French law on privacy in the workplace

The debate concerning employers' versus employees' rights in France is not a new one. But, says **Nancy E Muenchinger**, the development of new technologies in the workplace has meant that the entire subject has once again come to the forefront of the judicial landscape and is having to be seriously rethought.

"The dividing line [between the tie of subordination and private life] can no longer be drawn at the door of the workplace and the end of the work day. Everything has become more complex and more blurred" *(Rapport pour le Ministre du Travail, de l'Emploi et de la Formation Professionnelle, December 1991, Documentation Française, Professor Gérard Lyon-Caen).*

In 1991, when these words were written, they set the groundwork for the law of December 31st, 1992 on Employment, Part-Time Work and Unemployment. This law was devised to implement a "Law on Information Technology and Human Rights" in the workplace to parallel the existing data protection law of January 6th, 1978, known as the "Loi Informatique et Libertés".

The principal tenets of the employment law of December 31st, 1992 were:

1. The principle of "finalité" (purpose) and of proportionality

> "No one can place restrictions on individual and collective rights which are not justified by the nature of the task to be performed and are not proportional to end sought" - **Article 120-2 of the Labour Code.**

This provision has been interpreted so as to allow employers to place restrictions on employee privacy which are justified by the circumstances. For example, in one case it was held that an employer, who was concerned by bomb alerts, legitimately allowed the opening of handbags in front of security agents. The action was justified by exceptional circumstances and was proportional to the objective, in that there was no full-scale search of the handbags.

2. The principle of transparency

The employers' obligation of transparency takes several forms.

a. Consultation of the Works Council

> "The Works Council is [to be] informed and consulted prior to any important plan for introduction of new technologies, when these are susceptible of having consequences on employment, qualifications, remuneration, training, or the conditions of work of personnel" - **Article L-432-2.**

The introduction of "new technologies" has been held to include the implementation of a new computer information system in a bank, when the system was significantly different from the previous one and it required special training. Even the replacement of a third generation computer by a higher performance model has qualified as "new technologies".

Moreover, the Works Council "is [to be] informed prior to any implementation in the enterprise of methods and techniques permitting the control of employees" - **Article L-432-2-1 section 3.**

Such "methods and techniques" would not only include electronic identification and entry systems and video cameras, but also special software used to establish Internet usage, websites visited, connection times, etc.

b. Prior information of salaried workers

> "No information concerning a salaried employee or a candidate for employment may be collected by any means which has not previously been brought to the attention of the employee or the candidate" - **Article L121-8 of the Labour Code.**

This requirement is significant in that it places the burden of informing an employee about monitoring squarely on the employer, rather than on an employee to obtain the means to inform himself. Thus the presence of a monitoring device such as video surveillance equipment in plain view does not do away with the employer's obligation to inform his staff that they are being monitored.

Another aspect of the employer's obligation of transparency toward employees relates to recruitment techniques:

> "A job candidate must be explicitly informed, prior to implementation, of methods and techniques aiding recruitment which are used in regard to him" - **Art L121-7 of French Labour Code.**

In one case, which was judged prior to the effective date of Article L121-7, a company required a handwriting analysis of a job application letter, and the candidate had had his wife write his letter. The court held that the company bore the burden of proving that it would not have hired the candidate in the absence of the tactics which he had employed to obtain the job.

FRENCH DATA PROTECTION LAW: THE LAW OF JANUARY 6TH, 1978

A law created to prevent data collection on individuals interfering with human rights was enacted early on by French legislators. The Law on Information Technology and Human Rights ("Loi Informatique et Libertés"), referred to above and passed on January 6th, 1978, was a precursor to similar laws of its kind in Europe. This law formalised the principle that:

> "information technology must be at the service of the citizen...It must not be detrimental to human identity, human rights, private life, individual or collective liberties" - **Article 1.**

The law created a data protection authority called the Commission Nationale de l'Informatique et des Libertés (CNIL) which acts as a kind of central clearinghouse for all questions concerning data protection. The principal mechanism of the law is the requirement of a declaration: any data processing treatment of "nominative information" (ie. information which identifies or is susceptible of identifying a named individual) must, prior to its implementation, be the subject of a declaration to the CNIL. Thus, any employers wanting to compile databases on their French employees must first proceed to make a declaration to the CNIL.

