Law/Technology

3rd Quarter 2007
Volume 40 / Number 3

World Jurist Association

WORLD JURIST ASSOCIATION

Section on Law/Technology

7910 Woodmont Avenue, Suite 1440; Bethesda, MD 20814; U.S.A.

ISSN 02.78-3916

Law/Technology 3rd Quarter 2007

VOLUME 40 NUMBER 3

The World Jurist Association believes that technology is particularly relevant to the progress and growth of worldwide law and legal institutions. The editors welcome for publication in this journal news on current activities in the field, manuscripts dealing with the relation of technology to law, and letters and comments of general interest.

CONTENTS

Law/Technology is published quarterly by the World Jurist Association, Section on Law/Technology, Suite 1440, 7910 Woodmont Avenue; Bethesda, Maryland 20814, U.S.A., Telephone (202) 466-5428. Individual subscriptions to Law/Technology are available and included in the Section fee of US$90.00 annually, which is in addition to Association or Center Fees. To join the Section, one must be a member either of one of the Associations of the WJA or of the general membership of the WJA. Library subscriptions are US$100.00 annually.

Postmaster: Send address change to World Jurist Association, Suite 1440, 7910 Woodmont Avenue; Bethesda, Maryland 20814, U.S.A

Editor's Note:

Are you interested in becoming more involved in the World Jurist Association? Are you looking for ways to join your colleagues in more active dialogue?

The Law/Technology Section of the World Jurist Association welcomes application from members to serve leadership capacities for the Section. As one of the oldest and most active sections of the WJA, the Law/Technology Section provides timely, authoritative and global perspectives on the interaction between technological developments and legal practice. Section officers are responsible to oversee the publication of this journal – *Law/Technology*, work closely with the WJA staff to design panels and programs for presentation, and set direction and objectives within the framework of the Association's strategic plan.

Members of the World Jurist Association are eligible to seek nomination to the Section Leadership. To express interest, and confirm your eligibility please contact the World Jurist Association. Section Leadership appointments will be made by the Board of Governors throughout the year until positions are filled. Appointments will be made based on expertise in the field, global diversity, and recommendations of colleagues.

For more information or to express interest please contact us at:

The World Jurist Association
Law/Technology Section
7910 Woodmont Avenue; Suite 1440
Bethesda, Maryland 20814
USA
Ph: +202 466 5428
Fax: +202 452 8540
E-mail: wja@worldjurist.org
Internet: www.worldjurist.org

NEW TECHNOLOGIES AND EMPLOYEES' RIGHT TO PRIVACY

By Dr. João Marques de Almeida

1. INTRODUCTION

Since the end of 20th century, the global community has been living in what has been named **the age of information**. This digital revolution – or even Third Industrial Revolution[1] – is based on the recent and overwhelming technological developments mankind has been witnessing.

It is unquestionable that information technologies currently available to most people have transformed the planet into a "global village" where information – once a precious asset – is now available to everyone in an immediate manner, rather than remaining a privilege of only a few.

This technological revolution has changed profoundly our society in several aspects. We do not intend to analyse all legal repercussion resulting from the provision of new technologies to the masses. However, we will focus on the issue of labour relationships and its adjustment to the advances in IT area.

2. REPERCUSSIONS OF THE TECHNOLOGICAL REVOLUTION IN WORK PERFORMANCE

Nowadays, IT tools are one of the most important elements to any company that, in its search for efficiency and profitability, wants to have the most suitable means to undertake its activity in the most expeditious and profitable way possible by reducing costs and increasing profits.

[1] After the steam engine that originated the first industrial revolution (1760 to 1850) and the second industrial revolution (1860 to 1980) caused by (i) the discovery of electricity, (ii) Henry Ford's assembly lines and (iii) Frederick Taylor's scientific management method, some claim that we are currently living a third industrial revolution – see, *inter alia*, *Lester Thurow, in Building Wealth: The New Rules for Individuals, Companies, and Nations in a Knowledge-Based Economy* (1999).

Accordingly, there are considerable investments in technological means being made, which must obviously be placed at the disposal of the work force employed by the company.

Thus, it is in the company's best interest to provide its employees with advanced technical tools so that they can have immediate access to all information they need to carry out their work. Nevertheless, such availability of technological means does not come without risks which, in an increasingly competitive market, all companies try to eliminate or, at least, mitigate as much as possible.

