Lessons learned from the Italian law on privacy

Pierluigi Perri

CIRSFID, Università di Bologna
via Galliera, 3; 40121 Bologna (Italy)

Stefano Zanero [1]

D.E.I., Politecnico di Milano
Via Ponzio 34/5; 20133 Milano (Italy)

Abstract

In this article, we analyze the italian privacy law, and its technical regulations, in the framework of various European Directives. We point out both its strong points and its flaws, and the difficulties found in its real-world implementations. We also analyze a recent revision of the law, and how it tries to address these shortcomings. In conclusion, we try to highlight some lessons that can be learned from this attempt to regulate privacy and data security.

Key words: privacy, confidentiality, privacy regulations, privacy laws, security

1 Introduction

Privacy is probably one of the foremost goals of the information security discipline. In the information age, personal data on our health, our preferences and our behavioral patterns are valued by almost every business and corporation, leading often to a real trade of personal data collected, harvested and analyzed by professional data miners.

Email addresses: perri@cirfid.unibo.it (Pierluigi Perri), zanero@elet.polimi.it (Stefano Zanero).
URL: http://www.elet.polimi.it/people/zanero (Stefano Zanero).

[1] This work was partially supported by the FIRB-Perf project, http://www.perf.it

While this is sometimes done at least partially in the interest of the consumer (for example, when user behavior on a website is analyzed to customize the interface to his needs [1]), most of times we feel that our privacy is violated by abusive handling of our personal data. The European Union and its member countries have approached this problem, and created legislative solutions to grant their citizens a right to control diffusion and communication of their personal data. The United States also approached the problem of privacy, but under a totally different perspective.

In this article, we will focus on the Italian and European laws and regulations on privacy. Since they have been evolving for years (the first Italian privacy law was enacted in 1996) we think that lessons can be learned from the results of the application of these directives, in particular regarding what can and cannot work in privacy legislation.

2 Security and privacy in EU directives on telecommunications and their reception in Italy

The problem of the security of computer networks and infrastructures is addressed in various EU directives on telecommunications, as well as in the Italian legislation designed to implement such directives (it must be remembered that in the European Union, European Directives must be implemented by each member state in their own national legislation in order to be enacted). These directives are usually concerned with the efficiency and resiliency of the telecommunication infrastructures, and with their ability to interconnect; security is not directly addressed as a standalone need, but rather as a part of an extensive interpretation of the directives.

Due to space limitations, we will describe only briefly this framework: a complete analysis can be found in [2]. We will also address the differences between the European and American approaches, but for a more complete review of these concept we refer the reader to [3].

Directive 90/387/CEE [4] ("On the establishment of the internal market for telecommunications services through the implementation of Open Network Provision", ONP), which is no longer in force, set out the fundamental requirements for the ONP, and in doing so it invoked "non-economic reasons in the general interest" that could induce a member state to limit access to a public network or to public telecommunications services. In particular, these reasons are the "security of network operations, maintenance of network integrity and, in justified cases, interoperability of services and data protection". The principle of data protection applies to "personal data", but also to the "confidentiality of information transmitted or stored" (regardless of the

medium) as well as to the protection of privacy.

Directive 97/66/CE [2] of 15 December 1997 [5] "concerning the processing of personal data and the protection of privacy in the telecommunications sector", in article 4 specifically addresses security. It forces every provider of a telecommunication service offered to the public to adopt appropriate technical and organizational measures in order to ensure the security of the services provided, by working in conjunction with the public network provider if necessary. They must also inform service subscribers anytime a security risk threatens the network, making this assessment on the basis of Directive 95/46/CE [6], article 17, which specifies the security measures for personal data and its treatment.

The D.Lgs. [3] 171, of 13 May 1998 [7] (which implements the Directive 97/66 CE and the European Parliament and Council provisions on journalistic practice), under article 2 (Security), requires the providers of public telecommunications services to adopt the technical and organizational measures set forth under article 15, paragraph 1, of law no. 675/1996 [8] (for details see section 3). It also enforces the two constraints, regarding cooperation whenever necessary between the provider and the public network owner, and the responsibility to inform the subscribers of any security risk, pointing out as well all the available remedies, along with their costs.

DPR [4] 318, of 19 September 1997 [9], regulates the technical implementation of the European directives on telecommunications (including the aforementioned Directive 90/387/CEE). The DPR draws some guidelines on the reasons of "general interest" that may induce the State to require service providers to meet certain requirements. Among these basic reasons there are network security and the protection of personal information, as specified in article 12.

