RFID Privacy and Security Risks: Italian Case Study

Maria Concetta De Vivo, Alberto Polzonetti, and Pietro Tapanelli

School of Science and Technology,
Computer Science Division, University of Camerino, Camerino, Italy
{concetta.devivo,alberto.polzonetti,pietro.tapanelli}@unicam.it

Abstract. Radio Frequency Identification (RFID) technology can be used in different areas such as in occupational safety and health. This article discusses the development of the RFID technology and its legal implications in the context of the Italian law. This is one of the most advanced European Union law when legal framework for RFID systems is considered. The paper will also face the important problem of the workplaces security. When implementing certain types of systems the workplaces security can be a critical issue to be addressed. In these systems the workplace security laws can affect the RFID legal framework application. Provisions of data protection can be weakened in order to fully apply workplace security laws. The article will conclude with useful legal guidelines that must be followed when implementing an RFID system for applications with workplaces security issues.

Keywords: RFID, privacy, security, workplace, data protection.

1 Introduction

The term RFID denotes any RF device that is used to identify an object or a person. An RFID system consists of as tag, a reader and a computer to which the reader is connected. An RFID tag is small wireless device. It is generally connected to an antenna. The appearance is that of a small sticker which can vary in size. An RFID tag can communicate data in response to requests from an RFID reader. This usually consists of antennae and electronic circuit. There are different versions of RFID readers some with separated antennae and circuit while some have these components integrated. Computers can have very small dimensions and usually is a build-in part of RFID reader.

The use of RFIDs is continuously increasing and today RFID market is $6.37 million with a total amount of 2.93 billion tags sold. RFIDs are increasingly used in applications demanding high security and safety such as transit, healthcare, banking, smart houses, smart environment [1], works of art authentication, passports [2]. Thus it is very important to understand the use of the RFID technology and its legal implications in the context of laws after subject.

This paper investigates the use of RFID systems in the context of the Italian law where privacy is ensured by the Data Protection directive, transposed by the Italian Code (legislative decree no. 196/2003) while security by the Workers' Statute (law no. 300/1970). Although the use of RFID systems for monitoring, identifying and

B. Papasratorn et al. (Eds.): IAIT 2013, CCIS 409, pp. 173–183, 2013.

tracking employees is not permitted exceptions are allowed. For instance when the system is shown to be objectively necessary and required for the company strategy monitoring of workers can be performed. This requires the agreement between the company and various institutional bodies. Monitoring can be also allowed when this is necessary for the heath and safety of the workers.

This papers analyzing the difficult matters of deciding when RFID systems that monitor the employee activities are allowed.

2 Remote Control of Employees' Activity : Italian Cases

The first paragraph of the article 4 of the Italian law no. 300/1970 (henceforth the Workers' Statute) prohibits the installation of audio-visual and other equipment that can be used in order to remotely control the activities of employees [3]. Although this paragraph seems to forbid the use of any monitoring technology, the second paragraph of the same law allows the monitoring of employees in the following two cases:

1. The company requires a system that is proven to be necessary for its strategy and for production purposes;
2. The company requires the monitoring for workplaces security. Even if the system has a side effect of monitoring the workers this is allowed.

This law is completed by a ministerial report. This specifies that a company can use monitoring technology for organization and production purposes when the "human dignity" is not affected [4]. The legislative decree no. 196/2003 (hereinafter the Privacy Code) must also be considered. It adds to the article 4 the concept of privacy protection. Thus when building an RFID system we need to comply with both Workers' Statute and the Privacy Code.

When monitoring of employees is legal the second paragraph of the article 4 states that the company must reach an agreement with its internal trade unions. In the case there is no trade union the company must reach an agreement with the internal committee of employees. If the agreement with the trade union and committee of workers is not achieved or these bodies do not exist the company must request the possibility of monitoring the workers to the "Inspettorato del lavoro" (Labour Office of Province). The article 4 of the Workers' Statute tells specifically about worker's activity. For instance, this includes the working time and the pause time that is the time between entering and leaving the work place. In contrast, to stress the different concept, the article 3 talks about employment that is only the working activity. It does not include activities such as coffee time and lunchtime.

The article 4 also states that "other equipment" cannot be used in order to monitor employees' activity. The term "other equipment" is so general that can include potentially any kind of technology in order to keep the law up to date with any technological advance. Generally speaking "other equipment" could include any systems for workstation security. It is therefore necessary that any equipment (that is not exclusively designed to monitor workers' activity) must perform a careful balancing between the workers' dignity and occupational safety and health in the workplaces.

