Evisa Kambellari[1]

Employee email monitoring and workplace privacy in the European perspective

1. Introduction

The question of workers' electronic surveillance has recently drawn considerable attention due to the increased use of information technology in the workplace, and the eventual implications of monitoring operations, with the right to respect private life. It is broadly accepted among European countries that employees should enjoy a certain reasonable expectation of privacy and confidentiality of their communications in their workplace since in the course of their working lives, they might develop relations which extend beyond the professional domain. Given that working activity results from a constant combination of professional tasks with employees' individual values, it becomes difficult to clearly separate professional actions from those having a personal nature. In this respect, employers should recognize a certain degree of employees' privacy at the workplace and implement proper organisational and operational measures towards protecting their *private sphere*, within the work environment.

However, the employees' right to confidentiality of their communications must be balanced with the legitimate interests of the employer to run his business efficiently, and to protect himself from the liability that employees' actions may cause[2]. Some of the main legitimate grounds for applying workers' email monitoring methods consist of: safeguarding employee productivity from any waste of time dealing with e-mails that are not relevant to his job; protecting the company from potential lawsuits resulting from e-mail misuse such as sexual harassment, bullying or racist comments, or the unlawful downloading of materials; ensuring the confidentiality of company information that can inadvertently or intentionally be disclosed, and minimizing the viruses and spywares risks exposed to the company network due to the careless sending and opening of emails[3]. In conclusion, before undertaking any monitoring operation, it is essential for the employer to designate special technical and operational measures, in order to avoid the disclosure of employees or third parties personal information, not necessarily related to the work activity.

---

[1] Assistant Professor of Criminal Law at Faculty of Law, University of Tirana, Albania.

[2] See: Mitrou. L. & Karyda. M. (2006). Employees' privacy vs. employers' security: Can they be balanced ? *Journal of Telemaics and Informatics.* Vol. 23 (3), pp. 164–178.

[3] See: Wallach. Sh. (2011). The Medusa Stare: Surveillance and Monitoring of Employees and the Right to Privacy. *The International Journal of Comparative Labour Law and Industrial Relations.* Vol. (27) 2, pp. 189–219.

2. The EU legislative framework

In the legislative framework of the European Union there are no specific provisions concerning employees' email monitoring. However, the confidentiality of communications in the employment sector is mainly guaranteed in accordance with international instruments relating to human rights, in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms and the Charter of Fundamental Rights of the European Union. The first point of reference is the Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms of 1950, which in Article 8 states that *"Everyone has the right to respect for his private and family life, his home and his correspondence"*. In the second paragraph of the disposition it becomes clear that the right is not absolute, and under some exeptional situations public authorities may interfere in its exercise. So, the interference should be in accordance with legal norms and necessary in a democratic society, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. The Charter of Fundamental Rights of the EU, proclaimed in December 2000, also has a special passage on the right to respect of private life. Within Article 7 it is promulgated that there is an existance of *'the right of every citizen to respect for his private and family life, home and communications'*. The term correspondence has been replaced by the term communication in order to make the provision more adaptable to new technological developments.

The European Union does not have a statutory provision that generally addresses an employer's right to monitor his employees' electronic mail, but there are provisions in the EU Data Protection law that deal with privacy issues specific in employment situations[4]. The right of privacy in the workplace can be inferred by referring especially to Directive 95/46/EC on the protection of individuals with regard to the processing of personal data, and Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.

2.1 The Data Protection Directive (Directive 95/46/EC)

Directive 95/46/EC is the main reference text at the European level on the protection of personal data. In terms of the Directive, "personal data" means any information relating to an identified or identifiable natural person, while "data processing" should be understood as any operation such as collection, recording, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available… performed upon personal data. Given that, it can be stated that the monitoring of workers' email by the employer involves the processing of personal data[5], and as such, falls within the scope of the Directive.

Its primary aim is to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the

[4] See: Kierkegaard. S.M. (2005). Reading Your Keystroke: Whose Mail is it ? - Trust, Privacy, and Security in Digital Business. *Lecture Notes in Computer Science* . Volume 3592, pp. 256-265.

[5] See: Opinion 8/2001 of the Data Protection Working Party of 13 September 2013 on the processing of personal data in the employment context, p.13. Available from: http://ec.europa.eu.

processing of personal data by setting out major standards that should be met from the processors. In this respect, the main rules are those related to the data quality, the legitimacy of their processing and the possible restrictions that can be applied on the processor. The *data quality* provisions require that personal data be processed fairly and lawfully, collected for specified, explicit and legitimate purposes[6]. They must also be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed[7]. In terms of the legitimacy of processing, there are two major questions to be considered: whether the subject whose data is being disclosed has given his unambiguous consent or processing is necessary for the purposes of the legitimate interests pursued by the controller[8]. It is important to note that the controller's right to access and process personal data in the case of *extrema ratio*[9], is subject to some restrictions. *First*, the disclosure of personal data for satisfying a legitimate interest of the controller cannot be carried out when such an interest is overridden by the interests for fundamental rights and freedoms of the data subject. *Second*, in any case that a lawful controlling practice is being held, the controller has the duty to provide to the data subject information, as to whether or not data relating to him is being processed, and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data is disclosed[10].