The latest version of the revised draft law implementing the EU Data Protection Directive (95/46/EC) (after adoption on first reading by the Senate) provides that declarations and requests for authorisation must include:

1. the identity and address of the data controller (employer) or its representative, if it is not established on national territory

2. the purpose(s) of the data processing and the general description of its functions

3. the interconnections with other data processing

4. the personal data processed; its origin and the categories of individuals involved

5. the duration of conservation of the information processed information

6. the services responsible for implementing the processed

7. the parties intended to receive transmission of the data

8. the function of the person or the department providing access to the relevant individuals

9. the security measures to be employed in relation to the data; and

10. the transfers of personal data intended for transmission to non-EU member states.

The same draft requires that all persons from whom data is collected, and thus by extension, employees, be informed of certain aspects of the data collection, namely:

1. the identity of the controller (employer) or of its representative

2. the intended purpose(s) of the data collection

3. the obligatory or optional nature of the reply

4. the consequences of a failure to reply

5. the parties destined to receive the data

6. the data subject/employee's right to access, oppose, or correct data collected; and

7. if applicable, of transfers of data to non-EU member states.

Thus, in addition to its obligation to notify any actions involving technological monitoring in the workplace, the employer must notify employees about the compilation of databases of information concerning them and the uses to which it will be put, including any transfers to a parent company.

It should be noted that the basic obligation to notify data subjects/employees was not instituted by the EU Data Protection Directive. The provision, which already exists under the 1978 law, has merely been updated under the terms of the transposition draft.

Concerning the privacy of its employees, the employer is therefore constrained to deal with a fairly onerous system of principles and rights of employees which act as a type of direct counterbalance to the tie of subordination characterising the employer-employee relationship in France.

Beyond the above specifics, it is important to note that the entire regime on the protection of personal data in France is undergoing profound changes at the moment. Pending the adoption of the draft law, there are still many questions being posed by employers and others to which there are not always clear answers. But at least one element remains stable, and that is the key space which the CNIL will occupy in this sector in the future. In the absence of clear-cut procedures, some companies are making a regular practice of consulting the CNIL for an opinion, rather than waiting for the legislative to be finalised. This is one indication of the increase in power and stature of the CNIL in the last several years, and is a trend which is not likely to be reversed.

SECRECY OF CORRESPONDENCE: THE LAW OF JULY 10TH, 1991 RELATIVE TO SECRECY OF CORRESPONDENCE

Before the introduction of e-mail on the scale attributable to the growth of Internet, there was already existing legislation protecting the secrecy of correspondence that was susceptible of applying to e-mail. Hence, an employer who, in bad faith, engages in "opening, deleting, delaying or diverting correspondence addressed to a third party, whether or not it has arrived at its destination" may be punished by a year in prison or a fine of €45,000 - **Article 226-15 of France's Criminal Code.**

Furthermore, the "fact of [an employer's] intercepting, misappropriating, using or disclosing the correspondence emitted, transmitted or received by a telecommunications network or proceeding to install devices conceived to affect such interceptions" would be punished by the same penalties - **Article 226-15(2).**

The legislation clearly targets all types of networks and telecommunications. The definition of "correspondence" provided in the Postal and Telecommunications Code includes "any transmission, emission, or reception of signals, writings, images, sounds, or information of any nature by optical wire, radio electricity, or other electromagnetic system" - **Article L.32 of Postal and Telecommunications Code**. Thus, employee use of Internet messaging, Minitel, faxes and Intranet, in addition to simple telephone calls, all fall clearly within its scope.

