DATENSCHUTZ AM ARBEITSPLATZ

LÄNDERBERICHT BUNDESREPUBLIK DEUTSCHLAND

VERFASSER

Dipl.-Jur. Falk Hagedorn[1]

Das Projekt ist Bestandteil des Finanzierungsprogramms im Zusammenhang mit den Grundrechten und der Unionsbürgerschaft der Europäischen Union.

JUNI 2011

[1] Der Verfasser ist Wissenschaftlicher Mitarbeiter am Lehrstuhl für Bürgerliches Recht, Wettbewerbs- und Immaterialgüterrecht, Medien- und Informationsrecht von Prof. Dr. Andreas Wiebe, LL.M. (Virginia), am Institut für Wirtschaftsrecht der Georg-August-Universität Göttingen.

INHALT

1. EINFÜHRUNG UND HINTERGRUND

Dank der rasanten Entwicklung der modernen Informationstechnologie können Arbeitgeber heutzutage auf ein umfassendes Repertoire von Maßnahmen zur Mitarbeiterüberwachung zurückgreifen. Gleichzeitig stellen die neuen Errungenschaften des Informationszeitalters das geltende Datenschutzrecht vor eine Zerreißprobe und fordern den verstärkten Einsatz von Datenschützern. Angesichts diverser sogenannter Datenskandale in deutschen Unternehmen[2] wurde die bereits jahrzehntelang geführte öffentliche Diskussion um die Schaffung eines separaten Arbeitnehmerdatenschutzes nun auch endlich gebührend in den rechtspolitischen Fokus gerückt. Wissenschaft, Rechtsprechung und auch der Gesetzgeber sind bemüht, sich den neuen Sachverhalten zu stellen und Lösungsmöglichkeiten zu entwickeln, um ein angemessenes, mit Blick auf die Kollisionslage innerhalb des Arbeitsverhältnisses interessengerechtes Schutzniveau im Bereich des Beschäftigtendatenschutzes zu etablieren. Doch welchen Gefahren sind Beschäftigte an ihrem Arbeitsplatz ausgesetzt? Wann stoßen die Kontroll- und Überwachungsmaßnahmen der Arbeitgeber an ihre rechtlichen Grenzen? Wie gelingt die Handhabung neuer technischer Möglichkeiten wie GPS, GSM oder RFID?[3] Wie können sich einzelne Betroffene zur Wehr setzen? Welche Möglichkeiten sind dem Arbeitgeber zur Seite gestellt? Worauf ist in der Praxis zu achten und was sind gangbare Alternativen zu derzeitigen Vorgehensweisen? Diese und weitere Fragen gilt es vor dem Hintergrund eines verantwortungsvollen Umgangs mit Arbeitnehmerdaten zu beantworten. Dabei ist die Schwelle zwischen zulässiger und unzulässiger, rechtmäßiger und rechtswidriger Überwachung bisweilen sehr niedrig. Der Arbeitgeber wandelt auf einem schmalen Grad zwischen der Durchsetzung seiner berechtigten Interessen und der ungerechtfertigten Beeinträchtigung der Persönlichkeitsrechte seiner Beschäftigten.

1.1. Zielsetzung und Methodologie

Die folgenden Ausführungen sollen einen Überblick über die wesentlichen Fragen der aktuellen und geplanten Rechtslage im Bereich des Arbeitnehmerdatenschutzes verschaffen und dazu dienen, den Leser für den Bereich der Privatsphäre am Arbeitsplatz zu sensibilisieren. Gleichzeitig sollen Denkanstöße zu einem datenschutzfreundlichen Umgang mit Arbeitnehmerdaten vermittelt werden, um bestenfalls dem Missbrauch personenbezogener Daten im Arbeitsleben in gewissem Umfang Einhalt zu gebieten. Hierzu erfolgt zunächst eine Bestandsaufnahme, die essentielle Hintergrundinformationen liefert und neben dem verfassungsrechtlichen Kontext die Darstellung des Interessenkonfliktes zwischen Arbeitnehmern und -geber beinhaltet. Im Anschluss werden ausgewählte Überwachungsmaßnahmen vorgestellt und juristisch analysiert. Um den Praxisbezug herzustellen, wird der Standpunkt der Datenschutzbehörden im Hinblick auf einen verantwortungsvolleren Umgang mit Beschäftigtendaten dargestellt. Zuletzt wird aufgezeigt,

[2] Vgl. etwa die Übersichten bei Däubler, Gläserne Belegschaften?, Rn. 2a ff. sowie Schmidt, DuD 2010, 207, 207 f. und Oberwetter, NZA 2008, 609, 609.

[3] GPS = Global Positioning System; GSM = Global System for Mobile Communications; RFID = Radio Frequency.

welche Sanktionen datenschutzrechtliche Verstöße nach sich ziehen können, bevor abschließend eine Stellungnahme zu der Rechtslage erfolgt.

1.2. Grundsätzliche Konzeption des Datenschutzes in Deutschland und dogmatische Grundlagen des allgemeinen Persönlichkeitsrechts

Das deutsche Datenschutzrecht ist als spezielles Persönlichkeitsschutzrecht[4] ausgestaltet, dessen verfassungsrechtliche Grundlagen insbesondere in den Grundrechten der freien Entfaltung der Persönlichkeit (Art. 2 Abs. 1 GG) sowie des Schutzes der Menschenwürde (Art. 1 Abs. 1 GG) wurzeln[5] und dessen Behandlung Gegenstand zahlreicher Gerichtsentscheidungen war,[6] ist und bleiben wird. Das aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG abgeleitete[7] allgemeine Persönlichkeitsrecht gewährt dem Einzelnen ein umfassendes Recht auf Achtung und Entfaltung der Persönlichkeit.[8] Bezugspunkt des Schutzes ist die Privatsphäre des Grundrechtsträgers als solche.[9] Damit kommt „dem Grundrecht (…) die Aufgabe zu, Elemente der Persönlichkeit zu gewährleisten, die nicht Gegenstand der besonderen Freiheitsgarantien des Grundgesetzes sind, diesen aber in ihrer konstituierten Bedeutung für die Persönlichkeit nicht nachstehen.“[10] Das Bundesverfassungsgericht betont, dass die Notwendigkeit einer solchen lückenschließenden Funktion[11] insbesondere „auch im Blick auf moderne Entwicklungen und die mit ihnen verbundenen neuen Gefährdungen für den Schutz der menschlichen Persönlichkeit“[12] besteht. Damit kommt dem allgemeinen Persönlichkeitsrecht eine im Hinblick auf die „Effektivität eines dynamisch anzupassenden Grundrechtsschutzes“[13] entscheidende Bedeutung zu. Es steht außer Frage, dass dieser Persönlichkeitsschutz auch an Arbeitsplätzen effektiv umgesetzt werden muss.

1.3. Bestandsaufnahme zum Persönlichkeitsrechtsschutz an Arbeitsplätzen

Durch die Möglichkeiten von Staat und Privatwirtschaft, nahezu sämtliche Arbeitsbereiche vollumfassend zu kontrollieren, laufen Arbeitnehmer Gefahr, ihre Privatsphäre nicht mehr in dem erforderlichen Maße schützen zu können. Angesichts der technologischen Neuerungen der letzten Jahre ist die Gefahr des missbräuchlichen Umgangs mit personenbezogenen Daten stetig gewachsen. Von der Einsichtnahme in den E-Mail-Verkehr bis hin zu der Möglichkeit,

---

[4] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 45. Zu der historischen Entwicklung des Persönlichkeitsrechtsschutzes vgl. Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 1 ff.
[5] Kerstin Orantek, Datenschutz im Informationszeitalter, S. 51.
[6] Vgl. nur BVerfGE 27, 1 (Mikrozensus); 34, 238 (Tonband); 65, 1 (Volkszählung); 80, 367 (Tagebuch) oder aus der jüngeren Vergangenheit das Urteil zur Online-Durchsuchung vom 27. Februar 2008 (NJW 2008, 822). Vgl. hinsichtlich der höchstrichterlichen Rechtsprechung zur Verarbeitung von Arbeitnehmerdaten Gola/Wronka, Handbuch des Arbeitnehmerdatenschutzrechtes, S. 575 ff.
[7] St. Rspr. des BVerfG, vgl. nur: BVerfGE, 35, 202, 219; BVerfGE 72, 155; 82, 236, 269; 90, 263, 270.
[8] BGHZ 13, 334, 338; 26, 349, 354.
[9] BVerfGE 27, 1; Ehmann, JuS 1997, 193, 196; Schmidt, JZ 1974, 241, 243.
[10] BVerfGE 54, 148, 153; 95, 220, 241; 99, 185, 193; 101, 361, 380.
[11] BVerfGE 106, 28, 39.
[12] BVerfGE 54, 148, 152; 65, 1, 41.
[13] Di Fabio, in: Maunz/Dürig, GG, Art. 2 Rn. 127.

aussagekräftige Bewegungs- und Persönlichkeitsprofile von Mitarbeitern zu erstellen und auszuwerten, gibt es kaum noch Bereiche, in denen nicht sämtliche Arbeitsschritte zumindest theoretisch nachvollzogen werden können. So wundert es nicht, dass gerade im Arbeitsumfeld viele unterschiedliche Facetten des Persönlichkeitsrechts der Arbeitnehmer beeinträchtigt sein können.[14]

1.3.1. Der Anspruch des Arbeitnehmers auf Persönlichkeitsrechtsschutz

Geht es um Überwachungsmaßnahmen am Arbeitsplatz, sind Beschäftigte nicht rechtlos gestellt, sondern können sich gegenüber ihren Arbeitgebern auf den Persönlichkeitsrechtsschutz berufen. Über die Lehre der mittelbaren Drittwirkung der Grundrechte muss das Verfassungsrecht nicht nur von staatlicher Seite beachtet werden,[15] sondern strahlen die Grundrechte als objektive Werteordnung über die Generalklauseln[16] auch auf Arbeitsverhältnisse im Bereich der Privatwirtschaft aus.[17] Insofern droht den Arbeitnehmern die Verletzung ihrer Persönlichkeitsrechte, die im beruflichen Umfeld besonders mannigfaltig zu Tage treten können, gleich in mehrfacher Hinsicht.

1.3.1.1. Persönlichkeitsrechtsschutz über das Recht auf informationelle Selbstbestimmung[18]

Mit Blick auf den Bereich der Arbeitsverhältnisse[19] benötigt nicht nur der Staat zur Erfüllung seiner Aufgaben Daten, sondern ist auch die Privatwirtschaft auf diese angewiesen, etwa wenn es um die Abwicklung von Vertragsverhältnissen geht.[20] Losgelöst von der Art der Überwachung und Kontrolle sowie der hierbei durchzuführenden Datenverarbeitungsvorgängen ist der Arbeitgeber zunächst zur Achtung des Anspruchs der betroffenen Mitarbeiter auf Persönlichkeitsschutz in Gestalt des Rechts auf informationelle Selbstbestimmung (sog. Grundrecht auf Datenschutz) verpflichtet.[21] Hierzu führte das BVerfG aus, dass „unter den Bedingungen der modernen Datenverarbeitung (…) der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe

---

[14] Selbstverständlich erschöpft sich die Palette potentiell verletzbarer Beschäftigtenrechte nicht in der Verletzung derer Persönlichkeitsrechte. Mit Blick auf die Privatsphäre an Arbeitsplätzen konzentrieren sich die Ausführungen im Rahmen dieser Abhandlung hingegen im Wesentlichen auf diesen Bereich.

[15] Gemäß Art. 20 Abs. 3 GG besteht eine Grundrechtsbindung von Legislative, Exekutive und Judikative.

[16] Wie etwa die Generalklauseln von BDSG und BGB, Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 342.

[17] Roloff, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 5 Rn. 2; vgl. grundlegend zu der Einordnung der Grundrechte als objektive Grundentscheidung BVerfGE 7, 198, 203 ff. sowie speziell zur mittelbaren Drittwirkung des allgemeinen Persönlichkeitsrechts BVerfGE 35, 202, 219 ff.

[18] Sog. Grundrecht auf Datenschutz, Tinnefeld/Petri/Brink, MMR 2010, 727, 727. Vgl. hierzu auch die Broschüre des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/Dokumentation25JahreVolkszaehlungsurteil.pdf?__blob=publicationFile.

[19] Zur Wirkung der Grundrechte im Beschäftigungsverhältnis vgl. etwa Müller-Glöge, MüKo-BGB, § 611 Rn 278 ff.

[20] Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 7.

