Vom Kavaliersdelikt zur Kündigung

IT-NUTZUNG *Der allzu sorglose Umgang mit der IT am Arbeitsplatz kann erhebliche rechtliche Risiken für die Beschäftigten haben, die bis hin zum Arbeitsplatzverlust reichen können. Ein Überblick zeigt die Risiken und den richtigen Umgang mit ihnen.*

VON **GÖTZ GERLACH**

Globale Vernetzung, Industrie 4.0, digitale Transformation. Schlagworte, die nicht nur für zukunftsorientierten, digitalen Fortschritt stehen, sondern auch dafür, dass der alltägliche Umgang mit der IT aus unserem Arbeitsleben nicht mehr wegzudenken ist.

Weniger beachtet hingegen werden oft die rechtlichen Gefahren und Risiken, die die Allgegenwart der IT im Arbeitsleben für die Beschäftigten haben kann, wenn man sich nicht an Spielregeln hält oder leichtfertig mit der – in der Regel fremden – IT umgeht.

Privates Surfen während der Arbeitszeit, Verstöße gegen den Datenschutz durch Weitergabe von personenbezogenen Daten ohne ausreichende Rechtsgrundlage sind leider ebenso oft anzutreffen wie Urheberrechtsverletzungen durch das Schaffen oder Nutzen einer sogenannten Schatten-IT. Dass damit oft auch eine Verletzung der arbeitsvertraglichen Pflichten einhergeht, die zum Verlust des Arbeitsplatzes führen kann, wird dabei oft vergessen oder ausgeblendet. Es gilt, diese Risiken und Gefahren zu erkennen. Nötig ist dafür, das Bewusstsein der Beschäftigten zu schärfen, um den sicheren und vernünftigen Umgang mit der IT zu erleichtern.

Klare Spielregeln nötig

Entgegen einer weit verbreiteten irrtümlichen Annahme gibt es kein »Recht zur Privatnutzung« der IT am Arbeitsplatz: Auch ohne ausdrückliches Verbot ist es nicht zulässig, die unternehmenseigene IT für private Zwecke zu nutzen.[1] Ausgangspunkt ist § 106 Gewerbeordnung (GewO). Die Vorschrift regelt das Weisungsrecht – auch Direktionsrecht genannt – des Arbeitgebers:

»Der Arbeitgeber kann Inhalt, Ort und Zeit der Arbeitsleistung nach billigem Ermessen näher bestimmen, soweit diese Arbeitsbedingungen nicht durch den Arbeitsvertrag, Bestimmungen einer Betriebsvereinbarung, eines anwendbaren Tarifvertrages oder gesetzliche Vorschriften festgelegt sind. Dies gilt auch hinsichtlich der Ordnung und des Verhaltens der Arbeitnehmer im Betrieb.«

Auf die unternehmenseigene IT bezogen bedeutet dies, dass es allein Sache des Arbeitgebers ist, die Spielregeln für den Umgang mit der IT festzulegen. Er darf und kann – unter Beachtung der Mitbestimmungsrechte des Betriebs- oder Personalrats – festlegen, ob die unternehmenseigene IT überhaupt für private Zwecke genutzt werden darf. Das Bundesarbeitsgericht (BAG) hat schon vor langer Zeit ausdrücklich festgestellt:

»Bei einer privaten Internetnutzung während der Arbeitszeit verletzt der Arbeitnehmer grundsätzlich seine (Hauptleistungs-)Pflicht zur Arbeit.«[2]

Ist die private Nutzung der IT durch eine betriebliche Regelung untersagt, so haben sich die Beschäftigten daran zu halten. Verstöße können – je nach Schwere – nicht nur eine Abmahnung, sondern auch eine fristlose Kündigung nach sich ziehen.

»Nötig ist dafür, das Bewusstsein der Beschäftigten zu schärfen, um den sicheren Umgang mit der IT zu erleichtern.«

GÖTZ GERLACH

Vorsicht bei privater Nutzung

Aber auch, wenn die private IT-Nutzung erlaubt ist, ist dies kein Freibrief: Das »Herunterladen einer erheblichen Menge von Daten aus dem Internet […], insbesondere wenn damit einerseits die Gefahr möglicher Vireninfizierungen oder anderer Störungen des – betrieblichen – Betriebssystems verbunden sein können oder andererseits von solchen Daten, bei deren Rückverfolgung es zu möglichen Rufschädigungen des Arbeitgebers kommen kann, beispielsweise weil strafbare oder pornografische Darstellungen heruntergeladen werden«, kann eine außerordentliche Kündigung rechtfertigen.[3]

