Madrid, July 2014

Some Reflections on National Legislation on the Protection of Personal Data

Countries that have, or have adhered to, codes for the protection of personal data, are generally of the opinion that in a globalized and interconnected world a high standard of private data protection offers competitive advantages. Business transactions in an increasingly digital world benefit if both cyber security and the protection of sensitive data are guaranteed: they are the prerequisites of business confidence, and cyber confidence is a precious asset. In addition, the protection of privacy and person-related data are also a requirement of human rights, as proclaimed in the Universal Conventions and also the European Human Rights Conventions.

If the same or comparable standards and levels of protection prevail across frontiers, these benefits are enhanced. If, on the other hand, there are substantial cleavages between countries that nevertheless maintain intensive business relations, transborder data flows are more complex, and need additional instruments providing data protection at the desired level. Thus, the considerable differences between European countries, especially the European Union with its elaborate data protection norm systems and the United States – where commensurate legislation is lacking – have required the Safe Harbor treaty, an equalizing device that with the advent of Big Data and the recent massive infringements of data security by US agencies – but by no means only they – has increasingly shown is inadequacy, has come under attack, and probably needs to be refounded.

There is thus an important reason for countries that wish to endow themselves with data protection laws to incorporate themselves into,

or approximate, data protection systems already existing and applied in larger geographical contexts. The larger the area of uniform high data protection levels, the better for business, and the easier is transfrontier data use. In this connection, the OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data, recently amended by OECD Council Decision, C(2013)79, and the Council of Europe European Data Protection Convention (Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data, CETS Nº 108) deserve attention. The OECD Guidelines are recommendatory, but the Council of Europe Convention is a Treaty, already in force for most of the CoE member countries, and some non-members. Perhaps the most relevant regulatory systems can be found in the European Union, where the Directive 95/46/CE of 1995 is in force and has been transposed by all member countries; it is also binding on the new members that have joined the Union since the adoption of the 1995 document. There is now in the EU member countries compatible and similar legislation maintaining a high level of data protection.

Before addressing the most recent attempts of the European Union since 2010 to revise and update the extant legislation, and to adjust it to the current developments (emergence of social networks, exponential growth of a digital society with unlimited connectivities, permeating all walks of life) a reminder as to the extent of the protection is in order. All documents cited refer to personal, person-related data and thus do not cover business information or other non-person data. They thus do not protect against data theft and espionage in a broader sense. Espionage is not sanctioned by international law. Spies –whether they try to collect personal or industrial data - are not likely to appear before an international court of justice; the only protective device being the Vienna Convention on

diplomatic immunities, protecting the integrity of embassies and diplomatic baggage.

However, there are other legal instruments. In most digitally important countries the Budapest Convention on Cybercrime is in force and has informed national legislation; alternatively, countries that have not signed and ratified the Convention (nearly 50 countries have) have adopted very similar penal laws and law enforcements modes themselves. Any interference with the functioning or contents of a digital device or net structure is a cyber crime, and in countries that follow the *ex officio* principle in law enforcement, the state prosecution authorities have to act. Espionage and violation of privacy relating to non-personal data, especially industrial espionage, is practiced under the menace of penal sanction and civil liabilities for damage.

Reverting to the most topical European Union data protection move, it is important to study document COM(2012)11, the "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)". With its almost 150 pages, it is probably the most comprehensive legislative text on the subject, a true codification. Several features have to be noted.

In the first place, and distinct from the 1995 EU data protection directive, the proposal is for a regulation. Under EU law, regulations become immediate law in all member states, while a directive is binding only in its general policy lines, and has to be transposed individually in each member country. The new proposal will thus create a uniform corpus of data protection law for the entire Union.

And beyond. Past experience, also in other legal fields, has shown that European legislation, involving 28 highly industrialized countries

with an advanced digital culture – and also with a very complete legislative process - , has a model function for many other countries considering legislative action. If the principle established above, that data protection is more effective if the same standards prevail among many members of the international community, a country introducing new legislation in this field might well take the Regulation as a guide post.

The Resolution incorporates the principles of the 1995 Directive, introducing more precision and rigor. It also establishes the right of individuals to demand elimination of personal data (the "right to forget"). The procedural provisions are more elaborate, and the sanction regime is more explicit. The Regulation foresees penalties that can attain the level of millions of euros in case of breach of the law.

The legislative process has not been concluded. The Ministers forming the Council of Ministers are still bending over the text, and there are many amendments – some say, in the hundreds – to be considered before a final text will emerge. The process will be concluded by end of 2014 at earliest. But the main lines of the Regulation and the necessity to have such a codification are agreed.

Henning Wegener