УДК 349.2

ЭЛЕКТРОННЫЙ КОНТРОЛЬ В СФЕРЕ ТРУДОВЫХ ОТНОШЕНИЙ

Т.К. Морейра, Ф. Андраде

Высшая школа права университета г. Минью, Португалия

fandrade@direito.uminho.pt

Поступила в редакцию 22.06.2015

Наблюдение и контроль за сотрудниками стали одной из самых обсуждаемых проблем современности, учитывая что использование информационных технологий на рабочем месте возросло в геометрической прогрессии. Развитие информационных технологий в сфере охранного телевидения и видеонаблюдения, биометрии, генетического и алко-/наркотестирования, отслеживания местоположения сотрудников по GPS при движении на автомобиле или при помощи радиометки, медицинские осмотры, сбор информации при найме, увольнении сотрудника и иной личной информации, внедрение технологий «окружающий разум» вызывают небывалые опасения по поводу обеспечения приватности.

Современные технологии, применяемые при обработке персональных данных, содержат в себе угрозу фундаментальным правам личности, не только по отношению к населению в целом, но и по отношению к работникам и работодателям. Использование информационно-коммуникационных технологий на рабочем месте, которые позволяют собирать, хранить, извлекать и обрабатывать персональные данные в большом объеме и с высокой скоростью, с одной стороны, предоставляет новые возможности, а с другой – создает новые угрозы для конфликта права и интересов работодателей и работников, что требует установления четких границ.

Новые ИКТ-технологии, в частности Интернет, электронная почта, «облачные вычисления», «окружающий разум», даруют бесчисленное множество преимуществ для работников и работодателей, но в то же время содержат новые проблемы и вызовы, а также способствуют переосмыслению старых. Международное сообщество пытается найти соответствующие подходы к решению этих проблем, комбинируя инструменты открытости и гласности, запреты, правовые и технические меры для того, чтобы обеспечить, насколько это возможно, реализацию права на информационное самоопределение.

Ключевые слова: конфиденциальность, электронное управление, трудовые отношения, облачные вычисления, окружающий разум, права человека.

1. Introduction

In the last years we have been witnessing an enormous increase and development of ICT in the workplace resulting in great changes at the workplace level.

The use of information technology in the workplace has grown exponentially and surveillance and monitoring have become contentious 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 recourse to RFID technology, medical examinations and information for hiring or retaining an employee and ownership of personal information have raised unprecedented concerns about privacy.

Developments in technology make our daily lives easier, assisting us in communication and protecting us from certain dangers and have a huge impact on Labor law.

But they can also 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 privacy not only on the people in general but also on all employees and even employers. The use of information and communications technology in the workplace 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 [1, 2].

The Internet changed the business landscape, making it far more competitive and the workplace considerably faster 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: the concept of work-life balance gained a 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 [3].

By the late 1990s 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 and the huge increase in the power of control by the employer.

Also by the late 1990s, the volume of email traffic surpassed the volume of telephone traffic, making a milestone in the Internet's influence on our patterns of communication. Also, instant messaging has grown exponentially along with several other forms of communication that rely on this new ICT.

With these new information and communication technologies 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 causing 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 implications.

If on the one hand it allowed a huge reduction in the costs and the times of work and it accelerated the transmission of information, on the other hand, this revolution provoked a change 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.

This type of control impregnated the genetic code in the way of organization of the work from the application of Taylor's theory in Ford's version. In this organization a very important role is accomplished by this control and by the surveillance done by the personnel's administration, in a way to obtain the accomplishment of certain objectives. But, if originally one could understand the analysis of this control as a mere aspect of the directive power, nowadays, such developments as the control of the e-mail and of the Internet, the use of the computer as an instrument to control the workers, and the surveillance through audiovisual means or GPS or RFIDs or biometric data or even smart cards, have transformed this matter to very complex dimensions that justify, possibly, the consideration of this power of control as an autonomous one.

2. The electronic control

2.1. The transformations in companies' 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 favoring the emergence of new ways of control and surveillance. If the control by the employer is neither new nor forbidden, the innovation comes from the fact that these new technologies changed this control and have a capacity to collect data that, sometimes, seem to have no limits. These new technologies, directly related to informatics instruments, can even determine a change in the power of control of the employer in the measure that great part of the direction, control and surveillance will be accomplished remotely through the computer. In this measure, to "work on information will imply to know who treated, elaborated and made circulate the information". This reality demands that we increase the efforts in the sense of assuring the worker's position and that the worker's fundamental rights are ensured.

If the power of the employer's control configures an essential aspect of the workers' subordination and of the work relationship, the proliferation of informatics systems, unavoidably associated with the new technologies, has increased to a great extent the potentialities of this power.

The introduction of the new information and communication technologies (NICT) in the companies is not a neutral instrument, but, on the contrary, it is complex and capable of changing the power of control and the surveillance of the employer, directly on the "nervous system of the organization and of the whole society". Through NICT a new balance is operated among the different powers of the employer, being these powers centered in the control of the activity, and the use of these technologies turned into a "privileged observatory" [4] of the evolution and performance of the worker.

We have to understand that one of the most disturbing aspects of the introduction of the new technology is related to the new forms of exercise of the employer's electronic power, because they increased it in an unusual way, without precedents. It is true that this power has always existed, but in the traditional (limited) surveillance and control. Now, the monitoring and electronic surveillance presupposes a "qualitative jump" and today we have an electronic "control at distance, which becomes cold, incisive, surreptitious and seems to know everything" [5], making thus possible a total control, or almost total, of all of the movements of the workers' life, which means that the worker becomes "transparent" for the employers and stops feeling free [6]. Actually, with the adoption of the new technologies, the electronic control increased exponentially because it is much more present. The use of the traditional technologies like badges or the control of the access of the workers constitutes a type of control that is related basically to the presence or the individual's physical location, still being in the "periphery of the work" process. Howev-

er, with the emergence of the new communication technologies and, particularly, with the introduction of the Internet in the company, the process of "true migration of the technologies of control from the periphery to the heart of the work" [7] began. Jean-Emmanuel Ray [8] when referring to the new technologies of the information and communication, argues that the subordinate work, inspired in Taylor's model, is totally different from these new types of social relations based on an opposite basis: the autonomy and "if the intellectual work allows the accomplishment of an old dream, it will be able to, thanks to the new technologies, transform it into a nightmare: the ubiquity", considering that one of the main difficulties of NICT is the fact that they are "fundamentally ambivalent: they are an evident source of freedom and autonomy but inversely they can send *Big Brother* to the stone age, and pass Taylor for an apprentice" because after their emergence it is possible to accumulate an incomparable amount of information in the computer's memory.

With these new technologies we entered a new stage in the surveillance and control of the worker, since the computer allows to know the way the workers think, the workers' actual thoughts, and the employer can make assessments about them, through the control of their work techniques but equally by finding out about the focus of their personal interests as reflected in their several connections to the Internet. This can create a profile of the worker. It can be argued that the control has passed from a physical to an undeniably qualitative level. It becomes easy for the employer to know the way the workers think, and it becomes difficult to separate the private life from the professional one [9, 10].

