THE PROTECTION OF WORKERS' PERSONAL DATA AND THE SURVEILLANCE BY RFID

Teresa Coelho Moreira*
tmoreira@direito.uminho.pt

ABSTRACT:

Developments in technology present a challenge from the perspective of fundamental rights, as the use of personal data in the application of new technologies has an impact on the privacy of the workers. The use of information and communications technology in the workplace, especially RFID, that allows data to be collected, stored, retrieved and processed in vast quantities and at great speed presents significant new opportunities and at the same time new threats to employers and employees, raising many questions about areas where interests and rights are in conflict and clear boundaries have to be drawn.

The technological innovation allows, through several instruments as the use of radio-frequency identification, the continuous surveillance and monitoring of the workers and new questions arise in the horizon. These new forms of control constitute powerful means of surveillance and of memorization, but also of analysis and of interference in the people' privacy, and one of the major challenges put today is the regulation of this new forms of control in the workplace. And the question that arises before the use of this technology is to know what limits should be established. And the answer is related, it seems, with the principles of data protection, being these principles the ones that we intend to analyze in this paper.

Keywords: *Privacy, Data protection, workers, RFID*

* PhD in Labour Law. Professor in the University of Minho Law School, Portugal. Member of the Human Rights Center for Interdisciplinary Research of University of Minho Law School.

I. INTRODUCTION

1.1. In 1890, in their seminal Harvard Law Review article "The Right to Privacy", SAMUEL D. WARREN AND LOUIS D. BRANDEIS lamented that '[r]ecent inventions and business methods' such as '[i]nstantenous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life'. In the same article they referred 'to the next step which must be taken for the protection of the person.'

Nowadays, protecting personal data and privacy of individuals has become increasingly important. Any content including personal data, can instantly and permanently be made accessible in digital format. The new technologies of information and communication have revolutionised our lives by removing technical and institutional barriers to dissemination and reception of information, and have created a platform for various information society services. These benefit consumers, undertakings and society at large.

But, at the same time, it has given rise to unprecedented circumstances in which a balance has to be struck between several fundamental rights, such as to conduct a business, on one hand, and protection of personal data and the privacy of individuals, on the other.

On the other hand, we know that technological evolution has radically modified human labor. Work tools and forms of organization have changed and very sophisticated methods of collecting personal information are available. Technological development permits employers to increase the efficiency of production through an intense activity of surveillance of workers' performance, which gives rise to the necessity of verifying the fall-out of technological evolution on the regulatory dynamics of human relations in workplaces.

1.2. Radio Frequency Identification is a subset of a group of technologies often referred to as automatic identification that are used to help machines identify objects, and which include bar codes and smart cards and is set to become one of the most pervasive new technologies[1].

[1] See Recommendation from the European Commission, from 12th May 2009, *On the implementation of privacy and data protection principles in applications supported by radio-frequency identification*.

RFID has a role, it seems, literally *from cradle to grave*. Some maternity hospitals are choosing, for safety purposes, to place RFID-tagged bracelets on newborn babies, and a number of old peoples' homes for similar reasons are tagging residents with dementia.

RFID has been around for a long time, one of its original uses being the identification of aircraft during the Second World War. Until some years ago it was viewed as being too expensive and too limited in functionality for many commercial applications[2]. But advances in technology have both reduced the cost of individual system components and provided increased capabilities.

The use of RFID for different purposes and applications may benefit business, individuals and public services[3]. And in reality few new technologies attract as much attention from industry, consumer organizations and politicians as RFID. The interest in RFID largely derives from the technology's rapid movement from the research lab to mass application[4].

The main components of Radio Frequency Identification technology *or* infrastructure are a *tag* (i.e. a microchip), a *reader* and the necessary supporting infrastructure (both hardware and software). The tag consists of an electronic circuit that stores data and an antenna which communicates the data via radio waves. The reader possesses an antenna and a demodulator which translates the incoming analogue information from the radio link into digital data. The digital information can then be processed by a computer.

