Spyware im Betriebsrats-PC?

Zur Entscheidung des Arbeitsgerichts Augsburg vom 4. 10 . 2012 – 1 BV 36/12

Der Sachverhalt

Im Produktionsbetrieb einer Großbäckerei im Augsburger Raum sind 475 Mitarbeiter beschäftigt. Vor einer Reihe von Jahren wurde erstmals ein elfköpfiger Betriebsrat gewählt. Geschäftsführer des Unternehmens sind zwei Brüder, die zugleich maßgebende Gesellschafter der Arbeitgeber-GmbH und der übrigen zur „Gruppe“ zählenden Unternehmen sind.

Zwischen der Geschäftsführung und dem Betriebsrat, insbesondere seinem Vorsitzenden, gab es seit einiger Zeit erhebliche – auch persönliche – Spannungen. Besonders wenig Verständnis brachte die Geschäftsführung dafür auf, dass nicht nur Betriebsratsmitglieder, sondern auch zahlreiche andere Beschäftigte Mitglieder der Gewerkschaft NGG geworden waren.

Der Betriebsratsvorsitzende war nach § 38 Abs. 1 BetrVG in vollem Umfang von seiner beruflichen Tätigkeit freigestellt. Im Betrieb wurde ein Zeiterfassungssystem praktiziert: Bei Beginn und Ende der Arbeitszeit hatte jeder Beschäftigte einen personalisierten Chip an ein Zeiterfassungsterminal zu halten, was zu einer „elektronischen Buchung“ führte. Trotz der Freistellung wurde auch der Betriebsratsvorsitzende in dieses System einbezogen; dem Hinweis, in einem anderen Betrieb der „Gruppe“ seien „Freigestellte“ ausgenommen, wurde seitens des Arbeitgebers keine Beachtung geschenkt.

Die Betriebsausschussmitglieder hatten ebenso wie die Schicht- und Abteilungsleiter eine Leseberechtigung in Bezug auf die gespeicherten Daten. Ergaben sich irgendwelche Ungereimtheiten, konnte man durch Anruf bei der Personalabteilung eine Berichtigung erwirken. Die Mitarbeiter der Personalabteilung hatten nicht nur ein Lese-, sondern auch ein Änderungsrecht, das durch ein Passwort gesichert war. Änderungsbefugt waren weiter die beiden Mitarbeiter der EDV-Abteilung, die Administratorenrechte hatten, die sie mithilfe des Benutzernamen „EDV“ und eines Passwortes ausüben konnten. Auch ein externer EDV-Dienstleister hatte vergleichbare Befugnisse.

Der Betriebsrat verfügte über drei Rechner und einen Laptop. Ein PC und der Laptop befanden sich im Büro des Betriebsratsvorsitzenden. Dieser konnte auch von zu Hause aus über seinen Router u. a. auf das Arbeitszeitkonto zugreifen.

Am 10.1.2012 wurde festgestellt, dass tags zuvor unter dem Benutzernamen „EDV“ Nr. 79 das Arbeitszeitkonto des Betriebsratsvorsitzenden geändert worden war: Nachträglich wurde für den 9. 12. 2011 eine Arbeitszeit von 7 ½ Stunden eingetragen. Dies führte zu einer Überprüfung aller Eintragungen bis zurück zum Mai 2010 (wobei nachträgliche Änderungen immer farblich gekennzeichnet waren). Als Ergebnis wurde festgestellt, dass die Korrekturen allesamt unter demselben Benutzernamen erfolgt waren und zu einer Erweiterung der „Arbeitszeit“ des Betriebsratsvorsitzenden um insgesamt 165 Stunden geführt hatten. Von welchem Rechner aus die Korrekturen vorgenommen wurden, war nicht festgehalten worden.

