Briefing

January 2016

SHEPHERD+WEDDERBURN

Can employers really snoop through private emails? A closer look behind the headlines



Elouisa Crichton
elouisa.crichton@shepwedd.co.uk
Katie Russell
katie.russell@shepwedd.co.uk
Joanna Boag-Thomson
joanna.bt@shepwedd.co.uk

In a case that came hot on the heels of the recent Safe Harbour ruling, the European Court of Human Rights has ruled that an employer did not breach Article 8 of the European Convention on Human Rights (the right to privacy) by reading an employee's private messages. While at first glance this may look like a controversial decision, it does not go any further than existing law, and the facts themselves show that the employer acted proportionately in the circumstances.

In this update we explain the decision in Bărbulescu v Romania. We look behind the headlines and explore the wider legal issues around employers rights to investigate employees' use of technology for private purposes in the workplace.

The Bărbulescu v Romania case

Mr B was employed in Romania. He was dismissed in 2007 for sending private messages from his work Yahoo Messenger account. He raised legal proceedings challenging his dismissal and arguing that by reading his messages his employer had breached his right to privacy. The European Court of Human Rights (ECtHR) ultimately determined that his right to privacy had not been breached.

The facts

- The employer asked Mr B to set up a Yahoo Messenger account for professional purposes. The employer did not know that Mr B also set up a linked personal Yahoo Messenger account.
- There was a strict policy prohibiting employees from using work internet or devices for personal purposes. This policy was clearly communicated to all employees.
- On 13 July 2007, Mr B was informed that his employer had monitored his Yahoo Messenger communications for one week and identified that he had been using the work internet for personal purposes during working time. Mr B denied this and said that he had only used the account for professional purposes.
- On the back of this assertion, his employer presented a 45 page transcript of personal messages (some relating to his health and sex life) sent from his 'work' account to his brother and fiancée amongst others. Five short messages between the employee and his fiancée from his private Yahoo Messenger account were also included on the transcript, although none of these messages included any intimate information.
- Mr B was dismissed for breaching the company's IT policy.

The decision

The Romanian Court of Appeal determined that the dismissal was fair and the employer had acted proportionately: it had the right to monitor the 'work' messenger account (particularly as the employee had claimed that all the messages were sent for professional purposes).

Mr B continued his challenge to the ECtHR arguing that his dismissal breached his Article 8 right to privacy. The ECtHR started by deciding that Mr B's Article 8 right to 'respect for private and family life, the home and correspondence' had been engaged. It then had to decide whether the employer's interference with Mr B's right to privacy was justified. The key question was whether the correct balance had been struck between Mr B's right to privacy, and the employer's legitimate interests. The ECtHR held that:

- it was reasonable for an employer to check that its employees were working during work hours. The employer had accessed the account in the belief that it contained client related communications. The messages had only been accessed for one week. The transcripts were reviewed following the employee's assertion that the messages had been work related to establish whether there had been a disciplinary breach.
- Mr B had been able to raise his arguments in the domestic courts. During those proceedings, the transcripts were used appropriately: the court judgements referred to the fact that private messages had been sent but the content of those messages was not revealed in any of the judgments.

The majority decision of the ECtHR was that the Romanian courts had fairly balanced the employee's right to privacy against the employer's legitimate interests. There was no breach of the Convention.

What do employers need to know?

The Bărbulescu v Romania case has been widely covered in the media with the suggestion being that it gives employers carte blanche to read employees' private emails (and potentially dismiss employees for sending such emails at work). However, the headlines can be quite misleading. We have explained below the key issues that employers and employees should be aware of.

IT policies

In this case, the company had a very clear, well communicated and strict policy prohibiting personal use of work internet or devices. Any personal use would therefore breach the policy. It was in this context that the employer was found to have acted reasonably in monitoring the messages. Organisations with more lenient IT policies permitting some degree of personal use would not necessarily have been justified in monitoring messages in this way, or dismissing an employee for sending personal messages while at work.

It is important to consider this case in its proper place and time: the events occurred in Romania nearly a decade ago when people were far less likely to have easy access to the internet or messaging services at home or on smart phones as we do today. The employer was justifiably concerned about employees misusing the facilities it offered. Most employers in the UK today do not have IT policies imposing a blanket ban. It is far more common to prohibit excessive or inappropriate use of work IT facilities (although there will be some environments where a complete ban may be justifiable). The ECtHR confirmed in its judgment that it would not be acceptable for employers to carry out unregulated snooping of staff's private messages.

