Ausarbeitung

Erlaubnistatbestände im Arbeitnehmerdatenschutz

[redacted]

Erlaubnistatbestände im Arbeitnehmerdatenschutz

Verfasser/in: [redacted]
Aktenzeichen: WD 3 – 3000 – 007/13
Abschluss der Arbeit: 28. Januar 2013
Fachbereich: WD 3: Verfassung und Verwaltung
Telefon: [redacted]

Inhaltsverzeichnis

1. Einleitung

Gemäß § 4 Absatz 1 des Bundesdatenschutzgesetz[1] (BDSG) sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten **grundsätzlich unzulässig**.

§ 4 Absatz 1 BDSG lautet in seiner Fassung seit dem 29. August 2002 wie folgt:

*„Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind **nur zulässig**, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies **erlaubt** oder **anordnet** oder der Betroffene **eingewilligt** hat."*

Die Nutzung personenbezogener Daten ist demnach **nur zulässig**, **soweit** das **BDSG** oder eine **andere Rechtsvorschrift** dies **erlaubt** oder **anordnet** oder der betroffene Arbeitnehmer nach § 4a BDSG **eingewilligt** hat. Rechtstechnisch bedeutet dies ein **grundsätzliches Verbot** von Datenerhebungen mit Ausnahme eines gesetzlich geregelten **Erlaubnisvorbehalts**.

Die **normierten** und **ausschließlich** in der **Rechtsprechung ausgeformten** Erlaubnisvorbehalte gestatten dem Arbeitgeber einen **Zugriff** auf personenbezogene Daten und **bilden** damit einen **Sonderbereich**, der hinter dem sonst üblichen Datenschutz **zurückbleibt**.

Die Bundesregierung beabsichtigt, die Regeln zum **Arbeitnehmerdatenschutz** zukünftig durch einen noch einzufügenden Abschnitt im Bundesdatenschutzgesetz **neu und konkreter** zu fassen.[2]

2. Normierte Erlaubnistatbestände

2.1. § 28 BDSG[3] (bis 2009)

Bis zum 31. August 2009 war § 28 BDSG a.F. die bedeutendste Norm für den **Arbeitnehmerdatenschutz**. Dort war die Datenerhebung, -verarbeitung und -nutzung personenbezogener Daten für die Erfüllung eigener Geschäftszwecke geregelt. Seit dem 1. September 2009 besteht mit **§ 32 BDSG** nun jedoch eine **Spezialvorschrift für Beschäftigungsverhältnisse**, die **vorrangig anzuwenden** ist. Die **verbliebene Bedeutung** des § 28 BDSG für arbeitsrechtlich relevante Sachverhalte ist zwar **umstritten**[4], was jedoch den Arbeitnehmerdatenschutz im Verhältnis zwischen Arbeitnehmer und Arbeitgeber angeht, enthält § 28 BDSG **unstreitig** keinen für die Beantwortung der Anfrage relevanten Regelungsbereich mehr.

1 In der Fassung vom 14.01.2003, BGBl. I 2003, S. 66.

2 BT-Drs. 17/4230.

3 In der Fassung vom 14.01.2003, BGBl. I 2003, S. 66.

4 Übersicht: Franzen, in: Erfurter Kommentar zum Arbeitsrecht, 2013, BDSG, § 28, Rn. 1.

2.2. § 32 BDSG (seit 2009)

Mit der Einführung von § 32 BDSG sollte eine **allgemeine Regelung** zum Schutz von Arbeitnehmerdaten geschaffen werden. Die Normierung beabsichtigte die von der Rechtsprechung erarbeiteten Grundsätze des Arbeitnehmerdatenschutzes **abstrakt zusammenzufassen**.[5] Sie bezweckte darüber hinaus eine lediglich **vorläufige Regelung** der Rechtslage bis zum Erlass eines **Arbeitnehmerdatenschutzgesetzes**.[6] Hierin ist der Grund für die **fehlende Konkretisierung der einzelnen Erlaubnistatbestände** zu sehen.

