SUMMARY

2010/70: Illegal monitoring of employees makes collected evidence of computer abuse inadmissible in dismissal proceedings (IT)

<p>An employee was discovered having repeatedly accessed the Internet during working time and was dismissed on the grounds that such computer use was in breach of the company’s regulations. The employer had found out about the transgression with the aid of ‘Superscout’ software. This made the discovery illegal. Hence the evidence of the transgression was inadmissible and the dismissal was ineffective.</p>

Summary

An employee was discovered having repeatedly accessed the Internet during working time and was dismissed on the grounds that such computer use was in breach of the company's regulations. The employer had found out about the transgression with the aid of 'Superscout' software. This made the discovery illegal. Hence the evidence of the transgression was inadmissible and the dismissal was ineffective.

Facts

The employee in this case was dismissed following an internal disciplinary procedure, which had been initiated after it had been established that she had repeatedly accessed the Internet for private purposes on her computer while at work, which the company's regulations prohibited. The employer had found this out with the aid of 'Superscout' software, which enables employers – *inter alia* – to monitor their staff's computer behaviour. An Italian law dating back to 1970 (Section 4 of the *Statuto dei lavoratori*) outlaws the use of any device

designed to monitor employees' activities 'remotely'. The essence of 'remote' monitoring is that the employee does not know he is being monitored and that, as a rule, the results of the monitoring are not known until afterwards. It also outlaws devices that, although not designed to do this, can be used for that purpose, unless the devices have been approved either by the relevant trade unions or by the local Employment Inspectorate.

The employee challenged her dismissal in court. Both the court of first instance and the appellate court held the dismissal to be ineffective, for a combination of two reasons: (1) as it was illegal for the employer to use the Superscout software, the evidence of computer abuse had been collected unlawfully and was therefore inadmissible and (2) the employer had failed to comply with the principles of proportionality and 'graduated response', which hold that a disciplinary sanction must be proportionate to the transgression and must, where appropriate, be preceded by a lesser sanction. The employer appealed both to the Court of Appeal (who rejected the Appeal) and to the Supreme Court.[1]

As the principles of proportionality and graduated response are based on domestic Italian law, this case report will deal only with the evidentiary aspects of the case.

Judgment

The Supreme Court upheld the appellate court's judgment. It ruled, inter alia, that even if the employee knew that accessing the Internet during work was not permitted, and even if she knew that her employer might monitor her computer use, the employer was still not permitted to use the Superscout program.

Commentary

The novelty of this judgment is that the Supreme Court is partially departing from previous doctrine. Up until this judgment it had held that 'remote' monitoring of employee behaviour was excluded from the scope of said Section 4 if the purpose of the monitoring was to prevent illegal activities. In this case, however, the Supreme Court had unequivocally outlawed computer monitoring, even if the employee has been warned by an internal regulation not to access the Internet for private use and that computer use might be monitored. The Supreme Court held that, since the employer's purpose in doing the remote monitoring was simply to check compliance with company rules, this should be considered as illegal monitoring – which is inadmissible, and cannot be used as the basis for disciplinary action.

Comments from other jurisdictions

France (Claire Toumieux and Aude Pellegrin): In France, unlike Italy, surveillance and

monitoring of employees in their place of work and during their working time, as well as the option to sanction reprehensible behaviour, is a prerogative of the employer.

The monitoring of employees may be done provided, notably, that the employer informs the works council and the employees of the means and techniques used to monitor their activities prior to their implementation and that the means of control put in place by the employer do not place disproportionate restrictions on the rights and freedoms of the employees.

It is only if the employer does not comply with such conditions that he may be prevented from using the evidence gathered to justify the dismissal of an employee.

Germany (Dr. Gerald Peter Müller): The protection of employees' personal data has very recently been an issue of broad discussion in Germany. Currently the German Act on the Protection of Personal Data ("*Bundesdatenschutzgesetz*") is being reformed and tightened up in this respect following a number of recent scandals in well-known companies.

The question of the admissibility of evidence obtained illegally has also been broadly discussed in German judicial literature. The basic dilemma is that two legitimate interests clash in the event information has been found, while it is clear that the way in which it was obtained breached the law in general or in terms of legitimate personal interests. The German civil law courts, along with the labour courts in Germany, have held that to admit evidence that has come into being illegally is alien to the German civil law system. There are, however, exceptions to this. Developing from the legal principle that an individual has the 'right to informational self-determination' (as made clear by the German Constitutional Court), an individual has the constitutional right to decide about the disclosure and use of his or her personal data. A distinction must be made between those cases where evidence was obtained in a way that seriously violated that right and those cases where there was no such violation.

Returning to the question of the admissibility of illegal evidence in court, it can be said that the public interest in ascertaining the truth clashes with the individual's right to informational self-determination. With respect to the use of collected computer data, the following case-law has evolved.

The scope of permissible monitoring of the use of an employee's computer system is split into two categories. The first being cases where private use of the computer equipment is generally permitted and the second, where such private use is specifically prohibited by the employer. Within the first group, the employer is subject to the rules for providers of telecommunication installations and is thus generally barred from examining the content accessed by employees on the employer's computer system. In such cases, the employer would not be allowed to

monitor, for example, the amount of time that an employee has spent on the private use of the internet or control the pages that the employee has visited. The second category is where any private use of the employer's computer installations has been prohibited. Under these circumstances, any use of the computer is deemed to be a professional one and since the employer generally has the right to access any professional files (i.e. especially paper files) there is no reason to bar it from viewing the computer files. This being said, systematic or continuous monitoring is still not permitted. Violations of these rules will lead to the inadmissibility of the evidence in court.