[21] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 45. So besteht beispielsweise nach § 75 Abs. 2 S. 1BetrVG für Arbeitgeber und Betriebsrat die Pflicht, die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern. Ferner haben sie die Selbstständigkeit und Eigeninitiative der Arbeitnehmer und Arbeitsgruppen zu fördern (§ 75 Abs. 2 S. 1 BetrVG). Das Recht auf informationelle Selbstbestimmung wurde vom BVerfG in seinem Volkszählungs-Urteil (BVerfGE 65, 1) entwickelt.

seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht (…) umfasst (wird). Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."[22] Damit kann dieser grundsätzlich selbst entscheiden, wann und innerhalb welcher Grenzen er persönliche Lebenssachverhalte offenbaren will.[23] So gibt es „unter den Bedingungen der automatischen Datenverarbeitung" (…) „kein ‚belangloses' Datum mehr."[24] Jedes personenbezogene Datum genießt den Schutz des Grundgesetzes – unabhängig davon, ob es eine sensible Information enthält oder nicht.[25] Mit Blick auf Beschäftigungsverhältnisse wird so außerhalb des Anwendungsbereichs des Bundesdatenschutzgesetzes[26] und in Bereichen, in denen keine personenbezogenen Daten gespeichert werden,[27] der Rahmen abgesteckt, innerhalb dessen der Arbeitgeber zulässigerweise Beschäftigtendaten verarbeiten darf.[28] Hiernach werden dem Einzelnen im Hinblick auf neue Technologien nicht nur Bereiche der Privatheit und Intimität freigehalten, sondern verpflichten den Arbeitgeber dazu, die Einhaltung diverser Grundsätze sicherzustellen.[29] So müssen Daten grundsätzlich unmittelbar bei dem Betroffenen erhoben werden (Grundsatz der Direkterhebung).[30] Gänzlich verboten sind neben Totalerhebungen auch umfangreiche Rasterfahndungen, da und soweit sie die Möglichkeit bieten, umfassende Persönlichkeitsbilder über den Betroffenen zu erstellen.[31] Gemäß dem Erforderlichkeitsprinzip muss der Umgang mit den personenbezogenen Daten tatsächlich notwendig sein, d.h. auf das erforderliche Maß begrenzt werden.[32] Nach dem Gebot der Zweckbindung dürfen Daten nur für bestimmte, legitime Zwecke verwendet werden.[33] Ebenso ist der Kernbereich privater Lebensgestaltung eines Menschen unantastbar.[34] So dürfen unzumutbare Intimitäten des Beschäftigten oder Selbstbezichtigungen nicht erhoben werden.[35] Darüber hinaus ist in der Regel ein offener Umgang mit den Daten angezeigt (Transparenzgebot).[36] Diesbezüglich stehen dem Einzelnen Kontrollrechte (auf Auskunft, Akteneinsicht und Benachrichtigung) sowie Korrekturrechte (auf Berichtigung, Sperrung oder Löschung) zu.[37] Nicht unberücksichtigt bleiben darf darüber hinaus die Möglichkeit der Betroffenen, Rechtsschutz über die Datenschutzinstanzen wahrzunehmen.[38]

[22] BVerfGE 65, 1, 44.
[23] BVerfGE 65, 1, 44.
[24] BVerfGE 65, 1, 44.
[25] BVerfGE 65, 1, 45.
[26] Vgl. hierzu ausführlich Gliederungspunkt 1.4.2.2.
[27] So etwa bei dem Abhören von Telefongesprächen oder im Bereich der Videoüberwachung, Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 46.
[28] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 46.
[29] Tinnefeld/Petri/Brink, MMR 2010, 727, 727.
[30] Vgl. hierzu Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 454 ff.
[31] BVerfG, NJW 2010, 833, 839; 1 BvR 370/07 unter Verweis auf BVerfGE 65, 1, 42.
[32] BVerfGE 65, 1, 44.
[33] BVerfGE 65, 1, 45.
[34] BVerfGE 109, 279, 291.
[35] BVerfGE 65, 1, 46.
[36] Tinnefeld/Petri/Brink, MMR 2010, 727, 727.
[37] Vgl. BVerfGE 65, 1, 46; Tinnefeld/Petri/Brink, MMR 2010, 727, 727 f.
[38] Vgl. BVerfGE 65, 1, 46.

1.3.1.2. Persönlichkeitsrechtsschutz über das Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme[39]

Aus der jüngeren Rechtssprechungsgeschichte ist das seitens des Bundesverfassungsgerichts in seinem Urteil zur Online-Durchsuchung entwickelte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu nennen.[40] Dieses erweitert die aus dem Recht auf informationelle Selbstbestimmung abgeleiteten, verfassungsrechtlich verbürgten Garantien.[41] Dabei wird der persönliche und sachliche Lebensbereich des Einzelnen vor Zugriffen im IT-Bereich insoweit geschützt, „als auf das informationstechnische System insgesamt zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten".[42] Heimliche Zugriffe auf informationstechnische Systeme, die ein Mitarbeiter nutzt oder nutzen darf, sind danach unzulässig.[43] Dabei soll neben der Vertraulichkeit abgespeicherter Daten auch die Steuerbarkeit von Datenverarbeitungsprozessen als solchen vom Schutz erfasst sein.[44] Das IT-Grundrecht ist subsidiär und tritt bspw. gegenüber dem Telekommunikationsgeheimnis (Art. 10 Abs. 1 GG) oder dem Recht auf informationelle Selbstbestimmung zurück.[45] Als Auffanggrundrecht hat es die Funktion, Schutzlücken zu schließen und so den Schutz der Privatsphäre weiter auszubauen und zu vereinheitlichen.[46] Hierdurch soll insbesondere den neuartigen Gefährdungen entgegengetreten werden, die durch wissenschaftlich-technischen Fortschritt und gewandelte Lebensverhältnisse auftreten können.[47]

1.3.1.3. Weitere Ausprägungen des Persönlichkeitsrechtsschutzes

Auch kann der Persönlichkeitsrechtsschutz der Beschäftigten in manchen Fällen über deren Rechte am eigenen Wort und Bild realisiert werden.[48]

1.3.1.3.1. Das Recht am gesprochenen Wort[49]

Der Schutz des gesprochenen Wortes verleiht dem Einzelnen die Befugnis, grundsätzlich selbst darüber zu bestimmen, ob ein Kommunikationsinhalt nur dem Gesprächspartner oder einem größeren Kreis zugänglich sein soll.[50] Geschützt werden soll die spontane Rede gegen die Verfestigung und jederzeitige Abrufbarkeit, mithin das Recht der Selbstbestimmung über

---

[39] Sogenanntes IT-Grundrecht, Tinnefeld/Petri/Brink, MMR 2010, 727, 727.
[40] NJW 2008, 822.
[41] Tinnefeld/Petri/Brink, MMR 2010, 727, 727.
[42] BVerfG – 1 BvR 370/07, 1 BvR 595/07 (Ziffer 201).
[43] Tinnefeld/Petri/Brink, MMR 2010, 727, 727 f. Zu dem Problem, inwieweit Beschäftigte IT-Systeme des Arbeitgebers als eigene nutzen, vgl. BVerfG, NJW 2008, 822 sowie das Fallbeispiel von Petri, in: Kartmann/Ronellenfitsch, Vorgaben des Bundesverfassungsgerichts für eine zeitgemäße Datenschutzkultur in Deutschland, S. 55 ff.
[44] BVerfG, NJW 2008, 822, 824.
[45] BVerfGE 120, 274, 302.
[46] Durner, in; Maunz/Dürig, GG, Art. 10 Rn. 59.
[47] BVerfG, NJW 2008, 822, 824 unter Rückriff auf BVerfGE 54, 148, 153; 65, 1, 41; 118, 168.
[48] Vgl. hierzu BVerfG – 1 BvR 1611/96; E 106, 28; NZA 2003, 1193, 1194; NZA 2008, 1187, 1189; Dieterich, in: ErfK zum Arbeitsrecht, Art. 2 GG, Rn. 43.
[49] Zu dem Recht am gesprochen Wort vgl. BVerfGE 34, 238, 246 f.; 54, 148, 154.
[50] BVerfGE 54, 148, 153; BGHZ 27, 284, 286; BAGE 80, 366, 376; Dieterich, in: ErfK zum Arbeitsrecht, Art. 2 GG Rn. 43.

das gesprochene Wort.[51] Hiervon sind etwa Konstellationen wie heimliche Tonbandaufnahmen[52] oder das Mithören mittels Abhöreinrichtungen[53] erfasst. In Bezug auf den Schutzumfang liegt keine Kongruenz mit dem Recht auf Privatsphäre vor.[54] Vielmehr schützt das Recht am gesprochenen Wort allgemein die Selbstbestimmung über die unmittelbare Zugänglichkeit der Kommunikation als solcher, ohne sich einerseits auf bestimmte sensitive Gesprächsinhalte oder anderseits Orte der Gesprächsführung aus dem Bereich der Privatsphäre zu beschränken.[55]

1.3.1.3.2. Das Recht am geschriebenen Wort

Als Teil des Persönlichkeitsrechts beinhaltet das Recht am geschriebenen Wort den Schutz nicht zur Veröffentlichung bestimmter privater Aufzeichnungen, mithin das sogenannte Briefgeheimnis.[56] Im Einzelnen kann das Recht am geschriebenen Wort im Arbeitsleben immer dort an Bedeutung gewinnen, wo es um den Umgang mit verkörperten Schriftstücken geht, etwa bei brieflicher Dienstkorrespondenz.[57]

1.3.1.3.3. Das Recht am eigenen Bild

Durch das Recht am eigenen Bild wird der Einzelne vor jeder Art der unbefugten Anfertigung, Verbreitung und Veröffentlichung einer bildlichen Darstellung seiner Person durch stoffgleiche Fixierung und auch vor der mittels technischer Geräte bewirkten Direktübertragung seines Erscheinungsbildes geschützt.[58] Damit hat der Betroffene ein Selbstbestimmungsrecht dergestalt, dass es grundsätzlich nur ihm obliegt, ob und wie er sich gegenüber Dritten oder der Öffentlichkeit darstellen möchte,[59] ferner, wer die Daten in Form eines Bildes speichert, nutzt und übermittelt.[60] Denkbar ist eine solche Rechtsbeeinträchtigung etwa im Bereich der Videoüberwachungsmaßnahmen. Gesetzlich geregelt ist das Recht am eigenen Bild durch die §§ 22 ff. KUG und ebenfalls durch § 201a StGB.[61]

1.3.1.3.4. Der Schutz der Vertraulichkeit der Kommunikation in Art. 10 GG

Als weiteres Schutzgut, das dem Persönlichkeitsrecht unterfällt, enthält Art. 10 GG für den Einzelnen die Gewährleistung der Vertraulichkeit der Kommunikation.[62]

Schutzbereich

Nach der Postulation in Art. 10 Abs. 1 GG sind das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis unverletzlich. Art. 10 GG enthält eine gegenüber dem Recht auf informationelle Selbstbestimmung vorrangige spezielle Freiheitsgarantie, die die allgemeine Ge-

---

[51] BGHZ 80, 25, 42; BVerfG, NJW 1992, 815, 816.
[52] BVerfG 1992, 815, 816; BAG, NJW 1998, 1331, 1332.
[53] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 48.
[54] BVerfGE 106, 28, 41.
[55] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 49. Vgl. ferner BGH, NJW 2003, 1727, 1728.
[56] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn 51.
[57] Vgl. ferner BVerfGE 80, 367 (Tagebuch).
[58] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 58.
[59] BVerfGE 63, 131 und 142; st. Rspr. des BGH, vgl. NJW 1996, 985, 986 m.w.N.
[60] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn 58.
[61] Seitz, in: Hoeren/Sieber, Handbuch Multimedia-Recht, Teil 8 Rn. 6.
[62] BVerfGE 85, 386, 398; 100, 313, 366; 115, 166, 183; Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 94

währleistung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verdrängt.[63] Art. 10 GG findet unabhängig von Inhalt oder Art und Weise des Versands eines Briefes oder der per Telekommunikation erfolgenden Informationsübermittlung Anwendung.[64] In den sachlichen Schutzbereich des Fernmeldegeheimnisses fallen alle mittels Telekommunikationseinrichtungen vorgenommenen Übermittlungen von Informationen.[65] Maßgeblicher Anknüpfungspunkt für das Fernmeldegeheimnis ist damit das Kommunikationsmedium als solches sowie die Gefahren der Vertraulichkeit, die sich gerade aus der Verwendung des Mediums ergeben.[66] Der Schutz erstreckt sich auf den gesamten Kommunikationsvorgang als solchen, d.h. auf den Zeitraum von Beginn bis Ende der Übertragung.[67] Während der Beginn des Schutzes bislang weder in Rechtsprechung noch Literatur diskutiert wurde,[68] endet der Schutz nach der Rechtsprechung des BVerfG grundsätzlich „in dem Moment, in dem die Nachricht bei dem Empfänger angekommen und der Übertragungsvorgang beendet ist."[69] Neben seiner abwehrrechtlichen Seite (Schutz gegen Kenntnisnahme des Inhalts und der näheren Umstände der Telekommunikation durch den Staat) beinhaltet das Fernmeldegeheimnis gleichzeitig den Auftrag, dass der Staat den Einzelnen auch insofern schützen muss, als private Dritte Telekommunikationsanlagen betreiben.[70]

Abgrenzung zum Recht auf informationelle Selbstbestimmung durch Kriterium der faktischen Herrschaft der Daten

Die Abgrenzung des Fernmeldegeheimnisses zum Recht auf informationelle Selbstbestimmung erfolgt danach, ob Daten außerhalb der Sphäre des Betroffenen liegen oder nicht.[71] Kommunikationsverbindungsdaten, die nach Abschluss des Übertragungsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers gespeichert sind, genießen nicht mehr den Schutz von Art. 10 Abs. 1 GG, sondern werden vielmehr durch das Recht auf informationelle Selbstbestimmung geschützt.[72] Der Schutz des Fernmeldegeheimnisses endet also, wenn der Übertragungsvorgang abgeschlossen ist und der Empfänger die faktische Herrschaft der Daten hat.[73] Im Herrschaftsbereich des Empfängers bestehen die spezifischen Gefahren der Fernkommunikation gerade nicht mehr, da dieser selbst geeignete Schutzvorkehrungen gegen einen ungewollten Datenzugriff treffen kann.[74]

[63] BVerfGE 67, 157, 171; 100, 313, 358.
[64] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 94.
[65] BVerfGE 85, 386, 396; 100, 313, 358.
[66] BVerfGE 124, 43, 54 f.
[67] Gerhards, (Grund-)Recht auf Verschlüsselung?, S. 192.
[68] De Wolf, NZA 2010, 1206, 1209.
[69] BVerfGE 115, 166, 184.
[70] BVerfG, NJW 2002, 3619, 3620; Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 95.
[71] BVerfG, NJW 2006, 976, 978.
[72] BVerfG, NJW 2006, 976, 978.
[73] BVerfG, NJW 2006, 976, 978. Gerhards, (Grund-)Recht auf Verschlüsselung?, S. 193; de Wolf, NZA 2010, 1206, 1209; Vietmeyer/Byers, MMR 2010, 807, 809.
[74] BVerfGE 115, 166, 184; BVerfG, NJW 2008, 822, 825.

