SUMMARY

2016/32 Window sticker sufficient to allow evidence collected by surveillance camera (SP)

<p>A decision issued by the Constitutional Court on 3 March 2016 upholds a High Court decision on whether evidence obtained through video surveillance at the work place without previously informing the employee or the works council of the recording infringes employees' privacy. The existence of cameras in the workplace was only made known via a sticker on the shop window, but the Constitutional Court found that it provided sufficient information to employees. The Court found that, as there was a prior suspicion of theft by the employee, temporary recording of the cashier area was lawful and did not require prior consent. The judgment sets out the criteria to be used to determine a fair balance between the competing interests of employee privacy and the employer's right to compliance.</p>

Summary

A decision issued by the Constitutional Court on 3 March 2016 upholds a High Court decision on whether evidence obtained through video surveillance at the work place without previously informing the employee or the works council of the recording infringes employees' privacy. The existence of cameras in the workplace was only made known via a sticker on the shop window, but the Constitutional Court found that it provided sufficient information to employees. The Court found that, as there was a prior suspicion of theft by the employee, temporary recording of the cashier area was lawful and did not require prior consent. The judgment sets out the criteria to be used to determine a fair balance between the competing

interests of employee privacy and the employer's right to compliance.

Facts

The owner of a 'Bershka' clothes store (the 'company') had a reasonable suspicion that the plaintiff in this case, one of its sales staff (the 'employee') was withdrawing funds from cash registers. The company retained a security service provider to place cameras in the workplace to record the cash register area. No prior notice or warning was given to employees or to the works council about the recording. A sticker was placed on the store window with a symbol to indicate that the store had cameras. After a week, the employer had recordings of the employee's misappropriation and her employment was terminated.

The employee sued the employer claiming reinstatement. She based her claim on infringement of her privacy rights. The first and second instance courts held the termination to be lawful. The plaintiff applied to the Constitutional Court.

Judgment

The Constitutional Court upheld the lower courts' decision. It held that in this case, placing cameras in the workplace and using their recordings for disciplinary purposes was lawful, even though the company had not specifically informed its employees or (the relevant committee of) the works council that cameras were being installed to record the workplace. The court declared that there had been no infringement of fundamental rights because the recordings were adequate, reasonable and proportionate to enable the company to monitor employee compliance. The court reasoned as follows:

-
the company had a real need to install cameras, because it was necessary to identify the employee who was withdrawing funds from the cash register and the cameras were not installed until after the suspicion of misconduct had arisen;

-

The measure was proportionate, because the cameras were only placed during the limited time necessary to identify the offender;

-
the measure was appropriate, because this was the only way to find out who the offender was.

The court declared that consent to install the cameras was not necessary because the measure met the exception provided for under the Spanish Data Protection Act to the effect that no consent is required for data collection justified in connection with a contractual relationship (the employment relationship) and conducted for this purpose.

There were two dissenting votes to the Court decision. The first objection, by Judge Fernando Valdés (with which Judges Adela Asua and Juan Antonio Xiol agreed), was that a fundamental right such as the protection of personal data cannot be trumped by a non-fundamental one, such as the employer's right to monitor employees' compliance and thus the former should prevail. The second objection, raised by Judge Juan Antonio Xiol, was that by merely putting a general sticker on the store window, the company had not provided the employee with the appropriate information about the camera surveillance.

Commentary

Images of a person collected by means of CCTV constitute 'personal data' within the meaning of Directive 95/46

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Article 8, Charter of Fundamental Rights of the European Union (2010/C 83/02), Protection of personal data:

- Everyone has the right to the protection of personal data concerning him or her.

- Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

- Compliance with these rules shall be subject to control by an independent authority.

Advocate General Opinion on Schrems vs Data Protection Commissioner (C-362/14).

For many years, the case law of the Constitutional Court offered broad protection to employees' right to privacy at work. For example, in a 2013 decision

CC 29/2013 of 11 February, BOE no. A-2013-2712, 12 March 2013.

The Constitutional Court changes its interpretation in this new ruling by holding that no consent is required for employer data processing (CCTV recording) insofar as this is required to manage the contractual relationship between the parties and for performance of the employment contract, since this falls into the exception provided for in the Spanish Data Protection Act implementing Article 7b of the Directive. According to the Constitutional Court, CCTV recordings fall into this exception because they are a necessary tool to enable the employer to monitor employee compliance. The court further declares that by agreeing to the employment relationship, the employee is implicitly consenting to a privacy limitation.