Das BAG hat dazu wörtlich ausgeführt: »Deshalb muss es jedem Arbeitnehmer klar sein, dass er mit einer exzessiven Nutzung des Internets während der Arbeitszeit seine arbeitsvertraglichen Haupt- und Nebenpflichten

DARUM GEHT ES

1. Beschäftigte sind bei der Nutzung von IT am Arbeitsplatz zahlreichen Gefahren und Haftungsrisiken ausgesetzt.

2. Rechtsverstöße können schnell ernsthafte Konsequenzen für Arbeitnehmer und Arbeitgeber nach sich ziehen.

3. Klare Regeln für den Umgang mit Informationstechnologie am Arbeitsplatz sind nötig.

1 BAG 7.7. 2005 – 2 AZR 581/04, juris, Rn. 37

2 BAG, aaO., Rn. 27 mit weiteren Nachweisen

3 BAG, aaO., Rn. 24

erheblich verletzt. Es bedarf daher in solchen Fällen auch keiner Abmahnung.«[4] Beschäftigte sind also gut beraten, sich daran zu halten.

Es versteht sich von selbst, dass die unternehmenseigene IT auch für andere private Zwecke tabu ist, sofern dies vom Arbeitgeber nicht ausdrücklich erlaubt wird. Das regelmäßige Aufladen des Handys am Arbeitsplatz ohne ausdrückliche Genehmigung des Arbeitgebers rechtfertigt keine außerordentliche Kündigung.[5]

Anders jedoch, wenn Musik- oder Videodateien mit unternehmenseigenen Rechnern vervielfältigt werden. Ausgerechnet der »Verantwortliche IT« beim Oberlandesgericht (OLG) Naumburg hatte am Arbeitsplatz mehrere tausend Kopien urheberrechtlich geschützter Werke hergestellt. Die außerordentliche Kündigung war auch nach 21-jähriger Beschäftigungsdauer nach Ansicht des BAG gerechtfertigt: »Ein Arbeitgeber hat […] ein offenkundiges Interesse daran, dass nicht dienstliche Rechner dazu benutzt werden, unter Umgehung eines Kopierschutzes Vervielfältigungen privat beschaffter Musik- oder Film-CDs/DVDs herzustellen. Das gilt losgelöst von einer möglichen Strafbarkeit der Vorgänge […] und unabhängig davon, ob die Handlungen während der Arbeitszeit vorgenommen wurden.«[6]

Schatten-IT – Daten außer Kontrolle

Das letzte Beispiel berührt einen anderen Rechtsbereich, der mit dem Arbeitsplatz auf den ersten Blick weniger zu tun hat und deshalb oft unterschätzt wird: das Urheberrecht. Dieses hat im Zeitalter des IT-basierten Arbeitens und vor allem des Internets einen neuen Stellenwert erhalten. Urheberrechtsverletzungen sind kein Kavaliersdelikt, sondern können strafbar sein. Allerdings sind sie (leider) nach wie vor an der Tagesordnung. Nicht nur durch rechtswidrige Down- oder Uploads von Bildern, Musik, Videos oder Software.

Inzwischen dürfte jedem Beschäftigten klar sein, dass der neueste Hollywood-Blockbuster oder Nr. 1-Hit der Charts nicht »für lau« im Internet zu haben sind. Weniger bekannt sind Urheberechtsverletzungen durch »Übernutzung« von Software. Die Rede ist von der Schatten-IT, die das Risiko birgt, dass die gesamte IT-Infrastruktur gefährdet wird.

Aber was verbirgt sich dahinter? Laut Wikipedia umfasst der Begriff Schatten-IT »informationstechnische Systeme, -Prozesse und -Organisationseinheiten, die in den Fachabteilungen eines Unternehmens neben der offiziellen IT-Infrastruktur und ohne das Wissen des IT-Bereichs angesiedelt sind.«[7]

Sensible Unternehmensdaten oder personenbezogene Daten werden – in bester Absicht – über unsichere Kanäle verteilt. Damit geht ein Kontrollverlust einher: Wer, wann, wo, was, über welches Medium Daten austauscht, bleibt im Dunkeln. Gemeint sind beliebte Cloud-Speicherdienste wie Dropbox, Google-Drive, OneDrive, Evernote oder iCloud, aber auch Messenger wie WhatsApp & Co.

