LEGAL ASPECTS OF THE PROTECTION OF DATA CENTERS

by Bernard E. Amory

Computer security has been most often dealt with by lawyers from two main points of view. The questions which they have attempted to answer concern, on the one hand, the means of legal protection of software (protection by patents, copyright and specific protection) (1) and, on the other, the applicability of traditional criminal law concepts to computer fraud (2). As regards the latter, one of the questions in particular has been whether computer data is susceptible to "theft" in the legal sense of the term, when it is doubtful that it can be the subject of a right of property. The question has also arisen as to whether software can be the subject of forgery, when one of the conditions of this offence is that the falsification is carried out on a written document. The possibility of penalising misappropriation of funds by the abusive use of an electronic fund transfer system has also been discussed. Finally, the question has arisen as to whether the deliberate blocking of telecommunication lines in order to bring an undertaking to a standstill constitutes a crime. It is the principle of the restrictive interpretation of rules of criminal law which makes it difficult to apply these rules to computer fraud. The amendment of criminal legislation would facilitate the detection and punishment of the "computer criminals" and would also have a dissuasive effect.

Accordingly, the solution of these problems is the responsibility of the legislators and not of "risk managers". Nevertheless the latter must take the necessary preventive measures to minimise, on the one hand, the risk of accident and, on the other, when they happen, the consequences. Most of the precautions to be taken are of a technical kind: use of confidential codes, security software physical protection of premises, etc. One should also bear in mind the legal possibilities of maximising the security of data centres. The purpose of this note is to summarise these. These legal precautions should be taken at several stages and with regard to different persons: at the time of the purchase of computer systems, contracts offering sufficient guarantees should be obtained from the supplier and appropriate contracts should be concluded for insurance, maintenance, and back-up for newly acquired systems; finally one should protect oneself with regard to third parties, especially if the Data Center is connected externally by means of

---

(1) For a general study of this question see X. Thunis, Les Modes de Protection Juridique du Logiciel, Namur, 1983.

(2) See especially M. Briat, "La Fraude Informatique", l'Observateur de l'OCDE, no. 127, March 1984, p. 36 et seq. and "L'Informatique et la Delinquance", Revue de Droit Penal et de Criminologie, April 1985.

telecommunications. We shall therefore examine, from the point of view of the protection of the Data Center, six types of contracts: contracts of supply, contracts of maintenance, insurance and back-up; contracts with staff and contracts for telematic services, i.e., contracts which involve the combined use of computers and telecommunications.

1. Supply contracts (1)

When computer systems are being acquired which are to constitute the Data Center or form part of it, several clauses should be agreed with the supplier in order, on the one hand, to prevent mistakes or fraud occurring in the course of the functioning of the system and, on the other, to limit their effects (where they occur) by taking the necessary measures to ensure that the responsibility for them is borne by the person actually responsible.

We shall begin with a general comment regarding the negotiation of supply contracts. The negotiation of clauses for the protection of the acquirer will only be possible if, at the beginning of his contacts with the supplier, he makes his legal requirements known to the supplier. Otherwise, when the parties reach agreement on the commercial aspects, the supplier will present the acquirer with a contract which he will be persuaded to sign as it is, as quickly as possible, without the possibility of adapting it to his requirements for fear of delaying the supply of the system.

By virtue of his preliminary contacts with the acquirer (especially in the context of the feasibility studies and the preparation of his offer) the supplier will probably have access to information which is confidential from the acquirer's point of view. At this stage, it is advisable to request the potential supplier to undertake in writing to the acquirer not to divulge, use for other purposes or retain longer than necessary any information of a confidential nature which he may acquire in the course of these preliminary contacts (2). If the parties agree that the purchaser is to collaborate with the supplier in developing software, it is extremely important to decide at the outset who will be the owner of the developed product, and in the case of joint ownership, the share which will belong to each party. In order to avoid any possible dispute between the parties on the definition of the product which is the subject of the property right, the parties should leave a copy of the jointly-developed software in the hands of a third party chosen by common agreement.

---

(1) For a comprehensive approach to computer contracts we refer to the collective study published by the Facultes Universitaires de Namur "Le Droit des Contrats Informatiques, Principes - Applications", Namur 1983.

(2) On this point see Y. Poullet, Le Droit des Contrats Informatiques, Namur 1983, p. 182.