1.3.2. Einschränkbarkeit der Persönlichkeitsrechte der Arbeitnehmer

Wie andere Grundrechte auch beanspruchen Persönlichkeitsrechte der Arbeitnehmer keinen absoluten Schutz, sondern sind sie einschränkbar.[75] Bei der Prüfung der verfassungsrechtlichen Rechtfertigung eines Eingriffs in die Persönlichkeitsrechte sind betroffene Grundrechte des Arbeitgebers zu berücksichtigen.[76] Somit wird der Persönlichkeitsschutz durch schützenswerte betriebliche Interessen des Arbeitgebers[77] beschränkt.[78] Eingriffe in das Persönlichkeitsrecht des Arbeitnehmers können daher durch die Wahrnehmung überwiegender schutzwürdiger Interessen des Arbeitgebers gerechtfertigt sein.[79] Diese Grundrechtskollision ist im Rahmen der Herstellung einer praktischen Konkordanz[80] verfassungsmäßig nach dem Prinzip des schonendsten Ausgleichs[81] derart in Einklang zu bringen, dass die konfligierenden Grundrechte zu optimaler Wirkung gelangen können.[82] Als betroffene Grundrechte des Arbeitgebers kommen neben der wirtschaftlichen Handlungsfreiheit (Art. 2 Abs. 2 GG) auch etwa die Berufsfreiheit (Art. 12 Abs. 1 GG) sowie die Eigentumsgarantie (Art. 14 Abs. 1 GG) in Betracht.[83] Bei der Abwägung muss darauf geachtet werden, selbst bei Vorliegen wichtiger arbeitgeberseitiger Belange (wie beispielsweise der Beachtung von Compliance-Aspekten)[84] die datenschutzrechtlichen Grundsätze in einem angemessenen Umfang zu berücksichtigen.[85] Diese Abwägungsmechanismen finden sich auch einfachgesetzlich wieder, etwa im BDSG, wo die Abwägung zwischen Interessen der Betroffen und denen der datenverarbeitenden Stellen eine zentrale Rolle für die Bewertung der Zulässigkeit des Datenumgangs spielt.

1.3.2.1. Die verschiedenen Regelungen im öffentlichen und privaten Sektor

Innerhalb des öffentlichen und privaten Sektors gibt es eine Vielzahl von Bestimmungen auf Bundes- und Landesebene, die im Zusammenhang mit der Beeinträchtigung von Persönlichkeitsrechten am Arbeitsplatz an Bedeutung gewinnen können. Im öffentlichen Bereich finden sich beispielsweise bereichsspezifische Regelungen im Melde- und Archivwesen, im Bereich des Sozialdatenschutzes oder für das Schulwesen, den Krankenhausbereich oder Sicherheitsbehörden.[86] Innerhalb des privaten Sektors wurden u.a. im Areal der IuK-Technik Bestimmungen für den Umgang mit Multimedia geschaffen, etwa im Bereich des Telekommunikationsgesetzes oder des Telemediengesetzes.[87] Herauszuheben ist, dass im häufig ein-

[75] Tinnefeld/Petri/Brink, MMR 2010, 727, 728.
[76] Tinnefeld/Petri/Brink, MMR 2010, 727, 728.
[77] Oder entsprechende Interessen der Kollegen des Mitarbeiters, Moll, Münchener Anwaltshandbuch Arbeitsrecht, § 32 BDSG Rn. 45.
[78] Moll, Münchener Anwaltshandbuch Arbeitsrecht, § 32 BDSG Rn. 45.
[79] BAG –2 AZR 485/08 Anm. 36.
[80] BVerfGE 89, 215, 232; 97, 169, 175; Hesse, Staatsrecht, Rn. 317 ff.
[81] BVerfGE 39, 1, 43.
[82] Dieterich, in: Erfurter Kommentar zum Arbeitsrecht, Einleitung Rn. 71.
[83] Tinnefeld/Petri/Brink, MMR 2010, 727, 728.
[84] Tinnefeld/Petri/Brink, MMR 2010, 727, 728: Der Begriff Compliance wird häufig als die Gesamtheit der organisatorischen Maßnahmen verstanden, die erforderlich sind, damit sich ein Unternehmen im Ganzen rechtskonform verhält.
[85] Vgl. dazu z.B. Petri, Compliance und Datenschutz, in: Schweighofer et al., Globale Sicherheit und proaktiver Staat, 2010, S. 305 ff.
[86] Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 31.
[87] Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 31.

schlägigen Regelungsbereich des Bundesdatenschutzgesetzes § 12 Abs. 4 BDSG bei Rechtsverhältnissen von Beschäftigten im öffentlichen Dienst auf bestimmte, anwendbare Vorschriften für die Privatwirtschaft verweist.[88] Telos dieser Norm ist zum einen, für alle bei der öffentlichen Hand Tätigen ein einheitliches Datenschutzrecht sicherzustellen.[89] Zum anderen soll dem Grundsatz der Gleichbehandlung von öffentlichen und nicht-öffentlichen Arbeitsverhältnissen Rechnung getragen werden.[90] Über §§ 2 Abs. 4, 1 Abs. 2 Nr. 3 BDSG erstreckt sich zudem der Anwendungsbereich des BDSG zudem auf alle privaten Arbeitgeber, so dass auch im Arbeitsverhältnis personenbezogene Daten umfassenden Schutz genießen.[91]

1.3.2.2. Das Interesse des Arbeitgebers an der Kontrolle des Arbeitnehmers

Auf Seiten des Arbeitgebers können eine Reihe nachvollziehbarer Kontrollmotive vorliegen. Grundlegend kann der Arbeitgeber etwa ein Interesse daran haben, den Betrieb beziehungsweise die Dienststelle und/oder die sich dort aufhaltenden Personen, etwa in besonderen Gefährdungsbereichen wie Kernkraftwerken, per Video zu überwachen.[92] Im Bereich der Telekommunikation könnten beispielsweise Aspekte wie die Überprüfung verlorener Arbeitszeit des Arbeitnehmers durch Nutzung von TK-Diensten, die Gefahr der Beeinträchtigung der betrieblichen EDV durch Viren oder Spam via Internet und E-Mail, die Begehung von Straftaten am Arbeitsplatz,[93] der Zugriff auf das E-Mail-Postfach des Beschäftigten im Abwesenheitsfall[94] sowie allgemein die Sicherstellung reibungsloser Betriebsabläufe[95] bis zu der Vermeidung straf- beziehungsweise zivilrechtlicher Mitverantwortlichkeiten und Auskunftspflichten gegenüber Sicherheitsbehörden[96] eine Rolle spielen.[97] Auch kann beispielsweise durch die Begehung von Straftaten im Arbeitsverhältnis ein Imageverlust auf Seiten des Arbeitgebers drohen.[98] Generell sollte daher vermieden werden, sich ohne eine vorherige Gegenüberstellung der Belange des Arbeitgebers verfrüht und unreflektiert auf die Seite des Arbeitnehmers zu stellen.

1.3.2.3. Die Grenzen der Kontrolle: Die Linie zwischen legaler Kontrolle und illegaler Überwachung

Die Einhaltung der Grenzen zulässiger Arbeitnehmerkontrollen gestaltet sich für den Arbeitgeber bisweilen recht schwierig. Maßgeblich für die Frage, ob und in welchem Umfang der

---

[88] Zu der Kritik an dieser Regelung vgl. Heckmann, in: Taeger/Gabel, BDSG, § 12 Rn. 29 mit Verweis etwa auf Dammann, in: Simitis, BDSG, § 12 Rn. 22 und Simitis, RDV, 1989, 49, 52 f. Vgl. ferner Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 216 ff. Trotz der Umsetzung der EG-Datenschutzrichtlinie ist im BDSG die grundsätzliche Trennung zwischen öffentlichem und nicht-öffentlichem Bereich beibehalten worden.

[89] Gola/Schomerus, BDSG, § 12 Rn. 7.

[90] Wedde, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 12 Rn. 14.

[91] Vgl. Weißnicht, MMR 2003, 448, 450; Mengel, BB 2004, 2014, 2015.

[92] Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutzrecht, Rn. 833.

[93] Mit der einhergehenden Gefahr der Rufschädigung des Arbeitgebers, Tinnefeld/Petri/Brink, MMR 2010, 727, 728, die unter Rückgriff auf Rechtsprechung des BAG (NJW 2006, 2939 ; E 111, 291) als Beispiel Downloads von pornografischem Bildmaterial ins Feld führen.

[94] Vietmeyer/Byers, MMR 2010, 807, 808.

[95] Vgl. Pauly/Osnabrügge, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 6 Rn. 128.

[96] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 28, 29, 198.

[97] Vgl. hierzu Holzner, ZRP 2011, 12, 13, der sich gegen das neben dem Kosten- und Gefahrenargument auch gegen das Arbeitszeitargument ausspricht.

[98] Pauly/Osnabrügge, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 6 Rn. 127.

Arbeitgeber zu der Kontrolle seiner Beschäftigten befugt ist, ist die vorzunehmende Abwägung der widerstreitenden Rechtsgüter und Interessen auf Seiten der Arbeitgeber und -nehmer unter Wahrung des Verhältnismäßigkeitsprinzips.[99] Ausgehend von der Zweckbestimmung des Arbeitsverhältnisses, dem Austausch von Arbeitsleistung gegen Zahlung von Arbeitsentgelt,[100] können sich durchaus Konstellationen ergeben, in denen ein überwiegendes berechtigtes Interesse des Arbeitgebers vorliegt. Dem technischen Fortschritt Rechung tragend, wird dem Arbeitgeber im Hinblick auf das informationelle Selbstbestimmungsrecht des Arbeitnehmers beispielsweise ein berechtigtes Interesse zugebilligt, sich durch den Einsatz technischer Hilfsmittel „diejenigen Kenntnisse, die er berechtigterweise benötigt, in wirtschaftlich sinnvoller Wiese schnell und kostengünstig zu verschaffen.“[101] Pauschale Antworten hinsichtlich der Grenzziehung zwischen legalen und illegalen Überwachungsmaßnahmen zu treffen, verbietet sich aber strikt. Die Bewertung und Analyse des datenschutzrechtlichen Kontexts hat vielmehr einzelfallabhängig unter Würdigung der Gesamtzustände zu erfolgen.[102]

1.3.2.4. Die gegenseitige Abhängigkeit innerhalb des Beschäftigungsverhältnisses

Regelmäßig handelt es sich bei Beschäftigungsverhältnissen um Dauerschuldverhältnisse.[103] Allgemein kennzeichnen sich derartige Austauschverhältnisse neben der auf Dauer angelegten Beziehung der Parteien zueinander durch eine erhöhte Pflichtenanspannung.[104] Für die Arbeitsvertragsparteien bedeutet dies, dass sie innerhalb des Beschäftigungsverhältnisses stark voneinander abhängig sind. Dies wiederum wirft einerseits die Frage auf, ob überhaupt eine Möglichkeit für den Beschäftigten besteht, wirksam in den Umgang mit seinen personenbezogenen Daten einzuwilligen. Andererseits ist fraglich, ob der Arbeitgeber effektiv imstande ist, sich des Datenmissbrauchs durch die Arbeitnehmer zu erwehren.

1.3.2.4.1. Die Einwilligung des Arbeitnehmers und das Freiwilligkeitskriterium

In Art. 2 lit. h der RL 95/46/EG[105] wird als Einwilligung der betroffenen Person jede Willensbekundung definiert, die ohne Zwang,[106] für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden.[107] Aufgrund der gestörten Vertragsparität und des hieraus resultierenden Verhandlungsungleichgewichts der Vertragsparteien,[108] mit dem eine

[99] In mehreren Entscheidungen hat sich das Bundesarbeitsgericht dieser Problematik angenommen (vgl. etwa NJW 1984, 2910; NJW 1986, 2724 oder jüngst NZA 2011, 571).
[100] BAG, NJW 86, 2724, 2726; Pauly/Osnabrügge, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 6 Rn. 43.
[101] BAG, NJW 1986, 2724, 2726.
[102] BVerfG NJW 2002, 3619, 3624 unter Rückgriff auf E 34, 238, 248 und E 80, 367, 373 ff.
[103] Müller-Glöge, in: MüKo-BGB, § 611 Rn. 16.
[104] Kramer, in: MüKo-BGB, Buch 2 Einführung Rn. 97.
[105] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personbezogener Daten und zum freien Datenverkehr v. 24. Oktober 1995, ABl. v. 23.11.1995, Nr. L 281/31.
[106] Zu den Anforderungen an die Freiwilligkeit i.S.d. § 4a Abs. 1 S. 1 BDSG vgl. BGHZ 177, 253, 254 sowie Maties, NJW 2008, 2219, 2220.
[107] 95/46/EG Art. 2 lit. h (ABlEG Nr. L 281, S. 31). Im deutschen Recht versteht man unter Einwilligung die vorherige Zustimmung, § 183 BGB, Gola/Schumerus, BDSG, § 4a Rn. 2.
[108] Gola/Schomerus, BDSG, § 4a Rn 6 f.

