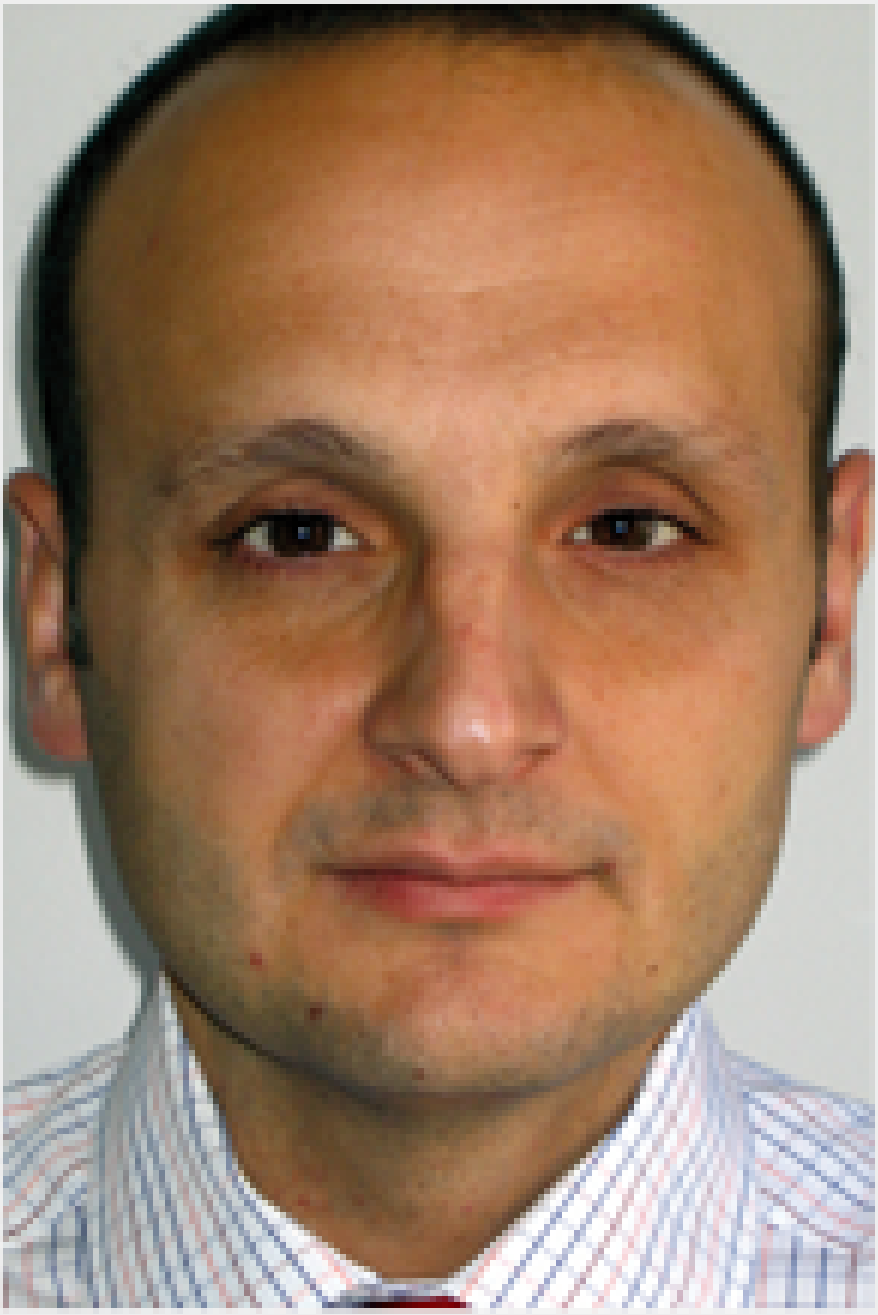
CYBER SECURITY: ADJUSTING TO A VIRTUAL REALITY

Posted on 02/09/2013



Category: Opinions

EU Data Protection Regulation currently under discussion could certainly help in preventing unreasonable practices affecting our privacy, says Manuel García Sánchez

These days, we are getting used to terms that, until recently, were confined to science fiction novels. 'Cyberspace', 'cyberwar' or 'cyber security' seemed to be the perfect environment for William Gibson's multi-award winning novel Neuromancer, for example, but not for our daily, 'not so modern nor exciting', life. Until today that is.

