Der Dienstwagen im Arbeits- und Steuerrecht

von
Dr. Peter Schrader, Dr. Gunnar Straube

1. Auflage

Thematische Gliederung:

Arbeitsvertrag, Arbeitsentgelt

Verlag C.H. Beck München 2013

Verlag C.H. Beck im Internet:
www.beck.de
ISBN 978 3 406 65278 3

chung kein Beweisverwertungsverbot anzunehmen gewesen wäre. Zwar war der Arbeitgeber durch die Videoaufzeichnungen auf das strafrechtliche Verhalten des Arbeitnehmers aufmerksam geworden, die Kündigung konnte der Arbeitgeber dann aber anhand anderer Beweismittel darlegen. Damit kam einer möglichen Verletzung des allgemeinen Persönlichkeitsrechtes kein derartiges Gewicht zu, dass ein Beweisverwertungsverbot anzunehmen gewesen wäre[207].

Stimmt der Betriebsrat der Verwendung eines Beweismittels und der darauf gestützten Kündigung **zu**, nimmt das BAG regelmäßig **kein Beweisverwertungsverbot an**. Gleiches gilt, wenn dem Arbeitnehmer im Rahmen einer Anhörung die Videoaufnahme vorgelegt wird und er daraufhin den Sachverhalt gesteht. Die Theorie der „Frucht des verbotenen Baumes", welche die Verwertung von Beweisen untersagt, die aus nicht verwertbaren Beweisverwertungen hervorgehen, ist weder im Straf- noch im Zivilprozessrecht anwendbar. Räumt der Arbeitnehmer im Kündigungsschutzprozess die den dringenden Verdacht begründende Handlung ein oder stellt er sie unstreitig, indem er behauptet, die am Arbeitsplatz trotz Verzehrverbot konsumierten Lebensmittel gehörten ihm und nicht dem Arbeitgeber, ist eine Verdachtskündigung, unabhängig von der Verwertbarkeit des Videos und des Geständnisses, bereits aufgrund des unstreitigen Sachverhaltes wirksam, hier ist in der arbeitsrechtlichen Praxis genau zu differenzieren[208]. **260**

Unter Berücksichtigung dieser Maßstäbe wird im Einzelfall entschieden werden müssen, ob die erlangte Information verwertbar ist oder nicht. **261**

II. Verwertbarkeit datenschutzrechtswidrig gesammelter Daten und Informationen

Daneben stellt sich die Frage, ob der Arbeitgeber Daten und Informationen verarbeiten darf, die er datenschutzrechtswidrig, also unter Nichtbeachtung der Bestimmungen des Bundesdatenschutzgesetzes gewonnen hat. **262**

Auch mit dieser Frage hatte sich das BAG bereits zu beschäftigen. Im konkreten Fall[209] ging es darum, dass der Arbeitgeber eine **Videoüberwachung** durchgeführt hatte, ohne die gesetzlichen Bestimmungen des § 6b BDSG zu beachten. **263**

---

[207] BAG 16.12.2010 – 2 AZR 485/08, NZA 2011, 571.

[208] BAG 27.3.2003 – 2 AZR 51/02, NZA 2003, 1193; 13.12.2007 – 2 AZR 537/06, NZA 2008, 1008; 16.12.2010 – 2 AZR 485/08, NZA 2011, 571.

[209] BAG 26.8.2008 – 1 ABR 16/07, NZA 2008, 1187.

264 In der arbeitsrechtlichen Praxis werden Arbeitnehmer relativ häufig bei Pflichtverletzungen mit Hilfe von Videoüberwachung „erwischt". Insbesondere im Einzelhandel ist eine Videoüberwachung geradezu gang und gäbe, und zwar nicht nur zur Kontrolle der eigenen Arbeitnehmer, sondern natürlich auch um Ladendiebstähle durch Kunden zu vermeiden.

