Monitoring employees' emails — how far is too far?

Davinia Brennan, Associate, A&L Goodbody, examines this question in light of a recent decision from the European Court of Human Rights which appears to go against employees' rights

The monitoring of employees in the workplace has drawn considerable media attention recently due to the decision by the European Court of Human Rights ('ECHR') in *Barbulescu v Romania* (12th January 2016) (copy of the judgment available at: www.pdpjournals.com/docs/88507). The ECHR ruled that an employer could monitor and access personal emails sent by an employee during work hours from his Yahoo Messenger account.

Misleading media reports that the decision means that employers will from now on enjoy a carte blanche to monitor employees' emails caused shockwaves amongst employees.

However, the decision was based on some very specific facts — in particular, a prohibition on work equipment for personal use — and does not set a precedent for unrestricted monitoring by employers of emails sent by employees during office hours. It does, however, serve as a useful reminder of the importance for employers to have a clear policy in place regarding personal use of company equipment and monitoring of employees at work.

This article considers the implications of the ECHR's decision, and steps employers can take to ensure they comply with data protection and privacy laws when monitoring employees' communications in the workplace.

Background

Mr Barbulescu set up a Yahoo Messenger account for professional use, at his employer's request. Mr Barbulescu's employer subsequently informed him that his account had been monitored over several days, and the records showed that he had used the internet for personal purposes contrary to the company's internal regulations. The company had a clear policy in place which provided that: "It is strictly forbidden to disturb order and discipline within the company's premises and especially...to use computers, photocopiers, telephones, telex and fax machines for personal purposes."

When Mr Barbulescu denied using the Yahoo Messenger account for personal purposes, his employer presented him with a forty-five page transcript of his communications, including messages exchanged with his fiancée and his brother which contained personal and sensitive data (about his health and sex life). Mr Barbulescu was subsequently dismissed, and the transcript was used as evidence in disciplinary proceedings and in the courts.

The Bucharest County Court upheld Mr Barbulescu's dismissal. Mr Barbulescu then appealed to the Bucharest Court of Appeal, claiming that his emails were protected by Article 8 of the European Convention on Human Rights (the Convention), as pertaining to his 'private life' and 'correspondence'. The Bucharest County Court dismissed his appeal.

The Court of Appeal held that the employer's conduct had been reasonable and that the monitoring of his communications had been the only method of establishing if there had been a disciplinary breach. Mr Barbulescu complained to the ECHR that his employer's decision to terminate his contract had been based on a breach of Article 8 of the Convention, that the interference was not justified, and that the domestic courts had failed to protect his rights.

Decision of the ECHR

The ECHR did find that there had been an interference with Mr Barbulescu's right to respect for private life and correspondence within the meaning of Article 8 of the Convention — but ultimately concluded that there had been no violation of this Article.

It found that the domestic courts had struck a fair balance between Mr Barbulescu's right to privacy and the interests of his employer. The ECHR ruled that it was not unreasonable for an employer to want to verify that employees are completing their professional tasks during working hours, and that the employer had accessed Mr Barbulescu's account in the belief that it contained client-related communications. The ECHR was satisfied that the employer's monitoring was limited in scope and proportionate, as the messages on the employee's Yahoo Messenger account were examined, but not other documents stored on his computer. The ECHR

(Continued on page 4)

(Continued from page 3)

also noted that the Romanian courts had only used the transcript to prove the employee had broken the company's regulations, rather than focusing on its content.

Implications of the decision

This case is unusual, as most workplaces tolerate a limited amount of personal use of company equipment on the grounds that a blanket ban would be impractical, particularly for office-based employees working long hours.

It is important to note that the decision does not overrule prior ECHR case law. Earlier cases recognised that employees have a reasonable expectation of privacy, particularly in the absence of a warning of monitoring, in respect of:

- phone calls made from work (as held in *Halford v United Kingdom* (1997));
- email and internet usage (*Copland v United Kingdom* (2007)); and
- personal belongings kept in work (*Peev v Bulgaria* (2007)).

The ECHR distinguished previous case-law from the present case on the grounds that it did not involve a prohibition on personal use of company equipment or forbid employees from keeping personal belongings in the office. The ECHR effectively found that the prohibition in the present case rebutted any reasonable expectation of privacy that might exist.