Each telecommunication entity is also required to adopt suitable measures in order to ensure the integrity and the proper functioning of the telecommunications network, and to follow specific request and directions in this field from the communications authority.

The need to ensure the security and the privacy of the data, the integrity of the network, and the protection of network equipment and software cannot lead to a priori refusal of access to a third party, nor does it justify restricted access and usage of the PSTN network and/or other public telecommunications networks. Any restrictions imposed must be kept down to the minimum

[2] Directive 97/66/CE was subsequently superseded by Directive 2002/58/CE, which we will introduce in section 6

[3] Decreto Legislativo: legislative decree, a decree by the Government, for which the Parliament has issued a law which exceptionally extends the legislative power to the executive organ

[4] Decreto del Presidente della Repubblica: Presidential Decree

necessary for keeping the network functional, must be proportional to the risks incurred, and must be based on objective criteria and applied in a non-discriminatory fashion. This is of particular importance in countries (such as Italy) where a single telecommunications operator holds the vast majority of the PSTN network.

Exceptional measures can be taken during emergencies, in which case the organizations can interrupt or limit the services provided or deny access to new users in order to safeguard the network. This formulation makes obviously important to clearly define an emergency: each organization must institute procedures to immediately inform users and the authorities of any emergency situation (the beginning and the end of it), and also all the service restriction that will be in effect throughout the period of emergency.

The communications authority has regulatory power to make sure that the conditions for accessing a network are not discriminatory or disproportionate to the risks incurred and are adherent to the objective criteria mentioned, acting on request by any of the parties.

With concern to data protection and privacy defense, article 12 of the DPR 318/97 simply refer to laws no. 675 [8] and 676 of 31 December 1996 [10] and to any provision that will be issued in the future on the protection of personal data. We will talk about these laws in the following sections.

In summary, the European legislation on telecommunications, as it was received in Italy, is concerned with protecting both the data through which personal communications can be identified (i.e. the billing data and the logs of the calls) and the privacy, security and integrity of communication itself. Continuity, openness of access, interoperability, and privacy of the content of communications are declared to be of general value, superior to the economic requirements. Thus, businesses and public administrations which operate on-line services and telecommunication infrastructures should have them as one of their top objectives. The definition of communications and infrastructure security thus embraces both networks and service providers, hence making it necessary to adopt common strategies and measures with which to analyze and reduce risks. Of course, different degrees of risk are involved, depending on the type of economic activity (ranging from simple business-to-consumer e-commerce, to business-to-business transactions, and to communications and network services), and on the type of interactions and technologies involved.

The U.S. approach to the security, instead, is very different from EU, and this is very strange if we consider that the U.S. legal doctrine was the first to theorize the existence of a right to privacy. In 1890, in fact, Samuel Warren and Louis Brandeis published the influential article “The Right to Privacy” [11], in which privacy was described as ”the right to be left alone”.

Now the concept of privacy is different from that, and while in the EU the right to privacy is strictly connected with the fundamental right of the human dignity, in the U.S. some authors are talking about the failure of American Privacy Law [12], and that because there is often a conflict between the right to protect privacy and other rights such as free speech, and the law values free speech over privacy, and there is a judicial reluctance to protect privacy, "because judges are extremely reluctant to decide what is private". In conclusion, however, an ineffectual law of privacy is better than none at all.

3 The original Italian legislation on privacy

In this complex scenario, we need to choose and impose the basic security conditions that make possible to counteract illicit techniques used to access personal data or confidential information stored in electronic archives, with the highest possible degree of confidence. An important point that should not be forgotten, however, is that the scope of protection cannot be limited to the "personal" data stored in such archives. The European directive is very clear in defining security as a precondition to electronic data processing and online interaction, that should embrace the entire information systems, as well as the flow of information between systems, rather than just the data stored in them. So we also need to ensure that communication networks can be used as a medium through which users can send qualified messages, meaning messages that serve to transact private or public business and services.

Law 675 of 31 December 1996 [8] (which in the following will be referred to as "the law") set forth a number of measures for the protection and security of personal data, in a complex context, not devoid of contradictions. Service providers who manage such data are required to notify the National Authority on Privacy ("Garante", www.garanteprivacy.it) of the security measures implemented to protect the data for which they are responsible, thereby enabling this authority to assess the adequacy of the measures implemented and make sure that they are compliant with the legislation on communications security and the handling of personal data. Service providers are required to disclose two kinds of information: the experience they have with telecommunications security and the specific technical and structural task entrusted to them as service providers.

