Data Protection, Information Privacy, and Security Measures: an essay on the European and the Italian Legal Frameworks

Versione 1.0 – December 2008

Paolo Guarda

Data Protection, Information Privacy, and Security Measures: an Essay on the European and the Italian Legal Frameworks

Versione 1.0 December 2008

Paolo Guarda[*]

1. Introduction

The growing interest in the instruments provided by the digital technology, and by Internet in particular, assumes considerable value by an economic and a sociological point of view. The future and the success of the diffusion of e-commerce in the European market will be determined by belief in or distrust of the Net by its users. There is a widespread fear of the new; psychological elements, such as the mistrust and the lack of confidence, represent serious obstacles to the approach to the electronic markets by the new users[1].

The advent of computers required the adoption of specific means to safeguard personal information. The problem was to prevent the risks coming from the ease of collating and processing citizen's personal data. The digital revolution requires even the change of the notion itself, as well as of the contents, of the right to privacy[2].

The regulation of the relationships among the users of the electronic networks is a pivotal point for a well-balanced development of this important business sector. We have to bear in mind that Internet has not only a visible dimension, but also an invisible

* Paper already published in *Ciberspaizo e dir.*, 2008, 65-92. Version 1.0 – December 2008 in pdf -

[1] Since in the digital environment the buyer cannot have a direct contact to the product, it is of main significance to create the needed confidence in the good quality and the trustworthiness of the commercial activity carried out on Internet.

[2] See G. PASCUZZI, *Il diritto dell'era digitale*, 2nd ed., Bologna, 2006.

one. There are many kinds of data processing that occur without the knowledge of people: cookies, web-bugs, spywares, Persistence Internet Explorer, adwares, etc.[3].

The ease of collating and processing personal data mirrors the difficulty to find out legal means to guarantee effectively privacy on the net.

The studies of consumer behaviour in the digital market are still at a preliminary stage. Several theories lack empirical verification and firms change their strategy too quickly: assessing the consumers' reaction becomes very difficult. At a first glance, the adjustment of information research strategy turns out to be much more difficult than expected. In this scenario we could predict heated competition among firms and significant benefits for consumers. At the moment, the development of digital markets denies such expectations.

The users are overcome by an uncheckable flow of information: the risk is that they will suffer an information asymmetry corresponding to the situation that characterized the traditional markets.

The digital technologies, conceived to change the relationship among firms and consumers, do not guarantee an automatic increase in the welfare of both the categories. It is essential to identify the forms of intervention that give consumers the relevant information in order to permit them to choose appropriately.

There are two levels of intervention to solve the problem: privacy law and incorporation of privacy values and principles in the digital architectures. We must avoid the false belief that they are alternative means. Some years ago we have thought that law could represent an adequate way of approaching to the problem. Now it is obvious that the digital markets are looking for a delicate balance between law and digital technology.

But there are also other issues to talk about. We need focusing our attention on the relationship between two pivotal, and generally quite popular, concepts of the digital age law: privacy and security[4].

These concepts are characterized by an ambiguous relationship since the point of reference is unclear.

According to some authors, privacy can assume different definitions depending on which of the several dimensions it is applied to[5]. There is an informational dimension of privacy, referring to the activities related to intellectual consumption, in which there should be freedom of thought. But there is also a spatial dimension, that

[3] Careful attention has also to be given to consumers' confidence on the new technologies, in particular in e-commerce: consumers who lack confidence in functioning of the market and the protection on their interests at home and abroad will be even more reluctant to make major purchases outside their own country. The solutions to the problems have to be found either in the regulatory instruments, or in privacy standards to be adopted and incorporated in the new technologies.

[4] As regarding the relationship between privacy and security after the Twin Towers attacks, see P. GUARDA, *Agenti software e sicurezza informatica*, in G. PASCUZZI (edited by), *Diritto e tecnologie evolute del commercio elettronico*, Padova, 2004, 315.

[5] See J. E. COHEN, *Drm and Privacy*, 18 *Berk. L. J.* 575, 576 ss. (2003); R. CASO, *Digital Rights Management*, Padova, 2004, 103 ss. (available on the Web site: http://www.jus.unitn.it/users/caso/pubblicazioni/drm/home.asp?cod=roberto.caso). The debate on the several privacy dimensions is due to a research trend dedicated to the conceptualizing of privacy (see J. E. COHEN, *Drm and Privacy*, 18 *Berk. L. J.* 575 (2003)).

represents the zone of freedom traditionally enjoyed by activities in private spaces. Adopting a more general point of view, we face also the dichotomy between privacy intended as the right to be let alone. We refer both to the famous essay by Warren and Brandeis, which we are going to discuss shortly, and to privacy, meant as the control over our flow of data, which is typical in the digital age.

Furthermore, the widespread diffusion of computers carries also an increasing anxiety on several levels: the awareness that personal data of people could be used in malicious and harmful ways[6]; the ever-growing dependence of advanced societies upon computer and computer systems; the vulnerability of these systems; and the violations of them, which has already caused several economic damages and frustrated the users' reliance. Then we talk about security anxiety[7]. The same concept of security could be used either to refer to data protection of confidential information or to identify the public interest, in order to guarantee and justify a less cogent defence of citizens privacy (for instance, on the national security field). In this case, security becomes a way to unloosen the safeguard to reduce the protection of personal data and to violate privacy[8].

In the Part II of this essay we will briefly describe the starting point of the right to privacy and we will provide the main framework of European regulation on this matter. The Part III is dedicated to the analysis of security and data protection in the Italian legal system. Last but not least, in the Part IV we will sketch some considerations regarding standards, sources of law, and new technologies.