IT-RISIKEN

Gefahren beim sorglosen Umgang mit der Unternehmens-IT

- Pflichtverletzungen und Vertragsverstöße durch unzulässige oder extensive private Nutzung der Firmen-IT, die Abmahnungen oder gar Kündigungen nach sich ziehen können.
- Gefährdung der IT-Sicherheit durch unabgestimmte Nutzung beliebter Cloud-Dienste oder Messenger, die zudem oft zu Datenschutzverstößen oder Urheberrechtsverletzungen führen.
- Es drohen dadurch auch Bußgelder oder Geld- und in schwersten Fällen auch Freiheitstrafen.

So bequem es sein mag, unternehmens- oder personenbezogene Daten über eine dieser Plattformen auszutauschen, die Risiken für Unternehmen und Beschäftigte sind enorm. Zunächst ist nicht immer klar, ob der jeweilige Dienst – der oft kostenfrei ist – auch für kommerzielle Zwecke genutzt werden darf. Ist dies nicht zulässig, weil die kommerzielle Nutzung ein kostenpflichtiges Upgrade voraussetzt, so stellt die betriebliche Nutzung eine Urheberrechtsverletzung dar.

Manche Anbieter erlauben dem Benutzer, ein Exemplar der Software auf dem PC und ein Exemplar auf dem Smartphone oder Tablet-PC zu installieren (Personal Licence), wenn sichergestellt ist, dass entweder nur das eine oder das andere genutzt wird. Dies ist aber nicht gleichzusetzen mit der Erlaubnis sowohl

4 BAG, aaO. Rn. 38
5 ArbG Oberhausen – 4 Ca 1228/09, www.kostenlose-urteile.de, Kündigung wurde zurückgenommen, das Gericht musste nicht mehr über den Sachverhalt entscheiden
6 BAG 15.7.2015 – 2 AZR 85/15, juris, Rn. 32; siehe dazu auch Lutz, Kündigung wegen Raubkopien am Arbeitsplatz, in: CuA 9/2015, 34
7 Wikipedia, Schatten-IT, https://de.wikipedia.org/wiki/Schatten-IT

dienstlicher als auch privater Nutzung. Nutzt der Beschäftige diese Anwendung dienstlich für seinen Arbeitgeber, verstößt er gegen seinen Vertrag mit dem Anbieter!

Urheberrechtsverletzungen können sehr unangenehme Rechtsfolgen für Unternehmen und die Beschäftigten, die den Verstoß begangen haben, nach sich ziehen: Unterlassung und Beseitigung der Störung, vor allem aber auch Schadenersatzansprüche.

Um letztere geltend machen zu können, bestehen umfangreiche Auskunfts- und Einsichtsansprüche, zum Beispiel in Bank-, Finanz- oder Firmenunterlagen. Im Fadenkreuz steht der Beschäftigte selbst, unabhängig davon, wo, wann oder warum er die Verletzungshandlung begangen hat, aber auch der »Inhaber« eines Unternehmens, wenn ein Mitarbeiter die Verletzungshandlung im »Unternehmen« begangen hat.

Der »Unternehmer« kann urheberrechtlich als »Raubkopierer« gelten, er muss die Verletzungshandlung durch Arbeitnehmer gegen sich gelten lassen. Er kann sich nicht damit entschuldigen, dass die ihm zugute kommende Urheberrechtsverletzung von Beschäftigten oder Beauftragten begangen worden sind. Online-Dienste lassen sich in ihren Allgemeinen Geschäftsbedingungen (AGB), die beim Einrichten überwiegend unkritisch akzeptiert werden, die verschiedensten Rechte einräumen. So heißt es in den AGB von Evernote:

»Das bedeutet also, dass Sie […] durch das Hochladen des Inhalts Evernote die Erlaubnis geben, Ihre Inhalte anzuzeigen, auszuführen, zu verteilen, zu modifizieren […] und zu vervielfältigen, […] Sie erkennen außerdem an, dass Evernote berechtigt ist, nach eigenem Ermessen Inhalt nicht zu akzeptieren, zu posten, zu speichern, anzuzeigen, zu veröffentlichen oder zu übermitteln. Sie stimmen zu, dass diese Rechte und Lizenzen gebührenfrei, weltweit und unwiderruflich gültig sind (solange Ihre Inhalte bei uns gespeichert werden) und das Recht für Evernote einschließen, derartigen Inhalt Dritten zur Verfügung zu stellen und diese Rechte an Dritte zu übertragen, mit denen Evernote ein Vertragsverhältnis bezüglich der Bereitstellung des Evernote-Diensts geschlossen hat.«[8]