Am 16. 4. 2012 ließ der Arbeitgeber im Rechner des Betriebsratsvorsitzenden durch die Dienstleistungsfirma ein Kontrollprogramm installieren; dies geschah „aus der Ferne“, also ohne dass jemand das Betriebsratsbüro betreten hätte. Sobald von dem Rechner aus ein Zugriff auf das Zeiterfassungssystem erfolgte, aktivierte sich das Programm und erstellte fünf Minuten lang im Sekundentakt sogenannte Screenshots, auf denen festgehalten wurde, was sich im jeweiligen Augenblick auf dem Bildschirm befand. Dem Benutzer blieb das alles verborgen. Der Betriebsrat wurde von dieser Maßnahme nicht informiert und (natürlich) auch nicht um seine Zustimmung gebeten.

Am 3. 5. 2012 aktivierte sich gegen 8.43 Uhr das Programm und hielt fest, dass unter dem Benutzernamen „EDV“ (plus Passwort) für den 24. 4. 2012 eine „Nachbuchung“ vorgenommen wurde, wonach die Arbeitszeit um 6.30 Uhr begonnen und um 15.45 zu Ende gegangen sei. Anschließend war der Nutzer in den privaten E-Mail-Account des Betriebsratsvorsitzenden gegangen und hatte E-Mails beantwortet; nach fünf Minuten endeten die Aufzeichnungen.

Der Arbeitgeber vertrat den Standpunkt, es bestehe ein dringender Verdacht, dass der Betriebsratsvorsitzende seine Zeiten manipuliert habe. Dies sei ein wichtiger Grund für eine fristlose Kündigung. Der Betriebsrat verweigerte nach § 103 Abs. 1 BetrVG seine Zustimmung. Der Arbeitgeber rief daraufhin das Arbeitsgericht (ArbG) Augsburg an, um die

fehlende Zustimmung des Betriebsrats ersetzen zu lassen. Das Gericht wies den Antrag zurück.

Die Argumentation des Gerichts

Im Anschluss an die Rechtsprechung des BAG ging das ArbG Augsburg davon aus, dass eine Verdachtskündigung zulässig ist, wenn sich der Verdacht auf Tatsachen stützt, wenn er sich auf eine so schwerwiegende Pflichtverletzung bezieht, dass für den Arbeitgeber eine weitere Zusammenarbeit unzumutbar ist, und wenn er schließlich „dringend" ist, also eine hohe Wahrscheinlichkeit dafür spricht, dass die Pflichtverletzung tatsächlich begangen wurde.

Der „dringende Tatverdacht" scheiterte nach Auffassung des Gerichts daran, dass die mit Hilfe des Kontrollprogramms gewonnenen Erkenntnisse nicht verwertet werden durften. Die übrigen Erkenntnisse mochten einen „einfachen" Verdacht begründen, doch konnte ja auch ein Dritter die Veränderungen vorgenommen haben – sei es, dass er aus irgendwelchen Gründen dem Betriebsratsvorsitzenden einen Gefallen erweisen oder aber ihm (z. B. im Auftrag des Arbeitgebers) etwas „anhängen" wollte. Dies steht zwar so nicht ausdrücklich in der Entscheidung, doch ergibt es sich aus dem Zusammenhang.

Das Verwertungsverbot ergab sich für das ArbG Augsburg allerdings nicht schon daraus, dass der Arbeitgeber bei der Installierung des Kontrollprogramms das Mitbestimmungsrecht des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG verletzt hatte. Vielmehr sei die heimliche Installierung ein Eingriff in das allgemeine Persönlichkeitsrecht des Betriebsratsvorsitzenden gewesen. Ein solches Vorgehen sei nach der Rechtsprechung des BAG nur dann zulässig, wenn überwiegende Interessen des Arbeitgebers dafür sprechen würden. Daran fehle es jedenfalls deshalb, weil die ergriffene Maßnahme unverhältnismäßig gewesen sei: Während der fünf Minuten dauernden Aufzeichnungen seien auch andere Dinge als die Nutzung und Veränderung des Arbeitszeitprogramms (hier etwa die E-Mail-Bearbeitung) erfasst worden. Dieser über das legitime Erkenntnisinteresse des Arbeitgebers hinaus gehende Eingriff wäre dadurch zu vermeiden gewesen, dass sich das Kontrollprogramm automatisch abgeschaltet hätte, sobald kein Kontakt mehr zum Arbeitszeitprogramm bestand. Dies wäre durch eine entsprechende Programmierung möglich gewesen; den damit verbundenen Aufwand hätte der Arbeitgeber in Kauf nehmen müssen. Der Antrag des Arbeitgebers wurde deshalb zurückgewiesen.