2. Privacy, Data Protection, and the European Union Law

The story of the "right to privacy" starts at the end of the eighteenth century. In the 1890 Warren and Brandeis published in the Harvard Law Review an essay titled "The Right to Privacy" defining this new right as "the right to be let alone"[9].

The idea to write the paper was due to a news item as stupid as popular in newspapers and magazines: Warren, a young and talented lawyer in Boston, gets married with the daughter of a famous and rich politician and changes his style starting

[6] See Trib. Orvieto, November, 25, 2002, in G. PASCUZZI (edited by), *Lex Aquilia. Giornale didattico e selezione di giurisprudenza sull'illecito extracontrattuale*, Bologna, 2005; Trib. Biella, March, 29, 2003, in *Dir. informazione e informatica*, 2003, 538, regarding the publication on a newspaper of a picture without the consent of the person portrayed on it.

[7] See PASCUZZI, *Il diritto dell'era digitale*, cit., 51.

[8] The terrorist attacks of September 11th gave rise to an increase of intelligence activities and interference by the intelligence agencies into the people life. See GUARDA, *Agenti software e sicurezza informatica*, cit..

[9] S. D. WARREN, L. D. BRANDEIS, *The Right to Privacy*, 4 *Harv. L. Rev*. 193 (1890); see also AA.VV., *Symposium: The Right to Privacy One Hundred Years Later*, 41 *Case W. Res*. 643 (1991). The topic was discussed by chance by T. COOLEY, *A Treatise on the Law of Torts or the Wrongs which Arise Indipendent of Contract*, Chicago, Ill., 1888, as regarding the tort system. To tell the truth, some comparative researches questioned this argument and claims that the term "privacy" started off in the English legal dictionary and for the first time in the case *Prince Albert v. Strange* (1849). In the civil law family, the first case of use of "privacy" dates back to the German legal system by Kohler (*Das Autorrecht*) as cited by M. BESSONE, *Danno ingiusto e norme di création prétorienne: l'esperienza francese del diritto all'intimità della vita privata*, in *Nuovi saggi di diritto civile*, Milano, 1980, 169. On the contrary other scholars refer to R. STEPHEN, *Liberty, Equality, Fraternity*, published in 1873.

to live a fashionable way. Obviously this draws the attention of the media. Warren gets upset because of the "cost of the success": he decides to face the problem with his own tools, the pen and the legal background, and contacts his former colleague Brandeis. They write the essay that will become the milestone of any following paper, and contributions on the topic of privacy. Then, we have the first definition of privacy: the individual has the *right to be let alone*!

The US legal system was the first to elaborate on the right to privacy: it surfaced and developed by means of several cases and finally came to be codified in statutory rules.

The right to privacy struck in the Italian legal landscape after a delay of more than half a century. The first cases regarded the diffusion of facts concerning the private life of famous people in the media or movie plots[10].

In the first cases, the Italian Corte di Cassazione denied the right on subject and established that it was not part of our legal system (see among others the case regarding the tenor Caruso)[11].

Only in 1975 the Corte di Cassazione recognized the existence of the right to privacy. In the decision of May 27, 1975, n. 2129, the Supreme Court said that the circulation of false information, not relevant for the public opinion, constitutes an injury to the privacy of a person (the case was about pictures that portrayed the ex-empress Soraya Esfandiari with a man inside her house)[12].

Again, in this period, the right to privacy means "the right to be let alone".

The story of the right to privacy continues and the new change is due to the technology development. There is a complex relationship between the history of ideas and technological change. A rather deterministic view perceives technological changes as provoking economic changes, thereby transforming social institutions. But the relationship between technology and ideas also acts in reverse. In other words, technology not only affects new paradigms but also assumes, reflects, and serves these paradigms.

The final acknowledgment of the privacy in the Italian legal system occurred at the same time with the beginning of widespread distribution of personal computers[13].

---

[10] As regarding to the cases development, see PASCUZZI, *Il diritto dell'era digitale*, cit., 40 ff.; PARDOLESI (edited by), *Diritto alla riservatezza e circolazione dei dati personali*, cit., 14 ff..

[11] In *Foro it.*, 1957, I, 4. As regarding the doctrinal debite see *ex plurimis* G. PUGLIESE, *Il diritto alla riservatezza nel quadro dei diritti della personalità*, in *Riv. dir. civ.*, 1963, I, 605; B. FRANCESCHELLI, *Il diritto alla riservatezza*, Napoli, 1960; F. CARNELUTTI, *A proposito della libertà di pensiero*, in *Foro it.*, 1955, IV, 143; ID., *Diritto alla vita privata*, in *Riv. trim. dir. pubbl.*, 1955, 3; G. PUGLIESE, *Il preteso diritto alla riservatezza e le indiscrezioni cinematografiche*, in *Foro it.*, 1954, I, 116.

[12] In *Foro it.*, 1976, I, 2895. For closer analysis, see R. TOMMASINI, *Osservazioni in tema di diritto alla privacy*, in *Dir. fam. e pers.*, 1976, 242; A. PIZZORUSSO, *Sul diritto alla riservatezza nella Costituzione Italiana*, in *Prassi e Teoria*, 1976, 29; T. AULETTA, *Riservatezza e tutela della personalità*, Milano, 1978.

[13] The temporal subdivision has been taken by PASCUZZI, *Il diritto dell'era digitale*, cit., 43 ff.. For closet analysis, see also S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973; R. FRANK, *Tutela della riservatezza e sviluppo tecnologico*, *in Giust. civ.*, 1984, IV, 26; E. ROPPO, *Informatica, tutela della privacy delle persone*, Padova, 1984; A. BESSONE, G. GIACOBBE (edited by), *Il diritto alla riservatezza in Italia e Francia*, Padova, 1988; A. SCALISI, *Il valore della persona umana nel sistema e i nuovi diritti della personalità*, Milano, 1990; B. FERRI, *Diritto all'informazione e diritto*

We can divide the digital development in three periods. The first one occurred with Seventies of twentieth-century and it is characterized by the presence of few big computers due to their very expensive cost - only public administrations could afford these kind of machines. During the Eighties we have another stage: the computers are less expensive and less voluminous and many companies could get and use them. The final step refers to the period during the Nineties, when computers are much cheaper and can be found in all private homes.