Kaum ein Beschäftigter wird zuverlässig beurteilen können, ob er oder das Unternehmen tatsächlich berechtigt sind, Inhalte »gebührenfrei, weltweit und unwiderruflich gültig« einem fremden Dritten wie Evernote zu übertragen. Hat beispielsweise das Unternehmen im Rahmen eines Entwicklungsprojekts eine Geheimhaltungsvereinbarung mit dem Projektpartner abgeschlossen, so kann der Austausch von Projektdaten über einen Cloud-Dienst außerhalb der Unternehmens-IT einen Verstoß gegen diese Geheimhaltungsvereinbarung sein. Im schlimmsten Fall drohen dem Unternehmen Vertragsstrafen. Es kann nur dringend davor gewarnt werden, »inoffizielle« Kanäle zu dienstlichen Zwecken zu nutzen.

Noch schnell Unternehmensdaten in die Cloud geladen, damit man nach Feierabend zu Hause weiter arbeiten kann. Dieses Engagement birgt erhebliche Risiken – für den Arbeitgeber und den Arbeitnehmer.

»Alles verboten, was nicht ausdrücklich erlaubt ist«

Neben den Urheberrechtsverletzungen ist bei der Nutzung der Schatten-IT das Risiko, gegen Datenschutzbestimmungen zu verstoßen, extrem hoch. Im Datenschutzrecht gilt – und daran wird sich auch unter der Geltung der EU-Datenschutzgrundverordnung (DSGVO) ab Mai 2018 nichts ändern – vereinfacht ausgedrückt: Es ist alles verboten, was nicht ausdrücklich erlaubt ist. Es liegt auf der Hand, dass die Weitergabe personenbezogener Daten an einen Dritten – und das sind die Anbieter der Cloud-Speicherdienste durchweg – ohne die erforderliche Einwilligung der Betroffenen oder ohne eine ausreichende gesetzliche Ermächtigung erfolgt.

8 Evernote, Nutzungsbedingungen, https://evernote.com/intl/de/legal/terms-of-service

KÜNDIGUNG

Die massenhaften Abrufe von Meldedaten durch eine Mitarbeiterin im Bürgeramt rechtfertigen eine außerordentliche Kündigung, auch wenn sie nur einen kleinen Personenkreis betreffen und aus reiner Neugier erfolgt sind.
LAG Berlin-Brandenburg, Urteil vom 1.9.2016 – 10 Sa 192/16
(Leitsatz des Gerichts)

Saftige Strafen drohen

Beschäftigte, die auf die beschriebene Weise rechtswidrig handeln, begehen dadurch immer auch Pflichtverletzungen im Arbeitsverhältnis. Diese Pflichtverletzungen rechtfertigen in aller Regel eine Abmahnung. Schwere Verstöße können sogar – unter Umständen auch ohne vorherige Abmahnung – eine (fristlose) Kündigung rechtfertigen, wie das Beispiel des IT-Verantwortlichen bei einer Entscheidung des OLG Naumburg zeigt.[9] Daneben kann das Fehlverhalten Schadenersatz- und Schmerzensgeldansprüche auslösen.

Es drohen zudem Bußgelder oder Geld- beziehungsweise Freiheitsstrafen. 2013 zum Beispiel verhängte das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) gegen ein Unternehmen wegen einer E-Mail mit »offenem« Verteiler 2013 ein Bußgeld. Ein Mitarbeiter hatte einen kurzen Text versandt, dabei jedoch alle Empfänger (neuneinhalb Druckseiten!) in das »An«-Feld der E-Mail gesetzt, so dass jeder sehen konnte, an wen die elektronische Post gerichtet war.[10]

Das BayLDA verhängte 2015 ein Bußgeld in je fünfstelliger Höhe gegen zwei Unternehmen, die Mail-Adressen von Kunden im Rahmen eines Unternehmenskaufs untereinander weitergegeben hatten. Thomas Kranig, Präsident des BayLDA, teilte dazu mit: »Bei Asset Deals werden personenbezogene Kundendaten bisweilen unter Verstoß gegen das Datenschutzrecht veräußert. Um die Sensibilität der Unternehmen zu erhöhen, werden wir in auch in weiteren geeigneten Fällen dieser Art Verstöße mit Geldbußen ahnden.«[11]

In beiden Fällen lag ein klarer Verstoß gegen datenschutzrechtliche Bestimmungen vor, da natürlich nicht die Einwilligung jedes einzelnen Empfängers vorlag, seine E-Mail-Adresse an andere weiterzugeben.