§ 32 BDSG enthält nämlich lediglich **drei abstrakte Regelungen**, die dem Arbeitgeber ein **Zugriffsrecht** auf personenbezogene Daten seines Arbeitnehmers gestatten.[7]

2.3. Die Erlaubnistatbestände des § 32 BDSG

Der **erste Erlaubnistatbestand** (§ 32 Absatz 1 Satz 1 Variante 1 BDSG) regelt die Erhebung personenbezogener Daten zum Zwecke der **Begründung eines Arbeitsverhältnisses**. Umfasst wird damit die Gruppe der **zukünftigen** Arbeitnehmer, für die die sonst üblichen Datenschutzregeln nur in einem geringeren Maße gelten. Anwendungsfälle der Vorschrift sind Fragen des Arbeitgebers nach fachlichen Fähigkeiten, Kenntnissen und Erfahrungen von **Bewerbern**, die für die **Einstellungsentscheidung** erforderlich sind.[8]

Der **zweite Erlaubnistatbestand** (§ 32 Absatz 1 Satz 1 Variante 2 BDSG) lässt den Zugriff auf personenbezogene Daten für **Zwecke des (laufenden) Beschäftigungsverhältnisses** zu. Betroffen hiervon ist die Gruppe der **„gegenwärtigen“** Arbeitnehmer. Anwendbar ist diese Norm, wenn der Arbeitgeber sich bei seinen Beschäftigten über Umstände informiert oder Daten verwendet, um seine vertraglichen Pflichten gegenüber den Beschäftigten erfüllen zu können. Hierunter fallen beispielsweise **Pflichten im Zusammenhang mit der Lohn- und Gehaltsabrechnung**. Der Erlaubnistatbestand wird darüber hinaus auch herangezogen in Fällen, bei denen der Arbeitgeber seine **Rechte aus dem Beschäftigungsverhältnis** wahrnimmt, etwa bei der **Ausübung des Weisungsrechts** oder bei der **Kontrolle der Leistung oder des Verhaltens der Beschäftigten**. Im Rahmen dieser Eingriffe hat der Arbeitgeber stets die Grenze der **Erforderlichkeit** einzuhalten.[9]

Als einzige Konkretisierung nennt § 32 Absatz 1 Satz 2 BDSG als **Beispiel für den zweiten Erlaubnistatbestand** Maßnahmen, die zur **Verhinderung von Straftaten** oder sonstigen Rechtsverstößen, die im Zusammenhang mit dem Beschäftigungsverhältnis stehen, erforderlich sind.

Der **dritte Erlaubnistatbestand** (§ 32 Absatz 1 Satz 1 Variante 3 BDSG) umfasst die **Beendigung des Beschäftigungsverhältnisses**. Er betrifft insbesondere die **Abwicklung** eines Beschäftigungs-

5 BT-Drs. 16/13657, S. 35.

6 BT-Drs. 16/13657, S. 34.

7 Erfurth, Der „neue” Arbeitnehmerdatenschutz im BDSG, NJOZ 2009, S. 2914.

8 BT-Drs. 16/13657, S. 36.

9 Erfurth, Der „neue“ Arbeitnehmerdatenschutz im BDSG, NJOZ 2009, S 2915.

verhältnisses. Daher können sowohl Maßnahmen im Zusammenhang mit einer Abmahnung als auch mit einer Kündigung auf diesen Erlaubnistatbestand gestützt werden.[10]

Auf Grund der **lediglich abstrakten Benennung** der Erlaubnistatbestände fehlt es bisher an einer **gesetzlichen Konkretisierung**, wie sie etwa der Gesetzentwurf der Bundesregierung zur **Regelung des Beschäftigtendatenschutzes** vorsieht.[11] Es blieb daher auch nach der Einführung von § 32 BDSG bei einer **Ausgestaltung** des Arbeitnehmerdatenschutzes **durch** die **Rechtsprechung (siehe unten 4.)**.