Article 29 of Directive 95/46/EC create a Working Party on the Protection of Individuals with regard to the Processing of Personal Data, whose main task is to examine any issues covering the application of the Directive at a national level[11]. In May 2002, this Advisory Body issued

---

[6] The need of the employer to protect his business from significant threats, such as to prevent transmission of confidential information to a competitor, can be such a legitimate interest.

[7] See: Article 6 of Directive 95/46/EC.

[8] Under Article 7, Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed.

[9] The term means that any act of intrusion into the worker's email should be authorised only when the pursued interest can not be accomplished by using other means.

[10] See: Article 14 of Directive 95/46/EC .

[11] The Committee has an advisory status which consists on advising the Commission on any proposed amendment of the Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data, as well as making recommendations

the Working Document *'On the Surveillance of Electronic Communications in the Workplace'*. Regarding worker's email monitoring the Document provides guidelines about what constitutes legitimate monitoring activities, and the possible limits of the employer's right to control. In practical terms, it seeks to substantially explain the fundamental principles which must govern all personal data processing activities in the employment context. In the following part of this paper we shall present the principles and their basic requirements.

Legitimacy of processing. This principle means that any data processing operation can only take place if it has a legitimate purpose, as provided for in Article 7 of the Directive, and national legislation transposing it. The legal grounds for the processing range from consent of the data subject to a balance of interests test, which confronts the legitimate interests pursued by the employer with the eventual infringement of the fundamental rights of the workers.

Proportionality. Under the proportionality clause personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. However, the Working Party emphasized that even when workers have been informed about the processing operation and such processing activity is legitimate and proportionate, such a processing still needs to be fair with the worker. The monitoring of e-mails should, if possible, be limited to traffic data on the participants and time of a communication rather than the contents of communications, if this would suffice to allay the employers concerns[12].

Transparency principle means that as very minimum workers need to know which data the employer collecting about them, what are the purposes of processing operations envisaged, or carried out, with these data presently or in the future. The employer is also under the obligation to provide his workers with a readily accessible, clear and accurate statement of his policy with regard to e-mail monitoring, describing in detail the extent to which communication facilities owned by the company may be used for personal/private communications by the employees, and reasons and purposes for which surveillance, if any, is being carried out and so on.

The principle of purpose limitation[13]. Purpose limitation protects data subjects by setting limits on how data controllers are able to use their

---

on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

[12] The Data Protection Working Party also notes that in case of absolute necessity of having access to the worker's email content, account should be taken to respect the privacy of those outside the organisation. The employer, for instance, cannot obtain the consent of those outside the organisation sending e-mails to his workers. The employer should make reasonable efforts to inform them of the existence of monitoring activities to the extent that people outside the organisation could be affected by them. A practical example could be the insertion of warning notices regarding the existence of the monitoring systems. See: *Working document on the surveillance of electronic communications in the workplace*, of 29 may 2002 of the European Working Party on Protection of Personal Data, p. 17. Available from: http://ec.europa.eu

[13] The purpose limitation principle, known also as the *finality principle*, is listed among key data protection principles under Article 6(1)(b) of Directive 95/46/EC. Considering the need for a more consistent and harmonized approach

data while also offering some degree of flexibility for data controllers. The concept principle has two main building blocks: personal data must be collected for 'specified, explicit and legitimate' purposes (purpose specification) and not be 'further processed in a way incompatible' with those purposes (compatible use).

First, any purpose must be specified, that is, sufficiently defined to enable the implementation of any necessary data protection safeguards, and to delimit the scope of the processing operation. The purpose of the collection must be clearly and specifically identified: it must be detailed enough to determine what kind of processing is and is not included within the specified purpose[14]. *Second*, personal data must be collected for explicit purposes. The ultimate objective of this requirement is to that the purposes are specified without vagueness or ambiguity as to their meaning or intent. It allows an unambiguous identification of the limits of how controllers are able to use the personal data collected, with the special aim of protecting the data subjects[15]. *Third*, the legitimacy requirement goes beyond the requirement to have legal ground for the processing under Article 7 of the Directive. In addition, it also requires that the purposes must be in accordance with all provisions of applicable data protection law, as well as other applicable laws such as employment law, contract law, consumer protection law, and so on[16]. It means that the purposes must be 'in accordance with the law' in the broadest sense, which includes both primary and secondary legislation.

Under the second building block of the purpose limitatin principle it is required that personal data shall not be 'further processed in a way incompatible' with the specified legitimate purposes.

The *compatibility test* is based on a formal and substantive assessment. The formal assessment compares the purposes that were initially provided by the data controller with any further uses to find out whether these uses were covered (explicitly or implicitly), while the substantive assessment goes beyond formal statements to identify both the new and the original purpose, taking into account the way they were (or should have been) understood, depending on the context and other factors[17].

