2018/5

Evidence from long-term keylogger surveillance cannot be used in a dismissal lawsuit (GE)

CONTRIBUTOR Paul Schreiner*

Summary

The German federal court for labour law matters, the *Bundesarbeitsgericht* (the 'BAG'), has held that evidence cannot be used in a dismissal lawsuit if the employer has obtained it from long-term surveillance using keylogger-software. Employers must not keep their employees under constant surveillance and must therefore expect their legal position to be weak if they try to dismiss an employee based on findings from such monitoring. The court ruling preceded the ECtHR *Barbulescu* ruling of 5 September 2017 (featured in EELC 2017/4) in a similar case.

Facts

The plaintiff was a web developer employed at a German IT firm, which was the defendant in this case.

The defendant did not allow private use of its IT systems. In particular, the private use of the internet was not allowed. In April 2015, the defendant informed its employees by email, that it would log and save all internet traffic. The defendant asked the employees to object if they disagreed with this measure. No employee objected.

The defendant installed so-called 'keylogger' software onto the plaintiff's workplace computer. This recorded every time the employee touched the keyboard and created desktop-screenshots on a regular basis. As a result, the defendant found out that the plaintiff very often used the internet for private reasons: he programmed and played a sci-fi computer game and dealt with email correspondence for his father's firm. The plaintiff admitted that he used the internet for some private matters, but only to a limited extent, and not enough to justify dismissal. He claimed that he had spent a maximum of three hours on the game over several months, and that he had spent a maximum of 10 minutes a day on emails for his father's firm – and in each case, only during breaks and other times that he was not required to work. However, the defendant had obtained proof through the keylogger data that the plaintiff had used the internet privately much more than he said.

The defendant dismissed the plaintiff. The plaintiff took legal action against the dismissal and won in all instances, including at the BAG.

Judgment

The BAG held that long-term surveillance via keylogger software violated German data protection law, and that the employer could not use the information derived from this surveillance as evidence in court. Therefore, the defendant could not substantiate the reasons for the termination. As a result, the termination was declared invalid and the plaintiff was reinstated. The BAG founded its judgment on the following reasons.

It is established case law in Germany that evidence cannot be used in court if it violates a party's privacy rights. This fundamental right follows (implicitly) from the German Constitution and this has, essentially, the same content as Article 8(1) ECHR (on the right to privacy and family life).

The BAG repeated its established case law that German data protection law (*Bundesdatenschutzgesetz*[1], the 'BDSG') sets out the details of the fundamental right to privacy and hence applies to the question of whether evidence can be used in court – even though there are no explicit rules on court evidence in the BDSG.

The BDSG prohibits the collection of personal data unless there is a legal justification. Consequently, the BAG dealt with possible justifications. First, the BAG looked at the first ground of justification: that the affected person gave his or her consent, and held that the

* Paul Schreiner is an attorney at law at Luther Rechtsanwaltsgesellschaft mbH.

1. Germany was one of the first countries to have a data protection law. It has existed since 1978 and is relatively strict by international standards.

doi: 10.5553/EELC/187791072018003001006

defendant did not obtain the plaintiff's consent. Although the defendant had informed its employees about the surveillance, it had not said that every key they used would be logged and saved and it had in fact downplayed the extent of the surveillance it would use. The BAG noted that the absence of any objection does not count as consent. Last, the BAG hinted that the surveillance measures taken in this case would not have been allowed even with the employee's consent.

Secondly, the BAG dealt with the legal justifications for data use in employment situations. The BDSG stipulates that collecting personal data about employees is only allowed if, either it is *necessary* for the employment relationship, or there is a documented suspicion that the employee has committed a crime whilst employed. As there was no suspicion of a crime, the only question was whether the surveillance measures were *necessary*.

The BDSG does not explicitly contain an explanation of this term, so the court interpreted it in the light of the underlying basic principles: i.e. the general right of privacy versus the interests of the employer. The BAG concluded that, in the case at hand, the plaintiff's right to privacy outweighed his employer's interests. Surveillance using keylogger software was not a slight, but severe interference with the plaintiff's rights, comparable to constant video surveillance. The BAG held that such significant surveillance measures could only be justified as in the interests of the employer if there was hard evidence to suggest the employee was in serious breach of his contractual obligations, which was not the case in this case. Ultimately, the BAG held that the defendant could not use the keylogger evidence in court.