Das Amtsgericht (AG) Tiergarten verurteilte eine Mitarbeiterin des Bürgeramts, die in 561 Fällen personenbezogene Daten aus dem Melderegister unbefugt an Dritte weitergegeben hatte, zu einer Geldstrafe:

»Darüber hinaus handelte es sich nicht um wahllose Abfragen bezüglich völlig unbeteiligter Bürger, sondern um die immer gleichen fünf Betroffenen aus ihrem persönlichen Umfeld. […] Gegen die Angeklagte sprach jedoch die Vielzahl an Verstößen. Überdies sind derartige Taten geeignet, das Vertrauen der Bevölkerung in die Lauterkeit der Verwaltung ernsthaft zu erschüttern.«[12]

Die deswegen ausgesprochene außerordentliche Kündigung hielt das Landesarbeitsgericht (LAG) Berlin-Brandenburg trotz 34-jähriger Betriebszugehörigkeit auch ohne Abmahnung für gerechtfertigt.[13]

Fazit

Urheberrechts- und Datenschutzverstöße sowie Verstöße gegen betriebliche Regelungen über den Umgang mit der firmeneigenen IT können ernsthafte Konsequenzen für die Beschäftigten und deren Unternehmen haben. Häufiger als die Fälle, in denen mit erheblicher krimineller Energie Unternehmen als Kopieranstalten oder Tauschbörsen missbraucht werden, aber nicht minder risikoreich, sind die Fälle, in denen in größerem Umfang während der Arbeitszeit private Internetnutzung stattfindet, eine Schatten-IT geschaffen und genutzt wird oder aus schlichter Unwissenheit oder Unachtsamkeit Rechtsverstöße erfolgen.

»Urheberrechts- und Datenschutzverstöße können ernste Konsequenzen für Beschäftigte und Unternehmen haben.«

GÖTZ GERLACH

Trotz der hohen Anforderungen, die das höchste deutsche Arbeitsgericht zu Recht an die Aufklärung solcher Verstöße stellt – zuletzt in der Keylogger-Entscheidung[14], ist erhöhte Aufmerksamkeit und Sensibilität im Umgang mit der IT angebracht. ◁

Dr. Götz Gerlach, Kleymann, Karpenstein & Partner mbB, Wetzlar
g.gerlach@kleymann.com
www.kleymann.com

9 BAG 15.7. 2015, aaO.
10 Sicking, Bußgeld wegen offenem E-Mailverteiler, www.heise.de
11 Schmidt, Kundendaten: Datenschutzrecht beim Unternehmenskauf, www.datenschutzbeauftragter-info.de
12 AG Tiergarten 17.3.2015 – (249 Ds) 253 Js 2131/14 (232/14), juris
13 LAG Berlin-Brandenburg 1.9.2016 – 10 Sa 192/16; Wurzberger, Rausschmiss wegen Schnüffeleien, in: CuA 3/2017, 23
14 BAG 27.7.2017 – 2 AZR 681/16; ausführlich dazu Frowein, Mitarbeiterkontrolle per Keylogger, in: CuA 12/2017, 16 ff. und Gerlach, Klare Grenzen für heimliche Kontrollen, in: CuA 12/2017, 13 ff., jeweils in diesem Heft

Klare Grenzen für heimliche Kontrollen

BESCHÄFTIGTENDATENSCHUTZ *Nicht jedes Mittel, das der Aufklärung von vermuteten Verstößen der eigenen Mitarbeiter gegen arbeitsvertragliche Pflichten dient, ist zulässig. Erkenntnisse aus unrechtmäßigen Schnüffeleien zählen vor Gericht nicht.*

VON **GÖTZ GERLACH**

Arbeitnehmer zu überwachen oder ihr Verhalten zu kontrollieren, ist bei den heutigen technischen Möglichkeiten ein Leichtes: Videoüberwachung, Auswertung des E-Mailverkehrs oder des Browserverlaufs durch schlichte Einsichtnahme am Computer, Auswertung der Logfiles der Firewall oder anderer IT-Sicherheitssysteme bis hin zur lückenlosen Überwachung mittels sogenannter Keylogger-Programme, die jeden Tastenanschlag an einem PC protokollieren und damit mühelos ein minutiöses Tätigkeitsprofil erstellen. Was technisch möglich ist, ist natürlich bei Weitem nicht rechtlich zulässig. Aber auch »herkömmliche« Untersuchungsmethoden, wie die Spindkontrolle oder der Einsatz eines Detektivs, sind stets unter datenschutzrechtlichem Blickwinkel zu betrachten.

