohibition is clearly stated and there has been notification regarding the rule. There are, however, additional problems.

1. Identification of the True Author of the Mail or the Connection.

Even when it is technically easy to identify the computer that sent a communication or made an Internet contact, there may be problems identifying the individual responsible for the activity.[56] For example, if it is apparent that the conduct will carry criminal or disciplinary penalties, the temptation is high to use one's neighbor's computer while he is away. Access codes, of course, are designed to minimize this problem. They are known, in principle only, by the jobholder whose position imply their use and by the Webmaster and, therefore, theoretically allow pinpointing the identification of a sender from any computer. However, in practice, for reasons often related to team work, multi-skill, convenience, transparency, or other reasons, often they are known by coworkers, bosses, if not by the entire office, or even may be inscribed on a Post-it affixed to the employee's desk.

Most companies' guidelines forbid these careless practices. For instance, the University of the Mediterranean warns employees that "anyone must identity oneself clearly, no one has the right to wrongly assume the identity of someone else or to act in an anonymous way. Authorizations for access are strictly personal and cannot be transferred to anybody (including colleagues, friends and family members) whatever the degree of confidence regarding these persons." The March 1999 intranet guidelines of the Coal Group "Charbonnages de France," provides that every user commits himself not to "mask his own identity, appropriate someone else's password, access information belonging to other users without their authorization."

The necessary character of that individualization has been recently recognized by the High Court: "The fact for a bank to set up an operating system including a tracing process allowing to identify the accounts users cannot be assimilated to the collection of personal information in the meaning of section L. 121-8 of the Labor Code, neither to the use of an unlawful mode of proof, the performance of work by computer cannot have for effect to confer anonymity to the tasks carried out by employees" (Cass. Soc. 18 juillet 2000[57]).

56. Of course, identification at the most sensitive work sites can be improved by equipping them with a Webcam that takes a picture of whoever is using the computer at any time.

57. No. 98-43-485

2. What Sanctions?

Acceptance of sanctions for violations of use guidelines require that the mode of proof is acceptable to the court, the contents of the shop rules have the needed clarity and relevance, and the penalty weighs the seriousness and the recurrence of the offense. Thus, in a case in which an internal notice had warned employees of the monitoring of mailboxes and against communicating to third parties information that was to be kept as internal, the Conseil des Prud'hommes of Montbéliard, September 19, 2000, decided that a simple suspension of an accounting employee was justifiable and proportioned to an excessive use of Internet involving a private correspondence with a former employee and communication of confidential information. A simple, real, serious offense will justify dismissal, as will the multiplication of repeated "light" offenses, which by themselves would only warrant a warning.

A grave offense allows immediate dismissal without severance pay or any kind of compensation, including vacation days due and not taken. The Social Chamber, on March 14, 2000, accepted the existence of such an offense in the case of an employee of a stock market trading firm, who regularly placed bets on company time and with the company's equipment. In that case, the employer had informed employees in a meeting that it would use telephone taps and recordings to be able to justify its conduct in the event of disagreement with a customer regarding trading orders.

In French Law, as mentioned above, the strongest category of offense by an employee, is limited to cases characterized by the willfulness of the wrongdoing, performed intentionally in order to prejudice the employer's interests.[58] French law also allows the employer to sue the employee proven guilty for civil liability for the prejudice suffered by the enterprise, because of the consequences of his offense. However, it appears that a heavy offense will seldom be found in matters of electronic mail, for the High Court has determined that it was a grave offense, not a heavy one, where an employee transferred a file of customers to a competitor. On the other hand, the opposite result was reached where an employee sent multiple communications, by post one day and e-mail the next, addressed to third parties as well as to administrative and financial authorities, which stated that the general management of the company

58. On the gradation of offenses, *see* J. Rojot, *Employment Security in France*, *in* EMPLOYMENT SECURITY, LAW AND PRACTICE 111-138 (R. Blanpain & T. Hanami eds., 1994).

was guilty of criminal offenses. The court noted that such conduct "can only throw discredit on the company" and, thus, constituted a heavy offense. (Cass. Soc. 30 mai 1995, No. 2341). Almost a caricature, but similar, would be the case of willful and deliberate opening of files known to be contaminated by viruses.