On the one hand, the employing company wants to guarantee that the significant IT investment made to provide its employees with adequate tools and ensure a competitive advantage over its competitors, is being effectively used in the performance of their tasks (and not for their personal use). On the other hand, storing information in a digital support carries the danger of confidential information leakage (whereas today it is possible to store massive amounts of data in increasingly reduced and inconspicuous instruments).

Although it is essential to provide employees with rapid and effective means of accessing and exchanging information, great care should be taken to ensure that these resources are used in the best interest of the company that made the IT investment and not for the employees' personal use or against the company itself. For this reason, new technologies also brought new ways of monitoring the employee's activities, which raises pertinent legal issues that we will address below.

3. MEANS OF MONITORING EMPLOYEE'S ACTIVITY

With the implementation of the new information technologies, the companies now have at their disposal the possibility of greater control over the employee's activity and the employee himself. There are means of distance surveillance available to any company, even the most modest one, that if taken to extremes allow access in real time to all employee's activities, revealing his every move within the company. Basically, the well known *Big Brother* would keep an eye on the

employee during the entire time in which he is at employer's service. We refer not only to (i) audio and video records of the employees' activity, but also to (ii) the files and Internet web sites he accesses trough the company's network, (iii) the time he spends with each daily task, (iv) records of telephone calls and (v) the content and addressees of his *e-mails*. To sum up, all of the employee's work, exercised by whatever means the employer makes available to such effect. Some companies even monitor the time employees spend in the bathroom[2].

Among all monitoring means of supervising the work performed within the company, we will only focus on the so called *cyber-surveillance – i.e.* surveillance using computerized tools. In particular, the monitoring activity by which, through computerized mechanisms, all work carried out through the PCs is monitored and controlled by the company.

This monitoring method is probably the most intrusive of all methods currently available to the companies. As a matter of fact, the arrival of new information technologies enhanced the control of the work process itself, no longer being limited to mere location and scrutiny of the employee's physical presence and allowing direct control of the work that is (or not) being performed. Nevertheless, our article will focus mainly on the supervising of the use of the companies' Internet and e-mail account, which raises important questions in respect of the employees' right to privacy as we shall see below.

4. MONITORING THE USE OF COMPANY INTERNET AND E-MAIL

Under the aegis of defending employers' interests some acts of surveillance that attempt against fundamental rights of employees have been practiced. It is true that the protection of the employers' legitimate interests should not be neglected. If one takes into consideration that the employer is providing the PCs and e-mail accounts to the employees, paying all related electricity and Internet connectivity bills, in addition to purchasing all software licenses

[2] By ruling of the National Commission of Data Protection nr. 32/96, of 4 June 1996, the automated processing of data (trough magnetic card) in Portugal was considered illegal since it aims to control the employees' presence in the bathroom and constitutes an attack on their privacy and human dignity.

necessary for the performance of their tasks and supporting the costs of network maintenance, he certainly has the right to demand that these means be used in the best interest of the company.
In accordance with its power of direction (Article 150 of the Portuguese Labour Code) the employer is entitled to demand that its employees perform their tasks in an appropriate manner, and refrain from using the means available to them (which required considerable investment) for their personal entertainment or during working hours at the company's expenses. There are also legitimate concerns as to the leakage of confidential information by accessing certain potentially dangerous websites and being exposed to attacks by hackers. Downloading illegal contents or material from unknown sources bears the risk of viral infection with disastrous consequences to the company's IT system and productivity, thus causing economic damage.

Corroborating what has been said above, we cannot fail to emphasize that the majority of studies suggest that Internet users spend more time and money online at their workplace than in any other location[3]. There is also the danger of sending e-mail messages with sensitive contents to unknown recipients under the employer's signature, which could lead not only to the leakage of inside information but also cause damages to third parties (e.g. through the dissemination of computer viruses or inappropriate content) who may in turn demand compensation to the company for the aforementioned damages.

It has also been stated that enabling employees to use the *Internet* and e-mail for personal or recreational purposes, is in line with the best labour practices (*i.e.* those rules referring to the creation and maintenance of a good working environment and, consequently, to the increase of the employees' productivity and business' profitability), as long as they do so with appropriate moderation and reasonableness. Indeed, it seems preferable to allow the effective use of the Internet and e-mails for personal purposes rather than banning them entirely, which could result in a labour conflict and/or discourage and reduce the employees' productivity, which would, of course, also affect the company.