Accuracy and retention of the data is referred to the employer's obligation to keep accurate and up to date employment records. The employer must take every reasonable step to ensure that data inaccurate

---

of the meaning of this principle, the Working Party have recently elaborated a specific opinion for clarifying the role of the principle and offering guidance regarding its practical application. See: Opinion 03/2013 of the Data Protection Working Party of 02 April 2013 on purpose limitation, p.6. Retrieved from: http://ec.europa.eu.

[14] A purpose that is vague or general, such as for instance 'marketing purposes', or 'IT-security purposes' will - without more detail - usually not meet the criteria of being 'specific'pp.

[15] See above: Opinion 03/2013 of the Data Protection Working Party on purpose limitation, p. 17.

[16] Ibid., pp. 19-20.

[17] In this context, "the compatibility principle" means, to use an example, that if the processing of data is justified on the basis of the security of the system, this data could not then be processed for another purpose such as for monitoring the behaviour of the worker. See above: *Working document on the surveillance of electronic communications in the workplace*, of 29 may 2002, p. 14.

or incomplete, having regard to the purposes for which they were collected or further processed, are erased or rectified[18].

Security principle requires that the employer implements appropriate technical and organizational measures at the workplace to guarantee that the personal data of his workers is kept secured, especially, as regards to unauthorized disclosure, or access.

Awareness of the staff. Last but not least, the adequate training of staff handling personal data is considered essential for ensuring the respect of privacy of workers in the workplace.

2.2 The ePrivacy Directive (Directive 2002/58/EC)

Directive 2002/58/EC[19] particularises and complements Directive 95/46/EC, with respect to the processing of personal data in the electronic communication sector, and is generally known as the ePrivacy Directive. In particular, this Directive seeks to ensure full respect of the rights to respect for private life and the protection of personal data, as set out in Articles 7 and 8 of the EU Charter of Fundamental Rights. The Directive reinforces the EU principle that all Member States must ensure the confidentiality of communications made over public communications networks, and the personal and private data inherent in those communications.

It applies to communications over publicly available electronic communications networks and services and covers among others e-mail, fax, sms and the Internet. Moreover, it contains specific rules on the processing of personal data, the protection of privacy in the electronic communications sector, rules on spam/unsolicited commercial communications, cookies etc. Regarding the confidentiality of communications it requires that parties to the communications should be informed prior to the recording, about the recording, its purpose, and the duration of its storage. The recorded communication should be erased as soon as possible, and in any case at latest by the end of the period during which the transaction can be lawfully challenged. In relation to the use of so-called spyware, web bugs, hidden identifiers and other similar devices, which can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user, it is highlighted that they may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned[20]. Special attention is also paid to the appropriate technical and organisational measures that should be taken by the provider of a

[18] Employers, for instance, should specify a retention period for e-mails in their central servers based on their business needs and have procedures in place to ensure that retention period is not exceeded.

[19] This Directive, has replaced Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector by adapting its provisions to the new technological developments in the electronic communications sector.

[20] See: Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, clause 24. Retrieved from : http://eur-lex.europa.eu.

publicly available electronic communications service, in order to safeguard security of its services[21]. Directive 2002/58/EC translates the principles set out in Directive 95/46/EC into specific rules for the publicly available electronic communications services. In this respect, as well as falling within the scope of Directive 95/46/EC, the monitoring of electronic communications by employers, might also fall within the scope of this Directive. Hence, it can be said that the Directive presents an instrument of safeguards concerning workers' email monitoring. However, it is still unclear whether the given provisions would find application regarding the confidentiality of workers communications held under virtual private networks[22]. The Article 29 Working Party has not given clarification regarding the scope of the term 'public' but it has emphasized that:

> *"The fact that provisions of the ePrivacy Directive only apply to provision of publicly available electronic communications services in public communication networks is regrettable because private networks are gaining an increasing importance in everyday life, with risks increasing accordingly, in particular because such networks are becoming more specific (e.g. monitoring employee behaviour by means of traffic data). Another development that calls for reconsideration of the scope of the Directive is the tendency of services to increasingly become a mixture of private and public ones*[23]*".*

In this respect, if the requirement of 'public' networks and services will be upheld in the future, it would broaden the scope of the European legal framework regarding electronic communications.

3. Employees' right to privacy under ECHR case-law

In general, from the case law of the European Court of Human Rights on the right to respect for private life in the employment context we can extract three principles[24]:

a) Workers have a legitimate expectation of privacy at the workplace, which is not overridden by the fact that workers use communication

---

[21] The measures shall at least: ensure that personal data can be accessed only by authorised personnel for legally authorised purposes; protect personal data stored/transmitted against accidental or unlawful destruction and unauthorised or unlawful storage, processing, access or disclosure, and, ensure the implementation of a security policy with respect to the processing of personal data (Article 4).

[22] A **virtual private network** (**VPN**) is a private network that uses a public network (usually the Internet) to connect remote sites or users together. The VPN uses "virtual"connections routed through the Internet from the business's private network to the remote site or employee. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefitting from the functionality, security and management policies of the private network. See: Mason, A. G.(2002). *Cisco Secure Virtual Private Network*. Cisco Press, p. 7.