The data security framework comes from article 15 of the law, which reads:

> "The personal data subject to treatment needs to be guarded and kept under control, and the protection afforded must be gauged to the kind of data handled and the kind of handling it receives; the latest technology available must be used to this end, and preventive security measures must

be adopted that will forestall the risk of data loss or destruction (whether intentional or accidental), as well as any unauthorized access or unallowed treatment or any treatment of the data incongruent with the purpose of its collection."

The second paragraph of the same article 15, however, makes mandatory only "minimal" security measures, which are to be implemented preventively, i.e. before any kind of data treatment process can take place. These measures are not specified into the law, and were meant to be described no later than 180 days since the law took effect, through a set of regulations enacted by a decree of the President of the Republic, on the basis of a proposal made by the Secretary of Justice, after hearing the Authority for Information Systems of the Public Administrations (AIPA) and the Authority for Privacy (Garante). These measures were to be reassessed on a biannual basis, and to be made compliant with every subsequent regulation, issued through the same procedure, and designed to keep abreast of advancements in communications security technology.

The DPR 318 of 28 July 1999[15] (which in the following will be also referred to as "the regulation"; please note that it is a different decree than the aforementioned DPR 318/1997) was actually issued with a time lapse of two years, rather than within the prescribed 180 days; this is already quite indicative of the ability of such a legislative process to keep abreast of the changes in information security needs and technology.

DPR 318 specifies the "minimum" security measures, defining them in broad terms as "the complex of such technical, organizational, logistical, and procedural security measures that can guarantee a minimum level of protection against the risks singled out under article 15, paragraph one, of the law". The provision applies to the "electronic or otherwise automated means by which data is treated". There is also a definition of system administrators as "those people whose task is to oversee the resources of an operating or database system and make its use possible".

There are a few exceptions to these minimal security measures: for instance, collections of personal data maintained for personal use on a stand-alone computer (i.e. personal electronic address books, for example) are exempted. What a "stand-alone" computer is, however, is debatable: an handheld device with personal information connected to the Internet could be considered an "accessible" computer, and could thus be subject to these regulations.

The regulation makes a distinction between automated and manual treatment, and in the first case between stand-alone workstations (inaccessible from other machines or terminals) or by computers accessible on a network (either private or public). Details will be discussed further in section 4.

Current legislation in Italy still leaves unresolved some questions emerging from the unstoppable advancement of technology. An example here is data transfer by way of wireless or blue-tooth technology, which makes this operation possible using any kind of mobile devices, such as cellular phone, handheld devices, or laptop computers. The regulations in place here are ambiguous and on several occasions have made it necessary for the telecommunications authority to intervene; even more significant, they have made it necessary for the lawmaker to intervene, by postponing their coming into force, securing in the meantime a provisional enactment.

We should still be acquainted with these security regulations, however, where they concern privacy (the question of protecting the integrity and authenticity of personal data), for in this regard the regulations speak clearly, even considering the approximations and inaccuracies sometimes made when the matter at hand is of a more general nature. Thus, the previously indicated article 15 concerns personal data and not data-treatment systems; it follows from this that the security measures implemented pursuant to this article must be confined to the functional objective of preserving the security of the data being treated, such that the security in place brings into operation the latest technology available and is gauged to the specific kind of data-treatment made.

The legislative provisions follow closely the EU legislation, especially article 16 of Directive 95/46/CE [6], which makes explicit reference to "adequate" security measures (which must afford "a sufficient guarantee of security"), as opposed to the "minimal" measures subsequently set out in Italian legislation. Measures are adequate when, based on the state of the art of technology, and on the implementation costs, they guarantee a level of security proportional to the risks associated with the kind of data requiring protection and the kind of treatment they are subject to. So, where the Italian legislation simply define a "minimum" subset of security measures, the EU directive defines a set of metrics and parameters that can be verified on an objective basis, on which the appropriateness of security measures can be judged. This gap between our law no. 675 and Directive 95/46/CE will be partially closed by the forthcoming "Testo Unico" ("Unified Text") on the handling of personal data. We will talk extensively about it in section 6.