---

[3] According to Amadeu Guerra, in "A Privacidade no Local de Trabalho – As Novas Tecnologias e o Controlo dos Trabalhadores através de Sistemas Automatizados, uma abordagem ao Código do Trabalho", Almedina, 2004, p. 366

In other words, more than the fundamental rights of the employees ruled by Portuguese Constitutional Law (e.g. the right to privacy and preservation of a private life), the right to a personal life at work is also at stake[4].

In view of the above, there is a collision between the company's right to demand that the performance of work by its employees is carried out in a proper manner and the right of the latter to privacy and/or preservation of their private life, which requires a careful balancing of interests. Thus, the question should be whether the company can be allowed to control the access of its employees' to the Internet and the internal e-mail accounts and, if so, in which way.

5. CONTROL OF INTERNET AND E-MAIL USAGE IN INTERNATIONAL LAW

International law includes a serie of provisions, such as Article 8 (1) of the European Convention on Human Rights (ECHR), establishing that everyone has the right to their private and family life, their home and correspondence.

On the other hand, the European Court of Human Rights has made use of the aforementioned Article 8 (ECHR) in several cases concerning communications through classic mail. In the "*Niemitz*" case (1992), the Court considered that commercial correspondence (e.g. work communications) is included in the aforementioned Article[5].

As far as EU Law is concerned, one of the most important set of rules is the Directive 95/46/EC of the European Parliament and of the Council, which regulates the protection of personal data and the free circulation of such data ("Data Protection" Directive[6]). This directive acknowledges the right to privacy in the same way as Article 8 of the ECHR[7].

---

[4] On the issue of the right to a personal life at work, see Maria Regina Redinha, in "Os Direitos de Personalidade no Código do Trabalho: Actualidade e Oportunidade da sua Inclusão" and Larissa Darraq, in "La Proteccion de la vie personnelle du salarié au travail", Semaine Sociale Lamy, supl. Nº 940, 28-6-99.

[5] See the opinion of the "Data Protection" Work Group, created by Article 29 of the Directive 95/46/EC about the rendering of e-mail filtering services, approved in 21 of February 2006, available in http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm.

[6] Available for reading in http://eur-lex.europa.eu

[7] See recital nr. 10 of Directive 95/46/EC

The same position is taken by Directive 2002/58/EC of the European Parliament and of the Council – recently modified by Directive 2006/24/EC of the European Parliament and of the Council, 15 of March 2006 – concerning the processing of personal data and the protection of privacy in the electronic communications sector, which deals with the treatment of personal data in the context of performing electronic communication services in public networks[8].

More recently, the Data Protection Work Group created by Article 29 of Directive 95/46/EC published an opinion on the performance of e-mail filtering services, focusing on the filtering of contents of e-mail messages sent by Internet services (ISP – Internet Service Providers) and by electronic mail services (ESP – Email Service Providers). According to such opinion, filtering e-mails with the intent of finding viruses and detecting spam (mass forwarding of non-solicited electronic messages) are, in principle, allowed since it guarantees the security and proper functioning of computer systems. Nonetheless, the confidentiality of the information must be assured and in the cases of anti-spam control it is recommended that users are given the possibility to choose whether or not to submit their messages to such filtering.

As to the filtering of messages to detect any other predetermined contents, such action is no longer considered by the Data Protection Work Group as a technical and organized mean of protecting the safety of services and, consequently, is no longer admissible and constitutes an attack to the right to privacy and the freedom of communication.

6. CONTROL OF INTERNET AND E-MAIL USAGE IN OTHER LEGAL SYSTEMS

In the United States of America, the *Electronic Communications Privacy Act* (1986) regulates, in general terms, the monitoring and control of the use of Internet (and other electronic communications means) either by the employer or any other entity. In the US the *monitoring* activity is being used by major companies and the employer is considered not only as the owner of the technical means at its employees' disposal but also possesses the power to control the said means.

[8] Portuguese version available in www.icp.pt

In *Bourke v. Nissan* (1993), two employees were discharged on account of having exchanged messages with sexual contents through their company's e-mails. The employees argued in court that those messages had a private nature and were illegitimately intercepted by the employer. However, the court sided with the employer, considering that the computer system is its property and the company has the right to access all contents of the aforementioned computer system. The court also decided that the individuals' constitutional right to privacy (established in Amendment 4 of the American Constitution) is only violated if the person has a reasonable expectation of privacy which in this matter was not the case since the subject at hand was the employer's e-mail.