With respect to the use of the monitoring technologies there are different doctrines. One is in favor of the use of monitoring technology as long as it does not violate the article 4, paragraph 2 of Workers' Statute [5]. A different doctrine is against any use of such devices [6] while another perhaps, with a more liberal spirit, states that monitoring systems can be always used when they are crucial for the organization needs. More precisely, the company should not ask the permission of any committee [7]. For instance, nowadays PCs have become essential for the organization needs, thus the article 4 should be not applied [8].

Currently we are moving into the direction of so-called "defensive controls". These are monitoring controls performed after some events have happened inside the company. The Italian Supreme Court has established that there are not absolute defensive controls. In other words, whether or not there is the need of absolute controls must be assessed in each single case depending on the monitoring purposes. The Italian Supreme Court mentioned some examples of defensive controls in the Cass. 3 April 2002, n. 4746: "certainly allowed outside the scope of the application of the rule on direct controls to detect illegal conduct (access to restricted areas such as illegal conduct) of the employee (so-called defensive controls) such as, for example, access control systems to restricted areas or, indeed, the apparatus to detect unwarranted calls.".

3 Occupational Safety and Health

The key figures concerned with occupational safety and health are the following ones, according to Italian legislative decree no. 81/2008 (hereinafter TUSL). They are listed in a top-down way considering also their active role.

- Employer: he is the person who signed the employment contract. Otherwise he can be the person who has the responsibility of his own organization or each single production unit because he can exercise decision-making powers. More precisely, he can manage the employees. Furthermore, three sub-definitions of employer can be listed. The employer can be:
  - the person who formally signs employment contract, as specified by the article 2082 of the Italian civil code;
  - the employer's delegate, who is delegated by the employer for some company functions;
  - the employer de facto, who in practice has decision-making powers.

  Therefore is possible that in a company there are more than one employer. For instance if we consider several production units, owned by the same property, we will have a different employers (responsible for each single unit) even if, formally, there is a sole company chief.

  The employer must prepare the risk assessment and police document that identifies the hazards and the control measures to safeguard employees' security and health. Moreover, the employer has to attend to the implementation of this document.

- Manager: he is the person who, for his professional and power skills, have to put in practice the employer's directives for organizing and supervising the employees' activity. More precisely, the manager is independently of any delegation (which may be or not) and he uses to play an active role in the company management, included the management of issues related to occupational safety and health. It is not necessary an employment contract (with this position) to qualify a person as a manager, but it is sufficient a "simply" situation in which this person puts in practice crucial decisions for the company. In this way there are similar skills and similar responsibilities with employer.
- Individual in charge: he is a person who has to supervise the work activity and ensure the implementation of the directives received. More precisely, he checks the correct employment performance by workers and he also exercises some management functions for his professional competence and within the limit of his functional hierarchy. Therefore, the individual in charge, according to the definition provided by TUSL, has an intermediate function: the junction between managers and employees. Indeed, the individual in charge, as the manager, is directly responsible for the failure of risk assessment and police implementation. However, in absence of any express delegation with full powers and decision-making autonomy, the individual in charge can never obtain obligations and responsibilities as the employer (or manager).
- Employee: he is a person who does a specified type of work, regardless of his employment contract, in a private or public organization, with or without salary, also in order to learn a craft, an art or a profession excluding domestic and family services. In this category, regarding occupational safety and health as provided by TUSL, we have to list also:
  - worker-members of a cooperative or corporation;
  - associate members;
  - beneficiaries for job training or guidance;
  - students from education institutions and universities;
  - participants in training courses in which they use chemical, physical and biological laboratories or equipment. This qualification is limited for all the training period;
  - volunteers.
- Responsible for occupational safety and health: he is a person, with specific professional skills, defined by the article 32 of TUSL. He is nominated by the employer, from whom depends, to coordinate the entire process of a company for occupational safety and health.

Defined those key figures, we can say that the entire topic of occupational safety and health determines not only rights and duties, but also helps to identify a unique group where all company key-figures (above-mentioned) are co-responsible in order to achieve the highest quality standards.

Obviously there are also dangerous jobs where the hazards cannot be eliminated from the beginning. In this case those hazards can and should be limited, for example, minimizing the number of workers involved in specified operations or some preventative measures can be improved to guarantee hygiene in specific locations using

appropriate equipment (a first aid stations or an acoustic system of warning, for instance). It means that there is a reasonableness limit which cannot be exceeded because, eliminating from the beginning some hazards, we would get the impossibility of execution of some job performances.