COMPUTER FRAUD: THE LAW OF JANUARY 5TH, 1988 OR "LOI GODFRAIN"

In addition to the types of prohibitions listed above, based on telecommunications law, another regime applies to, and protects, information systems from pirating and computer fraud. This regime is the so-called "Loi Godfrain", which went into effect on January 5th, 1988.

The "Loi Godfrain" places criminal sanctions on (1) the fact of acceding or maintaining oneself fraudulently in all or part of an automated data processing system (one year imprisonment and €15,000 in fines); (2) the fact of impeding or falsifying the functioning of an automated data processing system (three years imprisonment and €45,000 in fines); (3) the fact of introducing data fraudulently into an automated data processing system or deleting or modifying the data which it contains (two years imprisonment and €30,000 in fines) - **Article 323-1 and 323-2 of French Penal Code.**

These provisions, although theoretically applicable to employers, might be more difficult to maintain and to prove against an employer when the data processing system is clearly his own creation, it is under the virtually complete control of a systems administrator hired by the employer, and this administrator is responsible for the architecture of the system, as well as its day-to-day operations.

WORKPLACE PRIVACY CASE LAW: E-MAIL AND INTERNET USE

After some initial hesitation, French judges have come down firmly on the side of employee rights in relation to e-mail monitoring and Internet use. Some of the cases have dealt with personal use of Internet and the potential abuse that can occur, while others have dealt more directly with the concept of violation of correspondence.

In one of the former cases involving IBM, the Employment Court of Nanterre handed down a judgment on July 16th 1999, condemning the employer for wrongful dismissal. IBM had fired one of its employees for gross misconduct in connecting to and downloading onto his hard disk, various files from websites "covering a full range of pornographic practices". However, the court found the employer had not borne the burden of proof of its allegations, since the hard disk had not been under seal following its seizure, and the photographs produced bore dates that were subsequent to the facts, or no date at all. Moreover, an internal document that IBM produced as evidence that it had provided warnings to employees against sexual surfing, did not refer explicitly to this practice. As a result, the company lost the case.

In a second case confirming the trend, the Court of Appeals of Montpellier found imperative the obligation to inform employees as to telephone wiretapping or Internet e-mail monitoring prior to the implementation of employer controls. The facts in that case were that an employee with 16 years of service had used his workstation in a fraudulent manner by sending many e-mail messages during and outside working hours. The terms of the dismissal letter mentioned evidence that had been obtained from a "huissier", or sheriff, in the absence of the employee, and without his authorisation. The only document which the employer had been able to show by way of proof of notice, was a letter sent to the employee at the time of the installation of his computer system - the letter did not mention monitoring at all.

After some initial hesitation, French judges have come down firmly on the side of employee rights in relation to e-mail monitoring and Internet use.

The Court held that the employer had failed to establish gross misconduct justifying the dismissal, and awarded the employee damages equal to six months' salary.

Among the cases dealing with the violation of private correspondence by an employer, two are worthy of note. In the first case, the Tribunal de Grande Instance de Paris (TGI) formally accepted the principle that an electronic mail message constitutes private correspondence, by its decision of November 2nd, 2000.

The case can by summarised briefly as follows: An IT student from Kuwait filed a criminal complaint with the judge (of criminal instruction) alleging (1) theft; (2) opening of private correspondence; and (3) discrimination, ostensibly based on a romantic disagreement.

Three civil servants with a public service role at the "Ecole Supérieure de Physique et de Chimie Industrielle" acknowledged their actions, but maintained that they had acted to preserve the security of the school's network. The court disagreed and said that the motive of "good faith" was immaterial in a case of a criminal act committed by an official of a public service.

The opening of the e-mails on the school network was held to be a violation of the principle of privacy of correspondence under Article 432-9 of the Penal Code. This article provides that a public authority may not abuse its power by ordering, committing, or facilitating the interception or redirection of correspondence sent by means of

telecommunications networks, nor may it use or disclose their contents.

