Журнал правовых и экономических исследований.
Journal of Legal and Economic Studies, 2018, 4: 61–67

УДК 342.738:341.645(4)

Lourdes Mella Méndez

THE FUNDAMENTAL RIGHT TO THE PRIVACY OF COMMUNICATIONS IN THE WORKPLACE: THE APPLICATION OF ECTHR DOCTRINE

Lourdes Mella Méndez – Professor, University of Santiago de Compostela (Spain); **e-mail: lourdes.mella@usc.es**.

The article examines the traditional doctrine of the Spanish Constitutional Court regarding protection of fundamental rights of the employee, in particular the privacy of communications and dignity in the workplace. In addition, special attention is given to the important Judgment of the Grand Chamber of the ECtHR dated September 5 2017 (Bărbulescu v. Romania case), whereby Art. 8 of the European Convention of Human Rights shall apply to protection of the privacy of e-mails in the workplace, since the ones are considered to be a part of the employee's exercising his or her private life. In this regard, employer's control over the computing resources used by the employee should correspond to the principle of fair balance. Due to this new judgment, the Spanish Constitutional Court should have changed its standpoint so that to interpret appropriate norms in accordance with the legal positions of the ECtHR.

Keywords: *the European Court of Human Rights; fundamental right;, privacy of communication; privacy; labour relation.*

Лурдес Мелла Мендес

ФУНДАМЕНТАЛЬНОЕ ПРАВО НА ТАЙНУ КОММУНИКАЦИЙ НА РАБОЧЕМ МЕСТЕ: ПРИМЕНЕНИЕ ДОКТРИНЫ ЕВРОПЕЙСКОГО СУДА ПО ПРАВАМ ЧЕЛОВЕКА

Лурдес Мелла Мендес – профессор Университета Сантьяго-де-Компостела (Испания); **e-mail: lourdes.mella@usc.es**.

В настоящей статье исследуется традиционная доктрина Конституционного суда Испании, касающаяся защиты основных прав работника, в частности – секретности его коммуникаций и достоинства. Кроме того, особое внимание уделяется важному решению Большой палаты ЕСПЧ от 5 сентября 2017 года (дело «Бэрбулеску против Румынии», п. II), согласно которому ст. 8 Европейской конвенции о защите прав человека применяется к защите конфиденциальности электронных сообщений на рабочем месте, поскольку они являются частью «осуществления социальной частной жизни» сотрудника. В этом смысле контроль работодателя за компьютерными ресурсами, используемыми сотрудником, должен соответствовать принципу пропорциональности. Вследствие этого нового решения Конституционный суд Испании должен был изменить свою позицию и толковать соответствующие нормы в свете правовых позиций Европейского суда по правам человека.

Ключевые слова: *Европейский суд по правам человека; фундаментальное право; секретность коммуникаций; неприкосновенность частной жизни; трудовые отношения.*

I. THE RECENT DOCTRINE OF THE ECHR ON THE NECESSARY RESPECT OF THE FUNDAMENTAL RIGHTS OF THE EMPLOYEE IN THE LABOUR RELATIONSHIP

The possibility of employershaving control over the use that employees make of computer equipment at work, and if this use is incorrect, thesanction that follows, is an aspect of utmost importance currently. In this sense, it is important to analyse the latest criteria of the European Court of Human Rights(ECHR) and the Spanish Constitutional Court (CC) to determine the extent to which the Spanish legal system respects them.

In this sense, we can start from the recent and important Judgment of the Grand Chamber of the ECHR of September 5 2017, which rectifies the previous one of the Fourth Chamber of the Court of January 12 2016. In the case at hand, the employee was dismissed because he failed to comply with the internal regulations of the company -known by all staff - prohibiting the use of technological resources made available bythe employer for personal purposes (that employee used a corporate Yahoo Messenger instant messaging account to send private emails, thus violating the objective of its exclusive professional use). Theregulations also provided for the possibility of corporate control of such computer resources. The company checked both the professional and private email accounts of the employee and discovered the irregular use, but as he initially denied it, the company proceeded to broadcast a transcript of the private messages exchanged with his family and girlfriend. The employee challenged the dismissal in his country (Romania) and requested its nullity for violation of his right to private and family life, as well as the secrecy of communications, which covers private correspondence, recognised in the national constitutional norms and Article 8.1 of the European Convention on Human Rights. Both at first instance and onappeal, the claim was dismissed because the Court understood that the employer had acted in accordance with the law (internal regulations) and that theirconduct was reasonable and proportionate. The reasoning was that the surveillance of the email accounts was the only way to find out if the employee had breached his contractual obligations and there was no other method of surveillance less harmful to his fundamental rights. In addition, the employee had been advised of the possibility of online activity being monitored and, therefore, he had no reasonable expectation of privacy.