4 Technical limitations of the original Italian privacy law

As we have discussed in the previous section, the technical regulations for the first Italian law on privacy (DPR 318/1999) tried to describe a minimal subset of a security policy. Minimal, is, indeed, euphemistic; however, it is noteworthy that for once the law tries to give a detailed technical explanation

to a vague term. An additional positive note is that the law calls for "technical, computer, organizational, procedural, and logistic security measures", implying an holistic view of computer security.

Given that, these measures will now be discussed in detail. They are focused, substantially, on the identification of different roles in the data processing flow, and on the mechanisms for granting, revoking and auditing access privileges to the people in charge of the data management. In other words, a scheme for user provisioning is drawn.

Three classes of roles are identified, in addition to the "Person responsible of personal data handling" (in the following, the Responsible) who has a political and regulatory power, rather than a technical one:

- System Administrators: they are in charge of the system and network management, and are thus endowed with high access privileges for technical reasons. They are not, however, entitled to data processing
- People in charge of data handling: they are the people who actually work with the data, and are entitled to access reserved data, according to their role
- Password keeper(s): they hold in custody the passwords of all the people involved in the data processing.

The regulation makes a distinction between data processing done with or without automated systems, and in the former case it introduces a taxonomy based on the systems used for data processing:

- Standalone: systems that are not, and will never be, connected to a computer network
- Networked, but not public: systems that are interconnected with a network, but not accessible by a public network
- Networked on a public network: systems that are accessible via a public network

It is noteworthy that the telephone network is, by itself, a public network. In addition, to be on the safe side, the legislator has specified that the term "accessible" does not mean "a system configured to allow access", but means "reachable": thus, a system connected to the Internet behind a firewall which does not allow inbound connection is considered "Networked on a public network", since it *could* be reached by the public network, even if it is not configured to allow this. This also means that any computer with a modem connected to a phone line should probably be included in the third category, even if not configured to respond to incoming calls. Even if the connection is not permanent, the computer should be classified according to the worst case. Fundamentally, today most systems fall in the third category.

In the case of standalone systems, a simple access control mechanism based on logins and passwords is required. These passwords are provided to those in charge of data treatment. It must be noted that the access control mechanism is for the data, not for the system itself: thus, it can be implemented either at the operating system level, or as a password to access the database, for example. The only, obvious requirement, is that access privileges are verified before allowing access to data.

The only unusual quirk here is that logins and passwords must be stored "securely" by the "password keepers". In the usual implementation of this procedure, every user writes down his password on a piece of paper, seals it into an envelope, and signs it. The envelopes are then stored in a safe, in case that a user account needs to be unlocked in an emergency. It's easy to observer that this procedure means a lot of pain for absolutely no gain, since in almost every standard operating system the administrator can override any user password. It is also a common opinion that the law implicitly requires that no login can be used to override another login: this assumption is obviously not true in almost every COTS operating system.

Additionally, the regulation prescribes that, whenever possible, the users should be able to change their passwords on their own, updating at the same time the backup copy in the envelope. The whole process is cumbersome, and will inevitably lead to infrequent changes of passwords. This negative consequence alone makes the whole scheme flawed.

In the case of computer systems that are connected to public networks, additional passwords are required in order to identify the user when he logs on to the machine. This means that a multiple level authentication is required by law, against the current trend which tends to implement single-sign-on systems throughout a network. An additional requirement, which is quite difficult to implement in the exact wording of the law, is that "a single login" should not be able to access contemporaneously a "single application" from different "workstations". A simple shortcut would be to limit the use of any login just to one user session on a single machine, but this would be overrestricting; in addition, the lawmaker seems to be concerned here with the "application and data" logins, not with the network OS logins.

If the data processing will deal with "sensitive" data, additional restrictions apply. "Sensitive" data are described as any bit of information that reveals something about a person's state of health, religious beliefs, political orientations or sexual preferences.

The law is not extremely clear on this point, but we can easily derive a few requirements. The access is granted to users (or to workgroups), on a need-to-know, need-to-access base: the responsible should grant to the people in

charge of data handling only the minimum access that is required to perform their duties. The same principle should apply also to administrators, who should be able to perform only maintenance duties. This is evidently more difficult to obtain. Privileges should be verified "at least once a year". This is a ridiculously long lapse of time, but it's also true that in many cases even this minimal requirement is not met. Yearly, the responsible should also verify that the stored data is the absolute minimum amount necessary for the treatment and for system upkeep.

