anno IV, n. 4, 2014
data di pubblicazione: 18 gennaio 2015

Editoriale

Threatening privacy in the Digital Age: towards a global legal framework

di Artemi Rallo Lombarte*

I

If there is one sector in which the need for a quick legal response is particularly important, it is new technologies. In this digital environment we are not dealing with a revolution, but with a constant, rapid evolution. While technology has clear and obvious advantages, its widespread use also presents challenges.

If a field were to be identified that would exemplify an area in which the law has difficulties in keeping up with reality, it would have to be the Internet. The concepts of sovereignty and territoriality, traditional limitations to the international application of laws, are being superseded every day by a reality in which interconnection and globalisation are no longer the exception but the norm against a background of vast

* Constitutional Law Professor at Jaume I University (Spain), Former Director of the Data Protection Spanish Agency.

telecommunications networks. In this respect, the profusion of international flows of data in the "information age" has highlighted the need for privacy legislation that is consistent at a global level.

For this reason, we need to reflect on the challenges that we face, on which agents are involved and how we can protect privacy appropriately.

We can identify three challenges in this digital environment: Firstly, the fast development of tools that allows mass use of information in a more perfect way and that offers a multitude of information-processing possibilities. This results in at least two knock-on effects:

a) The possibility to store, process and transfer large quantities of information, which has contributed to the high economic value of these services. On the Internet, personal information is a leading source of wealth. The most obvious example of this can be seen in advertising being individually tailored according to our browsing habits - behavioral advertising.

b) Omnipresence is another phenomenon in this field today, which can be seen the convergence of Internet services with mobile technology.

Another challenge that we face is the transnational nature of these services: companies operate in dozens of countries with different legal frameworks. At the same time, data are no longer kept in a specific location, but are rather spread among hundreds of servers around the world, as is the case with cloud computing.

Finally, but no less importantly, the Internet gives everyone a presence and a voice. The digital world has changed the role of individuals. People have also taken on an active role, which poses a challenge to current privacy regulations. People express themselves in blogs, microblogging networks or they share their experiences on social networks.

All of these factors, together with the increasing complexity of society, technology and business structures, lead us to consider the nature of the roles and responsibilities of users, business and governments.

The clearest example of the complexity in assigning responsibility can be found in online social networks. When publishing information on a social network, who is responsible?

The Article 29 Working Party (which integrates all European Data Protection Authorities) has looked into this situation and come up with a series of criteria. A paradoxical situation arises in which an individual becomes both the active and passive subject, making decisions on the personal information they process. This means such a person may be considered the processing controller, in the terminology of data protection legislation, subject to the same obligations as controllers.

It is important to clarify that data protection legislation excludes data processing carried out by people "*carrying out exclusively personal or domestic activities*".

The Article 29 Working Party has set out some situations in which processing by social network users may go above and beyond this domestic activity exception.

The first situation is when the user uses the social network as a collaboration platform for an association or company, for commercial, political or social purposes.

Another sign of the domestic scope being exceeded is when the user clearly has more contacts than could rationally be considered to be real contacts, for example when a user has willingly allowed a large number of contacts or a whole social network to access their data.

There is a third important case in which a user may be considered to be a data processing controller. This is in cases where processing of other people's data violates these third parties' rights. In other words, the domestic activity exception is also limited by the need to guarantee rights, particularly in relation to sensitive data.

When any of the aforementioned circumstances arise, individuals are obliged to offer certain security guarantees: to ensure the confidentiality of the information published, and to offer measures for users to exercise their data protection rights.

III

But businesses also play a fundamental role. The complexity of businesses that operate on a global scale and that outsource services must also be studied.

It is important to determine who is in control of processing the data (that is, who determines the purpose to which they will be put), as this helps to ensure greater effectiveness in compliance.

The tendency in data protection regulations is to combine proactive and reactive measures to ensure compliance (which may include self-regulation measures). Reactive measures are applied when have been unlawfully processed.

It is necessary to mention the principle of Accountability. This principle, which was included in the Organisation for Economic Cooperation and Development's privacy guidelines back in 1980, requires the processing controller to implement appropriate and effective measures to implement the principles and obligations of data protection.

This firstly involves demonstrating compliance externally and secondly an internal process to create control mechanisms

to ensure compliance. It must also be possible to demonstrate these when required to do so by the authorities.

Companies are responsible for respecting the privacy of their clients and users. For this reason, companies have been called on for some time now to take an active part in designing these services and platforms.

One example of this can be seen in Privacy Enhancing Technologies. The Data Protection Directive establishes the processing controller's obligation to put in place technical and organisational measures that will guarantee an appropriate degree of security. These Privacy Enhancing Technologies are technological measures aimed at protecting the right to privacy by deleting personal data or preventing data from being unnecessary processed. These systems have been supported by the European Commission.

Also of unquestionable importance is Privacy By Design, which requires privacy protection measures to be in place from the initial design phase of systems or services, thus guaranteeing the privacy and protection of personal data.