Zwangslage für die Arbeitnehmer einhergehen kann,[109] steht in der Arbeitspraxis das Freiwilligkeitskriterium als eines der entscheidenden Aspekte der Einwilligung in Frage.[110] Insofern ist umstritten, ob in Beschäftigungsverhältnissen eine Einwilligung überhaupt wirksam erteilt werden kann. Teile der Literatur lehnen die Einwilligungsmöglichkeit generell ab,[111] u.a. mit der Begründung, dass unzulässige Eingriffe in das Persönlichkeitsrecht des Arbeitnehmers nicht durch eine Einwilligung legitimiert werden können[112] oder dem Arbeitnehmer die nötige Unabhängigkeit fehle,[113] so dass stets die Gefahr bestünde, dass die Einwilligung unter Ausnutzung der Machtposition des Arbeitgebers erzwungen wird.[114] Dem könne auch nicht dadurch vorgebeugt werden, dass der Arbeitgeber eine Klausel aufnimmt, wonach der Arbeitnehmer erklärt, bei seiner Entscheidung über die Einwilligung nicht unter Druck gesetzt worden zu sein.[115] Anders solle sich die Situation darstellen, wenn ein Betriebsrat besteht und mit diesem die Rahmenbedingungen in einer Betriebsvereinbarung ausgehandelt werden.[116] Wiederum andere betonen, dass eine generelle, uneingeschränkte Ablehnung einer freiwilligen Einwilligung gerade nicht erfolgen könne.[117] Vorgeschlagen wird etwa, eine freie Entscheidung des Beschäftigten dann nicht zu versagen, mithin eine wirksame Einwilligung zuzulassen, wenn die Einwilligung weder erzwungen noch durch arglistige Täuschung erschlichen wurde.[118] Oft wird der Einzelne faktisch aber kein Wahlrecht bzgl. der Preisgabe seiner Daten haben.[119] Dies gilt allein schon vor dem Hintergrund, dass die Ausübung seines Berufes letztlich der Schaffung und Erhaltung der Lebensgrundlage des Beschäftigten dient.[120] Neben diesem finanziellen Aspekt kann aber auch etwa das Ansehen gegenüber dem Vorgesetzen oder Kollegen eine Rolle spielen. Ratsam ist zumindest, die Einwilligung losgelöst vom Arbeitsvertrag einzuholen, da bei einer Koppelung von Arbeitsvertrag und Einwilligung schnell der Anschein der Unfreiwilligkeit entstehen kann.[121] Ferner ist zu beachten, dass eine Beschränkung der Einwilligung einen Verstoß gegen europäisches Recht darstellt, da Art. 7 lit. a der Datenschutzrichtlinie die

---

[109] Büllesbach, in: Roßnagel, Handbuch DSR, Kap. 6.1, Rn. 14; Gola, RDV 2002, 109, 110; Simitis, in: Simitis, BDSG, § 4 a Rn. 64 f.; Backes/Eul/Guthmann/Martwich/Schmidt, RDV 2004, 156, 159; Schmidt, BB 2009, 1295, 1298; Maties, NJW 2008, 2219, 2220.

[110] Vgl. hierzu Wedde, in: Däubler/Klebe/Wedde/Weicher, BDSG, § 28 Rn. 24; Bergmann/Möhrle/Herb, BDSG, § 28 Rn. 22; Richardi/Kortstock, RdA 2005, 381, 384; Maties, NJW 2008, 2219, 2220.

[111] Siehe nur Simitis, FS Dietrich, 601, 628; ders., AUR 2001, 429, 431; Meyer, in: Taeger/Wiebe, Von AdWords bis Social Networks, 369, 372; ders., K&R 2009, 14, 16; Trittin/Fischer, NZA 2009, 343, 344; Kunst, Individualarbeitsrechtliche Informationsrechte des Arbeitnehmers, S. 77.

[112] Kunst, Individualarbeitsrechtliche Informationsrechte des Arbeitnehmers, S. 77.

[113] Hamburger DSB, 18. Tätigkeitsbericht, 197; ähnlich Meyer, K&R 2009, 14, 17.

[114] Däubler, CR 2005, 767, 770; Gola/Schomerus, BDSG, § 4 a BDSG Rn. 7.

[115] Meyer, K&R 2009, 14, 17.

[116] Gola/Schomerus, BDSG, § 4a BDSG Rn. 9 zum Verhältnis von Einwilligung und Betriebsvereinbarung. Zu Fragen des Betriebsverfassungsrechts vgl. ausführlich Roloff, in: Besgen/Prinz, § 5 Rn. 53 ff.

[117] Taeger, in: Taeger/Gabel, BDSG, §4 a Rn. 60; Hilber, RDV 2005, 143, 147; Hold, RDV 2006, 249, 252; Schuster, Die Internetnutzung als Kündigungsgrund, 2009, 135 f.; Müller, Die Zulässigkeit der Videoüberwachung am Arbeitsplatz, 2007, 36.

[118] Grimm/Schiefer, RdA 2009, 329, 337.

[119] Wohlgemuth, Datenschutz für Arbeitnehmer, Rn. 12; Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 324.

[120] Vgl. grundlegend BVerfGE 7, 377, 397 zu der Definition des Berufs, der über Art. 12 Abs. 1 GG verfassungsrechtlichen Schutz genießt (sog. Berufsfreiheit).

[121] Maties, NJW 2008, 2219, 2221.

Einwilligung als Rechtfertigungsgrund anführt.[122]

1.3.2.4.2. Arbeitgeberseitige Möglichkeiten bei missbräuchlicher Weitergabe von Daten durch Arbeitnehmer

Arbeitgeber können ein legitimes Interesse an dem Schutz ihrer Daten haben. Durch die missbräuchliche Weitergabe der Daten an Dritte drohen schwere Nachteile sowohl in ideeller als auch wirtschaftlicher Hinsicht.[123] Aus diesem Grund wird durch die Einschaltung unternehmensinterner Sicherheitsabteilungen oder Detekteien mit Abwehr- und Aufklärungsmaßnahmen versucht, die Schäden möglichst gering zu halten.[124] Faktisch ist dies kaum in dem Umfang möglich, den der Arbeitgeber vorsieht. Er hat zumindest aber die Möglichkeit, seine Daten vor unbefugtem Zugriff zu schützen, etwa durch die Implementierung effektiver Sicherheitssysteme. Letztlich wird sich der Arbeitgeber aber darauf einstellen müssen, repressiv Datenmissbrauch zu pönalisieren, indem er beispielsweise gegen Mitarbeiter über § 17 UWG vorgeht, wenn eine Verletzung von Geschäfts- oder Betriebsgeheimnissen vorliegt.

1.4. Überblick über die relevanten Rechtsquellen

Das Arbeitnehmerdatenschutzrecht schöpft aus einer Vielzahl unterschiedlicher Rechtsquellen.

1.4.1. Europarechtliche Dimension[125]

Grundlegend ist festzuhalten, dass sich die nationalen Regelungen innerhalb des europarechtlich vorgegebenen Rahmens halten müssen.

1.4.1.1. Datenschutzrichtlinien

Eine übergeordnete Bedeutung kommt in diesem Kontext der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personbezogener Daten und zum freien Datenverkehr v. 24. Oktober 1995 zu. Sie ist zum Großteil Grundlage des heutigen BDSG und kann dementsprechend als Interpretationshilfe in Zweifelsfragen dienen.[126] Auf dem Gebiet des Datenschutzes im Bereich elektronischer Kommunikation gilt die Richtlinie 2002/58/EG v. 31. Juli 2002.[127]

1.4.1.2. Charta der Grundrechte der Europäischen Union

Mit Inkrafttreten des Vertrages von Lissabon[128] hat die Charta der Grundrechte der Europäischen Union[129] rechtliche Verbindlichkeit erlangt.[130] Der europäische Grundrechtsschutz, der

---

[122] Forst, NZA 2010, 1043, 1044.
[123] Gastell, NJW 2008, 2945, 2945. Hinsichtlich der Bekämpfung von Wirtschaftskriminalität durch Unternehmen vgl. Langrock/Samson, DB 2007, 1684.
[124] Gastell, NJW 2008, 2945, 2945.
[125] Vgl. ferner zu völkerrechtlichen Aspekten Däubler, Gläserne Belegschaften?, Rn. 64 ff.
[126] Däubler, Gläserne Belegschaften?, Rn. 61. Zu den Einzelfragen vgl. Klug, RDV 2001, 266.
[127] Richtlinie des Europäischen Parlaments und des Rates vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. v. 31.7.2002, Nr. L 201/37.
[128] ABl. 2007 C 306/01.

durch den EuGH auf Grundlage der gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten sowie der EMRK[131] als Rechtserkenntnisquelle geschaffen wurde,[132] erfährt durch Art. 6 Abs. 1 UAbs. 1 EUV eine Erweiterung um einen Grundrechtskatalog, der zu den europäischen Verträgen gleichrangig ist.[133] Auf den Schutz personenbezogener Daten wird explizit in Art. 8 EUGR-Charta eingegangen.[134]

1.4.2. Weitere Rechtsquellen des nationalen Datenschutzrechts

Neben den verfassungsrechtlichen Grundsätzen[135] gewinnen mehrere andere Rechtsquellen im Bereich der Privatsphäre am Arbeitsplatz an Bedeutung.[136]

1.4.2.1. Bereichsspezifische Datenschutzregelungen

Geht es um bereichsspezifische Sachzusammenhänge auf dem Feld des Arbeitnehmerdatenschutzes, bietet das deutsche Recht – in Ermangelung eines bereichsspezifischen Arbeitnehmerdatenschutzrechtes – eine Vielzahl von Gesetzen und Rechtsverordnungen, die dieses Thema aufgreifen.[137] Aufgrund der Subsidiaritätsklausel des § 1 Abs. 3 S. 1 BDSG gehen die Rechtsvorschriften des Bundes, die den Umgang mit personenbezogenen Daten einschließlich deren Veröffentlichung regeln, dem BDSG vor.[138] Ferner bleibt die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, nach § 1 Abs. 3 S. 2 BDSG unberührt. Für das Verhältnis des besonderen Datenschutzrechtes zu den Landesdatenschutzgesetzen[139] folgt aus dem Grundsatz des Art. 31 GG (Bundesrecht bricht Landesrecht), dass das besondere Datenschutzrecht des Bundes Anwendungsvorrang genießt.[140]

---

[129] Die Grundrechtecharta der EU wurde im Dezember 2000 auf dem Gipfel von Nizza verabschiedet. Zu der Bedeutung dieser im Arbeitsrecht vgl. Däubler, AuR 2001, 380.
[130] Calliess, in: Calliess/Ruffert, EUV/AEUV, Kap. I Rn 1.
[131] Vgl. Art. 6 Abs. 3 EUV
[132] Calliess, in: Calliess/Ruffert, EUV/AEUV, Kap. I Rn 1.
[133] Vgl. Art. 6 Abs. 1 EUV.
[134] Vgl. darüber hinaus auch die in Art. 16 Abs. 2 AEUV niedergelegte Kompetenz zum Erlass von Datenschutzvorschriften auf europäischer Ebene.
[135] Vgl. hierzu bereits oben, Gliederungspunkte 1.2 und 1.3.
[136] Zu der Frage, ob der private Datenschutz in das BGB integriert werden sollte, vgl. die Auseinandersetzung zwischen Steffen und Weichert, ZRP 2009, 95.
[137] Z.B. AEntG, AFBG, AGG, AktG, AltZG, AO, ArbMedV, ArbSchG, ArbSiG, ArbZG, AÜG, AufenthG, AWG, BbiG, BetrVG, BGB, BildscharbV, BKV, DEÜV, EntgFG, EStG, FeV, FreizügG/EU, GenG, GenDG, GewO, GGBefG, GefStoffV, HeimarbeitsG, HGB, IfSG, JArbSchG, KUrhG, LadSchlG, LuftSiG, SGB 2–7, 9–10, SÜG, StGB, StPO, StVG, TKG, TMG, UrhG, VVG, ZPO, vgl. Tinnefeld/Petri/Brink, MMR 2010, 727, 728 Fn. 27. Vgl. auch die Aufzählung bei Thon, FS 25 Jahre ARGE des DAV 2006, S. 1377. Auf die Einzelheiten kann aufgrund des enormen Umfangs nicht eingegangen werden. Insofern erfolgt hier lediglich eine rein exemplarische Skizzierung, die keinerlei Anspruch auf Vollständigkeit erhebt.
[138] Schmidt, in: Taeger/Gabel, BDSG, § 1 Rn. 32.
[139] Auf die Landesdatenschutzgesetze der Bundesländer, in denen der Datenumgang in der Landes- und Kommunnalverwaltung geregelt wird (Däubler, Gläserne Belegschaften?, Rn. 49) wird nicht separat eingegangen. Die aktuellen Fassungen sind unter http://www.datenschutz.de abrufbar.
[140] Schmidt, in: Taeger/Gabel, BDSG, § 1 Rn. 32.

1.4.2.2. Datenschutz im Anwendungsbereich des Bundesdatenschutzgesetzes

Häufig greifen keine bereichsspezifischen Regelungen, so dass der Umgang[141] mit Beschäftigtendaten an den Regularien des BDSG zu messen ist.

1.4.2.2.1. § 32 BDSG als Grundsatzregelung für den Beschäftigtendatenschutz

Innerhalb des BDSG werden arbeitsrechtliche Probleme bislang nur am Rande berücksichtigt. Im Rahmen des präventiven Verbots mit Erlaubnisvorbehalt des § 4 Abs. 1 BDSG[142] enthält § 32 BDSG als Grundsatzregelung für den Beschäftigtendatenschutz in Abs. 1 diverse Erlaubnistatbestände für den Datenumgang im Arbeitsverhältnis.[143]

1.4.2.2.2. Grundtatbestand, § 32 Abs. 1 S. 1 BDSG

§ 32 Abs. 1 S. 1 BDSG enthält drei verschiedene Erlaubnistatbestände, nach denen eine Durchbrechung des Verbots mit Erlaubnisvorbehalt des § 4 Abs. 1 BDSG möglich ist. Damit der personale Anwendungsbereich des § 32 Abs. 1 S. 1 BDSG eröffnet ist, muss es sich bei dem Betroffenen um einen Beschäftigten i.S.v. § 3 Abs. 11 BDSG handeln. Der Begriff ist weit gefasst und deckt sich nicht mit dem sozialversicherungsrechtlichen Begriff des Beschäftigten, der sich allein auf Arbeitnehmer bezieht.[144] Vielmehr werden u.a. auch zur Berufsausbildung beschäftigte Personen, arbeitnehmerähnliche Personen, Bewerber sowie Personen, deren Beschäftigungsverhältnis beendet ist, erfasst.[145] Nach § 32 Abs. 1 S.1 BDSG kann sich die Zulässigkeit des Umgangs mit Beschäftigtendaten aus Zwecken des Beschäftigungsverhältnisses ergeben. Zulässige Beschäftigungszwecke in diesem Sinne können sich aus gesetzlichen Vorschriften, Kollektivvereinbarungen sowie dem Arbeitsvertrag ergeben.[146] Entgegen des Wortlauts sollen neben den konkret im Gesetz benannten Zwecken[147] auch alle übrigen Zwecke des Beschäftigungsverhältnisses zulässig sein.[148] Mit Blick auf den Wortlaut des § 32 Abs. 1 S. 1 BDSG müssen die Anforderungen an den Datenumgang dem Erforderlichkeitskriterium genügen.[149] Gemäß dem gesetzgeberischen Willen[150] wird das Merkmal der Erforderlichkeit weitestgehend in dem Sinne verstanden, dass eine Verhältnismäßigkeitsprü-

---

[141] Unter Umgang mit Daten versteht man die Erhebung, Verarbeitung und Nutzung dieser, Zöll, in: Taeger/Gabel, § 32 Rn. 1. Vgl. zur Terminologie im Einzelnen die Legaldefinitionen in § 3 Abs. 1 BDSG.