3. Einwilligung des Arbeitnehmers gemäß § 4a BDSG

Der Arbeitnehmer kann **in den Zugriff** auf seine personenbezogenen Daten durch den Arbeitgeber **gemäß § 4a BDSG einwilligen** und somit Erlaubnisbereiche jeder Art ermöglichen.[12] Als Kernvoraussetung der Einwilligung ist erforderlich, dass die Einwilligung **freiwillig** vom Arbeitnehmer abgegeben wird.

Teilweise wird in der **Literatur** die Auffassung vertreten, das **Kriterium der Freiwilligkeit** einer Einwilligung sei **nicht geeignet**, die Arbeitnehmerdatenschutzrechte ausreichend zu wahren.[13] Begründet wird die Kritik damit, dass im Arbeitsverhältnis überwiegend ein **Machtgefälle** besteht und daher **Zweifel an der notwendigen Freiwilligkeit** der Auskünfte bestehen. Dies gelte insbesondere für das Verhältnis zwischen Arbeitgeber und einem Bewerber, der sich um die Anstellung bemüht.[14] Denn der Bewerber stehe in solchen Fällen vor der Wahl, dem Ansinnen des Arbeitgebers nachzukommen oder auf den Abschluss des Arbeitsvertrags zu verzichten.[15]

4. Einzelfallrechtsprechung zu den Erlaubnistatbeständen

Aufgrund der lediglich **abstrakten Regelung** im BDSG wurden die **Erlaubnistatbestände** im Arbeitnehmerdatenschutz, in denen die sonst üblichen Datenschutzregelungen nicht gelten, durch eine umfangreiche **Einzelfallrechtsprechung ausgeformt**.

---

10 Erfurth, Der „neue“ Arbeitnehmerdatenschutz im BDSG, NJOZ 2009, S 2916.

11 BT-Drs. 17/4230.

12 Franzen, in: Erfurter Kommentar zum Arbeitsrecht, 2013, BDSG, § 4a, Rn. 1.

13 Däubler, in: Däubler/Hjort/Schubert/Wolmerath, Arbeitsrecht, 2010, BDSG, § 4a, Rn. 3; Müller-Glöge, in: Münchner Kommentar zum BGB (MüKo), 2012, § 611, Rn. 624; Grobys, Die Überwachung von Arbeitnehmern in Call Centern, 2007, S. 321.

14 Thüsing, in: MüKo zum BGB, 2012, AGG § 11, Rn. 25; Maties, Arbeitnehmerüberwachung mittels Kamera?, NJW 2008, S. 2219; Thüsing, in: Arbeitnehmerdatenschutz und Compliance 2010, Rn. 128.

15 Müller-Glöge, in: MüKo BGB, 2012, § 611, Rn. 624.

Bei der folgenden Darstellung der Rechtsprechung soll **unterschieden** werden zwischen der Gruppe der **„zukünftigen" Arbeitnehmer** (§ 32 Absatz 1 Satz 1 Variante 1 BDSG) und der Gruppe der **„gegenwärtigen" Arbeitnehmer** (§ 32 Absatz 1 Satz 1 Variante 2 BDSG).

4.1. Gruppe der „**zukünftigen**" Arbeitnehmer

4.1.1. Psychologische Tests

Gerade bei der Anbahnung eines Arbeitsverhältnisses kann es zur Durchführung von **psychologischen** Tests kommen. Diese sind nach ständiger Rechtsprechung **zulässig**, soweit der Bewerber **einwilligt** und sich die Tests von vornherein auf solche **Eigenschaften** beschränken, die für die in Aussicht genommene Tätigkeit **von Bedeutung** sind.[16] Begründet wird die Zulässigkeit mit dem **berechtigten Interesse des Arbeitgebers** daran, ob der Bewerber den erhöhten Anforderungen eines bestimmten Berufszweiges entspricht oder nicht.[17] Derartige Tests treten vermehrt bei **Kraftfahrern**, **Piloten**, Mitarbeitern der **Feuerwehr**, der **Bundeswehr**, dem **Zoll**, der **Justiz** und der **Polizei** auf, sowie bei Bewerbern auf Führungspositionen, die ein sog. **Assessment-Center** durchlaufen.