265 Die **Videoüberwachung öffentlich zugänglicher Räume**, wie etwa Verkaufsräume oder Schalterhallen ist in § 6b BDSG geregelt. Nach § 6b II BDSG ist die Beobachtung erkennbar zu machen. Wenn die in derartigen, der Öffentlichkeit zugänglichen Arbeitsräumen erhobenen Bilddaten einem bestimmten Arbeitnehmer zugeordnet, verarbeitet oder genutzt werden, so ist dieser über die Verarbeitung und Nutzung zu informieren. Zur Kenntlichmachung ist es erforderlich, dass der Arbeitgeber geeignete Maßnahmen trifft. Häufig wird die Tatsache der Beobachtung bereits dadurch erkennbar sein, dass die Videokamera für jedermann sichtbar ist[210]. Ob noch weitere Maßnahmen wie konkrete Hinweise, beispielsweise wie häufig anzufinden im Eingangsbereich eines Einzelhandelsgeschäftes oder unterhalb einer Kamera als Textnachricht befestigt, erforderlich sind, ist streitig. Meines Erachtens reichen offensichtlich erkennbare Kameras aus, um sicher zu gehen, sollte aber eine weitere Kenntlichmachung erfolgen.

266 Die Videoüberwachung ist nach § 6b I Nr. 3 BDSG nur dann zulässig, wenn sie zur **Wahrnehmung berechtigter Interessen** für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Solche Fälle können dann gegeben sein, wenn die Videoüberwachung zum Schutz des Betriebes und der sich dort aufhaltenden Personen erfolgt. Beispiel ist die Videoüberwachung in einer Filiale, in der sich eine Mitarbeiterin nur alleine befindet. Zulässig ist auch eine offene Überwachung mit dem Ziel, Diebstähle durch Kunden oder Mitarbeiter zu verhindern beziehungsweise zu entdecken. Bei der Abwägung der Zulässigkeit ist aber in jedem Einzelfall die Intensität der Beobachtung relevant, ob also die Mitarbeiter nur gelegentlich (z.B. beim Betreten eines öffentlich zugänglichen Flures) oder dauernd erfasst werden. Eine dauernde Überwachung dürfte eher unzulässig sein, wie das BAG im Zusammenhang mit der Überwachung in einem Briefverteilungszentrum entschieden hat[211]. Eine temporäre, natürlich angekündigte, Überwachung dürfte hingegen eher zulässig sein[212].

267 Für **nicht öffentlich zugängliche Räume**, wie z.B. Sozialräume oder ähnliches, gilt § 6b BDSG nicht, so dass es besonderer Regelungen bedarf[213]. Hier ist insbesondere das Allgemeine Persönlichkeitsrecht der Arbeitnehmer zu beachten.

---

[210] *Gola/Schomerus*, BDSG, 10. Aufl., § 6b Rn. 23.
[211] BAG 14.12.2004 – 1 ABR 34/03, NZA 2005, 839.
[212] Vgl. auch *Gola/Schomerus*, BDSG, 10. Aufl., § 6 b Rn. 20 f.
[213] BAG 26.8.2008 – 1 ABR 16/07, NZA 2008, 1187.

Daraus folgt insgesamt, dass heimliche Videoüberwachungen in öffentlich zugänglichen Verkaufsräumen wie auch bei nichtöffentlichen Arbeitsplätzen unzulässig sind, auch wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachtes ausgeschöpft sind und die Überwachung nicht unverhältnismäßig ist. **268**

§ 6b BDSG wurde 2001 in das Bundesdatenschutzgesetz eingefügt. Vor dessen Einführung wurde unter der Voraussetzung, dass der konkrete Verdacht einer strafbaren Handlung oder einer schweren Verfehlung besteht, weniger einschneidende Mittel zur Aufklärung ausgeschöpft waren und die Überwachung nicht unverhältnismäßig ist, eine Videoüberwachung in der Rechtsprechung für zulässig gehalten[214]. **269**

Das bedeutet, dass eine Videoüberwachung nur noch zulässig ist, wenn der Umstand der **Beobachtung** und die **verantwortliche Stelle kenntlich gemacht** werden und wenn dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Eine **präventive Überwachung** der Arbeitnehmer ist **nicht zulässig**. **270**