Also in *McClaren vs. Microsoft* (1999), one employee pleaded that his right to privacy had been violated by his employer who, during an investigation of a sexual harassment claim, read his e-mail messages, stored and password-protected in a personal folder in the employee's computer, discharging him based on the contents of those messages. In this case, the employee had previously informed the employer that the said folder contained personal information which was what induced the employer to read its contents. The court considered once again that there was no reasonable expectation of privacy from the employee since the e-mail account belongs to the company.

In view of the above, it is possible to draw the conclusion that electronic surveillance of employees under the US legal system is generally allowed.

In the French legal system, it has been defended[9] that the employer may use computer mechanisms to control the usage of Internet and e-mail, as long as it is done with respect to the principles of loyalty, transparency, relevance and proportionality foreseen in Article L. 120-2 of the French Labour Code and as long as information of professional character is involved. Companies will have to (i) report to the *Comission Nationale de l'Informatique et des Libertés* which control mechanisms they intend to activate, (ii) consult previously with the employees' commission (under Article L. 432-2-1 of French Labour Code) and (iii) inform the employees

[9] See « La Cybersurveillance Sur Les Lieux de Travail » published by the ***Comission Nationale de l'Informatique et des Libertés (2004 edition)*** available at: http://www.cnil.fr/fileadmin/documents/approfondir/rapports/Rcybersurveillance-2004-VD.pdf.

about the supervision measures to be put into effect, but always respecting the limits of their private life.

In respect of English and Wales Law, *The Regulation of Investigatory Powers Act 2000*, rules the interception of electronic communications, subjecting all monitoring and interception actions to the consent of the user which can, however, be presumed. On 24 October 2000, came into effect the *Lawful Business Practice Regulations,* which regulate the interception of electronic communications by the employer even without consent. These regulations rule (i) the control of e-mail messages exchanged at the workplace and, (ii) the control of electronic communications by the government. In general terms, interception of electronic messages is restricted, except: i) if authorised by the government for public safety reasons, ii) if consented, or iii) if it is a work message. However, the concept of "work message" is open for different interpretations. One could even argue that all messages sent through the company e-mail address are work messages and are therefore subject to its scrutiny. Such interpretation originated strong reactions from the unions.

Spanish law rules that any measures of surveillance and control of the employees' activity are to be implemented bearing in mind their human dignity (see Article 20 (3) of the E*statuto de los Trabajadores*). It is therefore acknowledged to the company the power to adopt procedures of surveillance and control of the employees, with the aim of ensuring the fulfilment of their obligations and duties under the employment contract. However, the legislator sought to establish certain limits, namely those ruled by the Spanish Constitution which guarantee the right to the confidentiality of communications (Article 18 (3)) and the employee's right to privacy (Article 18 (1)). The violation of any of these rights is subject to criminal punishment and to the payment of several fines, according to Article 197 (1) of the Spanish Penal Code.

Spanish courts have considered that the employer can, in fact, monitor the employee's labour activities and even justify the termination of the employment relationship on the basis of said monitoring. However, the powers of the company will always be limited by an unrelenting respect for the employee's dignity and privacy, as described above.

7. CONTROL OF INTERNET AND E-MAIL USAGE IN PORTUGAL

Before the entering into force of the Labour Code approved by Law 99/2003, 27 of August, there was no any specific law or regulation in the Portuguese legal system on the electronic control of labour activity.

As explained above, the biggest obstacle to the monitoring of the use of the Internet and the employee's e-mails consists on the protection of the individual right to privacy as a fundamental principle of Constitutional Law that any employer must comply with.

Article 26 of the Constitution of the Portuguese Republic (CPR) establishes the principle of respect for the right to privacy of personal and family life of all people. On the other hand, Articles 34 and 35 sanction the inviolability of "*correspondence and other means of private communication*" and the appropriate use of information technologies in the processing of personal data. These rules are considered as fundamental rights, freedoms and guarantees. As such, they can only be restricted in cases expressly provided for in the Constitution, and all restrictions must be limited to a certain extent, in order to protect other constitutionally protected rights or interests – see Article 18 (2) CPR.

Furthermore the "*right to intimacy of private life*" is acknowledged as a right of personality under Articles 70 and 80 of the Portuguese Civil Code. It is well known that rights of personality originated from the principle of respect for human dignity and personality, a principle of natural law which overcomes the legislator itself – even the constitutional legislator –, the judges, the lawyers and all individuals. This principle is applicable even if not mentioned in the Constitution or in ordinary law and regardless of what might be ruled differently. Thus, we are face to face with a form of *supra* legal guardianship that derives from the very notion of Law[10].