[23] See: Opinion 8/2006 of the Data Protection Working Party of 26 September 2006 on the review of the regulatory framework for electronic communications and services, with focus on the ePrivacy Directive.

[24] See: *Working document on the surveillance of electronic communications in the workplace*, of 29 may 2002 of the Data Protection Working Party, p.9.

devices or any other business facilities of the employer. However, the provision of proper information by the employer to the worker may reduce the workers legitimate expectation of privacy.

b) The general principle of secrecy of correspondence covers communications at the workplace, and is likely to include electronic e-mail and related files attached thereto.

c) Respect for private life also includes to a certain degree the right to establish and develop relationships with other human beings. The fact that such relationships, to a great extent, take place at the workplace puts limits to employer's legitimate need for surveillance measures.

So, in **Niemitz v. Germany**[25] the European Court of Human Rights held that the right to respect for private life extends to professional or business activities.

> *'Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of 'private life' should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationship with the outside world. A fact that has been underlined by the commission confirms this: it is not always possible, in someone's occupational activities, to disentangle what falls within the professional domain from what lies outside it*[26]*'.*

As to the obligation of the employer to provide proper information to his employees on the electronic communications monitoring operations, in **Copland v UK**[27], the Court clearly illustrated the dangers of not having a proper technology use policy. A college employee was subjected to 18 months of monitoring which covered her telephone, e-mail and internet use. The monitoring took place in order to ascertain whether the applicant was making excessive use of College facilities for personal purposes. According to the charged party claims, the employee's monitoring pursued the legitimate aim of protecting the rights and freedoms of others by ensuring that the facilities provided by a publicly funded employer were not abused. The interference had a

---

[25] In Niemietz v. Germany, a local judge received a letter signed with a pseudonym on behalf of an anti-clerical group affiliated with a political party. The letter criticized a pending criminal prosecution of a private employer for and accused the presiding judge of being both biased and incompetent. The criminal investigation into the insulting letter led the German police to obtain a court order directing a search of Niemietz's office as part of an effort by the police to learn the identity of the letter writer. Niemietz was targeted for the search based upon his known affiliation with both the anti-clerical group and the related political party. In November 1986, the police conducted a search of Niemietz's law office, pursuant to the court order, including examining his client's files, but found no relevant documents. Niemietz challenged the search under ECHR, Article 8. See: Herbert. W. A. (2008). Workplace privacy protections wideworld: the whole wide world is watching. *University of Florida Journal of Law and Public Policy*. Vol. 19(3). pp. 396-397.

[26] See: Niemietz v. Germany, 16 Eur. Ct. H.R. 97 (1992).

[27] See: Copland v United Kingdom 25 B.H.R.C. 216 (2007).

basis in domestic law in that the College, as a statutory body, whose powers enable it to provide further and higher education and to do anything necessary and expedient for those purposes, had the power to take reasonable control of its facilities to ensure that it was able to carry out its statutory functions[28]. The ECHR held *that:*

> *'Telephone calls, e-mails and personal internet usage on business premises are protected by the right to respect for private life and correspondence for the purposes of Article 8. As the applicant had not been warned of the monitoring she had a reasonable expectation of privacy while at work, and the collection and storage of personal information relating to her e-mail usage, without her knowledge, amounted to an interfernece with her right to respect for her private life and correspondence'.*

The Court found violation of Article 8, in that no provisions existed, either in general domestic law or in the governing instruments of the college, regulating the circumstances in which employers could monitor the use of telephone, e-mail and the internet by employees.

4. Workers privacy expectations at national level

Anytime that within a collective public or private organization there is an application of special mail surveillance technologies there is great concern as to whether the employer is invading his employees' privacy. It is commonly accepted, among EU member states, that the confidentiality of electronic communications at the workplace is protected by the provisions on the protection of secrecy of correspondence, as a substantial aspect of an individuals' right to private life. In an attempt to give a representative picture of employer's privacy rights legislation at national level, the following part of the paper focuses on the experience of France and Italy. It provides a comprehensive introduction to the basic features of French legal theory and practice concerning email monitoring in workplace, in contrast with the Italian approach. The aim is to present the differences in the legal reasoning of each countries case law and doctrine, in particular in reference to the issue of to what extent should what privacy expectations should workers have while at work.

4.1 France

Within the French perspective, more emphasis is put on the workers right for private life and secrecy of correspondence in the workplace. The surveillance of employees' electronic mail, if carried out in lack of a major legitimate interest pursued by the employer, would more likely constitute a breach of their right of secrecy of correspondence. Some of the main arguments supporting this idea are:

a- The international instruments and the domestic law recognize the right of every citizen to secrecy of correspondence and communications, without making any distinction regarding the place where this right is

[28] Under this position, it was reasonably foreseeable that the facilities provided by a statutory body out of public funds could not be used excessively for personal purposes and that the College would undertake an analysis of its records to determine if there was any likelihood of personal use.

exercised, whether it as a private environment or the workplace. Therefore, opening and reading the correspondence exchanged by the employee during the performance of his work activity should be considered as an action which constitutes the offence of breach of the secrecy of correspondence.

b- Even if the employee uses his work email for personal reasons, this mere fact does not cause any harm to the employer, as long as the employees' actions do not violate any law provision, or put at risk the security of the employer's computer system.

c- The right of the employee to private life is extended even at his workplace. Taking this into consideration, his work email should also remain private and protected by any intrusion by the part of the employer.