Following an appeal to the ECHR, the Fourth Chamber decided in 2016 by majority decision – of 6 to 1 – that the employer acted correctly by virtue of his power to monitor and control work, without noting anyoverreaching or interference in life private, from the assumption that the email account was professional, and it ratified the national judgments. However, the minority vote opinedthat it was not fully proven that the worker had sufficient knowledge of the limitations imposed by the internal ruleson the private use of technology, something thatthe employer has to prove[1].

The employee appeal to the Grand Chamber wasadmitted due to the seriousness of the issue. The new Judgment of the Grand Chamber of the ECHR of September 5 2017 held that Art. 8 ECHR appliesto protection of the privacy of electronic communications in the workplace, since they are part of the 'exercise of a social private life'. Thus, after different references to the international framework for the protection of fundamental rights and the necessary protection of personal data, the EC pointed to the specific nature of the subordinate employment relationship and the need for States and social agents to set the legal or conventional framework in which the working life of the employee should be developed, which includes the regime applicable to electronic communications. In this line of argument, if states and social agents do not act, the employer may approve an internal regulation or code of conduct, although it has to be equally protective of the interests of workers. The

[1]Cfr. SYCHENKO E.: *Individual labour rights as human rights. The contributions of the European Court of Human Rights to Worker's Rights Protection* (2017, The Netherlands), pp. 94 et seq.

employee must be duly informed about the limits to his usage and the control capacity of the employer, to make his decisions with full knowledge of their consequences.

In the case discussed, the Grand Chamber of the ECHR concluded that, from the facts established, it could not be held that the employee had been adequately informed in order to respect their rights and the contractual balance between the parties. The obligation of adequate informing requires that the information be made available, first, in a certain way (clearly and precisely, in an accessible and direct language, without ambiguity orunnecessary reiteration) and in written form in the code of conduct. Second, the information should be made available at a specific moment: before the commencementof the work activity or, as the case may be, the entry into force of the business measure adopted. In other words, the informative act must be done with sufficient anticipation so that the employee has time to know the rules of the game and consciously choose to adhere to them or not.

Third, the information also requires a certain content and scope. Sufficient data must be given so that the recipient has complete knowledge of the situation, which implies that, when it comes to restricting and controlling the private use of computer resources, theinformation should clearly refer to: 1) the limitations that will govern the private use of those instruments, including the confidentiality of the communications that the employee makes using them; that is, the employee must know exactly what is allowed and what is prohibited; 2) the extent and nature of the monitoring to be carried out by the employer, for example, its scope and the degree of interference in the employee's private life. It should also be indicated, where appropriate, that possible access to 'the content'of communications made during working hours; and 3) the concrete procedure to be followed by the employer, which implies knowing who will carry out the monitoring, how, when and where it will be carried out and how long it will last.

In any case, even when employer control proceeds and is justified, it is necessary to passthe so-called 'proportionality test', that is, that that control is proportionate to the damage caused in the violation of the worker's fundamental right. In effect, the activation of the principle of proportionality requires that the control be: 1) suitable, in other words, that it is appropriate and useful to achieve the proposed objective; 2) necessary or indispensable, which implies that there is no other more moderate or less invasive measure to achieve that control with equal effectiveness; and 3) weighted, which means that the control must result in greater advantage for the general interest than the damage to the fundamental right in conflict.

