Foreword

Our initiative to make a collective work on privacy and personal data protection law started to take shape not only through the talks and debates we had, but also through the innumerable exchange of e-mails, and, most importantly, through the positive answers we started to receive from the authors who take part in this project.

The aims of this book are the following : (1) to promote the study and development of privacy and data protection law ; and (2) to analyse new trends in this field of law from a national, international and comparative perspective. Nevertheless, this publication is not sufficient for the achievement of these aims, since the active participation of the reader will be necessary to fulfil them.

The idea to promote the study and development of the subject matter has its origin in the observation of a growing problem in the application and enforcement of the law. We are all « data subjects », our personal data is routinely processed both in the public and private sector, sometimes with our knowledge, sometimes not...« Data controllers » also experience a growing number of questions to solve, such as : their obligations and liability *vis-à-vis* the data subjects, the limits to their processing activities, the possibility or not to share the data (for instance, requested by the national State or a third country for the fight against crime), the procedures to grant the data subject their rights (such as information, access, rectification, etc.).

A recent case being heard before the European Court of Justice illustrates the increasing risks derived from personal data processing (and retention, in this example) (1). *« La présente affaire illustre le fait que le stockage de données à certaines fins suscite l'envie de les utiliser à plus large échelle »* (2). With these words, Advocate General Juliane Kokott started a very well reasoned analysis of the data protection law implications of the potential use in civil litigation cases of Internet traffic data that have been stored by ISPs for the fight against « serious crimes ». This is clear evidence of the dangers that could derive from the non-respect of the purpose limitation principle, one of the core foundations of data protection legislation.

---

(1) Case C-275/06, Productores de Música de España (Promusicae) vs. de España SAU.

(2) Conclusions de l'Avocat Général M^me^ Juliane Kokott, présentées le 18 juillet 2007, Affaire C-275/06, Productores de Música de España (Promusicae) contre Telefónica de España SAU, available at : http://curia.europa.eu/jurisp/cgibin/form.pl?lang=en&Submit=Rechercher&alldocs=alldocs&docj=docj&docop=docop&docor=docor&docjo=docjo&numaff=C275/06&datefs=&datefe=&nomusuel=&domaine=&mots=&resmax=100.

The study and development of the field should take into account the characteristics of emerging new technologies. Recourse to IT specialists is needed in order to understand the different applications used for the processing of personal data, and to attribute the relevant legal rules and principles to those operations. Conversely, IT specialists should also be aware of the legal rules, to design and implement the architecture in a « privacy-friendly » way.

Notwithstanding, new technologies are deployed, in many cases, without properly conducting a privacy risk evaluation. RFID could be an example of that (3). Yet, this reality is, in most cases, inevitable. Technology moves ahead faster than law. However, one of the principles described in Recital 2 of Directive 95/46/EC (4) has to be kept in mind, as a guiding value : « Whereas data-processing systems are designed to serve man ; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals... ». That is a clear invitation for standardisation institutions and software companies to enter into a discussion with all other stakeholders in order to define privacy compliant technologies and to more strictly apply the principle of precaution (5).

---

(3) Radio-frequency identification (RFID) is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders. « New applications for Radio Frequency Identification (RFID) technology include embedding transponders in everyday things used by individuals, such as books, payment cards, and personal identification. While RFID technology has existed for decades, these new applications carry with them substantial new privacy and security risks for individuals. These risks arise due to a combination of aspects involved in these applications: 1) The transponders are permanently embedded in objects individuals commonly carry with them 2) Static data linkable to an individual is stored on these transponders 3) The objects these transponders are embedded in are used in public places where individuals have limited control over who can access data on the transponder. », Marci MEINGAST, Jennifer KING and Deirdre MULLIGAN, « Embedded RFID and Everyday Things : A Case Study of the Security and Privacy Risks of the U:S : e-Passport », available at :http://www.truststc.org/pubs/157/Meingast_king_King_Mullighan_RFI2007_Final.pdf .

(4)Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Official Journal L 281, 23/11/1995, p. 31-50. See also : Article 29 Working Party, Working document on data protection issues related to RFID technology 19 2005 WP 105, available at : http://www.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp106_fr.pdf.

(5) See Article 3 of Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity, Official Journal L 091, 07/04/1999, p. 10-28, which reads as follows : « 3. In accordance with the procedure laid down in Article 15, the Commission may decide that apparatus within certain equipment classes or apparatus of particular types shall be so constructed that: (...)(c) it incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected; (...) ».

