

# Legal aspects of computer programs security in Spain

*Enrique Batalla*

---

The protection of computer programs and the data contained in them is a necessity arising directly from the development of communications and the treatment of computer science in general.

In order to achieve the introduction of a single market in Europe, the harmonisation of the laws of the different countries has become an important issue. To accomplish this idea of a single market without any barriers it is essential that computer data and other means of support enjoy a protection that makes them practical for the business world. In Spain, this protection is disseminated within the legislation, i.e., no specific rule has been promulgated so principles, norms and obligations on computer programs security are found in civil, criminal and mercantile laws.

The computer program security, because it covers several fields of the law it turns to be extremely widespread. We will only refer to the two most relevant aspects of the computer programs security within the Spanish legislation which are the obligations and legal suggestions and the risks involved.

## ***Obligations and legal suggestions in matters of computer programs security***

The obligation to secure computer programs is included under several precepts of the Spanish legislation such as:

### ***Security systems imposed (or suggested) by the mercantile and civil laws***

According to the mercantile legislation companies are allowed to use computer science programs to carry the accounting books which must be kept for a period of six years.

Based on this idea it becomes necessary to adopt certain measures oriented to provide protection to these programs. It is not therefore an idea imposed by the mercantile laws, but rather is a recommendation that aims to give protection to these programs, in order to allow possible inspections, audits and judicial requirements.

On the other hand in civil as well as in mercantile matters, a private contract is considered as a law that obligates the parties. To such respect software contracts subscribed when acquiring licences usually provide for security systems to protect the integrity of the software as well as the exploitation rights held by the proprietor of the program.

It is a common practice (admitted by the Tribunals) that the Spanish legal advisors recommend to include in the software contracts a clause of subsidiary responsibility for the company that uses the program in case of unlawful conduct by its employees.

### ***Security systems imposed (or suggested) by the intellectual property laws***

There are not any provisions in intellectual property laws that impose any obligation to adopt measures over security systems for computer programs, although it is necessary to establish a security system preventing the violation of the copyrights of the software author.

This conclusion is based on an analysis of the legal texts that enshrine the protection of copyright against fraudulent actions besides specifying that an owner of copyright is allowed to adopt special measures of protection.

On the other hand the intellectual property laws prohibit most actions

pertaining to computer programs and allow the possibility of considering the employer as civil subsidiary responsible party of the violations committed within the workplace by employees.

It is important to mention other areas of the Spanish legislation, where the protection of computer programs makes the adoption of security measures necessary, such as the:

- **Tax Laws** Currently most tax documents are produced by computer. In these cases (especially if no graphic support is available) and as the documents must be kept for tax reasons for five years due to possible inspections, audits, etc, it is necessary to adopt security measures.
- **Administrative Laws** The protection becomes necessary as these laws allow the communication through computer means, giving full legitimacy to documents coming from these files.

### ***Security systems imposed by the LORTAD (Organic Law for the protection of computerised personal data)***

On 29 October 1992 the Spanish Parliament approved the LORTAD that protects data.

This law was enacted in accordance with a constitutional mandate under Article 18.4 of the Spanish Constitution according to which "*the law will restrict the use of computer science to guarantee the honour and personal intimacy of the citizens and the full exercise of their rights*".

The above law clearly establishes the need to implement security systems for computer programs which embodies four basic concepts:

---

## Computer programs security in Spain

---

- **Confidentiality** The privacy of personal data is an obligation firmly incorporated in different articles of the Law, which has been subsequently developed in order to determine the requirements and the conditions that must be met for files as well as for persons that participate in the process.

The professional secret is established as an additional security measure for the individual that holds responsibility over the files and for those that participate in any of the phases involved by the process.

This obligation to keep the professional secret does not end with the life of the subjects involved, as it continues and may give rise to liability for damages.

The general principles that must be respected in order to maintain the privacy of the personal data are:

- To avoid alterations, losses, treatments or non authorised accesses.
- Setting up of technical and organisational security measures.

The Agency for Data Protection is the institution in charge of ensuring that these principles are complied with.