Around the same time, in Europe we had a proliferation of statutes enacted with the intention of regulating the computer processing of personal data. These rules are affected by the development of the digital revolution, and are referred to as first, second, and third generation acts[14].

We have the first cases of legal intervention in West Germany: the statutes of Assia (October, 7, 1970) and Bavaria (October, 12, 1970), followed by a federal statute of 1977 on data protection (*Bundesdatenschutzgesetez, Bdsg*). By 1981, in all the German Länders we find specific statutes on data protection.

Then we have statutes in Sweden (1973)[15], France (1978)[16], Luxembourg (1979), Denmark (1979), Austria (1980), Norway (1980), Icelands (1982), Great Britain (1984)[17], Finland (1988), The Netherlands (1990), Portugal (1991), Spain (1993)[18], Belgium (1993), and Switzerland (1993). Furthermore Spain, Portugal, Austria, the Netherlands, Germany and Greece have amended their own Constitution to include privacy clauses.

---

all'oblio, in *Riv. dic. civ*., 1990, I, 801; S. RODOTÀ, *Privacy e costruzione della sfera privata*, in *Politica del diritto*, 1991, 521.

[14] For a chronological mapping, see PARDOLESI (edited by), *Diritto alla riservatezza e circolazione dei dati personali*, cit., 32; M. G. LOSANO, *Il diritto pubblico dell'informatica*, Torino, 1986, 54; E. GIANNANTONIO, M. G. LOSANO, V. ZENO-ZENCOVICH, *La tutela dei dati personali. Commentario alla Legge 675/1996*, Padova, 1997, 24.

[15] Statute May, 11, 1973 (Data Lag).

[16] Loi n. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, amended many times (the last one by Loi n. 2004-64 du 23 janvier 2006). This statute established the Commission national de l'informatique et des libertés with monitorino function on the enforcment of the regulation. See L. GUERRINI, *Prime informazioni in margine alla nuova legge francese sulla protezione dei dati personali*, in *Dir. informazione e informatica*, 2004, 645; M. DECKER, *Aspects internes et internationaux de la protection de la vie privée en droits francais, allemand et anglais*, Aix-en-Provence, 2001, 85; P. CENDON, *Profili della tutela della vita privata in Francia*, in *Riv. dir. civ*., 1982, I, 76. The French legislator amended in 1970 the art. 9 of *Code Civil*, recognizing explicitely the "*droit a la vie privée*".

[17] In 1984 the Great BritainNel modified the Data Protection Act in order to harmonize it with the European Directive. See P. CAREY, *Data protection: a practical guide to UK and EU law*, New York, 2004; J. MCDERMOTT, *Privacy: An Overview of Recent English Law Developments*, 3 *Tolley's Communications Law* 163 (1998); S. CHALTON, S. GASKILL, *Data Protection Law*, London, 1988.

[18] See T. E. FROSINI, *La nuova legge spagnola sui dati personali*, *id*., 2000, 769; M. G. LOSANO, *La legge spagnola sulla protezione dei dati personali*, in *Dir. informazione e informatica*, 1993, 867; O. ESTADELLA-YUSTE, *Spain's Data Protection Act Enters into Force*, 23 *Privacy Laws and Business* 2 (1993).

The Italian statute of December, 31, 1996, n. 675 ("Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali") represents one of the last legislative interventions on privacy in Europe (it came first only with respect to Greece)[19].

The European Union has enacted its own acts, including[20]:

- Directive 95/46/EC of the European Parliament and 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;
- Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector;
- Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), abrogating directive of 1997.

  In particular, these regulations include:
  - the definition of general principles with regard to the processing modalities,
  - the acknowledgment of specific rights to every data subjects:
    - the right of access to his personal data;
    - the right to object to a data processing;
    - the right to delete his personal data;
    - the right to have inaccurate personal data updated or deleted;
    - the right to prevent that personal data are used to achieve purposes different from those for which the consent has been given;
  - specific regulation of the so called "sensitive data".

The technology development imposed the implementation of specific protection mechanisms, since the pivotal point was no longer simply to safeguard the private life of famous people from the inquisitiveness of the media. It was represented by the necessity to avoid the, more or less manifest, risks to every citizen deriving from the ease of collating and processing data by means of information and communication systems.

An Italian author wrote: "the digital revolution involves even the change of the

[19] See *ex plurimis* T. M. UBERTAZZI, *Il diritto alla privacy: natura e funzione giuridiche*, Padova, 2004; PARDOLESI (edited by), *Diritto alla riservatezza e circolazione dei dati personali*, cit.; M. G. LOSANO (edited by), *La legge italiana sulla privacy. Un bilancio dei primi cinque anni*, Roma - Bari, 2001; A. CLEMENTE (edited by), *Privacy*, Padova, 1999; C. M. BIANCA ET AL. (edited by), *Commentario sulla tutela della privacy (legge 31 dicembre 1996, n. 675)*, in *Nuove leggi civ*., 1999, 219; S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv*., 1998, 583; V. ZENO-ZENCOVICH, *Una lettura comparatistica della legge 675/96 sul trattamento dei dati personali*, in *Riv. trim. dir. e proc. civ*., 1998, 733; G. BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella Società dell'Informazione*, Milano, 1997.