In der **Literatur** wird teilweise das durch die Rechtsprechung eingeführte **Einwilligungskriterium** als für den Arbeitnehmerdatenschutz ungeeignet **kritisiert (siehe oben 3.)**.

4.1.2. Lichtbilder

Auch das Recht am eigenen Bild ist vom Datenschutz umfasst. Es gibt jedoch **Berufsbereiche**, bei denen die Pflicht des Arbeitnehmers besteht, sich **ablichten** zu lassen und einen **Hausausweis zu tragen**. Lichtbilder auf Werksausweisen, die die Identifikation der Mitarbeiter durch den Wachdienst erleichtern sollen, dienen der Erfüllung der Arbeitsverträge. **Begründet** wird die Zulässigkeit der Ablichtung mit dem **Sicherheitsinteresse** des Unternehmens, das die Beeinträchtigung der Persönlichkeit durch ein unerwünschtes Bild überwiegt.[18]

4.1.3. Politische, religiöse oder gewerkschaftliche Aktivität

Politische, religiöse oder gewerkschaftliche Aktivitäten eines Bewerbers fallen grundsätzlich in seinen Privatbereich und dürfen **nicht erfasst** werden. **Ausnahmen** gelten jedoch für sogenannte **Tendenzunternehmen**.[19] Tendenzunternehmen sind solche, die bestimmten ideellen (z.B. politi-

16 BVerwG 20. 12. 1963, Az. VII C 103/62, NJW 1964, S. 607**;** zusammenfassend: Riesenhuber, Die Einwilligung des Arbeitnehmers im Datenschutzrecht, RdA 2011, S. 258.

17 Exemplarisch für die Einstellung eines Piloten: LAG München, Urteil vom 20.04.2004, Az. 8 Sa 1273/03, NZA-RR 2005, S. 466.

18 Gola, in: Gola/Schomerus, Bundesdatenschutzgesetz, 11. Auflage 2012, § 32, Rn. 14.

19 Franzen, in: Erfurter Kommentar zum Arbeitsrecht, 2013, BDSG, § 32, Rn. 9.

schen, pädagogischen, religiösen) Zielsetzungen dienen.[20] Hier dürfen durch den Arbeitgeber bei **sachlicher Rechtfertigung** Datenerhebungen erfolgen.[21] So ist beispielsweise bei der Stellenausschreibung einer Gewerkschaft eine Datenerhebung bezüglich der gewerkschaftlichen Aktivität des Bewerbers zulässig, soweit es um eine zukünftige **inhaltliche** Tätigkeit geht.[22]

Diese Rechtsprechung stößt in der **Literatur** teilweise auf **Kritik.**[23] Kritiker bemängeln, dass ein im Einzelfall bestehender **direkter Zusammenhang** der Informationserhebung mit der auszuübenden Tätigkeit nur **schwer nachzuvollziehen** ist. Sie sehen darin die Gefahr einer uferlosen Ausweitung des Fragerechts bei solchen Unternehmen.

4.1.4. Gesundheitszustand, körperliche Behinderung

Datenerhebungen zum **Gesundheitszustand** sowie zu einer eventuellen **Körperbehinderung** sind zulässig, soweit **gezielt** Beeinträchtigungen der Verwendung auf dem vorgesehenen **Arbeitsplatz** ermittelt werden sollen. Begründet wird dies damit, dass der Arbeitgeber klären darf, ob beispielsweise eine Ansteckungsgefahr für Kollegen und Kunden besteht und ob eine Arbeitsunfähigkeit zum vorgesehenen Dienstantritt oder in absehbarer Zeit danach besteht.[24]

In der Literatur wird im Zuge dieses Erlaubnistatbestands darauf hingewiesen, dass bei **ungenügender Aufklärung** des Bewerbers eine **Missbrauchsmöglichkeit** durch den Arbeitgeber besteht.[25] So kann der Arbeitgeber seine Frage nach der Schwerbehinderung eines Bewerbers stets auch auf sein Interesse stützen, die **Quote nach § 71 SGB IX**[26] zu erfüllen. Der Arbeitgeber darf in diesem Fall nach der Behinderung fragen, muss dem Bewerber jedoch seine Absicht, die Schwerbehinderung als **positives Kriterium** verwenden zu wollen, mitteilen. Zweifelt der schwerbehinderte Bewerber an der tatsächlichen Intention des Arbeitgebers, **bleibt ihm das Recht, wahrheitswidrig zu antworten**. Auf dieses **„Recht zur Lüge“** müsste der Arbeitgeber ihn im Einzelfall **hinweisen**.[27]

