Hewitsons' Employment
LEGAL UPDATE

January 2018
Vol.20 No.1

What's New

Use of covert cameras at work was in breach of the right to privacy and data protection law

In the recent case of *Lopez Ribalda & Ors v Spain* the European Court of Human Rights (ECtHR) held that the use of covert surveillance at work was in breach of the right to privacy under Article 8 of the European Convention of Human Rights. The ECtHR also held that the employer had acted in breach of data protection requirements.

Workers at a Spanish supermarket were told that surveillance cameras had been installed to address suspected theft. The workers were however only told about the cameras which were visible, not other covert cameras that had been installed. Following the installation of the cameras a number of employees were caught stealing via the covert cameras and were subsequently dismissed.

The employees alleged that the supermarket had breached their Article 8 right to privacy and their data protection rights. In the first instance the Spanish court held that the employer's use of cameras was justified, appropriate, necessary and proportionate.

However, the ECtHR disagreed and held that the employees' right to privacy had been breached. It held that video surveillance in the workplace is a considerable intrusion into private life. The supermarket had failed to strike a fair balance between its own rights as the employer, and its employees' rights. Further, for the employer to comply with data protection law, employees must be explicitly, precisely and unambiguously informed of the existence of a personal data file, how the data will be processed, the purpose for collection and the recipients of the data. By installing covert cameras the employer in this case had acted in breach of its data protection obligations.

Perceived disability discrimination claim succeeds

In the case of *Chief Constable of Norfolk v Coffey* the Employment Appeal Tribunal upheld a claim for direct discrimination based on perceived disability. This is the first case to address the issue of perceived disability under the Equality Act 2010.

Mrs Coffey was a serving police officer in Wiltshire. She was diagnosed with a hearing condition in 2011. Her hearing was just short of the police national standard. However, the Wiltshire Constabulary arranged a practical functionality test, which Mrs Coffey passed. Mrs Coffey was therefore able to work as a police constable without any adjustments.

In 2013 Mrs Coffey requested a transfer from Wiltshire to Norfolk Constabulary. As part of he transfer Mrs Coffey was required to undertake a medical assessment, which showed that her hearing loss was at the same level as in 2011. However, Norfolk Constabulary refused the transfer request on the basis that she did not meet the police national standards for hearing.

Mrs Coffey brought a claim against Norfolk Constabulary for direct discrimination. She claimed that Norfolk Constabulary perceived that she had a disability, and that the decision to reject her application was direct discrimination on the basis of that perceived disability.

The ET held that Norfolk Constabulary perceived that Mrs Coffey had a progressive condition within the meaning of the Equality Act 2010. The ET also found that a person with the same abilities as Mrs Coffey, whose condition the employer did not perceive to be likely to deteriorate in the same way, would not have been treated in the same way. Mrs Coffey's claim for direct discrimination based on a perceived disability was therefore successful.

Norfolk Constabulary appealed but EAT upheld the ET's decision and found that the ET had been entitled to hold that the decision to reject Mrs Coffey's application amounted to direct discrimination in relation to a perceived disability.

Employer vicariously liable for employee's data protection breaches

In the case of *Various Claimants v WM Morrisons Supermarkets Plc* the High Court has ruled that an employer can be vicariously liable for data protection breaches by a rogue employee.

A senior IT manager at Morrisons published personal details of almost 100,000 Morrisons' employees online and sent the details to three newspapers. The details included salary and bank account details. The employee held a grudge against Morrisons following a formal verbal warning the previous year and published the information with the deliberate intent of harming his employer. The employee had been given access to the payroll data so that he could pass it on to an external auditor as part of its annual audit. He had taken a copy of the data without the employer's knowledge, and had published the information from his personal computer at his home outside working hours. The employee was convicted under the Data Protection Act 1998 and sentenced to 8 years in prison.

Over 5,000 employees and former employees brought a claim against Morrisons for breach of the Data Protection Act 1998, on the basis that Morrisons was either directly liable or vicariously liable for the data protection breach. The employees also claimed that by allowing the IT manager access to the data and then failing to ensure that he had deleted the data, the employer had failed to comply with the 7th Data Protection Principle ("DPP7") which requires a data controller to have appropriate technical and organisational measures against authorised or

unlawful processing.

The court held that Morrisons was not directly liable for the breach. Morrisons had not directly misused the employees' personal information and did not authorise the breach. The data controller is the person who makes decisions about how and why personal data is processed, Morrisons was not therefore the data controller at the time of the breach. The court also held that Morrisons was not liable under DPP7 as it had adequate and appropriate controls in place. There was also no indication that the employee could not be trusted to do his job, and it would have been impracticable for the employer to actively monitor its employees' internet searches to check for any breaches.

The court found however that Morrisons was vicariously liable for the employee's actions. The employee had received the data as part of his role and had been entrusted with it. There was therefore sufficient connection between the employee's employment and the wrongful conduct to say that the employee's actions were in the course of his employment and that Morrisons were therefore vicariously liable.

This is the first decision which has found that an employer can be vicariously liable for data protection breaches committed by an employee.

WHAT TO LOOK OUT FOR

Gender pay gap reporting deadline

Employers with 250 or more employees have until 4 April 2018 to publish statutory calculations showing how large the pay gap is between their male and female employees.

Six calculations must be published showing the employer's:

- Average gender pay gap as a mean average;
- Average gender pay gap as a median average;
- Average bonus gender pay gap as a mean average;
- Average bonus gender pay gap as a median average;
- Proportion of males receiving a bonus payment and proportion of females receiving a bonus payment; and
- Proportion of males and females when divided into four groups ordered from lowest to highest pay

The employer must also provide a written statement signed by an appropriate senior person which confirms that the calculations are accurate. The statement can include a narrative explaining why a gender pay gap is present and how the employer intends to close it. These calculations will need to be published annually for employers with over 250 employees.

Follow

Follow