



Luxembourg newsflash

13 October 2017

Monitoring of the use by an employee of a professional instant messaging service for personal purposes: court decision in *Bărbulescu v. Romania*

On 5 September 2017, the Grand Chamber of the European Court of Human Rights (hereinafter the “**ECHR**” or the “**Court**”) examined for the first time the issue of the monitoring of electronic communications of an employee by a private employer, within the framework of an action brought by Mr Bărbulescu, an engineer employed by a private company in Romania. Mr Bărbulescu had been dismissed for using for personal purposes, in breach of the provisions of the internal regulations of the company, a professional *Yahoo Messenger* account created at his employer’s request for the purpose of responding to customers’ enquiries.

The decision handed down last month overturns a ruling made less than two years earlier in the same case¹. The ECHR had then held, by six votes to one, that the monitoring by the employer of the communications of Mr Bărbulescu had been reasonable in the context of disciplinary proceedings deeming that the domestic Romanian courts had struck an adequate balance between the employee’s right to respect for his private life and correspondence and the employer’s interests.

This decision in which the Grand Chamber has just held, by eleven votes to six, that there has been a violation of the applicant’s right to respect for his private life does not however constitute an absolute enshrinement of the right of employees to protection of their privacy to the detriment of the employer’s right to carry out monitoring. In reality, its impact on employers in Luxembourg will be limited (I). However, in the light of the facts of the decision (II), it is highly advisable that employers eager to implement a monitoring system to ensure that their employees spend their working time performing their professional duties, should make sure that they observe a particular time schedule as well as follow the methodology suggested by the Court (III).

¹ ECHR, 12 January 2016, decision no. 61496/08 (Fourth section of the Court)

I. A limited impact for employers in Luxembourg

Actually, and contrary to certain alarmist comments, this decision should not fundamentally change domestic law as Luxembourg already offers adequate and sufficient safeguards against interferences with private life within the framework of the employment relationship.

In Luxembourg, an employer who wishes to implement a system for the monitoring of its employees must obtain prior authorisation from the National Commission for Data Protection (hereinafter the “**NCDP**”). The employer is also required, in accordance with article L. 261-1 of the Labour Code, to inform employees as well as the staff delegation prior to the implementation of such a monitoring system.

As regards the use of the Internet or instant messaging, an outright ban on accessing the internet or using an instant messaging for private purposes during working hours could under no circumstances justify the individual monitoring of the use made thereof by an employee on the grounds that the use of the internet or of an instant messaging at work is presumed to be conducted exclusively for professional purposes in the light of the fact that all employees are entitled to respect for their private lives, including in the workplace. The employer retains the right to impose certain conditions in relation to the use of the internet or instant messaging at the workplace for private purposes, but is required, in the event that it plans to monitor and control the use made thereof by its employees, to inform them in clear terms of the contemplated monitoring system and in respect of the methods of control likely to be applied before their implementation.

The monitoring of employees must be graded and global, without leading to the identification of any employee in particular. It is only at a second stage, when the employer has concrete evidence that a use of the internet is detrimental to the company, that the employer may then take appropriate control measures and undertake individual monitoring.

Finally, this decision is an opportunity to separate the wheat from the chaff: in the same way as before an employee cannot dedicate his working hours to personal activities with total impunity. It is simply that an employer who wishes to dismiss an employee on this basis may only invoke evidence in this regard if such evidence has been obtained faithfully. Indeed, the manner in which the employer obtained the evidence of the employee's breach of the internal regulations is precisely the issue which proved to be the deciding factor in the Bărbulescu case.

II. The time schedule for the implementation of the monitoring of the employee's communications: a determining element in assessing the lawfulness of the monitoring

The chronology of the facts in the case at hand was a deciding factor in assessing the lawfulness of the monitoring of the employee's instant messaging account.

The dispute involved a private Romanian commercial company and one of its employees, Mr Bărbulescu, a sales engineer. Mr Bărbulescu had been dismissed for using during working hours and for personal purposes, in breach of the provisions of the internal regulations of the company, a professional *Yahoo Messenger* account (an online chat service offering real-time text transmission over the internet) created at his employer's request for the purpose of responding to customers' enquiries. The internal regulations in question prohibited in effect the use of computers for personal purposes without however specifying explicitly that the employer had the possibility to monitor the communications of its employees.