Es ist völlig legitim, dass ein Gericht nicht allen denkbaren Rechtsfragen nachgeht, sondern sich auf *einen* Gesichtspunkt stützt, der das gefundene Ergebnis trägt. Inhaltlich ist ihm insoweit auch voll zuzustimmen. Mit Rücksicht auf mögliche andere Fälle, bei denen es keinen solchen Ausweg gibt, sei hier jedoch noch auf zusätzliche Gesichtspunkte hingewiesen.

Das übergangene Mitbestimmungsrecht

Was das Mitbestimmungsrecht des Betriebsrats bei der Installierung des Kontrollprogramms betraf, so ging das ArbG Augsburg als selbstverständlich davon aus, dass dieses Recht auch dann besteht, wenn sich der Verdacht gegen ein Betriebsratsmitglied richtet. Dies trifft zu, weil das Gesetz insoweit keine Ausnahme kennt. In der Praxis führt das allerdings dazu, dass der Arbeitgeber im Regelfall auf eigene Ermittlungen verzichten wird, weil sie wegen der „Warnung" des Verdächtigten ohne große Aussicht auf Erfolg sind. Er kann sich aber auf andere Weise zur Wehr setzen: Ihm bleibt wie jedem anderen potentiell geschädigten Mitbürger die Möglichkeit, sich an Polizei und Staatsanwaltschaft zu wenden. Sie können ein Ermittlungsverfahren einleiten und mit den in der Strafprozessordnung (=StPO) vorgesehenen Mitteln die Wahrheit zutage fördern.

Dass Verstöße gegen ein Mitbestimmungsrecht nicht zu einem Verwertungsverbot im Prozess führen sollen, begründet das ArbG Augsburg mit der Erwägung, gegen mitbestimmungswidriges Verhalten des Arbeitgebers gebe es bereits ausreichende betriebsverfassungsrechtliche und individualvertragliche Sanktionen, so dass es einer darüber hinaus gehenden prozessualen Sanktion nicht bedürfe. Dabei beruft es sich auf eine Entscheidung des BAG vom 13. 12. 2007 (2 AZR 537/06), wo sich unter Nr. 31 in der Tat eine solche Aussage findet. Nur lag der damals entschiedene Fall anders: Dort war eine Betriebsvereinbarung über Ermittlungsmaßnahmen im Betrieb offen und für den Betriebsrat wahrnehmbar nicht beachtet worden; außerdem hatte der Betroffene in die (illegalen) Kontrollmaßnahmen eingewilligt. Im vorliegenden Fall geschah jedoch alles heimlich, so dass die betriebsverfassungsrechtlichen Sanktionen wie der Unterlassungsanspruch und etwaige arbeitsvertragliche Sanktionen wie die Zurückbehaltung der Arbeitsleistung leer liefen. Hätten sich keinerlei „Zusatzerkenntnisse" ergeben, wäre es möglich gewesen, über Jahre hinweg eine entsprechende Spyware einzusetzen. In solchen Fällen ein Verwertungsverbot

anzunehmen, hätte den gewichtigen Vorteil, dass sich die „Heimlichkeit“ unter keinen Umständen lohnen würde. Außerdem war es in der BAG-Entscheidung in der Hauptsache nur darum gegangen, ob rechtswidrig erlangte Erkenntnisse überhaupt in das gerichtliche Verfahren eingeführt werden durften, was noch nichts darüber sagt, ob sie das Gericht auch dann verwerten darf, wenn die Gegenseite ihre Richtigkeit mit nachvollziehbaren Erwägungen bestreitet.