Für die Frage der Wirksamkeit der Kündigung kommt es also darauf an, ob man, wenn man die Bestimmungen des Datenschutzgesetzes nicht einhält, die dennoch gewonnenen Informationen verwerten darf oder nicht. Das BAG hat hierzu festgestellt, dass der Umstand, dass eine Partei die Kenntnis der von ihr behaupteten Tatsachen auf rechtswidrige Weise erlangt hat, **nicht notwendig** zu einem **Verbot der prozessualen Verwertbarkeit** führt. Unstreitiger Tatbestand darf verwertet werden. Ein Verwertungsverbot sei nur dann anzunehmen, wenn eine solche Sanktion unter Beachtung des Schutzzwecks der verletzten Norm zwingend geboten erscheint. In einem gerichtlichen Verfahren sei darauf Bedacht zu nehmen, dass das Gericht den Verfahrensbeteiligten in Ausübung staatlicher Hoheitsgewalt gegenüber tritt. Es sei bei der Urteilsfindung nach Art. 1 III GG an die Grundrechte gebunden und zu einer rechtsstaatlichen Verfahrensgestaltung verpflichtet. Aus dem Rechtsstaatsprinzip folge seine Pflicht zu einer fairen Handhabung des Prozess- und Beweisrechts. Daraus folge für den Zivilprozess zwar nicht, dass jede unzulässig erlangte Information prozessual unverwertbar wäre. Sie sei es aber im Einzelfall dann, wenn mit ihrer gerichtlichen Verwertung ein erneuter Eingriff in rechtlich geschützte, hochrangige Positionen der anderen Prozesspartei oder die Perpetuierung eines solchen Eingriffs verbunden wäre und dies auch durch schutzwürdige Interessen der Gegenseite nicht gerechtfertigt werden könnte[215]. **271**

---

[214] BAG 7.10.1987 – 5 AZR 116/86, NZA 1988, 92; LAG Köln 26.2.1999 – 11 Sa 795/98, BeckRS 1999, 40729.

[215] BAG 16.12.2010 – 2 AZR 485/08, NZA 2011, 571.

272 Im konkreten Fall ließ das BAG die Verwertung der Videoaufnahmen zu. Habe eine Partei den Tatsachenvortrag der Gegenseite nicht bestritten, sei ihr die Möglichkeit, sich auf die Rechtswidrigkeit der zugrundeliegenden Informationsbeschaffung zu berufen, nur dann genommen, wenn in ihrem Nichtbestreiten zugleich die Einwilligung in eine prozessuale Verwertung der fraglichen Tatsachen liegt. Im konkreten Fall hatte die unzulässige Videoüberwachung zu weiteren Beweismitteln geführt, die zu einem unstreitigen Sachverhalt geführt haben, so dass insgesamt auch die auf Basis der unzulässigen Datenerhebung gewonnenen weiteren Daten zulässig waren.

273 Das BAG nimmt damit datenschutzrechtlich eine **Güteabwägung im Einzelfall** vor. Dies bestätigt auch die jüngste BAG-Entscheidung[216]. Danach hat das Gericht zu prüfen, ob die Verwertung von heimlich beschafften persönlichen Daten und Erkenntnissen, die sich aus diesen Daten ergeben, mit dem allgemeinen Persönlichkeitsrecht des Betroffenen vereinbar ist. Bei einer Kollision des allgemeinen Persönlichkeitsrechte mit den Interessen des Arbeitgebers ist nach dem BAG durch eine Güterabwägung im Einzelfall zu ermitteln, ob das Persönlichkeitsrecht den Vorrang verdient. Das BAG kam in dem konkreten Fall zu dem Ergebnis, dass ein Beweisverwertungsverbot nicht schon aus einer Verletzung des Gebots in § 6b II BDSG, den Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen, folgt[217].

III. Bedeutung

274 Die Frage des Datenschutzes in der Verwertung von gesammelten Informationen durch den Arbeitgeber hat erhebliche **Bedeutung**, insbesondere im Rahmen von **verhaltensbedingten Kündigungen**.

1. Beispiel Internet- und E-Mail-Nutzung

275 In Unternehmen ist heutzutage der Gebrauch von E-Mails sowie des Internets Standard. Dabei kann die Nutzung von Internet und E-Mail allein auf dienstliche Belange beschränkt werden. Es kann allerdings auch erlaubt sein, dass die Nutzung zumindest teilweise privat möglich ist.

276 Als kündigungsrelevante Verletzung arbeitsvertraglicher Pflichten kommen bei der privaten Nutzung des Internets oder des Dienst-PCs ohne Erlaubnis insbesondere in Betracht:

---

[216] BAG 21.6.2012 – 2 AZR 153/11, NZA 2012, 1025.
[217] BAG 21.6.2012 – 2 AZR 153/11, NZA 2012, 1025.