The decision shows that the key issue as to whether there has been a violation of Article 8 of the Convention will depend on whether, on the facts, the employee has a reasonable expectation of privacy. It highlights the importance of employers having a well drafted phone, email, and internet usage policy in place which sets out the extent (if any) to which company equipment can be used for personal purposes.

> ***"The decision shows that the key issue as to whether there has been a violation of Article 8 of the Convention will depend on whether, on the facts, the employee has a reasonable expectation of privacy. It highlights the importance of employers having a well drafted phone, email, and internet usage policy"***

This policy should also give notice to employees of any monitoring of their communications and the purpose of such monitoring.

Ideally, employees should receive a copy of this policy as part of their induction training, and it should be readily accessible at all times on the company's intranet, or employee handbook.

Is the decision legally binding in the UK?

The Convention was incorporated into UK law by the Human Rights Act 1998, which requires the UK courts to take into account any decision of the ECHR. This means that decisions of the ECHR are of persuasive value to the UK courts.

It is worth noting that the ECHR's decision was wholly concerned with whether there was a violation of Article 8 of the Convention. The ECHR did not examine whether there was a breach of data protection laws under the EU Data Protection Directive 95/46/EC, as it does not have jurisdiction to do so.

Considerations for employers

The decision does not override the position under the UK Data Protection Act 1998 ('DPA') which also imposes restrictions on the ability of employers to carry out monitoring of employees.

Employers should be aware that the monitoring of employees' use of email, internet or the telephone, involves the processing of personal data and as such, data protection law applies to such processing. The DPA requires that personal data are obtained and processed fairly, for specified purposes, and are adequate, relevant and not excessive.

The UK Commissioner has issued an employment practices code (copy available at: www.pdpjournals.com/docs/88508) containing a whole section (Part 3) on Monitoring at Work. It highlights, in particular, the importance of being transparent with employees about any monitoring.

The Article 29 Working Party has also adopted a Working Document (WP55, copy available at: www.pdpjournals.com/docs/88509) which offers helpful guidance on the acceptable limits of monitoring of employees. Its main guiding principle is that any limitation of an employee's privacy should be proportionate to the likely damage to the employer's legitimate interests. It recommends that any monitoring measure must pass a list of four tests:

- is the monitoring activity transparent to the employees?
- is it necessary?
- is it fair?
- is it proportionate to the concerns it tries to allay?

The guidance suggests that employers inform employees of the use and purpose of any detection equipment activated at his/her working station, and of any misuse of electronic communications detected (email or internet), unless covert surveillance can be justified. It notes that prompt information can easily be delivered by software such as warning windows, which pop up and alert the

worker that the system has detected and/or taken steps to prevent an unauthorised use of the network.

Conclusion

The decision serves as a warning to employees that monitoring is permissible in circumstances where an employer has a transparent phone, email and internet usage policy in place. However, it also demonstrates that such monitoring must be fair, necessary and proportionate in regard to the concerns it seeks to allay. Employers should ensure they approach any monitoring of employees with caution, as excessive monitoring, where an employer acts as a distrustful big brother, is likely to lead to poor employee relations and a hostile working environment.

Top ten tips

Employers who intend to engage in surveillance of employees should ensure:

- the presence of a clear and comprehensive written company policy with regard to personal use of the phone, email and internet, in particular accessing social networking and instant messaging websites and blogs;
- transparency with any monitoring of employee communications — employers should clearly set out in their policies the extent and purpose of such monitoring;
- that any monitoring is necessary, proportionate and not excessive in regard to the concerns it seeks to allay;
- that any monitoring is carried out in the least intrusive manner possible (e.g. monitoring traffic data rather than content of data);
- that the policy is brought to the attention of the employees and readily accessible — ideally, a copy of the policy should be given to employees at their induction training, and should be available on the company intranet and/or in the employee handbook;
- that they carry out a Privacy Impact Assessment to ensure any monitoring strikes a fair balance between the privacy rights of the employee and the legitimate business interests of the employer;
- that the policy is regularly reviewed and updated to take account of developments in technology (e.g. wearable technology);
- that employee emails marked personal/private are not accessed by employers unless they have a legitimate reason for doing so;
- that where employees use personal devices for work purposes, a BYOD (Bring Your Own Device) policy is in place explaining acceptable usage of such devices during office hours and any monitoring of such devices; and
- that covert surveillance is only undertaken in limited circumstances, such as to prevent and detect crime.

Davinia Brennan
A&L Goodbody
dbrennan@algoodbody.com