With the introduction of these NICT, there is a change in the electronic power of the employer, renewing the classic subject of their limits and the workers' space of freedom.

2.2. Another characteristic of NICT that increases quite significantly the possibility of the control is the ambivalent character in which these technologies are used, simultaneously, as an instrument to carry out the activity and as a mechanism for controlling the work executed by the worker. Thus, a perfect combination of the activity and of control in the same machine is achieved in such a way that while the computer is used for productive ends by the worker, it is, at the same time, providing an enormous amount of data to the employers, contributing to increase the sphere of exercise of their power, and also making the worker participate directly in the control of his own activities. The worker becomes, simultaneously, an active and a passive subject of a machine in such a way that it is possible to accomplish a bidirectional control [11].

The use of the computer produces an enormous expansion in the quantitative plan but also in the qualitative plan, marking a "notable jump" of quality in the capacity of control by the employer.

2.3. Associated to this, this control seems to have no limits. Previously to the introduction of the NICT, the surveillance always implicated a certain physical interference: a hierarchical superior or, still, searches to the workers and their goods. On the other hand, to intercept the workers' communications it was also necessary certain physical accomplishment and it was easy to detect when a mail had been open. Actually, however, with the help of these new technologies, the employers can access all the data stored in a computer without workers knowing it and "when the worker sits down in front of the computer and looks at the monitor, on the other side, someone can see him without his knowledge" [12].

These new technologies have a huge control capacity that seems to have no limits and that affects the work relationship, getting the attention for a true "risk of corruption" of this power that originates a deep change in the electronic power because great part of the exercise, given the ambivalent character of these new technologies, will be done at the distance through the computer, passing this power of eventual element of the activity for a real part of that activity. Thus being, there is an extension of the power of control, as well as a decentralization of the subordination and a difficulty in distinguishing between the structure of control.

2.4. Through the NICT there is a clear disappearance of the borders between professional and personal life. The new technologies allow the notion of time to be transcended, with the enormous capacity of storage of the computers and the possibility of always leaving track and of being invisible, originating that computers can constitute a great help for the employers when allowing to gather proofs for litigations with their workers. The computers turned "into the new supervisors" of the workers [13].

On the other hand, it is more and more visible a smaller separation among the borders of the personal and professional life in the measure that the workers can enjoy, through these technologies, some personal time (sometimes very private time) during the working hours. However, simultaneously, they invade the home and the worker's private life and so "the official working hours don't mean anything when the work can be taken home to continue to be accomplished there, without any temporary limit" [14]. As Alain Supiot [15, 16] wrote, the new technologies are "creating new forms of sub-

ordination", defending that the worker must be entitled the right to disconnect, as the right to private life of the XXI century. The worker is entitled to be not (at least not permanently) online. He has a right to the disconnection, to effective rest. It is a technical disconnection that, like Jean-Emmanuel Ray [17] wrote it is favorable for the company because the workers that don't have a free time turn neither more productive, nor more faithful to the company.

In reality, like Jean-Emmanuel Ray wrote, we are facing "a war of times" [18]. The official hours don't have any meaning when the worker is not entitled legally to rest. By having to be constantly on line and not to disconnecting, the worker cannot enjoy the necessary physical and psychological re-establishment. And if, until some time ago, we could argue that these workers, *Net-Addicts*, also had a personal time in the workplace, and by that they had a certain balance among personal life in the office and professional life at home, nowadays that is no longer arguable in the same terms. Nowadays, the professional life absorbed great part of the personal life and, supporting Jean-Emmanuel Ray, the juridical subordination, one of the elements of the existence of a labor contract, according to article 11.º of our labor code, became, actually, permanent criteria of the worker's life.

The big problem in this type of situations is the one that, in most of the cases, there is no expressed order of the employer in this sense. However, one must not forget that there are imposed legal rules, even at European level in relation with the organization of the work time and specifically related with the respect of the workers' rest, and that exists to ensure better protection of the worker's safety and health. It doesn't look possible a step back in this matter and any agreement that violates the established minimum in the community rules will be illegal.

2.5. This control becomes, many times, potentially vexatious, continuous and total, bringing, inclusively, risks for the workers' health, so much physical, as psychic, namely for knowing or feeling oneself constantly watched. This can provoke a great psychological pressure and this can lead, *inter alia*, to cases of *mobbing*, depressions and stress. Important stressors are, for example, the blurring of boundaries between work and family life and the extension of the working day.

These may cause increased stress and mental fatigue, which in turn may have long-term consequences, including a weakening of the immune system, psychosomatic diseases, sleep disorders and cardiovascular diseases.

On the other hand**,** social networking websites like *Facebook* and *Twitter* offer extensive possibilities for interacting with people and sharing photos, opinions and other information online, for advertising and even making recruitments online.

But as these websites also contain personal data, which must be protected, the EU Data Protection Authorities reminded the companies who signed the Safer Social Networking Principles of their obligation to respect EU data protection rules. For example, personal data on social networking websites cannot be shared and further processed without the consent of the individuals concerned and that is very important in labor law. Can the employer punish the employee who criticizes, in his Facebook account, the way the company works? And what about the pictures that employees display on these websites, can these be relevant to the evaluation of the worker?

Also, searching for information online (surfing) is part of a daily routine for many people. Even though many think they surf the Internet anonymously, this is often not the case, as they leave behind a history of what they have searched for online. Can the employers control everything the employees are searching?

The problem is that one of the most fundamental challenges may be seen in the fact that most of the personal information published in social network services is being published at the initiative of the users and based on their consent.

3. The control of the worker's emails by the employer

3.1. The theme of privacy and the electronic control of the employer and in this case the control of the electronic communications (mainly the e-mail) has been turning in the last years into a matter of considerable interest. It is surrounded by great controversy, mainly because the technological progress allows the reception and recording of conversations at any distance, and it becomes essential to protect in an appropriate way the safety and the secrecy of these new types of communication, widely used at the workplace as an important working instrument [19].

These new forms of communication constitute powerful means of control and of information storage, but also of analysis and of interference in the people's privacy, and one of the major challenges facing us 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.

In many companies these communications systems are no longer mere working tools since these are now the way to offer services and

products to the market. But with this concentration new problems have emerged because the main working tool the workers use is also the instrument that actually controls them, thus a new form of control emerges that is much more intrusive and able to control almost everything including the way the worker thinks, since these instruments leave tracks that are immediately perceptible by the employer. In this case, we deal with the new *fingerprints* [20] related to different features of the person: personal, professional, political, social. The worker leaves these fingerprints, consciously or not, and an easy and simple research in the Internet allows the employer to build up the worker's and the candidate's profiles. The idea of the *Big Brother* that could identify and control everything, seems old and very simple, when compared with these countless "Little Brothers" that can follow us and know everything about us, to the tiniest detail, and the ghosts of the panoptic seem very real!