RFID is a general term used to describe technologies that comprise the use of data stored on small chips or tags which can be communicated to a reader from a distance by means of radio transmission. There are three basic components to the technology: the RFID tags themselves, which consist of an antenna attached to a microchip, the RFID readers, and the supporting database infrastructure, hardware and software. And it is important to define the term RFID broadly, because the technical capabilities and distinctions among RF technologies will evolve over time.

---

[2] *RFID, Radio Frequency Identification OECD , RFID, Radio Frequency Identification OECD Policy Guidance – A Focus on Information Security and Privacy; Applications, Impacts and Country Initiatives*, Seoul, 17-18 June, 2008, p. 20.

[3] See for more details *Working document on data protection issues related to RFID technology* by the Article 29 Data Protection Working Party, p. 2.

[4] In the same sense see European Commission, Memo/08/145, from 5th March 2008.

An important feature of RFID technology is that tags do not require a direct line of sight for reading and may be read through hard material such as book covers or other material. Additionally, more than one tag can be read at a time. Each tag can identify the specific object to which it is attached, even if that object is one of a multitude of identical items. When using bar codes, for example, one bottle of juice has the same barcode as all other bottles of juice of that particular brand. However, RFID technology allows each individual bottle to have its own unique ID.

And the use of RFID technology is used in a variety of *sectors*. Moreover, the specific *functions* that RFID tags can deliver in the different sectors are also increasing and its possibilities are huge, raising a large number of privacy concerns.

II. WORKERS PRIVACY AND CONTROL BY RFID

1. Introduction

1.1. RFID is a technology that uses radio waves to transfer data from an electronic tag attached to an object, through a reader for the purpose of identifying and tracking the object. And RFID systems, in comparison with the previously existing access control systems make possible one essentially more accurate monitoring of employees, in which, by means of radio tags, information can be retrieved about the location, movement, or audio signals associated with their use. And this technology has improved extensively since the 1990's, the cost of RFID devices have dropped, and real-time tracking are now available, giving the possibility of individual object tracking that can be use legally for logistics operations such as warehousing and delivery. Due to their small size, these tags can be used in workplaces as an in-house pass or for other purposes and can, in radical cases even be fixed to the clothing[5]. With the help of RFID technology personal data can be handled if information with the identification data of a person, like photo, name, address, and recurring ID number, can be loaded on an RFID tag.

The control by RFID raise new challenges for personal data protection and privacy, first and foremost the issue of their invisibility or quasi-invisibility. How can compliance with the law be guaranteed in the presence of invisible technologies? Furthermore, anyone equipped with the appropriate reader can access the contents of the

[5] See DÄUBLER, *Gläserne Belegschaften? Das Handbuch zum Arbeitnehmerdatenschutz*, Bund-Verlag, Frankfurt, 2010, p. 324.

RFID tag. And a chip can contain personal data, or data that can become personal via interconnections with a database that enables a remote identification of its bearer. If all the objects of our daily life, transport cards, clothes, telephone, car, bracelet, books, cosmetics, etc., are tagged in this manner, it will then become possible to track individuals in every single act of their daily life[6].

Whenever RFID devices enable any direct or indirect identification of a physical person, then they fall under the remit of the Portuguese Data Protection Act and there are many concerns related to this treatment.

1.1.2. A first type of data protection concerns arises when the deployment of RFID technology is used to collect information that is directly or indirectly linked to personal data. A second type of privacy implication arises where personal data is stored in RFID tags. And a third and last type of data protection implication arises from uses of RFID technology which entail individual tracking and obtaining access to personal data.

Also, it is very important to remember that since the owner of an item will not necessarily be aware of the presence of an RFID tag and the tag can be read within two digits in terms of meters without the knowledge of the individual, it is possible to gather sensitive data about an individual without is consent.