Although some regulations have been promulgated by the passage of the Statute of the Agency for Data Protection and Royal Decree No. 1332/94 of 20 June 1994, that develops several aspects contemplated by the Law, the most important regulation is the Royal Decree of 20 June 1994, developed by the Law.

This regulation also establishes the "responsibility over the files" that according to Article 3 is defined as the individual or legal entity with decision making capacity over the purpose, content and use of the data processing.

- **Veracity and integrity** both of these principles are included as they regulate the right to rectification and cancellation.

- **Availability.**

- **Claims** This regulation establishes also the principle of filing claims and requesting indemnification for the damages suffered as a result of violations against the law. However, it does not specify the procedure throughout which the indemnity will be obtained, leaving it to the Regulation to decide on the guardianship of rights as well as on the sanctioning procedure.

The need to have security systems does not suppose a simple recommendation or a listing of principles, as the Law provides for a number of specific measures oriented to achieve such protection, such as:

- That the Agency for Data Protection may inspect such measures. The proprietor of the file or the responsible person shall allow the corresponding access.
- The failure to meet the principles listed by the LORTAD may give rise to serious sanctions (between Pesetas 83.300 and 416.000) or to very serious sanctions (Pesetas 830.000.-).
- The security measure available must be specified in order to register the file with the General Registry for Data Protection.
- The individuals who are responsible for the files shall also be responsible for their lack of security and any damage arising from it.
- Anybody may demand payment for damages if affected by any breach of the provisions of this Law.

### **Legal risks**

It is not possible, due to the extension, to refer to all risks involved in computer security, so, and being aware that we are omitting issues such as hardware security, failures in the software, insurance contracts covering computer collapse, we will refer to those we believe are more interesting or problematic from the viewpoint of the Spanish labor, civil and criminal legislation.

### **Labor risks**

Two kinds of labor risks may arise in connection with computer systems: those referring to the ownership of the programs and those that may arise when the operation of the system is relocated.

In the first case the Spanish legislation allows a company to own the copyrights, provided such copyright has been already published as collective work and disclosed under the name of the company involved.

On the other hand, the Intellectual Property Law provides that the ownership of the economic rights derived from the development of a computer program by an employee that receives a salary shall belong exclusively to the company. However, the mentioned Law admits agreements between the worker and the impresario with respect to a different ownership.

In summary, it is essential to set up security systems to guarantee that the rights inherent in the software developed by employees of a company belong exclusively to the company.

With respect to the relocation of the employees, it is obvious an effective protection against external threats is required that may prevent the use of the systems developed.

### **Penal Risks**

The so-called "computer felony" is most difficult to prosecute due to diverse reasons such as:

- Quickness in the preparation
- Facility to erase the evidences
- Facility to cover-up the action
- Difficulty to find a proof on a magnetic support.

It is therefore necessary to adopt security measures, as the methods to perpetrate this kind of felonies may be diverse:

- Manipulation of data existing on somebody else's file
- Access to information and its use without authorisation

- Use of programs of a third party without authorisation to the own benefit
- Use of practices to destroy information that belong to others (viruses)
- Use of personal data for purposes different to those authorised
- Manipulation of programs, etc.

The new Spanish Penal Code enforceable since 24 May 1996 includes a number of new improvements over its predecessor:

- Categorical punishment for misappropriation of personal data in any instrument, file or magnetic support, and also against the unfolding and disclosure of secrets through the interception of electronic mail.
- Extension of the documents definition to diskettes, hard disks, etc.
- Higher protection against computer espionage.

### **Civil Risks**

If the civil field the risks are higher and as a result higher measures must be adopted, keeping in mind the following aspects:

#### **Ownership of the Programs**

The computer supplier is the only owner of the Exploitation Rights over the programs supplied by him and as a result he will be the only person capacitated to assign the use or the ownership of said programs. A system then becomes necessary to protect the supplier when transmitting the licenses of use of the computer programs.

The Spanish Intellectual Property Law provides the withdrawal of the unlawful issues and their destruction as measures oriented to protect the author rights.