The second case was a landmark decision of the French Supreme Court involving the dismissal in 1995 of an employee of Nikon, for gross misconduct owing to the sending of numerous personal e-mails during working hours. To obtain proof of the employee's actions, the employer had opened and copied onto a diskette a file marked "personal" in the employee's absence. The French Supreme Court found that:

> "an employer cannot read the personal e-mail messages sent by the employee and received by him on a computer placed at his disposition for his work, without infringing his fundamental freedoms, even in the event that the employer has expressly prohibited the use of the computer for non-work related purposes."

The French High Court by this case thus placed important limits on the employer's power to control and monitor its employees during their work hours. In effect, it has carved out a right to protection of private life and a right to secrecy of correspondence which must be respected, even in the workplace and during work time.

CNIL REPORTS

Amid the doubts raised by the recent and sometimes conflicting court decisions, the CNIL has issued two reports relating to e-mail monitoring. The reports contain the main points of the CNIL's recommendations on employees' privacy in the workplace, and the employer's monitoring rights for security reasons. The reports include proposals such as *a posteriori* monitoring of employees, informing employees of filtering tools, use of logging systems, the appointment of privacy officers, and negotiation of the conditions of use of new technologies with workers' representatives. The CNIL also advocates the elaboration of corporate charters of computer system usage in the enterprise as a means of avoiding disputes between workers and employers.

The CNIL reports are merely advisory, however, and are not binding upon a French judge.

CONCLUSION

The net effect of the above laws can be summed up as follows: The "lien de subordination" which is inherent in the employer-employee relationship in France gives the employer certain prerogatives in regard to his employees - in particular the right to monitor in order to evaluate job performance.

Nevertheless, the employer must exercise these prerogatives while respecting the principles of "finalité", proportionality and transparency described in the applicable sections of the Labor Code.

Moreover, before putting into place any control or monitoring process, the employer must:

• inform its employees in a pro-active manner of the existence of monitoring or surveillance systems - **Article 121-8 of the Labour Code**

• declare the creation of databases containing personal data regarding its salaried employees to the CNIL

• consult the Works Council (if the company employs more than 50 people) prior to the introduction of "new technologies" into the workplace, when such technologies may have an impact on employment, remuneration, or other conditions of employment (Article L. 432-2, section 1) or prior to the implementation of any monitoring system (whether telephone, computer, or video surveillance) (Article L. 432-2-1, section 3). It is essential to note that the consequences of the employer's failure to adhere to the above requirements will be criminal sanctions, ie. fines and possible imprisonment.

The drafting of a "code of good conduct" for the use of the company IT system, while not yet mandatory for the employer, can place a company on the "good side" of the CNIL...

The drafting of a "code of good conduct" for the use of the company IT system, while not yet mandatory for the employer, can place a company on the "good side" of the CNIL and can generally assist in defusing uncertainty as to what is/is not acceptable behaviour on the part of the employee.

In summary, the law on workplace privacy in France, while currently evolving in favor of employees' rights in the recent case law, is still a moving target. A brief tour of the international horizon and notably a project of the European Commission for EU action in the field of protection of workers' data, may mean that the current unsettled state of the law will get worse, before it gets better.

AUTHOR: Nancy E Muenchinger is Avocat à la Cour and Attorney-at-Law at Paris-based law firm Denton Salès Vincent & Thomas. She can be contacted at Tel: +33 1 5305 1600 (ext 1692), E-mail: nmuenchinger@dentonwildesapte.com

FURTHER INFORMATION: For details on France's Labour Code, see the International Labour Organisation website at: www.ilo.org/public/english/employment/gems/eeo/law/france/l_lc.htm
Guidance on workplace privacy can be found on the CNIL's website at: www.cnil.fr/thematic/index.htm