[142] Generell kann sich die Zulässigkeit des Umgangs mit personenbezogenen Daten neben der Einwilligung des Betroffenen, aus den gesetzlichen Erlaubnistatbeständen des BDSG oder Rechtsvorschriften, die einen bestimmten Datenumgang erlauben oder anordnen (hierunter fallen etwa Betriebsvereinbarungen und Tarifverträge, vgl. Franzen RdA 2010, 257, 259 f.) , ergeben. Auf §§ 227 BGB, §§ 32, 34 StGB, die u.a. ebenfalls Rechtsvorschriften in diesem Sinne darstellen sollen (vgl. etwa BAG, NJW 2005, 313, 316 sowie Richardi/Korstock, RdA 2005, 381, 382; zweifelnd Bayreuther, NZA 2005, 1038, 1040; im Ergebnis ebenso Grosjean, DB 2003, 2650, 2651), wird nicht gesondert eingegangen.

[143] Zöll, in: Taeger/Gabel, BDSG, § 32 Rn. 1. Zu der Entstehungsgeschichte vgl. Schmidt, RDV 2009, 193, 200.

[144] Zöll, in: Taeger/Gabel, BDSG, § 32 Rn. 13.

[145] BT-Drs. 16/13657, S. 27; vgl. § 3 Abs. 11 BDSG.

[146] Gola/Schomerus, BDSG, § 28 Rn. 14 f.; Simitis, in. Simitis, BDSG, § 28 Rn. 101 ff.; Lembke, in: Henssler/Willemsen/Kalb, Arbeitsrecht Kommentar, BDSG Einführung Rn. 41; Zöll, in: Taeger/Gabel, BDSG, § 32 Rn. 15.

[147] D.h. Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses.

[148] Zöll, in: Taeger/Gabel, BDSG, § 32 Rn. 17, Thüsing, NZA 2009, 865, 867.

[149] Kritisch zur Ablösung des in § 28 Abs. 1 Nr. 1 BDSG a.F. in Bezug auf Beschäftigungsverhältnisse verwendeten Rechtsbegriff der Dienlichkeit durch das Erforderlichkeitskriterium: Thüsing, NZA 2009, 867.

[150] BT-Drs. 16/13657, S. 35 f. unter Bezugnahme auf die Rechtsprechung des BAG (BAGE 46, 98 = NZA, 1984, 321; BAG, NZA 1985, 57; BAGE, 81, 15 = NZA 1996, 536, 528; BAGE 53, 226 = DB 1987, 1048).

fung vorzunehmen ist.[151] Dabei muss zunächst geprüft werden, ob auf den Umgang mit personenbezogenen Daten verzichtet werden kann oder zumindest ein für die Zweckerreichung gleich geeignetes, aber weniger intensives Mittel zur Verfügung steht.[152] In einem zweiten Schritt ist danach zu fragen, ob der Umgang mit den Beschäftigtendaten nach Abwägung der Interessen von Arbeitnehmer und -geber für den Beschäftigungszweck angemessen ist.[153] Der Erforderlichkeitsprüfung ist dabei ein subjektiver Maßstab zugrunde zu legen, mithin muss sie am konkreten Einzelfall und unter Würdigung der konkreten Gegebenheiten erfolgen.[154]

1.4.2.2.3. Aufdeckung von Straftaten, § 32 Abs. 1 S. 2 BDSG

In Relation zu dem Grundtatbestand stellt § 32 Abs. 1 S. 2 BDSG[155] schärfere Anforderungen, wenn die Zulässigkeit des Datenumgangs zur Aufdeckung von Straftaten[156] in Frage steht. Von der gesetzlichen Formulierung sind neben Straftaten, die im Zusammenhang mit der Arbeitsaufgabe verübt werden auch solche erfasst, die nur bei Gelegenheit der Beschäftigung begangen werden.[157] Rein vertragsbrüchiges oder ordnungswidriges Verhalten fällt hingegen in den Anwendungsbereich von § 32 Abs. 1 S. 1 BDSG, der sonstige Rechtsverstöße regelt.[158] Mit Blick auf den letzten Halbsatz der Norm dürfen i.R.d. vorzunehmenden Interessenabwägung insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sein. Laut Gesetzesbegründung ist unter dem Anlass der Datenerhebung einerseits Art und Schwere der Straftat sowie anderseits die Intensität des Verdachts zu verstehen.[159] Je stärker der Verdacht wiegt und je schwerer die Verletzung oder Gefährdung des Rechtsguts ist, desto intensiver darf in das Persönlichkeitsrecht der Beschäftigten eingegriffen werden.[160] Eingriffsintensive Maßnahmen müssen aber ultima ratio sein.[161] Hinsichtlich der Gewichtung der gegenläufigen Interessen wird vorgeschlagen, weitestgehend auf die Rechtsprechung des BVerfG[162] zurückzugreifen.[163] Bei staatlichen informationsbezogenen Grundrechtseingriffen hängt danach das Gewicht des Eingriffs unter anderem davon ab, welche Inhalte von dem Eingriff erfasst werden, insbesondere welchen Grad an Persönlichkeitsrelevanz die betroffenen Informationen je für sich und in ihrer Verknüpfung mit anderen aufweisen und auf welchem Wege diese Inhalte erlangt werden.[164] Ferner richtet sich der Umfang der Beeinträchtigung des Rechts auf informationelle Selbstbestimmungen nach den drohenden oder nicht

---

[151] Schmidt, RDV 2009, 193, 198 f.; Zöll, in: Taeger/Gabel, BDSG, § 32 Rn. 17.
[152] Zöll, in: Taeger/Gabel, BDSG, § 32 Rn. 17.
[153] Zöll, in: Taeger/Gabel, BDSG, § 32 Rn. 17.
[154] Zöll, in: Taeger/Gabel, BDSG, § 32 Rn. 17.
[155] Vom Wortlaut her ist die Regelung § 100 Abs. 3 S. 1 TKG nachempfunden; inhaltlich entspricht sie den Anforderungen, die seitens der Rechtssprechung an eine verdeckte Überwachung von Arbeitnehmern gestellt wurden, Thüsing, NZA 2009, 865, 868 unter Rückgriff auf BAG, NZA 2003, 1193 und NZA 2008, 1187.
[156] Z.B. Diebstahl und Korruptionsfälle, BT-Drs. 16/13657, S. 36. Zu der Frage, in welchem Verhältnis § 32 Abs. 1 S. 1 und S.2 BDSG stehen, siehe Franzen, RdA 2010, 257, 260 f.
[157] Deutsch/Diller, DB 2009, 1462, 1462.
[158] BT-Drs. 16/13657, S. 36; Schmidt, RDV 2009, 193, 195 zu den problematischen Aspekten der Regelung.
[159] BT-Drs. 16/13657, S. 36.
[160] Zöll, in: Taeger/Gabel, BDSG, § 32 Rn. 46.
[161] Zöll, in: Taeger/Gabel, BDSG, § 32 Rn. 46.
[162] BVerfGE 115, 320 (Rasterfahndung II).
[163] So Thüsing, NZA 2009, 865, 868, der die wechselseitigen Austauschbeziehungen der Arbeitsvertragsparteien in den Mittelpunkt der Bewertung rückt und ferner auf Hillgruber, JZ 2007, 209 und Bausback, NJW 2006, 1922 verweist.
[164] BVerfGE 115, 320, 347 unter Rückgriff auf E 100, 313, 376; 107, 299, 318 ff.; 109, 279, 353.

grundlos befürchteten Konsequenzen der Datenerhebung für den Betroffenen.[165] Die Heimlichkeit einer Maßnahme führt dabei zur Erhöhung ihrer Intensität.[166]

1.4.2.2.4. § 32 Abs. 2 BDSG als Erweiterung für manuelle Datenverarbeitung

Nach § 32 Abs. 2 BDSG findet Abs. 1 auch auf die manuelle Datenverarbeitung Anwendung.[167] Gemäß der Gesetzesbegründung werden insofern die Grundsätze des Datenschutzes im Arbeitsverhältnis aufgegriffen.[168] Dadurch unterfallen jegliche Datensammlungen mit Arbeitnehmerbezug (z.B. Aufzeichnungen von Führungskräften und Interviewern aus Bewerbungs- und Jahresführungsgesprächen sowie sämtliche Notizen zum Leistungsverhalten) dem Schutzbereich des § 32 Abs. 1 BDSG.[169]

1.4.2.2.5. Konkurrenzverhältnis zu § 28 BDSG[170]

Bislang unzureichend geklärt ist das Verhältnis von § 32 BDSG zu § 28 BDSG. Nach der Gesetzesbegründung sollten durch die Neuregelung des § 32 BDSG die seitens der Rechtsprechung entwickelten Grundsätze des Beschäftigtendatenschutzes nicht geändert, sondern lediglich zusammengefasst werden.[171] Insofern wird teilweise vorgeschlagen, überwiegend auf die zu § 28 BDSG entwickelten Grundsätze zurückzugreifen.[172] Laut Gesetzesbegründung konkretisiert[173] und verdrängt § 32 BDSG für Zwecke des Beschäftigungsverhältnisses § 28 Abs. 1 S. 1 Nr. 1 BDSG[174] und stellt mithin eine Spezialregelung (lex specialis) dar.[175] Ebenso werde § 28 Abs.1 S. 2 BDSG verdrängt.[176] Weiterhin neben § 32 BDSG anwendbar sollen § 28 Abs. 3 S. 1 Nr. 1 BDSG und § 28 Abs. 1 S. 1 Nr. 2 BDSG sein.[177] Im Einzelnen ist hier aber vieles offen, so dass keine Rechtsklarheit besteht.[178]

---

[165] BVerfGE 115, 320, 347 unter Rückgriff auf E 100, 313, 376; 109, 279, 353.
[166] BVerfGE 115, 320, 353 unter Rückgriff auf E 107, 299, 321; NJW 2006, 976, 981.
[167] Vgl. zu der Ausweitung des Anwendungsbereichs des BDSG auch § 8 Abs. 1 BewachV.
[168] BT-Drs. 16/13657, S. 37 unter Rückgriff auf BAGE 54, 365; 119, 238.
[169] Wank, in: ErfK zum Arbeitsrecht, § 32 BDSG Rn. 2.
[170] Soweit unter Gliederungspunkt 2. eine rechtliche Auseinandersetzung mit der Zulässigkeit in Frage stehender Überwachungsmaßnahmen erfolgt, ist der Leser angehalten, sich ergänzend das Verhältnis von § 32 BDSG zu § 28 BDSG in das Gedächtnis zu rufen.
[171] BT-Drs. 16/13657, S. 35.
[172] Wellhöner/Byers, BB 2009, 2310, 2311. Kritisch: Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 58 ff.
[173] Dies widerlegend: Thüsing, NZA 2009, 865, 867.
[174] BT-Drs. 16/13657, S. 34.
[175] Zöll, in Taeger/Gabel, BDSG, § 32 Rn. 5.
[176] BT-Drs. 16/13657, S. 34. Dies kritisieren etwa Vogel/Glas, DB 2009 1747, 1750 f. Thüsing, (NZA 2009, 865, 869) spricht sogar von einem „gesetzgeberischen Motivirrtum“ und geht (ebenso wie im Ergebnis Däubler, Gläserne Belegschaften?, Rn. 186) von der Anwendbarkeit des § 28 Abs. 1 S. 2 BDSG aus. Andere (Deutsch/Diller, DB 2009, 1462, 465) befürchten, bestimmte Anwendungen im Zusammenhang mit Arbeitsverhältnissen zukünftig nicht mehr durchführen zu können sowie, dass Probleme im Hinblick auf den Umgang mit der Norm in der Praxis auftreten.
[177] So zumindest die Gesetzesbegründung, BT-Drs. 16/13657, S. 35. Dies ist umstritten. Vgl. hierzu Thüsing, NZA 2009, 865, 869 sowie Grentzenberg/Schreibauer/Schuppert, K&R 2009, 535, 539 f. und Zöll, in: Taeger/Gabel, BDSG, § 32 Rn. 6.
[178] So auch Thüsing, NZA 2009, 865, 869.

