Labour Law remark

Judgment handed down by the Grand Chamber of the European Court of Human Rights on 5 September 2017 on the control of e-mail use by employers

September 21st 2017

Recently, most media picked up on a judgment handed down by the Grand Chamber of the European Court of Human Rights on 5 September 2017 in *Barbulescu vs. Romania* (app. 61496/08). This chamber concluded by eleven votes to six that the Romanian state had violated Article 8 of the European Convention on Human Rights.

Specifically, the ECHR judgment (the wording of which can be accessed on the ECHR website in French and English) states that monitoring messages sent by an employee using company equipment and accessing the content of these messages constituted a violation of the right to privacy and the confidentiality of communications if the employee had not first been informed of this possibility, even if the company had rules in place banning the use of company equipment for personal purposes.

1.- The **circumstances** of the case are as follows:

Mr. Barbulescu was employed as an engineer in charge of procurement. At the request of his superiors, he created a Yahoo Messenger account for the purpose of answering enquiries from clients. However, after three years he was informed that his account had been being monitored and was shown evidence of the account being used for personal purposes. As a result of this use, he was informed of his dismissal.

Initially, Mr. Barbulescu denied having used the account for personal purposes. The company then proceeded to publish a transcript of messages he had exchanged with his brother and fiancée in relation to his personal life. It also transcribed messages that Mr. Barbulescu had exchanged with his fiancée using a personal Yahoo account.

Mr. Barbulescu challenged his dismissal in the courts, arguing that his dismissal was null and void due to the fact that his right to privacy had been violated. His claim was dismissed by the Bucharest County Court. Mr. Barbulescu appealed the decision. The appeal was also dismissed, with the decision of the court based on **EU Directive 95/46/CE**, explaining that according to this directive company resources must not be used for personal purposes and that the monitoring of communications was the only method of establishing if there had been a disciplinary breach.

Based on Article 8 of the ECHR (the right to respect for one's private and family life, home and correspondence), the appellant referred his case to the ECHR, arguing that the decision to terminate his employment contract after his electronic communications had been monitored and accessed was based on a violation of his privacy, and that the courts in his country had not protected his right to respect for his private life and correspondence.

2.- What doctrine has the ECHR put in place?

The ECHR judgment states that in order to assess the legality of the monitoring of employee communications, the following factors must be assessed:

> If the employee has been informed of the possibility that their correspondence may be monitored.
>
> The degree of intrusion by the employer (the duration of monitoring, the files accessed and how many people have access to the results of the monitoring process).
>
> The existence of legitimate business reasons for monitoring correspondence (given that, by default, it is an intrusive and invasive measure).
>
> Whether or not less intrusive methods of monitoring could have been used than direct access to the content of communications by the employee.
>
> The use made by the company of the results of monitoring activity, and if the results are used to achieve the objective that provided the grounds for the monitoring.
>
> The existence of protection mechanisms for the employee, ensuring that the employer does not access the content of communications without first informing the employee.

These factors must be evaluated by national courts to weigh up the opposing interests (the disciplinary power of the employer versus the right to privacy and the confidentiality of correspondence of the employee), and thus to determine whether or not the monitoring is in accordance with the law.

In the case of interest here, the court has ruled in favour of the employee, Mr. Barbulescu, due to the fact that:

Romanian authorities had not adequately protected the right of Mr. Barbulescu to have his private life and correspondence respected.

Jurisdictional bodies had not determined whether or not the plaintiff had received prior notification from his employer of the possibility that his communications could be monitored.

Consideration had not been given to the fact that the employee had not been informed of the nature or scope of the oversight, or of the degree of intrusion into his private life and correspondence.

National courts had not determined the specific reasons for the introduction of monitoring measures, or if the employer could have used measures that would result in less intrusion into the private life and correspondence of Mr. Barbulescu, or if his correspondence could have been accessed without his knowledge.

3.- What are the consequences of this judgment for companies in Spain? Will we see a change in the corporate doctrine of the courts and tribunals?

A priori and in practice, there should be no significant consequences. Indeed, as stated in the current doctrine of the Constitutional Court (CC) and case law of the Supreme Court (SC), **companies must inform the employee of its policies for control of the use of IT tools before adopting disciplinary measures.**

There is a line of case law that stems from the protection of fundamental rights and which establishes the need for restrictions on the exercise of rights to be duly justified, proportional to the sacrifice made by employees and that the regulation that imposes it (whether it be conventional or for internal use) must be sufficiently familiar to personnel.