In the case of systems interconnected to public network, the responsible must also designate the external workstations and tools that are enabled to access the sensitive databases (he can also revoke such authorization at any time). In other words, the law requires that servers with sensitive data should have strict access lists, that allow incoming connections only from authorized external systems, with approved software. In this case, the law also requires that a Security Standards Document (Documento Programmatico Sulla Sicurezza) is elaborated and updated on a yearly basis. This document should begin with a detailed risk analysis, and clearly state responsibilities and duties related to data security, and also provide an appropriate disaster recovery strategy. While appreciating this attempt to guide enterprises towards a correct approach to information security, we must note that, since there is absolutely no requirement to actually enact what is described in the Documento Programmatico, most businesses simply created a useless document stating all the best practices, and then forgot it quickly into a drawer. It is not easy to impose good security practices by law.

The regulation requires that "memory supports" (mass memory, magnetic media, optical media ...) that have been used for sensitive data can not be reused, and must be disposed properly, unless the previously stored sensitive information cannot be recovered in any way. While scrupulous and probably necessary [16], this requirement is not technically easy to implement: in first place, what is and what is not technically recoverable from magnetic media is widely debatable. In second place, the data recovery process is driven by a complex interaction between the operating system, the applications and the media; let's suppose that the sensitive data were encrypted: in this case, is the destruction of the decryption key enough to ensure that the information "cannot be recovered" ? In information security terms, yes, it is, provided that the encryption algorithm is sound and the key is sufficiently long. But would this position hold, legally, in the unlikely but possible case that someone successfully breaks the cryptosystem, or obtains the key by brute force?

An additional, almost ironic disposition, requires all computer systems used for treatment to be protected with an antivirus program, updated at least every *six* months.

Finally, the law contains two important exceptions, for personal data "of which diffusion is allowed", and for "statistical data". Both these exceptions pose important threat to data confidentiality. As discussed in many articles [17], disclosing separate bits of information, each harmless if considered singularly, can become a security problem. The problems of inference in statistical databases is widely discussed, and we refer the reader to [18] for a complete survey of possible attacks and defense strategies. Both these weaknesses have been completely overlooked by the lawmaker.

5 An analysis of the adoption of these measures

The "Authority for privacy guarantees" publishes a yearly report for the Parliament, on the status of the adoption of the measures we described and on its own activities. We extract some data from the reports of year 2002 [19] and 2001 [20] (the figures for year 2002 actually span from 01-01-2002 to 30-04-2003). In year 2002 the total number of data handling processes recorded since 1996 was recorded as 315000; in year 2001 the same figure was recorded as 310000, with a net increment of 5000. However, the number of new notifications in year 2002 was of 17500, meaning either that some handling processes have terminated, or that the records of the authority are not totally reliable.

There is, however, a strong decrement in the number of new notifications: there were 17500 new notifications in year 2001, and 12227 in year 2002. These two figures seem to indicate that the start-up transient has ended, and the situation is stable. We can thus suppose that most businesses have already complied with the notification requirement, and are thus aware of the requirements of the law.

However, if we analyze the figures resulting from the inspections of the authority in year 2002, we see a different situation. The first striking figure is the total number of inspections, 40, which means one every 10000 data handling notifications. We do not have data on how these 40 targets were selected, so we can not draw any conclusion on the statistical validity of this subset. We just know that 3/4 of them are from the private sector (31 versus 9). 35 of the inspection were autonomous, under art. 32 provisions, while 1 was performed under consent of the database owner, and just 4 were performed by the means of a search warrant.

The results are not dramatic, with only 5 violations severe enough to be reported to law enforcement for prosecution. Of these, 3 are violations of the categories of data that can be handled under the privacy law, and 2 are violations of the minimum security requirements. However, even if drawing statistical conclusions from so few inspections may be misleading, this means that

$5 - 10\%$ of the organizations handling personal data did not enact even the simplicistic minimal measures.

If we look to the other violations found, outside a formal inspection (45 in total), we see that most of them refer to bureaucratic obligations and not to substantial security violations: in 28 cases the parties were not correctly notified, in 13 cases requests for information were not answered, and in 2 cases the authority was not correctly notified of the treatment. However, in at least two other cases, sensitive health-related data were disclosed. Since these violations were found without a thorough inspection, we can safely assume that they were totally evident, human mistakes or deliberate decisions, and not caused by obscure vulnerabilities. These violations, that are probably just the tip of the iceberg, show that even the most basic principles of security are still ignored sometimes, even by law-abiding businesses.