It is worth mentioning though, that this viewpoint is not categorical. It is accepted that under a certain, given, set of circumstances the employer might be authorised to check the employees' mail. The employer can monitor the electronic post of his employee when he has strong reasons to believe that it contains data which proves the involvement of the employee in an illegal activity (such as sending or receiving documents, or images, with illegal content, or if the content discloses confidential information of the company)

4.1.1 The jurisprudence of France

In France, the *Cour de Cassation* has ruled in several cases regarding the question of employees' email monitoring. The first leading case was that of *Nikon France v.Onof* [29]. The highest court of France affirmed that employees enjoy a right to private life in their workplace, including a right to privacy of personal correspondence maintained on the employer's systems. It also stated that:

> 'the employer can not violate this fundamental right by reading personal messages sent or received by the employee through a special workplace device, even if the company has prohibited the personal use of computers'.

In another case the highest court ruled that a company's internal rules may limit the right of an employer to read his employees' work-related emails[30]. In the current case, an employee was suspected of breaking into the email account of his employer in order to access some data related to salary increase proposals. To confirm the suspicion, the employee's emails were opened by the company officials on his work computer, whilst he was absent. However, the company's internal rules stated that the employer had no right to access the employee's computer and email in his absence. *The Cour de Cassation* established that:

> 'if there is a general prohibition of the employer reading employees' emails in their absence in the internal rules of a company, no distinction between personal and professional communications will be made – none of the communications may be read[31]'.

[29] Decision of the French Court of Cassation, the Social Division, 2 october 2001, no. 99-42942.

[30] See: *Monsieur X v.YBC Helpevia*. Decision of the French Court of Cassation, the Social Division, 26 June 2012 no. 11-15310.

[31] See: Smith. R., & Kadar. D. (2012). *Protection of employee privacy rights in France: measures controlling employees in the workplace must be treated with*

The highest court of France has also held that loyalty should be an essential prevailing element of work relations and that the employer has the right to control and supervise his employees during the working hours[32]. Hence, the employer who has provided his employees with an email address may establish special mail monitoring equipment, provided that he has previously informed the employees on this fact. The control excercised by the employer must be justified by the presence of a legitimate interest and the used means must be proportionate to the interest being pursued[33]. The term 'email monitoring' means that the employer might check the recipients or senders of emails, but he can not read the email content[34]. If the employer provides his employees with an electronic mail address he has to consult the company's work committee about its terms of operation, and in any case he can gain information only on the content of professional mails[35]. It is traditionally affirmed under French case law that personal emails sent by the employee from his work email address are protected by the right to secrecy of his correspondence, and this rule is applied even in cases where the employer had explicitly informed the employees to respect the professional use of the email. However, special attention should be paid to the classification of electronic messages by the employee himself. This idea is clearly illustrated in the following situation. The case concerns an employee who had been fired because of sending two emails to one of his colleagues at work, which was considered a serious misconduct from his employer. The Versailles Court of Appeal held that the employer had breached the fundamental right of secrecy of correspondence, for the email had not been of a professional nature. When the case was brought before the Court of Cassation, it dismissed the decision of the Court of Appeal by emphasizing the fact that it should have verified whether the opened files were identified by the employee as personal or not[36]. So, the Court noted that it is necessary to pay attention not only to the content of the messages sent during work time,

---

caution - employers should avoid placing restrictions upon themselves. http://www.lexology.com. Accessed 14 august 2013.

[32] In fact, the employer's right to monitor the professional correspondence of his workers, is just an expression of his general right of controling and supervising their working activity. See: Decision of the French Court of Cassation, the Criminal Division, 19 may 2004, no. 03-83953.

[33] According to the Court, the principle requires that the degree of control must be proportional to the potential risks associated with the use of electronic mail such as: negative influence on the brand image, loss of productivity, contractual confidentiality risks etc. See: Decision of the French Court of Cassation, the Social Division, 2 june 2004, no. 03-45269.

[34] If the employer exceeds his supervising rights by reading the email content, he commits the offence of "breach of secrecy of correspondence", provided by article 226-15 of the French Penal Code.

[35] Decision of the French Court of Cassation, the Social Division, 14 march 2000, no. 98-42090. According to the European Working Party on Data Protection, the practice of employers to inform and consult worker representatives before introducing worker-related policies, is a further example of the transparency principle. See above: *Working document on the surveillance of electronic communications in the workplace*, of 29 may 2002, p.15.

[36] Decision of the French Court of Cassation, the Social Division, 30 may 2007, no. 05-43102.

but also to their naming. This ruling was in fact necessary for ensuring a fair level of protection of the employer who could not have any practical mean to realize the personal nature of the email.