The problem is that with these new technologies bring along a totally new type of control (much more intrusive), with programs capable to record the worker's actions in such a way that the employer can observe all the details, the mistakes, the written words and several other things that, in any other way, would escape his knowledge.

Computers make surveillance imperceptible. Before the age of computers, surveillance at work almost always involved some form of physical intrusion that the employee was bound to be aware of: a supervisor looking over his shoulder or a physical search of his place of work or a locker or personal belongings, such as bags or even a physical search, and it was possible to detect whether a mail had been opened. Now it is possible, by using the net, to arrange for an exact copy of a particular employee's screen to be reproduced on the employer's screen or to read his e-mail without the employee noticing anything [21].

On the other hand the notion of oblivion does not exist on the *Internet*. Data, once published, may stay there literally forever - even when the data subject has deleted them from the "original" site, there may be copies with third parties (including archive services and the "cache" function provided by a service provider). Additionally, some service providers refuse to speedily comply (or even to comply at all) with user requests to have data, and especially complete profiles, deleted [22].

3.2. Also this new form of electronic control allows an easy collection 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 estimation concerning its relevance to the aptitude requirements or with the derived obligations of the work contract.

The problem is related to the fact that together with this logical and necessary use of NICT, the employer can use such information and personal data for other purposes, neither legitimate nor lawful, disguising them under the form of productive interests when in reality they are forms of true behavior control (of the employee) which are forbidden, not only at national but also at international level [23].

The workers don't leave behind their rights as persons (and certainly not their right to privacy and 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 there they develop a significant part of their relationships with other human beings and there is a reasonable expectation in relation to data protection and to the right of secrecy of communications [24, 25].

3.3. The business efficiency is enhanced through the use of electronic communications in the workplace. On the other hand, the implementation of this new type of communications brings along new problems related to the protection of certain fundamental rights, especially, privacy related to the right of the informative self-determination and the constitutionally protected secret of communications.

The problem is centered on the establishment of limits to this huge form of control, and these are related to the application of the data protection principles that are a part of the right of privacy. Through this type of control, the employer knows individual information that integrates the concept of personal data. But the employer has to comply with the principles established in the Law 67/98, 26 October, that transposed the Directive 95/46/EC, namely the principle of transparency, and the principle of proportionality, which presumes that the obligation of informing the employer of the treatment, and that the collected information cannot be destined to incompatible purposes with the original purpose, but also the fact that personal data must be processed fairly and lawfully and must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

3.3.1. The employer, before the adoption of any form of this type of control and specifically before the control of the e-mail of the employees has to respect the legitimate purpose. This principle is stated in article 6, No.1, paragraph b) of the Directive 95/46/EC, and in art. 5, 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, the explicit definition of these purposes being essential.

This principle constitutes the truly fundamental and main principle of data protection [26, 27, 28]. In fact, the other principles are all related to this legitimacy principle because data should be appropriate, pertinent and not excessive in relation to the intended and legitimate purpose; the data should be exact, complete, accurate and precise in relation to that purpose; and data should only be conserved for the time and the needs of the original purpose.

On the other hand, the original purpose also assumes relevance when the right to information is assured in the terms of art. 10, No.1, of Portuguese Data Protection Act, as well as when the authority of control will appreciate the authorization requests (or notification) of the treatment of personal data because not only the Portuguese data protection Act but also the Labor Code has that as a requirement to several types of control.

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 original purpose [29].

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 performed.

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 in any form, mainly imposing restrictions on the elaboration of automatic profiles based on the personal data treated.

It should nevertheless be clear when studying employee data protection and privacy, that specific attention must be drawn to the particularities of the employment environment. Indeed, an employment relationship implies, as a general rule, a subordinate relationship. This means that the employer is contractually allowed to exercise authority upon the employee. Still, the individual is only subject to the authority of the employer in so far as this is embodied in the specific employment relationship, in other words, in so far as this is relevant for the employment contract. Furthermore, the existence of an employment relationship does not take away the respect of the right to privacy and human dignity. More in particular, monitoring issues will need to take the employee's right to privacy and the protection of his/her personal data into account.

This purpose and legitimacy principle seeks, this way, to avoid the pretension of the employer of converting the labor contract and the work relationship into a means to collect personal information of the workers and to build up profiles of the employees.

3.3.2. The employer will always have to respect the proportionality principle. This principle specifies that the only personal data that may be collected is the one that is necessary to achieve the purposes of the data collection operation. In so far as doing so, the employer or the person or organization in charge of the operation should choose for secondary rather than primary data collection, anonymous rather than nominal monitoring, sampling rather than full-scale control, and for voluntary rather than compulsory surveillance and forms of control.

This principle tends to accomplish a balance between the worker's obligations that stem from their labor contract, and the extent of constitutional freedom of their privacy, guaranteeing that the modulation of this fundamental right will be accomplished in order to fully respect this principle, that is, with strictly indispensable restrictions (in amount and quality).

This proportionality principle, when applied to the labor contract, presupposes a previous judgment on the need or indispensability of the measure and on the proportionality of the sacrifices that it holds for the workers' fundamental rights.

This principle is established in article 6.º, No.1, paragraph c) of Directive 95/46/EC, and in art. 5.º, No.1, paragraph c), of the Portuguese Data Protection Act, and it means that the treatment of personal data should respect this principle and must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

This proportionality principle is associated with the quality of the personal data, constituting a fundamental factor for the legality of all data treatment.

In this way, it imposes the exclusive treatment of the pertinent data in relation to the purpose for which they are collected, being the *ratio* of the norm that the treatment of personal data can only take place when it is indispensable for the original purpose. It is always necessary to accomplish a previous judgment on the need or indispensability of the measure and a subsequent judgment on the proportionality of the sacrifices imposed on the worker.

3.3.2.1. Specifically in the case of the *e-mail*, this principle means that the employer will have to pay attention to the whole constitutional protection, and thus not only to the right of privacy but, above all, to the right of secrecy of communications established in article 34.. These principles are consecrated constitutionally, but also at penal and labor level and the employer has to obey to all these principles when he intends to regulate the control of the workers' e-mails.

This principle means that the employer cannot invoke his legitimate organization and power of control in order to limit the exercise of the constitutional right established in article 34 and also in article 22 of the Portuguese Labor Code – establishing the "confidentiality of messages and access to information", which states 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 that "The preceding clause does not prejudice the employer's right to establish rules regarding the use of undertaking's electronic resources, namely e-mail".

This principle also means that even if the computer used by the worker is the property of the employer, it doesn't justify the access to the electronic communications accomplished through the company [30]. The labor contract doesn't transform the employer into an active part of the message or in a qualified third party to transgress the secrecy of communications. The employer is a third party in the personal e-mails and the access to the content of the e-mails sent or received by the worker can violate the constitutional right of the secrecy of communications.

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 make a distinction betweendifferent situations.

In the first place we should make a distinction between professional e-mails and personal e-mails, even if, sometimes, the distinction is difficult.

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

In the second place, we consider that it is better to separate professional e-mails from personal ones in relation to different forms of control of the employer.