6 The New Unified Text on Privacy

The new Italian "Unified Text on Privacy", or "Privacy Code" ("Testo Unico sulla Privacy", which in the following will be referred to as "the Code"), drafted in application of law 127/2001, has been enacted through a legislative decree [21], and has begun to be applied on 01-01-2004, replacing Law 675/96.

The Code is the result of a consolidation between the Italian legislation about privacy (affected by many legal texts coming from different authorities and regulatory bodies), the EU directives and some international agreements. In particular we can see that the Directive 2002/58/CE [22], regarding the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications), permeates the new Testo Unico. This approach of consolidation is somehow new, but it is possible that the other States members of the EU will follow the road traced by Italy, trying to regulate, adjust and harmonize their respective national data protection law.

Law 675 was brought out in a rush, with the institutions having to work frantically to respond to urgently pressing needs, and consequently resulted in a fragmented and often inaccurate regulatory framework, as we have observed in our examination. The matter at hand, being already a delicate affair in and of itself, was needlessly complicated in an unextricable way, calling for a complete review of legislation. The fundamental principle of the new Code is the simplification of the procedures for compliance, both for public administration agencies and for private businesses, and also of the formalization of the procedures to exercise one's own rights.

The Code consists of three parts: Part 1 (articles 1 to 45) sets out the general principles and obligations that apply to any data processing operation. It explicitly proclaims (art. 1) that everyone has the right to the protection of personal data - a right that was recently reaffirmed also by Article 8 of the Charter of Fundamental Rights of the European Union. Part 1 also describes the general rights that each subject retains on the data, and the fundamental rules to follow.

Part 2 (Sections 46 to 140) addresses the processing of personal data in specific sectors. Considerable attention is paid to law enforcement and judiciary system procedures. Specific provisions address the processing of genetic and biometric data, and also of data which can disclose the geographic location of individuals, because such data is more likely to affect the rights and freedom of people. The "Garante" is granted power to further regulate these matters, by adopting detailed regulations.

Data processing carried out by government agencies for defense, military and State security purposes is also regulated, in the light of the Amann/Switzerland and Rotaru/Romania decisions of the European Court of Human Rights. The sentences can be found on the court's database [23], while a commentary can be found in [24].

It is, however, worth noting that DL[5] 354 of 12/24/2003 has recently reformulated art. 132 of the Code, which dealt with the keeping of accounting data for telecommunication traffic. Among other modifications, the new art. 132 raises from 30 to 60 months the required amount of time during which service providers must keep these data available. In these additional months, data can be accessed only with a warrant for crimes such as terrorism (art. 407, comma 2, lett. a, penal procedural code), or for crimes dealing with computer and telecommunication systems. This decree has been heavily criticized by the Garante, since it simplicistically treats telephone and telecommunication data in the same way. Keeping trace of computer communications for as long as 5 years could obviously generate worries for the privacy of Internet Users.

Finally, administrative and judicial remedies, sanctions and the powers and activity of the Supervisory Authority are regulated in Part 3 of the Code (Sections 141 to 186).

The Code approaches the problem with a wider normative setup, and introduces the general concept of "adequate" security measures, described in article 31. Whereas "minimal" security measures are designed to avert the risk of only the most serious kinds of risk to the data being treated, the adequate measures

[5] Decreto Legge: Decree-Law, a "necessary and urgent" government act which has the force of law but must be converted within 30 days by the Parliament or be nullified

described in article 31 are designed to prevent a wider array of risks:

> "... data destruction or loss, even if accidental; unauthorized access; and data treatment that is disallowed or incongruent with the purpose of its collection."

These measures are not specified in any detail in this legislation; rather, each company must work out its own measures, on the basis of four elements set out in the same article 31, namely:

(1) the technological advancement of security,
(2) the type of data treated,
(3) the kind of treatment received by data, and
(4) the specific risks incurred.

The Code approaches from a new perspective the problem of working out and implementing security measures. As we have previously seen, the older legislative setup, and DPR 318/99 in particular, had set out an all-embracing distinction between two different kinds of protection specific to different "classes" of data (personal and sensitive), and considered only the structure of the information system used (accessible from other computers, or inaccessible).

