Protection of data, a new goldmine for consultancy firms

Roberto García Castro
Expansión
31/05/2002

New technology has cast doubt on the security of companies’ data bases, so much so that they have turned to consultancy firms to receive advice on how to protect this information.

The consultancy world has discovered a goldmine in the New Economy. Data bases corresponding to clients or suppliers have become critical information, the loss of which could be very costly for companies. To avoid surprises, corporations have placed the management and custodianship of this type of data in the hands of consultancy firms. It is becoming more and more common for lawyers and technical specialists in new technology to advise companies, hospitals, educational institutions and governments on the handling of data from third parties.

Not since the millennium bug has a singular phenomenon captured the attention of so many professionals in so many fields. Big consultancy firms like PricewaterhouseCoopers and Deloitte&Touche have formed teams of experts in privacy to offer consultancy services to big companies valued at between 54,294 euros and 162,884 euros each. Other consultancy firms like IBM have gone from having two experts in privacy in 1998 to more than sixty three years later. We are talking of a business that will go from turning over 325 million euros in 1999 to 1,954 million euros in 2003, according to estimations by Gartner Dataquest. "We are making a lot of money in this field, but the best years have still to come", affirmed Steve DelVechio, partner at PricewaterhouseCoopers.

The reasons for this are to be found in the ethical-legal and technological fields. If it was not for the spectacular advances brought about by the widespread use of applications provided by Oracle, IBM or SAP, today we would not be discussing this topic. The new technologies make possible a wide variety of processes for storing data. Nowadays a company can share with its subsidiaries or strategic allies the same data base via wireless systems, laser and the Internet. These mediums are also what allowed users to receive on average 571 pieces of junk mail in 2001, according to Jupiter Media Metrix. The regulator, in his attempts to normalise the situation, found himself overwhelmed and with very little jurisprudence that could act as a guide in these cases. The Data Protection Act (La Ley Organica de Proteccion de Datos), the new LSSI, and the Automated Treatment of Data Act (La Ley Organica sobre el Tratamiento Automatizado de Datos- LORTAD) establish the operative framework that companies must abide by.

Organisations that do not respect this framework will face penalties that range from 601
euros, in less serious cases, to 601,000 euros, in the more serious cases. A deeper analysis of the problem leads to the terrain of personal freedom. Within this freedom, the problem will be the level of control that an individual can have of himself and his data. Nowadays, society has a number of tremendously sophisticated techniques available that allow this control to be passed to other people. Society has solicited and manifested more protection. From the ethical-legal perspective it has gone from the traditional concepts of intimacy, privacy and respect for the honour and the good name of a person to a new conception of privacy based on the idea that people are the owners of their own personal data, a concept guaranteed by a ruling of the Constitutional Tribunal.

**Advice**
Consultancy firms in this field base themselves on validating this emergent right and for this reason advise their clients, firstly, to declare all files with data on third parties to the Protection of Data Agency in order to legalise their data bases. Secondly, they secure the consent of the interested party to handle and make their data available, as in this way the file remains legitimate. In these first two phases it would be advisable to have a legal expert at hand. The legalisation and legitimisation of files will have to go hand in hand with protection. On this last point the consultancy expert will be determinant. Legalising, legitimising and protecting data bases are the three concepts on which all privacy consultants must base themselves.

"What aspects must a privacy consultant analyse?"

**Management must compromise themselves**
**Joan Fontrodona, IESE Teacher**
The principal objective of the privacy consultant is to ensure that companies have their strategies and policies in accord with the increasing importance of the protection of personal data. That is why it is crucial, in the first place, to know the juridical framework and to adapt company practices to that framework. Secondly, the company has to be helped to draw up a map of possible risks related to the storing and use of personal data. Later, concrete policies have to be drafted, with special reference to consumer and employee data, and training programmes have to be established to make them known in the company. Finally, control and supervision mechanisms must be created to ensure that policies are complied with, and there must be correction mechanisms for when they are not. The success of these programmes requires the compromise of senior management and interdepartmental work teams.

**The law above all**
**Javier Ribas, Managing Director of e-business, Landwell-PwC**
The percentage of digitalised information as a whole in the company has tripled in the last ten years. Thus, accessibility and the opportunity of copying are easy. The Protection of Personal Data Act (La Ley Organica de Proteccion de Datos de Caracter Personal) states in this sense and especially through the Royal Decree 994/1999 11th of June, the obligation to establish security measures that guarantee the confidentiality of information with the object of preserving honour, personal and family privacy and the full exercise of personal rights in the face of any violation. Furthermore,
the aforementioned Royal Decree ensures the application of and compliance with the
security measures that the company must implement, establishing the obligation of
submitting their information systems to a biannual audit when dealing with data of a
high or medium level.
The obligations that the said guideline establishes are not only centred on technical
measures, but also impose confidentiality measures in the communication of data with
third parties.