On 20 December 2006, Mr Bărbulescu signed the above-mentioned internal regulations after having duly inspected them. On 3 July 2007, Mr Bărbulescu, like his colleagues, received an information notice reminding that the time spent in the company had to be time spent dedicated to the company and not to occupations of a private nature. In this notice, the employer also informed the employees that it had "*a duty to supervise and monitor employees' work and to take punitive measures against anyone at fault*" and emphasised that the misconduct of employees "*will be carefully monitored and punished*". To illustrate this, the employer pointed out that an employee had been dismissed for disciplinary reasons for private use of the communications tools of the company. The applicant acquainted himself with the notice between 3 and 13 July 2007. From 5 to 13 July 2007, the communications of Mr Bărbulescu were recorded in real time by the employer.

On 13 July 2007, the employer summoned Mr Bărbulescu to allow him to explain the reasons for the use of the company's resources for personal purposes. In the relevant notice the employee was informed that his *Yahoo Messenger* communications had been monitored and that there was evidence that he had used the internet for personal purposes, in breach of the internal regulations. The employer had also attached some charts to the notice indicating that the employee's internet activity was materially exceeding that of his colleagues. The employee informed the employer in writing informing that he had used the messaging service in question for work-related purposes only. Less than one hour later, the employer again summoned the employee asking him to explain why the correspondence exchanged between 5 and 12 July 2007 pursued private objectives. In this second notice, the employer annexed a 45-page transcription of messages which the applicant had exchanged with his brother and his fiancée, the messages related to personal matters and some were of an intimate nature.

On 1 August 2007, the employer dismissed the applicant for disciplinary misconduct. Mr Bărbulescu challenged his dismissal before the domestic courts of Romania arguing that his right to respect for his personal life and correspondence had been infringed.

On 12 January 2016, a chamber of the Fourth section of the ECHR ruled, by six votes to one, that the monitoring by the employer of the communications of Mr Bărbulescu was reasonable within the framework of disciplinary proceedings, since the monitoring implemented had enabled the employer to prove the breach of the internal regulations.

On 5 September 2017, this decision was overturned by the Grand Chamber of the ECHR which held, by eleven votes to six, that there had been a violation of article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter the “**Convention**”), deeming that the domestic Romanian courts had not performed an adequate balancing exercise between the employee’s rights to respect for his private life and correspondence and the employer’s interests.

Finally, the Court agreed with the reasoning of the applicant who was of the opinion that the issue of the tolerance or the outright ban of the employer in respect of the use of the internet for personal purposes was not a decisive factor for the analysis, in contrast to the issue of the time at which the employee had to be informed of the monitoring of his communications.

Indeed, even in the event of an outright ban on personal internet use, the employer must directly and explicitly inform the employee of its intention to have recourse to a system of monitoring of the communications of the employee before implementing such a monitoring system.

In addition, the employer will only be entitled to use the results of the monitoring of the professional digital tools used by the employee provided that it has scrupulously followed the methodology set out by the Court, a methodology which it should be reiterated is already applied in Luxembourg and integrated into its domestic law.

III. Criteria for the assessment of the legitimacy of an infringement of an employee’s private life.

As was the case before this decision, the proof of the failure attributed to the employee may not be reported in any manner whatsoever. The end does not justify the means, the employer must remain loyal towards its employee even when it is a matter of proving the disloyalty of an employee. The decision of 5 September is therefore an opportunity to remind that the employer may not conjure up its duty to safeguard the interests of the company or even the outright ban for the employees on personal internet use in order to legitimise the implementation of monitoring which violates the respect for the private lives of the said employees.

It is in this respect that the Court provides a clear methodology in the form of a questionnaire divided into seven parts which the domestic courts called to rule in similar cases are invited to comply with. It is also in the interest of employers wishing to ensure that their employees spend their working time in the exercise of their professional duties to use this questionnaire before implementing a monitoring system.

1. Has the employee been informed of the possibility that the employer might take measures to monitor correspondence and other communications, and of the implementation of such measures?

To satisfy the requirements of article 8 of the Convention, the information given to the employee must in principle be clear about the nature of the monitoring and be given prior to the implementation of such monitoring.

The fact that an information notice contains sufficient information enabling employees to understand that their communications are likely to be monitored is not sufficient. The information delivered by the employer must not be made by means of innuendos but must be explicit. As a consequence, the employer must not merely inform that the work of employees may be monitored, but must explicitly indicate to the said employees that their emails/messages exchanged during working hours on a duly identified messaging service may be subject to monitoring. This information must be provided beforehand, i.e. before the implementation of such monitoring.