Finally, in the case analysed, in the Judgment of the Grand Chamber of the ECHR, it was concluded that neither the power of corporate control nor the disciplinary sanction (dismissal) imposed on the employee were reasonable or proportionate. Regarding the first point, apart from holdingthat the subject was not properly informed of the scope of the corporate control (specifically that the employer could access the content of his private mail), the existence of thenecessity judgmentrelated that controlwas challenged. It was held that the employer could have achieved the same purpose of monitoring the activity of the worker usinga method that was less invasive and harmful to their fundamental rights. It should be notedthat when the employer discovered the irregular useof corporate email, and the employee denied it, the employer proceeded to disseminate a transcript of private messages exchanged by the non-compliant subject with his family and girlfriend. Of course, such reading of these private messages and their subsequent dissemination were not absolutely necessary to prove the extra-limitation in the professional use of the computer resources. In other words, he interfered illegitimately with the privacy of the employee by violating the right to privacy of his private communications, as he read and disseminate it, being aware that the communications were private.

With regard to the sanction imposed on the dismissed employee, the Grand Chamber also criticisedthe Romanian national courts for not assessing the proportionality of the dismissal tothe contractual breach commit-

ted, as no serious damage to the company wasincurred. Finally, the Grand Chamberwas very precise when assessing all the specific circumstances of the case in the interest of the necessary protection of the fundamental rights of the employee. This allowed to the European Court to reach the conclusion that neither the corporate control nor the disciplinary sanction (the dismissal) imposed on the employee were reasonable or proportionate. The inadmissibility of the sanction wasbased on the lack of sufficient gravity of the fault of the worker, as long as there was no material damage to the company.

II. THE TRADITIONAL POSITION OF THE SPANISH CONSTITUTIONAL COURT ON EMPLOYER CONTROL OF EMPLOYEE EMAILS

In Spain, there are two Constitutional Court Judgments directly related to the case examined in the ECHR, in which the fundamental rights to privacy and secrecy of communications have also been analysed. Theprinciple of proportionalitywas studied, also in relation to employer control of new information and communication technologies used in the work environment. This principle acts as an essential condition in the exercise of corporate control for the 'constitutionality of any restrictive measure of fundamental rights' of the employee within the framework of the employment contract[2]. These rulings are nº241/2012, of December 17, and nº 170/2013, of October 7. In the latter, the CCdidnot go much further and limited itself to applying its restrictive majority doctrine adopted in the first judgment, which is of greater interest, especially with its dissenting vote, which linked directly with the last ECHR Judgment. The CC 170/2013 Judgment, of October 7, confirmed the legality of employer control ofthe corporate email accountsof employees and the non-infringement of their privacy and secrecy rights. In the case at hand, the control was held to be legal in light of the following circumstances: 1) the existence of an express prohibition of the private use of computer resourcesin the applicable collective agreement, which highlighted such conduct as punishable misconduct; 2) the lack of prior tolerance of such use, so that the employeecould notclaim a reasonable expectation of privacy or confidentiality of the communications made; 3) the existence of well-founded suspicions of irregular use of the tools (disclosure of company secrets to third parties); and 4) supervision of the employer control, carried out by a computer expert. In light of such a combination of circumstances, the CC heldthat the corporate control passedthe proportionality test with respect to the damage it may have causedtothe fundamental rights of the employee, as long as the control measure wasjustified, appropriate and balanced.

Greater attention can be devoted to the first Judgment, which, due to its restrictive nature and content, represents a step backwards in the protection of workers' fundamental rights, in line with the ECHR Judgment of January 2016. In fact, in the CC ruling nº 241/2012, of December 17, the majority of the Chamber held to be legal, thecontrol of the employer consisting of their access to one of the company's computers to check whether theban on the installation of aninstant messaging application had been violated and in the opening of files and the subsequent reading of the written conversations (which wasdone only by the person in charge of the service, before the supervisors and the workers who installed the programme) to verify its purpose and use. The reason forthe majority decision of the CC wasbased on the specific factsof the case, which werethe following: 1) the installation of such applicationswas expressly prohibited by the employer, andwas known to all; 2) the computer concernedwas not access password protected and was commonly used by the staff; 3) the prohibition to install this type of application, known to all, prevented the existence of a reasonable expectation of privacy or confidentiality for the user.

