LaBoUR & Law Issues
Rights | Identity | Rules | Equality

The Electronic Control of the Employer in Portugal

Teresa Coelho Moreira
University of Minho

vol. 2, no. 1, 2016

ISSN: 2421-2695

LaBoUR & Law Issues
Rights | Identity | Rules | Equality

The Electronic Control of the Employer in Portugal

TERESA COELHO MOREIRA
University of Minho
tmoreira@direito.uminho.pt

ABSTRACT

The way the work is made has been suffering in the last years countless changes related with the huge increase and development of the use of new information and communication technologies in the work relationship. The theme of privacy and surveillance of the employer have been turning in a matter of considerable interest and surrounded of great controversy in the last years all around the world and Portugal is no exception.

The technological innovation allows, through several instruments as the use of video surveillance, GPS, RFID, control of electronic communications, control of online social networks or the internet, 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 because the advancement of modern technology has made it possible to collect and store information on a seemingly limitless scale, while also facilitating access to it. 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, mainly, in Portugal, articles 20, 21 and 22 of Portuguese Labour Code and also the Portuguese Data Protection Act, Law number 67/98, from 26th October, and, most of all, the legitimate principle, the proportionality principle and the transparency principle.

This as led to a new form of control much more intrusive and that controls almost everything even the way the worker thinks.

Keywords: electronic control; video-surveillance; GPS; electronic communications; data protection; workers

The Electronic Control of the Employer in Portugal

SOMMARIO: 1. Introduction. - 2. The electronic control of the employer. - 3. Means of remote control – articles 20 and 21 of Portuguese Labour Code. - 4. Control of the electronic communications of the workers. - 5. Conclusions.

1. Introduction

The use of new information and communication technologies has made extensive employee monitoring and surveillance by employers inexpensive and easy and nowadays it is clear widespread and more and more organizations are monitoring their employees. Perhaps the most substantive issue raised by monitoring and surveillance in the workplace relates to the fundamental right to privacy for workers. As an EU report has put it, "Workers do not abandon their right to privacy and data protection every morning at the doors of the workplace" (1). In fact, privacy becomes even more important given that the traditional clear boundaries between work and personal time are increasingly becoming blurred through developments such as teleworking, flexible hours contracts, adaptability of working time and many other forms (2).

On the other hand, people expect to have some privacy at work, even if they are on their employer's premises. At the same time, it is normal that working for someone will mean giving up some privacy. Employers have a legitimate interest to control the activities of employees while on working time and they 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 (3). The question is that today the monitoring of employees and their activities can be taken to a point where the employee suffers an

(1) FRANK HENDRICKX, *Protection of Workers Personal Data in the European Union*, EU, 2002.

(2) In Portugal there are many possibilities of work time arrangements like the "bank if hours" – articles 208, 208-A, and 208-B, along with telework – articles 165 to 171 as other possibilities.

(3) See DÄUBLER, *Internet und Arbeitsrecht*, third edition, Bund-Verlag, Frankfurt am Main, 2004, p. 122, and ANDREA RAFFLER and PETER HELLICHE, *Unter welchen Voraussetzungen ist die Überwachung von Arbeitnehmer-e-mails zulässig?*, in *NZA*, No. 16, 1997, p. 862.

unacceptable loss of privacy that will have an impact on his dignity and autonomy (4).

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.

2. The electronic control of the employer

2.1. Today, there is a changing of the legal landscape of the right of the employer to control and monitor employees behaviour and the possibilities for infringing on privacy in the workplace are greater than ever before. Employers are increasingly keeping track of employees through many systems and can monitor and control virtually every aspect of an employee's working time - from psychological tests to web-browsing records, video surveillance, keystroke monitoring, genetic testing, RFID, control of electronic communications, online social networks and global positioning systems, among others (5). And if the employee monitoring is not new, the ability to monitor has become greatly expanded due to advances in technology. So, it seems very important to protect personal data and privacy of individuals. And nowadays any content including personal data, be it in the form of texts or audio-visual materials, can instantly and permanently be made accessible in digital format worldwide. The internet has revolutionized our lives by removing technical and institutional barriers to dissemination and reception of information, and has created a platform for various information society services. These benefit consumers, undertakings and society at large (6). But, at the same time, this has given rise to unprecedented cases in which a balance has to be struck between different fundamental rights, such as freedom of

(4) 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 *et seq*, and *The Worker's privacy and the electronic control*, in *Journal of Law and Social Sciences*, vol. 2, n.º 1, 2012.

(5) See DOUGLAS TOWN and LORNA COBB, *Notes on: GPS Technology; Employee Monitoring Enters a New Era*, in *Labor Law Journal*, 2012, p. 203 and TERESA COELHO MOREIRA, *O controlo dos trabalhadores através de sistemas de geolocalização*, in *XIX Congresso Nacional de Direito do Trabalho*, 2015.

(6) See for more information TERESA COELHO MOREIRA, *A Privacidade dos* ...cit. pp. 585 *et seq*.

expression, freedom of information, on one hand, and protection of personal data and the privacy of individuals, on the other.

2.2. The employment relationship is a perfect example of the existence of an imbalance relationship. In reality, the worker and the employer don't have the same freedom in what concerns the celebration of the contract nor the stipulation of the terms of the same, what creates the emergence of a contractual imbalance that is increased in unemployment eras as, unhappily, it happens nowadays in Portugal.

This imbalance situation has new developments with the increase of the NICT because today is a very common situation of many companies to *googalize* the candidates in the hiring process in the measure in that aids very much the person that does this process or even when they are already hired. Through a research at distance, extremely fast, free, and above all discreet, it is possible to know the intimacy of the candidates and the workers because frequently these data, sometimes very private, are in a free access, and many times are the candidates or the workers who, voluntary or involuntarily, give these information and personal data in online social networks.

This new form of electronic control allows an easy collection and gathering of the workers' personal data. Data that one finds disseminated in several sources of information, appears instantly gathered in a database without having been submitted to a previous examination.

2.3. The NICT changed the business landscape, making it far more competitive and the workplace considerably more fast-moving.

But, on the other hand, it also hastened the advent of widespread twenty-four-hour connectivity, particularly through net centric technologies.

Together, these factors led to a re-conceptualization of work time and private life, making that the concept of work-life balance gained new meaning in a highly competitive and global economy in which each worker is accessible any time, any place and employees can access their colleagues, documents, and data from just about anywhere.

Nowadays many people are "always on, always connected" and for many this has become a kind of second nature, with the raising of new problems related to health, the *right to disconnect*, and the huge increase in the power of control by the employer.

