Überwachung von Arbeitnehmern mittels Keylogger – Zu den Möglichkeiten und ihrer arbeitsgerichtlichen Verwertbarkeit

26.09.2017

Arbeitsrecht | Compliance & Interne Ermittlungen | IT & Outsourcing

Zum Nachweis von Pflichtverletzungen sind Arbeitgeber oftmals auf Hilfsmittel angewiesen, um bestehende Verdachtsmomente gegen Arbeitnehmer aufzuklären. Wurden früher Mittel wie Taschenkontrollen, Videoüberwachung oder der Detektiveinsatz genutzt, beschäftigen die Arbeitsgerichte heute zunehmend auch neue Formen der technischen Überwachung. Hierzu zählen nicht nur die Auswertung von Chatprotokollen (siehe LAG Hamm, Urt. v. 10.07.2012 – 14 Sa 1711/10) oder des Browserverlaufs (siehe LAG Berlin-Brandenburg, Urt. v. 14.01.2016 - 5 Sa 657/15), sondern etwa auch der Einsatz von spezieller Überwachungssoftware am Dienstrechner. Eine solche neue Form der technischen Überwachung durch eine sog. Keylogger-Software hatte das Bundesarbeitsgericht in seiner Entscheidung vom 27. Juli 2017 (BAG, Urteil vom 27.07.2017 – 2 AZR 681/16) – vor allem datenschutzrechtlich – zu bewerten.

Was war geschehen?

Der Kläger war bei der Beklagten als „Web-Entwickler“ beschäftigt. Im Zuge der Freigabe eines Netzwerks teilte die Beklagte ihren Mitarbeitern mit, dass der gesamte Internetverkehr und die Verwendung ihrer Systeme „mitgeloggt“ werde. Weil die Arbeitgeberin die Vermutung hatte, dass der Kläger während der Arbeitszeit nicht arbeitete, sondern Privattätigkeiten nachging, installierte die Beklagte auf dem dienstlichen Computer des Klägers eine Software. Diese protokollierte sämtliche Tastatureingaben und fertigte regelmäßig Screenshots an („**Keylogger**“). Die Auswertung der aufgezeichneten Daten ergab, dass der Kläger während der Arbeitszeit in einem erheblichen Umfang Zeit dafür aufwendete, ein Computerspiel zu programmieren und E-Mails für die Firma seines Vaters zu bearbeiten. Nachdem der Kläger in einem darauf anberaumten Gespräch die private Nutzung des Dienst-PCs während der Arbeitszeit eingeräumt hatte, kündigte die Beklagte das Arbeitsverhältnis außerordentlich fristlos, hilfsweise ordentlich.

Die hiergegen erhobene Kündigungsschutzklage hatte in allen Instanzen Erfolg. Das Bundesarbeitsgericht stellte fest, dass die Datenerhebung mittels Keyloggers durch den gesetzlichen Erlaubnistatbestand des § 32 Abs. 1 BDSG nicht gerechtfertigt gewesen sei. Da die Beklagte beim Einsatz der Software gegenüber dem Kläger keinen auf Tatsachen begründeten Verdacht einer Straftat oder einer anderen schweren Pflichtverletzung hatte, sei die Maßnahme unverhältnismäßig gewesen. Dadurch sei das Recht des Klägers auf informationelle Selbstbestimmung (Art. 2 I GG i.V.m. Art. 1 I GG) verletzt worden. Dies führte gleichzeitig auch zu einem Verwertungsverbot, so dass die auf diese Weise erhobenen Daten nicht im Prozess verwertet werden dürften.

Die wesentlichen Fragen

Da die Entscheidung des Bundesarbeitsgerichts bislang nur als Pressemitteilung (Nr. 31/17) vorliegt, bleiben die genauen Erwägungsgründe abzuwarten. Zentral waren hier aber zwei Fragestellungen, die in Fällen vergleichbarer Art immer wieder eine Rolle spielen:

1. Welche rechtlichen Anforderungen bestehen für eine zulässige Überwachung von Arbeitnehmern?

2. Sind datenschutzwidrig erlangte Informationen im späteren Prozess verwertbar?

Wann ist eine Überwachung des Arbeitnehmers zulässig?