IT policies should set out what information employers can collect and how they will do this. Employers will be entitled to monitor work related documents and correspondence (including email and instant messenger) to ensure that employees are properly carrying out their work during work hours. However, they should still ensure that they act reasonably in doing so.

In the absence of a warning to the contrary, employees will have a reasonable expectation that personal emails, messages and documents stored on work devices will not be monitored. As such, employers will need to be very clear if they intend on monitoring such communications/documents. Where there is a 'bring your own device' (BYOD) policy in force, employees will have an even greater expectation of privacy. Employers should make it very clear to employees in the employment contract or BYOD policy what, if any, monitoring they can expect.

IT policies should include specific rules on the use of emails, instant messaging, social networks, blogging and web surfing. They should also explain what will be monitored, for example communications/documents sent via the employer's server and those stored on or sent from the employer's device (or the employee's own device where a BYOD policy is in place). Monitoring of private information must only be done to the extent necessary and the policy should be guided by the principles of necessity and proportionality. The rights and obligations of employees should be set out clearly, with transparent rules on how the internet may be used, how and why monitoring is conducted, how data is secured, used and destroyed, and who has access to it. Employees should ideally be asked to confirm their consent to the policy in writing.

When can an employer read personal messages?

In this case, the employer asked the employee if the messages were personal. As the employee denied that the messages were personal the employer needed to read the content to understand whether the messages were sent for work purposes. Employers may not be justified in reading the content of messages where the employee acknowledges that they are personal and there is no reason to presume that the content is inappropriate.

Also, Mr B was using the Yahoo Messenger system as

opposed to email. Unlike emails, many instant messenger systems do not allow you to add a message 'subject'. If an employee has clearly marked or stated in the subject that an email is 'private' or 'personal' then the employer may not be justified in reading the content of that message. This is not a hard and fast rule as in some cases, emails sent in a professional capacity will appropriately be titled as 'private' and the employer would still have a legitimate interest in reading them. If an employer suspects that an email is personal, it may wish to speak with the employee before reading the content.

Mr B's employer accessed both a work messenger account and a personal account. However, it did not know that the second account was personal when it accessed it. Again, while an employer may have a policy that work IT facilities should not be used to access personal email accounts and could legitimately check whether such accounts have been accessed, it would not normally be reasonable for the employer to go further and read the content of such messages.

In most cases, the employer would have no legitimate interest in reading emails in a personal email account. The exception to this may be where an employer reasonably suspects an employee of stealing confidential information be sending it on to a personal email account. If accessing the personal email account is the only method of checking whether the employee has done this, then it may be permissible for the employer to carry out such checks, provided it goes no further than is necessary, and has the right in its IT policy or employment contracts to carry out such checks.

Data protection issues

Neither the Romanian domestic courts nor the ECtHR undertook a detailed examination of the data protection implications of the monitoring of Mr B's Yahoo messages. However, it was noted that the initial monitoring period was short, and did not examine other data or documents on Mr B's computer. Also, the employer accessed the Yahoo Messenger accounts on the assumption that the information in question related exclusively to professional activities. The ECtHR therefore found that the employer's monitoring was limited in scope and proportionate.

What is the impact on investigations?

When looking at personal information, there is a need to strike the right balance between the employee's right to private life, and the employer's interest. In carrying out investigations, employers should:

- Have in place an appropriate IT policy which makes it clear what you are entitled to look at, communicate this policy to employees and act in accordance with that policy.
- Have a legitimate reason for looking at any personal communications.
- Go no further than is necessary and consider whether there are less intrusive ways of finding out the required information.
- Where possible, speak with the employee before looking at the content of messages or documents.

How to protect your business

Both this case and the recent Safe Harbour ruling have brought the issues of employee data processing and monitoring into the spotlight. Organisations may wish to take steps now to review their IT policies and practices to reflect the principles from the ECtHR's judgment.

The full case report can be found **here.**

If you would like assistance updating your policies, or any further information on this case, please get in touch with your usual Shepherd and Wedderburn contact.

Elouisa Crichton
Solicitor
T +44(0)141 566 7429
M +44(0)770 214 1289
E elouisa.crichton@shepwedd.co.uk

Katie Russell
Partner
T +44(0)131 473 5266
M +44(0)787 269 9897
E katie.russell@shepwedd.co.uk

Joanna Boag-Thomson
Partner
T +44(0)141 566 8570
M +44(0)775 387 1607
E joanna.bt@shepwedd.co.uk