It seems to us excessive to include in the scope of the protection of the secrecy of the communications professional e-mails in the case of existing clear policies concerning the use of these and separate bill accounts from these e-mails. In the case of professional e-mails there is a professional relationship between the worker and the employer and the latter can control the content of these messages, respecting all of the requirements for the correct exercise of the power of control, mainly the requirement of proportionality, in the measure that it doesn't seem to us that the employer is a third party for effects of obtaining a previous judicial authorization. In these cases, the communication is transmitted by "closed" channels of transmission, although these communications contain simply orders related to work. But we cannot stop underlining, however, that this control has to be the least intrusive possible, and that the worker's consent exists in this sense, especially because he sends and receives messages in agreement with the orders that he previously received from the employer. The content of the professional e-mail messages cannot be considered exclusively the worker's property.

Nevertheless, the employer cannot control everything because there is the Data Protection Act, namely the legitimacy of the purpose and of the compatibility with the declared purpose, and all the principles that have to be respected in the exercise of the electronic power of the employer, mainly the principle of proportionality.

When clear policies exist concerning the use of these means with the establishment of proportional limits and in agreement with the principle of good faith and when the workers are aware of these, thus the principles of information and publicity are being respected, we believe that the access of the employer to the worker's professional e-mail without the need of a judicial authorization should be considered lawful.

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 argue that there should be an objective reason for the exercise of this control and surveillance and that arbitrary, indiscriminate or exhausting control of the workers e-mails cannot be acceptable. 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 not becoming more aware than necessary and using the less intrusive techniques, in respect to the principle of proportionality. Only when it is not possible, through these less intrusive ways, to obtain the satisfaction of the employer's interest, will it be legitimate to control the content of professional e-mails.

In the case of messages marked as personal or of messages that are not qualified as such but when it can be deduced by the content of the external data that they are personal, the situation is totally different [31]. In these cases the messages are protected by the right to the secrecy of communications in the constitutional terms and also by article 22.º of our Labor Code, being, thus, inviolable. The employer cannot control the content of these messages 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 in the terms of article 32.º, No.8, of the Portuguese Constitution.

The employer, before reasonable suspicions of contractual infringements by the worker, cannot control the content without a previous judicial authorization, in the terms of article 34.º of the Portuguese Constitution, even if the worker has violated the established rules imposed by the employer, because the property of the instruments doesn't remove the rights constitutionally established.

In the case of inexistent policies about the use of electronic communications or even if these exist, but allow an indiscriminate use, that is, in the case that the worker has only one e-mail account and uses it both for personal or professional purposes, 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 communications.

The employer, in spite of not controlling the contents of the messages in the case of the personal e-mails or in the case of an indiscriminate use, will be able to control some external data to try to verify or control if the workers are using correctly or not their instruments of communications.

It should be noted that, considering the principle of proportionality, the knowledge of certain external data configures a smaller intensity of the intrusion in this fundamental right. On the other hand, it seems that we have to protect, in a certain way, the interests of the employer and, for that, if it were not permitted to control these data he would be without any possibility of control.

To support 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 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 Law No.41/2004, of August 18, that transposed this Directive. As we can see, the Directive admits in certain circumstances the possibility of treatment of certain traffic data.

The problem is in 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 behavior. He can control, for example, the cost of the work tool, the time spent by workers in its use and the access to the *Internet*. He can even control data traffic, that, although in principle protected by the right to the secrecy of communications, through the new characteristics of these means, become patent and easily discovered, 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 presence in the net. By controlling these circumstances, the employer, applying the principle of good faith – or, at least not transgressing it, - can put an end to the labor relationship, based on an inadequate or abusive use of the work instruments.

We think, however, that it should not be possible to control the receiver in the measure that he is a third party and he ignores the policies of the company in relation to electronic communications. The knowledge of the traffic data should be limited to the sender, to the subject, to the hour of the sending, to the size of the attachment as well as to the type of it, but not to the content because the right to the secrecy of communications also includes this. It seems to us that the knowledge of this type of data is enough for the employer to control the use of these means and to establish sanctions for the ones who violate the rules.

But even the control of professional e-mails has to follow the principle of minimalist data processing; meaning that personal data has to be deleted or rendered anonymous once it is no longer required for the purposes for which it has been kept. And 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.

3.3. The employer, before adopting any measures of control will still have to respect the principle of transparency that consists in the knowledge of the surveillance and of the control exercised by the employer. This principle is essential for the correct treatment of personal data, in general, and of the workers, in particular.

The workers have to be informed on how, where and when the control is made [21]. The employers have to clearly notify the workers on the limits to the use of these new technologies and these limits must 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 communication means, not forgetting that the information about the control is imposed by the principle of legitimacy and lawful data treatment and good faith in the exercise of the electronic power of the employer and, thus being, it is forbidden to exercise hidden control, a control without the worker's knowledge.

The employer, in respect of this transparency principle and good faith, has to allow his workers an immediate, clear and explained access to his policies concerning the use and eventual control of the e-mail. The employer should provide to the workers all indications about the use of the electronic mail inside the company, describing the ways how the company's means of communication can be used for personal communications by the workers, namely the limitations and the allowed duration of the time of use, as established in the *Working Document on the Surveillance of Electronic Communications in the Workplace* by the Article 29 Working Party (an advisory group of representatives of the data protection authorities of the Member states), and referring, still, in relation to the electronic mail, *inter alia*, if a worker is entitled to an electronic mailbox for merely personal use, if the use of private webmail mailboxes is allowed in the workplace and if the employer recommends the use, for the workers, of a webmail mailbox for merely personal use, separated from the professional mailboxes. He should also inform on the period of storage of a possible backup copy and information on when and how the messages are definitively destroyed.

We think that the most appropriate way to accomplish this transparency principle is to elaborate some "Rules of good conduct related to informatics" or a kind of "Document on informatics" [32, 33, 34, 35, 36, 37, 38, 39], about the use of this type of communication instruments, establishing the internal rules and subject to all the legal formalities.

In these *Documents* the employer should set out the right of each worker to a personal mailbox for e-mail, in the measure that is preferable for the separation between personal mailboxes and professional ones, or, at least, for the possibility to have a personal folder inside the normal mailbox; voluntary encryption of the personal communications should still be permitted; 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, these *Rules* could also state that personal e-mails should be legal and not include scandalous statements, or harass people or discriminate anyone based in their origin, race, ethnicity, age, disability, nationality, gender, sexual orientation, religion or belief.

Professional e-mails cannot contain any of these situations and the worker that violates these rules can be sanctioned, as it happened in France where a worker sent to the company's customers e-mails containing attachments with pornographic pictures "to improve the professional relationships" with them. The worker was dismissed, decision confirmed by the *Cour de Cassation*, the French Supreme Court, on October 22, 2008 [40].

The employer, in the *Rules of Good Conduct* about the use of the communication means, can establish limits such as the time that the workers can be using them, as well as the type of attachments that they can send, limiting certain types that can be related to the practice of crimes.