[20] See L. A. BYGRAVE, *Data Protection Law. Approaching Its Rationale, Logic and Limits*, The Hague – London - New York, 2002. At the European level, the Charter of fundamental rights of the European Union stated at the article 8: "Everyone has the right to the protection of personal data concerning him or her".

notion itself and of the content of the right to privacy: no more right to be let alone, but the right to maintain control on our data"[21].

2.1 Data Protection Principles

Data protection regulations in the EU set the main principles that establish how data processing shall be performed. We can summarize privacy principles as follows:

- **Fair and Lawful Processing**: the collection and processing of personal data shall neither unreasonably intrude upon the data subjects' privacy nor unreasonably interfere with their autonomy and integrity, and shall be compliant with the overall legal framework.
- **Consent:** personal data shall be collected and processed only if the data subject has given his explicit consent to their processing.
- **Purpose Specification**: personal data shall be collected for specified, lawful and legitimate purposes and not processed in ways that are incompatible with the purposes for which data have been collected.
- **Minimality**: the collection and processing of personal data shall be limited to the minimum necessary for achieving the specific purpose. This includes that personal data shall be retained only for the time necessary to achieve the specific purpose.
- **Minimal Disclosure**: the disclosure of personal data to third parties shall be restricted and only occur upon certain conditions.
- **Information Quality:** personal data shall be accurate, relevant, and complete with respect to the purposes for which they are collected and processed.
- **Data Subject Control**: the data subject shall be able to check and influence the processing of his personal data.
- **Sensitivity:** the processing of personal data, which are particularly sensitive for the data subject, shall be subject to more stringent protection measures than other personal data[22].
- **Information Security:** personal data shall be processed in a way that guarantees a level of security appropriate to the risks presented by the processing and the nature of the data[23].

2.2. Categories and Typologies of Data

Different kinds of data can be involved in a processing:

- *personal data*: any data that can be used to identify a person (art. 2, lett. a, Directive 95/46/EC);
- *sensitive data*: any data that disclose information about racial or ethnic origin, religious, philosophical or other beliefs, political opinions,

[21] PASCUZZI, *Il diritto dell'era digitale*, cit., 47.

[22] These are: personal data allowing the disclosure of racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organizations of a religious, philosophical, political or trade-unionist character, as well as personal data disclosing health and sex life. See art. 7 of Italian Data Protection Code; art. 12 of directive 95/46/CE.

[23] For instance, using cryptography: see G. ZICCARDI, *Crittografia e diritto*, Torino, 2003.

membership of parties, trade unions, associations or organizations of a religious, philosophical, political or trade-unionist character, as well as personal data disclosing health and sex life. An important subcategory of this kind of data are medical data (art. 8, Directive 95/46/EC);

- *identification data*: personal data that permit the direct identification of the data subject (art. 4, co. 1, lett. c, Italian Data Protection Code[24]);
- *anonymous data*: any data that cannot be associated to any identified or identifiable data subject (Italian Data Protection Code art. 4, co. 1, lett. n). This category of data is not regulated by data protection regulations.

The distinction of categories of data is necessary for the principles of sensitivity and information security since the measures adopted to protect data shall be adequate to the nature of data.

2.3. Actors

Different actors can be involved in a data processing:

- *Data Subject*: the person to whom personal data refer (art. 4, co. 1, lett. 1, Italian Data Protection Code)[25];
- *Data Controller*: the person who determines the purposes for which and the manner in which personal data are processed (art. 2, lett. d, Directive 95/46/EC);
- *Data Processor*: any person who processes personal data on behalf of the data controller (art. 2, lett. e, Directive 95/46/EC)[26];
- *Persons in charge of the processing*: any person that has been authorized by the data controller or processor to carry out processing operations (art. 4, co. 1, lett. h, Italian Data Protection Code);
- *Third party*: any person other than the data subject, controller, processors, and persons in charge of the processing (art. 2, lett. f, Directive 95/46/EC);
- *Recipient*: any person to whom data are disclosed, whether a third party or not (art. 2, lett. g, Directive 95/46/EC);
- *Privacy Authority*: special authorities appointed to oversee the implementation of the data protection laws (art. 28, Directive 95/46/EC)[27].

[24] When the specific actor was not provided for, we referred to the Italian implementation of the European regulation. The following paragraph is dedicated to the analysis of the Italian Data Protection Code.

[25] The concept of data subject is also expressed using the terms *donor of the personal information* or *data owner*. However, they are not equivalent in the EU legal framework. For instance, the latter relates privacy to the concept of property. On the contrary, privacy is a fundamental right in the EU legal framework.

[26] In the EU legal framework, the relationship between the controller and the processor must be governed by a contract or a legal agreement. Due to the nature of this relationship, a data processor cannot be an employee of the data controller. On the contrary, in the Italian legal context it could be also a member of the organization of the data processor.

[27] Most countries with data protection laws have established these special authorities. In carrying out their tasks, they are required to be functionally independent of the governments and/or legislatures which establish them. The powers of data protection authorities are often broad and largely discretionary. In most cases, they are empowered to issue legally binding orders.

The identification of the actors involved in the data processing is necessary to set the responsibilities and powers imposed by the privacy principles.

2.4. Purpose

The *purpose* is the rationale of the processing, on the basis of which all the actions and treatments have to be performed.

The notion of purpose plays a key role in data protection and it is at the basis of most of the principles presented before. The purpose specifies the reason for which data can be collected and processed. Essentially, the purpose establishes the actual boundaries of data processing. As an example, we mention the privacy policies usually published in commercial websites. They describe the organization's practices including the intended use of personal data (i.e., the purpose). Collected data can be processed by the company only for those purposes. Any other kind of processing is not allowed, unless explicitly permitted by the data subject[28].