The ever growing use of electronic communication brings along the threat of a permanent connectivity, *Homo Conectus*, with a consequence of the rights of privacy and data protection being somewhat compromised.

Electronic communication networks bring along new problems and new techniques from which other problems arise: cloud computing, ambient intelligence and further possibilities of surveillance, either performed by the state authorities or by powerful third parties. The growing role of technologies in all our activities, brings along some evident effects, such as the progressive disappearance, or at least a blurring, of the borders between professional and personal, between public and private spheres. This inevitably shall have consequences also at the level of the relationship between employers and workers, having regard to the exercise of a now ever enhanced controlling power of the employer: workers may now be monitored not only in the working places, but anywhere and whatever they do.

With these NICT there are countless benefits for the workers and also for the employers, but, at the same time, these new technologies, namely the Internet, have been originating new challenges, raising new questions and the rethinking of old ones.

So, as we can see, the introduction of this new technology in the work relationship has multiple connections and many interrogations (7).

If on one side it allowed a huge reduction of the costs and the times of work and it accelerated the transmission of information, on the other hand, this revolution forced an adaptation in the ways of work organization and an enormous increase in the power of control of the employer, causing, sometimes, an *inhuman dimension* of this power.

2.4. The transformations in companies' organization in the productive structure and the changes in the organization of work originated by the introduction of the new technologies, are affecting this power of control and demanding new rationalization forms and administration of the human resources, as well as to favour the emergence of new ways of control and surveillance. If the control by the employer is not new nor forbidden, the

(7) According to the Eurobarometer, number 431, from June 2015, presented by the European Commission about Data Protection, "Respondents who said previously that they provide personal information online were asked how much control they feel they have over the information they provide. Just 15% of people in this group feel they have complete control, while half (50%) say they have partial control, and nearly a third (31%) feel that they have no control at all over their personal information online".

innovation comes from the fact that these new technologies changed this control and have a capacity to collect data that, sometimes, seems to have no limits. These new technologies can even led to a change in the power of control of the employer because the most part of the control and surveillance will be done at the distance through the computer, the smartphone and the cloud computing.

The introduction of the NICT in the companies is not a neutral instrument, but, on the contrary, it is complex and capable of change the power of control and the surveillance of the employer, directly on the *nervous system of the organization*.

We have to understand that one of the most disturbing aspects of the introduction of the new technology 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. It is true that this power has always existed, but in the traditional surveillance and control, limited, the monitoring and electronic surveillance makes a *huge jump* and today we have an electronic control «at distance, cold, incisive, surreptitious and seemingly to know everything» (8), becoming possible a total control, or almost total, of all of the movements of the workers' life, what causes that the worker become "transparent" for the employers and stop feeling free (9). At the present time, with the new technologies, the electronic control increased exponentially because it is much more present (10).

Another quality of these NICT that increases, and a lot, the possibility of the control is it ambivalent character in the measure that these technologies are used, simultaneously, as instrument to carry out the activity and as mechanism of control of the work done by the worker. It is operated, this way, a perfect concentration in the same mechanism of the activity and of control, in such a way that while the computer, or the smartphone or the laptop, is used as work instrument, it is, at the same time, providing a huge amount of data to the employers originating a direct participation of the

(8) See PATRICIA WALLACE, *The Internet in the workplace: How New Technology is Transforming Work*, Cambridge University Press, Cambridge, 2004, pp. 3-4 and also JAVIER THIBAULT ARANDA, *El derecho español*, in *Tecnología Informática y Privacidad de los Trabajadores*, Thomson Aranzadi, Navarra, 2003, p. 59.

(9) LARRY O. NATT GANTT, II, *An affront to human dignity: electronic mail monitoring in the private sector workplace*, in *Harvard Journal of Law & Technology*, vol. 8, n.º 2, 1995, p. 345.

(10) TERESA COELHO MOREIRA, *As novas tecnologias de informação e comunicação e o poder de controlo electrónico do empregador*, in *Estudos de Direito do Trabalho*, reimp., Almedina, Coimbra, 2016, pp. 14-15.

worker in his control. The worker becomes, simultaneously, an active and passive subject of a machine in such a way that is possible to accomplish a bidirectional control (11).

And with this concentration new problems have emerged because the main work tool of the workers is also the instrument that controls them, arising a new form of control much more intrusive and that controls almost everything even the way the worker thinks, because these instruments leave tracks that are immediately perceptible by the employer. It is the new *fingerprints* (12) related with different features of the person: personal, professional, political, social, that the worker leaves, consciously or not, and that through an easy and simple research in the Internet allows to build the workers and the candidates profiles. The idea of the *Big Brother* that could control everything seems old, very simple and almost a dream, when compared with these countless "Little Brothers", truly nightmares that can follow us and know everything to the tiniest detail and the ghosts of the panoptic seem very real, like strange mirrors that we look and we see a different person (13). And if we add the possibility that many companies give to their employees to bring their own devices, we can see how this control seems to have no limits. If the employer encourages his workers to bring their devices their smartphones, their tablets, their laptops, their touchscreens to the workplace, where do we draw the line? What are the limits?

And the answer is related with data protection and the positive notion of privacy because just data that is pertinent, necessary and appropriate should be collected for the lawful treatment of personal data and in Portuguese legal framework we can find some answers.

3. Means of remote control – articles 20 and 21 of Portuguese Labour Code (14)

3.1. As with other technologies, the main obstacle to the widespread implementations of instruments of remote control like video surveillance and GPS or even RFID systems was the cost of it but, nowadays, the costs are

(11) TERESA COELHO MOREIRA, *Every breath you take, every move you make*: cybersurveillance in the workplace and the worker's privacy, in *Masaryk University Journal of Law and Technology*, volume 7, n.º 1, 2013.

(12) JEAN-EMMANUEL RAY and JEAN-PAUL BOUCHET, *Vie professionnelle, vie personnelle et TIC*, in *DS*, n.º 1/2010, p. 45

(13) EMMANUEL HOOG, *apud* JEAN-EMMANUEL RAY and EAN-PAUL BOUCHET, *op.* cit., p. 45, footnote number 3.

(14) In Portuguese "meios de vigilância à distância".

falling steadily and the images or the localization can now be fed directly to the Internet. Employee monitoring can be done using minute surveillance cameras pointed directly at the selected host computer to monitor and record everything that is said and done by the worker on that specific host or it can be done by real time surveillance, including the use of Internet minute cameras or RFID or GPS instruments that record and transmit real-time information over the Internet.

Today the amount of digitalised content available online has exploded. It can be easily accessed, consulted and disseminated through social media, as well as downloaded to various devices, such as tablet computers, smartphones and laptop computers.