In the end, it is worth mentioning that the right of the employer for respect of his secrecy of correspondence regarding personal mails, sent or received at his workplace, is not absolute and can be restricted when necessary for avoiding serious risks posed to the employer. According to a decision of the highest court of France[37],

> the employer may obtain, upon request, a judicial order which authorizes a baliliff to access data contained on the employee's computer and to read or save the content of email messages sent by him to other unidentified persons, which had no relation with the company[38].

The aim of this procedural measure is to give to the employer the possibility of having knowledge of his workers's personal mail when there are reasonable grounds to suspect actions that can be deemed as unfair competition. Such an action does not affect any fundamental freedom since the act is justified by the presence of a legitimate interest, and the control is made in the presence of the worker.

4.1.2 The French doctrine

According to French scholars, the right of every citizen for respect of his private life is promulgated under article 9 of the French Civil Code, which states that *"everyone has the right to respect for his private life"*. The provision in question is applicable even for employees at their work environments. However, the employer has the legitimate right to monitor his employees' in order ensure that their working activity is being performed under the proper legal and organizational requirements. Given that such a situation implies two major interests, it is of primary importance to determine what is the exact meaning of the term "employee's right to private life", and what aspect of his work activity can be monitored by the employer.

While trying to explain this relation, it is worth reminding that the employee uses the workplace facilities to maintain his correspondence, and he can reasonably be expected to not use them for personal interest. In addition, if the employer had expressly informed his employees about the conditions of computer use, and his scope of monitoring of the content of the emails sent/received at the workplace, he would significantly limit the possibilities of being found in violation of the legal provisions protecting the secrecy of correspondence. Currently, the right of the employer to monitor the email of his employees consists somehow on a compromise between the employees' right to privacy and employer's supervising interest. In order for the employee to avoid intrusions in his private communications, he must be cautious to maintain the professional nature of his email. On the other hand, the employer must take all necessary measures for ensuring that his staff be properly informed

[37] Decision of the French Court of Cassation, the Social Division, 23 may 2007, no. 05-17818.

[38] Under the facts of the case, the employee had constant relations and was involved in unfair practices with two persons outside the company in order to establish a competing company.

about the possible conditions of email surveillance[39]. He must also prove that in a given factual situation there was a legitimate interest, which justified the monitoring act and that all the used means were proportionate with the aimed scope. Among French scholars there is a well-established opinion that the employer is not authorised to gain knowledge of his employees' private messages, despite the fact that the latter might have wrongfully diverted the use of professional email address to private use. The commission of such an act could be considered a legitimate cause for dismissal, but would not justify the reading of private messages [40].

4.2 Italy

According to the approach of Italian courts, the control of employee's electronic mail is considered lawful provided that some reasonable grounds justify the employer's decision to act so. In this respect, the mere act of controlling the employees mail is considered as an extension of the employer's right to inspect their work performance. As long as the employee is required to use his work email for only sending and receiving messages related to his working activity, any control exercised by the employer in this form of communication will not constitute a breach of the right to privacy due to the fact that in accordance with law he has the right to systematically control the employees' activity. In addition, the reason why the employee has been provided a work email is to use it for interests related to his job activity, and not for private purposes. It is now a well-established idea that the right of secrecy of correspondence is a special aspect of a persons' right to respect for private life. Taking into consideration this relation, the employer does not violate the secrecy of the correspondence of their employees since the application of this right is related to private correspondence. By nature, it is presumed that the work email does not contain any data exposing an aspect of the worker's private life, which as such, should not be accessed without his expressed consent. If the employee uses his work email only for conducting official communications, as he should indeed do, any monitoring operation applied by the employer would not lead to the disclosure of personal data.

4.2.1 The Italian jurisprudence

Among decisions of Italian courts on email monitoring operations in workplace, a principal ruling is that of 19 december 2007 of the Italian Court of Cassation. The facts presented in this case refer to the opening and reading, from the employer G.T, of the emails of one of his employees R.M, by using the password which was previously made known to him due to the company's internal policy. The Court stated that

> 'an employer who reads his employees' emails does not commit the offence of breach of secrecy of

[39]For a more detailed look on this position see: Patin. J-C. (1999) *La surveillance des courriers électroniques par l'employeur*. http://lthoumyre.chez.com/pro/1/priv19990810.htm. Accessed 24 August 2013.

[40] See: Cahen. M. (2007). *Courrier electronique et vie privee.* http://www.muriellecahen.com/publications/p_courrier.asp. Accessed 29 Jully 2013.

> correspondence[41], provided that the company had previously issued a rule under which the employee should give to his employer his computer and email password. [42]'

The criminal provision in question could not be applied because it referred to any act of reading a closed correspondence, while under the facts surrounding the case, the possible access on the employee's email was not denied to the employer. Under Italian Penal Code, a person who reads a correspondence, in which he had been provided free access, would commit an offence only if he omits it or changes its destination and this was not the case. The Court emphasized that:

> 'It is undeniable that the respective criminal provision is applied also to informatic and telematic communications. Such a way of communication, will be considered as closed only towards those subject which are not authorized of having free access on the informatics systems of sending and receiving the messages. The right to have access on the information exchanged by these systems depends not as much from ownership rights than from the rules which discipline the systems' use. If the telematic system, is protected by a specific password, it can be considered that all those subjects which do legally possess the informatic key of access, might have knowledge of the exchanged correspondence [43].'