Das Bundesdatenschutzgesetz (BDSG) stellt in § 4 Abs. 1 BDSG ein Verbot mit Erlaubnisvorbehalt auf. Danach ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Für Arbeitsverhältnisse enthält § 32 BDSG zwei gesonderte Erlaubnistatbestände:

- Nach § 32 Abs. 1 S. 1 BDSG dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses

genutzt werden, wenn dies für die Entscheidung über die Begründung, die Durchführung und die Beendigung des Beschäftigungsverhältnisses erforderlich ist.

- Geht es um die Aufdeckung von Straftaten dürfen nach § 32 Abs. 1 S. 2 BDSG personenbezogene Daten eines Beschäftigten nur genutzt werden, wenn (i) zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, (ii) dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, (iii) die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und (iv) das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. Dabei reicht ein Anfangsverdacht aus, der über vage Anhaltspunkte und Mutmaßungen hinausreichen muss.

Keine Sperrwirkung des § 32 Abs. 1 S. 2 BDSG gegenüber der Erlaubnisnorm des § 32 Abs. 1 S. 1 BDSG

Die insoweit gegenüber S. 1 spezifischere Regelung des § 32 Abs. 1 S. 2 BDSG bedeutet nach Auffassung des Bundesarbeitsgerichts (BAG, Urt. v. 29.06.2017-2 AZR 597/16) dabei aber nicht, dass anlassbezogene Fälle der Datenerhebung zu anderen Zwecken als zur Aufklärung einer Straftat nicht zulässig wären. Das Bundesarbeitsgericht versteht § 32 Abs. 1 S. 2 BDSG nur als einen Sonderfall einer Datenerhebung und verbindet hiermit jedoch keine Sperrwirkung. Ob eine Maßnahme im konkreten Fall nach § 32 Abs. 1 S. 1 BDSG gerechtfertigt werden kann, hängt daher maßgeblich von der Eingriffsintensität der Maßnahme selbst ab. Je schwerwiegender die konkrete Maßnahme in das allgemeine Persönlichkeitsrecht des einzelnen Arbeitnehmers eingreift, desto höher setzt die Rechtsprechung den Maßstab für die Erforderlichkeit nach § 32 Abs. 1 S. 1 BDSG an. Bei besonders eingriffsintensiven Maßnahmen wie etwa der Videoüberwachung ist die Überwachungsmaßnahme nur zulässig, wenn ein konkreter Verdacht einer schweren Verfehlung zu Lasten des Arbeitgebers besteht und sich der Verdacht auf die schwere Verfehlung gegen einen zumindest räumlich und funktional abgrenzbaren Personenkreis richtet.

Tipps für die betriebliche Praxis

Ob eine beabsichtigte Überwachungsmaßnahme datenschutzrechtlich zulässig ist, ist damit eine Frage des Einzelfalls. Als Leitlinien für die Praxis kann das Folgende gelten:

- Reine Vorfeldmaßnahmen können nur Maßnahmen mit geringerer Eingriffsintensität, wie etwa Stichproben, rechtfertigen.
- Verdachtsunabhängige Vollkontrollen, die sogar heimlich durchgeführt werden, sind regelmäßig nicht erforderlich und damit unzulässig.
- Bestehen konkrete Anhaltspunkte für eine erhebliche Pflichtverletzung des Arbeitnehmers, können eingriffsintensive Maßnahmen wie etwa Videoüberwachung oder etwa auch ein Detektiveinsatz zulässig sein. Voraussetzung ist dabei, dass keine anderen gleich wirksamen und weniger eingriffsintensiven Maßnahmen existieren.

Entsprechend war im vorliegenden Fall der Einsatz des Keyloggers datenschutzrechtlich nicht zu rechtfertigen. Denn sein Einsatz erfolgte „ins Blaue hinein“, also letztlich verdachtsunabhängig. Es hätten zudem andere, weniger eingriffsintensive Ermittlungsmaßnahmen zur Verfügung gestanden (so etwa die Durchsicht von E-Mails in Anwesenheit des Mitarbeiters), die ein heimliches Vorgehen des Arbeitgebers unnötig gemacht hätten.

Verwertbarkeit datenschutzwidrig erlangter Informationen im Prozess?