This leads us to understand how the worker's security, in the Italian legal system, is not itself an absolute value but it is a preeminent value compared to other constitutional values. The only absolute value, in this case, is that all the people are equal and they had to be protected with the same approach. More precisely, the occupational safety and health topic must be compared with other constitution principles. For instance, in our Constitutional fundamental charter we find principles of full development of the individual, free choice of employment, freedom of movement, freedom of information and protection of public order [9].

In this delicate topic the main tendency, also at supranational level, is to level up the best practices necessary to increase occupational safety and health: so it is definitely acceptable the implementation of quality standards, which are useful to limit hazards, through the use of RFID technology. For these reasons, in compliance to the balance of above-mentioned principles and to the importance of workers' safety, it is acceptable a "voluntary" standardization upwards (for instance we could find a precious allied in the international bodies for certification of processes and/or products, such as ISO standards).

4 In Depth with "Defensive Controls"

The idea of defensive controls has been developed by Italian courts and also positively appreciated by Italian doctrine. This definition allows to overcome an interpretative obstacle and permits the introduction of devices suitable for workers' monitoring but only if these devices are installed to suppress unlawful conducts. Indeed, the idea of defensive controls has led to the development of polyvalent protection both for the employer and employee when the unlawful conduct must be avoided. Without a doubt, the same idea is not oriented to censor or to cancel any workers' guarantee of dignity and privacy. More precisely, it is necessary to speak about a process ruled by the "information idea" where the employee takes part to the employer's decision. In this way the contribution of trade unions becomes fundamental: therefore we are coming back to the provision of the article 4 of the Workers' Statute where the trade unions' role is active [10].

To understand how Italian courts are interpreting the defensive control, it is necessary to quote a recent decision of the Italian Supreme Court. The court has ruled that a layoff decided by the control of some employee's e-mail can be considered legal, respecting the article 4 of Workers' Statue. The same court, based on uncontested fact, has however ruled that "the employer has implemented ex post controls, after the unlawful conduct of his employee, because he had uncovered evidence to recommend the notification of a job complaining. […] In this case the employer has used some control activities over ICT network. This conduct is not the direct monitoring of the execution of the employment performance […]. The so-called defensive control, in other words, was not about the correct fulfillment of the obligations raised from the

employment contract, but it was oriented to ascertain the employee's conduct that put in danger the same image of the company." (Cass. 23 February 2012, n. 2722).

At this point it is clear how many difficulties are arising from this topic: these uncertainties, for this part only connected to occupational safety and health, make very difficult, if not impossible, to determine when there are crossed the border of defensive controls. The employer's conduct must be controlled always with the support of trade unions and, specifically, in compliance with article 4, paragraph 2, of Workers' Statute.

5 New Technologies, Privacy and Controls

The "information idea" and the collaboration between employer and employee are becoming the central themes. We have seen how it is important the application of Workers' Statue and, in this paragraph, we are facing how the privacy legal framework can be useful to add defenses for personal data processing of employees. It is strictly connected to the paper topic because the development of any system (in this papaer is about RFID, but it could be also an NFC system), necessary to improve occupational safety and health, has to respect the data protection legal framework. In Italy, to adopt both European Union's directives 95/46/CE and 2002/58/CE, there is the legislative decree no. 193/2003 (hereafter Privacy Code).

Indeed the processing of personal data, also in workplaces, must necessary consider the provisions contained in the Italian Privacy Code. The relations between Privacy Code and Workers' Statute are very closed. More precisely, the Title VIII - Labour and Social Security (of Privacy Code), clears the field from any doubts when, both in the articles 113 and 114, refers to provisions of the articles 8 and 4 of law no. 300/1970 (Workers' Statute) [11].

Moreover we have to consider the most important decisions ruled by Italian courts and by the Italian privacy guarantor. The evolution of technologies, applied for occupational safety and health, has been constantly increased during last years. For this reason it is important to underline some decisions that have been pointed out the attention to RFID systems. It was a step-by-step way towards the RFID technologies, in fact the early decision never mentioned this kind of technology. However, these decisions are fundamental to stress the basic principle that must be followed.