1.4.2.3. Ausblick: Neuregelung eines Beschäftigtendatenschutzes, §§ 32-32l BDSG n.F.

Seit Einführung des § 32 BDSG beschäftigt sich die Literatur häufig mit der Analyse der Norm.[179] Im Zusammenhang mit der geäußerten Kritik wurde sogar von einer „anlassbezogene(n), symbolische(n) Gesetzgebung" gesprochen, „die allzu hastig reagiert und damit mehr einer politischen als sachlichen Logik folgt."[180] Dem vielfach geäußerten Wunsch nach einer umfassenden Kodifizierung eines Arbeitnehmerdatenschutzrechtes[181] folgend, hat die Bundesregierung am 25.10.2010 den „Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes"[182] beschlossen.[183] Zu der Stellungnahme des Bundesrates vom 5.11.2010[184] nahm wiederum die Bundesregierung am 15.12.2010 Stellung.[185] Zuletzt hat der Bundestag am 25.2.2011 über den Gesetzesentwurf der Bundesregierung in erster Lesung beraten.[186] Am 23.5.2011 wurde im Rahmen einer öffentlichen Sachverständigenanhörung im Innenausschuss des Bundestages der Regierungsentwurf kontrovers diskutiert. Neben dem Entwurf der Bundesregierung liegen zwei weitere Gesetzesentwürfe der SPD-Fraktion[187] sowie von Bündnis 90/Die Grünen[188] vor, die ebenfalls am 23.5.2011 angehört wurden. Der Gesetzesentwurf der Bundesregierung sieht vor, kein eigenes Arbeitnehmerdatenschutzgesetz zu erlassen, sondern den Umgang mit personenbezogenen Daten von Beschäftigten lediglich im BDSG zu kodifizieren.[189] So soll der aktuelle § 32 BDSG wie folgt durch die §§ 32-32l BDSG n.F. ersetzt werden:

- § 32 Datenerhebung vor Begründung eines Beschäftigungsverhältnisses
- § 32a Ärztliche Untersuchungen und Eignungstests vor Begründung eines Beschäftigungsverhältnisses
- § 32b Datenverarbeitung und -nutzung vor Begründung eines Beschäftigungsverhältnisses

---

[179] Vgl. allein die Beiträge von Albrecht/Maisch, DSB 3/2010, 11.; Behling, BB 2010, 892; Beisenherz/Tinnefeld, DuD 2010, 221; Forst, RDV 2010, 8; Kamp/Körffer, RDV 2010, 72; Kramer, DSB 5/2010, 14; Salvenmoser/Hauschka, NJW 2010, 331; Kort, MMR 2011, 294 sowie die Abhandlungen bei Däubler, Gläserne Belegschaften?, Rn. 183 und Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 847 ff.

[180] Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 77.

[181] So geht die wissenschaftliche Auseinandersetzung weit zurück, vgl. etwa Simitis, Schutz von Arbeitnehmerdaten, Regelungsdefizite, Lösungsvorschläge, Gutachten erstattet im Auftrag des Bundesministers für Arbeit und Sozialordnung, 1981 oder Zöllner, Daten- und Informationsschutz im Arbeitsverhältnis. Vgl. ferner Fleck, BB 2003, 306 sowie Grobys, BB 2003, 682 und Simitis, RdA 2003, Sonderbeilage zu Heft 5, S. 43.

[182] BT-Drs. 535/10.

[183] Im Vorfeld hat das Bundesministerium des Innern (BMI) bereits mehrere Referentenentwürfe veröffentlicht (vgl. etwa Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes vom 28.5.2010, abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_Beschaeftigtendatenschutz.pdf?__blob=publicationFile), die auf Kritik gestoßen sind.

[184] BR-Drs. 535/10(B).

[185] BT-Drs. 17/4230.

[186] Zu den Stellungnahmen der Redner im Bundestag vgl. Wybitul, MMR-Aktuell 2011, 315091.

[187] BT-Drs. 17/69.

[188] BT-Drs. 17/4853.

[189] Hierin besteht die Umsetzung der Vereinbarung aus dem Koalitionsvertrag der Regierungsparteien, vgl. Wachstum. Bildung. Zusammenhalt, Koalitionsvertrag zwischen CDU, CSU und FDP, S. 106.

- § 32c Datenerhebung im Beschäftigungsverhältnis
- § 32d Datenverarbeitung und -nutzung im Beschäftigungsverhältnis
- § 32e Datenerhebung ohne Kenntnis des Beschäftigten zur Aufdeckung und Verhinderung von Straftaten und anderen schwerwiegenden Pflichtverletzungen im Beschäftigungsverhältnis
- § 32f Beobachtung nicht öffentlich zugänglicher Betriebsstätten mit optisch-elektronischen Einrichtungen
- § 32g Ortungssysteme
- § 32h Biometrische Verfahren
- § 32i Nutzung von Telekommunikationsdiensten
- § 32j Unterrichtungspflichten
- § 32k Änderungen
- § 32l Einwilligung, Geltung für Dritte, Rechte der Interessenvertretungen, Beschwerderecht, Unabdingbarkeit.

1.4.3. Das Konzept der Selbstregulierung

Selbstregulierung[190] kann als Mittel der Absicherung von Datenschutzbelangen dienen.[191] So gibt Art. 27 EU-DSRL[192] etwa den Rahmen für Verhaltensregeln (Codes of Conduct) von Verbänden verarbeitender Stellen vor, der mit Einführung des § 38a BDSG in deutsches Recht umgesetzt wurde.[193] Das Telos von § 38a BDSG besteht laut der Gesetzesbegründung u.a. in der Vereinheitlichung interner Verhaltensregeln zur Förderung und Durchführung datenschutzrechtlicher Regelungen.[194] Die Verhaltensregeln werden dabei im Vorfeld von der Aufsichtsbehörde geprüft (Prinzip der regulierten Selbstregulierung).[195] Codes of Conduct stehen nicht auf einer Stufe mit Rechtsnormen, sind mithin grundsätzlich unverbindlich.[196] Werden sie hingegen durch die Aufsichtsbehörden gebilligt, entfalten sie eine Bindungswirkung nach dem Grundsatz der Selbstbindung der Verwaltung.[197] Obwohl durch die Etablierung von Verhaltensregeln einerseits Rechtssicherheit bzgl. branchentypischer Datenflüsse geschaffen[198] und andererseits die Transparenz der Art des Datenumgangs für die Betroffenen erhöht wird,[199] hat sich in Deutschland das Modell der Selbstregulierung im Bereich des Datenschutzrechtes bislang nicht in dem Maße durchsetzen können, wie dies bisweilen etwa von der BITKOM[200] eingefordert wurde.[201] Der damalige Bundesinnenminister Thomas de

[190] Für eine Stärkung der Selbstregulierung plädiert etwa Franzen, RdA 2010, 257, 261 f.
[191] Weichert/Kilian, in: Kilian/Heussen, Computerrecht, Teil 13 Kap. 5.1 Rn. 46.
[192] RL 95/46/EG.
[193] Weichert/Kilian, in: Kilian/Heussen, Computerrecht, Teil 13 Kap. 5.1 Rn. 48.
[194] BT-Drs. 14/4329, S. 30
[195] Roßnagel, in: Roßnagel, Handbuch DSR, Kap. 3.6, Rn. 47 f., 68 ff.
[196] Weichert/Kilian, in: Kilian/Heussen, Computerrecht, Teil 13 Kap. 5.1 Rn. 49.
[197] Weichert/Kilian, in: Kilian/Heussen, Computerrecht, Teil 13 Kap. 5.1 Rn. 49.
[198] LT-Drs. Schleswig-Holstein 16/2439, S. 89.
[199] Kinast, in: Taeger/Gabel, BDSG, § 38a Rn. 3.
[200] Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

Maizière sprach sich in seinen entworfenen Thesen zu den Grundlagen einer gemeinsamen Netzpolitik der Zukunft[202] für eine Stärkung der Selbstregulierung aus.[203] Diesem Trend schließt sich sein Amtsnachfolger, Dr. Hans-Peter Friedrich an und betont vor allem, dass „der Weg der Selbstregulierung fortgesetzt (…) werden (müsse)".[204] Von Seiten der Datenschutzbeauftragten begegnet man dem Ausbau der Selbstregulierung tendenziell eher mit Bedenken und sieht die bloße Konzeption einer regulierten Selbstregulierung als unzureichend an.[205] Insofern bleibt abzuwarten, wie der regulierte Rahmen der Selbstregulierung zukünftig im Bereich des Beschäftigtendatenschutzes ausgestaltet wird.

---

[201] Vgl. im Einzelnen den Internetauftritt der BITKOM (http://www.bitkom.org). So wurde jüngst beispielsweise der Rahmen zu der Selbstverpflichtung zum Datenschutz bei RFID (vgl. hierzu ausführlich Gliederungspunkt 2.5.1.3) unterzeichnet, welches von Herrn Heinz Paul Bonn, Vizepräsident der BITKOM, begrüßt wurde, vgl. Presseinformation vom 6. April 2011, abrufbar unter: http://www.bitkom.org/files/documents/RFID_PIA_06_04_2011.pdf. Vgl. ferner das Statement zur PK „Datenschutz im Internet" von Prof. Dr. Dieter Kempf vom 8. Februar 2011, S. 5 (Datenschutz-Kodex für Geodatendienste); abrufbar unter: http://www.bitkom.org/files/documents/BITKOM_Statement_Datenschutz_Prof_Kempf_08_02_2011.pdf sowie die Stellungnahme des Düsseldorfer Kreises (oberste Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich) vom 8. April 2011 hierzu (http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/080420111 DatenschutzKodex.pdf?__blob=publicationFile).

[202] Abrufbar unter: http://www.bmi.bund.de/cae/servlet/contentblob/1099988/publicationFile/88667/thesen_netzpolitik.pdf.

[203] Vgl. http://www.bmi.bund.de/cae/servlet/contentblob/1099988/publicationFile/88667/thesen_netzpolitik.pdf, S. 1 (These 2 – Rechtsordnung mit Augenmaß weiterentwickeln).

[204] Financial Times Deutschland vom 26. Mai 2011; abrufbar unter: http://www.ftd.de/it-medien/medien-internet/:gastkommentar-des-innenministers-das-internet-braucht-nicht-immer-gleich-gesetze/60056634.html.

[205] Vgl. nur die kritischen Ausführungen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Peter Schaar, abrufbar unter: http://www.bundestag.de/dokumente/textarchiv/2011/33500340_ kw08_pa_schaar/index.html sowie die Ausführungen des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, Prof. Dr. Johannes Caspar, im Rahmen eines Interviews mit dem Verfasser vom 18. Mai 2011, abrufbar unter http://www.pawproject.eu/de/dokumente.

2. ZULÄSSIGKEIT AUSGEWÄHLTER ÜBERWACHUNGSMAßNAHMEN DE LEGE LATA

Im Hinblick auf die einzelnen Überwachungsmaßnahmen muss auch und gerade der Frage nach der entsprechenden Rechtslage nachgegangen werden.

2.1. Die Überwachung von Personalcomputern und Notebooks

Für die Erledigung der anfallenden Büroarbeiten ist der Einsatz von Personalcomputern und Notebooks (inkl. des entsprechenden Zubehörs wie Bildschirm, Software oder Drucker) am Arbeitsplatz heutzutage unerlässlich.

2.1.1. Das Direktions- beziehungsweise Weisungsrecht des Arbeitgebers als Ausgangspunkt für die Nutzung von Personalcomputern und Notebooks

In der Regel finden sich in Arbeitsverträgen keine gesonderten Regelungen für die Nutzung von Personalcomputern und Notebooks.[206] Oft wird die Tätigkeit der Beschäftigten nur pauschal beschrieben, lediglich vereinzelt erfolgt eine Bezugnahme auf Arbeitsplatz- oder Stellenbeschreibungen.[207] Die Nutzung von PC und Notebook wird individualrechtlich auf der Grundlage des Direktionsrechts des Arbeitgebers als Inhaber der betrieblichen Mittel geregelt, dessen rechtlicher Maßstab die Billigkeit nach § 315 BGB ist.[208] Aus dieser Norm folgt regelmäßig die Pflicht des Beschäftigten, den ausgestatteten Arbeitsplatz zu dienstlichen Zwecken zu nutzen.[209] In Ausnahmefällen können einzelne Mitarbeiter nach Maßgabe des § 315 BGB von dieser Verpflichtung befreit werden, was etwa bei älteren Mitarbeiten, die den Umgang mit der Technik massiv scheuen, der Fall sein kann.[210] Diesbezüglich ist zu beachten, dass sich gewisse Arbeitsbedingungen auch über einen längeren Zeitraum nicht so sehr verfestigen dürfen, dass sie zum einseitig unabänderbaren Vertragsbestandteil werden.[211] Darüber hinaus gebietet der allgemeine Gleichbehandlungsgrundsatz des Art. 3 Abs. 1 GG[212] dem Arbeitgeber, sämtliche vergleichbare Arbeitsplätze mit Computern einzurichten.[213] Es besteht die Pflicht, einzelne Beschäftigte oder Gruppen von Beschäftigten nicht aus sachfremden Gründen ungünstiger zu behandeln als andere Mitarbeiter in vergleichbarer Lage.[214] Bei Überlassung eines PC/Notebooks bedarf es einer arbeitsvertraglichen Regelung

[206] Pauly /Osnabrügge, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 6 Rn. 120.
[207] Pauly /Osnabrügge, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 6 Rn. 120.
[208] Pauly/Osnabrügge, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 6 Rn. 120. Vgl. auch § 106 GewO.
[209] Pauly/Osnabrügge, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 6 Rn. 120. Ob der Computer nur für dienstliche oder auch für private Zwecke genutzt werden darf, hängt damit von der Erlaubnis des Arbeitgebers ab, die i.W.d. Arbeitsvertrages beziehungsweise durch Betriebsvereinbarung erfolgen kann, Pauly/Osnabrügge, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 6 Rn. 122.
[210] Pauly/Osnabrügge, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 6 Rn. 120.
[211] BAG, NZA 1993, 89, 91.
[212] Vgl. hierzu Kania, in: Küttner, Personalbuch, Gleichbehandlung Rn. 9 ff.
[213] Pauly/Osnabrügge, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 6 Rn. 120.
[214] BAG, NZA 1984, 201, 202.