These *Documents* have to set out the 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 must have given their previous consent, although once again we reaffirm that such permission doesn't legitimate the possibility for the employer to open or to read the worker's private correspondence, under penalty of violation of article 34.º of our Constitution and of article 22.º of our Labor Code. It should be established that in the worker's absence there should be created an instantaneous message of warning for the worker's contacts and, if necessary, the e-mail address of the person who will be responsible for answering the worker's professional e-mails should be given. On the other hand, these responsible workers should always be the same ones and should be the only ones to have access to the e-mail account.

The workers have the obligation to distinguish correctly between the e-mails of professional nature and the ones of personal nature, assuming the obligation of not classifying professional e-mails as personal ones and vice-versa, and understanding

that the company will assume as professional all the e-mails that are not qualified as personal ones.

This seems to be the best way of informing workers on the possible correct or incorrect uses of the electronic means. The employer may not set out an absolute prohibition on use of telematics for personal purposes, but still will be able to interdict a personal use for certain purposes, even if they are not illegal. For instance, it will be allowed to prohibit access to discussion *forums* and to chats, in order to avoid the transmission of secrets of the enterprise, or the access to pornographic sites, as well as to games sites.

We consider that the desired decrease of the use of the e-mail for unlawful purposes arises from clear policies on the use of these new means of electronic communications.

4. The danger of the Homo Connectus

Electronic communication networks bring along new problems (geo-localization, the social networks) 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 much enhanced controlling power of the employer: workers may now be monitored not only in the working places, but anywhere and whatever they do [41].

Total and imperceptible surveillance becomes now possible. And the question must be: Is there a right to disconnect? Aren't we supposed to be permanently on-line? The figure of the "Homo Connectus" fits in the Contractual relationship?

In this paradigm, some important principles of law related to the fundamental rights of privacy and data protection may seem somewhat compromised. For instance, the notions of oblivion, the right to be forgotten, the right to be let alone. Most of our communication is now transmitted over telematics networks and the exercise of a right to erase our data is almost impossible. This was already a problematic issue when we had to consider just the in-house based systems, through a hard disk of our own. But, while using these devices, it looked that we had the right to erase or even to reset the system. Anyway, even in this situation it would always be possible to undertake actions of expertise in order to find out what had really happened in a hard disk. Electronic evidence seemed to have a promising future. But now the situation has to be looked up under a totally different view. Publication in virtual environments and social networks tends to be forever. It is becoming harder and harder to assure the right to oblivion. This is particularly relevant in the new paradigm of distributed computation, usually known as cloud computing.

5. Cloud Computing

Cloud computing or distributed computation is a new modality of services provided either on-premise or off-premise (but mainly off-premise, of course), allowing an ubiquitous access to a wide range of informatics resources [42].

Cloud Computing is understood as a "…new way to deploy computing technology to give users the ability to access, work on, share, and store information using the Internet. The cloud itself is a network of data centers – each composed of many thousands of computers working together – that can perform the functions of software on a personal or a business computer by providing users access to powerful applications, platforms and services delivered over the Internet" [43].

The availability of cloud computing services and the consequent delocalization of software and archive functions will necessarily generate complex relations between employers and service providers, and it will necessarily increase the international or trans-border flow of data and difficulties will arise concerning the warranties of personal rights in trans-border distributed environments [44]. Considering this, cloud computing intends a tremendous challenge for legal systems, both at national and international level, and it must be understood that the cooperation of national authorities and commercial and civil partners (employers and trade unions) will be essential in order to ensure that legal rights / citizens rights are respected [42]. But Cloud Computing will bring along other consequences: the liability of service providers may have to be re-thought, since the European legal framework for electronic commerce established a liability framework very favorable for service providers [45]. Yet, the technological and economic context has nowadays deeply changed.

6. Ambient Intelligence

There is now a whole new possibility of complete use of data ("things assumed as fact and the basis of reasoning or calculation" [46] or of "information" ("the communication of instructive knowledge, information or news" that require processing [46]) allowing the construction of so-

phisticated knowledge. This is quite clear when we analyze the possibilities offered by the introduction of technologies of ambient intelligence.

Sensing modules may now be used aiming at the mobile monitoring of the person [47]. The use of smart devices, the vision of the Virtual Residence [48, 49] and Virtual Workplace has come to stay, sometimes disguised as mere tools used for efficiency aims. Electrical or gas safety features using ubiquitous technologies are capable of developing smart environment and services by analyzing collected information [50].

Domotics and ambient intelligence are closely connected. A good example of this is the partnership between Toyota and Microsoft [51] for the construction of a global platform for telematics services using Windows Azure. Toyota has been experimenting with a pilot program aiming to connect people, cars and homes intended to achieve an integrated control of energy savings. But the danger is the concentration, interconnection, processing and diffusing of pervasive data. Your car and your electrical network may disseminate data about you!

This may also easily bring along an intense use of personal data. The threat of an intensive treatment of personal data is leading to our progressive transformation into electronic persons, allowing the systems to constantly survey us.

Even without considering the threatening possibilities of web bugs (devices for collecting data able to introduce themselves in a web page or in a mail message) or spyware programs (able to install itself in electronic environments without the users consenting or even being aware of it) [52], there are increased and enhanced possibilities of building up and keeping personal profiles. The massive collection of data by Ambient Intelligence (The Internet of things), the "availability and exchange of data between various systems, devices and databases" [41] allows the monitoring of the choices and activities of the user, through systems capable of adapting and of learning

Intelligent environments may now become an active subject based upon an electronic entity built upon devices and sensors. Ideally, this entity would be invisible to the eye of the user and the user would not be aware of being monitored, as the simple fact of knowing it might be enough to change his behavior. Nevertheless, the fact that this environment surrounds the users and constantly acquires information about them and their context of interaction, by means of regular devices with computational power (e.g., touch screens, video cameras, accelerometers, PDAs) brings along new requirements concerning the transparency of the systems, the consent of the users and the finalities of the use of the collected data [53].

7. Principle of transparency and secrecy of correspondence

Are the secrecy of communications and the secrecy of correspondence still applicable? Anything or anyone may be watching our mail accounts. The need of commercial ads is somewhat required for payment and sustainability of the services. Software agents are looking at what goes in the network trying to find useful information concerning the commercial purposes and requirements. Let's take a look at Gmail, a very well known provider of electronic service. Is there still a right to the secrecy of correspondence in such services? When we open our Gmail account and we take a look at the received mail messages, we easily notice advertisements inserted along with the main message, often having contents related to the contents of the message we received. We can say without any doubt that something or someone is reading our mail. (We hope that it will be something… I still want to think that these advertisements are the result of only the actuation of software agents… Anyway, we must feel deeply concerned about this situation…). Where is the secrecy of the correspondence in the electronic environments?

Technology brings along the possibilities of total monitoring, surveillance and control of data – we have to face a new danger, the one of dataveillance.

The use of software agents capable of collecting data, accessing data, keeping and processing data and transmitting it to third parties [54] is already challenging our views. Should we consider software agents as data controllers having "the same obligations and responsibilities" as legal subjects have? [54] Of course software agents are no legal persons (at least, not yet) although they may have something equivalent to intentional states [55, 56], which must not be ignored.

