Conference on "The future of the regulation of personal data in Europe: A French-Italian dialogue"

Maison du Barreau

Paris, 24 April 2013

Giovanni BUTTARELLI

Assistant European Data Protection Supervisor

The protection of personal data is going through a historic phase.

In the political and institutional agenda of the European countries of the past 40 years, there have been important stages in the evolution of the way in which we strengthen the safeguards of personality rights.

However, never before has there been such a sensitive time.

The choices we are making now, this time mainly at European level rather than in each country in its own way, will have a profound and lasting impact on the way in which public institutions, large multinationals, small businesses and individual internet users will operate in the digital age.

It is true that this legislation will once again address only one aspect of the information society, personal data processing, which is neither the only nor the most important aspect.

It is also true, however, that no public or private organisation can pursue its goals without personal data.

In other words, data protection is cross-cutting, embracing almost any activity, including those of the police, judicial authorities and intelligence services.

If we analyse how the principles of lawfulness, fairness, necessity and proportionality must be respected in practice in these areas, or if we discuss how to ensure the right to be forgotten, how to reconcile freedom of the press and transparency with the right to confidentiality, we realise just how pervasive data protection is. It impacts on many other sectoral regulations, obliges us to rethink how a public authority or a business must abide by these sectoral rules which do not necessarily take account of data protection profiles.

Accordingly, although data protection arose in relation to the protection of fundamental rights and freedoms, especially those relating to the personality, it is becoming an integral and sometimes predominant part of the rules and practices of good administration, with a decisive influence on any core business activity. It also affects your business, as lawyers, attorneys, advisers and protagonists in civil, criminal, commercial and family law proceedings, as all of these activities involve collecting masses of personal information, sometimes out of necessity and some of it very sensitive data, sometimes incorrectly or invasively.

How, to what extent and for how long can personal data be lawfully collected in order better to defend a right in a court of law? What precautions need to be taken when such information is kept and circulated by a lawyer, private investigator, the prosecutor or the judge?

Sometimes, national primary or secondary legislation can give precise answers to these questions.

For example, since later today we are also due to compare the Italian and French data protection systems, I am proud to say that my country is probably the only one in which a flexible tool, such as a code of ethics promoted by law by the national data protection authority (your CNIL), and again by law is binding on all civil and criminal lawyers, and on private investigators, offers these players reasonable and specific directions on how to balance an effective defence against the protection of the rights of third parties regarding the collection, keeping and production in court of evidence.

But national legislation is not always able to give definite answers. At other times, therefore, you have to find your own answers on issues of certainty, when called upon to apply to your activities the principles of data protection that are perhaps of a general nature and do not set out best practices as you expect.

But let us return to my introductory statement. Why is this a historic phase? Why are we talking about the moment of truth for data protection?

These questions are easier to answer if we look back at the origins of this topic, which has seen several generations of standards.

In the 1970s, the first pioneering experiments (for example, in Sweden and the German Länder), were often based on mechanisms involving prohibition, prior authorisation for the processing of personal data, and public inventories of computerised databases which at the time were mostly large and under the control of a few entities that people found hard to trust. Indeed, people feared the emergence of large computers, their ability to store and process information to produce results that were inconceivable with paper-based systems. Data flows abroad were allowed only to countries, including European ones, that guaranteed equivalent data protection.

The first German law of 1977 and your law of 1978 were drafted as more evolved forms of the early experiences. Even at that stage, however, the law continued to provide for mechanisms which today seem outdated, such as prior notification of a public data-processing authority. The idea was to allow a preliminary examination by an independent authority, as if it were possible to control the main data-processing activities in advance.

In the years immediately following those measures, an attempt was made at international level to impose an initial level of uniformity in this field, through the Council of Europe Convention of 1981 (which is still a valid model today on account of its flexibility and technological neutrality, and has been ratified by 45 countries), and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

In the 1980s a second generation of laws began to emerge in several European countries. It was felt that more specific guidance was needed on how to regulate certain categories of personal data (those on health, or processed by the police, for example).

At this stage, experience gained over the years led to a more realistic and selective approach (such as simplified notification to the supervisory authority) because information systems were no longer concentrated in the hands of a few organisations, but were based on small and medium-sized computers used by a much wider range of

stakeholders. Each country followed its own path, however. In essence, until the late 1990s, the situation in Europe was very diverse, with regulatory systems differing widely from one country to another to the extent that they affected the free movement of goods, persons, services, capital and professions (there was the famous textbook case of Fiat SpA, in which the French branch could not initially send data to the Italian parent company because there was no data-protection law in Italy. The case was settled using contractual clauses that are now widely used to handle cross-border flows).

Finally came a third phase, which began in October 1998 when the deadline expired for transposing EU Directive No 95/46, and we embarked on a very slow path towards an initial level of harmonisation of the laws of the various European Community Member States.

Under the EU Directive of 1995 and the first daughter Directive on telecommunications in 1997 (97/66/EC), all European countries adopted a more structured law on the subject, as well as certain sectoral laws and secondary regulations; they tried to address the initial challenges of biometrics and genetics, e-government, technological development, and those of a world constantly moving towards ubiquitous computing, not only connected to but also monitored by the web, interacting with but also victims of the social networks.

In this new phase, we left behind the world of the first large 'mainframe' servers linked to a number of clients in small proprietary networks: although the digital divide still affects sizeable minorities, computing resources, technology education and the hazards of internet browsing are part of all our everyday lives, especially for the younger generation. Information is no longer stored in large containers that the legislator has to regulate the use of and to which a privileged few have access, but is gathered, shared and updated in real time by a great many people.