Eingriff in Betriebsratsrechte

Ein Kontrollprogramm in den Rechner des Betriebsratsvorsitzenden einzuschmuggeln, ist nicht nur ein Problem des Persönlichkeitsschutzes. Vielmehr geht es gleichzeitig darum, dass die Betriebsratstätigkeit als solche betroffen ist. Auch wenn der Anwendungsbereich des Programms ein enger war, stellt es eine Behinderung der Betriebsratstätigkeit dar, wenn Aktivitäten des Vorsitzenden ausgespäht und gespeichert werden. Dies wird schon daran deutlich, dass das Programm bei jedem Kontakt mit dem Zeiterfassungssystem aktiviert wurde, also nicht nur dann, wenn es um die persönlichen Daten des Betriebsratsvorsitzenden ging. Nach § 119 Abs. 1 Nr. 2 BetrVG macht sich jedoch strafbar, wer die Tätigkeit des Betriebsrats „behindert oder stört“. Ein Rechtfertigungsgrund ist nicht ersichtlich: Notwehr oder eine „notwehrähnliche Lage“ schied von vorne herein aus, weil der „Angriff“ auf das Vermögen des Arbeitgebers ja nicht vom Betriebsrat als solchem, sondern (angeblich) von der Person des Vorsitzenden ausging.

Ob ein Verstoß gegen § 119 Abs. 1 Nr. 2 BetrVG zu einem gerichtlichen Verwertungsverbot führt, scheint wenig erörtert zu sein. Die Frage ist zu bejahen. Dies wird schon an dem spiegelbildlichen Fall deutlich, dass sich der Betriebsrat etwa mit Hilfe eines ihm verbundenen Systemadministrators illegal Material des Arbeitgebers beschafft, wonach dieser bewusst eine „Zermürbungsstrategie“ gegen den Betriebsrat praktiziert, wie sie einzelne Anwaltskanzleien empfehlen. Würde man dieses Material wirklich in einem arbeitsgerichtlichen Beschlussverfahren oder beim Erlass eines Strafbefehls zugrunde legen? Der Betrieb würde in einem solchen Fall zu einer Art Kriegsschauplatz, auf dem derjenige die besseren Karten hat, der schneller und raffinierter zu Werke geht und sich über dunkle Kanäle geschickter Material verschafft. Dem wird jedes Arbeitsgericht einen Riegel vorschieben.

Das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme

Der vorliegende Fall gibt schließlich Anlass, sich an die Entscheidung des Bundesverfassungsgerichts zur Online-Überwachung zu erinnern (BVerfG 27. 2. 2008 – 1 BvR 370/07 und 595/07), die einen heimlichen Zugriff auf informationstechnische Systeme grundsätzlich ausschließt. Ob sie auch im Verhältnis Arbeitgeber – Arbeitnehmer anwendbar ist, erscheint zweifelhaft, da das Gericht nur von Systemen spricht, die man „als eigene" nutzt (Nr. 206 des Entscheidungstextes). Der Betriebsrat wird sich jedoch auf dieses neu entwickelte Grundrecht berufen können, da ihm die fraglichen Geräte zur ausschließlichen Eigennutzung im Rahmen seines Amtes überlassen sind. Das „Infiltrierungsverbot" (Nr. 180 ff. des Entscheidungstextes) muss daher auch hier Anwendung finden.

Das Arbeitsgericht Augsburg hätte sich unter diesen Umständen noch auf weitere Gründe stützen können, um sein zutreffendes Ergebnis zu begründen. Vermutlich wird die Rechtsprechung auch in Zukunft Gelegenheit haben, sich zu diesem Problemkreis zu äußern: Heimliche Überwachung von Betriebsräten lässt sich nie mit Sicherheit ausschließen.

Prof. Dr. Wolfgang Däubler, Bremen