Konkreter Verdacht nötig

In der Sache handelt es bei derartigen Maßnahmen um das Erheben und Verarbeiten personenbezogener Daten. Seit dem Volkszählungsurteil des Bundesverfassungsgerichts (BVerfG) aus dem Jahre 1983 ist das Recht auf informationelle Selbstbestimmung als Teil des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz (GG) anerkannt.[1]

Der Schutz des Einzelnen gegen das unbegrenzte Erheben, Speichern, Verwenden und Weitergeben seiner persönlichen Daten ist daher auch bei internen Ermittlungen im Arbeitsverhältnis zu beachten. Dem trägt seit 2009 § 32 des Bundesdatenschutzgesetzes (BDSG) Rechnung. Danach ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten eines Beschäftigten nur zulässig, wenn dies »erforderlich« ist.

Wenn die Datenverarbeitung zur Aufklärung von Straftaten im Arbeitsverhältnis erfolgen soll, wird das Gesetz konkreter. Es müssen »tatsächliche« Anhaltspunkte einen Verdacht begründen, die Datenerhebung muss »erforderlich«, im überwiegenden Interesse des Arbeitgebers und insgesamt »nicht unverhältnismäßig« sein. Auch mit Inkrafttreten der EU-Datenschutzgrundverordnung (DSGVO) im Mai 2018 wird sich daran nichts ändern. Die Neufassung des § 32 BDSG in § 26 BDSG-neu hält an den strengen Voraussetzungen fest.

Das Bundesarbeitsgericht (BAG) hat in der jüngeren Vergangenheit mehrfach Gelegenheit gehabt, die Voraussetzungen und Grenzen für verdeckte Untersuchungs- oder Aufklärungsmaßnahmen klarzustellen, zuletzt in der sogenannten Keylogger-Entscheidung.[2] Es festigt mit dieser Entscheidung seine Rechtsprechung, inwieweit sich Verstöße des Arbeitgebers gegen datenschutzrechtliche Bestimmungen bei der Aufklärung von vermutetem Fehlverhalten Einfluss auf den erforderlichen Nachweis eben dieses Verhaltens auswirken.

Der Entscheidung des höchsten deutschen Arbeitsgerichts lag folgender Sachverhalt zugrunde: Der Kläger war bei der Beklagten als Webentwickler tätig; er hatte sich zu Beginn seiner Tätigkeit schriftlich verpflichtet, die un-

DARUM GEHT ES

1. Die verdeckte Überwachung der Mitarbeiter zur Aufklärung von Verstößen im Arbeitsverhältnis ist nur in sehr engen Grenzen möglich.

2. Das Recht der Beschäftigten auf informationelle Selbstbestimmung weist schnüffelnde Chefs in ihre Schranken.

3. Es müssen triftige Gründe für das heimliche Sammeln von Beweismaterial vorliegen.

1 BVerfG 15.12.1983 – 1 BvR 209/83; siehe auch: 30 Jahre informationelle Selbstbestimmung – Volkszählungsurteil des BVerfG, in: CuA 1/2014, 3

2 BAG 27.7.2017 – 2 AZR 681/16, juris; ausführlich dazu Frowein, Mitarbeiterkontrolle per Keylogger, in: CuA 12/2017, 16 ff., in diesem Heft

ternehmenseigene IT nur zu dienstlichen Zwecken zu nutzen. Die Beklagte versandte folgende E-Mail an alle Mitarbeiter:

»Hallo liebes […] Team, es ist soweit, die Telekom hat es endlich geschafft, uns einen schnellen Internet Anschluss bereitzustellen. Dieses möchte ich Euch natürlich nicht vorenthalten, aus diesem Grund erhaltet Ihr freien Zugang zum WLAN. Da bei Missbrauch, zum Beispiel Download von illegalen Filmen, etc. der Betreiber zur Verantwortung gezogen wird, muss der Traffic mitgelogged werden.