Pointed these examples of new uses to this type of surveillance we can see how it continues to be an issue which regularly leads to workplace disputes, particularly when these devices are installed without prior consultation or are used surreptitiously for employee performance monitoring or disciplinary purposes. It seems to us that, sometimes, the real privacy threat lies not so much in the existence of the surveillance itself, even though that is bad enough, but how and where they are deployed and the question of proportionality and transparency arise as also the issue of overt and covert monitoring of the workplace.

In several key aspects the use of surveillance cameras in the case of video surveillance today poses greater concerns than in the past, when camera images would be monitored in real time or recorded on magnetic tape (15). In reality, these new technologies transformed the nature of data processing and surveillance. Until recently the surveillance of employees and the processing of their personal data was subject to physical limitations but, now, these new technologies make intensive surveillance practical.

These days' data from cameras is more likely to be in digital form, and as such can be stored on an indefinite basis along with other digitised data. Potentially, for example, digitised data from surveillance cameras focused on individual employees could be linked to other digital data on that individual, for example HR data or data taken from email monitoring or recorded telephone conversations, forming a very powerful integrated set of

(15) *Vd.* TERESA COELHO MOREIRA, *Transparency and data protection in the workplace: the workers control by video surveillance*, in *Transparenz – Tagungsband des 17. Internationalen Rechtsinfomratik Symposions – IRIS 2014*, Oesterrechische Computer Gesellschaft, Áustria, 2014, and JOSH GREENBERG, *Supplementing panoptic paradigm: surveillance, moral governance and CCTV*, in *Theorizing Surveillance – The panopticon and beyond*, Willan Publishing, London, 2008, pp. 230-231.

information available to an employer (16). And, at the same time that cameras are shrinking in size and cost, their capabilities are expanding (17).

It is increasingly necessary in other words to see these forms of remote control not simply as a stand-alone security measure but as a source of data which is available for searching and analysis using the full power of contemporary computing.

Given this sort of development, it becomes even more important to ensure that the use of these ways of control are adequately used.

The specific features of the processing of personal information included in sound, image and localization data have been expressly highlighted by Directive 95/46/EC, which refers to them expressly in several points (18) and in Portugal by Law 67/98, that transposed this Directive, and articles 20 and 21 of Portuguese Labour Code.

3.2. In order to the use of video surveillance or GPS technology be legal, the employer has to obey to several principles related all with the protection of personal data.

The first principle is the legitimacy one meaning that just data that is pertinent, necessary and appropriate should be collected for the lawful treatment of personal data and in article 20, No. 2 of Portuguese Labour Code there are two possibilities of install this type of technology: for security of people or goods and when special features related with the activity justify that.

The employer cannot install this kind of remote control aimed directly at controlling, from a remote location, quality and amount of working activities, therefore entailing the processing of personal data in this context and that is clearly established in article 20, No 1 of Portuguese Labour Code (19). It is absolutely forbidden to use these instruments as a way to control the

(16) With the same opinion BELLAVISTA A., *Il controllo sui lavoratori*, Giappichelli, Torino, 1995, THIBAULT ARANDA, *El control multimédia de la actividade laboral*, Tirant lo Blanch, Valencia, 2006, p. 18, and GOÑI SEIN, *Controles empresariales: geolocalización, correo electrónico, Internet, videovigilância y controles biométricos*, in *Justicia Laboral*, No. 39, 2009, p. 42.

(17) As FREDERICK S. LANE III, *The Naked Employee – how technology is compromising workplace privacy*, AMACOM, USA, 2003, p. 119, if in the nightmarish *1984*, of GEORGE ORWELL, perpetual surveillance was a given and the omnipresent telescreen was warning enough that you might be under the critical eye of the Tough Police, nowadays, if GEORGE ORWELL were writing today he might felt different.

(18) And now also in the General Data Protection Regulation.

(19) "1 - O empregador não pode utilizar meios de vigilância a distância no local de trabalho, mediante o emprego de equipamento tecnológico, com a finalidade de controlar o desempenho profissional do trabalhador. 2 - A utilização de equipamento referido no

workers performance which has raise many questions and different decisions from the Appeal Courts in Portugal about whether it is possible to use as a proof in disciplinary cases the images or the data from these technologies because it can also be a proof about the performance of the workers.

The case is slightly different as regards these surveillance systems that are deployed, subject to appropriate safeguards, and occupational safety requirements and also entail distance monitoring, albeit indirectly.

We think that in some cases it is possible to use these data when we are facing a criminal offence, like theft or physical aggressions, committed by the worker. But, even in those cases, the employer cannot use as a proof the images to punish an employee if it is related with work performance (20) (21).

This principle of legitimacy comprises the truly fundamental and main principle of data protection (22). The other principles are all related with this

---

número anterior é lícita sempre que tenha por finalidade a proteção e segurança de pessoas e bens ou quando particulares exigências inerentes à natureza da atividade o justifiquem".

(20) There are many cases regarding this possibility. Recently from the *Tribunal da Relação do Porto* one from 19th of October 2015 - http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/b655a445dc93958780257b340054d89c?OpenDocument&Highlight=0,teresa,coelho,moreira –, from the *Tribunal da Relação de Lisboa* from 8th of October 2014 - http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/a7ba4c74d8f7a15780257d70004d5782?OpenDocument&Highlight=0,videovigil%C3%A2ncia , from the *tribunal da Relação de Coimbra*, 6 of February 2015 - http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/fe545bb508b68e6980257dee004bf0bd?OpenDocument&Highlight=0,videovigil%C3%A2ncia, from the *Tribunal da Relação de Guimarães*, 25 June 2015 - http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/51296bb510548a9580257eb60055f9d6?OpenDocument&Highlight=0,videovigil%C3%A2ncia.

See, for example, the case of Tribunal da Relação de Lisboa, where it was accepted as a proof the images of a worker in a casino that committed theft against his employer: "É de aceitar as imagens captadas por sistema de videovigilância como meio de prova em processo disciplinar e na subsequente acção judicial em que se discuta a aplicação de sanção disciplinar, mormente o despedimento, desde que sejam observados os pressupostos que decorrem da legislação sobre a protecção de dados e concomitantemente se conclua que a finalidade da sua colocação não foi exclusivamente a de controlar o desempenho profissional do trabalhador. Num quadro circunstancial assim apurado, o trabalhador não merece – nem a lei lhe confere - maior protecção do que aquela que é conferida aos demais cidadãos e, logo, o meio de prova é lícito e admissível".

