Client Alert | Employment, Compensation & Benefits

Employee monitoring – avoiding pitfalls in a changing landscape

October 2017

Authors: Stephen Ravenscroft, Tim Hickman, Matthias Goetz

Recent developments in case law and regulatory guidance have emphasised the need for employers to be cautious when implementing systems to monitor employees.

The decision of the European Court of Human Rights ("**ECtHR**") in the case of *Bărbulescu v Romania* (61496/08), and Opinion 2/2017 on data processing at work ("**Opinion**") issued by the Article 29 Data Protection Working Party ("**W29**"), each provide employers with important pointers on monitoring in the workplace. While such monitoring is not necessarily unlawful, employers need to take great care to ensure that they are not tripped up by the applicable requirements.

Bărbulescu v Romania

Mr Bărbulescu, a Romanian national, was employed by a private company based in Bucharest. At his employer's request, he created an instant messaging account. The employer's internal policies prohibited the use of company IT systems for personal purposes. Mr Bărbulescu received notification of this policy on two occasions, and he acknowledged the policy in writing. However, he was not specifically informed in the policy that his use of the company IT systems could be monitored by the employer.

The employer suspected Mr Bărbulescu of using the instant messaging account for private purposes, in breach of the policy. After monitoring the usage of his instant messaging account, the employer provided Mr Bărbulescu with a transcript of the personal messages he had exchanged on the system, and stated that he had breached the employer's policy. His employment was terminated by the company shortly thereafter, and his claims in respect of this dismissal were unsuccessful in the Romanian domestic courts. He brought a further claim in the Fourth Chamber of the ECtHR, alleging infringement of his right to privacy under Article 8 of the European Convention on Human Rights.

On appeal to the Grand Chamber of the ECtHR, it was determined that the Romanian courts had not given adequate protection to Mr Bărbulescu. In particular, Mr Bărbulescu had not been informed in advance that the employer would monitor his instant messaging account, and the Romanian courts had not given sufficient consideration to the level of intrusion into his private life caused by this monitoring, to the potential for alternative means of monitoring, or to the seriousness of the consequences of the monitoring.

The Grand Chamber held that the employer had a legitimate interest in monitoring the use of its IT systems, but concluded that such legitimate interests were outweighed by Mr Bărbulescu's right to privacy. Though the decision reverses that of the Fourth Chamber, our previous guidance on *Bărbulescu* remains substantially unchanged, as discussed further below.

The W29 Opinion

The W29 Opinion analyses the balance between the legitimate interests of EU employers and the privacy rights of their employees. Though largely a reaffirmation of the WP29's existing guidance (here and here) and the existing EU data protection framework under Directive 95/46/EC, the Opinion also provides additional useful guidance on the position under the EU General Data Protection Regulation ("**GDPR**").

The Opinion applies to all relationships between an employer and its employees (or individual contractors) and identifies a number of scenarios in which new technologies have resulted in heightened risks to the privacy of employees and contractors. In each scenario, guidance is intended to highlight the balance between the competing interests of the employer and employee. The Opinion notes that employers are subject to an overarching requirement to consider whether any given processing activity is: **(a)** necessary (and if so, the legal basis for that activity); **(b)** fair to the employees; **(c)** proportionate (taking into account the impact on the privacy of employees and contractors); and **(d)** transparent.

In particular, the Opinion considers the monitoring of employees by an employer, both within and outside of the workplace. If the employer permits employees any degree of private use of its IT systems, then employees should be able to designate private spaces within the IT infrastructure which the employer cannot access other than in exceptional circumstances, and the employer must be transparent and open with employees regarding its data processing activities. Monitoring of employees outside the office must be proportionate, and personal devices used in a professional context (i.e., 'Bring Your Own Device' or "**BYO Device**" schemes) must have strictly delineated boundaries between the employer's data and the employee's private data. This is often achieved through the use of "containerising" software to segregate the employer's data from other data.