Mit dem Verstoß gegen das BDSG steht die Unverwertbarkeit der erlangten Informationen im Prozess jedoch noch nicht zwangsläufig fest. Denn weder das Arbeitsgerichtsgesetz (ArbGG) noch die Zivilprozessordnung (ZPO) enthalten Regelungen über Sachvortrags- oder Beweisverwertungsverbote. Vielmehr verpflichtet der Grundsatz der freien Beweiswürdigung (§ 286 ZPO) und der Anspruch auf rechtliches Gehör (Art. 103 I Grundgesetz (GG)) die Gerichte dazu, alle angebotenen Beweise zu berücksichtigen. Daher geht die ständige Rechtsprechung (siehe etwa zuletzt BAG, Urt. v. 29.06.2017-2 AZR 597/16) davon aus, dass die Annahme eines Sachvortrags- bzw. Beweisverwertungsverbots nur durch eine verfassungskonformen Auslegung des Prozessrechts begründet werden kann. Da Gerichte gegenüber Verfahrensbeteiligten in staatlicher Hoheitsgewalt gegenübertreten, sind sie bei der Urteilsfindung auch an die Grundrechte gebunden (Art. 1 Abs. 3 GG). Greift die Verwertung des Sachvortrages oder eines Beweismittels in Grundrechte einer Prozesspartei ein, ist dieses nur dann verwertbar, wenn das Interesse an der Verwertung dieses Vortrages oder Beweises gegenüber dem Schutz der Grundrechte des betroffenen Arbeitnehmers überwiegt. Dazu müssen aber weitere über das schlichte Beweisinteresse hinausgehende Aspekte hinzutreten. Der Arbeitgeber muss sich letztlich in Beweisnot befinden, weil alle anderen Möglichkeiten, die Pflichtverletzung des Arbeitnehmers aufzudecken, keinen Erfolg versprechen (sog. Abwägungslösung).

In der Praxis werden daher datenschutzwidrig erlangte Informationen häufig unverwertbar sein. Ausnahmen, etwa bei der Verwertung von Zufallsfunden sind aber denkbar (siehe hierzu etwa BAG, Urt. v. 22.09.2016 - 2 AZR 848/15). Im Umkehrschluss folgt daraus aber auch: War bereits die Erhebung der Daten datenschutzrechtlich zulässig, kommt ein Sachvortrags- bzw. Beweisverwertungsverbot nicht in Betracht.

Fazit und Praxistipps

Die vorliegende Entscheidung veranschaulicht, dass der Überwachung von Arbeitnehmern durch das BDSG enge Grenzen gesetzt werden, die den Ausgang eines arbeitsgerichtlichen Prozesses maßgeblich prägen können. Hieran wird sich zukünftig durch die ab dem 25. Mai 2018 anzuwendende Datenschutz Grundverordnung (DSGVO) und das dann neu geltende BDSG nichts ändern, da die bisherigen Grundsätze des § 32 BDSG dann nahezu unverändert in § 26 BDSG n.F. fortgeführt werden.

Im konkreten Einzelfall muss daher jede beabsichtigte Überwachungsmaßnahme einer strengen Erforderlichkeitsprüfung unterzogen werden. Hierbei ist insbesondere zu prüfen, ob im konkreten Fall andere gleich wirksame und weniger eingriffsintensive Maßnahme zur Verfügung stehen (Bsp. klärendes Gespräch, Stichprobenkontrollen, Durchsicht in Anwesenheit statt in Abwesenheit des Arbeitnehmers, offene Videoüberwachung statt heimliche Videoüberwachung etc.). Gleichzeitig müssen Arbeitgeber die genauen Umstände der Ermittlungsmaßnahme (wie etwa Schaden, Verdachtsmomente und Schlussfolgerungen auf einen möglichen „Täterkreis“) genauestens dokumentieren, um im Ernstfall ihrer Darlegungs- und Beweislast im Prozess nachkommen zu können und so nicht an einem Sachvortrags- oder Beweisverwertungsverbot zu scheitern.

Haben Sie Fragen? Kontaktieren Sie gerne: Dr. Jacek Kielkowski
Practice Group: Arbeitsrecht , Compliance & Interne Ermittlungen