However, despite the apparent reasonableness of these arguments, related to the careless action of the affected employees, there wasan interesting dissenting opinion[3]

[2] Judgment of Constitutional Court 186/2000, of 10 July (BOE of 11 August).

[3] Magistrates Fernando Valdés Dal-Ré and Adela

which disagreed with the ruling. First, this vote put the focus of attention on the restrictive decision of the employer. It wasassumed that Art. 18.3 Spanish Constitution guarantees the freedom of communications, not only the secret of same, and for that reason an analysis of the validity of the prohibition of the private use of the computer was required, because, on the one hand, 'the employment contract does not deprive the employee of the ability to communicate with others', that is, 'it does not put him in a situation of solitary confinement in relation to the outside world'(ECHR: the worker does not leave their rights at the door of the company) and, on the other hand, that the employer is the owner of these information and communication technologies do not give him the right to introduce 'capricious restrictions' on their use. In other words, the dissentingvote seemed to hold thatthe private social use of the computer tools owned by the company, could not be unjustifiably prohibited.

Second, the dissenting opinionwentfurther and statedthat the fundamental right to secrecy of communications must be understood from a formal and absolute point of view, that is, regardless of the content of the communications, and in any situation, even in onewhich may involvea contractual breach by the employee of an employer order (as in the case at hand). The employer may sanction such a breach, but, indoing so, mustaccess the content of the communication, because this would violate the essential basisof the fundamental right to the secrecy of same. From the moment that the employer or a non-recipient third party reads or knows the content of the communication, the latter is no longer secret and the employer control measure does not pass the proportionality test.

Third, that same absolute nature of the fundamental right (to the secrecy of communications) protects its essential content even when the employee performing the communication acts carelessly and does nothing to protect it (as when private communication takes place on a common computer and with no access password). The individual who opens a link or a file knowing that it contains conversations of others acts in the same way as one who findsa letter addressed to another person and mistakenly placed in their mailbox, and opens it. In the case at hand, it is true that when the person in charge of the company accesses the installed file and reads the written messages, the employees who sentthem are there, but their consent to the reading of them and the judicial authorisation are not proven.

As can be seen, the vision of this excellent individual dissenting opinion is in line with the recent criterion adopted in the ruling of the ECHR Grand Chamber.

III. THE NECESSARY ADAPTATION OF THE SPANISH JUDICIAL DOCTRINE TO THE NEW POSITION OF THE ECHR

As discussed, the current predominant doctrine of the Spanish Constitutional Court is less protective than that of the European Court of Human Rights, however, this will have to change, given the binding force of the doctrine of the European Court, which is directly applicable tothe Spanish legal system and requires an interpretation of the Spanish Constitution according to it. In this sense the Art. 10.2 Spanish Constitution (SC) establishes that 'the rules relating to fundamental rights and freedoms' recognised therein 'shall be interpreted in accordance with the Universal Declaration of Human Rights and international treaties and agreements on the same matters ratified by Spain'.

In view of the binding nature of the ECHR doctrine, it should be noted that Spanish courts often readilyaccept it, despite the changes. So, at first, the courts started to apply the doctrine of the *Barbulescu I* case, and declared – expressly citing this European judgment – that 'an employer can control the professional electronic mail of his employees without violating their right to privacy', and can consequently 'dismiss the employee who fails to comply with the code of internal conduct'[4]. In this case, at first, there were elements that justifiedas logical thestatement about theemployer control over computers, because, on the one hand, the investigation

Asua Batarrita.

[4] Judgment TSJ Madrid of the 6 May 2017 (nº sentence 391/2016).

was not carried out directly by the employer, but he commissioned a specialised advisory firm to do so, making sure to safeguard the rights of the affected workers. The computers were deposited withthe notary in order to make two copies of the content in the presence of the notary, one for the expert and the other for the advisory firm. In addition, on the other hand, the company had a manual for the use of information systems (known by the employee and published on the intranet), which stated that only professional use was permitted and, therefore, the employees could not harbour any expectation of privacy; likewise, the possibility of carrying out the controls that the company 'estimate necessary' was highlighted. The same warnings were duplicated in theemployee employment contract.

