French courts define criminal liability and impose fines and prison sentences for DP crime

In recent years, there have been two apparently contradictory trends: to reinforce the data protection principles through strict court decisions and the enactment of sectoral laws; and to withdraw certain issues, for example, closed-circuit TV, from the competence of the CNIL, France's Data Protection Authority. Ariane Mole, a specialist lawyer, explains.

How the statute law has been interpreted by the courts.

The Data Protection Act has been interpreted very strictly and, in particular, the Supreme Court has specified the circumstances in which a penalty may be applied.

The first element is that to be criminally liable, malice is not necessary. *Anyone who engages in the automatic processing of data without declaring it to the CNIL even through ignorance or carelessness, is criminally liable.* There was a case where the manager of an estate agent had been robbed of his customer file. He, therefore, notified the robbery to the public prosecutor to sue the thief. The manager was in turn prosecuted because he had failed to declare his file to the CNIL. He claimed that he was not aware of the duty to do so. So this means that even ignorance of the legislation is not sufficient to avoid prosecution.

The second element is that *there can be no limitation on the time of complaint.* This principle is the result of the 1991 Supreme Court case on telephone logging. An employee was dismissed because telephone logging equipment had proved that he had used his phone for private use. As he had been dismissed, he sued his former employer for not having declared the personal data processing which was involved in the telephone logging system. The first Court and the Court of Appeal decided that the complaint was not valid any more because the complaint had been made three years after the telephone logging equipment was put in place. But then it came to the Supreme Court. The Supreme Court ruled in 1991 that there could be no limitation on the time of the complaint because the logging had never been declared to the CNIL. When the personal data processing has never been declared, there can be no limit on the time of the complaint. The case was on telephone logging, but the principle has now been extended to any kind of personal data processing.

Since 1991, what has happened in the courts? The number of criminal prosecutions has increased and there were two noteworthy judgements in 1994. They reflect a strict interpretation of the Data Protection Act.

Security violation leads to false identification

The first case was on 15 February 1994. The president of France's central company operating the national central credit database on bad payers was prosecuted and fined FFr.50.000 (£6,500) and FFr.5,000 (£650) for compensation by the Paris Court of Appeal for violation of the duty of security laid down in section 29 of the French Data Protection Act. The Court ruled that it had not taken all necessary precautions to identify precisely enough the persons recorded in the bad payers database. This error resulted in an individual with a good payment record being refused credit as he was mistaken for another of the same name who had a bad payment record. In this case, the database was declared to the CNIL but the information which was provided was not reliable enough.

Non-declaration to the CNIL and unfair obtaining leads to fines and prison

In December 1994, two managers of an insurance company were sentenced to 15 months imprisonment and to a fine of FFr.200,000 each (£26,000), because they paid employees of the national electricity board to obtain names and addresses of the people who had recently moved to new homes. Their purpose was to identify the recent movers to send them mailings on house insurance. They were prosecuted because they had failed to declare the mailing list addresses they possessed to the CNIL; and also on the basis of fair obtaining of the data. Ten employees of the national electricity board were also prosecuted and they were sentenced to pay a fine.

Labour code strengthens data law

In recent years, there has been a tendency to reinforce the data protection principles through

sectoral laws which have been added to France's 1978 Data Protection Act.

The labour code has been revised by a law adopted on 31 December 1992 which came into force at the beginning of 1993. The new labour code now incorporates several provisions which refer not only to the data protection principles in the Data Protection Act, but also refer to CNIL recommendations. They have now become binding because they are incorporated in the labour code together with some new data protection principles:

- information about employees or job applicants may be collected only if they are aware of the means of collection
- The applicant or the employee must previously have been informed of the methods and the means that are used to appraise his professional competence or to recruit him.

Such provisions are aimed against a recruitment decision-making process based solely on the use of computers, and against computerised recruitment evaluation tests or professional tests as the sole basis of an assessment. It also means that such tests or computers may be used but the employees or the applicants must be made fully aware, not only of the information which is used, but also of the methods or the techniques which will be used.

"there is a duty to inform the employees' representatives of any processing..... Otherwise it is illegal."

There is another new article in the labour code which provides that the employees' representatives must always be informed of every automated processing of personal data on employees which is being used and of any change or modification of such processing. So there is a duty to inform the employees' representatives of any processing of personal data concerning employees. Otherwise, it is illegal.

Enforcement of the labour code is carried out by the labour inspectors, who are based in every region of France. As a result, data protection principles are now not only under the control of the CNIL but as far as the labour sector is concerned, also under the control of the labour inspectors.