At the same time, millions of internet users are increasingly beginning to be monitored in a far from transparent manner about their tastes, preferences and habits.

We call them 'personal' data because they are ours. They are a projection of our own person; we should be the ones to decide, at least in some cases, who can use them and for what purposes. We should be able easily to identify all those who use them, and be able to exercise our rights effectively when they are violated.

Yet internet users have become the subject of intense and repeated profiling online by others who, even if they do not use our names directly, carefully monitor our behaviour by analysing our traces and the 'pieces' of our identity we leave on the web (such as our IP address). We are broken down, classified and catalogued in real time in thousands of ways that we are totally oblivious to. The more recent and more analytical the data we leave on the web, the greater their commercial value. We are constantly asked to provide information because it helps to surf the net, but we are in fact being monetised behind our backs. Unknown people are always creating our identities, several times over, which may not correspond at all to the way we live, even though they have been created on a sophisticated computer.

You may wonder why I have indulged in this long historical digression. I think it may help us to understand what it is important to protect in the digital age and what choices the European legislator needs to make today.

In future, society will certainly tend to restrict our privacy. In some respects, it is reasonable for that to happen, especially if we expect to manage our entire private life through a tablet or smartphone, reading a newspaper online, connecting to the bank, applying for and obtaining administrative certificates, airline reservations and health appointments, socialising with many other people through blogs, free calling systems and social networks.

The solution is not, therefore, to reduce the flows of information, which are now growing inexorably all over the planet.

The restriction of our privacy will become increasingly inevitable in a world where, in addition to video cameras, satellites, and GPS systems, to save money and for ecological reasons, we use 'smart meters' (that measure and analyse our domestic consumption) or intelligent cars (that warn us of everything that is happening around us in terms of hazards, traffic, theft and accidents, but also track and analyse our movements).

Furthermore, our fragile democracies continue to be exposed to risks of security, and petty and major crime. The effectiveness of the police, security services and the judiciary relies once again on obtaining reliable information in real time. Privacy and security are not incompatible, but large databases and border controls clearly pose a number of challenges.

We are paying a price for all of this, in terms of personality rights and also freedom of movement, which from a modern perspective means not only freedom of physical movement, but also freedom of movement on the web without being forced to leave an unreasonable number of traces of our movements.

This price must be offset by a major improvement in our ability to control the data flows about us, first of all by knowing who has information about us and what it is used for. Being informed means being able to make free choices, especially when we have to make a conscious decision to give up important areas of our private lives.

It is for all these reasons that, more than thirty years after the adoption of the Strasbourg Convention, and almost twenty years after the first European Directive entered into force, we want to take a step forward towards modern rules that are more harmonised, ambitious and future-proof.

Not only have the technologies changed, as they are constantly evolving and detailed rules cannot keep pace with them.

The Lisbon Treaty has changed the architecture of rights in Europe.

The Charter of Fundamental Rights formally recognises the fundamental right to data protection, in a distinct and independent provision on privacy. What does this mean?

It means that our right covers the way in which a public or private entity manages our information, ensures transparency, implements security measures, identifies responsibilities within its organisation and with external entities working with it, where, for example, it offers a cloud computing service, keeps the information for a reasonable period of time, etc. The Charter classifies this as a fundamental right.

This right exists regardless of any breach of these rules on the processing of personal data that may also cause moral or material damage. This fundamental right can be enforced in a court of law, quite apart from any more detailed rules on the matter, or the fact that the processing of data also leads to an unwarranted interference in our privacy.

In other words, compliance with the rules of the game in terms of lawful and fair processing of data is our right in itself, even if we do not suffer any specific damage.

The focus will increasingly shift from the protection of the static right (in which we are merely asked bureaucratically for prior consent to the processing of our personal data) towards dynamic protection allowing us to check exactly how our data are being processed, even if this sometimes happens after the event.

Prior, free and informed consent will not disappear, especially for online monitoring and profiling, but it will not always have the central importance it had in the first-generation laws.

The Treaties on European Union and on the Functioning of the European Union clearly state that uniform European rules in this area are now not just an option but an obligation in the EU. The Treaties take over, if only implicitly, the case law of the European Court of Human Rights in relation to Article 8 of the Convention on Human Rights, whereby the States parties to the Convention have obligations which are both 'negative' (in the sense that States must not interfere disproportionately in people's private lives) and 'positive' (in the sense that States must take action by introducing the necessary measures, including legislative measures, to ensure that people enjoy a reasonable level of privacy and that other public or private entities do not interfere unduly in personal privacy).

The whole world (not just the United States of America where the administration is seeking to submit to Congress a Bill of Rights that could foster interoperability of principles at international level) is closely following the ongoing debate in the European Parliament and the Council of the European Union on the package presented by the European Commission in January of last year, which comprises a proposal for a horizontal regulation and a proposal for a directive on police and judicial activities.

The rules that we manage to introduce, and which should be applicable from about 2016, will have to try and overcome the fragmented framework brought about by the 27 laws in force in the EU countries. We will aim to take the best that exists in some countries and put an end to the less positive experiences. We should try to preserve the specific cultural features that exist in some countries. And, most importantly, we must strive to consider the citizen's viewpoint, to make sure that while data processing is increasingly globalised throughout the world, citizens still have a significant point of reference in the national authorities.

Now is not the time to reinvent data protection. We need to make its principles more effective, and integrate them with new principles suited to the digital age, such as privacy by design, privacy by default, and accountability. We need rules that are technologically neutral, that can withstand rapid obsolescence at least until 2025.