2.5. Consent

The *consent* is a unilateral action producing effects upon receipt that manifests the data subject's volition to allow the data controller to process his data.

According to the Directive 95/46/EC (art. 2, lett. h), processing of personal data by private entities or profit-seeking public bodies shall be allowed only if the data subject gives his/her explicit consent. This corresponds to the principle of consent. It is worth noting that the consent must be written if the processing concerns sensitive data.

Data subjects can withdraw the consent at any time exercising the rights that the data protection laws recognize to them, as the right to object to the processing or to delete collected data (art. 14, Directive 95/46/EC). As a consequence, a privacy-aware infrastructure shall allow data subjects to withdraw their consent.

Our final remarks points out to the fact that though the consent may be intuitively seen as a contract, the right of data subjects to withdraw it, and the inalienability of fundamental rights, as for privacy, makes a contractual approach inadequate to data protection in the European legal system. This approach however can be adopted in other legal systems.

2.6. Retention Period

The *retention period* defines how long data shall be kept. Retention period is inevitably related to the principle of purpose specification since data must be deleted as soon as there is any purpose associated to them. Retention period is also necessary to implement the principle of minimality that requires the data controller to delete, destroy, or anonimize personal data when the processing purpose is fulfilled[29].

---

[28] To simplify the management, purposes can be organized in a hierarchical structure: see E. BERTINO, J.-W. BYUN, N. LI, *Privacy-Preserving Database Systems*, in *FOSAD 2004/2005*, Vol. 3655 of LNCS, 2005, 178.

[29] It is worth noting that the notion of retention period is different from *data retention*. Data retention refers to the storage of call detail records and Internet traffic and transaction data by governments and commercial organizations. It is related to public security issues and to oppose the criminality (Directive

3. Security and Data Protection in the Italian Law

3.1 Data Protection Code

The new Italian "Data Protection Code" (d.lgs. June 30th, 2003, n. 196) embodies the new rules on privacy matter. It gathers up all the old Italian acts on privacy and gives new rules in a systematic way. It shall ensure that personal data is processed by respecting data subjects' rights, fundamental freedoms and dignity, particularly with regard to confidentiality, personal identity, and the right to personal data protection.

The Code can be divided in three main sections.

The first one concerns the general provisions and defines the main principles of the regulation. These principles include: the right to data protection, which becomes a fundamental right established and guaranteed also at the European level; the data minimization principle, established by art. 3 and aimed at reducing the process of personal data; the concept of "high protection level", important because it involves a level of hierarchy, and, at the same time, imposes to measure this level.

Data Protection Code guarantees that data process takes place respecting the rights and the fundamental freedoms of the data subject, with particular attention to privacy, personal identity, and the new data protection right (art. 2).

All the definitions are gathered together in a unique article (art. 4), in order to simplify the understanding of them.

In the first part, the Code establishes systematically the rules to follow in order to process data, specifying which are the measures to be taken, depending on if the process is carried out by private or public parties and on the specific kinds of processing.

The provisions referring to data and systems security are based on the former statute n. 675 of 1996 and on the d.p.r. n. 318 of 1999, but they introduce relevant innovations, in particular concerning the adoption of specific security measures.

Another innovation regarding the notice procedure to the Privacy Authority is that it has been significantly simplified: it is now compulsory only for a few specifically identified cases (see art. 37 and 38)[30].

2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks).

[30] Art. 37 establishes the compulsory notification for: genetic data, biometric data, or other data disclosing geographic location of individuals or objects by means of an electronic communications network; data disclosing health and sex life where processed for the purposes of assisted reproduction, provision of health care services via electronic networks in connection with data banks and/or the supply of goods, epidemiological surveys, diagnosis of mental, infectious and epidemic diseases, seropositivity, organ and tissue transplantation and monitoring of health care expenditure; data disclosing sex life and the psychological sphere where processed by not-for-profit associations, bodies or organisations, whether recognised or not, of a political, philosophical, religious or trade-union character; data processed with the help of electronic means aimed at profiling the data subject and/or his/her personality, analysing consumption patterns and/or choices, or monitoring use of electronic communications services except for such processing operations as are technically indispensable to deliver said services to users; sensitive data stored in data banks for personnel selection purposes on behalf of third parties, as well as sensitive data used for opinion polls, market surveys and other sample-based surveys; data stored in ad-hoc data banks

The second section of the Code is dedicated to the regulation of specific sectors and includes, among other things: processing operations for purposes of justice and by the police; processing operations in the public sector; processing of personal data in the health care sector; processing of job and employee data.

In the third section of the Code, we find the provisions regarding the procedure to safeguard the data subject. There are three remedies to be claimed before the Privacy Authority: the cirumstantial claim ("reclamo circostanziato"), used to report an infringement to the regulation regarding personal data processing; the report ("segnalazione"), that is used when you cannot claim by a "reclamo" to ask for the monitoring of the Privacy Authority; and the claim ("ricorso"), when you claim specified rights (art. 141).

Finally, we have to underline that the Data Protection Code represents a new chapter with respect to the relationships between the technology development and the identity of people.

3.2 Security Measures

The Data Protection Code dedicates Title V to the regulation of data and systems security ("Sicurezza dei dati e dei sistemi"), devoting Item I to the security measures in general and Item II to the minimum security measures[31].

The new regulation is contained in articles 31 and following, in the "Technical Specifications Concerning Minimum Security Measures (Annex B)", and in article 3 on "Data Minimization Principle".

Therefore, data security regulations state that a reorganization should guarantee at least a more systematic nature. This intervention maintains a sort of general coherence with respect to the provisions in force, and defines the extent of the general and "minimum" measures which guarantee security, providing some legal rules with a prescriptive purpose.