Issues such as distribution of data (and distributed computation), monitoring through cameras and sensors ("sensorship" is not less dangerous than censorship) and profiling are an open door to intrusion, to privacy elimination and to the use of personal data. The issue is not restricted to data and its use, but also to information, and from the crossing of information arises the possibility of building up real knowledge (and even context based knowledge).

Furthermore, the use of sophisticated technology – data and information processors, databases, networks, information retrieval systems, data mining, intelligent software agents, ambient intelligence – causes a severe loss of control on the use of personal information. The principle of transparency may be at a serious risk. In the situation of an employer – worker relationship, it is mandatory

to ask whether the power of control of the employer allows the collection of personal information of the workers and the creation of profiles of the employees? It looks unavoidable to rethink the employer's powers of control accordingly.

8. Effectiveness of Fundamental Rights?

Article 8 of the European Convention on Human Rights established the existence, at the European level, of a Fundamental Right to Privacy. On the other hand, article 7 of the Fundamental Rights Charter of the European Union established a right of the person against undue and illegitimate intrusions either by public authorities or by third parties [57].

But also data protection was considered as a fundamental right, in article 8 of the European Charter of Fundamental Rights. Yet, it is true that Member States still have wide possibilities of appreciation concerning the regulation of this right [58].

Privacy is now deeply threatened. The technological possibilities of a constant monitoring of a person, especially through the use of RFIDs and geo-localization positioning system (GPS) allow something or someone to follow everything we do wherever we go [41]. The establishment of relations between persons and objects (the Internet of things) is particularly dangerous in this regard.

An important question to be asked at this level will be the one related not only to one's right to privacy but also to what may be considered a "reasonable expectation" of privacy [41]. As it was mentioned by De Hert, Gutwirth et al. "Is it reasonable to expect any privacy when everything we do can be constantly monitored"? [41]. It becomes true that what we are really getting, more and more, is a clear expectation of being monitored. Should we count on that and act accordingly?

There are wide possibilities of collecting or mining data (data mining) and of building up personal profiles, by observing choices, behavior, emotions, to a point where persons are less and less capable of living according to their own choices and upon totally free and autonomous behavior [59]. This enhancement of monitoring brings along this progressive blur on the distinction between the public sphere and the private sphere. And it certainly brings along the danger of "Surveillance" and "Surveillance of Data", or, as someone already called it "Dataveillance" [41]. An issue that obviously is at stake is whether or not there is still margin for ensuring the warranties of confidentiality and of two distinctive aspects of intimacy: the negative aspect of intimacy, aiming at excluding any knowledge by third parties of what is own to the person, and the positive aspect of intimacy, aiming at ensuring a control of the person over his (her) own information [60].

Even though we could admit that the use of electronic systems might have to respect legal impositions concerning the rights and warranties of the persons[61], it must be recognized that there will always be evident risks associated with the use of the technologies. There is an obvious risk of constant monitoring, profiling and "dataveillance" (or surveillance based on the collection, processing, use and transmission of data). A distinction may have to be made between requirements of privacy and requirements of data protection, between warranties of opacity and warranties of transparency [41].

Thus being, it is clear that a legal affirmation of rights is not enough anymore. It is mandatory to ensure the effectiveness of these. And in this regard, not only the important role of Law and Regulations must be recognized, but also the important role that Technology, itself, may and must play. Privacy Enhancing Technologies are welcome [41]. If, on the one hand, technology may become a nightmare to legal values, bringing along innumerous threats to persons' fundamental rights, on the other hand, we should ask ourselves if the same technology must not be considered as an unavoidable part in getting the solutions for the arising problems, by enhancing a use in conformity with the legal requirements in terms of privacy and data protection. As Jane Winn puts it "Just as technical standards make networked communications possible, increasing the risk that data may be processed without regard to the requirements of data protection law, they may also lower the cost of compliance with data protection laws and increase access to privacy-enhancing technologies" [62]. This is an idea already formulated years ago by Lawrence Lessig [63] who displayed the existence of multiple normative dimensions well beyond the range of actuation by the State through legislation and regulations [64]. According to this author, issues such as the architecture of the network may have implications concerning state regulations and personal rights.

Anyway, Lessig's view can certainly be criticized and a major difficulty arises from the fact that the issue can't be dealt with either at a local level or at a national level, as it was recognized recently by the deputies at the French National Assembly (Resolution nr. 2837 of the 5th October 2010): there is an urgent need of an international convention concerning the protection of private life and of personal data, addressing the new problems of a global interconnected society.

Along with the enhanced possibilities of collection of personal data and of using ambient intelligence and more and more powerful capabilities of geo-localization, are there still a personal, a private and an intimate sphere of the person? [65] The issue of transparency is certainly at stake, but it is not the only one. Should we accept a new notion of

Digital territories? [48] (People's body as a the first territory – complete control of the individual; people's homes as the second territory – the individual or group has some control, ownership and regulatory power; the third territory would be public space). But this notion of digital territories implies a possibility of choice of the individual on "how much personal information" is disclosed "to whom and for what purpose" [41]. That is to say, the usual protective role of the State must be rethought, and probably there must be an involvement of both technology and individuals. As Antoni Roig puts it: "IT researchers tend to shift privacy protection into the hands of the individuals and to provide them with privacy protection mechanisms and tools" [66]. Privacy may tend to become not only a question of public policies and regulations, but also a relevant role of technology and service providers (the concept of privacy by design) and ultimately the very own choices of individuals. Only this way will it be possible to talk about the self-determination right.

But of course, at the workplace, this must be balanced with the definition of the powers of the employer and his relation with the employee. In this sense we have to agree that the respect of the transparency principle will be of utmost importance and that it is at least advisable to elaborate, at the company's level or even at the collective negotiation level, some "rules of good conduct related to informatics".

Conclusions:

1. The recognized values promoted by privacy are directly in cause in the work relationship. Autonomy, dignity, trust, respect and diversity acquire fundamental importance in this relationship, mainly when we know that the workers are spending more and more time in professional matters. Workers must be protected as well as their privacy, mainly when it is their dignity that is at stake.

2. It seems to us, in this matter, that we should reflect upon what a German philosopher's H. Jonas said, "not everything that is technically possible is unavoidably maintainable." In the Law field, and specifically in Labor Law, we could state that not everything that is technically possible is juridically acceptable. The rights to privacy and to the workers' dignity can never give in before arguments of greater productivity or greater efficiency. With these new forms of electronic control of the employer a new form of taylorization is appearing, now at the informatics level. If we allow the employer to have access to the content of all of the e-mails, to the sites visited by the workers, as well as all their gestures and conversations, we are creating a place of automatic work where the worker is seen as any other work tool, not very different from the computer that he uses. 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.

3. 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.

4. The availability of cloud computing services will increase the international flow of data and there will be a need, at national and international level, of rethinking the legal framework of liability for service providers.