der Rückgabeverpflichtung im Fall einer Kündigung oder Freistellung.[215] Hierbei kann der Arbeitgeber je nach Sachlage verschiedene Herausgabeansprüche geltend machen.[216] Als Inhaber der betrieblichen Mittel[217] hat der Arbeitgeber grundsätzlich das Recht, frei darüber zu entscheiden, ob und inwieweit er seinen Arbeitnehmern die Nutzung von Internet- und E-Mail-Diensten ermöglichen möchte.[218] Damit hat der Arbeitnehmer zum einen grundsätzlich weder einen Anspruch auf Gestattung der Privatnutzung,[219] noch darf das Internet bei fehlender Gestattung des Arbeitgebers (gleich, ob expressis verbis oder konkludent) grundsätzlich nicht privat genutzt werden.[220] In Not- beziehungsweise Eilfällen[221] ist die private Nutzung, unabhängig von der Art des verwendeten Kommunikationsmittels, ausnahmsweise zulässig.[222] Generell verboten sind hingegen Nutzungen, die gegen Gesetze verstoßen oder offensichtlich Unternehmensinteressen zuwiderlaufen.[223]

2.1.2. Fälle aus der Rechtsprechung[224]

Bereits mehrfach hat sich die Rechtsprechung mit dem Einsatz von Computern und deren Überwachung beschäftigt.[225] Die Frage, in welchem Umfang der Arbeitgeber dienstliche Internetkommunikation kontrollieren darf, war hingegen bislang noch nicht Gegenstand höchstrichterlicher Rechtsprechung.[226]

---

[215] Pauly/Osnabrügge, in:Besgen/Prinz, Neue Medien und Arbeitsrecht, § 6 Rn. 121.
[216] Vgl. zu den Einzelheiten Pauly/Osnabrügge, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 6 Rn. 11 ff.
[217] BAG, NZA 2006, 98.
[218] Beckschulze, DB 2003, 2777, 2779; Ders./Henkel, DB 2001, 1491, 1494; Däubler, K&R 2000, 323, 324. Dies gilt i.Ü. auch für die Nutzung privater Smartphones der Beschäftigten, mit denen auf das Internet zugegriffen werden kann, LAG Rheinland-Pfalz, BeckRS 2010, 66924 (vgl. hierzu auch die Anmerkung von Stück, ArbRAktuell 2010, 432). Zu den einschränkenden Vorgaben bei der Erlaubnis privater Nutzung vgl. Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 193 ff. Hinsichtlich der Gestaltung betrieblicher Regelungen zur IT-Nutzung siehe Kramer, ArbRAktuell, 2010, 164.
[219] Bloesinger, BB 2007, 2177, 2177; Mengel, BB 2004, 1445, 1446 (m.w.N.); Vietmeyer/Byers, MMR 2010, 807, 808; Beckschulze/Natzel, BB 2010, 2368, 2373; Mengel, BB 2004, 2014, 2014 f.; Weißnicht, MMR 2003, 448, 448.
[220] Rath/Karner, K&R 2007, 446, 449. Zu der konkludenten Erlaubniserteilung vgl. Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 185.
[221] Hanau/Hoeren, Private Internetnutzung durch Arbeitnehmer, S. 20.
[222] Holzner, ZRP 2011, 12, 12; vgl. ferner BAG, NZA 1986, 643 (Telefonnutzung) sowie Ernst, NZA 2002, 585, 588 (Gestattung der Kommunikation via E-Mail oder VoIP).
[223] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 197, der neben beleidigenden, rassistischen sexistischen, gewaltverherrlichenden und verfassungsfeindlichen Inhalten auch solche nennt, die gegen persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Regelungen verstoßen.
[224] Vgl. generell zu den relevantesten höchstrichterlichen Entscheidungen Gola/Wronka, Handbuch des Arbeitnehmerdatenschutzes, S. 575 ff.
[225] Vgl. exemplarisch die bei Pauly/Osnabrügge, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 6 Rn. 120 ff. genannten Entscheidungen: BAG, NZA 1993, 89 (Einrichtung von Arbeitsplätzen), NZA 1984, 201 (Gleichbehandlungsgrundsatz); LAG Köln, NZA 2006, 106; ArbG Düsseldorf – 4 Ca 3437/01 (n.v.; weitestgehende Übertragung der Grundsätze zu Privattelefonaten auf private Internetnutzung); ArbG Frankfurt a.M. 2.1.2002 – 2 Ca 5340/01 (n.v.; Duldung der Privatnutzung); BAGE 115, 195 (Internetnutzung bei fehlender ausdrücklicher Gestattung oder Duldung); LAG Köln, NZA 2006, 106; ArbG Düsseldorf 1.8.2001 – 4 Ca 3437/01 (n.v.); BAG, NJW 2006, 540; LAG Rheinland-Pfalz 9.5.2005 – 7 Sa 68/05 (n.v.); NZA-RR 2005, 303 (Kündigung und Abmahnung; vgl. hierzu weiterhin BAGE 115, 195; NZA 2007, 922, 924 sowie LAG Rheinland-Pfalz, NZA-RR 2010, 297, 299).
[226] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 206.

2.1.3. Wissenschaftliche Auseinandersetzung

Oft wird die private E-Mail- und Internetnutzung arbeitgeberseitig weder ausdrücklich verboten noch explizit erlaubt.[227] Es stellt sich die Frage, wie diese Situation rechtlich zu bewerten ist. Auch wenn in diesem Zusammenhang keine pauschalisierenden Antworten gegeben werden können, so haben sich doch einige Grundsätze zur privaten E-Mail- und Internetnutzung am Arbeitsplatz herausbilden können, die im Folgenden dargestellt werden sollen.

2.1.3.1. Keine zugelassene Privatnutzung bei fehlender ausdrücklicher Regelung

Teilweise wird vertreten, bei fehlender ausdrücklicher Regelung eine private Nutzung zuzulassen.[228] Der Arbeitnehmer könne von einer Duldung derartiger Handlungen ausgehen, da in der Nutzung der betrieblichen technischen Einrichtungen in angemessenem Umfang eine am Maßstab der heutigen Zeit gemessene sozialadäquate Erscheinung liege.[229] Diese Ansicht verkennt aber zum einen, dass der Arbeitgeber aufgrund der verlorenen Arbeitszeit seiner Mitarbeiter erheblich geschädigt wird.[230] Andererseits bestimmt nach wie vor der Arbeitgeber über die Nutzung und Verwendung der betrieblichen Mittel, so dass der Arbeitnehmer nicht annehmen darf, dass er zu einer Privatnutzung berechtigt ist.[231] Insofern ist eine Privatnutzung ohne ausdrückliche Gestattung oder Duldung des Arbeitgebers grundsätzlich abzulehnen.[232]

2.1.3.2. Ausdrückliche und konkludente Nutzungsregelungen

Mittels Aushängen, Rundmails an die gesamte Belegschaft (Gesamtzusagen), individualvertraglichen Klauseln oder Betriebsvereinbarungen kann die Privatnutzung ausdrücklich geregelt werden.[233] Ferner wird die Einrichtung einer privaten E-Mail-Adresse durch den Arbeitgeber als konkludente Gestattung der privaten Nutzung qualifiziert.[234] Anders ist die bloße Bereitstellung des Internetzugangs zu bewerten.[235] Darüber hinaus kann

---

[227] Rath/Karner, K&R 2007, 446, 448.

[228] LAG Köln, NZA 2006, 106; ArbG Wesel NJW 2001, 2490; ArbG Frankfurt a.M., NZA 2002, 1093.

[229] AG Köln, NZA 2006, 106; ArbG Frankfurt a.M., NZA 2002, 1093; LAG Rheinland-Pfalz , NZA-RR 2005, 303.

[230] Pauly/Osnabrügge, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 6 Rn. 123 mit Verweis auf Dickmann, NZA 2003, 1009 Fn. 4, der den jährlichen Schaden für Firmen in Deutschland allein aufgrund unerlaubter Internetbenutzung auf 50 Milliarden EUR pro Jahr beziffert.

[231] Kratz/Gubbels: NZA 2009, 652, 652; im Ergebnis ebenso: Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 181.

[232] Vgl. hierzu BAGE 115, 195 sowie Beckschulze, DB 2003, 2377, 2377; Ernst, NZA 2002, 585, 586; Dickmann, NZA 2003, 1009; Kramer, NZA 2004, 458, 461; Mengel, NZA 2005, 752, 753.

[233] Nägele/Meyer, K&R 2004, 312, 313; Beckschulze, DB 2003, 2777, 2777; Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 183. Bei Betriebsvereinbarungen zwischen Arbeitgeber und Betriebsrat müssen aus rechtlichen Gesichtspunkten sowohl den Wertungen des Grundgesetzes, zwingendem Recht (ius cogens) sowie den allgemeinen Grundsätzen des Arbeitsrechtes besondere Aufmerksamkeit geschenkt werden, Brink/Schmidt, MMR 2010, 592, 593. Vor allem mit Blick auf § 75 Abs. 2 Satz 1 BetrVG wird solchen Vereinbarungen vielfach eine rechtfertigende Wirkung hinsichtlich Eingriffen in das Individualrecht der Beschäftigten auf informationelle Selbstbestimmung abgesprochen, Brink/Schmidt, MMR 2010, 592, 593.

[234] Erler, Die private Nutzung neuer Medien am Arbeitsplatz, 2003, S. 18; ebenso Kratz/Gubbels, NZA 2009, 652, 652.

[235] Mengel, BB 2004, 1445, 1446; ders., BB 2004, 2014, 2015; Ernst, NZA 2002, 585, 586; Kratz/Gubbels, NZA 2009, 652. Ob in der ausdrücklichen oder konkludenten Gestattung privater Telefonate eine konkludente Erklärung des Arbeitgebers enthalten ist, auch eine private Internet- und E-Mail-Nutzung zuzulassen, ist

eine stillschweigende Gestattung darin liegen, dass der Arbeitgeber trotz Kenntnis von der Privatnutzung der betrieblichen Kommunikationsmittel seiner Beschäftigten nicht eingreift, mithin diese erkennbar dulden möchte.[236]

2.1.3.3. Betriebliche Übung

Umstritten ist, ob bei fehlender ausdrücklicher Vereinbarung durch konkludentes Verhalten des Arbeitgebers ein Anspruch des Mitarbeiters auf Privatnutzung nach den Grundsätzen der betrieblichen Übung entstehen kann.[237] Denkbar wäre dies, wenn in der bloßen Duldung der Privatnutzung über einen längeren Zeitraum durch den Arbeitgeber ein derartiger Erklärungswert enthalten wäre, auf den der Beschäftigte hinreichend vertrauen dürfte.[238] Dies wird von einer Ansicht abgelehnt,[239] wobei u.a. wiederum mit der Stellung des Arbeitgebers als Inhaber der Arbeitsmittel argumentiert wird.[240] So solle der Grundsatz gelten, dass sämtliche nicht erlaubten Handlungen des Arbeitnehmers verboten sind.[241] Der Mitarbeiter begehe durch die private Nutzung beziehungsweise das Überschreiten des vom Arbeitgeber präzisierten Erlaubnisrahmens eine Pflichtverletzung, die der Arbeitgeber nicht hinzunehmen habe.[242] Diese Ansicht verkennt jedoch den qualitativen Unterschied zwischen einem bloßen Unterlassen und einer Duldung.[243] Während in einem Unterlassen ein Verhalten des Arbeitgebers liegt, dass die Schaffung eines Vertrauenstatbestandes nicht zu leisten vermag,[244] verhält es sich im Fall einer Duldung anders. Hier hat der Arbeitgeber Kenntnis von der privaten Nutzung[245] und nimmt diese über einen längeren Zeitraum[246] beanstandungslos hin.[247] Der Umfang der Duldung ist gem. §§ 133, 157 BGB vom objektiven Empfängerhorizont her auszulegen, mithin aus Sicht eines verständigen Arbeitnehmers unter Berücksichtigung der gegenseitigen arbeitsvertraglichen Interessen.[248] Orientierungsmaßstab bilden mithin die vertraglichen Haupt- und Nebenleistungspflichten des Beschäftigten.[249] Letzterer ist im Rahmen seiner Hauptleistungspflicht gehalten, primär seine Arbeitsaufgaben zu erfüllen, damit weder die Qualität seiner Arbeitsergebnisse noch seine Leistungsfähigkeit in unverhältnismä-

---

umstritten. Dies bejahen z.B. Ernst, NZA, 2002, 585 sowie Däubler, Internet und Arbeitsrecht, Rn. 184a und Hanau/Hoeren, Private Internetnutzung durch Arbeitnehmer, S. 22. Ablehnend hingegen Uecker, ITRB 2003, 158 Kratz/Gubbels, NZA 2009, 652, 652 (m.w.N.).

[236] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 185.

[237] Kratz/Gubbels, NZA 2009, 652, 652.

[238] Kratz/Gubbels, NZA 2009, 652, 652.

[239] So etwa Beckschulze, DB 2009, 2097; Koch, NZA 2008, 911; Waltermann, NZA 2007, 529, 531.

[240] Beispielsweise Bissels/Lützeler/Wisskirchen, BB 2010, 2433, 2433.

[241] Bissels/Lützeler/Wisskirchen, BB 2010, 2433, 2433 unter Rückgriff auf BAG, NJW 2006, 540; LAG Hamm, BeckRS 2010, 67373; Beckschulze, DB 2009, 2097.

[242] Bissels/Lützeler/Wisskirchen, BB 2010, 2433, 2433.

[243] In diese Richtung gehend argumentieren auch Kratz/Gubbels, NZA 2009, 652, 652 sowie Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 186.

[244] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 186; Kratz/Gubbels, NZA 2009, 652, 652.

[245] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 186; Kratz/Gubbels, NZA 2009, 652, 652.

[246] Die zeitlichen Grenzen werden in der Literatur unterschiedlich angesetzt (Beckschulze/Henkel, DB 2001, 1491, 1492 und Ernst, NZA 2002, 585, 586 sowie Däubler, Internet und Arbeitsrecht, 2004, Rn. 180 setzen ein halbes Jahr an. Kramer, NZA 2004, 457 geht hingegen von einem Jahr aus.)

[247] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 186.

[248] BAG, NZA 2006, 107, 108.