Within Privacy by Design, Privacy Impact Assessment methods have an ever greater presence. These are a way to determine the privacy, confidentiality and security risks associated with personal data processing. They also define measures to reduce and eliminate these risks.

IV

Finally, we must ask ourselves if existing data protection legislation is able to deal with these new challenges. Over the years, a series of legal instruments have been created to protect privacy: some of the most significant of these being Convention

108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, the OECD Guidelines on the Protection of Privacy and the APEC Privacy Framework. The United Nations also approved guidelines on computerised personal data files in 1990.

Data protection has achieved significant importance in Europe under the Treaty of Lisbon. The European Union Charter of Fundamental Rights and Article 16 of the Treaty on the Functioning of the European Union introduce a new legal basis for data protection, applicable to any kind of processing.

Personal data processing is also regulated by Directive 95/46/CE on Data Protection. This Directive is technologically neutral and provides a reference model for good practice at an international level. However, it is technologically obsolete. For this reason it is so relevant to revise this legal framework with the new European Data Protection Regulation that European institutions are closed to adopt.

The Article 29 Working Party has actively participated in the process to review this Directive. In its Opinion (WP168) of December 2009, it analysed the Directive and put forward a series of recommendations. The main message was that the principles of data protection are still valid, but they may benefit from a better application. The Working Party used this opportunity to:

- Clarify the application of some key regulations and principles of data protection (consent and transparency).
- Overhaul the framework to introduce additional principles (privacy by design and accountability).
- Make the system more efficient by modernising provisions by cutting red tape.

Outside the EU, there are different data protection regulations. Mexico is one of the latest countries to have adopted a new data protection law. Uruguay, Costa Rica, Morocco, Nicaragua, Dominican Republic, Peru and Russia have also adopted their own laws while others are working to develop new legislation on this issue.

But the territorial limitations of the current systems require us to reflect on the need for a comprehensive data protection framework, which will cover these new situations but also future situations as has been demonstrated by the ruling adopted on 13th may 2014 by the Court of Justice of the European Union on the "right to be forgotten".

The ongoing differences in terms of data protection, and especially the lack of guarantees in many countries, lead to reduced protection of individual rights. This harms the exchange of personal data and prevents a sufficient and effective level of data protection from becoming universal.

Legislation relating to the protection of privacy and personal data differs substantially from one State to another, to the point that there are still many legal systems in which these rights, considered as fundamental in a large part of the world, lack an appropriate framework of guarantees. The consequences are easy to understand: information is not uniformly protected, people find it increasingly difficult to assert their rights and data exchanges are therefore at risk – something that would not occur if a universally accepted set of rights, principles, obligations and procedures, applicable to all processing of personal data, were to exist.

Data Protection Authorities from around the world, which meet during the International Conference of Data Protection and Privacy, have in recent years expressed a constant concern about the problems stemming from the different protection

regimes existing in different geographical areas, including the fact that some countries or areas have no data protection or privacy regulation whatsoever.

V

This growing interest culminated in the 31st International Conference of Data Protection and Privacy, which approved in 2009 the Madrid Resolution on International Privacy Standards.

This Joint Proposal for Setting International Standards on Privacy was not an international agreement, nor a binding legal regulation. However, its value and relevance as a reference text comes from the fact that the international data protection community participated greatly in creating it, and it includes elements that are present in all data protection systems currently in force. This text was of course supported by all the Authorities participating at the International Conference.

This Joint Proposal aims,

- Firstly, to promote data protection and privacy rights internationally, providing a regulation model that guarantees a high level of protection. It was also designed in a way that meant it could be adopted in any country, with only minimal adaptations that may be required for the purposes of legal, social or economic requirements of each region.

- Secondly, to help ensure the fluid of personal data internationally. The fact that different national legislations currently exist side by side means that data transfers between countries in different geographical regions can require complex authorisation systems. The situation can be even more complex for multinational corporations, which have to abide by several different regulatory systems, depending on the countries where their various offices are based. This generates obstacles and

delays in international data flow, additional costs for companies and an imbalance in terms of competitiveness.

In this sense, the Joint Proposal for Setting Standards establishes a universal model for what can be considered to be an appropriate level of protection, and makes it possible to carry out data transfers with a minimal level of formalities between countries or entities with protection systems that are in line with this model.

The Proposal also incorporates principles, rights and concepts that are common to the main international instruments on data protection and privacy.

It is clear that the Internet's development is unstoppable, both in terms of technical quality and the evolution of user services and functions. Technology gives people power, and increases development possibilities. For this reason, it is essential that development is accompanied by rules that govern its proper use.

Regional legislation, including European legislation, may provide answers but, in practice, technology and globalisation oblige us to create standards that ensure a satisfactory level of protection worldwide.

Data protection will always be a "work in progress" that must keep pace with the new trends that are taking place continuously in the digital environment.