(21) For more developments and with the analysis of more cases see TERESA COELHO MOREIRA, *A Privacidade dos* Trabalhadores…, cit., pp. 439 *et seq.*, and *Estudos de Direito do Trabalho*, reimp., Almedina, Coimbra, 2016.

(22) BELLAVISTA A., *I poteri dell' imprenditore e la privacy del lavoratore*, in *DL*, Vol. 76, No. 3, 2002, p. 152, GRAGNOLI E., *La prima applicazione della lege «sul trattamento dei dati personali» ed il rapporto di lavoro privato*, *in RCDP*, No. 4, 1997, p. 703, and AIMO M.P., *I «lavoratori di vetro»: regole di trattamento e meccanismi di tutela dei dati personali*, in *RGL*, No. 1, 2002, pp. 106-107.

legitimacy principle because data should be appropriate, pertinent and not excessive in relation the legitimate purpose; 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 in abstract acceptable in abstract, they should always be justified according to the nature of the activity and proportional to the initial purpose (23).

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 represents 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.

3.3. Another very important principle is the principle that data must be adequate and proportionate to the purposes. This principle means that this equipment may only be deployed on a subsidiary basis that is to say for purposes that actually justify the use of such systems, as established in article 21, No. 2, of Portuguese Labour Code (24).

The principle under which data must be adequate, relevant and not excessive entails careful assessment of the proportionality of the arrangements applying to the data processing once the lawfulness has been validated (25).

The filming arrangements will have to be taken into account in the first place, by having regard, in particular, to the following issues: the visual angle as related to the purposes sought the type of equipment used for filming, *i.e.*, whether fixed or mobile; concrete installation arrangements, like, *inter alia*, location of cameras, use of fixed view and/or movable cameras; possibility of magnifying and/or zooming in images either at the time the latter are filmed

(23) JEAN SAVATIER, *La liberté dans le travail*, in *DS*, No. 1, 1990.

(24) "A autorização só pode ser concedida se a utilização dos meios for necessária, adequada e proporcional aos objetivos a atingir".

(25) See TERESA COELHO MOREIRA, *A Privacidade dos Trabalhadores...*,cit., pp. 500-502, and GOÑI SEIN, *La Videovigilancia Empresarial y la Protección de Datos Personales*, Thomson Civitas, Navarra, 2007, p. 123.

or thereafter, *i.e.*, as regards stored images; it is necessary to consider the decision to be taken as to retention of images and retention period. This latter one has to be quite short and in line with the specific features of the individual case (26).

3.4. The last but not the least important principle that the employer has to respect is the principle of transparency which is directly connected with the problem of covert surveillance.

Openness and appropriateness in the use of this surveillance equipment entail the provision of adequate information to data subjects pursuant to article 20, No 3, of Portuguese Labour Code (27). This article establishes that

(26) There is a Decision of the Portuguese Supreme Court – Supremo Tribunal de Justiça - from 8th February of 2006 - http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/65e859e4729cc7688025712d00421026?OpenDocument&Highlight=0,videovigil%C3%A2ncia, that dealt with this principle of proportionality.- This Decision is also very important because it clarified the meaning of "security reasons" and we think it is a very important clarification. "Protecção da segurança das pessoas e bens, enquanto finalidade específica da recolha e tratamento de dados pessoais, tem em vista a prevenção da prática de crimes, o que pressupõe, pela natureza das coisas, que a utilização de videovigilância com esse objectivo deva reportar-se a locais onde exista um razoável risco de ocorrência de delitos contra as pessoas ou contra o património. E isso tanto é válido para a utilização de câmaras de vídeo pelas forças policiais relativamente a espaços públicos (conforme resulta expressamente do disposto no artigo 2º, n.º 1, alínea c), da Lei n.º 1/2005), como para a vigilância em instalações ou estabelecimentos privados. Neste último caso, o risco é potenciado essencialmente pela circunstância de se tratar de locais abertos ao público, e decorre da eventualidade de esses locais serem frequentados por pessoas anónimas sem possibilidade de qualquer prévio controlo de identificação". On the other hand it was decided that "Não se prova, em suma, que exista uma situação de mera captação difusa de imagens, com intersecção de diversos planos de movimento, e dirigida apenas à detecção de factos, situações ou acontecimentos incidentais, num circunstancialismo externo de potencial risco para os interesses patrimoniais ou a integridade física das pessoas. Antes se constata que se verifica uma incidência directa e necessariamente constrangedora sobre o campo de acção dos trabalhadores, and "A colocação de câmaras de vídeo em todo o espaço em que os trabalhadores desempenham as suas tarefas, de forma a que estes se encontrem no exercício da sua actividade sob permanente vigilância e observação, constitui, nestes termos, uma intolerável intromissão na reserva da vida privada, na sua vertente de direito à imagem, e que se não mostra de nenhum modo justificada pelo simples interesse económico do empregador de evitar a desvio de produtos que ali são manuseados".

(27) In Portugal there are many Decisions from the Appeal Courts about this principle. For example from the Tribunal da Relação do Porto there is a very interesting case from 17th of December of 2014 - http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/d8b30e6de8712dd580257dc700551703?OpenDocument&Highlight=0,teresa,coelho,moreira , where the employer used as proofs in a dismissal case images that he had collected by remote video surveillance without the prior knowledge of the employer and without the specific authorization of the

"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".

However, in our opinion, we have to make a broader interpretation of this information because it is also applicable to GPS devices, RFID and web surveillance.

The employees along with other persons that visit the employer's premises, should be aware of the fact that this surveillance is in operation, even where the latter is related to public events and shows or to advertising activities. They should be informed in a detailed manner as to the places monitored. It is not necessary to specify the precise location of the surveillance equipment, but, nevertheless, the context of surveillance is to be clarified unambiguously and the information should be positioned at a reasonable distance from the places. Information must be given to employees and every other person working or visiting the premises. This should include the identity of the controller and the purpose of the surveillance and other information necessary to guarantee fair processing in respect of the data subject, for instance in which cases the recordings would be examined by the management of the company, the recording period and when the recording would be disclosed to the law enforcement authorities. However, the provision of information through a symbol cannot be considered as sufficient in the employment context.

The Portuguese Labour Code in articles 20 and 21 stresses the importance of key data protection principles, including the proportionality of use and prior notification of those subject to surveillance. In the particular context of the workplace, it is important to highlight the safeguarding of employees' "rights, freedoms and dignity". Surveillance is absolutely forbidden in premises that either are reserved for employees' private use or are not intended for the discharge of employment tasks – such as toilets, shower rooms, lockers and recreation areas, like the places where the employees eat.