Where software is acquired the acquirer should ensure that a clause is inserted in the contract obliging the supplier to retain a copy of the product supplied (a copy of the software, the sources and the documentation) for the use of the purchaser. In the event of loss, theft or destruction in the hands of one of the parties, the other can produce the copy. Nevertheless, the acquirer must make sure that the supplier takes the necessary precautions to ensure that the retention of the copies by him (or a third party) does not lead to the further risk of piracy (for example, by the supplier's or third party's employees).

Before signing a supply contract, the acquirer should ensure that it contains a guarantee that spare parts will be provided during the whole of the equipment's "lifetime". Often the supplier will request, in return for this guarantee, the exclusive right to supply the spare parts. This clause should only be accepted on the condition that the parts are supplied within a reasonable period, to be specified in the contract. The acquirer can also request from the supplier an obligation that the supplier must inform him if he is unable to supply certain components (for example, as a result of an interruption in supplies from the manufacturer) in order to allow him to order a reserve supply or to look for other suppliers.

Finally, the acquirer should pay particular attention to general guarantee clauses. Firstly, he should obtain a guarantee regarding delivery periods. However, as regards computers, the observance of a precise delivery period may be extremely difficult if not impossible. Moreover, it is often in the interests of both parties to provide for a certain flexibility as regards delivery periods. It should be sufficient therefore to agree on a particular period as a guideline but providing that where the non-observance of this time-limit is due to the fault or negligence of the supplier, compensation will be payable for the delay. The acquirer should also ensure that his requirements are clearly defined (for example, in the preamble to the contract or the pre-contractual documents). This will be very useful for the parties in the event of a dispute between them as to the conformity of the system supplied with the one ordered. Similarly, particular attention should be paid to the method of enforcing the guarantee, the ideal being that the acquirer has the choice between repair or replacement of the defective parts. Provision should be made for who is to be responsible for the transport and labour costs involved in the repair or replacement of the parts. It is also useful to provide for the possibility of recourse to a back-up system where the repairs lead to the system being immobilised. When the equipment is received, the acquirer should be especially careful to watch out for the possible existence of a latent defect and, as soon as a problem is discovered, to invoke the guarantee clauses (otherwise the benefit of these may be lost).

These are, briefly, the main contractual precautions which should be taken with regard to the supplier of equipment. Of course, each contract will have to be treated individually, depending on the type of acquisition (purchase, rent, leasing time-sharing), the type of equipment (hardware, package software, application software, operating system) and the characteristics of the parties.

2. Maintenance Contracts

The proper functioning of a Data Center also depends on its maintenance. If the undertaking does not carry out its maintenance itself, it will conclude a maintenance contract with a company specialised in this type of service. Before signing such a contract, the following points in particular should be borne in mind:

- what are the parts excluded from maintenance (for example, parts of foreign origin, parts which are damaged due to use which is not in conformity with the technical specifications);

- the time, duration and frequency of maintenance visits (always reserving, subject to notice, the right to modify these matters);

- the time limit for service in the case of a break-down;

- the possibility of the maintenance company itself installing a back-up system;

- the rectification of errors in software and the adaptation to possible new standards (for example, for accountancy software, adaptation to a change in accountancy legislation).

3. Back-up Contracts

Some large undertakings which are heavily dependent on their Data Center have their own complete back-up system situated in a building separate from that where the Data Center is situated. This emergency system can immediately be substituted for the Data Center if the latter, for some reason, fails. The problems arising from the installation and functioning of such an alternative system are essentially the same as those relating to the Data Center itself. If, however, an undertaking does not have its own standby Data Center but is nevertheless heavily dependent on its computerisation it can conclude a back-up contract. Such a contract will be concluded either on a reciprocal basis with an undertaking which has the same need for a back-up system and has compatible equipment, or with an undertaking specialised in the provision of back-up services. Such contracts have to be drafted with great care so that if an accident happens, the parties know exactly and immediately what their respective rights and duties are regarding use and assistance. The main clauses (1) which should be included in these contracts are as follows:

- A clause defining precisely the situations in which the party whose Data Center has a problem can have recourse to back-up. Only a precise description of these circumstances will ensure that when there

---

(1) For further details on this point we refer to the excellent article by David A. Feldheim, "Computer Back-up and Disaster Recovery Agreements", Jurimetrics 1984.

is an urgent need for back-up, the other party will not dispute the right of recourse to a rescue system. Often it is provided that this right will not exist unless the break-down has lasted for a minimum period of time or if it is due to the fault of those in charge of the Date Center.