Still on the subject of rights of personality and as a development of the right to intimacy of private life, Articles 75 to 80 of the Portuguese Civil Code protect the content of letters and other writings. Any violation of correspondence or telecommunications is considered as a criminal offence under Article 194 of the Portuguese Penal Code, as a way to protect the individual right to privacy. According to this Article 194:

[10] On this issue see Pedro Pais de Vasconcelos, in "Teoria Geral do Direito Civil", Almedina, 2005, p. 44 and subsequent.

"(...)

1. Whosoever opens a package, letter, or any other sealed item not addressed to him, without consent, or becomes aware of its contents through technical procedures, or prevents in any way the addressee from receiving it, will be punished and sentenced to up to one year in prison or fined.

2. The same penalty is also applied to whoever meddles or retrieves the content of communications without consent.

(...)".

Law 67/98, 26 of October, which adopted Directive 95/46/EC of the European Parliament and Council, 24 of October, on the protection of individuals with regard to the processing of personal data and the free movement of such data[11], also establishes as a general principle the processing of personal data in the strict respect for individual privacy[12].

Therefore, the electronic control of the employee's activity was already prohibited, before the new Labour Code came into effect, provided said control endangered the employee's right to privacy (with magnitude to be measured according to the limits imposed by the very nature of things[13]). With the new Portuguese Labour Code (approved by the Law 99/2003, 27 of August), this matter is now expressly regulated in the Portuguese labour law.

The new Labour Code includes a section on rights of personality, although some may consider such section unnecessary considering that rights of personality do not require express legal provision and were already ruled by Article 70 and seq. of the Civil Code. In any case, the new Labour Code expressly sanctioned (i) the right to privacy of both the employer and the employee (Article 16), (ii) the prohibition of the use of remote means of surveillance at the work place with the aim of controlling the employee's professional performance (Article 20) and (iii) the confidentiality of messages and of the access to information (Article 21). We consider that by introducing these express rules, the new Portuguese Labour Code had the virtue of clarifying certain previous doubts in this matter.

---

[11] According to chapter 4.1 above.

[12] Article 2 of Law 67/98, 26 of October.

[13] See ARTHUR KAUFMANN, *"Analogie und "Natur der Sache" – Zugleich ein Beitrag zur Lehre vom Typus"*, 2. Aufl., Decker & Müller, Heidelberg, 1982, p. 55-57 and Pedro Pais de Vasconcelos, in "A Natureza das Coisas, Estudos em Homenagem ao Professor Doutor Manuel Gomes da Silva", Faculdade de Direito da Universidade de Lisboa, 2001.

We must also point out that the protection granted by these rules works both ways since it is established that the said rules apply to employee and employer. Moreover, the position of the employer is also protected under the constitutional rules (e.g. the right to freedom of trade granted to all company under Articles 61 and 80 (c) CPR). Since the employee is likely to suffer abuses, considering that in most cases he/she is the weakest link of the contractual relationship, the legislator had greater concern with the protection of his/her rights, but this does not mean that those will prevail over the interests and rights of the employer. It is necessary to make a case-by-case careful assessment of the interests in conflict.

As far as the means of remote surveillance are concerned, the Labour Code[14] establishes that the company cannot implement them, through the use of technological equipment with the goal of controlling the work performance of employees. However it is allowed the use of means of remote surveillance to ensure the protection and safety of individuals and property, or in other particular requirements inherent to the nature of the activity. In this case, the company must notify the employee in advance of the implementation and purpose of these means of surveillance which include not only the installation of video cameras and microphones in the workplace, but also the control of the tasks performed through quantitative and descriptive computer records. Thus, telephone communications, Internet connections, any movements in the workplace, the employee's exact geographic location, etc., everything can be technically monitored. However, the Law only allows it for the protection and safety of individuals and property (e.g. installation of video cameras outside gas stations) or in other special requirements inherent to the activity (e.g. the supervision of casino employees or bank cashiers), bearing in mind that the use of those means may not be omitted to the employee.

We must reiterate that, by virtue of the new information technologies, these new forms of control of work performance often reach intolerable levels, not only through the imposing of super-human work rates, but also by tearing down the employee's private life. The rules of the new Labour Code recognize that employees are entitled to a personal life at work[15], as a corollary of their right to privacy.

[14] Article 22 of the Labour Code.
[15] See note 4 above.