The Constitutional Court's view was that the sign on the store window was sufficient to inform the employee of the fact that there were cameras recording in the store. The court took the view that there was no need for the employer to further explain that the cameras would not only be used to avoid theft by customers in the store (as could have been inferred), but also for disciplinary purposes.

The Court declared that the use of a camera to record the workplace was lawful for the following reasons:

- it was a justified measure, since it was not used to infringe employees' privacy as such but with the specific purpose of identifying who was removing funds from the till based on a prior reasonable suspicion of misconduct;

- it was appropriate for that specific purpose;

- it was necessary, because recordings were the only way to provide evidence of the infringements; and

- it was proportionate, because there was only one camera, it was directed specifically at the cash register and the recordings were made over a limited term only.

This case seems to follow a current trend, which is to limit employee privacy rights or, at least, delineate them. Indeed, the ECtHR has in the past held that employees have a reasonable

expectation of privacy unless they have been clearly warned previously that communications might be monitored.

However, in the recent ECtHR Barbulescu decision

ECHR 12 January 2016 re Barbulescu – v – Romania.

Unlike most relevant cases from the past (e.g. Halford in 1997 and Copland in 2007) where the employer had tolerated or even authorised the private use of communications, in the Barbulescu case, the company had expressly forbidden the private use of communications. Therefore, there was no prior expectation of privacy. The court further concluded that the employer's monitoring was limited in scope and proportionate. The claim was therefore dismissed.

The Barbulescu decision had a dissenting opinion by Judge Pinto de Alburquerque, who stated that the employer interfered with the employee's privacy and went far beyond what was necessary, including accessing private messages by the employee which had sexual content and accessing his personal Yahoo account. Judge Alburquerque reminded the court of the following quotation: "Workers do not abandon their right to privacy and data protection every morning at the doors of the workplace."

Article 29 Working Party Working document on surveillance and monitoring of electronic communications in the workplace, page 4.

Following ECtHR case law, the Spanish Court has drawn the boundaries of employees' privacy rights by holding that no prior consent – or even specific information – is required to monitor employees' privacy. General information about the recording is sufficient. The decision declares that such monitoring is lawful insofar as it is required to manage the employment relationship and compliance and is subject to the principles of need, justification, appropriateness and proportionality. This includes a prior reasonable suspicion of misconduct and limitation to the interference in employees' privacy to the time strictly necessary for the purpose.

Comments from other jurisdictions

Austria (Erika Kovács, University of Vienna): In a similar case in Austria, it would be possible to install a camera to monitor a salesperson to prevent him from stealing. However, as this would involve the privacy of the worker, before installation of the camera the employer would need to ask the works council for its permission. If there was no works council at the workplace, the employer would need to obtain the written permission of the affected worker

himself. Monitoring without the prior permission of the works council or the worker is invalid and the employer can be sued for failure to obtain it.

However, the catch is that there is currently no prohibition against using evidence obtained without permission in court. Indeed, in Austria there have been no similar cases, in which the court has decided to treat the evidence as inadmissible because the consent was missing.

Sections 50a-50e of the Data Protection Act 2000 regulate monitoring by cameras. They provide that video surveillance for the purpose of the general control of workers is not permitted. However, the protection of a subject to monitoring and the safeguarding of evidence can be legal aims of monitoring. This can enable employers to install a monitoring system to prevent theft. The principle of proportionality must be observed in such cases.

Finland (Kaj Swanljung and Janne Nurminen, Roschier): According to the Finnish Act on the Protection of Privacy in Working Life, employers are permitted to conduct camera surveillance in the workplace for security and production supervision purposes. Camera surveillance targeting a particular employee is prohibited, unless the employee handles property of high value or potentially encounters violence or other similar threats in the line of duty, or the employee requests the surveillance him- or herself. Employers are required to consult the employee representatives when implementing technical surveillance in order to ensure transparency, regardless of the reason for it. However, even if the employer has not done so, material gathered as a result may still be admissible in court, in line with the principle of free evaluation of evidence.