5. Ambient Intelligence brings along electronic entities as new active subjects and a consequent need for new requirements concerning the transparency of the systems, the consent of the users and the finalities of the use of the collected data.

6. The principles of transparency and of secret of correspondence may be in serious risk. It is unavoidable to rethink the powers of control of the employer accordingly.

7. Effectiveness of fundamental rights to privacy and data protection is at stake. There is a need of considering, besides law (at national and international level), an active role of technology and of individuals in enhancing these rights. Only through an active intervention of individuals will it be possible to talk about informational self-determination right.

8. Compliance with the transparency principle is of utmost importance and the elaboration, at the company's level or at the collective negotiation level of "rules of good conduct related with telematics" should be promoted.

Список литературы

1. Fischer J. (2002). Implications of electronic mail policies for fairness and invasion of privacy: a field experiment. URL: http://sunzi1.lib.hku.hk/ER/detail/hkul/2652996 P. 1.

2. Kizza J. & Ssanyu J. (2005). Workplace surveillance. Electronic Monitoring in the Workplace: Controversies and Solutions, (coordination Weckert, J., Idea Group Publishing, USA. P. 3–4.

3. Wallace P. The Internet in the workplace: How New Technology is Transforming Work. Cambridge: Cambridge University Press, 2004. P. 3–4.

4. Fevrier F. (2003). Pouvoir de contrôle de l'employeur et droits des salariés à l'heure d'Internet – les enjeux de la cybersurveillance dans l'entreprise. Url last checked 20th November 2013 http://www.droit-technologie.org/upload/dossier/doc/102-1.pdf P. 13.

5. Aranda J.T. El derecho español. Tecnología Informática y Privacidad de los Trabajadores, (coord. Jeffery, M. & Aranda, J. T. & Jurado. A.), Navarra: Thomson Aranzadi, 2003. P. 59.

6. Däubler Internet und Arbeitsrecht. Bund-Verlag, Frankfurt am Main, 20, and Gantt L.O.N. (1995). An

affront to human dignity: electronic mail monitoring in the private sector workplace. Harvard Journal of Law & Technology, 2004. V. 8. № 2. P. 345.

7. Bouchet H. (2001) Rapport d'étude et de consultation publique – La cybersurveillance des salariés dans l'entreprise. URL last checked 20th November 2013 http://www.univ-paris1.fr/diplomes/master-droit-du-numerique/bibliotheque-numerique-du-droit-de-ladministration-electronique/droit/protection-des-donnees/rapport-detude-et-de-consultation-publique-la-cybersurveillance-des-salaries-dans-lentreprisem-hubert-bouchet-vice-president-delegue-de-la-cnil-mars-2001/ P. 3.

8. (2001) Le droit du travail à l'épreuve des NTIC. Editions Liaisons, Rueil-Malmaison, pp. 9 e 88 and (2002) Avant-propos de la sub/ordination à la sub/organisation". DS, № 1. P. 7.

9. Bouchet H. À l'épreuve des nouvelles nouvelles technologies: le travail et le salarié. DS, 2009. № 1. P. 78.

10. Aranda T. La vigilância del uso de internet en la empresa y la protección de datos personales. RL, 2009. № 5–6. P. 68.

11. Santini F. La corrispondenza elettronica aziendale tra diritto alla riservatezza e potere di controlo del datore di lavoro. ADL, 2007. № 3. P. 759.

12. Finkin M.W. El Derecho de los EE UU. Tecnologia Informática y privacidad de los trabajadores. Jurado A. & Jeffery M. & Aranda J. T. (eds), 2003. P. 300.

13. Vigneau C. El control judicial de la utilización del correo electrónico y del acesso a internet en las empresas en Francia. RL, 2009. № 5–6.

14. Supiot A. Travail, droit et technique. DS, 2002. № 1. P. 21.

15. Les nouveaux visages de la subordination. DS, 2000. № 2. P. 132.

16. Delawari M. & Landat C. Les enjeux de la relation salariale au regard du dévéloppement du réseau Internet. URL: http://www.droit-ntic.com/pdf/cybersurv.pdf P. 43 and on.

17. Avant-propos de la sub/ordination à la sub/organisation. DS, 2002. № 1. P. 7.

18. La guerre des temps: le NET? Never Enough Time. DS, 2006. № 1. P. 3.

19. Rubert M.B.C. Informática y contrato de trabajo (Aplicación de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los datos de carácter Personal). Tirant monografías Tirant lo Blanch, Valencia, 1999. P. 63.

20. Ray J. & Bouchet J.P. (2010) Vie professionnelle, vie personnelle et TIC. DS, № 1. P. 45.

21. Moreira T.C. (2010) 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. Moreira T.C. (2011). Estudos de Direito do Trabalho. Almedina, Coimbra.

22. International Working Group on Data Protection in Telecommunications (2008) Report Guidance on Privacy in Social Network Services. P. 2.

23. Ford M. (2002) Two conceptions of worker privacy. ILJ, vol. 31, № 2. P. 237.

24. Lasprogata G. & King N. & Pillay S. (2004) Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada. Stan. Techn. L. Rev., № 4. P. 13.

25. Golisano G. (2007). Posta elettronica e rete internet nel rapporto di lavoro- USA, Unione Europea e Italia. in ADL, № 6. P. 1310–1311.

26. Bellavista (2002). I poteri dell' imprenditore e la privacy del lavoratore. DL, V. 76. № 3. P. 152.

27. Gragnoli E. (1997). La prima applicazione della lege «sul trattamento dei dati personali» ed il rapporto di lavoro privato. RCDP. № 4. P. 703.

28. Aimo M.P. (2002). I «lavoratori di vetro»: regole di trattamento e meccanismi di tutela dei dati personali. RGLPS. № 1. P. 106–107.

29. Savatier J. (1990). La liberté dans le travail. DS, № 1.

30. Alonso I.M. (2005). El poder de control empresarial sobre el uso del correo electrónico en la empresa – su limitación en base al secreto de las comunicaciones. Tirant monografías, Valencia. P. 159–160.

31. The decision of the Portuguese Supreme Court of 5 of July 2007. URL: http://www.dgsi.pt.

32. Aalberts & Townsend & Whitman & Seidman (1997). A proposed model policy for managing telecommunications-related sexual harassment in the workplace. Labor Law Journal, P. 617.

33. Stenico E. (2003). L'esercicio del potere di controlli «informático» del datore di lavoro sugli strumenti tecnologici di «ultima generazione». RGLPS, I. P. 131–132.

34. Anton G. & Ward J. (1998). Every breath you take: employee privacy rights in the workplace – an Orwellian prophecy come true? Labor Law Journal, № 3. P. 906.

35. Kesan J. (2002). Cyber- working or Cyber-Shrinking?: a First Principles Examination of Electronic Privacy In the Workplace. Florida Law Review, V. 54. P. 299–300.

36. Fischer J. (2002). Implications of electronic mail policies for fairness and invasion of privacy: a field experiment. URL: http://sunzi1.lib.hku.hk/ER/detail/hkul/2652996. P. 3.