An additional 'pitfall' is added where the employer's establishment is subject to the rules of co-determination of the works council. Basically the introduction of (electronic or technical) measures to monitor employees' conduct is subject to the works council's right of co-determination. While the question of whether monitoring measures taken by the employer which have not been approved by the works council are automatically inadmissible in court was controversial for a long time, the federal employment court (*Bundesarbeitsgericht*) ruled in 2007 that where unapproved measures are taken by the employer in the face of the works council's right to co-determination, this will not in itself lead to the inadmissibility of the evidence in court. For the evidence to be ruled inadmissible, the violation must impact on the works council's ability to protect the employee's right to informational self-determination.

The Netherlands (Peter Vas Nunes): I find two aspects of this case noteworthy. The first relates to the Italian prohibition on monitoring employee behaviour. The second has to do with inadmissibility of illegally collected evidence.

If a Dutch court had been called upon to adjudicate the case reported above, it would most likely have based its decision on a combination of Article 8 of the European Convention on Human Rights (ECHR), which provides that 'Everyone has the right to respect for his private life, his home and his correspondence', and the Data Protection Act, which is the Dutch transposition of Directive 95/46/EC. Article 8 ECHR has been invoked frequently, both before Dutch courts and before the European Court of Human Rights (ECtHR), in situations where an employer monitored computer use. Notable is the ECtHR's judgment in the Copland case (3 April 2007, case No 62617/00) in which the court held that 'the collection and storage of personal information relating to [an employee's] [É] internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8'. The employee in the Copland case had been given no warning that her internet usage would be liable to monitoring, therefore she had a 'reasonable

expectation as to the privacy' of the usage. Had Ms Copland been warned that her internet usage would be monitored, she would not have had a reasonable expectation of privacy and the monitoring would not have violated Article 8 ECHR. This is also the Dutch courts' position. However, the Data Protection Act goes further to protect employees' privacy than does Article 8 ECHR. Based on this Act, Dutch courts tend to find that, although employers may take reasonable steps to prevent private internet usage during work, they may not be informed (by their IT departments) which sites the employee has accessed. Also, any corporate policy in this field must be vetted by the works council in advance.

My second observation of this is that the Italian Supreme Court seems to rule out unconditionally all evidence gathered illegally. The Dutch courts have so far been reluctant to adopt such a strict 'exclusionary rule'. It is generally held that an employer who has illegally gathered evidence of wrongdoing by one of its employees may be liable (criminally, administratively and civilly) for this breach of the law, but that a dismissal based on such evidence is not invalidated by this fact in itself. Not all courts take this view, however, and it would not surprise me if the Supreme Court took a stricter stance. In its well-known *Wennekes* case (2001) it allowed evidence gathered by means of a concealed video camera in a shop, that had been installed without the staff's knowledge and therefore illegally. The Supreme Court did not find it necessary to exclude this evidence because (1) the employer in question – the shop-owner – had a concrete suspicion that one of his employees was stealing money out of the till, (ii) there was no other means of discovering who the thief was and (iii) the camera was directed exclusively at the cash register. Had not all of these conditions been fulfilled, the Supreme Court might well have ruled the other way.

United Kingdom (Richard Lister): UK law ostensibly allows significant scope for employers to monitor employees' use of their computer systems, for various purposes, under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Notwithstanding this, it is becoming increasingly common for employees to use Article 8 of the ECHR and/or UK data protection legislation to challenge employer surveillance practices.

For example, cases have established that human rights law – including Article 8 – is relevant to the 'reasonableness' of a dismissal. Where surveillance has been used during disciplinary proceedings, an employee can argue that this renders the dismissal procedurally unfair or that a tribunal must disregard the evidence.

However, the courts appear to be taking a narrow view of when privacy rights will apply and when employer justifications will be challenged. In *McGowan – v – Scottish Water* [2005] IRLR 167, for example, the Employment Appeal Tribunal did accept that covert surveillance of an

employee's home to investigate falsification of timesheets raised a 'strong presumption' that the right to respect for private life was being infringed. But the EAT went on to find that this was justified because the employer was trying to protect its assets, had considered alternatives and the evidence went to the heart of the investigation.

The Data Protection Act 1998 (DPA) is the other main piece of UK legislation which regulates surveillance practices. Related to this is the *Employment Practices Code* published by the Information Commissioner – the UK's privacy watchdog – which places various limits on employers' monitoring powers. With regard to electronic communications and video/audio monitoring, the Code emphasises the need to have a clear policy, warn employees in advance and target the monitoring carefully. Covert monitoring is particularly difficult to justify, with the Code stating it should only be used where there are grounds for suspecting 'criminal activity or equivalent malpractice'.

Footnote

1 Following the court of first instance's judgment, the employer dismissed the employee again, for the same computer abuse, this time not based on evidence collected through the Superscout software but based on the server logs. This second termination was also declared invalid both by the court of first instance and the appellate court. The judgments on both terminations were appealed to the Supreme Court. The second dismissal has been left out of this report.

Subject: Privacy

Parties: Anonymous

Court: Supreme Court (*Corte di cassatione*)

Date: 23 February 2010

Case number: 4375

Internet publication: www.eelc-online.com

Creator: Corte di cassatione (Italian Supreme Court)
Verdict at: 2010-02-23

EELA EUROPEAN EMPLOYMENT LAWYERS ASSOCIATION

Case number: 4375