As a result, in the presented case the Court of Cassation found no violation of the employee's right to secrecy of her correspondence due to the fact that the employer lawfully took knowledge of her work email by using the legally possessed access key.

Similar questions are also handled in a decision of the Turin District Court[44]. The Court ruled that the enterprise email belongs to the employer, and any act of having knowledge about the content of the employees' electronic mail does not constitute the offence of breach of secrecy of correspondence. The only requirement that should be met by the employer is to ensure that the given action be preceded by a specific enterprise policy[45]. It also stated that *'the messages sent through the work email address are not private correspondence...they should be considered as a normal mail exhange held by the company in performance of its activities'*.

4.2.2 The doctrine of Italy

---

[41] The offence is provided for by article 616 of the Italian Penal Code, which states that "Everyone who gains knowledge of a closed correspondence not addressed to him, or omits or diverts a closed or open correspondence, aiming at having knowledge or providing to third parties the capacity of having knowledge of its content, or totally or partially destroys it, is fined or sentenced up to one year of imprisonment"

[42] Decision of the Italian Court of Cassation no. 47096, dated 11. 12. 2007.

[43] Ibid.

[44] Decision of the District Court of Turin, no. 143, dated, 20.08.2006.

[45] The term is refered to the specific policy adopted by the company about the use of electronic mail and Internet from its employees. It should provide the employees with a detailed overview of the conditions under which the employer can open their emails. If this policy, is made known, then the monitoring of employees' email would not be considered unlawful.

In Italian legal doctrine doctrine the question of email surveillance at the workplace has not found sufficient ellaboration. However, some scholars and law practitioners have tried to explain the possible legal implications associated with the problem. According to one view, the employer does not perform any illegal act when reading the electronic mail of the employees, for they are required to use their workplace mail only for professional reasons [46]. Hence, even if the employer opens a personal email, he can not be challenged of having violated his employee's secrecy of correspondence, as long as any email sent from the workplace facilities and during the working activity is supposed to have a professional nature. In fact, the answer of such matters, depends to a great extent on the specific clauses set out in the internal regulation of the company. If there are special internal rules that require the employees to use their work email only for reasons related to their job activity, the eventual control carried out by the employer should be seen as an aspect of his right to monitor his employees' work performance. Given the situation, the employer who opens the employee's email by presuming that it contains only work related messages, can not be rendered liable for breach of the secrecy of correspondence, since he lacks the intention to perform an illegal act.

On the other hand, some authors question the accuracy of the solution provided by the Italian courts. They do argue that the exercise of the employer's disposal right, over the informatic system, consists of taking proper measures for avoiding any unauthorised access by third parties, but it does not grant him any right of having knowledge about the content of electronic messages exchanged through the system[47]. When considering the legitimacy of the act of controling the employee's email messages, the court should pay much more attention to the fact whether such a practice was carried out with the data subject free will or not. It is the employee's will of permitting the control of his electronic mail that should determinate the legitimacy of the given act. According to these scholars, any other choice, which considers lawful the employer's intrusion on his employees' email for the mere fact that under the internal organisational rules, he possesses the informatic access key, would provide him with an unlimited and unjustified power of control [48].

---

[46] See: Frediani. V. *"Lettura della casella di posta elettronica da parte del datore di lavoro: lecito o illecito?"*, available at: http://www.consulentelegaleinformatico.it/; see also: Perfetti. T. *"Il controllo della mailbox aziendale*". http://www.filodiritto.com. Accessed 27 Jully 2013.

[47] See: Pecorella. C., & De Ponti. R. (2011). *Impiego dell'elaboratore sul luogo di lavoro e tutela penale della privacy, pg. 8-9.* http://www.penalecontemporaneo.it. Accessed 13 august 2013.

[48] Ibid., p.15. It is also stressed that the control of employee's email messages should be carried out only in indispensable cases and in the presence of a reasonable justificatory ground. Under such conditions, the employer might open the correspondence in the presence of the employee, and if that is not possible, he should address to aministrative bodies for obtaining a permission of access. See: Garri. F. (2007). *La tutela della privacy nei luoghi di lavoro*, pg. 22. Retrieved at: www.giustizia.lazio.it. Accessed 23 july 2013.

5. Concluding comments

Basically, the employer has a general right of monitoring workers' emails, which should be considered as an extension of his right to control their workplace performance. In addition, the employee uses the employer's facilities to manage his email address and he is supposed to use it only for purposes related to the professional activity. However, in the European context the right to respect for private life and secrecy of correspondence *extends to professional or business activities since the right for private life comprises, to a certain degree, the right to establish and develop relationships with other human beings, and it is in the course of their working lives that the majority of people have a significant opportunity of developing relationship with the outside world*. When addressing these issues, is very important for the employer to provide a clear, well-defined, written policy concerning the use of its e-mail system, and the special conditions under which a monitoring operation can take place. Despite that, the prior implementation of a detailed informative policy cannot be considered sufficient to justify any intrusion into workers' electronic mails[49].

