ECtHR: Monitoring of employee's emails breached right to privacy

September 2017

An employer's monitoring of an employee's work emails amounted to a violation of Article 8 (right to respect for private and family life, the home and correspondence) of the European Convention on Human Rights (ECHR), according to a recent judgment of the Grand Chamber of the European Court of Human Rights (ECtHR). It overturned a previous decision that the employer's actions did not violate Article 8 (*Bărbulescu v Romania*).

Workplace communications

B was employed by a Romanian company (S) as an engineer in charge of sales. At S's request, B created a Yahoo Messenger account for the purpose of responding to clients' enquiries. On 3rd July 2007, S informed its employees that one employee had been dismissed after she had privately used the internet.

Monitoring

S decided to monitor B's Yahoo accounts between 5th and 12th July. It found that B had been using the Yahoo Messenger account for personal purposes, to send messages to his fiancée and his brother. B denied using the account for personal purposes and S therefore presented him with a 45 page transcript of his personal emails, which related to intimate subjects including B's health and sex life.

Dismissal and claim

On 1st August S terminated B's employment contract for breach of S's internal regulations that prohibited the use of company resources for personal purposes. B unsuccessfully challenged his dismissal before the Romanian courts, which found that S had complied with the relevant dismissal proceedings, had been entitled to set rules for the use of the internet, and had informed B of those rules.

Privacy complaint

B appealed to the ECtHR, arguing that S's decision to terminate his contract after monitoring his electronic communications and accessing their contents was in breach of his privacy, and that the Romanian courts had failed to protect his right to respect for his private life and correspondence under Article 8 EHRC. In its initial judgment, the ECtHR held that there had been no violation of Article 8 ECHR, and that the domestic courts had struck a fair balance between B's Article 8 rights and S's interests.

Privacy at work

The Grand Chamber of the ECtHR allowed B's appeal. It confirmed that, although it was

questionable to what extent B could have had a reasonable expectation of privacy, in view of S's restrictive regulations on internet use (of which he had been informed), "an employer's instructions could not reduce private social life in the workplace to zero. The right to respect for private life and for the privacy of correspondence continued to exist, even if these might be restricted in so far as necessary."

Balance not struck

The ECtHR found that the Romanian courts had not struck the right balance between B's right to respect for his private life, and S's right to take measures in order to ensure the smooth running of the company. It noted in particular the following points:

B had not been informed in advance of the extent and nature of the monitoring, or the possibility that S might have access to the actual contents of his messages. The ECtHR confirmed that, in order to qualify as prior notice, the warning from an employer had to be given before the monitoring was initiated, especially where it entailed accessing the contents of employees' communications. In this case, employees were simply told, shortly before B's disciplinary sanction, that one of their colleagues had been dismissed for using the internet for personal purposes.

In addition, the degree of intrusion into B's privacy was significant, since S had recorded all of B's communications during the monitoring period in real time and had printed out their contents.

The Romanian court had failed to determine whether there had been any legitimate reasons justifying the monitoring. It had referred to the need to avoid S's IT systems being damaged, or liability being incurred by S in the event of illegal activities online. However, these examples could only be seen as theoretical, since there was no suggestion that B had actually exposed S to any of those risks.

Further, the Romanian court had also not sufficiently examined whether the aim pursued by S could have been achieved by less intrusive methods than accessing the contents of B's communications. It had also not considered the seriousness of the consequences of the monitoring and the subsequent disciplinary proceedings, namely the fact that S had received the most severe disciplinary sanction.

Implications for UK employers

This judgment should not require a step change in how UK employers approach monitoring of employee communications.

Many of the points made by the ECtHR in terms of advance notification of monitoring and the limitations on monitoring already apply in the UK, whether under the Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 or the Information Commissioner's Employment Practices Code. These principles are maintained under the General Data Protection Regulation (GDPR), which imposes strict notification requirements which employers must comply with before processing employee data.

For further details, see our briefing: What do employers in the UK need to know about the new General Data Protection Regulation (GDPR) from an employment perspective?

In practice, this means that:

- Employers cannot entirely deny any right to privacy for employees using work computer systems, no matter how clear and well-communicated the policy is.
- Employers must therefore ensure that they approach any monitoring of employee's communications with care, having a clear business rationale for doing so, and carrying it out in a reasonable manner.
- Any monitoring should be limited (in time and scope) to what is strictly necessary, and carried out in accordance with the employer's policy.
- The policy must be notified to employees in advance of the monitoring taking place.
- The policy should make it clear when or if personal use of the employer's communication systems may be permitted. It should also (if appropriate) make it clear that the contents of communications may be viewed.

This article was written by Rebecca Cousin and Charles Cameron. Slaughter and May advises on all aspects of data protection and privacy, including GDPR compliance audits. If you would like further information, please contact Rebecca or your usual Slaughter and May advisor. Further publications are available on our website.

Rebecca Cousin
T +44 (0)20 7090 3049
E rebecca.cousin@slaughterandmay.com

Charles Cameron
T +44 (0)20 7090 5086
E charles.cameron@slaughterandmay.com

Dated September 2017