In contrast, the Code looks not so much at the data itself or the systems through which it is treated, as it looks at the subjects who are performing the data treatment. Article 32 of the Code singles out three types of subject very similar to the ones described in Law 675:

- *titolare*, title holder, the ultimate responsible for the data handling process,
- *responsabile*, responsible, his functional delegate,
- *incaricati*, the people in charge of the data handling process

It also introduces the new concept of "*particolari titolari*" (specific titleholders), but the distinction goes beyond the scope of this article. The role of the system administrator, surprisingly, is no longer formally defined.

The title holder is required to set up an accurate user provisioning process (which follows at least the minimal security measures). If the security technologies in place are known to be limited or obsolete, and do not enable a system to be fully compliant with minimum security legislation, the title holder must keep within the facility a dated document detailing such limitations or obsolescence. This is not meant as an escape path to avoid keeping up to date the security measure, but rather as a temporary declaration of fault which should prelude to an upgrade.

Title 5 of the Code sets out the minimum measures of protection required to avert the risks of intentional or accidental data loss or destruction, and of

illegal or unallowed data treatment. These measures must be adopted before any kind of personal data handling may begin. Also, these minimal measures, because they fall within the general framework of obligations set out under article 31, must be kept up to date.

7 Technical analysis of the Code

The Code, in Section 2, remits the determination of the minimal security measures to an appropriate technical regulations annexed to the code (Annex B, "Technical specifications"), without a separate document, such as DPR 318/99 in the previous legislation. Also in this case, however, the annex should be updated by the authorities, in order to keep abreast of technical evolutions (hopefully, with better results than in the past). It is worthy to note that until 06/30/2004 there is a transition period, during which the security procedures for data treatment described by DPR 318/99 are still accepted. After that date, the Code, Annex B, will be the only valid regulation for data treatment in Italy.

The new system of security measures is simpler than the existing one, and is brought up to date with the latest developments in information security technology. Let's see briefly the new requirements.

First of all, the taxonomy on the systems is simplified: either the treatment is processed by electronic means, or manually. Distinctions between accessible or unaccessible systems disappear.

Electronic data treatment requires users to receive authentication (identification). This authentication can be obtained by the means of a secret, a token, or by using a biometric system (this was not accepted specifically in DPR 318/99). In addition, specifical guidelines for passwords are drawn. These guidelines are adherent to the current best practices (8 characters long, with no easy-to-guess references to the owner, ...).

Adequate procedures for managing authentication credentials are also required, with deactivation of unused account and revocation of privileges to individuals not entitled to access the data anymore (i.e. an adequate process of user provisioning is required). The obligation to make copies of authentication passwords is retained, but only if it is necessary in order to grant access to data in case someone in charge of data storage and protection is not available, and an emergency requires his privileges. This reduces the problems we noticed in section 4.

Authorization profiles (i.e., what an user or a group of users can do with the

data) must be set up before the treatment begins, and reviewed at least yearly. Unluckily, the ridiculous requirement to use an anti-virus program updated at least every six months is still retained, and it is extended to anti-intrusion programs. It is not clear if this refers to intrusion detection or prevention systems, or to the whole array of security systems and programs that can be deployed to secure a network. Patches must be updated at least yearly (every six months for sensitive data). A weekly backup procedure is enforced.

For the treatment of sensitive data, the Security Standards document is still required, but its structure is more strictly detailed. Still, there is no clearly defined need to realistically evaluate the real situation of the business processes and their adherence to the Security Standards document. The need for anti-intrusion measures is reinstated. Removable media are still subject to disposal, unless the information are not "understandable" or technically retrievable in any way. This seems to clarify that encryption is actually a safe way to protect and dispose of sensitive data. Backup and restore procedures must be designed to allow a complete restore of data in at most seven days.

In the case of health or sexual preference related data, encoding techniques or identification codes should be adopted, allowing this type of data to be treated separately from the identification data as long as possible. Particular precautions are to be observed in case of genomic data: this type of information must be stored in securely sealed locations, and must be transferred only in an encrypted form.

Two additional dispositions try to provide accountability for the application of these measures. If the organization resorts to a consultant or a managed services provider in order to implement these measures, the third party must release a document stating that their work is adherent to the regulations. In any case, if the organization has to file a public financial report to the authorities (which is required by law in Italy for many types of businesses), it must enclose in the report a note about the status of compliance with the preparation and revision of the Security Standards document.