20 Auszug aus Munzinger Online/Duden - Deutsches Universalwörterbuch, aktualisierte Online-Ausgabe. Mannheim, Leipzig, Wien, Zürich: Dudenverlag 1999-2009, abzurufen unter: https://www.munzinger.de/

21 Für den kirchlichen Kontext: BVerfGE vom 04.06.1985, Az. 2 BvR 1703/83, BVerfGE 70, 138, 139.

22 Thüsing, in: MüKo zum BGB, 2012, AGG, § 11, Rn. 21.

23 Thüsing, in: MüKo zum BGB, 2012, AGG, § 11, Rn. 25.

24 Franzen, in: Erfurter Kommentar zum Arbeitsrecht, 13. Auflage 2013, BDSG, § 32, Rn. 9.

25 Thüsing, in: MüKo zum BGB, 2012, AGG, § 11, Rn. 24.

26 § 71 SGB IX begründet die Pflicht des Arbeitgebers zur Beschäftigung schwerbehinderter Menschen.

27 Thüsing, in: MüKo zum BGB, 2012, AGG, § 11, Rn. 24.

4.2. Gruppe der **„gegenwärtigen“** Arbeitnehmer

4.2.1. Telefondaten

Der Arbeitgeber ist grundsätzlich zur **Erfassung** von **Telefondaten berechtigt**.[28] Begründet wird die Zulässigkeit der Erfassung von Gesprächsdaten, wie Tag, Uhrzeit, Beginn und Ende des Gesprächs oder Anzahl der vertelefonierten Einheiten, bei Dienstgesprächen mit dem **legitimen Interesse** des Arbeitgebers, die Kosten im Hinblick auf einen **wirtschaftlichen Einsatz** des Telefons zu kontrollieren und **Missbrauch**, zum Beispiel durch Führen unerlaubter Privatgespräche als angebliche Dienstgespräche, **zu vermeiden**. Dagegen ist die **heimliche Inhaltskontrolle** von Telefongesprächen **grundsätzlich unzulässig**.[29]

In der **Literatur** wird **teilweise** auf die besonderen **Gefahren** der modernen Datenverarbeitung und Kommunikationstechnologie und ihrer weit reichenden **Protokollierungs- und Auswertungskapazitäten** für die Privatsphäre hingewiesen.[30] Zum Schutz der Arbeitnehmer wird gefordert, eine **strengere** Bewertung an die **Erforderlichkeit** der Verarbeitung der anfallenden Daten zu stellen. Dies wird mit der Befürchtung begründet, dass sonst eine **flächendeckende** technische **Erfassung** des dienstlichen **Kommunikationsverhaltens** zu erwarten ist, die zu einer Auswertung der Daten zu anderen als Abrechnungszwecken genutzt werden kann (sog. **übermäßige Totalerfassung**).[31]

4.2.2. Call-Center

Stellt das **Telefonat** das eigentliche **Arbeitsprodukt** dar, wie es bei der Tätigkeit in einem **Call-Center** der Fall ist, so ist in gewissem Umfang auch eine **Leistungskontrolle zulässig**, indem der Arbeitgeber unter Einsatz automatisierter Anrufverteilungstechnik (ACD = Automatic Call Distribution) u.a. Zahl und Dauer der Anrufe registrieren darf und einen sogenannten **Bedienplatzreport** ermittelt.[32] Dieser beinhaltet Daten darüber, wie häufig sich der Mitarbeiter aus der Bearbeitung einkommender Gespräche ausgeschaltet oder wie viel Nachbearbeitungs- oder Abwesenheitszeiten vom Arbeitsplatz er hat.[33] Hinnehmen muss der hierüber **informierte** Callcenter-Mitarbeiter zudem das **Aufzeichnen seiner Gespräche**, wenn das aufgrund von **Dokumentationspflichten** erforderlich ist.