In any case, the employer's choice of methods of control must always respect the principles of necessity, sufficiency, reasonableness, proportionality and good faith in the work relations. The lawful use of these methods requires a prior notice to the employee(s) (Article 20 (3) of the Labour Code).

Under Article 28 of Law 35/2004, 29 July, the use of the aforementioned methods of remote surveillance are subject to previous authorization by the Portuguese Data Protection Commission, as regulated by Law 67/98, of 26 October (Law of Personal Data Protection). The application requesting such authorization must be accompanied by the opinion of the employees' committee or, if they fail to issue such opinion within 10 days, the initial message requesting their opinion.

Prior to these recent labour rules and regulations coming into effect, the Data Protection Commission had already defined the principles on privacy in the workplace[16], which can be summarized as follows:

i) before engaging in any type of data processing, the employer must inform the employees on (i) the terms and conditions in which they can use the company's technical means for personal purposes, (ii) the communications monitoring procedure used by the company and its purposes and (iii) the consequences of improper use of said means;
ii) the business interest that justifies such monitoring should be serious and non-abusive, which cannot be disproportionate to the level of protection of the employee's privacy;
iii) the implementation of generic methods of control is to be privileged, avoiding individual consultation of personal data.

These principles established by the Data Protection Commission render the total restriction of Internet and e-mail usage in the workplace for personal purposes unrealistic and counterproductive. We agree with this position. However, we must not forget that Articles 61

[16] Available in www.cndp.pt.

and 80 (c) of the Portuguese Constitution also recognise the right to incorporation of companies and trade.

The Supreme Court of the State, by ruling of 8 February 2006[17], has accepted these principles established by the Data Protection Commission and considered that the capturing of images with video cameras installed in the workplace and directed at the employees is illicit and violates their right to privacy by subjecting the performance of their work to continuous and constant surveillance. Furthermore, such measure was not considered as an appropriate means of protecting the company's assets from employees' theft.

On the other hand, Article 21 of the Labour Code establishes a right of reserve and confidentiality of the employee regarding the content of personal messages and access to the non-professional information that is sent, received or researched, namely through e-mail. In other words, the employee's right to a personal life at work is established, whether in accessing information available on the Internet, or in sending and receiving electronic mail.

However, paragraph 2 of the same Article grants the employer the possibility of establishing rules for the use of the company's means of communication, namely e-mail. This rule restores the balance required by the very nature of things, balancing the employee's right to privacy with the employer's right to the interests of the company.

So on the one hand, the confidentiality of the employee's messages of personal nature (either in the form of the traditional letter, or by electronic form, namely e-mails) and the confidentiality of the information accessed through Internet websites are protected. On the other hand, however, the employer's right to establish rules for the use of communication and technological means available for its employees is also established, being the employer free to establish time and access limits to certain predefined contents, always with due respect to the principles of proportionality and appropriateness.

[17] Available in www.dgsi.pt.

The doctrine[18] has supported that the viewing of the employee's personal messages by the employer is only justified in isolated cases. When this viewing is justified, the employee must be present and the said viewing should be limited to the recipient's or the sender's address, the subject, date and time of the message.

When there are no grounds for the control of the company's e-mail, such control should take place in random form instead of a persecuting way, having the purpose of ensuring network security.

By the same order of reason, the control of Internet websites to which the employee accessed should be undertaken in a generic, non-persecuting way.

The contents of the guiding principles set out by the Data Protection Commission are closely followed which, in the subject of e-mail control, establish that:

i) the fact that the employer forbids the use of e-mail for private purposes does not automatically allow the right to open e-mail addressed to the employee;

ii) e-mail control should especially pursue the safeguard of the computer system's safety and performance;

iii) the need for detection of virus does not allow *per se* the reading of received e-mail;

iv) any control based on the prevention or detection of disclosure of professional and/or commercial secrets should be exclusively directed at people who have access to those secrets and only when there are grounds for suspicion; and

v) access to the employees' e-mail should be the last resource to be used by the employer, and such access is to be preferably done in the presence of the employee and of a representative of the employees' committee.

Concerning the principles regarding the supervision of Internet usage:

[18] Among others, Pedro Romano Martinez, Luís Miguel Monteiro, Joana Vasconcelos, Pedro Madeira de Brito, Guilherme Dray and Luís Gonçalves da Sila, in "Código do Trabalho anotado, 3ª Edição", Almedina, 2004, p. 114 and Luís Menezes Leitão, in "Código do Trabalho Anotado", Almedina, 2003, p. 44.

i) a certain degree of tolerance towards Internet access for private purposes should be allowed, especially if it occurs after working hours;

ii) the advantages of Internet access are to be taken into consideration for both the company and the employee; and

iii) the performing of statistic and generic studies should be enough to establish if productivity is being affected by relentless Internet access, being allowed a search on which websites were accessed from the company without identifying specific workstations.