8 Conclusions

Security and privacy are continuously evolving concepts, where very few stable points have been reached. Formal methods are still very immature, and mostly we are dealing with "best practices" that need to be updated continuously. In this framework, it is difficult to draft laws that deal with the definition of security standards.

The evolution of the Italian Law on Privacy is, in our opinion, a case well

worth studying. The errors and problems found in its application should be carefully reviewed before international uniform laws on privacy are studied and enacted. The European Union directives are a good example of how an international uniform privacy law could look like.

The efforts for establishing laws on copyright set forth a good example of how uniform laws can be applied in an international scenario, and how difficult can be to correct their problems once they have been formulated. If an international privacy effort is going to begin at any point in the future, it is of the uttermost importance that the formulations of laws are thoroughly studied to avoid any kind of problems. For this reason we believe that learning lessons from the past is the only way to avoid repeating disastrous mistakes in the future.

References

[1] R. Cooley, J. Srivastava, B. Mobasher, Web mining: Information and pattern discovery on the world wide web, in: Proceedings of the 9th IEEE International Conference on Tools with Artificial Intelligence (ICTAI'97), 1997.
URL citeseer.nj.nec.com/cooley97web.html

[2] C. Kuner, European data privacy law and online business, Oxford University Press, 2003.

[3] B. R. Ruiz, Privacy in telecommunications : a European and an American approach, Kluwer law international, 1997.

[4] Directive 90/387/cee.
URL http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!cele%xapi!prod!CELEXnumdoc&lg=EN&numdoc=31990L0387&model=guichett

[5] Directive 97/66/ce.
URL http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!cele%xapi!prod!CELEXnumdoc&lg=EN&numdoc=31997L0066&model=guichett

[6] Directive 95/46/ce.
URL http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!cele%xapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett

[7] D. lvo 13 maggio 1998 n. 171, in italian.
URL http://www.interlex.it/testi/dlg98171.htm

[8] Law 31 dicembre 1996 n. 675, in italian.
URL http://www.interlex.it/testi/l675_96.htm

[9] D.p.r. 19 settembre 1997, n. 318, in italian.
URL http://www.interlex.it/testi/dpr31897.htm

[10] Law 31 dicembre 1996 n. 676, in italian.
URL http://www.interlex.it/testi/l676_96.htm

[11] S. D. Warren, L. D. Brandeis, The right to privacy, Harvard Law Review IV (5).

[12] B. S. Markesinis, Protecting Privacy, Vol. IV of The Clifford Chance Lectures, Claredon Press Oxford, 1999.

[13] D. J. Solve, Information Privacy Law, Aspen Publishers, 2003.

[14] W. Faulkner, Privacy, Random House, Inc., 1965.

[15] D.p.r. 28 luglio 1999, n. 318, in italian.
URL http://www.interlex.it/testi/dpr99318.htm

[16] S. L. Garfinkel, A. Shelat, Remembrance of data passed: A study of disk sanitization practices, IEEE Security & Privacy 1 (1).

[17] D. Dobkin, A. K. Jones, R. J. Lipton, Secure databases: protection against user influence, ACM Transactions on Database Systems (TODS) 4 (1) (1979) 97–106.

[18] N. R. Adam, J. C. Worthmann, Security-control methods for statistical databases: a comparative study, ACM Computing Surveys (CSUR) 21 (4) (1989) 515–556.

[19] VV.AA., Relazione 2002, Garante della Privacy, 2003, in italian.
URL www.garanteprivacy.it

[20] VV.AA., Relazione 2001, Garante della Privacy, 2002, in italian.
URL www.garanteprivacy.it

[21] D. lvo 30 giugno 2003, n. 196, english version.
URL http://www.garanteprivacy.it/garante/document?ID=311066

[22] Directive 2002/58/ce.
URL http://europa.eu.int/cgi-bin/eur-lex/udl.pl?REQUEST=See%k-Deliver&COLLECTION=oj&SERVICE=eurlex&LANGUAGE=en&DOCID=32002l201p0037

[23] Database of human rights court decisions.
URL http://hudoc.echr.coe.int/hudoc/

[24] Memorandum of laws concerning the legality of data retention with regard to the rights guaranteed by the european convention on human rights (Oct 2003).
URL http://www.privacyinternational.org/countries/uk/surveillance/pi_data_retention_memo.pdf