D. The Law of Evidence and NTIC

The French Act of March 13, 2000, bearing on the adaptation of the law of proof to the information technologies, recognizes the electronic signature. This has upset the former system in terms of judicial acts, but does not change the status of judicial facts, which covers most cases in Labor Law. For instance, on the issue of dismissals, the employer acts first, but even when defending that action in court, he is subjected to the rule that "the doubt benefits the employee," and thus he must convince the Judge of his case, and therefore bring elements of proof. NTIC can indeed help bring proof, but not without problems.[59]

1. Common Issues

The first issue concerns the reliability of control over the evidence. As expressed by the Court of Aix,[60] in a case involving numerical video monitoring: "Given the possibilities of editing and doctoring that the evolution of these technologies offer, such documentary evidence does not present sufficient guarantees of genuineness, authenticity and impartiality, concerning its date as well as its contents, to be considered as convincing."[61]

The Court of Appeals of Rouen, on May 14, 1996, considered as unacceptable proof the presentation of an affidavit drawn by a bailiff because of the possible manipulation of the hard disk, noting the presence on the disk of three software programs totally foreign to his occupational life. Exemplary of this trend is the judgment of the Conseil des Prud'hommes de Nanterre (M. R/IBM, July 16, 2000)

59. *See* J.E. Ray, *La preuve en Droit du travail: avec les NTIC, l'essentiel est invisible pour les yeux*, LIAISONS SOCIALES MENSUEL 60 (Apr. 2001).

60. *Cour d'Appel d'Aix-en-Provence*, DROIT SOCIALE 332 (1994).

61. The numerical signature proposed in Outlook Express, Version 5.5 processed through Verisign (http://www.verisign.com) vouches for the authenticity of the author of the message through the code used (key sentence) and allows obtaining acknowledgement of receipt. But, as it is often the case in France, it would also be necessary that the code would not be written in plain view on a Post-it affixed on the side of the screen. Also, even if the sender is individualized, nothing necessitates that the receiver have actual knowledge of the message and/or acknowledge it.

which notes: "The enterprise shows the Court a hard disk alleged to be the one on which Mr. X was working without having communicated its contents to the other party and that it is to the least surprising that the enterprise . . . would not have done everything possible within its means to justify the reasons for the dismissal of Mr. R. It was easy enough to have had the contents of the hard disk immediately under seal."

As to who is the exact author of a message, the answer is easier for a home worker than an employee at the office. A dedicated phone line paid for by the employer makes the issue even easier in this situation.

2. Presentation in Court by the Employer of Unlawfully Obtained Evidence

Some enterprises have adopted the practice of having managers systematically print and keep e-mails sent to employees, to be used later as proof. However, this practice can backfire. This can be the case, for instance, of congratulatory e-mails that are in the file of an employee later dismissed for unsatisfactory performance, or where the time registered in the message demonstrates a violation of the 35 hours law, etc. Besides, the presentation to the court of such e-mails can show a violation of private mail, a breach of the law on computer science and freedom, a hindrance to the functioning of the works council, and the like.

3. Presentation in Court by the Employee of Documents Issued from the Enterprise

The employee, in presenting evidence, must not place himself in an unlawful position as would be the case if, for instance, he illicitly read e-mail addressed to his supervisor. In the same way, it is a heavy offense for an employee to place a listening device in the office of a supervisor. Similarly, an employee would fall under the above mentioned new sections of the New Penal Code, with their heavy sanctions, if his evidence showed that he fraudulently added or subtracted data from a computerized data processing system. However, the High Court has decided that an employee can lawfully present in Court "documents containing information of which

employees can normally have knowledge," such as, for instances intranet pages accessible without a code.[62]

IV. USE OF EMPLOYER TELECOMMUNICATION FACILITIES TO ACCESS WORKERS AND WORKER SUPPORT ENTITIES

The Eurocommerce agreement on telework contains two sections on this issue. Section 17 provides that the teleworker has the right to communicate through the NTIC with his colleagues, including communication on occupational topics with the unions or employee representative institutions, which must allow full confidentiality and not be accessible to the employer. Section 18 states that the teleworker must be able to take part in all activities of the union and employee representative activities, with the proviso that this must not carry unreasonable costs for the enterprise.

When a Parliamentary question of intranet access was posed, the Minister offered a rather weak answer:[63] "It belongs to the unions to seek, by way of agreement with the employer, the details of implementation of access to the system and of the diffusion of messages emanating from the union." Intranet by nature being a strictly occupational tool, no provision can constrain the employer from granting access to it to the union. A decision of November 17, 1997 of the Tribunal (TGI) of Paris considered that the creation of a Web site on the Internet, external to the enterprise, freely accessible to employees, and the broadcasting on that site of union demands could not be considered as unlawful because "such practices do not seem to bring disorder to the normal performance of work or to the functioning of the enterprise."