We agree with these general principles which seem adequate to solve and protect the real rights of the employees and employers in a reasonable and proper way.

We must accept that the employer can, in certain situations, suffer damages due to the protection granted to their employees' right to privacy. However, we cannot forget that this is justified due to the legal degree of protection granted to the right to privacy as a fundamental right of personality, having the legislator restricted the lawful means of opposition to this right to situations of possible abuse, taking into consideration that the employee is usually the most fragile element in the employment relationship.

Thus what effective mechanisms does the employer have to protect its investment and to ensure the productivity of its business? The most important one would be the mechanism of Internal Regulation, establishing clear rules for the use of technological means having in mind the adequacy of these rules to the company (*i.e.* its size and area of operation), keeping also into consideration that excessive restriction is harmful, since it decreases productivity and profitability.

The first advantage of this Internal Regulation is the deterrent effect of the misuse of computer resources by the employees. On the other hand, being the rules clear and appropriate, the employee may not justify any misuse of these resources with the ignorance of those rules or with the fact that it is not legitimate to expect that he was aware that they could not be used in such

way. In what concerns possible damage to third parties (for example through the spreading of computer viruses) it will be easier for the employer to refuse to undertake responsibility, imposing it solely to the employee who violated the company's internal procedures.

Lastly, any violation of such rules will be a disciplinary infringement, which may justify a dismissal with just cause (being such infringement not existent if the employer does not regulate the use of e-mail and Internet). However, the doctrine[19] has also supported that said infringement does not legitimate the breach by the employer of the employee's right to privacy. How to solve this apparent contradiction? The solution[20] will be to consider the employee's appeal to his right to privacy in order to justify the wrongful compliance of his employment contract as a situation of abuse of rights ruled under Article 334 of the Portuguese Civil Code. Once again, a careful consideration of the interests in conflict prevails.

Regarding the institution of the abuse of rights, Article 334 of the Portuguese Civil Code establishes that:

> *The exercise of a right is considered illegitimate when the party in question manifestly exceeds the limits imposed by good faith, good customs, or the social or economic purpose of such right.*

The principle of good faith in contractual performance, implicit on the institution of the abuse of rights is expressed in Article 119 (1) of the Labour Code which states that: *The employer and the employee must proceed in good faith as to the performance of their respective obligations as well as to the exercise of their respective rights.*

Thus, the employer's and the employee's subjective rights must be exercised honestly. Consequently, the employee may, in certain circumstances, appeal to his right to privacy with bad faith in mind, in an attempt to conceal his own blameworthy conduct. The employer's interest should prevail in this kind of situation.

---

[19] See Pedro Romano Martinez, Luís Miguel Monteiro, Joana Vasconcelos, Pedro Madeira de Brito, Guilherme Dray e Luís Gonçalves da Silva, in "Código do Trabalho Anotado, 3ª Edição", Almedina, 2004, p. 114 and 115.
[20] *Idem.*

Regarding the decisions of Portuguese courts on this subject, we stress the sentence of the Supreme Court of Justice, dated 5 June 2007[21]. This Court found the following conclusions: (i) if the employer did not regulate the use of the company's e-mail, the use of it for personal purposes cannot be considered a disciplinary infraction; (ii) the circumstance of the addresser and the addressee referring to aspects of the company in the message is not sufficient to grant it a professional nature; (iii) the lack of clear indication that the message is of a personal nature does not impede the protection of Article 21 (2) of the Labour Code; (iv) said protection implies that proof obtained through violation of the employee's right to privacy is considered null – according to Article 32 (8) of the Portuguese Constitution.

This court goes even further by deciding that it would be legitimate for the superior of the employee who was ultimately dismissed, to access the e-mail of the latter (eg. the employee is on vacation or sick), if he believed he was accessing information of professional nature but, in case he found out that the message was of a non-professional nature, it would be the superior's duty to stop reading the said message and refrain from disclosing its contents, not being possible to use it as evidence in a disciplinary proceeding. In his appeal, the employer claimed that the employee incurred in a situation of abuse of right when the latter appealed to his right to privacy in order to justify his illicit action. However, considering what we described above, the Supreme Court of Justice found that such abuse has not occurred.

