Client Alert: European Court of Human Rights Spanish Supermarket Surveillance Privacy Ruling

Date : November 21, 2019

Introduction

In October 2019 the Grand Chamber of the European Court of Human Rights (ECHR) ruled that employees' privacy rights had not been infringed in what has been a somewhat controversial case about the covert video surveillance of Spanish supermarket employees (who were caught stealing on film); we previously wrote about the earlier judgement in this case here: https://www.corderycompliance.com/client-alert-another-european-court-cctv-damages-judgment-2/.

What's the case about?

The case of López Ribalda & Others v. Spain, concerns privacy rights and the use of CCTV/surveillance in the workplace, the salient facts being as follows:

- In 2009, in order to investigate and end irregularities between stock levels and what was being sold, a Spanish supermarket installed both visible and hidden surveillance cameras – the former were to record possible customer theft and the latter were to record possible employee theft. The business gave the supermarket workers prior notice of the installation of the visible cameras but the workers were not informed about the hidden cameras. The surveillance cameras captured employee theft following which five employees were dismissed;
- Cases for unfair dismissal were then brought before the local Employment Tribunal, which then went on appeal to the regional Spanish High Court, which considered that the covert video surveillance was justified (as there had been reasonable suspicion of theft) and the court upheld the dismissal decisions. The case went to the Spanish Constitutional Court and it then ended up before the ECHR where the applicant (ex)workers argued that the covert video surveillance which their employer had put in place in the workplace breached their Article 8 right to respect for private and family life under the European Convention on Human Rights;
- The First Chamber of the European Court of Human Rights ruled in the applicant workers' favour, awarding them (non-pecuniary) damages of 4,000 euros each (although a number of the judges disagreed with this) along with their costs. The First Chamber found that under Spanish data protection legislation the applicants should have been clearly informed about the storage and processing of personal data and that they were under surveillance. The First Chamber also highlighted that the surveillance was not aimed at particular individuals as such and was undertaken over some time with no time limit and during all working hours. The First Chamber ruled that the employer's rights could have been safeguarded by other means and that the applicant workers could have been provided with general information about the surveillance, as required under Spanish data law. The First Chamber also determined that the Spanish courts had failed to strike a fair balance between the applicant workers' rights and the employer's property rights. By way of dissent against this one of the judges upheld the actions of the employer and stated that the ECHR in its ruling was contradicting the legal principle that individuals should not be allowed to profit from their own wrongdoing.

This ruling was viewed in some quarters as being particularly hard on employers, especially given that theft by employees was involved.

What did the Grand Chamber rule?

The Grand Chamber ruled that the Article 8 right to respect for private and family life had not been breached in this case, reasoning as follows (in agreement with Spanish court findings):

- A fair balance has to be struck between an individual's right to respect for privacy and the possibility for an

employer to ensure the protection of its property and the smooth operation of its business, particularly by exercising its disciplinary authority;

- The installation of video-surveillance was justified by legitimate reasons, i.e. suspicion (on account of the significant losses recorded over several months) that thefts had been committed. The employer also had legitimate interests in taking measures in order to discover and punish those responsible for the losses, with the aim of ensuring the protection of its property and the smooth functioning of the business;
- The extent of the monitoring and the degree of intrusion into the workers' privacy was limited as regards the areas and staff being monitored, and its duration had not exceeded what was necessary in order to confirm the suspicions of theft; the monitoring did not cover the whole shop but targeted the areas around the tills, where thefts were likely to have been committed. The workers' duties were performed in a place that was open to the public and involved permanent contact with customers – the expectation of privacy is lower in places that are visible or accessible to colleagues or (as in this case) to the general public;
- Although the duration of the video-surveillance had not been set beforehand it only lasted for ten days and ceased as soon as the workers responsible had been identified – the length of the monitoring was therefore not excessive in itself. Only three individuals had viewed the video-surveillance (including the workers' trade union representative) before the workers had been informed. Therefore, the intrusion into the workers' privacy did not attain a high degree of seriousness.

The court's judgment can be found here: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-197098%22]}

What are the takeaways?

For the sake of clarity, in data protection terms the "simple" use of CCTV/surveillance is not necessarily in itself unlawful– lawfulness is determined by particular legal conditions, and the facts of a given matter also have to be determined in the light of this.

With regard to the EU General Data Protection Regulation (GDPR), employers are entitled to monitor their employees where they have a lawful basis to do this and where the purpose of the monitoring is clearly communicated to employees beforehand. Whilst covert monitoring may be possible this should only be used exceptionally, with appropriate safeguards in place and where there is no less privacy intrusive way of tackling the issue at hand – in such circumstances prior notification can be considered as (exceptionally) exempted.

Under GDPR the use of CCTV/surveillance monitoring to profile employees will likely be considered as high risk to employees' privacy rights. Consequently a Data Protection Impact Assessment will need to be undertaken in order to assess and deal with such risks, which in the case of covert monitoring would need to determine why open monitoring is not adequate along with the conditions for covert monitoring (such as doing so over short periods), and only target a limited number of individuals etc.

Businesses must therefore consider such issues carefully before installing CCTV/surveillance in the workplace. In this regard it is also worth noting that the UK's Information Commissioner's Office has (previously) issued detailed guidance on this topic entitled "In the picture: a data protection code of practice for surveillance cameras and personal information", which can be found here: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

For other articles that we have written about data protection and the European Convention on Human Rights, including the Antovic and Mirkovic case (also about CCTV) please see here http://www.corderycompliance.com/client-alert-european-court-cctv-damages-judgment/), and the Barbelescu case (which was about monitoring employee communications) please see here: http://www.corderycompliance.com/barbelescu-judgment-monitoring-employee-communications-data-protection/).

For more of our reporting about data protection issues see here https://www.corderycompliance.com/category/data-protection-privacy/

For more information on GDPR see details of Cordery GDPR Navigator here www.bit.ly/gdprnav

Generally-speaking, data breaches are a major compliance pain point – Cordery's Breach Navigator can help organisations respond to a breach and assess its consequences. There are more details here https://www.corderycompliance.com/solutions/breach-navigator/.

For more information please contact André Bywater or Jonathan Armstrong who are lawyers with Cordery in London where their focus is on compliance issues.

Image courtesy of gov.uk website

Jonathan Armstrong
Cordery
Lexis House
30 Farringdon Street
London EC4A 4HHOffice: +44 (0)20 7075 1784
jonathan.armstrong@corderycompliance.com

Andre Bywater
Cordery
Lexis House
30 Farringdon Street
London EC4A 4HHOffice: +44 (0)20 7075 1785
andre.bywater@corderycompliance.com