Da ein rechtlicher Missbrauch natürlich dann auch auf denjenigen zurückfallen soll, der verantwortlich dafür war. Somit: Hiermit informiere ich Euch offiziell, dass sämtlicher Internet Traffic und die Benutzung der Systeme (der Beklagten) mitgelogged und dauerhaft gespeichert wird. Solltet Ihr damit nicht einverstanden sein, bitte ich Euch mir dieses innerhalb dieser Woche mitzuteilen. […] Bitte benutzt dieses Netzwerk für alles wie Spotify, YouTube, etc. um unser Hauptnetzwerk zu entlasten.«

In einer Unterweisung sprach sich kein Arbeitnehmer gegen die Absicht des Unternehmens aus, den »Internettraffic« und die Benutzung ihrer Systeme zur Verhinderung von Missbrauch des Internetzugangs »mitzuloggen«. So wurde auf dem Dienst-PC des Klägers eine Software installiert, die alle Tastatureingaben protokolliert und regelmäßig Screenshots fertigt (Keylogger). Nachdem das Unternehmen die durch den Keylogger über einen Zeitraum von nur acht Arbeitstagen erstellten Dateien ausgewertet hatte, stellte sie den Kläger zur Rede, der einräumte, seinen Dienst-PC während der Arbeitszeit auch privat genutzt zu haben. Er habe etwa drei Stunden ein Computerspiel programmiert und etwa zehn Minuten täglich E-Mails für das Logistikunternehmen seines Vaters abgewickelt.

Das Unternehmen hingegen behauptete, nach Auswertung des Keyloggers ergäben sich 5.221 empfangene und 5.835 gesendete E-Mails. Weitere konkrete Anhaltspunkte für eine unerlaubte Tätigkeit des Klägers konnte das Unternehmen nicht vorweisen.

Bloße Mutmaßungen reichen nicht aus

Das BAG erteilte dem Vorgehen des Unternehmens allerdings eine deutliche Absage: Der Einsatz eines Keyloggers, ob offen oder verdeckt, stellt auch am Arbeitsplatz einen Eingriff in das Recht auf informationelle Selbstbestimmung dar.[3]

Dieser sei nur gerechtfertigt, wenn die Voraussetzungen des § 32 BDSG vorliegen. Im konkreten Fall war das nicht so: Es gab bereits keinerlei Anhaltspunkte dafür, dass der Mitarbeiter seinen dienstlichen Computer für private Zwecke genutzt hatte. (Verdeckte) Datenerhebung und -verarbeitung aufgrund bloßer Mutmaßungen seien von § 32 BDSG nicht gedeckt.[4]

Das Unternehmen konnte sein Verhalten auch nicht damit rechtfertigen, der Betroffene habe dem Einsatz des Keyloggers nicht wie in der E-Mail angekündigt, innerhalb einer Woche widersprochen. Das Schweigen der Betroffenen stelle keine ausreichende Einwilligung nach dem BDSG dar.[5]

»Der Einsatz eines Keyloggers, ob offen oder verdeckt, stellt auch am Arbeitsplatz einen Eingriff in das Recht auf informationelle Selbstbestimmung dar.«

GÖTZ GERLACH

Allerdings hat das höchste deutsche Arbeitsgericht auch klargestellt, dass die vorübergehende Speicherung und stichprobenartige Kontrolle der Verlaufsdaten eines Internetbrowsers zulässig sein können. Denn anders könne ein Verbot der Privatnutzung des Internets nicht kontrolliert werden, was dem Arbeitgeber aber möglich sein müsse.[6]

Keine milderen Maßnahmen möglich

Der Entscheidung ist in jeder Hinsicht zuzustimmen. Sie stellt letztlich nur klar, was das

3 BAG, aaO., Rn. 24 ff.
4 BAG, aaO., Rn. 27
5 BAG, aaO., Rn. 20
6 BAG, aaO., Rn. 31 unter Hinweis auf LAG Berlin-Brandenburg 14.1. 2016 – 5 Sa 657/15

MUSTERVEREINBARUNG

Leistungs- und Verhaltenskontrolle (Auszug)

5.1 Soweit personenbezogene oder – beziehbare Daten aufgezeichnet werden, dürfen diese ausschließlich für die genannten Zwecke dieser [Vereinbarung/Weisung/Richtlinie/Betriebsvereinbarung] verwendet werden. Daten über das Benutzerverhalten dürfen ausschließlich zur Gewährleistung der Systemsicherheit, zur Optimierung und Steuerung des Systems, zur Fehleranalyse und -korrektur sowie zur kostenstellenbezogenen Abrechnung der Systemkosten verwendet werden. Die Zugriffe auf diese Funktionen bleiben auf die mit der technischen Administration des Systems betrauten Personen begrenzt; diese Personen sind gem. § 5 BDSG und § 88 TKG verpflichtet. Der Mitarbeiter willigt ein, dass Daten, die den Verdacht bezüglich eines Verstoßes gegen die vorliegende [Vereinbarung ...] begründen, an die Geschäftsleitung weitergegeben werden. Soweit strafrechtlich relevante Inhalte betroffen sind, dürfen diese Daten auch an die Strafverfolgungsbehörden weitergegeben werden.