- A clause establishing the procedure according to which the wish to resort to a rescue system is to be notified to the supplier of the back-up system. The notification procedure should specify the exact time of the request for assistance so that if several Data Centers call on the back-up service at more or less the same time and the latter is not in a position to answer all the requests, there exists an order of priority based on objective criteria.

- A clause describing the back-up service offered and specifying in particular whether it includes technical assistance by the staff of the supplier of back-up services;

- A clause specifying which modifications the parties can make to their respective systems and the procedure for notification and acceptance, so that the compatibility of the systems with each other can be maintained. It is often provided that if one party refuses to accept the other party's modifications to his system, the contract can be revoked.

- As regards payment, the parties should specify which of them is to bear the costs of any contacts by means of telecommunications.

- Finally, one should make sure that the supplier of back-up undertakes personally and on behalf of his personnel and any co-contractors to respect the confidentiality of the information to which they have access when recourse is had to a back-up system.

As well as the back-up of systems, it is extremely important to ensure the back-up of data, although this is simpler and less expensive than back-up of systems. Undertakings can therefore usually provide for this themselves. If, however, they have to entrust this to a third party, it is especially important that the contract contains guarantees of confidentiality.

4. Insurance Contracts

Even if numerous precautions are taken on the technical as well as the legal level with regard to suppliers, staff (see below) and third parties and back-up procedures have been established, it is still necessary to cover by sufficient insurance the risks which inevitably still exist.

As far as insurance for property is concerned (insurance of hardware, operating software, application software) the party seeking insurance has the choice between different types of contracts: the "all risks" contract which lists the risks covered, the others being excluded or the "all risks except" contract which lists only the risks excluded, all others being covered

(except legal exclusions). The "all risks except" insurance is obviously preferable for the insured person especially in the field of computers where not all of the potential risks have been identified.

Whichever type of contract is chosen, a certain number of risks are excluded. Some of these are common to all fields (for example risks of war or natural disaster) and others are particular to computer insurance. We shall only deal with the latter.

Risks which are not connected with the object insured are obviously not covered. One should therefore make sure that all the components of the computer systems are covered but not insured twice: hardware, application software, operating systems, accessories and media. Often insurance contracts for computers are vague as regards the definition of the object covered and therefore implicitly exclude (even if they are of the "all risks except" type) certain components (particularly the application software and the accessories). Amongst the risks generally excluded are the following: risks caused by the accidental release of automatic protection installations, risks resulting from a use which does not conform with the supplier's specifications, loss of data due to the wearing away of supports or accidental erasure, risks due to transport of equipment, etc. Insurance for break-down costs can also be taken out to cover the back-up costs resulting from an accident or "loss of use" insurance if, for some reason, back-up is not possible. Finally, it may be useful to insure oneself against computer fraud. Few insurance companies offer this. A good "computer fraud" insurance should cover not only the insured's own risks (theft of data, unauthorised use, sabotage of equipment) but also the liability which the insured may have with regard to third parties (for example, for loss of data entrusted to him or delay in the performance of an obligation due to fraud). "Computer fraud" policies exclude certain risks such as, for example, damage committed with the complicity of the insured's staff: it is often the staff which is the source of computer fraud and indirect damage such as loss of use due to the disappearance of the list of clients or loss of know-how. One should therefore ensure that such risks are expressly included.

When computer equipment is rented or acquired on hire-purchase it is in principle the lessee or hire-purchaser who should, as guardian of the object, take out the necessary insurance. However, for several reasons, it is not unusual for the lessor himself to take out insurance to cover the equipment rented. In this case, the lessee should verify which risks are effectively covered by the owner and himself insure any risks which are not covered. He should also ask the proprietor to renounce any right of subrogation which the latter has against him.

5. Employment Contracts with EDP Personnel

One of the most important risks threatening the Data Center originates in the company's personnel. This is due to the relative ease of access which employees have to the Data Center. By copying licensed software from the Data Center and selling it to third parties the employees can render their

employer liable to the licensor. The personnel can also communicate to third parties very confidential information kept in the Data Center (for example, a list of clients).