For instance, connected to telephone line monitoring, the Italian Supreme Court (Cass. 3 April 2002, n. 4746) analyzed what was really the object of control. Indeed, if the object of control is the workers' activities it will apply the article 4 of the Statute (so we have the option specified by the article 4, paragraph 2, of Workers' Statute). On the other hand if the control is oriented to determine an unlawful use of working objects (so the employer is not monitoring the workers' activity), the article 4 will not apply and this system can be installed and used without any permission. The court specifies that:

- the control cannot be extended to the call content;
- the last three digits must be obscured;
- there must be an adequate privacy policy.

In sum, the criteria of proportionality (and adequacy), purpose, necessity and legality, that are the cornerstones of the entire Italian Privacy Code and European data protection legal framework, must always kept in mind.

The Italian privacy guarantor ruled with several acts (we cannot talk about sentences because the Italian privacy guarantor is an administrative authority but its decisions are anyway binding) about the data treatment combined with the evolution of technology related to the topic addressed in this paper. One relevant case was about a control system implemented by a roofing cement industry. The company management used this system, based on fingerprints detection, in order to calculate salaries. When the Italian privacy authority was invested by the case he ruled against the use of this system. More precisely, the guarantor stated doubts about the system security (it seemed vulnerable by data breaches) and he detected that the privacy policy was totally inadequate (one more time there is the "information idea"). Furthermore the authority ruled that the data treatment was certainly disproportionate and unnecessary in respect to the purpose. Indeed, in order to calculate the employees' salary should have been used a "simple" magnetic badge, without processing and archiving biometric data such as fingerprints [12].

In another case, also connected with biometrics issues, the Italian guarantor ruled in favor of using fingerprints accesses system implemented by a milling industry (processing of grain). In this circumstance the fingerprints was "detected and converted into a template encrypted smart card" and the card was in the exclusive availability of the single employee. Moreover the worker had to put the smart card into a card reader and his finger on a specific reader: the association of the two codes would open the plant doors. The Italian guarantor considered the data treatment technologically appropriate, proportionate and necessary as well. More precisely, the aim was to regulate the access to particular plant areas and only authorized personal could be admitted [13].

Following the same basic principles there is the general act of Italian guarantor entitled "Guidelines for the data treatment of private employee". This is not a case based act, but it is a general document that systematically regulate every given topic: indeed, the biometric data processing require that all fingerprints, once translated in a mathematical model and putted over a smart card, shall be deleted after 7 days (automatic deletion must be provided to avoid oversights by staff). This document confirms what the guarantor ruled with above-mentioned pronounces based on explicit cases and he adds also a specific prevision about data retention. This is a one more millstone that show the importance of personal data processing related to technology evolution.

In addiction, there is another recent decision of the Italian privacy guarantor (dated 4 October 2011) regarding vehicle tracking systems implemented by a logistic company. Also this decision is very important because of its several obiter dicta that are able to underline some principles applicable to all types of personal data processing in workplaces with the presence of new technologies. Indeed, the Italian guarantor makes explicit reference to the balancing of interests (an principles) involved. Talking about localization of vehicles with GPS systems, in order to admit this type of monitoring system, the Italian authority, in section 2.3, ruled positively about its installation. He stated that if the employer (both private and public) follows the guarantees

provided by the article 4, paragraph 2, law no. 300/1970 (Workers' Statute), the GPS monitoring system can be installed. In this case the management of his company, the topic of occupational safety and health and the trade union's involvement are all well balanced to make lawful this personal data processing and the installation of this system. Furthermore, specifies the authority, it is not necessary neither the workers' consent.

In conclusion, even if there are not specific pronounces or law about RFID technology, we can disclose that also an RFID system can be lawful installed especially in relation to improve the occupational safety and health. However the employer has to respect the basic principles listed above and the others, more detailed, showed below.

6 "Smart Labels" (RFID): The Italian Privacy Guarantor Established the Warranties for Their Use

There is a not recent document of the Italian privacy guarantor strictly related to RFID technology: it is a guideline useful to improve an efficient management of a retail distribution. It seems to be, for these reasons, far from occupational safety and health topic, but the Italian authority is also focused on the basic principles of personal data processing: in this way, even if there are different aims, we can affirm that the results are the same [14]. This document, in sum, states that the use of RFID system (but we could say any kind of technology) become relevant according to the data protection law when third parties' personal data are in. In fact, if smart labels are connect to some goods there will not be any issues, but when there are some personal data processes the data controller has to follow all the provisions up to know identified [15].