It is also important to notice that the images collected exclusively to safeguard property or detect, prevent and control serious offences should not be used to charge an employee with minor disciplinary breaches (28). It is also

Portuguese Data Protection Authority – CNPD. The proofs were considered inadmissible and the dismissal was found to be invalid.

(28) This is one of the most frequently cases in courts: the use of the images to disciplinary and punish employees.

crucial to highlight that employees should always be allowed to lodge their counterclaims by using the contents of the images collected (29).

There is some discussion around the issue of the possibility of covert surveillance because it presents particular concerns and it is not admissible in Portugal and in many European Countries. In Portugal if the employer uses the images as a proof it is not going to be accepted in courts because it is considered a clear violation of the principle of transparency and good faith (30).

3.5. According to article 21, No.1, it is crucial that prior to the installation of this technologies there is an authorization of the Portuguese Data Protection Authority (31). Without this any proof will be considered unlawful.

There is also the need to have an opinion of the workers' council, according to article 21, No. 4 (32). However this opinion is not binding and the employer can use these technologies even if the opinion of the workers' council is negative. He only needs the authorization of the Portuguese Data Protection Authority. Therefore, the employer, which is the data controller, cannot carry out any data processing operations before the Portuguese Data Protection Authority – CNPD - issues the due authorization.

3.6. The principles established in articles 20 and 21 of Portuguese Labour Code also apply to the use and control by GPS and there is even in the Portuguese Data Protection Authority site a form that all employers have to

(29) In Portugal we have cases where the employees asked to use as a proof the images in a litigation case, like the case of Tribunal da Relação do Porto, 9th February 2015, where it was decided that "O trabalhador pode autorizar o uso das imagens captadas por videovigilância para prova dos factos".

And there are cases related with the possibility of the employee to put an end to his labour contract due to the fact that he was put under surveillance without his knowledge – *vide* case from the *Tribunal da Relação do Porto* from 4th of March of 2013 - http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/b655a445dc93958780257b340054d89c?OpenDocument&Highlight=0,teresa,coelho,moreira – about this issue.

(30) The ILO accepts the secret monitoring only if: (a) if it is in conformity with national legislation; or (b) if there is suspicion on reasonable grounds of criminal activity or other serious wrongdoing. See *Protection of workers' personal data*, 1997, p. 10.

(31) Comissão Nacional de Proteção de Dados.

(32) "O pedido de autorização a que se refere o n.º 1 deve ser acompanhado de parecer da comissão de trabalhadores ou, não estando este disponível 10 dias após a consulta, de comprovativo do pedido de parecer".

fill in order to ask for the authorization prior to the installation of this means (33).

We also think that it should be applicable to cases of RFID, because 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 (34) (35).

4. Control of the electronic communications of the workers.

4.1. These new forms of control constitute powerful means of control and memorization, but also of analysis and of interference in the people' privacy, and one of the major challenges put today is the regulation of the electronic communications in the workplace, because the advancement of modern technology, notably computers and the Internet, has made it possible to collect and store information on a seemingly limitless scale, while also facilitating access to it.

The electronic control of the employer becomes, many times, potentially vexatious, continuous and total, bringing, inclusively, risks for the workers' health, so much physical, as psychic, namely for knowing or to feel constantly watched. This can provoke a great pressure psychological that it can drive, *inter alia*, to cases of occupational stress, burn-out syndrome, depressions and *mobbing*.

In Portuguese Labour Code there are special provisions related with the control of electronic communications in article 22 that is related with the

(33) https://www.cnpd.pt/bin/Duvidas/frm_geolocalizacao.aspx.

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

(35) For more developments see, among others, TERESA COELHO MOREIRA, *Estudos...*, cit., p. 145 *et seq.*, and *The protection of workers' personal data and the surveillance by RFID in Portugal*, in *Journal of Law and Social Sciences*, Vol. 3, No. 1, 2013.

"confidentiality of messages and access to information" (36). This article establishes this right not only to e-mail but all other forms of communication, including *messenger* (37) and online social networks (38).

In the case of e-mails the employer will have to pay attention to the whole constitutional protection and not only to the right of privacy. He has to respect, above all, to the right established in article 34 of the Portuguese Constitution and that is the secrecy of communications. This principal is established in our Constitution but also at a criminal and labour law level and the employer has to obey to all these principles when he intends to regulate the control of the workers' e-mails.

Having in mind this legal framework the employer cannot appeal to his power of control to limit the exercise of the constitutional right established in article 34 and, also, in article 22 of the Portuguese Labour Code, that establishes in number 1 that "The employee is entitled to reserve and to the confidentiality of contents of personal messages and access to non-professional information sent, received or consulted, namely through e-mail", and in number 2 – "The preceding clause does not prejudice the employer's right to establish rules regarding the use of undertaking's electronic resources, namely e-mail".

Even if the computer used by the worker is property of the employer, it doesn't justify the access to the electronic communications made by the

(36) "Confidencialidade de mensagens e de acesso a informação".

(37) It is worth mention a case of the *Tribunal da Relação de Lisboa* from 7th of March 2012 http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/109499c90995e66d802579bf0050cfa4?OpenDocument&Highlight=0,messenger – that dealt with the use of *messenger* by an employee using the employer's equipment. In this case it was decided that communications using *messenger* where protected by article 22 of Portuguese Labour Code and also by the Portuguese Constitution and Portuguese Criminal Code. *Vd.* TERESA COELHO MOREIRA, *Controlo do Messenger dos trabalhadores: anotação ao acórdão do Tribunal da Relação de Lisboa de 7 de Março de 2012*, in *Prontuário de Direito do Trabalho*, n.ºs 91/92, 2014.

(38) When using the possibilities of messenger in an online social network or the e-mail, there should be given the same legal protection. See two cases from Portugal that analysed the dismissal of workers using *facebook* and criticizing the employer. TERESA COELHO MOREIRA, *Até que o Facebook nos separe: análise dos acórdãos do Tribunal da Relação do Porto de 8 de Setembro de 2014 e do Tribunal da Relação de Lisboa de 24 de Setembro de 2014*, in *Prontuário de Direito do Trabalho*, forthcoming, *A privacidade dos trabalhadores e a utilização de redes sociais online: algumas questões*, in *Questões Laborais*, n.º 41, 2013, and *The digital to be or not to be: privacy of employees and the use of online social networks in the recruitment process*, in *Journal of Law and Social Sciences*, Vol. 2, No. 2, 2013.

employee (39). The labour contract doesn't convert the employer in an active part of the private message. The employer is a third part in the personal e-mails and the access to the content of the sent e-mails or received by the worker can violate the constitutionally right of the secrecy of communications (40).

In fact, the control exercised by the employer has always to respect the human dignity.