Now, we will briefly analyze the articles involved in the data and systems security issue.

Article 31 ("Security Requirements") states: "Personal data undergoing processing shall be kept and controlled, also in consideration of technological innovations, of their nature and the specific features of the processing, in such a way as

---

managed by electronic means in connection with creditworthiness, assets and liabilities, appropriate performance of obligations, and unlawful and/or fraudulent conduct.

[31] As regarding to the security measures issue, see P. PERRI, *Privacy, diritto e sicurezza informatica*, Milano, 2007, 195 ss.; C. RABAZZI, P. PERRI, G. ZICCARDI, *La sicurezza informatica e la Privacy,* in G. ZICCARDI (edited by), *Telematica giuridica. Utilizzo avanzato delle nuove tecnologie da parte del professionista del diritto*, Milano, 2005, 516 ff..; P. PERRI, *Le misure di sicurezza*, in J. MONDUCCI, G. SARTOR, *Il codice in materia di protezione dei dati personali*, cit., 137; A. BIASIOTTI, *Codice della privacy e misure minime di sicurezza: D.Lgs. 196/2003*, 2ed., Roma, 2004; G. CORASANITI, *La sicurezza dei dati personali*, in CARDARELLI, SICA, ZENO-ZENCOVICH (edited by), *Il codice dei dati personali*, cit., 112-163; ID., *Esperienza giuridica e sicurezza informatica*, Milano, 2003, 153-257; M. MAGLIO, *Le misure di sicurezza nei sistemi informativi: il punto di vista di un giurista alla luce della legge sulla tutela informatica*, in *Contratto e imp*., 2000, 1; P. PERRI, *Introduzione alla sicurezza informatica e giuridica*, in E. PATTARO (edited by), *Manuale di diritto dell'informatica e delle nuove tecnologie*, Bologna, 2002, 306; BUTTARELLI, *Banche dati e tutela della riservatezza*, cit., 327 ff..

to minimize, by means of suitable preventive security measures, the risk of their destruction or loss, whether by accident or not, of unauthorized access to the data or of processing operations that are either unlawful or inconsistent with the purposes for which the data have been collected".

Namely, the new statute states the implementation of "suitable preventative security measures" has to conform to the following four elements:

a) technological advance of security;
b) the types of processed data;
c) the kind of data process;
d) the specific risk incurred.

Furthermore, the "suitable preventative security measures" have not been standardized: we can agree with this technical choice, since it should not be possible to specify them, as they change constantly depending on the technological development. From a purely technical point of view, we are talking about anti-virus software, back-up procedures, and also physical measures, including burglar or fire alarms installed in the offices where data are stored.

Item II of the Code provides at article 33 a precise definition of the "minimum" security measures that data processors have to implement, in the framework of the more general requirements as established in art. 31, in order to assure a personal data protection minimum level.

Every person who wants to carry out personal data processing is obliged to adopt a generic protection duty and to implement the further minimum measures. Actually, they affect substantially the organization and the methodologies of data collection, introducing precepts directly binding whose non-compliance with is (criminally) sanctioned.

The distinction between processing by electronic means and without them (on paper medium) is unchanged, and there are no longer differences between stand-alone PCs and those connected to the net.

Article 33 ("Minimum Security Measures") states: "Within the framework of the more general security requirements referred to in Section 31, or else provided for by specific regulations, data controllers shall be required in any case to adopt the minimum security measures pursuant to this Chapter in order to ensure a minimum level of personal data protection". As regarding to processing personal data by electronic means, it shall only be allowed if the minimum security measures below are adopted, in accordance with the arrangements laid down in the technical specifications as in Annex B (art. 34):

- computerized authentication:
    - the process through which the system identifies in a irrefutable way the identity of the user through the use of specific identification system;
    - authentication credentials shall consist in an ID code for the person in charge of the processing as associated with a secret password that shall only be known to the latter person; alternatively, they shall consist in an authentication device that shall be used and held

exclusively by the person in charge of the processing and may be associated with either an ID code or a password, or else in a biometric feature that relates to the person in charge of the processing and may be associated with either an ID code or a password;

- implementation of authentication credentials management procedures;
- use of an authorization system, that can allow the user to access to specific resource to pinpoint the authorization profile;
- regular update of the specifications concerning scope of the processing operations that may be performed by the individual entities in charge of managing and/or maintenancing electronic means;
- protection of electronic means and data against unlawful data processing operations, unauthorized access and specific software,
- implementation of procedures for safekeeping backup copies and restoring data and system availability (i.e. back-up copies);
- keeping an up-to-date security policy document (DPS), that shall contain appropriate information with regard to:
    - the list of processing operations concerning personal data;
    - the distribution of tasks and responsibilities among the departments/divisions in charge of processing data;
    - an analysis of the risks applying to the data;
    - the measures to be taken in order to ensure data integrity and availability as well as protection of areas and premises insofar as they are relevant for the purpose of keeping and accessing such data;
    - a description of the criteria and mechanisms to restore data availability following destruction and/or damage as per point 23 below;
    - a schedule of training activities concerning the persons in charge of the processing with a view to inform them on the risks concerning the data, the measures that are available to prevent harmful events, the most important features of personal data protection legislation in connection with the relevant activities, the resulting liability and the arrangements to get updated information on the minimum security measures adopted by the data controller;
    - a description of the criteria to be implemented in order to ensure adoption of the minimum security measures whenever processing operations concerning personal data are externalized in accordance with the Code;
    - as for the personal data disclosing health and sex life referred to under point 24, the specification of the criteria to be implemented in order to either encrypt such data or keep them separate from other personal data concerning the same data subject;
    - implementation of encryption techniques or identification codes for specific processing operations performed by health care bodies in respect of data disclosing health and sex life.

