European Court of Human Rights revisits employee privacy

The Grand Chamber of the European Court of Human Rights (ECtHR) handed down its judgment in in *Bărbulescu v Romania* following an appeal from the Chamber of the ECtHR's decision in January 2016 (read our analysis of that decision here).Mr Bărbulescu had been dismissed by his employer following his use of a work Yahoo Messenger account set up to respond to customer queries to send numerous personal messages to his fiancée and brother. He claimed his dismissal was a violation of his right to privacy under Article 8 of the European Convention on Human Rights (ECHR).

In a surprising decision, the ECtHR departed from the earlier decision to find that there had been a breach of the applicant's right to privacy. Mr Bărbulescu was awarded €1,365 in respect of his legal costs, but did not receive any compensation. The ECtHR felt that the finding that his rights had been violated was sufficient redress.

In practice however, UK employers have no reason to lose sleep over this decision.

This is because the UK has heavily regulated employee privacy at work, primarily through the Data Protection Act 1998 and the Regulation of Investigatory Powers Act 2000. As the ECtHR noted, the UK is one of only a small handful of Council of Europe countries to have done so. This alone goes a long way to protect the UK from this decision. The ECHR applies to the private employment relationship in a limited way and only requires here that the member state has put in place relevant regulation that allows a balance to be struck between the competing interests at stake (employee privacy and the business need to ensure employees use work equipment appropriately, for example). As the UK has done this, the ECtHR is likely to give the UK a wide discretion.

Despite finding a violation of Mr Bărbulescu's right to privacy, the ECtHR emphasised that employee privacy is not unlimited and communications can be monitored in some circumstances. This judgment sets out factors they will consider when determining if an employee's privacy has been violated. From these we can draw out some key points for employers when formulating a policy of monitoring of employee communications at work.

- The employee should be notified in advance that the flow of communications will be monitored. (It is key therefore to include clear

guidance in either contracts of employment of employee handbooks on acceptable use of work IT equipment and any monitoring);
- If the *content* of communications is to be monitored, the employee must be notified as above but this type of monitoring will require more rigorous justification;
- You should carefully consider how intrusive the policy is on the employee's privacy. It may be safer to limit the duration of any monitoring, which communications are monitored, and/or the number of people who have access to the results of the monitoring in order to minimise the intrusion into the employee's privacy;
- You should consider the context of any communications. Monitoring of communications from an employee's personal email account or phone number will be very difficult to justify;
- Safeguards should be put in place to prevent abuse of any policy of monitoring employee communications.

These considerations broadly align with existing UK law and guidance from the Information Commissioner's Office so employers in compliance with UK law have little to fear from this decision.

The full judgment is available here.