The employer is limited in his power of electronic control and he cannot control the content of the personal e-mails and, at this point, we should made some distinctions.

First of all we should make a distinction between professional e-mails and personal e-mails, even if, sometimes, the distinction is very difficult.

But, before doing that, we have to distinguish between received e-mails and sent e-mails. The employer must assure that workers can eliminate received e-mails whose entrance in their mailbox are not able to control, like spam, and so on, and that sometimes are more related with a bad security of the employer than with a voluntary behaviour of the workers.

Second, we consider that it is better to separate professional e-mails from personal ones regarding different ways of control by the employer.

---

(39) Regarding this part there are also some jurisprudence about it. From the Supremo Tribunal de Justiça there is the case from 5th of July of 2007, *Tribunal da Relação do Porto*, from 8th of February of 2010, and Tribunal da Relação de Lisboa, from 5th of June 2008 and 30th of June 2011 – www.dgsi.pt. On these cases it was decided that "não é pelo facto de os meios informáticos pertencerem ao empregador que afasta a natureza privada da mensagem e legitima este a aceder ao seu conteúdo". Also, in the case of the *messenger* the Court decided that "Também não nos parece válido o argumento jurídico desenvolvido pela Ré no sentido dos referidos acesso e conhecimento serem permitidos pela circunstância das referidas conversas/mensagens se acharem guardadas no servidor central da empresa, a ela pertencente, pois, por um lado, não perderam a sua natureza de pessoais e confidenciais por esse facto e, por outro, face a tal justificação, não se vê porque a entidade empregadora, em função da simples propriedade sobre o computador profissional distribuído à Autora, não poderia proceder da mesma forma, para o caso desse registo estar conservado no disco rígido daquele. Essa tese, levada a um extremo, conduziria a resultados absurdos, franqueando à administração da Apelante ou aos funcionários em que delegasse tais tarefas, a possibilidade de, querendo, abrir as carteiras e fiscalizar o conteúdo das malas ou dos telemóveis dos trabalhadores pelo singelo facto de estarem guardados dentro de gavetas ou armários colocados dentro das suas instalações e de todo o mobiliário e demais equipamento existente na empresa lhe pertencer ou lhe estar afecto por um título jurídico legítimo, o mesmo se podendo dizer com referência às viaturas particulares estacionadas no seu parque ou garagem, caso existam."

(40) See INMACULADA MARÍN ALONSO, *El poder de control empresarial sobre el uso del correo electrónico en la empresa – su limitación en base al secreto de las comunicaciones*, Tirant monografias, Valencia, 2005, pp. 159-160.

It seems to us excessive to include inside the protection of the secrecy of the communications the professional e-mails in the case of existing a prior clear policy concerning the use of these and separate bill accounts from e-mails. In the case of the professional e-mails there is a professional relationship between the worker and the employer and the last one can control the content of these messages, but only if he respects all of the requirements for a correct control, mainly the principle of proportionality, good faith and transparency. However, this control has to be the least intrusive.

Nevertheless, the employer cannot control everything because there is the Data Protection Act and the principles laid down in Portuguese Labour Code, namely the legitimacy of the purpose and of the compatibility with this purpose, and all the principles of the electronic control of the employer, mainly the principle of proportionality and transparency.

When there is a clear policy concerning the use of these means with the establishment of proportional limits, in agreement with the principle of good faith and that the workers know, respecting the principles of information and publicity, we believe that it should be considered lawful the access of the employer to the worker's professional e-mail without the need of a prior judicial authorization.

Nonetheless, this type of control cannot be permanent and should respect the principle of proportionality. And the opening and reading of these e-mails should be exceptional, and should happen only in the worker's presence, unless he is not there for some reason and that is exactly the cause of the visualization.

We believe that is necessary the presence of an objective reason for the exercise of this control and surveillance and that it cannot be acceptable arbitrary, indiscriminate or exhausting controls of the workers e-mails. If this happens, this control is illicit and unlawful because it violates the principles that have to be present when the employer decides to control, mainly the transparency, the proportionality and good faith.

On the other hand, the employer has to respect the principle of the adequacy which means that he cannot know or control more than what is necessary according with the principle of legitimacy and using the less intrusive techniques respecting the principle of proportionality.

4.2. In the case of messages marked as personal or of messages that are not qualified as such but that is deemed by the content of the external data

that are personal, the situation is totally different (41). In these cases the messages are protected by the right to the secrecy of the communications established in article 34 of the Portuguese Constitution and also in article 22 of our Labour Code. The employer cannot control the content of these messages not even in exceptional situations when there are suspicions of abuse. Any act of interception of the communication contained in this part of the mail box will constitute a violation of the articles referred previously, and the obtained proof will be considered null and unlawful - article 32, No. 8, of Portuguese Constitution.

The employer, before reasonable suspicions of contractual infringements by the worker, cannot control the content without a prior judicial authorization, as established in article 34 of the Portuguese Constitution.

4.3. In the case of a lack of a clear policy about the use of these electronic communications or even if that exists, but allows a random use of the same, that is, in the case that the worker has only one e-mail account and he uses it for personal or professional the answer is not an easy one. In these cases it seems to us that the e-mail will be protected by the right to the secrecy of the communications enjoying, in principle, the inviolability of this right.

4.4. The employer, in spite of not controlling the content of the messages in the case of the personal e-mails, will be able to control some external data to try to see if the workers are using correctly or not these instruments of communication.

It seems to us that it is necessary to protect, in a certain way, the interests of the employer and, for that, if it was not permitted to control these data he would be without any possibility of control.

In the defence of this opinion we can add another argument established in Directive 2002/58/EC Article 6, No. 2, that "Traffic data necessary for the purposes of subscriber billing and interconnection payments may be

(41) See Decision of the Supremo Tribunal de Justiça of 5th of July of 2007 establishing that "a falta de referência prévia, expressa e formal da "pessoalidade" da mensagem não afasta a tutela prevista no art. 21.º, n.º 1 do CT." And that "Tendo o Director da Divisão de após Venda acedido à pasta de correio electrónico, ainda que de boa fé por estar de férias a destinatária da mensagem em causa, e tendo lido esta, a natureza pessoal do seu conteúdo e a inerente confidencialidade impunham-lhe que desistisse da leitura da mensagem logo que se apercebesse dessa natureza e, em qualquer caso, que não divulgasse esse conteúdo a terceiros".

processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued", as well as article 6, No. 2, paragraph b), of the Law n.º 41/2004, of August 18, that transposed this Directive. As we can see, the Directive accepts in certain circumstances, the possibility of the treatment of certain traffic data.