The non-compliance with the minimum security measure requirements is punished by detention for up to two years or by a fine between ten thousand and fifty thousand euro (art. 169).

3.3 Data Minimization Principle

Data Minimization Principle represents an Italian innovation on privacy regulations. Article 3 states: "Information systems and software shall be configured by minimizing the use of personal data and identification data, in such a way as to rule out their processing if the purposes sought in the individual cases can be achieved by using either anonymous data or suitable arrangements to allow identifying data subjects only in cases of necessity, respectively"[32].

This principle represents an advanced rule in respect to the fulfillment provided by Title V and it imposes to data controllers to adopt organizational measures able to minimize the use of personal and identification data.

That point can be reached using anonymous data or suitable arrangements to allow identifying data subjects only in cases of necessity.

The expediency of the use of pseudonyms has been stressed also by the Data Protection Working Party[33].

As regarding implementation, this provision requests something new and very expensive. It implies remarkable investment of computer and information resources (we need to reconsider the information systems in order to be able to incorporate and manage what the provision set) and by the point of view of human resources[34].

Up to now, the commentators proposed a narrow interpretation of article 3, pinpointing a technical organizational criteria of digital databases and suggesting the implementation of Privacy enhancing technologies[35].

The data minimizing principle acts as a general principle policy for the technological development, declaring that information systems and software shall be configured by minimizing the use of personal data and identification data.

Some authors claimed that this rule seems to impose an exorbitant requirement and that it aims at regulating the use of computer resources by private and public

[32] As regarding to this principle, see G. RESTA, *Il diritto alla protezione dei dati personali*, in CARDARELLI, SICA, ZENO-ZENCOVICH (edited by), *Il codice dei dati personali. Temi e problemi*, cit., 45 ss.; see also CASSANO, FADDA, *Codice in materia di protezione dei dati personali*, 46 ff.; AA.VV., *Codice della privacy. Commento al Decreto Legislativo 30 giugno 2003, n. 196 aggiornato con le più recenti modifiche legislative*, cit., 40 ff.; A. PALMIERI, R. PARDOLESI, *Il codice in materia di protezione dei dati personali e l'intangibilità della «privacy» comunitaria*. Nota a sent. Corte di Giustizia delle Comunità Europee 6 novembre 2003, n. causa C-101/01, in *Foro it*., 2004, IV, 59.

[33] This group has been established by art. 29 of the directive 95/46/CE and it is commonly known as "Group 29".

[34] See PALMIERI, PARDOLESI, *Il codice in materia di protezione dei dati personali e l'intangibilità della «privacy» comunitaria*, cit..

[35] See R. ACCIAI, S. MELCHIONNA, *Le regole generali per il trattamento dei dati personali*, in ACCIAI (edited by), *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo Codice*, cit., 71; S. NIGER, *Il diritto alla protezione dei dati personali*, in MONDUCCI, SARTOR (edited by), *Il codice in materia di protezione dei dati personali*, cit., 12-13 ff.. With respect to PETs, see PASCUZZI, *Il diritto dell'era digitale*, cit., 62-66; D. MARTIN, A. SERJANTOV (edited by), *Privacy Enhancing Technologies*, Proceeding of 4° international workshop, PET 2004, Toronto, May 2004, Berlin, 2004.

parties: that would rise manifest unconstitutionality problems with respect to the individual and company freedom[36].

The principle under discussion, although it could appear absurd as regarding to its generic character, bases its justification on the consideration that some security risks of the computer system can be avoided only we decide to implement data protection legal requirements when programming the architecture. The privacy can be reached only if the system is built up so as to protect it (for example, by allowing users to erase their cookies).

This entails value sensitive design[37]**.** In a technologically mediated information society, civil liberties can only be protected by employing value sensitive technology development strategies in conjunction with policy implementations. Value sensitive development strategies that take privacy concerns into account during design and development can build in technical features strategies that enable legal control mechanisms for the protection of civil liberties and allow due process to function. Code is not law, but code can restrict what law, norms and market forces can achieve. Technology itself is neither the problem nor the solution. Rather, it presents certain opportunities and potentials that enable or constrain public policy choice. Technical features alone cannot eliminate privacy concerns, but by incorporating such features into technological systems privacy protecting mechanisms are enabled.

The notion of value sensitive design is an outgrowth of the interdisciplinary study of science, technology, and society. Careful attention to the social embeddedness of technologies reminds us that technologies themselves are social artifacts; they constitute and are constituted by social values and interests[38].

4. Security Standards and Sources of Law

There is no privacy without secure information systems and networks. Data protection in the digital environment is dependent on the regulation of the security standards.

Then, the privacy of personal data represents a research field to study the role standards play in the digital age law.

Depending on the theoretical point of view that we choose, standards can be seen as a source of law or a technical rule that refers to one or more sources of law.

The first perspective aims at emphasizing the *de facto* pivotal importance that

[36] See CORASANITI, *La sicurezza dei dati personali*, cit., 142.

[37] See COHEN, *Drm and Privacy*, cit.; S. BECHTOLD, *Value-centered design of Digital Rights Management*, *Indicare* (2004) (available at: http://www.indicare.org/tikiread_article.php?articleId=39); B. FRIEDMAN, D. C. HOWE, E. FELTEN, *Informed Consent in the Mozilla Browser: Implementing Value Sensitive Design*, *Proceedings of the 35th Hawaii International Conference on System Sciences* (2002).