The BAG emphasized that surveillance measures are not prohibited in every case. Whether they are permissible might depend on how draconian they are. For example, there is a difference between just saving the browser history and accessing the content of the employee's internet use. The BAG was of the view that even if there was no prior documented suspicion, the rights of employees would not be infringed if only the browser history were monitored.

Commentary

There are two important aspects to the BAG's judgment:

1. Strict surveillance measures without evidence to support a suspicion are unlawful and evidence obtained from such measures is inadmissible in court.
2. Lesser surveillance measures, such as saving browser history without actual site-content can be justifiable based on the interests of the employer.

Relation to changes in data protection law

There are major changes to come in European data protection law as a result of the EU General Data Protection Regulation, which will enter into force on 25 May 2018. While these changes will also be reflected in amendments to the BDSG (including transferring provisions relevant to this case report to other articles), the law itself on this case will remain the same.

Relation to the ECtHR ruling in Barbulescu

Two months after the BAG, the ECTHR took a decision in a similar case. A Romanian employer monitored and saved the entire communications of an employee and dismissed him for private use of a messenger program, forbidden by the employer. The employee went through all the courts and finally won at the ECtHR. The court held that the surveillance had been unlawful and that the employer could not use the evidence obtained by it in court. The main reason was that the employer had not informed the employee about the measures it was taking.

Although the legal assessment in the two judgments differs a bit, they do not contradict each other, but should be seen as two factors that need to be in place to ensure the lawfulness of a surveillance measure. The employer must tell the employee about the measures to be taken and must be able to demonstrate that there is a reason for taking them (at least from a German point of view). In future, both of those factors will need to be considered by employers. The BAG's decision remains valid, but the ECtHR's judgment will ensure that there is an additional focus on the need to inform employees about planned monitoring.

Both judgments are clear on one thing: there is a major difference between continuously monitoring the flow of communication/internet use and accessing the content.

In practice, the combination of both judgments results in the following guidelines:

1. The possibility, extent and reasons for any surveillance measures should be addressed specifically in the employment contract and/or in a collective agreement.
2. If there is no criminal suspicion, only the flow of communication or the browser history should be monitored – not the actual content, as this is unnecessary and violates employee privacy.
3. Evidence should be obtained either based on random checks or as result of a specific, documented suspicion. Constant surveillance without either of these is unlawful and will mean the evidence obtained is inadmissible, at least in Germany.

doi: 10.5553/EELC/187791072018003001006

Comments from other jurisdictions

Austria (Birgit Vogt-Majarek, Kunz Schima Wallentin Rechtsanwälte): Based on the facts of the case and taking into account Austrian legislation and jurisprudence, the Austrian Supreme Court would probably decide as follows:

The BAG ruled that the collecting of personal data of employees was not allowed in the case at hand as there were no documented reasons to assume the employee violated his contractual obligations in a considerable way (and no suspicion of crime either). The ECtHR ruled that the employee has to know beforehand about data controlling measures to be taken.

In Austria, it is undisputed that the introduction of control measures and technical systems for the control of employees – insofar as these measures (systems) affect human dignity- is subject to the necessary co-determination of the works council by means of an appropriate works agreement ("Betriebsvereinbarung"). If there is no works council, the aforementioned control measures can be established in accordance with § 10 AVRAG provided that the consent of each individual employee has been given. Measures that violate human dignity are inadmissible and cannot be permitted to the employer neither by the competent works council nor by the individual employee.

In the cases underlying the current decisions of the BAG and the ECtHR, according to the information available, neither the introduction of the "Keylogger" program (BAG decision) nor the monitoring and saving of the whole communication (ECtHR decision) by the employer were based on a works agreement nor operated with the consent of the individual employee. Hence, the introduction of the systems would have been inadmissible according to Austrian law as well since both of the aforementioned measures at least affect human dignity. The works council or the affected employee(s) would be entitled to an injunctive relief as well as to claims for damages.