According to these guidelines, the employer has to start from the cornerstones of the data protection law when he needs to install an RFID system useful to process personal data of his employees. For this reason it is important also in relation to all the RFID systems suitable to improve workplaces security. The Italian authority lists these principles:

- principle of necessity (article 3 of Italian Privacy Code): RFID systems have be configured in order to avoid the use of personal data. These system have not to identify people (personal data subjects) unless it is strictly necessary for the purpose;
- principle of legality (article 11, paragraph 1, lett. a), of Italian Privacy Code): personal data processing is permitted only in compliance with privacy law. More precisely, the data controller always needs the privacy policy and, when required, the data subject consent. Furthermore, a specific notification, for very delicate data processing, has to be notified to the Italian privacy guarantor;
- principle of purpose and quality of personal data (art. 11, paragraph 1, lett. b), c), d) e e), of Italian Privacy Code): the controller may process personal data only for one or more specified and lawful purposes. Personal data must also be archived only for the time strictly necessary for these purposes. Moreover, personal data should also be relevant, accurate, not excessive and updated as well;

- principle of proportionality (art. 11, paragraph 1, lett. d) of Italian Privacy Code): personal data processing have not to be disproportionate according to the specified and lawful purpose.

In relation to the point no. 3 the employees' consent it is not required. In fact, the use of RFID system has to be considered as a measure included into the employment contract and for this reason it benefits of the exemption provided by the article 24, paragraph 1, lett. b) of the Italian Privacy Code. Furthermore, the employees' consent it is not necessary in according to the exemption of the article 24, paragraph 1, lett. a) of the Italian Privacy Code. Indeed, the personal data processing takes place to improve the legal obligation provided by the Legislative Decree no. 81/2008 (TUSL) and strictly related to occupational safety and health issues [16].

7 Data Retention

Defined the legal framework that must be followed to install an RFID system, it is necessary to face some issues related to data retention.

RFID systems need the archiving of personal data generated by tags records. For this reason the above-mentioned principle of proportionality becomes one more time the key point. Indeed, the temporary storage must be proportionate to one or more specific and lawful purposes decided by the employer. In fact, the data retention have to be limited for twenty-four hours subsequent to record registration. Only in some specific cases it can be provide for a longer term: for instance, in case of holidays or if personal data are required by police or judicial authorities. Even a longer data retention period can be established. This happens in some specific cases that are not listed by the law: in this way there is a discretionary fringe, but the Italian privacy guarantor recommends to not exceed over a period of seven days [17].

In all other cases, longer than a week, in which the employer wish to storage personal data, he has to notify a request to the Italian guarantor that, verified the security requirements of the RFID system, can allow an exception in order to authorize this long-lasting limit.

Nevertheless time limits above-mentioned, the RFID system must be configured in order to delete personal data automatically. It is necessary to make personal data unreadable or unusable and it is necessary also to avoid carelessness of staff that can forget to cancel data.

8 Conclusions

Personal data, occupational safety and health and Information and Communication Technology are strictly connect and RFID systems include the sum of these three main topics. All of these are contributing to improve the workplaces security but these are also oriented to care about the employees privacy as a fundamental principle (also provided by the article 8 of the Charter of Fundamental Rights of the European Union).

For this reason, to develop lawfully an RFID system in Italy, it is necessary to be in compliance with the Workers' Statute and with the data protection legal framework. To do that the employer has to follow the above-mentioned previsions about workers' activity controls (in accordance with its article 4, paragraph 2). Furthermore, the employer has to follow more delicate provisions regarding personal data processing. More precisely, to develop an RFID system lawfully, the employer has to achieve these followings points:

- Trade Unions involvement: if there is not any trade union, the employer has to involve the internal committee or (following the article 4, paragraph 2, of Workers' Statute) he has to notify a request to the "Inspettorato del lavoro" (Labour Office of Province);
- Adequate privacy policy given to the employees: it is necessary that the employees have knowledge about the RFID system. The article 13 of Italian Privacy Code states how the privacy policy has to be drafted by the employer;
- Identification of data subject: it is necessary that each RFID tag does not contain personal information. The most lawful solution is to give impersonal RFID tags containing data which are not strictly related to employees. In this case, the identification (association tag - employee) has to be able only in another phase: for instance, in case of employees' illegal conducts, judicial authorities requests, hazards and any other law provisions which require employees' personal identification. Moreover, all tags and readers have to be clearly visible and they don't have to be hidden. If it is impossible, or very hardly, to make visible these items (because of their size), the employer has to use images to disclosure readers with the purpose for which the system is established: the CCTV code of practice can be used as well because there are not specific provisions provided by law to disclosure an RFID system. Finally, the RFID system cannot constantly monitor the employees' position: for instance, to regulate accesses to some specific workplaces can be used "proximity readers", limiting their activity to entrances;
- Data retention: even if the maximum retention period can leap over a week, it is advisable the retention will not go beyond this limit;
- Security measures: the Italian Privacy Code provides some measures about security of personal data processing (articles 31, 33, 34, 35 and Appendix B). In order to achieve easily this aim, ISO/IEC 27000-series can be used to draft an efficient security policy;
- Persons in charge of processing personal data: three different persons in charge have to be listed, for three different processing areas of personal data, by the employer: a) the person who can access and process personal data relating to the RFID system functions. More precisely, he manages access levels for each impersonal tag, determining which tag is allowed in specific working areas; b) the person who can access and use the information only to perform the association tag - employee; c) the person who can access both types of personal data and he is therefore potentially able to associate employees to each entrance crossed during their activity.

References

1. Cook, D., Das, S.: Smart Environments: Technology, Protocols and Applications, p. XI - foreword. Wiley - Interscience, Hoboken (2005)
2. De Angelis, F., Gagliardi, R., Marcantoni, F., Polzonetti, A.: Ambienti Intelligenti a supporto della Sicurezza Personale in Congresso Nazionale AICA Smart Tech and Smart Innovation (AICA 2011), Turin (2011)
3. Zoli, C.: Il controllo a distanza del datore di lavoro: l'art. 4, l. n. 300/1970, tra attualità ed esigenze di riforma, Riv. it. dir. lav., vol. 04, p. 485 - foreword (2009)
4. Bellavista, A.: Il controllo sui lavoratori, Giappichelli, Torino (1995)
5. Toffoletto, F.: Nuove tecnologie informatiche e tutela del lavoratore, Giuffrè, Milano (2006)
6. Frezzi, M.: Le nuove frontiere del controllo sui lavoratori (il chip RFID), http://www.di-elle.it/index.php?url=/consultazione/approfondimenti_4/le_nuove_frontiere_del_controllo_sui_lavoratori_793/view/793/
7. Pisani, C.: I controlli a distanza dei lavoratori, in DLRI (giornale di Diritto del Lavoro e di Relazioni Industriali), p. 138 - foreword (1987)
8. Cass. Sez. V pen. 1/6/2010 n. 20722, L'ambito di applicazione dell'art. 4 dello Statuto dei Lavoratori tra finalità difensiva e caratteristiche delle apparecchiature di controllo, in Orient. giur. lav., con nota di Lorenzo Cairo, p. 323 - foreword (2010)
9. Ichino, P.: Il contratto di lavoro, in Trattato di Diritto civile e commerciale, a cura di Schlesinger P., Milano, p. 58 - foreword (2003)
10. Tullini, P.: Comunicazione elettronica, potere di controllo e tutela del lavoratore, in Rivista italiana di diritto del lavoro, vol. I, p. 323 - foreword (2009)
11. Pradelli, A.: Nuove tecnologie: privacy e controlli del datore, in Diritto e pratica del lavoro, vol. 7, p. 471 - foreword (2007)
12. The Italian data protection authority, Companies: The use of biometrics for time and attendance and working time, document n. 1664257 of 15 October 2009, http://www.garanteprivacy.it/garante/doc.jsp?ID=1664257
13. The Italian data protection authority, Processing of biometric data for the purpose of verification of the presence of employees and access to particular areas of production, document n. 1306551 of 15 June 2006, http://www.garanteprivacy.it/garante/doc.jsp?ID=1306551
14. The Italian data protection authority, RFID tags: the Italian data protection authority identifies the guarantees for their use, document n. 1109493 of 9 March 2005, http://www.garanteprivacy.it/garante/doc.jsp?ID=1109493
15. The European Union has already pronounced a Recommendation on RFID issues, but it's focalized especially on consumer protection over retail distribution. The Recommendations 2009/387/CE, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:EN:PDF
16. Cardarelli, F., Sica, S., Zeno-Zenchovic, V.: Il codice dei dati personali. Temi e problemi, Giuffrè, Milano (2004)
17. The Italian data protection authority, Video surveillance, document n. 1734653 of 8 April 2010, http://www.garanteprivacy.it/garante/doc.jsp?ID=1712680#3.4