1.2. Portuguese legal framework and the workers data protection

1.2.1. Workers expect to have some privacy at work, even if they are on their employer's premises and using the employer's equipment. At the same time, it is normal that working for someone will mean giving up some privacy. Employers need basic information about their employees for things like pay and benefits, and they have to be able to ensure that work is being done efficiently and safely by their workers. But the monitoring of workers and their activities can be taken to a point where the worker suffers an unacceptable loss of privacy. Such a loss of privacy will have an impact on

[6] *Vide*, *RFID, Radio Frequency Identification OECD Policy Guidance*…, cit., pp. 3-4, OCDE, *Foresight Forum "Radio Frequency Identification (RFID) Applications and Public Policy Considerations": Proceedings*, Paris, 5th October, 2005, pp. 2-3, GEORGE ROUSSOS and VASSILIS KOSTAKOS, "RFID in pervasive computing: State-of-the-art and outlook", *in Pervasive and Mobile Computing*, no. 5, 2009, pp. 111-113, and SERENA STEIN, "Where will consumers find privacy protection from RFIDS?: a Case for Federal Legislation", *in Duke Law & Technology Review*, no. 3, 2007, pp. 5-7. See, also, CAROLINA GALÁN DURÁN and ROIG BATALLA, "El uso de las etiquetas de identificación por radiofrecuencia en las empresas: un nuevo riesgo para los derechos de los trabajadores?", *in AL*, no. 8, 2010, pp. 2-3.

worker dignity and autonomy. And today, the possibilities for infringing on privacy in the workplace are greater than ever before.

Workplace privacy is an important part of the basic autonomy rights of individuals in our society. People spend a big part of their lives in the workplace. What happens in the workplace – including whether privacy is respected – can have a profound effect on employees' sense of dignity, their sense of freedom, and their sense of autonomy. Continual surveillance is dehumanizing.

The use of information technology in the workplace has grown exponentially and surveillance and monitoring have become permanent issues in the modern workplace. The growth of information and surveillance technologies, closed-circuit television and video surveillance, biometrics, genetic and drug testing, monitoring employees location by GPS in their cars or even with the resource to RFID's technology, medical exams and information for hiring or retaining an employee and ownership of personal information and have raised unprecedented concerns about privacy.

RFID systems raise new privacy risks in addition to other forms of surveillance of employee activity, such as video surveillance, because it includes both locational information and date and time information, and makes it possible to automate the tracking of workers and also to become more precisely aware of their interactions with other employees. There are certain risks that, while also present with some other surveillance technologies, must be highlighted and that are related mainly with two aspects. Firstly, the use of RFID cards for identification of goods and objects may lead to a disqualification of some activities and impose new forms of control of the workers with all the consequences that it leads at different levels including health level. Secondly, and with many implications for the workers' privacy is the opportunity that RFID has to locate and control the workers during working hours, and even on their private lives, invading their privacy[7].

1.2.2. We have to understand that one of the most disturbing aspects of the introduction of the new technology, including RFID, is related with the new forms of exercise of the electronic power of the employer, because they increased it in an unusual way, without precedents and the traditional notion of directive power established in

[7] Office of Privacy Commissioner of Canada, *Radio Frequency Identification (RFID) in the workplace: Recommendations for Good Practices*, 2008, p. 17.

Portuguese Labour Code has to be interpreted accordingly with this new power of control. It is true that this power has always existed, but the traditional surveillance and control was limited. Nowadays, the monitoring and electronic surveillance created a *qualitative jump* and we have an electronic control at distance, cold, incisive, surreptitious and seemingly to know everything, becoming possible a total control, or almost total, of all the activities of the workers' life, what makes that the worker becomes *transparent* for the employers and stops feeling free. At the present time, with these new technologies, the electronic control increased exponentially because it is much more present. [8].

1.2.3. The question that arises before the use of this technology is to know what limits should be established in the legal framework. And the answer is related with data protection and privacy because just data that is pertinent, necessary and appropriate should be collected for the lawful treatment of personal data.

Through the control by RFID the employer knows personal data of the workers and so we have to apply the fundamental principles established in the Portuguese Data Protection Act and in Portuguese Labour Code in particular the lawful principle, the transparency principle and the proportionality one; that is collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes, which implies the obligation to inform workers about the treatment.