The legitimacy of workplace email surveillance should rely to a great extent on the presence of a legitimate business interest such as avoiding the eventual liability resulting from e-mail misuse, protection of the company and/or the confidential information of the organization, ensuring the integrity of the ICT systems from any malware attached to emails, the measuring of workers productivity, and so on[50]. Employers, moreover, should not monitor e-mail messages unless it is clear that the legitimate business purpose being pursued cannot be achieved by other means. Any monitoring must be a proportionate, and a reasonable response to the risk faced by the employer, and must provide a fair balance between the legitimate interests of employers and the employees' privacy rights. Finally, all these considerations should be further ellaborated under the perspective that the conditions of work have evolved in a way that it becomes more difficult today to clearly separate work hours from private life. In particular, as the "home office" is evolving, many workers continue their work at home using computer infrastructure provided by the employer for that purpose, or not[51].

[49] This conclusion seems to be incompatible with the Working Party Guidelines. according to which, advance warning to the worker would not be sufficient to justify any infringement of their data protection rights.

[50] As about the measurement of employees' work performance, it should be noted that, the monitoring of traffic data and the subject of e-mails is considered as sufficient to achieve the business purpose and that any inspection of emails content would unreasonably exceed the purpose being pursued . This position is also highlighted by the European Data Protection Working Party ; See: *Working document on the surveillance of electronic communications in the workplace*, of 29 may 2002, p. 17.

[51] See: Working document on the surveillance of electronic communications in the workplace, of 29 may 2002 of the European Working Party on Protection of Personal Data, p. 6.

Bibliography

Cahen. M. (2007). *Courrier electronique et vie privee.* http://www.muriellecahen.com/publications/p_courrier.asp. Accessed 29 Jully 2013.

Frediani. V. *"Lettura della casella di posta elettronica da parte del datore di lavoro: lecito o illecito?"*, Retrieved from: http://www.consulentelegaleinformatico.it/; see also: Perfetti. T. *"Il controllo della mailbox aziendale"*. http://www.filodiritto.com. Accessed 27 Jully 2013.

Garri. F. (2007). *La tutela della privacy nei luoghi di lavoro*. Retrieved from: www.giustizia.lazio.it. Accessed 23 july 2013.

Herbert. W. A. (2008). Workplace privacy protections wideworld: the whole wide world is watching. *University of Florida Journal of Law and Public Policy*. Vol. 19(3). pp. 396-397.

Kierkegaard. S.M. (2005). Reading Your Keystroke: Whose Mail is it ? - Trust, Privacy, and Security in Digital Business. *Lecture Notes in Computer Science* . Volume 3592, pp. 256-265.

Mason, A. G.(2002). *Cisco Secure Virtual Private Network*. Cisco Press.
Patin. J-C. (1999) *La surveillance des courriers électroniques par l'employeur*. http://lthoumyre.chez.com/pro/1/priv19990810.htm. Accessed 24 August 2013.

Pecorella. C., & De Ponti. R. (2011). *Impiego dell'elaboratore sul luogo di lavoro e tutela penale della privacy.* http://www.penalecontemporaneo.it. Accessed 13 August 2013.
Smith. R., & Kadar. D. (2012). *Protection of employee privacy rights in France: measures controlling employees in the workplace must be treated with caution - employers should avoid placing restrictions upon themselves.* http://www.lexology.com. Accessed 14 august 2013

EU sources

Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data**.**

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
Working document on the surveillance of electronic communications in the workplace, of 29 may 2002 of the European Working Party on Protection of Personal Data.
Opinion 8/2001 of the Data Protection Working Party of 13 September 2013 on the processing of personal data in the employment context.
Opinion 8/2006 of the Data Protection Working Party of 26 September 2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive.

Opinion 03/2013 of the Data Protection Working Party of 02 April 2013 on purpose limitation.

Case law

Niemietz v. Germany, 16 Eur. Ct. H.R. 97 (1992).

Copland v United Kingdom 25 B.H.R.C. 216 (2007).

Decision of the French Court of Cassation, the Social Division, 2 october 2001, no. 99-42942.

Decision of the French Court of Cassation, the Social Division, 26 June 2012 no. 11-15310.

Decision of the French Court of Cassation, the Criminal Division, 19 may 2004, no. 03-83953.

Decision of the French Court of Cassation, the Social Division, 2 june 2004, no. 03-45269.

Decision of the French Court of Cassation, the Social Division, 14 march 2000, no. 98-42090.

Decision of the French Court of Cassation, the Social Division, 30 may 2007, no. 05-43102.

Decision of the French Court of Cassation, the Social Division, 23 may 2007, no. 05-17818.

Decision of the Italian Court of Cassation no. 47096, dated 11. 12. 2007.

Decision of the District Court of Turin, no. 143, dated, 20.08.2006.