Health data for research purposes

A stricter regime has been introduced for the processing of health data used for research purposes by a law which was adopted on 1st July 1994, and an application decree which was published in May 1995 which means that it is now in force. The powers of the CNIL have been increased, as it now has the power to approve or refuse the use of personal health data for research in both the public and the private sectors. The law has also created, in addition to the CNIL, a recently appointed consultative committee to which all research proposals must be submitted. In practice, this means that:

- all research proposals must now be submitted for the opinion of the consultative committee, and
- these research projects will have to be submitted for the *decision*, not just the *opinion*, of the CNIL.

It is also worth noticing that the Health Data Used for Research Act provides that the transborder data flows of personal health data used for research will only be permitted if a recipient country offers equivalent protection. In the new Act, it is the term "equivalent" protection which is being used although the EU Data Protection Directive provides that there should only be "adequate" protection. But it is also the responsibility of the EU Member States to give national rules on research and health matters.

The result will be that there might be two different sets of rules for transborder data flows:

- the general rules where adequate protection will be required for transborder data flows outside the EU, and
- a specific set of rules for health data used for research when such data will be transferred from France to another country. Even if such a recipient country is inside the EU, equivalent protection in the recipient country might be required. The difference between adequate and equivalent protection still has to be determined.

CNIL's scope narrowed

There is a new trend not to weaken the data protection principles, but to withdraw certain matters from the competence of the CNIL. The reason is because the CNIL was considered as making excessive use of its powers, especially towards the private sector. According to France's Data Protection Act, the obligation to declare to the CNIL consists only of a declaration, and the CNIL, according to the provision of the Act, may only check immediately that all required information has been provided. If it has, the CNIL has to issue a receipt. The CNIL has no power to refuse the automatic processing of data. But what happens in fact is that the CNIL very often suspends the issue of the receipt until the data user agrees to reconsider his processing and purposes and to comply with the CNIL's requirements.

As a result, closed-circuit television has been withdrawn from the scope of the Data Protection Act 1978 (PL&B Oct.'94 p.17, and Dec.'94 p.10). In its place, there is a new law, the Loi Pasquà, adopted on 21 January 1995. But the law has created a procedure which is very similar to that of the Data Protection Act. It has the same principles and the same criminal sanctions in case of violations. For example, closed circuit television projects require, in advance, the opinion of a consultative committee established in each regional *Departement* and it also needs approval by the Prefect who is the head of the *Departement*. The new law is a sectoral Data Protection Act and the only difference is that the CNIL cannot interfere and that was the exact purpose of the Loi Pasquà.

This report is based on a presentation by Ariane Mole at the *Privacy Laws & Business* 8th Annual Conference, July 10-12, 1995, St. John's College, Cambridge. **Ariane Mole, Lawyer, Cabinet Alain Bensoussan, 29 rue du Colonel Pierre Avia, 75508, Paris, Cedex 15, France. Tel: + (33) 1 41 33 35 35 Fax: + (33) 1 41 33 35 36**

France's Data Protection Act: Scope, Declarations and Sanctions

The scope of France's 1978 Data Protection Act is wider than that of the UK Data Protection Act. The two main differences concern the coverage of manual data and the definition of personal data.

France's Act covers both automated and manual processing of personal data.

Under the French Act, personal data means "any data which permit in any form directly or indirectly the identification of the natural persons to which they relate." Therefore, the concept of personal data is not restricted, as in the UK Act, to the information in the possession of the data user or to the information which is processed by reference to the data subject. In France, any data which permits, even indirectly, the identification of the data subject in any form, for example, even when data is encrypted for research purposes, fall within the scope of the French Act.

The French concept of personal data is very close to the definition provided in the EU Data Protection Directive.

Declaration to the CNIL

All automated processing of personal data has to be declared to the CNIL, France's data protection supervisory authority. In other words, any use of a computer involving data relating to individuals, even very indirectly, has to be declared in order to be lawful. As a result of the increase in computerisation generally, there is now an increasing duty of declaration to the CNIL in every sector of society.

The duty to declare in France exists not only in relation to common files such as employees' or customers' files, but also those involving any automated processing such as telephone logging, the use of mailing lists, chip cards, badges for access control, video or audio texts, electronic mail, telecommunication networks and word processing; even the use of fax machines must be declared in order to be used legally.

Sanctions

Infringement of the Act triggers criminal sanctions and the sanctions were increased in March 1994. For example, failure to submit a declaration to the CNIL attracts a maximum fine of FFr.300,000 (£40,000) and three years in prison. In the case of prosecution of a legal person, the fine can be multiplied by five, amounting to a fine of FFr.1,500 000 (£200,000).

The number of criminal prosecutions has increased since 1991. In that year, France's Supreme Court specified the circumstances in which the penalties can be applied.