Governments are forcing companies to adopt measures to avoid cyber crime, guarantee security and protect personal data.

For years the governments of the developed countries have been issuing rules and regulations in relation to the storage and treatment of information in electronic format. Besides protecting the copyright of data bases, these regulations try to make companies comply with a series of norms in material to do with public order, technical security and the protection of personal data. Depending on the legislative model adopted, companies will have to incur huge expenses. From the moment that the Internet became popular, governments have feared that the net might be used by organised crime as an instrument to exchange information.

Using this argument the regulators have imposed upon companies in the new technology sector a series of obligations forcing them to collaborate with the judicial and administrative authorities. An example of this can be found in Spain with the Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (Law of Services in the Information and Electronic Commerce Sectors), which comes into force on the twelfth of October. This law obliges Internet Service Providers (ISPs), electronic shops and other companies that use the net to retain data on their electronic communications for a maximum period of twelve months.

According to the National Association of Internet Companies (ANIEI), this obligation is economically inviable. If this association's figures are correct, complying with the legislation will entail an average annual investment for each company in the sector of between 104 and 120 million euros.

Technical security, considered in relation to problems caused by viruses, the loss of data and other physical damage to information, is another of the aspects that force up the cost of the maintenance of data bases. Governments are fairly reluctant to impose specific obligations on the manufacturers of software and the companies that use their products, preferring to rely on general commercial guidelines and, in more serious cases, to criminal penalties. This legislative policy is not the most adequate, taking into account the growing number of computer security incidents. According to the CERT Coordination Center, just in the United States, in more than a decade, this type of incident has doubled every year. As a consequence of this, North American companies suffered losses to the tune of six thousand million euros last year, according to a study by Ferris Research. The third regulatory element that influences company costs is the protection of personal data.

Models
In the field of personal data protection there exist two clearly differentiated models: the
European Union model, with regulations and some very strict administrative checks, and the majority of Anglo-Saxon countries, in which self-regulation is the norm. In both cases, the costs that the private sector faces are huge. In the communitarian model, if a company wishes to comply fully with the legislation in force it must acquire software and specific insurance, not to mention contract assiduously special plans for training personnel, audits and juridical services. If that is not enough, the authorities have reserved a sanctioning power that companies must take into account. In Spain this capacity has reached the point that our country leads the world in fines, both in relative and absolute numbers.

Dangers
In the other standard model, in which countries opt to cede to industry the capacity to create their own rules for data protection, companies face other types of danger. On the one hand, in these countries a greater amount of junk mail is produced, with the expense that this brings with it in terms of connection to the Internet and the loss of working hours. On the other hand, and what is clear from a study published this year by Electronic Privacy Information Center, an insufficient management of data can lead to some considerable indirect costs for the company: bad image (with the consequent loss of customers to the competition), legal fees, indemnities and the loss of business opportunities in other countries where the guidelines on the protection of data are stricter.

The Question

"Is the Spanish regulation of data bases adequate?"

Regulations that restrict freedom
Carlos Sancho, Associate Professor, IESE
It is unlikely that legislation restrictive of human liberty and based on the concept of a police state will appear. The restraints that follow from said legislation would nullify the very nature of the information society: universality, immediacy and free knowledge. General state legislation contains sufficient precepts in this sphere to track down and sanction illicit actions. Either the determination of the concept of public order is reduced or it will end up with computers connected to the nearest police station. Regarding technical security, there will have to be some thought given to the possibility of making the software manufacturers responsible. The regulations referring to the protection of personal data is clearly normative. An Anglo-Saxon model would be better, with less control and more self-regulation. The regulations are, to sum up, a manifestation of the fear that the legislator has of freedom.

Protection is suffocating companies
Javier Ribas, Associate Director, PwC-Landwell
It is necessary that legislation protects us from any abuse in the computer treatment of our personal data. However, the regulations on data protection do not appear to be the most suitable to obtain adequate protection of the right to privacy without suffocating companies, impeding their legitimate interest in marketing their products or imposing some excessive security obligations. There is the impression that the effort that the private sector makes to adjust itself to said regulations is greater than that of the public
sector. Whilst companies that carry out direct marketing have been the object of an implacable persecution, the same has not been the case in the public sector. An example of this can be found in the low-level courts, where case records are piled up in which anyone can read the name of the accused and on the computers of the tax authorities, where one can come across data from very diverse sources..