The purpose principle is in article 5.º, No. 1, paragraph b), of the Portuguese Data Protection Act, meaning that the purposes for which data are collected shall be specified, that these purposes must be explicit, i.e. fully and clearly expressed, and that the purposes must be legitimate.

It also means that workers' personal data can only be treated if such treatment respects these principles, being essential the explicit definition of these purposes.

The data quality principle requires personal data to be relevant and not excessive for the purposes for which they are collected. Thus, any irrelevant data must

[8] *Vd.*, for more details about the electronic control, TERESA COELHO MOREIRA, *A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação: contributo para um estudo dos limites do poder de controlo electrónico do empregador*, Almedina, Coimbra, 2010, pp. 413 e ss., "As novas tecnologias de informação e comunicação e o poder de controlo electrónico do empregador", *in Scientia Iuridica*, n.º 323, 2010, pp. 554 e ss., "As NTIC, a privacidade dos trabalhadores e o poder de controlo electrónico do empregador", *in Memórias do XIV Congresso Ibero Americano de Derecho e Informática*, Tomo II, México, 2010, pp. 865 e ss., and "The Worker's privacy and the electronic control", *in Journal of Law and Social Sciences*, vol. 2, n.º 1, 2012.

not be collected and if it has been collected it must be discarded and it also requires data to be accurate and kept up-to date.

This principle comprises the truly fundamental and main principle of data protection. The other principles are all related with this legitimacy principle because data should be appropriate, pertinent and not excessive in relation the legitimate purpose; the data should be exact, complete, accurate and precise in relation with that purpose; and data should only be conserved for the time and the needs of the initial purpose.

Restrictions to the workers' privacy should respect this legitimacy principle. That is to say that even if the restrictions are acceptable in abstract, they should always be justified according to the nature of the activity and proportional to the initial purpose.

It's essential that the purpose be defined in the most concrete and accurate way because it is only with this detailed specification that we will be able to prove the proportionality of the personal data that has been treated and to check the legitimacy of all other operations that were undertaken.

The purpose intended by the employer has to be legitimate, that is, it should be in accordance with the legal and ethical framework, mainly with the fundamental rights, especially since we are dealing with a work relationship. In fact, this principle embodies an important limit to the treatment and conservation of personal data under any form, mainly imposing restrictions in the elaboration of automatic profiles based in the personal data treated.

It is also very important the conservation principle that requires personal data to be kept for no longer than is necessary for the purpose for which the data were collected or further processed.

The proportionality principle means when applied to the electronic control by RFID, that it should be given to workers the possibility to disconnect their RFID during breaks, or limit its use only to certain areas of the company and that may not be used in rest areas or outside working hours.

On the other hand, the employer, previously to the adoption of any measure of control will still have to respect the transparency principle that consists on the knowledge of the surveillance and of the control made by the employer.

The workers should be informed about the purpose of RFID tags, the personal data that is processed and where the control is made, including the location of the labels, and the period during which the information is collected. And the workers as well as

others who use this RFID, should know where the readers are and their specific location and scope.

We think that this information should be provided throw the most comprehensively and efficiently way to all workers, and that should be used also signs to indicate the presence and location of readers, such as the provisions of article 20.º No. 3, of Portuguese Labour Code in relation with the use of means of remote surveillance, that establishes that "the worker has to be explicitly informed about the existence of remote surveillance in the workplace and the employer must publicize its existence by a poster saying «Location under vigilance of video technology» or «Location under vigilance of video technology with recording of images and sound»", not being possible covert surveillance.

Also, organizations should avoid using RFID systems to collect information for disciplinary purposes prior to assessing the situation through the lens of the proportionality test.

Consent is a cornerstone of the Portuguese Data Protection Act. If an organization wishes to collect personal information using RFID technology, the organization, having notified workers of the purpose for which the information is being collected, should, normally, also obtain their consent.