---

28 Franzen, in: Erfurter Kommentar zum Arbeitsrecht, 2013, BDSG, § 32, Rn. 23.

29 BVerfGE vom 19.12.1991, Az. 1 BvR 382/85, NJW 1992, S. 815; BAG Urteil vom 29.10.1997, Az. 5 AZR 508/96, NJW 1998, S. 1331. Gilt nur eingeschränkt, wenn ein Telefonat das eigentliche Arbeitsprodukt ist, siehe unten Punkt 4.2.2).

30 Hilbrans, in: Däubler/Hjort/Schubert/Wolmerath, Arbeitsrecht, 2010, BDSG, § 32, Rn. 21.

31 Hilbrans, in: Däubler/Hjort/Schubert/Wolmerath, Arbeitsrecht, 2010, BDSG, § 32, Rn. 21.

32 LAG Hamburg, Beschluss vom 26.11.2009, Az. 7 TaBV 02/09, BeckRS 2010, Nr. 69776.

33 Gola, in: Gola/Schomerus, Bundesdatenschutzgesetz, 2012, § 32, Rn. 17; BAG Beschluss vom 30.08.1995, Az. 1 ABR 4/95. BB 1995, S. 1960.

Eine Auswertung von mit seiner **Einwilligung** aufgezeichneter Gespräche zu **Zwecken des Coachings** ist im Rahmen des § 32 Abs. 1 Satz 1 BDSG und damit des **Verhältnismäßigkeitsprinzips** nur **stichprobenartig zulässig** (**zur Einwilligungsproblematik s.o.**). Ohne Information ist ein Mithören oder nur zu diesem Zweck bestimmtes Aufzeichnen zwecks Qualitätskontrolle unzulässig.[34]

4.2.3. E-Mail

Die für Telefongespräche entwickelten Grundsätze lassen sich dem Grunde nach auf **E-Mails** übertragen. Demnach ist es zulässig, wenn der Arbeitgeber auf die **äußeren Merkmale dienstlicher E-Mails** seiner Arbeitnehmer zugreift.[35] Umstritten ist die Zulässigkeit der **inhaltlichen Überprüfung** dienstlicher E-Mails.

Teilweise wird die **Auffassung** vertreten, dass die E-Mail mit dem herkömmlichen Schriftverkehr zu vergleichen und dementsprechend zu behandeln sei. Dies wird im Wesentlichen damit begründet, dass die E-Mail wie der Brief zur Kommunikation Schriftzeichen verwendet, wobei die Versendung auf elektronischem Wege keinen erheblichen Unterschied ausmache. Demzufolge sei ein Arbeitgeber befugt, E-Mails an bzw. von einer dienstlichen E-Mail-Adresse in gleicher Weise zu erfassen, wie er auch zum Lesen dienstlicher Post berechtigt sei.[36]

Dagegen wird **teilweise differenziert**, ob die E-Mail an eine **zentrale E-Mail-Adresse** der Firma bzw. einer bestimmten Firmenabteilung oder an eine E-Mail-Adresse gesendet wird, die einem **einzelnen Arbeitnehmer zugeordnet** ist. Unter ersterer Voraussetzung dürfe der Inhalt einer E-Mail vom Arbeitgeber eingesehen werden, da ein derartiger elektronischer Briefkasten ebenso wie ein physischer Briefkasten zu behandeln sei, wenn nicht die E-Mail als **persönlich bzw. vertraulich** gekennzeichnet ist.[37]