37. Fenoll-Trousseau M.P. & Haas (2002). La cybersurveillance dans l'entreprise et le droit – Traquer Être traqué. LITEC, Paris. P. 155-156.

38. Blanpain R. (2002). Some Belgian and European Aspects. Comp. Labor Law & Pol'y Journal, V. 24. P. 58.

39. Konrad-Klein (2006). Sinn und Unsinn von IKT-Sicherheitsrichtlinien. CF, № 9, p. 14. Also Becksschulze, M. (2003) Internet -, Intranet – und E-Mail-Einsatz am Arbeitsplatz. Der Betrieb, n.ºs 51/52. P. 2777.

40. Ray J.E. (2010). Actualités des TIC. DS, № 3. P. 273.

41. Hert P. & Gutwirth S. & Moscibroda A. & Wright D. & Fuster G.G. FUSTER G.G. (2008). Legal Safeguards for Privacy and Data Protection in Ambient Intelligence. Personal and Ubiquitous Computing, 13 (6). P. 435–444.

42. Valdés J.T. (2011). Computo en la nube: instrumento y objecto del derecho. Memorias del XV Congreso Iberoamericano de Derecho e Informatica, Buenos Aires, elDial.com.

43. Raport J. & Heyward A. (2009). Envisioning the Cloud: The next computing paradigm. Url last checked 20th November 2013 http://marketspacenext.com/inthemedia/envisioning-the-cloud/

44. Ponce J.P. (2011). Aspectos Jurídicos del Cloud Computing en Peru. Memorias del XV Congreso Iberoamericano de Derecho e Informatica, Buenos Aires, elDial.com

45. Ascensão J.O. (2003). Bases para uma transposição da Directriz nº 00/31 de 8 de Junho (comércio electrónico). Relatório, Conclusões e Parecer da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, Anexo 4, Diário da Assembleia da República, II Série-A, nº 79/IX/1, 2º/3/2003, Suplemento, pp. 3320 (41) – 3320 (55). P. 3320 (45).

46. Jones P. & Marsh D. (1993). Essentials of EDI Law. Electronic Data Interchange Council of Canada. P. 7

47. Carneiro D. & Novais P. & Costa R. & Gomes P. & Neves J. (2009). Embodied Monitorization. Tscheligi M. & De Ruyter B. & Markopoulos P. & Wichert R. & Mirlacher T. & Meshterjalkov A. (eds.) Ambient Intelligence. V. 5859. P. 133–142.

48. Daskala B. & Maghiros I. (2006). Digital Territories. Proceedings of 2nd IET International Conference in Intelligent Environments (IE06), Athens, Greece, July 2006.

49. Daskala B. & Maghiros I. Digital Territories Today – an example. URL: http://daisy.cti.gr/webzine/ Issues/Issue%203/Articles/Digital%20Territories%20today%20-%20An%20example/index.html

50. Oh J.S., Park J.S., Kwon J.R. (2010). A Study on autonomic decision method for smart gas environments in Korea. Ambient Intelligence and Future Trends – International Symposium on Ambient Intelligence (ISAmI).

51. Andrade F. (2012). Comunicações Electrónicas e Direitos Humanos: o perigo do "homo conectus". Direitos Humanos e sua efetivação na era da Transnacionalidade, Juruá Editora.

52. Solove D. (2009). La persona digital y el future de la intimidad. Derecho a la intimidad y a la protección de datos personales, Buenos Aires, Heliasta.

53. Andrade F. & Costa Â. & Novais P. (2011). Privacidade e Proteção de Dados nos Cuidados de Saúde de Idosos. Memorias del XV Congreso Ibero-Americano de Derecho e Informatica, Buenos Aires, elDial.com

54. Bettelli A.V. (2002). Agent Technology and Online Data Protection. Proceedings on the Workshop on the Law of Software Agents (LEA02).

55. Sartor G. (2003) L'intenzionalitá dei sistemi informatici e il diritto. Rivista Trimestrale di Diritto e Procedura Civile, Dott. A. Giuffrè Editore, Milano, Anno LVII. P. 23–51.

56. Sartor G. (2009). Cognitive Automata and the Law: electronic contracting and the intentionality of software agents. Artificial Intelligence and Law, Springer Science + Business Media B. V.

57. Rouvroy A. (2008). Privacy, Data Protection and the Unprecendented Challenges of Ambient Intelligence. Studies of Law and Technology, 2 (1). P. 8

58. Miguel C.R. (2004). El derecho a la proteccion de los datos personales en la Carta de Derechos Fundamentales de la Union Europea. Temas de Direito da Informática e da Internet, Coimbra Editora. P. 65.

59. Rouvroy A. & Poullet Y. (2009). The right to informational self-determination and the value of self-development. Reassessing the importance of Privacy for Democracy. Reinventing Data Protection, Springer. P. 45–76.

60. Janeiro D.B. (2002). La protección de datos de carácter personal en el derecho comunitário. Estudos de Direito da Comunicação, Instituto Jurídico da Comunicação, Faculdade de Direito, Universidade de Coimbra.

61. Brazier F. & Kubbe O. & Oskamp A. & Wijngaards (2002). Are Law-Abiding Agents realistic? Proceedings of the workshop on the Law of Electronic Agents (LEA '02)", CIRSFID, University of Bologna. P. 151–155.

62. Winn J. (2009). Technical Standards as Data Protection Regulations. Reinventing Data Protection, Springer. P. 191–206.

63. Lessig L. (2001). El código y otras leyes del ciberespacio. Taurus, Madrid.

64. Martínez R.M. (2009). Secreto de las comunicaciones y protección de datos en el âmbito laboral. Derecho a la intimidad y a la protección de datos personales, Heliasta, Buenos Aires. P. 83.

65. Farinho D.S. (2006). Intimidade da Vida Privada e Media no Ciber-Espaço. Almedina. P. 45–53.

66. Roig A. (2009). Privacy Enhancing Technologies (PET) and Web-Based Social Networks (WBSN). Proceedings of the 1st Workshop on Privacy and Protection in Web-based Social Networks, UAB Institute of Law and Technology, IDT Series, Barcelona.

ELECTRONIC CONTROL IN LABOUR RELATIONS

T.C. Moreira, F. Andrade

The use of information technology in the workplace has grown exponentially and surveillance and monitoring have become contentious 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 recourse to RFID technology, medical examinations and information for hiring or retaining an employee and ownership of personal information and the emergence of Ambient Intelligence have raised unprecedented concerns about privacy.

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 privacy not only to the people in general but also to all employees and even employers. The use of information and communications technology in the workplace 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.

With these new information and communications technologies, there are countless benefits for the workers and also for the employers, but, at the same time, these new technologies, namely the Internet and email, but also cloud computing and ambient intelligence, have been presenting new challenges, raising new questions and the rethinking of old ones. There is a need of an international approach to such issues, combining transparency tools and prohibitions, legal and technical measures, in order to enhance as much as possible the exercise of an informational self-determination right.

Keywords: privacy, electronic control, labour relations, cloud computing, ambient intelligence, fundamental rights.