The Opinion also warns that any material change that impacts the privacy of employees (e.g., the introduction by the employer of new software or systems used to process employee data) could mean that it is necessary for the employer to conduct a data protection impact assessment (an "**Impact Assessment**") under the GDPR, in order to identify and address any new data protection risks arising from the new software or systems. Where employers are unable to reduce such risks to a residual level, there is an obligation to consult with the relevant Data Protection Authority prior to the commencement of the relevant processing activity.

The Opinion, together with the WP29's previous employment-related guidance, encourages employers to communicate clearly with their employees regarding privacy-related issues, to choose privacy-friendly options as default on employer-issued software and devices, and to allow employees to prevent their data being captured by new technologies deployed by the employer, wherever possible.

How should employers react?

Notwithstanding the fact that the ECtHR judgement in *Bărbulescu* and the W29 Opinion are issued by separate bodies under entirely distinct legal regimes, there are several areas of overlap between them. In particular, employers who operate (or envisage operating) employee monitoring programs must be sensitive to the privacy risks associated with those programs. These risks broadly fall into the following categories: maintaining a balance between employer and employee interests; maintaining a separation between the employee's professional and private capacities; adequately informing the employee of the monitoring; and complying with the requirements of applicable data protection laws (including, from 25 May 2018, the GDPR).

Both the *Bărbulescu* decision and the W29 Opinion emphasise the obligation on employers to consider whether their legitimate interest in monitoring employees' use of the employer's IT systems is outweighed by the employees' right to privacy, taking into account the circumstances. The employer should assess whether its aims could be achieved with less intrusive methods. Any invasive monitoring activities should be limited to what is strictly necessary to achieve the employer's legitimate aims (e.g., the prevention of damage to its IT systems, or the avoidance of company liability).

The increasing ubiquity of connected technology has broken down old boundaries between work life and home life for many employees. As a result, employers should ensure that they maintain a clear distinction between the professional and private lives of employees, and areas of potential overlap should be identified and mitigated, to ensure that the employer does not inadvertently monitor private activities of its employees in which it has no legitimate interest. Careful planning of suitable measures is especially advisable where an employer has a BYO Device scheme in place.

Before commencing an employee monitoring program, an employer should provide appropriate notice to all affected employees. Effective prior notice must:

- be provided to the employee before monitoring activities start (especially where those activities will entail accessing the contents of an employee's communications);
- identify the employer entity responsible for the monitoring and explain to affected employees their available legal rights with respect to their privacy and the monitoring scheme;
- state that monitoring will take place and explain what communications or activities will be monitored and what data might be collected; and
- provide the employer's reasons for the monitoring.

Some employers have, in the past, sought to obtain consent from their employees in relation to monitoring activities. However, the W29 points out that in most cases there is an imbalance of power in the employer / employee relationship (because the employee is financially dependent on the employer) meaning that it would be difficult for an employer to show that any consent from its employees was genuinely "freely given" and completely voluntary. In addition, for activities such as network monitoring, the employee cannot realistically refuse consent without defeating the purpose of the monitoring. Consequently, it is generally inadvisable for employers to seek consent from their employees for most data processing activities. Instead, the legitimate interests balancing test considered above should be used by employers in most circumstances.

New technologies offer significant opportunities in terms of efficiency and business development, but it is important that employers remain cautious when using these technologies to engage in workplace monitoring. From 25 May 2018, the maximum fine applicable for non-compliance with the GDPR will be the greater of €20 million or 4% of global annual turnover. While the maximum fine is likely to be issued comparatively rarely, employers should bear in mind that Data Protection Authorities will also have the power to issue legally binding temporary or permanent bans on data processing activities that they consider unlawful (i.e., if a Data Protection Authority objects to an employer's monitoring program, it can shut that program down until such time as the employer can bring the program into line with the GDPR). Moreover, affected employees will have the right to bring collective claims against their employer in the event that their rights under the GDPR are infringed. Employers should therefore take these issues seriously and plan ahead. Further guidance on preparing for the GDPR is available in White & Case's extensive GDPR Handbook.

Kimberly Sharp and Francis Brown, trainees at White & Case, assisted in the preparation of this publication.

White & Case LLP
5 Old Broad Street
London EC2N 1DW
United Kingdom

T +44 20 7532 1000