– Das Herunterladen einer erheblichen Menge von Daten aus dem Internet auf betriebliche Datensysteme („unbefugtes Downloaden“), insbesondere wenn damit einerseits die Gefahr einer möglichen Vireninfizierung oder andere Störungen des betrieblichen Systems verbunden sein können oder andererseits von solchen Daten, bei deren Rückverfolgung es zu möglichen Rufschädigungen des Arbeitgebers kommen kann, beispielsweise weil strafbare oder pornographische Darstellungen heruntergeladen werden[218];
– die private Nutzung des vom Arbeitgeber zur Verfügung gestellten Internetanschlusses als solchem, weil dadurch dem Arbeitgeber möglicherweise – zusätzliche – Kosten entstehen können und der Arbeitnehmer jedenfalls die Betriebsmittel – unberechtigterweise – in Anspruch genommen hat sowie[219]
– die private Nutzung des vom Arbeitgeber zur Verfügung gestellten Internets oder anderer Arbeitsmittel während der Arbeitszeit, weil der Arbeitnehmer während des Surfens im Internet oder einer intensiven Betrachtung von Videofilmen oder -spielen zu privaten Zwecken seine arbeitsvertraglich geschuldete Arbeitsleistung nicht erbringt und dadurch seiner Arbeitspflicht nicht nachkommt und sie verletzt[220].

Bei allen diesen Fallgruppen stellen sich **Wertungsfragen,** insbesondere im Rahmen der Interessenabwägung, weil der Umfang der Internetnutzung, aber auch die besuchten Seiten, von Relevanz sein können. Arbeitsrechtlich am einfachsten zu handhaben ist die Problematik des Internetzuganges, wenn der Arbeitgeber grundsätzlich die private Nutzung untersagt. **277**

Bei der **zugelassenen Privatnutzung** ist umstritten, ob der Arbeitgeber als **„Dienstanbieter“** im Sinne der spezialgesetzlichen Vorschriften des § 3 Nr. 6 TKG und des § 2 S. 1 Nr. 1 TMG anzusehen ist oder nicht[221]. Als Dienstanbieter unterfällt er den Restriktionen dieser Gesetze. Dies gilt auch für den Fall, dass der Arbeitgeber die private Nutzungsmöglichkeit nur zu bestimmten Zeiten oder nur in einem bestimmten Umfang erlaubt und die Arbeitnehmer diese Nutzungsvorgaben überschreiten. Aufgrund der genannten telekommunikationsrechtlichen Vorschriften ist eine Kontrolle oder Einsichtnahme in die Kommunikationsdaten praktisch kaum möglich. Die Erfassung und Verwendung von Arbeitnehmerdaten, z. B. im Zusammenhang mit der Kontrolle der Nutzung elektronischer Kommunikationsmittel, ist eng begrenzt. Eine Einsichtnahme in die Daten, die mit dem Kommunikationsvorgang zusammenhängen und insbesondere in ge- **278**

[218] BAG 31.5.2007 – 2 AZR 200/06, NZA 2007, 922 m. w. N.
[219] ErfK/*Müller-Glöge*, 13. Aufl. 2013, § 626 BGB, Rn. 100.
[220] BAG 7.7.2005 – 2 AZR 581/04, NZA 2006, 98 m. w. N.
[221] ErfK/*Wank*, 13. Aufl. 2013, § 32 BDSG Rn. 26.

speicherte E-Mails, ist nach bislang herrschender Meinung praktisch kaum möglich. Eine Betriebsvereinbarung ist keine geeignete Rechtsgrundlage zur Rechtfertigung von Eingriffen in das **Fernmeldegeheimnis**, wohl aber die Einwilligung des Arbeitnehmers. Nach Auffassung des BVerfG erstreckt sich das Fernmeldegeheimnis (Art. 10 I GG, § 88 TKG) nicht auf die außerhalb eines laufenden Kommunikationsvorganges im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Inhalte und Umstände der Kommunikation. Der Schutz des Fernmeldegeheimnisses endet insoweit in dem Moment, in dem die E-Mail beim Empfänger angekommen und der Übertragungsvorgang beendet ist[222].