The problem is knowing what type of external and traffic data the employer can control.

He has at his disposal, without violating the fundamental right of secrecy of communications, enough juridical means to control and to sanction the worker's improper behaviour. He can control, *verbi gratia*, the cost of the work tool, the time spend for the workers in the use of the same and the access to the internet. He can even control data traffic, that, although in principle is protected by the right to the secrecy of communications, through the new characteristics of these means, becomes patent as it will be the case of the control of the senders of the messages, of the subject, of the type of attachment and its size, as well as the number of sent messages, and the time of permanence in the Internet. By controlling these circumstances, the employer, applying the principle of good faith can gather proofs for a disciplinary case, based in an inadequate or abusive use of the work instruments.

But even the control of professional e-mails has to obey to the principle of minimalist data processing, meaning that personal data has to be erased or rendered anonymous once it is no longer required for the purposes for which it has been kept. The employer has to take all reasonable steps to ensure that the data is not factually misleading. This is particularly so where the data is used to make decisions with respect to specific individuals.

4.5. The employer, previously to the adoption of any control has to respect the principle of transparency. The workers have to be informed of how, where and when the control is made. The employers have to inform with precision the limits to the use of these new technologies, limits that should be reasonable and not excessive in relation to the initial purpose. It is absolutely indispensable that the workers know the limitations in the use of these new ways of communication.

The employer, in respect of this transparency principle and the good faith has to allow his workers an explanation of his policy regarding the use and control of these communications. The employer should supply the workers the indications about the use of the electronic mail inside of the

company, describing the ways the means of communication of the company can be used for personal communications by the workers, namely the limitation of the hours and the duration of the use, seeming also, in line with what was established in the *Working Document on the Surveillance of Electronic Communications in the Workplace* by the Article 29 Working Party, *inter alia*, if a worker is entitled to a electronic mailbox for merely personal use, if the use of webmail mailboxes is allowed in the work and if the employer recommends the use for workers of a webmail mailbox for merely personal use. He should inform, also, on the period of storage of a possible copy of safety and information on when and how the messages are definitively destroyed.

We think that the most appropriate way to accomplish this transparency principle is the elaboration of *rules of good conduct related with informatics* or a kind of *Charters of informatics* about the use of this type of communication instruments, the internal rules and obeying to all the legal formalities (42).

In these *Charters* the employer should settle down the right of each worker to a personal mailbox of e-mail, in the measure that is preferable to the separation between personal mailboxes and professional ones, or, at least, to the possibility to have a personal folder inside the normal mailbox; it should still be permitted the voluntary encryption of the personal communications; the worker can use the e-mail for his communications with the trade unions and with the public administration for personal and professional subjects, as well as with third parties when he has personal needs. However in these *Charters* it could be included that personal e-mails should be legal and not include scandalous statements, or to harass people or to discriminate anyone based in their origin, race, ethnics, age, disability, nationality, sex, gender, sexual orientation, religion or belief (43).

---

(42) In the same sense, *inter alii*, AALBERTS, TOWNSEND, WHITMAN e SEIDMAN, *A proposed model policy for managing telecommunications-related sexual harassment in the workplace*, in *Labor Law Journal*, 1997, p. 617, STENICO E., *L'eserzicio del potere di controllo «informático» del datore di lavoro sugli strumenti tecnologici di «ultima generazione»*, in *RGLPS*, I, 2003, pp. 131-132, JAY KESAN, *Cyber- working or Cyber-Shrinking?: a First Principles Examination of Electronic Privacy In the Workplace*, in *Florida Law Review*, vol. 54, 2002, pp. 299-300, JENNIFER FISHER, *Implications of electronic mail policies for fairness and invasion of privacy: a field experiment*, University of Albany, 2002, *in* www.proquest.com, p. 3, ROGER BLANPAIN, *Some Belgian and European Aspects*, in *Comp. Labor Law & Pol'y Journal*, vol. 24, 2002, cit., p. 58, and WILLIAM BROWN, *Workplace Privacy and Technological Control*, University of Pittsburgh, 2003, *in* www.proquest.com, p. 14.

(43) RODRIGUÉZ-PIÑERO ROYO e LÁZARO SÁNCHEZ, *Hacia un tratamiento integrado de la comunicación electrónica no professional*, in *Relaciones Laborales y Nuevas Tecnologías*, La Ley, Madrid, 2005, , pp. 39-40.

But also the professional e-mails cannot contain any of these situations and the worker that violate these rules can be sanctioned, as it happened in France where a commercial sent to his customers e-mails containing attachments with pornographic pictures "to improve the professional relationships" with the same ones. The worker was dismissed, decision confirmed by the *Cour of Cassation*, on October 22, 2008 (44).

The employer, in the *Charters of Good Conduct* about the use of these communications, can establish limits as for the time that the workers can be using them, as well as to the type of attachments that they can sent, limiting certain types that can be related with crimes.

These *Charters* have to settle down rules on the access to the e-mails when the workers are temporarily absent, and that is exactly the reason why the employers can and have to control the workers' professional electronic mailbox. In these cases the workers are previously informed about this situation and have given their previous consent, although once again we reaffirm that such permission doesn't legitimate the possibility of the employer to open or to read the worker's private correspondence. When the worker is absent the *Charters* should establish the need to create an instantaneous message of warning for the worker's contacts and, if necessary, the e-mail of who is responsible for continuing to answer to the workers professional e-mails. On the other hand, these responsible workers should always be the same ones and should only be the ones to have access.

The workers have the obligation to distinguish correctly the e-mails of professional nature and the ones of personal nature, assuming the obligation of not classify professional e-mails as personal and vice-versa, owing the company to assume as professional all the e-mails that are not qualified as personal (45).

5. Conclusions

The use of new information and communication technologies have spread rapidly in recent years. This raises numerous questions for employers, employees and their representatives, especially in terms of the relationship between workers' privacy and employers' need to control. However one must not forget that even if with this new technologies it is technically possible to

(44) JEAN-EMMANUEL RAY, *Actualités des TIC*, in *DS*, No. 3, 2010, p. 273.

(45) TERESA COELHO MOREIRA, *A Privacidade dos Trabalhadores*…, cit., pp. 782 *et seq.*, and *The worker's privacy and electronic control*, in *Journal of Law and Social Sciences*, Vol. 2, No. 1.

control almost everything without the employee's knowledge, legally that is not admissible and employer cannot control everything or surreptitiously his employees because it is a clear violation of the principles laid down in Portuguese Constitution and in Portuguese Labour Code.

We have to remind and defend that the workers don't leave behind their rights as persons and mainly their right of privacy when they celebrate a labour 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 at work.