The situation gets complicated when an assignment is made to a third party to develop a specific work. In such cases the following measures should be adopted in order to obtain legal protection in Spain.

In the first place, the contract should clearly establish who will be the holder of the Exploitation Rights (the economic rights as the moral rights will always belong to its creator).

The possibility of involving an employee that gets a salary should be foreseen, in which case we will refer to paragraph "labour risks" above.

In this case, the Law for the Legal Protection of Software of 23 December 1993 (enforced to incorporate Directive 91/250/EEC of 14 May 1991 to the Spanish legislation) grants the ownership of the economic rights of the software developed by a salary earner to the impresario (although agreements on the contrary are admissible).

It is important to point out that the Spanish Courts have seen and understood that the impresario is also subsidiary responsible for the damages caused by his employees.

Therefore it is convenient for all parties to establish the security measures to avoid the employees may commit unlawful activities or against the ownership of the programs.

In the case of collaborations with third parties, it is advisable to obtain protection by adding confidentiality clauses to the contracts that demand responsibilities in case of unlawful activities.

On the other hand, a basic precaution measure is to inscribe the program with the Registry in order to identify the legitimate owner, as in the case of assignment to a third party, the software could be considered as collective work.

It is also important to mention the risk involved for the owner of the copyrights when not considering the possibility of future developments or improvements of the program.

#### **Electronic undertaking**

The formation of contract through electronic means is becoming more and more popular, hence the need to implement protection measures.

The first innovation brought by this kind of contract is that while in

conventional contracts according to the Spanish legislation the validity comes with the issuance of the acceptance, in the case of electronic contracts the validity comes with the reception of the document involved.

The major problems encountered with this kind of contract are:

Form of undertaking: contracts formalised through computer means are admissible.

The difficulty arises when having to prove the existence of such contracts if it has been formed through computer which means there is no written proof of its existence.

Security measures must then be adopted like for instance stipulating in the contracts that both parties admit as valid documents the "outputs" of the system.

Identification of the parties. The sign that identifies a person is the signature that indicates the will to undertake an obligation. Since in the case of electronic contracts it is not possible to sign, the contract must provide a clause by virtue of which the parties agree to give a binding value to the code or key.

In fact some official organisations in Spain admit the identification through codes like the Bank of Spain, the Mercantile Registry and the Securities Exchange Commission. (The Securities Exchange Commission is the organisation in charge of supervising and inspecting the stock market, assisting the Government and the Treasury Office in everything concerning the stock market, including imposition of fines to those companies that infringe the law ruling the stock market).

In the standard program proposed by the TEDIS (Trade Electronic Data Interchange System), contemplates and optional clause according to which the companies give probational value of digital signatures. These kind of clauses however, are not easily accepted by the Spanish legislation.

The identification of the parties is guaranteed by a security measure called the "Electronic Notary".

---

## Computer programs security in Spain

---

Security and reliability of the contents. Transactions made by computer mesne may be at risk if unable to prove their authenticity. Security measures such as the following may be adopted:

“Electronic Notary” or “Trusted Third Party” which are systems that store the exchange of messages.

Secret codes for documents, etc.

The clause considered by the TEDIS, according to which the parties undertake that in case of litigation they will not doubt the probational value of the documents submitted by the other party will not be easily accepted by the Spanish legislation.

Procedural security. An international harmonisation of the exchanges of computer data is necessary to enjoy juridical security.

The Cabinet of Ministers of the European Union is working on the harmonisation of the legislation in force in the different Member States with respect to the admittance of computer outputs as evidence in court cases.

In general terms, we may say that the “print out” is as valid as any other private document in the hand of any of the parties.

In the Spanish Tribunals, the computer support is usually accepted as a proof although in most cases is submitted to the opinion of the Judge.

*Enrique Batalla is a partner in the Madrid office and co-founder of national law firm Batalla and Larrauri in Spain. He can be reached at*

*ph (341) 431 1073*

*fax (341) 577 0763*

*email bpc10843@teleline.es*