In order to minimize such risks, companies implement internal organization measures to control access of their own personnel to the Data Center (use of secret access codes and personal identification numbers for access to premises and computer systems, appointment of a security officer, issuance of internal regulations with regard to access to the Data Center.

From a legal point of view, it is important to lay down specific provisions in the employment contracts with personnel regulating their contacts with the Data Center. Firstly, such contracts should contain a clause prohibiting employees from either communicating to third parties or using for personal purposes any confidential information acquired in the company. This is an ordinary clause appearing in most employment contracts. However, with respect to EDP personnel, it is useful to make a list in the employment contract of examples of the type of information or data the employer considers particularly sensitive and confidential. This could eventually facilitate dismissal for cause in the event of the employee violating this obligation or, if the confidential data are communicated after termination of employment, it can facilitate obtaining damages. Finally, one should introduce a non-competition clause, which in order to be valid would have to conform with legal requirements regulating this type of clause. If the EDP personnel are involved in developing software, one should provide in the employment contract who will be the owner of intellectual property rights attached to such software (1). For example, one can provide that any software or other product developed by the employee within the company during or after the business hours with the assistance (direct or indirect) of the company will be the employee's property.

6. Contracting for "Telematics"

The combined use of computers and telecommunications (known as "telematics") allows firms to link their respective Data Centers by telecommunications so as to exchange information and even to conclude transactions. Such technologies are presently thriving notably in the banking sector: telematics links between banks and their customers make it possible for the latter to obtain "on-line" information on their bank accounts in all subsidiaries and branches of their bank. It also permits customers to obtain information about exchange rates and to give instructions regarding payments.

---

(1) In France the law of July 3 1985 provides that as from January 1st 1986, property rights on software developed by employees are owned by the employer, in the absence of an explicit provision to the contrary.

Such telematics links raise new security problems with regard to the identification of the parties, authenticity and integrity of the contents of messages (i.e., absence of fraud and errors), determination of liabilities in case of damage occurring during the transmission of the message.

Technical devices have been developed to respond to these questions (notably the use of secret codes and cryptography). From the legal standpoint, it is very important when contracting for telematics services to provide for specific provisions which are required by such new technologies. For example, since there is no written signature in telematic transactions (e.g., execution by a bank of payment orders received from the customer by telematics) the parties should agree in the underlying contract that the secret code and/or personal identification number will be equivalent to a written signature (1). Otherwise, such transactions may be unenforceable. It is also important to provide that computer documents kept by the parties (e.g. magnetic tape, discs, computer microfilms, ...) will be considered as conclusive evidence of their contents (2). One should also provide within such contracts for the respective liabilities of the parties involved in the transmission of messages (including possible intermediaries but taking into account the fact that, generally, Postal and Telecommunications authorities escape any liability under continental law). Otherwise such liabilities may be very difficult to establish (notably by reason of the difficulty of locating malfunctioning in a telematic network). Without such provisions, one might apply by analogy the rule applicable in multimodal transport, i.e., that the sender of the message would be responsible for its arrival without taking into account any intermediaries. The jurisdiction and choice of law clauses in such contracts should also be drafted with particular care because of the often international character of telematic transactions.

---

(1) In France, however, the validity of the "electronic signature" has been very recently denied by a Court - See Tribunal d'Instance de Sete, May 9, 1984 - Dalloz, Jurisprudence, 1985, p. 359.

(2) However, under U.K. law, the admissibility of computer evidence has been regulated by the Civil Evidence Act 1968. In U.S. law, the hearsay rule objection to the admissibility of computer documents has been rejected on the basis of the "business records" exception.

Conclusion

Since companies are becoming more and more dependent upon their Data Centers, any malfunctioning or failure of the latter can result in a disaster for the company's business. The numerous types of technical and physical means of protection of the Data Centers do not eliminate all risks. That is why appropriate contracts have to be agreed by computerized undertakings in order to reduce the exposure of the Data Centers. This paper simply outlines the most sensible provisions of such contracts. Of course, the whole content of these has to be drafted very carefully and the various contracts relating to the Data Center have to be drafted as a whole in order to avoid any inconsistencies.

* * *