References.

AALBERTS, TOWNSEND, WHITMAN e SEIDMAN, *A proposed model policy for managing telecommunications-related sexual harassment in the workplace*, in *Labor Law Journal*, 1997, p. 617.

AIMO M. P., *I «lavoratori di vetro»: regole di trattamento e meccanismi di tutela dei dati personali*, in *RGL*, No. 1, 2002, p. 106.

ALONSO I. M., *El poder de control empresarial sobre el uso del correo electrónico en la empresa – su limitación en base al secreto de las comunicaciones*, Tirant monografias, Valencia, 2005.

ARANDA T., *El control multimédia de la actividade laboral*, Tirant lo Blanch, Valencia, 2006, p. 18

BELLAVISTA A., *Il controllo sui lavoratori*, Giappichelli, Torino, 1995.

BELLAVISTA A., *I poteri dell' imprenditore e la privacy del lavoratore*, in *DL*, Vol. 76, No. 3, 2002, p. 152.

BLANPAIN R., *Some Belgian and European Aspects*, in *Comp. Labor Law & Pol'y Journal*, vol. 24, 2002, p. 58.

BROWN W., *Workplace Privacy and Technological Control*, University of Pittsburgh, 2003, *in* www.proquest.com, p. 14.

COELHO MOREIRA T., *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 *et seq*, and *The Worker's privacy and the electronic control*, in *Journal of Law and Social Sciences*, vol. 2, n.º 1, 2012.

COELHO MOREIRA T., *Every breath you take, every move you make*: cybersurveillance in the workplace and the worker's privacy, in *Masaryk University Journal of Law and Technology*, volume 7, n.º 1, 2013.

COELHO MOREIRA T., *The protection of workers' personal data and the surveillance by RFID in Portugal*, in *Journal of Law and Social Sciences*, Vol. 3, No. 1, 2013.

COELHO MOREIRA T., *Até que o Facebook nos separe: análise dos acórdãos do Tribunal da Relação do Porto de 8 de Setembro de 2014 e do Tribunal da Relação de Lisboa de 24 de Setembro de 2014*, in *Prontuário de Direito do Trabalho*, forthcoming, *A privacidade dos trabalhadores e a utilização de redes sociais online: algumas questões*, in *Questões Laborais*, n.º 41, 2013.

COELHO MOREIRA T., *The digital to be or not to be: privacy of employees and the use of online social networks in the recruitment process*, in *Journal of Law and Social Sciences*, Vol. 2, No. 2, 2013.

COELHO MOREIRA T., *Transparency and data protection in the workplace: the workers control by video surveillance*, in *Transparenz – Tagungsband des 17. Internationalen Rechtsinfomratik Symposions – IRIS 2014*, Oesterrechische Computer Gesellschaft, Áustria, 2014.

COELHO MOREIRA T., *Controlo do Messenger dos trabalhadores: anotação ao acórdão do Tribunal da Relação de Lisboa de 7 de Março de 2012*, in *Prontuário de Direito do Trabalho*, n.ºs 91/92, 2014.

COELHO MOREIRA T., *O controlo dos trabalhadores através de sistemas de geolocalização*, in *XIX Congresso Nacional de Direito do Trabalho*, 2015.

COELHO MOREIRA T., *As novas tecnologias de informação e comunicação e o poder de controlo electrónico do empregador*, in *Estudos de Direito do Trabalho*, reimp., Almedina, Coimbra, 2016, p. 14.

DÄUBLER W., *Internet und Arbeitsrecht*, third edition, Bund-Verlag, Frankfurt am Main, 2004, p. 122.

FISHER J., *Implications of electronic mail policies for fairness and invasion of privacy: a field experiment*, University of Albany, 2002, *in* www.proquest.com, p. 3.

GRAGNOLI E., *La prima applicazione della lege «sul trattamento dei dati personali» ed il rapporto di lavoro privato*, *in RCDP*, No. 4, 1997, p. 703.

GREENBERG J., *Supplementing panoptic paradigm: surveillance, moral governance and CCTV*, in *Theorizing Surveillance – The panopticon and beyond*, Willan Publishing, London, 2008, p. 230.

HENDRICKX F., *Protection of Workers Personal Data in the European Union*, EU, 2002.

KESAN J., *Cyber- working or Cyber-Shrinking?: a First Principles Examination of Electronic Privacy In the Workplace*, in *Florida Law Review*, vol. 54, 2002, p. 299.

LANE III F. S., *The Naked Employee – how technology is compromising workplace privacy*, AMACOM, USA, 2003, p. 119.

NATT GANTT L. O., II, *An affront to human dignity: electronic mail monitoring in the private sector workplace*, in *Harvard Journal of Law & Technology*, vol. 8, n.º 2, 1995, p. 345.

RAFFLER A. and HELLICHE P., *Unter welchen Voraussetzungen ist die Überwachung von Arbeitnehmer-e-mails zulässig?*, in *NZA*, No. 16, 1997, p. 862.

RAY J.E. and BOUCHET J.P., *Vie professionnelle, vie personnelle et TIC*, in *DS*, n.º 1/2010, p. 45.

RAY J.M., *Actualités des TIC*, in *DS*, No. 3, 2010, p. 273.

RODRIGUÉZ-PIÑERO ROYO e LÁZARO SÁNCHEZ, *Hacia un tratamiento integrado de la comunicación electrónica no professional*, in *Relaciones Laborales y Nuevas Tecnologías*, La Ley, Madrid, 2005, , pp. 39-40.

SAVATIER J., *La liberté dans le travail*, in *DS*, No. 1, 1990.

SEIN G., *La Videovigilancia Empresarial y la Protección de Datos Personales*, Thomson Civitas, Navarra, 2007, p. 123.

SEIN G., *Controles empresariales: geolocalización, correo electrónico, Internet, videovigilância y controles biométricos*, in *Justicia Laboral*, No. 39, 2009, p. 42.

STENICO E., *L'eserzicio del potere di controllo «informático» del datore di lavoro sugli strumenti tecnologici di «ultima generazione»*, in *RGL*, I, 2003, p. 131.

THIBAULT ARANDA J., *El derecho español*, in *Tecnología Informática y Privacidad de los Trabajadores*, Thomson Aranzadi, Navarra, 2003, p. 59.

TOWN D. and COBB L., *Notes on: GPS Technology; Employee Monitoring Enters a New Era*, in *Labor Law Journal*, 2012, p. 203.

WALLACE P., *The Internet in the workplace: How New Technology is Transforming Work*, Cambridge University Press, Cambridge, 2004, p. 3.