5.2 Eine Verwendung der vorgenannten Daten zur weitergehenden Leistungs- oder Verhaltenskontrolle ist nicht gestattet. Die Regelungen der Absätze 5.3 – 5.5 bleiben hiervon unberührt.

5.3 Bei einem ausreichend begründeten Verdacht kann [falls vorhanden: ...mit Zustimmung des örtlichen Betriebsrates] eine gezielte Überprüfung eines Internet- und/oder E-Mail-Accounts stattfinden. Bei der Überprüfung ist der betriebliche Datenschutzbeauftragte hinzuzuziehen.

5.4 Maßnahmen, die den Missbrauch von Internet und/oder E-Mail verhindern oder beweisen helfen, können bei Gefahr im Verzug unmittelbar durchgeführt werden. [...]

[Quelle: Bitkom]

BAG bereits in vorangegangenen Entscheidungen zur verdeckten Videoüberwachung[7], einer Spindkontrolle ohne Wissen des Arbeitnehmers[8] oder einer Observation durch einen Detektiv[9] bereits entschieden hat. Aus den genannten Entscheidungen lassen sich folgende Grundsätze aufstellen: Die aus einer verdeckten Überwachung gewonnenen Erkenntnisse sind nur dann verwertbar, wenn vor Beginn der Maßnahme der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers bestand. Es darf keine Möglichkeit zur Aufklärung durch weniger einschneidende Maßnahmen (mehr) geben und die verdeckte Überwachung darf insgesamt nicht unverhältnismäßig sein. Bei einer Spindkontrolle ist zum Beispiel zu prüfen, ob diese nicht auch in Anwesenheit des Betroffenen vorgenommen werden kann.

Liegen die genannten Voraussetzungen vor, so sind auch »Zufallsfunde« verwertbar: der konkrete Verdacht des Diebstahls gegen bestimmte Mitarbeiter erwies sich bei einer verdeckten Videoüberwachung als unbegründet. Allerdings konnte ein vorher nicht in den Fokus geratener Arbeitnehmer des Diebstahls überführt werden.[10]

Fazit

Erkenntnisse, die der Arbeitgeber unter Verstoß gegen datenschutzrechtliche Grundsätze gewinnt, dürfen in einem arbeitsgerichtlichen Verfahren nicht verwertet werden, da die Erkenntnisse unter Verstoß gegen das grundrechtlich geschützte Recht auf informationelle Selbstbestimmung erzielt worden sind. Die Arbeitsgerichte dürfen einen entsprechenden Sachvortrag des Arbeitgebers im Prozess nicht berücksichtigen. Kündigungen oder andere Sanktionen können auf solche Erkenntnisse nicht gestützt werden.

Das gilt unabhängig davon, ob die Datenerhebung automatisiert, also unter Einsatz der Informationstechnik, einer Videoüberwachung oder auf irgendeine andere Weise, zum Beispiel im Rahmen einer Spind- oder Taschenkontrolle, stattfindet. Der Einsatz solcher Mittel ist also sehr sorgfältig vorzubereiten und abzuwägen. ◁

Dr. Götz Gerlach, Kleymann, Karpenstein & Partner mbB, Wetzlar
g.gerlach@kleymann.com
www.kleymann.com

7 BAG 21.6. 2012 – 2 AZR 153/11 und BAG 22.9. 2016 – 2 AZR 848/15
8 BAG 20.6.2013 – 2 AZR 546/12; dazu ausführlich Kiesche/Wilke, Regeln des BAG zur Mitarbeiterkontrolle, in: CuA 2/2016, 32 ff.
9 BAG 29.6.2017 – 2 AZR 597/16; siehe auch Wurzberger, Überwachung durch Privatdetektiv, in: CuA 11/2017, 35
10 BAG 22.9. 2016 – 2 AZR 848/15

ZUFALLSFUND

Die Verwertung eines »Zufallsfundes« aus einer gemäß § 32 Abs. 1 Satz 2 Bundesdatenschutzgesetz gerechtfertigten verdeckten Videoüberwachung kann nach § 32 Abs. 1 Satz 1 Bundesdatenschutzgesetz zulässig sein.
Bundesarbeitsgericht, Urteil vom 22.9.2016 – 2 AZR 848/15
(Leitsatz des Gerichts)