However, in the employment context, employers cannot rely on consent from workers on the processing of personal data. We are dealing with an imbalance relationship and the principle of consent cannot be interpreted or use in the same way in the work relationship. This is because workers find themselves in a position of dependence upon their employers and are therefore unable to give the voluntary consent demanded by the Portuguese Data Protection Act. Consent as a legitimate ground for processing is problematic in an employment context. Based on that, we think that the consent should not provide a valid legal ground for the processing of personal data because there is a clear imbalance between the data subject – the worker-, and the controller – the employer[9].

[9] See Recital 34 and article 7, No 4, of the *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* of 25th of January of 2012, that was approved by the European Parliament on April 2014, that states that "consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context" and that reinforced this idea in article 7, No 4, saying that "Consent shall

III- CONCLUSION

The use of RFID systems in the workplace means an up-to date technological threat to our privacy.

Given the increasing use of RFID technology for a variety of purposes and applications, some of which with huge data protection implications, we have to apply the principles of privacy and data protection established in the Portuguese Labour Code and in Portuguese Data Protection Act.

And we have to remind and defend that the workers don't leave behind their rights as persons and mainly their right of privacy that includes data protection when they celebrate a labor contract. In fact, they have a founded and legitimate expectation of a certain degree of privacy in the workplace, because they develop a significant part of their relationships with other human beings in this place and there is a reasonable protection of privacy and data protection.

It seems to us, in this matter, that we should reflect upon what a German philosopher's H. JONAS said, that "not everything that is technically possible is unavoidably maintainable." In the Law field, and specifically in Labour Law, we could sustain that not everything that is technically possible is juridical acceptable. The rights to privacy and to the workers' dignity can never give in before arguments of larger productivity or larger efficiency. And if it is unquestionable that the companies should be efficient, competitive and dynamic, it is not less clear that those objectives cannot be obtained at the expense of the workers' dignity.

References:

- DÄUBLER, Wolfgang - *Gläserne Belegschaften? Das Handbuch zum Arbeitnehmerdatenschutz*, Bund-Verlag, Frankfurt, 2010

- GALÁN DURÁN, CAROLINA; and ROIG BATALLA - "El uso de las etiquetas de identificación por radiofrecuencia en las empresas: un nuevo riesgo para los derechos de los trabajadores?", *in AL*, no. 8, 2010

not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller".

- MOREIRA, Teresa Coelho - *A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação: contributo para um estudo dos limites do poder de controlo electrónico do empregador*, Almedina, Coimbra, 2010
- MOREIRA, Teresa Coelho -"As novas tecnologias de informação e comunicação e o poder de controlo electrónico do empregador", *in Scientia Iuridica*, n.º 323, 2010,
- MOREIRA, Teresa Coelho - "As NTIC, a privacidade dos trabalhadores e o poder de controlo electrónico do empregador", *in Memórias do XIV Congresso Ibero Americano de Derecho e Informática*, Tomo II, México, 2010
- MOREIRA, Teresa Coelho -"The Worker's privacy and the electronic control", *in Journal of Law and Social Sciences*, vol. 2, n.º 1, 2012
- OCDE , *Foresight Forum "Radio Frequency Identification (RFID) Applications and Public Policy Considerations": Proceedings*, Paris, 5th October, 2005
- Office of Privacy Commissioner of Canada, *Radio Frequency Identification (RFID) in the workplace: Recommendations for Good Practices*, 2008
- Recommendation from the European Commission, from 12th May 2009, *On the implementation of privacy and data protection principles in applications supported by radio-frequency identification*
- *RFID, Radio Frequency Identification OECD , RFID, Radio Frequency Identification OECD Policy Guidance – A Focus on Information Securitiy and Privacy; Applications, Impacts and Country Initiatives*, Seoul, 17-18 June, 2008
- ROUSSOS, GEORGE and KOSTAKOS, VASSILIS - "RFID in pervasive computing: State-of-the-art and outlook", *in Pervasive and Mobile Computing*, no. 5, 2009
- STEIN, SERENA - "Where will consumers find privacy protection from RFIDS?: a Case for Federal Legislation", *in Duke Law & Technology Review*, no. 3, 2007
- *Working document on data protection issues related to RFID technology* by the Article 29, Data Protection Working Party