Auf der anderen Seite wird vertreten, dass die von der Rechtsprechung für die Telefonüberwachung entwickelten Grundsätze auch auf den **E-Mail Inhalt** entsprechend **übertragbar** seien.[38] Begründet wird dies damit, dass auch das Versenden von E-Mails einen - wenn auch nonverbalen - **Dialog** zwischen mindestens zwei **Kommunikationspartnern** in kürzester Zeit, wie dies für das Telefonat typisch sei, ermögliche. Es werde aufgrund der elektronischen Übermittlung die Möglichkeit eines **unmittelbareren und privateren Kontakts** geschaffen, wodurch eine quasi **gesprächsähnliche Situation** entstehe. Die Kommunikation per E-Mail sei insbesondere durch den **formlosen Informationsaustausch** geprägt, der nicht die inhaltlichen Formalitäten eines Briefwechsels annehme. Ein Arbeitnehmer rechne grundsätzlich nicht damit, dass seine E-

34 BVerfGE vom 19.12.1991, Az. 1 BvR 382/85, NJW 1992, S. 815.

35 Franzen, in: Erfurter Kommentar zum Arbeitsrecht, 2013, BDSG, § 32, Rn. 24.

36 Grosjean, Überwachung von Arbeitnehmern - Befugnisse des Arbeitgebers und mögliche Beweisverwertungsverbote, DB 2003, S. 2652; Beckschulze, Internet-, Intranet- und E-Mail-Einsatz am Arbeitsplatz, DB 2003, S. 2780.

37 Ernst, Der Arbeitgeber, die E-Mail und das Internet, NZA 2002, S. 589;

38 Mengel, Kontrolle der Kommunikation am Arbeitsplatz, BB 2004, S. 1449 m. w. N. (Fn. 61).

Mails von jemand anderen als von ihrem Empfänger geöffnet würden. Umgekehrt sei dem Arbeitnehmer beim **dienstlichen Schriftverkehr** durchaus bewusst, dass Briefe oftmals in einem **Umlaufverfahren** von mehreren Personen gelesen würden. Demzufolge stehe die E-Mail dem Telefonat näher als dem Brief, weshalb ihre inhaltliche Überwachung grundsätzlich unzulässig sei.

Eine Festlegung der Rechtsprechung auf eine der vorgenannten Ansichten ist nicht ersichtlich.[39]

4.2.4. Videoüberwachung

Sicherheitsinteressen können es für den Arbeitgeber erforderlich machen, eine Videoüberwachung durchzuführen. Die **Videoüberwachung** ist **zulässig**, soweit sie **transparent** ist und überwiegende **Sicherheitsinteressen** die Überwachung **erforderlich** machen.[40]

Zulässig ist die Videoüberwachung beispielsweise zum Schutz des Betriebes, der Dienststelle und der sich dort aufhaltenden Personen, wenn es das **geeignete** und unter dem **Verhältnismäßigkeitsprinzip schonendste Mittel** ist. Dies gilt beispielsweise für die Videoüberwachung in einem **Kernkraftwerk**, in einer **Bank**, eines **Flughafens** und eines **Bahnhofs**. Die dem Sicherheitszweck dienenden Aufnahmen dürfen dann jedoch **nicht zur Leistungsüberwachung** der Arbeitnehmer genutzt werden.

Die Videoüberwachung zum Zweck der Arbeitnehmerüberprüfung kann **zulässig** sein, wenn der Arbeitnehmer in die Überwachung **einwilligt**.

Auch hier wird die Entscheidungsfreiheit des Arbeitnehmers als Ausdruck des informationellen Selbstbestimmungsrechts von der **Literatur** auf Grund der häufig **ungleichgewichtigen Verhandlungspositionen kritisch** betrachtet **(siehe bereits oben 4.)**.[41]

Praktisch **einziger zulässiger Anlass** für eine gezielte Videoüberwachung **ohne Einwilligung** des Arbeitnehmers ist der **Verdacht einer Straftat** oder eines sonstigen Fehlverhaltens **gegen Arbeitnehmer**.[42]

4.2.5. GPS- und RFID-Systeme

Auch der Einsatz von **GPS-** (Global Positioning System) **oder RFID-** (Radio Frequency Identification) **Systemen** soll **zulässig** sein.[43] Der Einsatz solcher Systeme ermöglicht dem Arbeitgeber eine

39 Holzner, Neues zur Regelung der Nutzung von E-Mail und Internet am Arbeitsplatz?, ZRP 2011, S. 12; Raffler, Unter welchen Voraussetzungen ist die Überwachung von Arbeitnehmer E-Mails zulässig?, NZA 1997, S. 862.