More specifically, with regards to the verification of compliance by the employer with its industrial obligations when the office computer used by the employee to perform his duties is inspected, the CC and the SC have made important pronouncements (for all, CC 241/2012; 170/2013; SC 20-9-07, Rec. 966/06; SC 8-3-11, Rec. 1826/10). The doctrine of the CC and the SC can be summarised as follows:

a.- The IT systems of a business are a work instrument subject to the powers of control of the employer (CC 241/2012).

b.- The employer must put in place guidelines on the use of IT resources and warn of the existence of controls and of measures that should be adopted (where applicable) to guarantee the effective use of resources in the workplace, irrespective of the possible application of other preventative measures, such as the exclusion of certain connections (CC 241/2012). A failure to provide warning of possible limitations on use and the possibility of controls being carried out constitutes a violation of the right of the employee to privacy (SC 8-3-11, Rec. 1826/10).

c.- When there is an absolute ban on personal use, said use can be controlled and mechanisms put in place to ensure that IT equipment is used solely for professional purposes.

If the equipment is used for private purposes in violation of these bans and the employee is aware of the controls and measures applicable, the control cannot be deemed to have violated "a reasonable expectation of privacy" under the terms established in the following pronouncements: ECHR 25-6-97, the Halford case; and ECHR 3-4-07, the Copland case to assess the existence of a violation of ECHR art.8.

d.- The same rule applies when the prohibition on personal use is contained in the applicable collective agreement (CC 170/2013).

e.- Employer access to e-mails of the employee must meet requirements in terms of proportionality (CC 170/2013). Said access must meet the following conditions:

First of all, said access must be a ***justified measure*** based on suspicions of irregular conduct by the employee.

The measure must be ***suitable*** *for the stated objective* of the company, which is to confirm whether or not the employee had in fact committed the suspected offence (e.g. the disclosure of confidential company information to third parties) in order to adopt the appropriate disciplinary measures.

The control must also be considered ***necessary***, given that, as an instrument for the transmission of said confidential information, the content or text of e-mails would constitute evidence of said irregularity in view of the possible legal challenge filed against the penalty handed down by the company (thus, in the example cited mere access to other elements of the communication, such as the name of the sender or recipient, which on their own would not constitute evidence of the alleged offence, would not be sufficient).

Finally, the measure must be ***measured and balanced.*** In other words:

a) The company must carry out its control with *guarantees* **(**e.g. with the involvement of an IT expert and notary)
b) The content of messages must not reflect specific aspects of the *personal and family life of the employee* but rather only information relating to the activities of the business, the disclosure of which to third parties constitutes a breach of good contractual faith.
c) The measure must be carried out in such a way that, in view of the breach being investigated and its relevance to the company, the inspection conducted *cannot* be considered disproportionate in terms of its consequences for the privacy of the employee.

On the other hand, when there are no clear guidelines in place in relation to prohibition there is a general tolerance of certain types of moderate personal use of company IT and communications equipment that creates an expectation of confidentiality in its use, which, even if it does not become an impediment to company control due to the fact that, although the employee has a right to respect for their privacy, they cannot demand such respect when they use a medium provided by the company against instructions put in place by the company for its use and outside the controls provided for said use and to ensure the continuation of service.

4.- Conclusion

From a fundamental rights perspective, it is essential to determine whether the access to content of company computers or other company IT equipment is in violation of Article 18.3 of the EC, for which the conditions for making this equipment available must be met.

The company is limited in its ability to exercise control by the applicability of fundamental rights. However, the intensity and strictness with which company measures to monitor and control their employees should vary according to the configuration of the terms of use of IT equipment and instructions from the employer for its use.

Companies may monitor the internal e-mail and social network activity of their employees on company equipment provided, but must remember in particular that employees must be made aware in advance that their equipment may be monitored via prior notification or communication. The control must be proportionate, necessary and as non-invasive as possible, with a balance between the interests of the business and the privacy of the employee**.**

In short, the first thing that businesses must do is establish a policy, protocol or similar set of regulations governing the use of said IT tools that reduces, or even eliminates, what has been described as a "*reasonable expectation of privacy*" and provide information on controls of IT equipment that will be carried out, respecting fundamental rights at all times and, in particular, the right to privacy in communications, without prejudice to the possible application of other preventative measures, such as the exclusion of certain connections.

In the next few weeks, a number of legal studies of the ECHR judgment will be published, which must be analysed in order to find out about the different perspectives of the judgment. In particular, one must wait for upcoming legal pronouncements that pick up on this judgment.

For more information, you can consult the aforementioned judgment here

For further information, please contact:
Alfredo Aspra
alfredo.aspra@AndersenTaxLegal.es

José Antonio Sanfulgencio
jantonio.sanfulgencio@AndersenTaxLegal.es