4. Basic concepts and legal framework in the day-to-day activities of computer professionals

1. Introduction

Computer law does not exist as such; it refers to a set of rules governing other aspects and which can also be applied to computing science. But there is also an increasing set of standards that do address IT aspects only.

1.1. Basic concepts

The hierarchy of the set of laws is:

- Fundamental law: In Spain, the fundamental law is the Constitution, which regulates the basic rights and freedoms of individuals and organizes the political powers and institutions. It is above any law.
- Organic and ordinary laws: Organic laws are different from the ordinary laws in such a way that the former are those concerning the fundamental rights and public freedoms, those approving the Statutes of Autonomy and the general electoral system, and all the other ones referred to in the Constitution. The approval, amendment or repeal of organic laws shall require an absolute majority in Congress, in a final vote on the overall project.
- Decree-law: In case of extraordinary and urgent need, the Government may issue temporary legislative provisions which take the form of decree-laws and shall not affect the ordering of the basic state institutions, citizens´ rights, duties and freedoms contained in the Constitution, the system of Autonomous Communities nor the general election law. Decree-laws must be immediately submitted in full for debate and voting by the Congress, called for that purpose if not in session, within thirty days after its enactment. The Congress shall decide within that period specifically on their ratification or repeal, for which the regulation will establish a special and summary procedure. During the period established in the previous section, the Cortes may process them as draft laws by emergency procedure.
- Regulatory requirements: The regulations (royal decrees and ministerial orders) emanate from the executive branch power (the royal decree from the Council of Ministers and ministerial orders from the different ministries), and can not contradict any law.

It should be noted that there is supranational legislation as a result of the transfer of national sovereignty to perform common actions (or a unified action) between a set of countries. In the case of the European Union, there is a transfer of power to the European Council, Commission

and Parliament which have legislative initiative. We distinguish between regulations, directives and decisions. The regulations are legal standards issued by the European institutions that have direct effect in the member countries, which take precedence over national law. The directives contain targets that countries must comply within a time specified, and each country transcribe the directive into their own legislation in their own terms. Finally, the decisions also have a direct effect, but in this case they have a more administrative nature and are addressed to particular recipients.

1.2. Law of Information Society Services

The Spanish "Law of Information Society Services and Electronic Commerce"[1] arises to include in our legislation the Directive 2000/31/EC[2] of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

Information society service means "any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service" (Recital 17 of the Ecommerce Directive). This requirement should be broadly construed. For example, although a simple "brochure" website might not be an information society service, a website that earns money through advertising almost certainly will constitute an information society service, even if it is completely free to users.

1.3. Law on Citizens' Electronic Access to Public Services

The Law on Citizens' Electronic Access to Public Services[3] (also known as "Law on eGovernment") entered into force on 24 June 2007. It officially recognizes the right of citizens to communicate electronically with Public Administrations, i.e. to conduct their administrative business by electronic means on a 24-hour basis any day of the year.

The aim of the law is to enhance efficiency by doing away with the need to present paper documents to authorities, to promote "closeness to the citizen and administrative transparency" and to contribute to the development of eGovernment. It also establishes the basic principles for the use of IT between citizens and the Administration, but also among (central, regional and local) Public Administrations.

The purpose of the new legislation is to ensure that citizens have the right to electronic access to public services with full compliance by public authorities to legal issues such as data protection, access rights to information management, preservation of third party interest, etc. The fulfilling of this legislative requirement presents public administrations with a challenge in terms of requiring new media and technological tools to meet the strict compliance deadline of the 31st December 2009.

[1] Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y el Comercio Electrónico.
[2] Directive 2000/31/CE.
[3] Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

2. Civil liability

Civil liability is the potential responsibility for payment of damages as a result of an action or omission (for example, third party damage in car accidents, in hunting accidents, for leak contaminants into the environment from businesses, resulting from a professional error, etc).

In order to succeed with a claim for damages arising out of the action or omission of another, it is necessary to prove fault on the part of that person. Fault can take on the form of either: Intent, and Negligence.

From the point of view of intentionality we may distinguish two types of behaviors:

- Fraudulent behavior: Events where the subject is aware that he will cause harm (something done with the intention to harm).
- Negligent behavior: Lawful acts that cause damage because the appropriate precautions are not taken into account, that is, for acting negligently.

The compensation involves quantifying first the damages suffered by the person or entity due to the activity of one individual who has personal liability for it, and second repairing the damage caused. The right to compensation could include not only the value of the loss suffered (consequential loss), but the gain the creditor has ceased to get (ceasing gain). The amount so obtained is called full reparation so that the person suffering the damage is restored to the previous situation, before the occurrence of the act giving rise to compensation.