The Renault charter, signed by four out of the five unions present in the company is based on the principle of putting the intranet at the disposal of the union and works council. However, the union Web site is neither interactive nor can it send individual e-mails to employees. Currently, few French enterprises have signed such an agreement. To our knowledge, none of the computer manufacturers, very competitive and often very generous in media symbolic action, has agreed to the multiple union requests to that end, even if the enterprise committee as such has sometimes gained access under very specific conditions and exclusively for social and cultural activities as is the case for IBM-France, L'Oréal, Technip. This, however, does

62. Cour de Cassation, CHAMBRE SOCIALE D. 1999 431, note H. Gaba (Dec. 2, 1998).
63. Question 12.090, JO AN 618 (Feb. 1, 1999).

not mean that only a few French enterprises have accepted that their unions can communicate through intranet; some experiments in which some access is granted have taken place outside of agreements, codes of good conduct, or guidelines and have been elaborated by management. Conversely, unions have made use of the legal void to gain tactical ground. For instance, at the FNAC (distribution) union, activists, outside of any agreement, openly use the internal electronic mail system for union communication purposes as if it were for business-related mail. Management rejections of access to the intranet seems unfeasible in practice. It has resulted, on the one hand, in the creation of superb external Internet Web sites (IBM, Siemens, Technip) by their union sections, with the effect of bringing internal conflicts outside the enterprise. And, on the other hand, union activists use internal e-mail, potential sanctions notwithstanding, for they bet on delayed reactions by management after the harm is done, and on the deterrent of potential harmful media publicity for the high tech company if it invokes sanctions.

The unions are mindful that online rights for employees are an essential stake in the communication society, but are worried about employees without access and/or mastery of the NTIC. They also are aware that passive, even if electronic, communication cannot replace the direct contact between potential members and activists.

The existing agreements (Renault, Bull) are extremely cautious. They only allow a simple electronic posting of union messages, the access to which must be requested by individual employees wishing access to them.[64] All kinds of interactivity, such as sending union messages to all employees or union forums and chats, is excluded. In fact, they reproduce the written script, so familiar to lawyers, under the rights to "posting of union communications on panels appointed only to that end and the free handing of publications and leaflets of union origin at the times of entering and quitting work." (Section L. 412-8 of the Labor Code).

This likening of the electronic mode to the paper and pencil one is, in our view, at best misleading and at worst dangerous. It is misleading because an intranet message is both a poster and a tract (to be read and sent) and neither. Rules established in 1968 for the handling of tracts and the posting of union information are ill-suited to the electronic media. It is dangerous because the courts have never accepted the authority of an employer to *ex ante* censor any union message on its posting boards. He could only petition a judge in

64. This will quickly raise the issue of their identification, given the traceability of all mail.

chambers, after the posting, to require the removal of a litigious poster.

The parallel with union leaflets raises other problems. The law allows distribution to employees only at the times of entering and quitting work by employees. This obviously will not be the case with an e-mail, read during working time. Similarly, Section L. 412-8 of the Labor Code foresees that a copy of the posting must be simultaneously transmitted to the employer, so that he can eventually verify that it is not unlawful, and then warn the union activist, but never prevent the posting. In our view, the transmission of the electronic posting must follow the same approach.

It would be difficult to imagine that an enterprise could forbid a union from opening a Web site on the Internet.[65] In practice, employees of enterprises specializing in writing software, who did not have union representation, created Web sites, for a time anonymous, called "Ubi-free" and "Cryo-help," with remarkable media success. This was a considerable embarrassment for these enterprises that created games for the youth and, therefore, were very vulnerable to such publicity.

V. TRAINING AND RETRAINING

Gifts of computers to employees have spread to France. The remuneration package of Ford and Delta French companies have offered their employees a computer for free (Vivendi) or for a modest contribution, including a cheap connection to an access provider (20 FF per months for Vivendi). This is mostly coming from generally high-tech companies that, on the one hand, expect to build some company culture and increase the use of the Internet. Vivendi only increased the number of French connections to the Internet by 3%. These efforts benefit from a favorable tax treatment and can be considered a co-investment in training and employability in equipment by the company and, in time, by the employee beneficiary. However, they can threaten to bring not only the office, but the whole company into the home. It is for this reason the Vivendi agreement provides expressly that the equipment given by the company cannot be used professionally. Besides, it allows an increased blend of the work and home environments.

65. In spite of the difficult problem of the trademark, it would be important that the first term in the name of the Web site.