In conclusion, we consider that the employer's position will be effectively safeguarded by the establishment of clear internal rules which, for example, forbid the use of company e-mail for personal purposes, allowing employees to use e-mail addresses for such purposes. In this way, if the employer has good reasons to suspect that an employee is not performing his duty properly because of the use of company e-mail address for his own personal purposes, he may demand that the latter indicates if any message sent from said address is of a personal nature. Faced with this situation, either the employee denies the personal nature of the message and, as a consequence, must allow to the employer the access of the contents of said message, without violation to his right to privacy, or he confirms that there are indeed messages of a personal

[21] Available in www.dgsi.pt

nature, which would result in a disciplinary infraction without the need for the employer to access to the contents of such messages.

It is obvious that the seriousness of the infraction can only be determined by accessing the contents of the message. Bearing this in mind, we believe that, in certain specific cases, the employee may be in abuse of rights when he appeals to his right to privacy of communications, namely when relevant interests of the company are involved, such interests capable of harming the company's future and its constitutional right to trade (Articles 61 and 80 (c) of the Portuguese Constitution). However, a careful case-by-case consideration will always be needed, with the employee's right to the reserve of his private life as a rule. Any deviation of this rule will only be admitted in exceptional cases. Still, when good faith imposes it, the employer's interest may prevail with certain restrictions.

Thus, the courts must in a considerate way be aware of possible ungrounded claims of abuse of rights, which must always be of an exceptional character, having in mind, that the weakest link in the core of the labour relationship is usually the employee. It is still important however to be aware that, in an increasingly competitive world, companies may sustain serious damage with the performance of their employees, also capable of damaging the general public in as far as they reduce employment and wealth. Thus, the employer's protection may not be put aside in all circumstances simply by invoking that they are not the ones in need of protection.

SUBSCRIPTION AND ADVERTISING RATES 2007-2008

The World Jurist Association
Law/Technology Journal
7910 Woodmont Avenue; Suite 1440
Bethesda, Maryland 20814
USA
Ph: +202 466 5428
Fax: +202 452 8540
E-mail: wja@worldjurist.org
Internet: www.worldjurist.org

Law / Technology Journal

This quarterly law journal enjoys a worldwide circulation in over 50 countries and is received by private libraries, organizations, and every major law school in the United States and most schools overseas.

Law/Technology Journal Subscription Rates:

Libraries, Agencies, and Organizations:	$100.00 (4 issues)
Individual Members of the WJA:	$90.00 (4 issues)
Airmail Delivery, if desired:	$20.00 additional fee

World Jurist Newsletter

This bi-monthly newsletter is distributed to over 1500 members, subscribers and other NGOs in the field of international law. The distribution reached nearly every country in the world.

World Jurist Newsletter Subscription Rates:

Libraries, Agencies, and Organizations:	$90.00 (6 issues)
Individual Members of the WJA:	included in membership (6 issues)

Advertising Rates:

Full Page (7"w x 10"h):	$1000.00
2/3 Page (4 ½"w x 9 5/8"h—vertical columns):	$750.00
(7"w x 6"h—square):	$750.00
1/2 Page (7"w x 4 ¾"h):	$500.00
1/3 Page (2 ¼"w x 9 5/8"h—vertical columns):	$300.00
(4 9/16"w x 4 ½"h—square):	$300.00
1/6 Page (2 1/8"w x 4 ¾"h):	$250.00

Prices reflect the cost for placing a **camera-ready, black/white** advertisement in one issue of our quarterly journal (*Law/Technology*) or one issue of our bi-monthly newsletter (*The World Jurist*). For best results, ads should be sent electronically in PageMaker, Word, or PDF format. For color advertisements or for special requests please contact us - we will make every effort to accommodate your needs.

Both publications enjoy a wide national and international readership in more than 140 nations. In addition to private subscriptions, they are also featured in many highly acclaimed law schools around the world.

The World Jurist Association is a non-profit, non-political, non-governmental organization dedicated to the promotion of world peace through the Rule of Law. All advertisements will be strictly scrutinized to ensure that they are non-political in nature.

The World Jurist Association
Law/Technology Journal
7910 Woodmont Avenue; Suite 1440
Bethesda, Maryland 20814
USA
Ph: +202 466 5428
Fax: +202 452 8540
E-mail: wja@worldjurist.org
Internet: www.worldjurist.org