The analysis of trends in the data protection world must be conducted from the point of view of national, international and comparative law. This present text certainly cannot be considered as a work of comparative law, but through its methodology, it intends to bring to the reader the analysis of the same subject in different geographic spaces. Thuerefore the reader may be able to compare them. The international approach is necessary because global data transfers have grown exponentially and are no longer reserved to private activities. One can attest an increasing use of this kind of transfer at the request of public bodies. The processing of personal data is more and more transnational in its nature so it affects at the same time numerous individuals across different jurisdictions, which are subject to diverse legal regimes. Examples abound and it is easy to locate some clear-cut cases like the PNR case (6) or the Swift case (7). In addition, we believe that every geographical space can be nurtured by the experience of the others jurisdictions

We do not intend to exhaust the analysis of the data protection field by the topics we have selected. However, we believe that the topics analysed in this book are some of those that deserve more attention, from a conceptual point of view, such as the case of fundamental rights or sensitive data ; from a practical point of view, like the case of credit reporting or labour data ; or from an international standpoint, like electronic communications, international transfers of personal data or the fight against crime. For the selection of these subjects it has been very helpful to have the experience of the *Centre de*

(6) This case deals with the processing and transfer of passenger name record (PNR) data by air carriers (from the EU) to the United States Department of Homeland Security. The European Court of Justice has annulled the first Agreement signed in this arena (cases C-317/04 and C-318/04). A new Agreement has been signed recently. See :http://ec.europa.eu/justice_home/fsj/privacy/thirdcountries/_en.htm.

(7)« SWIFT is a worldwide financial messaging service which facilitates international money transfers. SWIFT stores all messages for a period of 124 days at two operation centres, one within the EU and one in the USA – a form of data processing referred to in this document as « mirroring ». The messages contain personal data such as the names of the payer and payee. After the terrorist attacks of September 2001, the United States Department of the Treasury (« UST ») issued subpoenas requiring s SWIFT to provide access to message information held in the USA. SWIFT complied with the subpoenas, although certain limitations to UST access were negotiated. The matter became public as a result of press coverage in late June and early July 2006. As a Belgian based cooperative, SWIFT is subject to Belgian data protection law implementing the EU Data Protection Directive 95/46/EC (« the Directive »). Financial institutions in the EU using SWIFT's service are subject to national data protection laws implementing the Directive in the Member State in which they are established. », Article 29 Working Party, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), 22 November 2006, WP128. In the US, two banking customers sued SWIFT on invasion-of-privacy grounds. The case is presently pending before a federal court in Alexandria (State of Virginia). On this case, read Eric LICHTBAU's article published in the International Herald Tribune : («U.S. may invoke 'state secrets' to squelch suit against SWIFT », 31 August 2007, available at :http://www.iht.com/articles/2007/08/31/America/swift.php .

Recherches Informatique et Droit (8), University of Namur, Belgium, in the field of academic research and the activities of the Habeas Data Forum (9), Argentina, an online community where data protection is discussed on a daily basis.

We would like to express our most sincere gratitude to the contributors, who are very well known and respected data protection specialists, for their enthusiastic attitude towards this book. We would like to thank them all for having had the necessary patience and flexibility that the preparation of this collective work has needed, particularly in order to adapt the time schedules of each of them to the general planning of the book. We would also like thank Madame Nelly Somme-Marchal for having done the formatting of this book, as well as Mr John Burns for having proofread those papers written by non-native English authors and Madame Jacqueline Spineux for having proofread those papers written in French.

Finally, as the topics developed, the geographical areas included are seen to be limited in relation to the global dimension of the subject matter. Data streams with Latin America, Africa and Asia urge the study of the data protection systems of those areas. However, this would have been an effort that would have exceeded our current possibilities. Nevertheless, we consider the geographical area enlargement as a challenge for future studies as a contribution towards the will to strengthen international recognition of the universal character of data protection principles, as expressed by the Data Protection and Privacy Commissioners in their Montreux Declaration (10).

2008

María Verónica PÉREZ ASINARI,
Brussels, Belgium.
Pablo Andrés PALAZZI,
Buenos Aires, Argentina.
Yves POULLET,
Namur, Belgium

(8) http://www.crid.be

(9) http://www.habeasdata.org

(10) 27th International Conference (14-16 September 2005), Montreux Declaration , «The protection of personal data and privacy in a globalised world : a unieversal right respecting diversities », available at:http://www.privacyconference2006.org/file.admin/PDF/montreux_declaration_e.pdf