279 Demgegenüber ist der zugangsgesicherte Kommunikationsinhalt in dem E-Mail-Postfach eines Providers, auf das der Nutzer nur über eine Internetverbindung zugreifen kann, durch das Fernmeldegeheimnis geschützt. Im Hinblick darauf hat der VGH Kassel entschieden, dass auch im Falle der Gestattung der Privatnutzung des betrieblichen E-Mails-Systems solche E-Mails, die von Mitarbeitern nicht unmittelbar nach Eingang oder Versendung gelöscht werden, sondern im Posteingang oder -ausgang belassen oder auf den lokalen Rechnern oder anderorts im innerbetrieblichen IT-System abgelegt werden, nicht mehr dem Fernmeldegeheimnis unterliegen. Das Fernmeldegeheimnis greife bei zugelassener Privatnutzung nur hinsichtlich der Verarbeitung und Auswertung von Daten während des laufenden Telekommunikations- oder Übertragungsvorganges oder hinsichtlich der nachträglichen Auswertung von während des laufenden Kommunikationsvorganges erfassten Daten. Im Falle der Gestattung der Privatnutzung rechnet der VGH Kassel das betriebliche IT-System, also den „Herrschaftsbereich“ des Arbeitnehmers, zu[223]. In Konsequenz dieser Rechtsprechung können E-Mails von Arbeitnehmern, die der Arbeitnehmer bereits einsehen konnte und die nach Abschluss des Übertragungsvorganges auf einem Speichermedium des betrieblichen IT-Systems liegen, also unter Beachtung datenschutzrechtlicher Grundsätze (also insbesondere bei Vorliegen einer Einwilligung oder einer Betriebsvereinbarung) auch bei erlaubter Privatnutzung eingesehen werden, um zu überprüfen, ob Straftaten begangen wurden oder um die E-Mails als Beweismittel zu verwenden.

280 Ob der Arbeitnehmer den Arbeitgeber durch eine pauschale schriftliche Erklärung von der Einhaltung des Telekommunikationsgeheimnisses befreien und somit auch bei erlaubter Privatnutzung eine Nutzungskontrolle dem Arbeitgeber ermöglichen kann, ist zweifelhaft[224]. Dies dürfte allen-

[222] BVerfG 27.2.2008 – 1 BvR 370/07, NJW 2008, 822; 2.3.2006 – 2 BvR 2099/04, NJW 2006, 976.

[223] Hessischer VGH 19.5.2009 – 6 A 2672/08.Z, NJW 2009, 2470.

[224] Dies bejahen: *Haußmann/Kretz*, NZA 2005, 259 (261); *Mengel*, BB 2004, 2014; ablehnend: *Schimmelpfennig/Wenning*, DB 2006, 2290 (2292).

falls dann der Fall sein, wenn sich der betroffene Arbeitgeber im Einzelfall unter Benennung der betroffenen Kommunikation für den aktuell konkret anstehenden Kontrollvorgang eine **schriftliche Zustimmungserklärung** des Arbeitnehmers einholt. Kurzum: Eine Kontrollmöglichkeit des Arbeitgebers besteht so gut wie nicht, letztendlich ist hinsichtlich der Eingriffs- und Kontrollmöglichkeit des Arbeitgebers so gut wie alles streitig.

Dies bestätigt auch ein Urteil des LAG Berlin-Brandenburg. Danach ist **281**
ein Arbeitgeber nicht per se als Dienstanbieter im Sinne des § 88 TKG einzustufen. Dies gilt nach dem LAG auch dann, wenn der Arbeitgeber seinen Beschäftigten gestattet, einen dienstlichen E-Mail-Account auch privat zu nutzen. Folge daraus ist, dass ein arbeitgeberseitiger Zugriff auf den auch privat genutzten E-Mail-Account nicht von vorneherein ausscheidet. Das Ergebnis bestätigt das LAG auch dadurch, dass es einen Verstoß gegen das Fernmeldegeheimnis verneint, soweit die Beschäftigten bei Nutzung ihres Arbeitsplatzrechners die eingehenden E-Mails im Posteingang beziehungsweise die versandten E-Mails im Postausgang lassen. Damit bleibt letztendlich alles streitig.

Anders sieht es dann aus, wenn eine **Privatnutzung nicht erlaubt** ist[225]: **282**
Die Vorschriften des Telemediengesetzes beziehungsweise des Telekommunikationsgesetzes greifen dann definitiv nicht ein. Bei E-Mails handelt es sich bei nicht erlaubter Privatnutzung um Geschäftspost, die der Arbeitgeber einsehen kann. Ferner kann er zumindest stichprobenartig kontrollieren, ob der Arbeitnehmer die Nutzungsregelungen hinsichtlich E-Mail und Internet einhält. Bei Verstößen liegen Pflichtverletzungen vor, die zum Ausspruch von Abmahnungen und im Wiederholungsfall einer Kündigung berechtigen.