Croatia (Dina Vlahov Buhin, Schoenherr): Before entering into a comparative analysis of the case at hand, it should be noted that even if it had been determined that the surveillance was unlawful, in Croatia this would not automatically have led the termination being declared unlawful. The notion of unlawfully obtained evidence does not apply in civil proceedings and so surveillance recordings could be used to support the termination. However, the manner in which the surveillance is conducted may trigger liability on the part of the employer if it has breached employees' privacy or infringed safety at work provisions.

In Croatia, the case at hand would have mainly been assessed in accordance with the provisions of three statutes: the Personal Data Protection Act, the Labour Act and the Safety at Work Act.

According to the Personal Data Protection Act, surveillance recordings are defined as personal data and the person subject to surveillance must be made aware of it and its purpose. Both the Labour Act and the Safety at Work Act stipulate that the employee must be notified prior to the surveillance, both by setting this out in the work regulations and by personally notifying

the employee either while applying for the job or before the surveillance starts. In addition, the three Acts provide for additional works council consultation and consent obligations, though these differ depending on the Act. As there is no recent case law, at the moment it is not clear which act should be applied. The answer depends on whether the provisions of the Safety at Work Act apply only to surveillance aimed at ensuring safety at work or apply to any video surveillance regardless of its purpose. If the latter, this would mean that the provisions in the Labour Act should be excluded.

Before the Safety at Work Act of 2014 entered into force there were no provisions explicitly regulating the usage of surveillance devices in employment relationships and the available court decisions had been reached based on the general provisions relating to data protection contained in the Personal Data Protection Act and the Labour Act. In one decision, the court declared the installation of cameras in a production hall unlawful as it determined that this represented a significant decision in terms of employee's rights, which generally require prior consultation with the works council (County Court in Zagreb, Gžr-389/07-2). Although the cameras had been essentially installed to monitor employees' efficiency and not for security reasons, the question of the appropriateness of the surveillance was unfortunately not analysed. This was because there was no consultation with the works council and therefore the surveillance was declared unlawful.

However, with the new Safety at Work Act, a provision explicitly regulating the use of surveillance devices as a means of securing safety at work was introduced. According to this, the employer is entitled to use surveillance devices only in order to control entry and exit from the workplace and to reduce the exposure of employees to the risk of robbery, theft and other crime. If the devices record all the movements of employees throughout their working time, the employer must obtain the consent of the works council prior to installation.

The requirement laid down by the Safety at Work Act is stricter than that laid down by the above case law, as in that case the employer had to obtain the explicit consent of the works council, whereas previously, consultation alone was sufficient, with no obligation on the employer to abide by any works council decision.

With this in mind, it is necessary to determine whether the purpose of the Safety at Work Act is to prohibit all types of surveillance, including those not aimed at ensuring safety at work or whether its scope should be limited to safety surveillance, in which case, other types of surveillance, such as monitoring of employees' conduct would fall under the general provisions of the Labour Act and Personal Data Protection Act. Unfortunately the answer has not yet been given and we are impatiently waiting how the issue will be resolved.

In Croatia, based on the way in which the surveillance in the case at hand was conducted, it would most probably have been declared unlawful, regardless of which Act applied, as neither the employee nor the works council were notified or consulted about the planned surveillance. However, in our view, a decision of this kind would be most welcome in Croatia, as the law does not provide for unusual situations in which it is important for the employer to react promptly and secretly to detect and prevent misconduct by the employee, especially where there is reasonable doubt.

This is especially valid in the context of termination proceedings, which are burdensome for the employer in terms of being able to show sufficient evidence. A visual record of the employee's misconduct in such cases would facilitate this. However, there also need to be sufficient safeguards to ensure surveillance is conducted as rarely as possible and that there is sufficient evidence of how it is conducted to enable verification of the fairness of the process.

Subject: data processing

Parties: Monica Rebeca Liberato Rodríguez – v – Spain

Court: Tribunal Constitucional (Constitutional Court)

Date: 3 March 2016

Case number: 39/2016

Publication: http://hj.tribunalconstitucional.es/HJ/nl/Resolucion/Show/24843

Creator: Tribunal Constitucional (Constitutional Court)
Verdict at: 2016-03-03
Case number: 39/2016