In the case at hand, the information notice communicated to employees did not indicate precisely that the employer could monitor their communications, including communications exchanged on the professional instant messaging service *Yahoo Messenger*. In addition, the employer only informed Mr Bărbulescu of the monitoring carried out on the said messaging service once the monitoring in question had been completed.

2. What were the extent of the monitoring by the employer and the degree of intrusion into the employee's privacy?

The Court points out that a distinction should be made between monitoring of the flow of communications and of their content. It is also important to verify whether all communications or only part of them have been monitored, and to determine whether the monitoring was limited in time or if the number of persons who had access to the results was restricted.

In the case at hand, the employer initially informed the applicant that the monitoring had related to the flow of communications and had attached as evidence graphic data indicating the internet traffic of the applicant. Finally, it turned out that the monitoring had been carried out on all communications exchanged on the instant messaging service over a period of several days, as the employer had recorded them in real time over the monitoring period, having had access thereto and having printed the contents thereof.

3. Has the employer provided legitimate reasons to justify monitoring the communications and accessing their actual content?

The Court recalls that since monitoring of the content of communications is a distinctly invasive method by nature, it requires weightier justification.

It is indisputable that the employer is entitled to verify the use of tools made available to its employees, and in particular the internet use during working hours, amongst others in order to verify that such use does not harm the company's interests. However, the employer cannot justify monitoring its employees' communications as well as having access to their

content by merely invoking the need to protect itself against the risk that the employees may damage the company's IT systems, may engage in illegal activities in cyber space thereby incurring the company's liability, or may disclose the company's trade secrets, if the risk invoked is merely hypothetical.

In the case at hand, the monitoring of the communications of Mr Bărbulescu and the access to their contents did not seem to have been aimed at protecting the company against one of the above-mentioned risks, but rather at establishing a breach of the internal regulations. At no time during the proceedings before the domestic courts was the applicant concretely accused of having exposed the company to the above-mentioned risks.

4. Would it have been possible to establish a monitoring system based on less intrusive methods and measures than directly accessing the content of the employee's communications?

The Court invites the domestic courts to assess, in the light of the particular circumstances of each case whether the aim pursued by the employer could have been achieved without directly accessing the full contents of the employee's communications.

In the case at hand, the Court is of the opinion that it is not impossible that the breach of the internal regulations attributed to Mr Bărbulescu could have been established by other means than access to the contents of the communications.

5. What were the consequences of the monitoring for the employee subject thereto? How did the employer use the results of the monitoring operation, in particular were these results used to achieve the declared objective of the measure?

The Court recommends that the domestic courts analyse the manner in which the results of the monitoring were used in relation to the employee. In particular, the disciplinary sanction imposed by the employer must be adapted to the misconduct attributed to the employee.

In the case at hand, the employer applied the most severe disciplinary sanction by dismissing Mr Bărbulescu.

6. Had the employee been provided with adequate safeguards, especially when the employer's monitoring operations were of an intrusive nature?

The Court specifies in this respect that such safeguards should in particular ensure that the employer cannot access the actual content of the communications concerned unless the employee has been notified in advance of such a possibility.

In the case at hand, it is likely that the employer had had access to the content of the communications of the employee before the employee was informed thereof. The fact that the employee stated that he had only used the instant messaging for professional purposes does not authorise the employer to examine the contents thereof given its failure to inform the employee of the possibility that his communications on the said messaging service may be monitored and its failure to specify the nature and extent of the monitoring.

7. Could the employee whose communications were monitored have access to a remedy before a judicial body with jurisdiction to determine how the criteria outlined above were observed and whether the impugned measures were lawful?

As a result, in order to assess the lawfulness of the implementation of a monitoring system, the domestic authorities will also have to verify whether the employee has benefited from a remedy.

In the case at hand, the employee had at his disposal several internal remedies enabling him to bring about an examination of the compatibility of the monitoring of his communications with his right to respect for his private life and correspondence. The employee had voluntarily chosen to limit his remedies to the lodging of a criminal complaint and referral to the labour courts.



For more information, please contact:



Philippe Schmit

Partner, Employment Law,
Pensions & Benefits

philippe.schmit@arendt.com

Tel: +352 40 78 78 240

This document is intended to provide you with general information on the subjects mentioned above.
Under no circumstances shall it constitute legal advice or replace adequate consultation with a legal advisor.