However, in line with the new *Barbulescu II* ruling, in the same case mentioned, the contrary and negative conclusion could be reached about the legitimacy of corporate control, and this was due to the breach of the informative obligation. Note that, according to the European ruling, business information requires a specific content and scope so that the recipient can gain thorough knowledge of the situation. This means that this information must refer, apart from the limitations related to the private use of computers, to the scope of the monitoring to be carried out by the employer, that is, the number and intensity of the controls and the degree of intrusion into the employee's private life. Besides, the concrete procedure for that control must also be explained.

As it cannot be otherwise, in light ofthe new position of the European Court, the Spanish courts have also begun to react to the above-mentioned test. Thus, it is appropriate to mention the judgment of Labour Court Nº. 19 of Madrid of November 17 2017 (Nº. 453/2017). In this case, the company had an internal policy for the management of the information, Internet and email systems which established, on the one hand, use for 'strictly professional purposes, excluding any' commercial, playful or personal use unrelated to the 'work' activity. However, on the other hand, some 'exceptions' were cited, which expressly permitted personal use of both the Internet and email, provided that this amounted to a 'necessary, minimum and reasonable use'. Besides, the internal document warned employees that the company: 1) could 'audit and access' the former as deemed necessary to verify the correct use of information technology, expressly stating that employees may not have a reasonable expectation of privacy regarding the information stored in the company's computer; and 2) the company reserved the right to carry out controls to verify and analyse access protocols, private and professional use of technological devices. Now, at this point, it was also stated that these controls must respect the exceptions provided for private use and must be carried out in compliance with the law and the principles of proportionality, rationality and suitability and in defence of legitimate interests.

In the caseanalysed, the employee adoptedincomprehensible and contradictory behaviour because, on the one hand, they refusedto do the assigned tasks and, on the other, demanded new ones. In addition, colleagues accused him of lying when hesaidthat he didnot have enough time to perform the tasks entrusted to him. Faced with such facts, the company sought to discoverhow the employeeoccupied histime during working hours and monitored the employee's computer activityusing a system that provided all the details of the emails sent from the workplace.

In the aforementioned judgment, this control was held to beexcessive and failed the test of proportionality laid down by the ECHR (*Barbulescu II*), as to achieve the stated purpose itwas 'unnecessary and disproportionate' to monitor computer activity and, much less, to access personal emails, in respect ofwhich there was an expectation of privacy. In other words, the criterion of the need to justify such access to emails was not met, since the objective pursued could have been achieved through less invasive means, such as directemployer monitoring of the worker's performance (who provided face-to-face services in the company and, therefore, could be monitored directly) or with the simple requirement to account for the tasks performed during the day, even on a daily

basis for a certain time.

On the other hand, it is worth mentioning that the employer used the information obtained through thecomputer monitoring to impose a disciplinary sanction encompassing dismissal on the employee. However, this sanction must be qualified as null because it was based on evidence that violated the fundamental rights of the employee.

IV. CONCLUSIONS

The main conclusions of this study are the following:

1. In 2017, the ECHR decided to maintain a position of maximum protection of the fundamental rights of the employee, in particular with reference tothe privacy and secrecy of communications, in the face of doubts raised previously. In this sense, corporate control over the computer resources used by the employee to do work must respect the principle of proportionality.

2. In Spain, the Constitutional Court ruled, in 2012 and 2013, on thecorporate monitoringof computers and emails used by the employee and, in view of the particular circumstances of the cases, validated the corporate monitoring performed, even when the content of private emails was accessed.

3. As a consequence of the *Barbulescu II* judgment, the Spanish Constitutional Court has been required to change its majority doctrine and align itself with this European judgment, following the dissenting opinionof case 241/2012. Worker's privacy and the confidentiality of personal communications should always be guaranteed, and, in order to achieve that, the employer must not access to the content of these emails, even when they have previously and clearly detailed the permitted use of IT tools and the possible monitoring of same by theemployer, anddespite the employee breaching their contract.