40 Gola, in: Gola/Schomerus, Bundesdatenschutzgesetz, 2012, § 32, Rn. 19a; Thüsing, in: Arbeitnehmerdatenschutz und Compliance, 2010, Rn. 335.

41 Maties, Arbeitnehmerüberwachung mittels Kamera?, NJW 2008, S. 2219.

42 BAG Urteil vom 27.03.2003, Az. 2 AZR 51/02, NJW 2003, S. 3436; BAG Urteil vom 29.06.2004, Az. 1 ABR 21/03, NJW 2005, S. 313.

43 Umfassend zu diesem Thema: Gola, Datenschutz bei der Kontrolle „mobiler“ Arbeitnehmer – Zulässigkeit und Transparenz, NZA 2007, S. 1139.

intensive Überwachung der Mitarbeiter durch Angaben zur **Standortbestimmung** und gegebenenfalls weiterer Informationen. Praxisrelevant ist hierbei insbesondere die **Ortung von Dienstwagen und Mobiltelefonen**.

Hinsichtlich der **Zulässigkeitsgrenzen** gilt, dass eine Überwachung des **privaten Lebensbereichs** des Arbeitnehmers **stets ausscheidet**. Eine heimliche Überwachung kommt lediglich in ähnlichen Fällen wie bei der verdeckten Videoüberwachung in Betracht. Etwa wenn die Überwachung das **letzte** zur Verfügung stehende **Mittel zur Überführung** eines Arbeitnehmers bezüglich einer **Straftat** oder anderer schwerer Pflichtverletzungen darstellt.[44]

Einen **Sonderbereich** hiervon bildet der Bereich der **neu produzierten Lastwagen und Busse** mit **mehr als neun Plätzen**. Diese müssen auf Grund der **Verordnung (EG) Nr. 561/2006 des Europäischen Parlaments und des Rates vom 15. März 2006 zur Harmonisierung bestimmter Sozialvorschriften im Straßenverkehr** mit digitalen **Tachographen** ausgerüstet sein. Diese elektronischen Fahrtenschreiber (Black Box) speichern – gegebenenfalls in Kombination mit einer fahrergebundenen Chipkarte – unter anderem folgende Daten: **Identität des Fahrers** bei gesteckter Chipkarte, **Lenk-, Ruhe- und Arbeitszeiten**, gefahrene **Geschwindigkeit**, zurückgelegte **Wegstrecke**. Begründet wird das Aufzeichnungsrecht mit dem Schutz der Fahrer hinsichtlich der Einhaltung von **Ruhepausen** und die **Steigerung der Verkehrssicherheit** durch Verbesserung der Kontrollmöglichkeiten durch Polizei und Gewerbeaufsicht.

In der **Literatur** wird teilweise **kritisiert**[45], dass diese Daten auch vom Arbeitgeber ausgelesen und verarbeitet und **zu nicht zweckentsprechenden Auswertungen** herangezogen werden können, **ohne** dass dies durch eine **normierte Begrenzung** derzeit verhindert wird. Denn die EU-Verordnung, deren Regelungen in die **Fahrerpersonalverordnung**[46] Eingang gefunden haben und die gleichzeitig die Anwendung des **Arbeitszeitgesetz** beeinflusst, eröffnet Erlaubnistatbestände im Sinne des § 4 Absatz 1 BDSG.

[redacted] [redacted]

44 Panzer-Heemeier, in: Grobys/Panzer Stichwortkommentar Arbeitsrecht, 2012, Nr. 114, Rn. 11.

45 Gola, Datenschutz bei der Kontrolle „mobiler“ Arbeitnehmer – Zulässigkeit und Transparenz, NZA 2007, S. 1142.

46 Durch eine Änderung von § 18 der Fahrerpersonalverordnung in seiner Fassung bis zum 31.01.2008, BGBl. S. 2008, S. 54.