A right to private life at work?

Peter Coe looks at *Bãrbulescu v Romania* in terms of monitoring versus privacy rights & the fast-approaching GDPR

IN BRIEF

- Employees have an irreducible minimum right to private social life while at work.
- Highlights five steps to help employers find the right balance.

I very much doubt that when Mr Bogdan Bãrbulescu created a Yahoo instant messenger (IM) account at his employer's request to deal with customer enquiries he had any idea it would end up the subject of litigation working its way all the way up to the European Court of Human Rights (ECtHR). But it has and, in doing so, it has given us an important ruling relating to employees' privacy in the workplace, particularly in light of the forthcoming introduction of the General Data Protection Regulation (GDPR) in May 2018. The case in question is *Bãrbulescu v Romania* [2016] App no 61496/08.

What's it all about?

On 3 July 2007, Bãrbulescu's employer sent a notice to all employees prohibiting personal use of the internet while at work. The notice also told employees that their work would be monitored. According to Bãrbulescu, he knew that he was not allowed to use his work computer for personal activity, but he did not realise that his communications would be monitored until after the notice had been circulated. It transpired that not long after the notice was sent, Bãrbulescu's employer began to monitor his internet use, including how and when he used the IM account he had created. On 13 July, Bãrbulescu's employer presented him with 45 pages of private IM messages he had sent using the work account he had created. Consequently, he was dismissed. This dismissal resulted in the litigation that ended up in the ECtHR, with Bãrbulescu claiming that his telephone, email and IM communications made while at work were subject to protection by virtue of his right to private life and correspondence pursuant to Art 8 of the European Convention on Human Rights.

What this means

As a general rule, to determine whether Art 8 has been engaged, the court involved would consider whether the individual had a reasonable expectation of privacy. An employer's policy (for instance) would tell an employee whether the employee has an expectation of privacy and what this looks like. However, the ECtHR's decision has thrown the cat among the pigeons. In finding that Bãrbulescu's Art 8 rights had been violated by his employer the court stated: '… an employer's instructions cannot reduce private social life in the workplace to zero. Respect for private life and for privacy of correspondence continues to exist, even if these may be restricted in so far as necessary.' Therefore, for the first time, we have an unequivocal statement from the ECtHR that, regardless of what an employer says, employees are subject to an irreducible minimum right to private social life while at work. Ultimately, this may well result in increased litigation based on Art 8 claims.

However, what the judgment definitely does not mean is that monitoring in the workplace by employers is now illegal. To the contrary, employers have a recognised, yet qualified, right to monitor their employees' communications. The ECtHR acknowledged, on behalf of employers, a '… right to engage in monitoring, including the corresponding disciplinary powers, in order to ensure the smooth running of the company'. Thus, in cases concerning a conflict between an employee's right to privacy and the employer's right to ensure the smooth running of the company (by monitoring employees' communications and/or internet use), a balance must be struck using the test of proportionality. Ultimately, if monitoring measures are challenged, then the domestic court will need to consider the consequences of the monitoring process for the employee as against the consequences for the employer. What domestic courts should consider when attempting to find this balance was set out by the court. Siân McKinley, in her excellent analysis of the judgment in *Counsel* magazine (see 'Snooping Bosses', December 2017, pp38-39), distills the court's guidance, the Article 35 GDPR impact assessment (discussed further below) and the relevant provisions of the Information Commissioner's Office (ICO) Employment Practices Code 2011, into five very helpful 'practical steps for employers' that I agree with entirely. These steps will help employers to defend their monitoring of employees' communications against Art 8 challenges:

(1) Employees should be told in advance that their employer may monitor their communications, and the way in which this will be done. The nature of the monitoring must also be made clear. So, if an employer wants to monitor the *content* of communications, this must be made clear to employees before it happens.

(2) Prior to monitoring their employees, employers should assess the extent of the monitoring they intend to carry out and its intrusion into employees' privacy. In doing so, they should consider the following questions:

- Can they limit the monitoring to the *flow* of communications, or does *content* also need to be monitored?
- Do *all* communications need to be monitored, or will monitoring *some* communications suffice?
- Can the monitoring be subject to a time limit?
- Can *physical* limits to monitoring be imposed?
- Can the number of people who have access to the results of the monitoring be limited?

(3) Legitimate reasons must be established for monitoring of the *flow* of communications. Due to its invasiveness, the monitoring of *content* will require even clearer reasons.

(4) Employers should assess whether a less intrusive monitoring system could be set up. In respect of monitoring *content* the employer must assess whether they could meet the legitimate reasons (see point 3) without directly accessing the full content of the communication(s).

(5) The monitoring process should be constantly reviewed by the employer, including the use of the results of the operation, the consequences for employees and whether the results achieve the identified 'legitimate reasons'.

> *"Ultimately, this may well result in increased litigation based on Art 8 claims"*

The GDPR

Prior to any monitoring taking place, the ICO's Employment Practices Code 2011 already recommends that employers complete an impact assessment, which is very similar in substance to the guidance above. The same can be said for Art 35 GDPR, pursuant to which data controllers that wish to process data (ie monitor data) which may result in a high risk to the rights and freedoms of individuals must carry out an impact assessment. In particular Art 35(3)(c) requires an assessment if the controller wants to carry out *systematic monitoring of a publicly accessible area on a large scale*. As McKinley states, this provision could include monitoring of a telephone system used by both the public and employees (such as a customer services call centre).

Conclusion

The ECtHR judgment corresponds, to a great extent, with the existing ICO's Employment Practices Code 2011 and the requirements, for certain situations at least, of the soon to be implemented GDPR. Thus, subject to the court's finding that employers cannot access the *content* of communications unless employees have been told beforehand that this may happen, employers' monitoring practices should already conform to the ECtHR's finding in *Bărbulescu*. In respect of the GDPR, Art 35(9) requires that data controllers, where appropriate, seek the views of data subjects or their representatives on the processing. However, this would not be appropriate if it would prejudice commercial or public interests or the security of processing operations. Thus, as McKinley observes, 'this appears to preserve the ability of businesses to carry out covert monitoring in exceptional circumstances'. **NLJ**

Peter Coe, senior lecturer in law, Aston University; barrister, East Anglian Chambers & Cornwall Street Chambers; consultant lawyer, Addleshaw Goddard (AG Integrate).