[38] In the context of DRM, for instance, this insight suggests that design for maximum control is but one direction that a DRM infrastructure could take. Alternatively, one might imagine developing a design process devoted to identifying the full range of values, both private and public, implicated in DRM design, and to operationalizing DRM in a way that preserves important public values. Such a value-centered design process for DRM technologies would seek, among other things, to create rights management infrastructures for information goods that respect and seek to preserve user privacy.

standards have gained and the erosion of the State supremacy. Since technical regulations production is completely delegated to skilled persons, who are qualified to regulate the technical matters, scholarship has focused its attention on the serious problem of the gradual erosion of the state sovereignty *vis à vis* private and public subjects, often with supranational nature[39]. Therefore, the analysis of technical norms is carried out with the acquired awareness of the crisis affecting the concept of State, due to the new organizational methodologies imposed by the building up of a single market and of a global economy.

Furthermore, we have also to outline the lack of democracy in the processes that produce the technical rules. Enacting a statute requires a special process as established by the Constitution: a proposal, the passage through the chambers of the Parliaments, the promulgation of the law by the President of the Republic. But what about the standards? How are they written and implemented? Standards are written by technicians--by programmers--but this does not occur through a democratic process.

These considerations involve other important consequences. Lawyers place a great importance on the sources of law hierarchy. For instance, we know that in the Italian legal system the sources of law are specified in the Civil Code and include: statutes, regulations, customs. We also know that we must put Constitutional and European Treaties at the top of the hierarchy. But what really is a source of law? Some lawyers are starting to analyze the problem and they believe a source of law is something influencing the behaviour of a person. At once we understand how the digital code can really influence the behaviour of a person, permitting some actions and preventing others (recall the example of cookies)[40].

The second perspective starts from the idea that state law, even if weaker than before, is still predominant in the enactment of the law. This approach focuses the attention on the several relationships that can exist among technical norms and legal norms (from the State). More and more frequently the legislation refers to technical norms. This can happen through three procedures[41]. The first is to "incorporate" it: a legal norm explicitly refers to a technical norm. This method has been quite popular since the second half of the Eighties: it is characterized by the fact that the technical norm vanishes into the legal norm. In the second method we have a legal norm referring to deeds emanated by relevant institutions - the so called "standardization institutions" - indicated by the act itself. The third and last method consists in emanating some peculiar technical norms of legal significance, the so called "harmonized norms", with specific properties as established by the European legislator.

---

[39] See L. FERRAJOLI, *La sovranità nel mondo moderno. Nascita e crisi dello Stato nazionale*, Roma – Bari, 1997; G. SILVESTRI, *La parabola della sovranità. Ascesa declino e trasfigurazione di un concetto*, in *Riv. dir. cost*., 1996, 3; M. LUCIANI, *L'antisovrano e la crisi delle Costituzioni*, *ibid*.., 1996, 731.

[40] See L. LESSIG, *Open Code and Open Societies: Values of Internet Governance*, 74 *Chi.-Kent L. Rev* 1045 (1999), *passim*; ID., *Code and Other Laws of Cyberspace*, cit., *passim* Other authors contrast this opinion: see E. DOMMERING, *Regulating Technology: Code is Not Law*, in E. DOMMERING, L. ASSCHER (edited by), *Coding Regulating. Essays on the Normative Role of Information Technology*, Amsterdam, 2006., 11 ff., where the authors asserts that the "code" represents the "hand of the law".

[41] See M. GIGANTE, *Effetti giuridici nel rapporto tra tecnica e diritto: il caso delle norme «armonizzate»*, in *Riv. it. dir. pubbl. com*., 1997, 313, 317 ff..

With specific reference to the Internet Standards, the Internet Society is responsible for the development and publication of many of the protocols that form the TCP/IP[42]. This organization oversees a number of boards and task forces involved in Internet development and standardization. Currently the organizations responsible for the actual work of standards development and publication under the Internet Society are:

- Internet Architecture Board (IAB): it defines the overall architecture of the Internet, providing guidance and broad direction to the IEFT;
- Internet Engineering Task Force (IETF): the protocol engineering and development arm of the Internet;
- Internet Engineering Steering Group (IESG): it is responsible for technical management of IETF activities and the Internet standards process.

In the following part we are going to describe in short the standardization process. To become a standard, a specification must meet the following criteria:

- be stable and well understood;
- be technically competent:
- have multiple, independent, and interoperable implementations with substantial operational experience;
- enjoy significant public support;
- be recognizably useful in some or all parts of the Internet.

A document must remain a Proposed Standard for at least six months and a Draft Standard for at least four months to allow time for review and comment. For a specification to be advanced to Draft Standard status, there must be at least two independent and interoperable implementations from which adequate operational experience has been obtained. After this process, which is characterized by significant implementation and operational experience, a specification may be elevated to Internet Standard, which can be divided into two categories:

- Technical specification (TS): it defines a protocol, service, procedure, convention, or format;
- Applicability statement (AS): it specifies how, and under what circumstances, one or more TSs may be applied to support a particular Internet capability.

5. Conclusion

Since privacy in the digital context can be really guaranteed only if security standards are implemented, the study on the standard production process represents a pivotal point in the field of data protection. We need to become aware of the dynamics that drive to the elaboration of the technological standards governing the digital architecture.

Our approach to the digital world is influenced by our expectations from digital networks. These expectations will shape the design of the digital environment in the

[42] As point of reference for this part we took into account W. STALLINGS, *Network Security Essentials. Applications and Standards*, 3rd ed., Upper Saddle River, New Jersye, 2007, 19-22.

near future. The next step is to incorporate values, principles and codes of conduct inside the designs, in order to make clearer the necessary interaction between the technology development and the aims pursued by our legal systems.

The collected information in our research represents only a first attempt – heralding further in-depth studies – to analyze data protection issues on the much more general level of the relation between privacy and security.