Controlling communications: can this be the way to prevent terrorism?

Javier Ribas, Director-Partner Landwell-PwC
e-business Center PwC&IESE
28/07/05

The decision of the European Union to control all telephone communication registers and messages sent over the Internet is not something new. In fact, the Directive 2002/58/CE – relating to the treatment of personal data and protection of privacy in the electronic communications sector — that was approved three years ago already foresaw the possibility of member states forcing operators to keep data on traffic for a certain time in order to protect national security, defence, public security, or the prevention, investigation, uncovering and prosecution of offences.

In Spain, the 2002 law on “Servicios de la Sociedad de la Información (LSSI)” or “The Information Society Services” already contemplated this point. As in Europe, the maximum period to keep data in Spain is twelve months, although this point is still awaiting a regulation to cover it.

In reality, the agreement reached by the European ministers does not refer to the content of the communications, but to the traffic data. In other words, these measures let the authorities know the day and time in which a user made a communication with someone else and the length of that conversation. However, it is not possible to know the content of a message or a conversation.

Then, the remaining question is how is this control going to be useful? In the investigation of an already committed crime, it is highly possible that these measures help to clear up some doubts or questions: they can map out the geographic and temporary circumstances, the sort of communication made and even the people or group of people who may be involved.

Highlights

1. The agreement reached by the 25 member states of the European Union to control communications is based on a draft drawn up after the March 11th attacks in Madrid in 2004. Since then, the United Kingdom, France, Sweden and Ireland have been insisting on the approval of a law to compel operators to keep data on communications.

2. The terms of the directive have given rise to quite a lot of controversy. One of the reasons for this is the reluctance to infringe on privacy laws. The British Home Secretary, Charles Clare, has played down this point, claiming that civil liberties will not be affected in the same way by the retention of telecommunications data as, for example, by the authorization of torture.

3. The delay in the approval of this law can also be put down to the fear of imposing excessive costs on the industry. AOL, that currently keeps Internet data for up to three months, thinks that extending this practice to one year will give them an additional initial investment of at least 23 millions pounds (some 33 million euros) and add 8 million pounds (11.5 million euros) to their annual costs.

4. For AOL, it is too soon to know whether this cost will mean an increase in their customers’ bills. For its part, the Home Ministry stated that the government would subsidize part of the costs this measure would create for the operators. Although no figures were given, sources from the industry are talking about some 20 million pounds (almost 29 million euros).
However, in a preventive investigation, the difficulties are indeed much greater due to the enormous number of communications and the lack of knowledge of the details that could make up a threat.

On the other hand, the delinquents are hardly going to communicate with each other without protecting the content of the information. If they belong to an organization that has some sort of training, however little, they will avail of their own encoded or simulation techniques. Moreover, an order to attack can be sent without any encoding at all. It can be as simple as a literary quotation or a specific sentence that the terrorists are waiting to receive and which has already been decided on by all the parties involved.

Technology can also be used so that contact or communication does not take place. For instance, the issuer and receiver of a message may share the same e-mail account and contact each other through message drafts that one writes and the other reads and destroys. That is without taking into account the possibilities of the 2P2 networks that allow anonymous file sharing between Internet users.

From a legal point of view, this type of investigation raises problems on a personal and territorial scope. To start with, the data analysed inevitably belong to thousands of people who have no relationship with the origin of the investigation. Secondly, non-European infrastructures and operators intervene in these communications.

There seems to be a widespread feeling that these measures are necessary for the fight against international terrorism and that it is worthwhile giving up certain areas of privacy if this, in any way, contributes to feeling safer. In this case, privacy is preserved by the fact that the traffic data only inform about what could appear on an envelope or parcel sent through the post and by the requirements in place in order to ask for these data from the operator.

The question is to know if this tightening of control serves any purpose or if it is simply to appease the population. So far this type of measure has not been able to prevent terrorist threats from becoming a dramatic reality.