Civil liability differs from criminal liability in that the latter is intended to designate the person who must answer for the damages caused to the society as a whole, not to a particular individual. Therefore, the damages in criminal liability are social, since they are considered as violations of public order. A violation of public order is legally defined as any act or conduct that is thought to seriously endanger or cause fear or significant unrest among the public. The civil liability is an attempt to repair the damage caused to victims, therefore, the sanction of civil liability is in principle compensatory, rather than punitive. Both responsibilities can coexist in the same event.

2.1. Civil liability in the field of engineering

In contractual relationships we distinguish between obligations of means and obligations of result:

- The obligations of means, whereby a party undertakes to make its best efforts, or to use the appropriate means, to do something for the other party. Obligations of means only require a debtor to act prudently and diligently and to use all reasonable means so as to endeavor to achieve a certain result. No result is guaranteed, however.
- The obligations of result, whereby a party undertakes to achieve a defined result. Obligations of result, to the contrary and as their name rightfully suggests, require a debtor to actually achieve the bargained for result except only where the debtor can rightfully invoke a force majeure or the creditor's fault to be excused.

Obligations will in principle be qualified as obligations of means when their execution bears a significant uncertainty or when the obligor plays a certain role in the execution of the obligation.

Professional liability can be defined as those legal obligations arising out of professional's errors, negligent acts, or omissions during the course of the practice of his or her craft. Traditionally, the scope of professional liability was limited entirely to liberal professions. A liberal profession is an occupation pursued in relation to an ideal of public service and requiring substantial mastery of complex skills in the liberal arts or sciences which cannot be delegated to assistants. It certainly covers the law and medicine. Nowadays, it covers any occupation requiring advanced technical knowledge or which can be followed in self-employment. Professional liability insurance protects professionals such as accountants, lawyers and physicians against negligence and other claims initiated by their clients.

In the case of computer engineers, one of the typical cases where he may incur liability is data protection.

In fact, the Data Protection Act states that the person who suffers damage or injury is entitled to compensation. For compensation to be claimed, the interested person claiming must have suffered some damage, proven, effective and real. It is not enough, for example, to demonstrate a breach of duty in relation to the processing of data.

2.2. Civil liability insurance

Civil liability insurance is only responsible for the other party's losses. Your person and your property are unprotected, but liability insurance protects you from being held responsible for the other party's damages.

There are different types of liability insurance, including general liability, which works in much the same way as auto liability insurance, but covers businesses. General liability protects a company from third party claims. Aside from general liability, there is also D & O liability, employer liability, and professional liability insurance.

The purpose for professional liability insurance is to protect those seen as professionals or "experts" in a given field, who may not be protected by general liability due to their expertise. When one is seen as a professional, he is held to a higher standard and is therefore often considered to hold greater liability towards his clients. Consequently, he needs more coverage than general liability insurance offers.

3. Computer crimes

An individual may incur criminal liability even where he was not aware that the activity constituted a crime.

The Spanish Penal Code does not cover computer crimes as such. Computer crime can be defined as a criminal activity which is committed through computerized means, such as crimes of fraud, offenses against intellectual property, etc., in other words facts that are criminalized in the Penal Code and based on computer mechanisms. In this sense, some legal experts do not consider the necessity of differentiating them from traditional crimes.

On the other hand, computer crime also refers to a criminal activity aiming to somehow damage computers, electronic means or Internet networks. Computer systems have become an attractive target for attack. The damage caused is enormous since it goes far beyond the material value of damaged items.

In summary, the computer may have been used in the commission of a crime, or it may be the target. Computer crime refers to any crime that involves a computer and a network.

3.1. Computer crime characteristics

According to Julio Téllez Valdés (1991), computer crimes present a number of common characteristics:

- Most are imprudent acts, which are not necessarily committed with intent.
- Sometimes these acts can be performed easily and quickly.
- They can cause serious economic losses.
- They require some technical skills to be performed and can become quite sophisticated.
- They do not require physical presence to be performed.
- They are too hard to audit because, in many cases, it is difficult to find the evidence.
- The proliferation and evolution of these crimes make it even more complicated their identification and subsequent persecution.

3.2. Computer crime classification

The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime or just the Budapest Convention, is the first international treaty seeking to address Computer crime and Internet crimes by harmonizing national laws, improving investigative techniques and increasing cooperation among nations. It was drawn up by the Council of Europe in Strasbourg with the active participation of the Council of Europe's observer states Canada, Japan and China.

The Convention on Cybercrime presents the following classification of computer crimes into four groups:

- Offences against the confidentiality, integrity and availability of computer data and systems.
- Computer-related offences, such as computer-related forgery and fraud.

- Content-related offences, which include exclusively offences related to child pornography.
- Offences related to infringements of copyright and related rights, for example illegal copies of software or computer hacking.

Later in 2003, the Additional Protocol to the Convention on Cybercrime added a fifth group. Those states that have ratified the additional protocol are requited to criminalize the dissemination of racist and xenophobic material through computer systems, as well as of racist and xenophobic-motivated threats and insults.