

Client Alert: Another European Court CCTV damages judgment

Date : February 12, 2018

Yet another recent European Court of Human Rights judgment, the case of *López Ribalda & Others v. Spain* (which can be found here: <http://www.bailii.org/eu/cases/ECHR/2018/14.html>), has highlighted the issue of the use of CCTV in the workplace.

The very basic facts of the case were as follows:

- In 2009 a Spanish supermarket noticed irregularities between its stock levels and what was being sold daily. In order to investigate and end the irregularities the business 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 neither they nor the business' staff committee were informed about the *hidden* cameras;
- Consequently a number of workers suspected of theft were called to individual meetings with the business, and, the applicants in the case before the European Court of Human Rights admitted their involvement in the thefts (in the presence of the union representative and the business' legal representative), following which they were dismissed from their employment, based on the *covert* video surveillance and also witness statements;
- The applicants then brought cases for unfair dismissal before the local Employment Tribunal arguing that the use of surveillance had breached their right to protection of their privacy – the tribunal upheld the dismissals and ruled that the use of *covert* video surveillance in the workplace without prior notice complied with Spanish law;
- The case then went on appeal to the regional Spanish High Court, which considered that the “*covert* video surveillance had been justified (in that there had been reasonable suspicions of theft), appropriate to the legitimate aim pursued, necessary and appropriate”, and the court upheld the dismissal decisions;
- After being declared inadmissible by the Spanish Constitutional Court the case ended up before the European Court of Human Rights where the applicants argued that the *covert* video surveillance that 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 Convention); claims were also brought concerning Article 6(1) of the Convention about their right to a fair hearing with regard to use of the video material before the Spanish courts, but this aspect is not addressed in this article (which were in any event dismissed by the court).

The European Court of Human Rights ruled in the applicants' 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 court 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, which had not been the case; the court 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 court ruled that the employer's rights could have been safeguarded by other means and that the applicants could have been provided with general information about the surveillance, as per Spanish data protection legislation. The court also determined that the Spanish courts had failed to strike a fair balance between the applicants' rights and the employer's property rights.

One of the judges gave an interesting dissenting ruling stating that the actions of the employer business and the Spanish courts was neither abusive, arbitrary or disproportionate and that the court in its ruling was contradicting the legal principle that the applicants should not be allowed to profit from their own wrongdoing, citing a nineteenth-century US court ruling.

This ruling may therefore seem hard on employers, especially as theft by employees was involved. But, for the sake of clarity, the use of CCTV is not necessarily in itself unlawful in data protection terms – lawfulness is determined by particular legal conditions, and the facts of a given matter also have to be determined in the light of this. Under 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. Covert monitoring should be only used exceptionally. Under GDPR the use of CCTV 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 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>

Looking to the future, Article 82(1) of GDPR states that individuals who have suffered "material or non-material damage as a result of an infringement of [GDPR] shall have the right to receive compensation from the controller or processor for the damage suffered" – we can expect that those who bring future compensation claims in connection with allegations about unlawful CCTV surveillance in the workplace will do so on this basis.

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 other articles that we have written about data protection compliance please see here: <http://www.corderycompliance.com/category/data-protection-privacy/> Our FAQs and video on the EU General Data Protection Regulation (GDPR) can be found here www.bit.ly/gdprfaq.

Cordery also has a GDPR Navigator subscription service which includes short films, straightforward guidance, checklists and regular conference calls to help you comply. More details about this can be found here: www.bit.ly/gdprnav.

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

[Jonathan Armstrong](#), Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com



[André Bywater](#), Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com



Farringdon