Governments are watching

Recent revelations on the nature and extent of some governmental surveillance programmes aimed at compiling, analysing and extracting relevant information from telecommunications services (including the Internet), have clearly shown how far they can go with currently available technology. With questionable legal coverage allowing extraterritorial application without adequate supervision, systems filled with data (mostly personal) have been plugged into core elements of the telecommunications networks to gather 'relevant' information. And these clearly seem to be excessive in relation to their intended purposes.

Furthermore, there have been increasing reports on a confusing web of interests surrounding those activities. Governments claim that they are only tracking foreigner's activities, while officials voice their opposition in countries whose secret services are actually benefiting from those systems and admitting using a 'broad' interpretation of national data protection laws. Meanwhile, telecommunications providers and big Internet companies deny their active involvement, voicing their tireless effort in protecting our privacy. In summary, there is general uncertainty in Europe and worldwide.

Data desires

There are simple reasons explaining such a big appetite for data. These days, we are continuously producing personal data – even when sleeping, unless you turn off your smartphone. And this data can be processed by using powerful systems that produce searchable information linked to individuals through multiple identifiers. And this is certainly covering almost every facet of our lives. Since most of the data is produced by private companies, public bodies need a legitimate legal reason or some kind of collaboration to access that data. But the implicit notion governing this behaviour is the so-called 'good to know' principle, which basically means that any single piece of information is or can be relevant to the public interest, so it is reasonable to put in place all the means necessary to gather such data. On the other hand, citizens have some fundamental rights.

Right to privacy

Article 8 of the European Convention on Human Rights enshrines the principle that everyone has the right to have their private and family life, home and correspondence respected. However, this general principle is touched on when the Convention adds that any interference with this right must be in accordance with the laws of a democratic society and needs to be necessary in order to protect a public interest, including those related to national security, public safety and the prevention of disorder or crime.

In legal terms, this means three things: There must be a valid legal rule that authorises the interference, citizens must have adequate access to the rule in question, and the citizen needs to be able to anticipate the circumstances in which the rule might be applied.

For its part, the notion of necessity in a democratic society implies that there is a pressing social need and, basically, that the interference is proportionate to the legitimate aim pursued. This involves what is called the 'proportionality test'. On the one hand, a measure will not be considered disproportionate if there are restrictions in its application and effect and, on the other, includes stringent safeguards so that the individual is not subject to arbitrary treatment.

That arrangement, as developed by the jurisprudence of the Court, entails the pre-eminence of the 'need to know' principle: that only personal data strictly necessary to achieve a legitimate purpose must be collected and processed, that only duly authorised personnel have access to it and that the whole process needs to be accountable through adequate controls and safeguards.

The solution

There is no need for profound legal analysis to conclude that, according to the information revealed by Edward Snowden and others, to some extent certain government programmes do not fit within the European legal framework.

Some EU governments are claiming that reinforcing the EU Data Protection Regulation currently under discussion could be the starting point for a solution. However, perhaps they should start by requesting that the European Commission introduce draft limits and safeguards that could prevent unreasonable practices affecting our privacy, as well as data protection rights when using the Internet, even if sourced from third countries.

When US President Barack Obama solemnly declared that we cannot have one hundred percent security and 100 percent privacy, others brought former US President Benjamin Franklin to the forefront: “Those who would give up essential liberty to purchase a little temporary safety, deserve neither liberty nor safety”. To be honest, I'm with Benjamin.