Für den Arbeitgeber ist es also exorbitant wichtig, Daten zu erlangen, **283**
die er später in einem Verfahren, entweder in Form einer Abmahnung oder in Form einer Kündigung gegen den Arbeitnehmer verwerten darf.

2. Beispiel: Bewegungskontrolle

Unter Bewegungskontrolle werden alle EDV-technischen Möglichkeiten **284**
zusammengefasst, um zu kontrollieren, wo ein Arbeitnehmer sich tatsächlich befindet. Es ist heutzutage EDV-technisch relativ einfach, mittels einer bestimmten Hard- oder Software, teilweise allein durch Nutzung des Handys zu kontrollieren, wo sich ein bestimmter Arbeitnehmer tatsächlich aufhält. Bewegungskontrolle ist ein relativ sperriges Wort. Es geht um die **Ortung des Arbeitnehmers**.

[225] ErfK/*Wank*, 13. Aufl. 2013, § 32 BDSG, Rn. 25. m.w.N.; *Gola/Schomerus*, BDSG, 10. Aufl., § 32 Rn. 18.

285 Es gibt technische Hilfsmittel, beispielsweise die GPS-Technik oder die Handyortung, nach der der Aufenthaltsort des Arbeitnehmers oder an ihn überlassene Betriebsmittel wie beispielsweise Firmenwagen oder Mobiltelefon, geortet werden können. Dass dies der **Mitbestimmung** des Betriebsrats nach § 87 I Nr. 6 BetrVG unterliegt, ist **selbstverständlich**[226]. Die Erhebung, Verarbeitung oder Nutzung der Daten über den Aufenthaltsort bedürfen für ihre Zulässigkeit einer **Rechtsgrundlage**, also insbesondere einer Einwilligung des Arbeitnehmers oder einer Betriebsvereinbarung. Bei der Gestaltung einer solchen Betriebsvereinbarung ist abzuwägen, und zwar einerseits das Interesse des Arbeitgebers an der Kontrolle der Arbeitsleistung sowie am Schutz seines Eigentums an den Betriebsmitteln, andererseits aber auch die Tatsache, dass ein genaues Bewegungsprofil des Arbeitnehmers erstellt und damit ein erheblicher Überwachungsdruck auf den Arbeitnehmer, unter Umständen auch in seiner Freizeit, ausgeübt werden kann[227]. Unter Berücksichtigung dieser Gesichtspunkte dürfte ein Einsatz technischer Hilfsmittel zur Ortung des Arbeitnehmers – bei fehlender Einwilligung – aufgrund der damit verbundenen Dauerüberwachung nur in Ausnahmekonstellationen und bei gewichtigen betrieblichen Interessen des Arbeitgebers zulässig sein, etwa bei Fahrern von Geldtransportern oder bei Sicherheitspersonal, das bestimmte Örtlichkeiten zu sichern hat.

286 Bei der Handyortung kann der Arbeitgeber seine Einwilligung zur Erhebung der Standortdaten abgeben, um den Aufenthaltsort des Handys zu erfahren, er muss aber den Arbeitnehmer hierüber unterrichten (§ 98 I TKG)[228].

287 Auch hier ist es wichtig für den Arbeitgeber, Daten zu erhalten und zu verwerten.

3. Beispiel: Zeiterfassung

288 Manipulationen bei der Zeiterfassung sind einer der klassischen Fälle der verhaltensbedingten Kündigung. Wer die Zeiterfassung manipuliert, begeht – vereinfachend gesagt – einen **Lohnbetrug**, indem er vortäuscht, entweder früher zur Arbeit gekommen oder später die Arbeit verlassen zu haben, um für diese Zeit, in der er nicht bei der Arbeit anwesend war, eine Vergütung zu erhalten.

289 Die Schutzbestimmungen des Bundesdatenschutzgesetzes greifen auch dann, wenn Daten nicht EDV-technisch erhoben oder verarbeitet werden (vgl. § 32 II BDSG)[229]. Eine manuelle **Erfassung der Arbeitszeit**, die typische „Stechuhr“ oder die Führung von Arbeitsbüchern zum Nachweis der

---

[226] ErfK/*Wank*, 13. Aufl. 2013, § 32 BDSG, Rn. 20.
[227] So bei Videoüberwachung: LAG Hamm 14.4.2011 – 15 Sa 125/11.
[228] *Gola*, NZA 2007, 1139.
[229] *Gola/Schomerus*, BDSG, 10. Aufl., § 32 Rn. 7 f.