In the BAG decision the court stated that evidence which has been obtained in the aforementioned illegal way is excluded from the court proceeding.

Different from Germany there is no explicit provision in the Austrian Civil Procedure Code (ZPO) that generally prohibits the exploitation of unlawfully obtained evidence.[2] Hence, an infringement of the "ban on taking evidence" generally remains unpunished insofar as even a "forbidden" taking of evidence does not fulfil the elements of essential procedural deficiency nor for procedural deficiency nor for nullity; therefore there is no specific right of appeal.[3]

According to parts of the Austrian doctrine[4] the exclusion of evidence unlawfully obtained is supported if it violates the core area of fundamental rights and freedoms of the person affected (like e.g. the torture convention, which is not relevant in the aforementioned cases). The predominant doctrine argues that a ban on the exploitation of evidence would require the judge to omit essential results of evidence and would therefore lead to an incorrect judgement[5]; exceptions are only supported in cases in which the evidence is the result of intolerable investigative measures.[6]

According to a decision of the Austrian Supreme Court (OGH 19.10.1999 GZ 4 Ob 247/99y) an unlawfully obtained tape recording may be used in exceptional cases (here: in case of obstacles to proof of evidence) and only after appropriate consideration of interests of the parties.[7]

To sum up, based on the facts in the case report, the Austrian Supreme Court would most probably decide that there is no general prohibition of the exploitation of unlawfully obtained evidence. As and insofar as the evidence in the cases underlying the decisions of the BAG and the ECtHR have not been obtained in breach of core areas of fundamental rights, even though the introduction of the controlling systems would be unlawful according to Austrian Law, the evidence unlawfully gathered could still be lawfully used and exploited in court.

Italy (Caterina Rucci, Fieldfisher): Under Italian law this scouting programme would have been equally considered as illegal. Italy, in fact, had a provision against remote control already in 1970, and this was an even criminally sanctioned provision.

More recently, some devices linked to work instruments, have been declared as admissible, and the data collected thought such devices can be used for "any employment purpose", although an explicit reference is made by the new law also to Italian Data Protection law, and therefore this will further change once GPDR will be fully applicable.

What is quite interesting is that there is an almost equal Italian case, where a similar system, called "Super Scout" was declared unlawful in 2005 by the Court of Appeal of Milan, which confirmed the 1st instance Tribunal decision, and established that the data collected

2. cf Graf/ Schöberl, ZAS 2004/30,172.
3. cf G. Kodek, ÖJZ 2001,345; OGH 20.11.1997,2 Ob 272/97g; Rechberger in Fasching/Konecny[2] Vor § 266 ZPO para 70 (status 30.04.2004, rdb. at).
4. cf Fasching, *Zivilprozessrecht*[2] para 936.
5. cf Rechberger in Rechberger, ZPO, para 24 Vor § 266; G. Kodek, *Rechtswidrig erlangte Beweismittel im Zivilprozeß*, 136 ff.
6. cf Rechberger in Rechberger, ZPO para 24 Vor § 266.
7. See G. Kodek, *Die Verwertung rechtswidriger Tonbandaufnahmen und Abhörergebnisse im Zivilverfahren*, ÖJZ 2001,334, who supports the subsidiarity of illegally obtained evidence.

doi: 10.5553/EELC/187791072018003001006

by such device could therefore not be used in in order to justify a termination.

The situation might be different now, after the changes introduced by the Jobs Act, but still an instrument enabling a continuous remote control on the websites visited by employees, would not be allowed.

Subject: Unfair dismissal, right to privacy

Parties: unknown

Court: *Bundesarbeitsgericht* (Federal Labour Court of Germany)

Date: 27 July 2017

Case number: 2 AZR 681/16

Hard copy publication: NJW 2017, pg. 3258

Internet publication: http://www.bag-urteil.com/27-07-2017-2-azr-681-16/

doi: 10.5553/EELC/187791072018003001006