[249] Kratz/Gubbels, NZA 2009, 652, 653. Ähnlich Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 193. Bzgl. der rechtlichen Pflichten zur Wahrung der IT-Sicherheit des Unternehmens siehe Trappehl/Schmidl, NZA 2009, 985, 987.

ßiger Weise negativ beeinträchtigt werden.[250] In diesem Zusammenhang findet die konkludente Nutzungsbefugnis ihre Schranken in dem Übermaßverbot,[251] wobei eine Einzelfallbetrachtung unter besonderer Berücksichtigung der bestehenden Arbeitsbelastung des Mitarbeiters zu erfolgen hat.[252] Regelmäßig beschränkt sich der Nutzungsumfang daher auf Zeiten, in denen keine betrieblichen Interessen beeinträchtigt werden.[253] Hierunter fallen Zeiträume, in denen der Beschäftigte keinen Pflichten nachkommen muss oder – wie etwa bei Arbeitsmangel – kann, mithin Pausen- und Freiraumzeiten.[254] Ebenso müssen Beschäftigte im Rahmen ihrer vertraglichen Nebenpflichten die betrieblichen und vermögensrechtlichen Interessen des Arbeitgebers achten.[255] Darüber hinaus kann der Arbeitgeber nicht nur nachträglich die Grenzen der Nutzungserlaubnis präzisieren,[256] sondern das Entstehen einer betrieblichen Übung im Vorfeld bereits dadurch verhindern, dass er aus Gründen der Rechtssicherheit[257] entsprechende Regelungen in Betriebs- und Dienstleistungsvereinbarungen trifft[258] und die Einhaltung des erteilten Verbots der Privatnutzung i.R.e. Monitoring durchsetzt und kontrolliert[259] sowie Verstöße sanktioniert.[260]

2.1.3.4. Einschränkung und Rücknahme der Erlaubnis

Einschränkungen der Erlaubnis privater Nutzung können in zeitlicher, örtlicher und inhaltlicher Hinsicht vorgenommen werden.[261] Auch steht dem Arbeitgeber die Möglichkeit der Rücknahme der Nutzungsgewährung offen, sofern die Privatnutzung als freiwillige Leistung ohne Bindungswillen gestattet wurde.[262] Besteht hingegen bereits aufgrund des Arbeitsvertrags oder – sofern zugelassen – einer betrieblichen Übung ein Anspruch des Mitarbeiters auf Privatnutzung, muss einer Rücknahme der Erlaubnis eine Änderungskündigung vorausgehen.[263]

2.1.3.5. Zulässiger Umfang der Kontrolle von E-Mail- und Internetnutzung

Es drängt sich die Frage auf, ob und in welchem Umfang die arbeitgeberseitige Kontrolle der E-Mail- und Internetnutzung zulässig ist.[264]

---

[250] Kratz/Gubbels, NZA 2009, 652, 653.
[251] ArbG Wesel, NJW 2001, 2490, 2492; Mattl, Die Kontrolle der Internet- und E-Mail Nutzung am Arbeitsplatz, S. 49; Kliemt, AuA 2001, 532, 534; Ernst, NZA 2002, 585, 586; Mengel, BB 2004, 2014, 2015; Kramer, NZA 2004, 457, 460.
[252] Kratz/Gubbels, NZA 2009, 652, 653.
[253] Kratz/Gubbels, NZA 2009, 652, 653.
[254] Kratz/Gubbels, NZA 2009, 652, 653 mit Verweis auf die a.A. von Ernst, NZA 2002, 585, 586 (mit Ausführungen zu der Vertrauensarbeitszeit) und Däubler, Internet und Arbeitsrecht, 2004, Rn. 170.
[255] Vgl. hierzu die bei Kratz/Gubbels, NZA 2009, 652, 653 genannten Beispiele bzgl. der Schädigung von Betriebsmitteln und anderen Rechtsgütern des Arbeitgebers (m.w.N.).
[256] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 188.
[257] Vietmeyer/Byers, MMR 2010, 807, 808.
[258] LAG Rheinland-Pfalz, NZA-RR 2005, 303, 306.; Rath/Karner, K&R 2007, 446, 449.
[259] Rath/Karner, K&R 2007, 446, 449.
[260] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 188.
[261] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 193. Zu den Einzelheiten vgl. Dickmann, NZA 2003, 1009.
[262] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 189.
[263] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 190. Vgl. ferner BAG, RDV 2010, 68.
[264] Vollkontrollen verbieten sich schon aus Verhältnismäßigkeitsgesichtspunkten, Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 291.

2.1.3.5.1. Abgrenzung zwischen rein dienstlicher und privater Internetkommunikation[265] als Ausgangspunkt für den Umfang arbeitgeberseitiger Überwachungsbefugnisse

Grundlegend ist festzuhalten, dass der Umfang arbeitgeberseitiger Kontrollbefugnisse bei privater E-Mail- und Internetnutzung wesentlich geringer ausfällt als bei rein dienstlicher, sodass eine Differenzierung vorgenommen werden muss.[266] Dienstlichen Charakter hat eine Nutzung grundsätzlich immer dann, wenn sie dazu bestimmt ist, die Arbeit zu fördern.[267] Sie liegt vor, wenn die Internetkommunikation einen Bezug zu den dienstlichen Aufgaben des Arbeitnehmers aufweist und den objektiven Interessen des Arbeitgebers entspricht.[268] Hierzu zählen auch private Nutzungen aus dienstlichem Anlass, die aufgrund von Umständen aus der Sphäre des Arbeitgebers getätigt werden.[269] Solche Nutzungen sind wegen der Fürsorgepflicht des Arbeitgebers aus §§ 611, 242 BGB[270] gestattet.[271] Ferner lässt sich der soziale Austausch am Arbeitsplatz, auch durch E-Mail-Verkehr, dem Bereich der dienstlichen Nutzung zuordnen.[272] Tatsächlich kann der Arbeitgeber diesen nicht vollständig unterbinden.[273] Sämtliche anderen Formen der Außenkommunikation sind dem Privatbereich zuzuordnen.[274]

2.1.3.5.2. Kontrolle dienstlicher Internetkommunikation (Verbot der Privatnutzung)

Besteht ein Verbot der privaten E-Mail- und Internetnutzung, das auch tatsächlich seitens des Arbeitgebers durchgesetzt wird, beurteilt sich die Zulässigkeit der Speicherung und Auswertung der Verkehrsdaten[275] des Arbeitnehmers nach der arbeitsvertraglichen Zweckbestimmung des § 32 Abs. 1 BDSG[276] unter Beachtung des Rechts der Mitarbeiter auf informationelle Selbstbestimmung.[277] Als Verbindungsdaten des E-Mail-Verkehrs können zum einen die äußeren Daten (z.B. Absender und Empfänger der E-Mail,[278] Zeitpunkt der Versendung) anfallen.[279] Bei der Internetnutzung können etwa der Zeitpunkt des Aufrufs,[280] die Dauer der

---

[265] Ist neben der rein dienstlichen Nutzung eine Privatnutzung gestattet, spricht man von einer sog. Mischnutzung, Rath/Karner, K&R 2007, 446, 450.

[266] Rath/Karner, K&R 2007, 446, 449; Rasmussen-Bonne/Raif, GWR 2011, 80; Hoppe, ArbRAktuell, 388; Vietmeyer/Byers, MMR 2010, 807, 807.

[267] Ernst, NZA 2002, 585, 588.

[268] Rath/Karner, K&R 2007, 446, 449.

[269] Rath/Karner, 2007, 446, 449 mit Beispielen.

[270] Rath/Karner, K&R 2007, 446, 447.

[271] Rath/Karner, K&R 2007, 446, 449. Vgl. ferner im Hinblick auf Telefongespräche BAG, NJW 1987, 674, 678.

[272] Ernst, NZA 2002, 585, 588.

[273] Rath/Karner, K&R 2007, 446, 449.

[274] Däubler, K&R 2000, 323, 324.

[275] Verkehrsdaten sind Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden, § 3 Nr. 30 TKG.

[276] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 287. Bestimmungen des TKG und TMG finden bei der rein dienstlichen Nutzung keine Anwendung im Arbeitsverhältnis; Däubler, Gläserne Belegschaften, Rn. 337, 342; Kratz/Gubbels, NZA 2009, 652, 653.

[277] Rath/Karner, K&R 2010, 469, 470 mit Verweis auf Mengel, BB 2004, 2014, 2015; Ernst, NZA 2002, 585, 588; Lindemann/Simon, BB 2001, 1950, 1951.

[278] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 288. Vgl. auch a.a.O., Rn. 289 (m.w.N.) zu der Frage der Speicherung der Empfängeradresse.

[279] Vehslage, AnwBl. 2001, 145, 148; Däubler, Gläserne Belegschaften?, Rn. 351, 354; Naujock, DuD 2002, 592, 593; einschränkend Ernst, NZA 2002, 585, 590 bzgl. der Speicherung der kompletten Adresse des Empfängers.

Internetnutzung und die Protokolle aufgerufener Websites[281] sowie etwaige Kosten[282] (beispielsweise aus Gründen der Missbrauchs- und Kostenkontrolle)[283] oder der Prävention und Behebung von Störungen des EDV-Systems[284] eine Rolle spielen. Bei der vorzunehmenden Abwägung kommt den Interessen des Arbeitgebers bei einer rein dienstlichen Nutzung grundsätzlich der Vorrang zu.[285] Damit wird zumindest bei einem regelmäßig kontrollierten Verbot der privaten Nutzung in der Regel von der Zulässigkeit der Kontrolle der rein dienstlichen E-Mail- und Internetnutzung ausgegangen.[286] Aus der inhaltlichen Kontrolle einer E-Mail resultiert dann auch keine Verletzung des informationellen Selbstbestimmungsrechts, da Arbeitnehmer in Anbetracht des Verbots der Privatnutzung damit rechnen müssen, dass die Kommunikation nicht ausschließlich im Verhältnis zum Empfänger stattfindet.[287] Damit darf der Arbeitgeber bei der Gestattung einer rein dienstlichen Nutzung grundsätzlich generell die Arbeitnehmerdaten speichern,[288] wozu ihm weitreichende Überwachungsmöglichkeiten zur Verfügung stehen.[289] So kann er bei Standard-Web-Browsern von dem Cache-Inhalt Kenntnis nehmen und Rückschlüsse auf das Surfverhalten (z.B. Internet-Adressen, Zeitpunkt des Aufrufs einer Website) der Arbeitnehmer ziehen.[290] Zudem kann mittels detaillierter Logfiles[291] der Datenverkehr des Mitarbeiters analysiert werden.[292] Zu beachten ist, dass im Vorfeld zu prüfen und konkret festzulegen ist, welchen Umfang das Protokoll haben darf und welche Daten ausgewertet werden sollen.[293]

2.1.3.5.3. Kontrolle privater Internetkommunikation

Weitaus komplizierter stellt sich die Rechtslage im Fall der über die rein dienstliche Nutzung hinaus gestatteten Privatnutzung (sog. Mischnutzung)[294] dar. Liegt eine solche Erlaubnis vor, greifen nicht nur die Vorschriften des BDSG, sondern ist der Arbeitgeber auch als Dienstean-

---

[280] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 288.
[281] Vietmeyer/Byers, MMR 2010, 807, 808.
[282] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 288.
[283] Raffner/Hellich, NZA 1997, 862, 867.
[284] Hoppe/Braun, MMR 2010, 80, 81; Kramer, ArbRAktuell, 2010, 164.
[285] Rath/Karner, K&R 2010, 469, 470.
[286] Rath/Karner, K&R 2010, 469, 470. So i.E. auch Hoppe/Braun, MMR 2010, 80, 81; Jenau, AiB 2010, 88, 90; Raif/Bordet, AuA 2010, 88; Braun/Spiegl, AiB 2008, 393, 394; Schmitt-Rolfes, AuA 2008, 391; Wolf/Mulert, BB 2008, 442, 443; Altenburg/v. Reinersdorff/Leister, MMR 2005, 135, 136. Oft wird hier ein Vergleich mit dem Öffnen und Lesen von Dienstpost durch den Arbeitgeber gezogen, vgl. nur Gola, MMR 1999, 322, 326; Weißnicht, MMR 2003, 448, 451; Lindemann/Simon, BB 2001, 1950, 1952; Mengel, BB 2004, 2014, 2017, Rath/Karner, K&R 2007, 446, 450.
[287] Gola, MMR 1999, 322, 326; Rath/Karner, K&R 2007, 446, 450.
[288] Rasmussen-Bonne/Raif, GWR 2011, 80.
[289] Besgen/Prinz, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 1 Rn. 53.
[290] Besgen/Prinz, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 1 Rn. 53.
[291] Hierunter sind in diesem Kontext Protokolldateien zu verstehen, die Informationen über Verkehrsdaten der Internetkommunikation (z.B. Zeitpunkt und Dauer der Verbindung zu Servern, Übertragung von Dateien) enthalten, Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 198.
[292] Besgen/Prinz, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 1 Rn. 53
[293] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 288. Vgl. ferner die Orientierungshilfe „Protokollierung“ des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Orientierungshilfen/OHProtokollierung.pdf?__blob=publicationFile.
[294] Rath/Karner, K&R. 2010, 469, 470.

bieter im Sinne des § 3 Nr. 6 TKG[295] und des § 2 S. 1 Nr. 1 TMG zu qualifizieren.[296] Dies hat zur Folge, dass er den telekommunikationsrechtlichen Restriktionen der §§ 88 ff. TKG und der §§ 11 ff. TMG unterworfen wird.[297] Die Vorschriften greifen selbst dann, wenn der Arbeitgeber den Nutzungsumfang in zeitlicher Hinsicht oder vom Umfang her beschränkt und die Mitarbeiter diese Nutzungsvorgaben überschreiten.[298] Letztlich verschließt sich damit dem Arbeitgeber de facto immer die Kontrolle oder Einsichtnahme in die Kommunikationsdaten.[299] Teilweise wird vertreten, dass der Arbeitnehmer den Arbeitgeber durch eine pauschale schriftliche Erklärung von der Einhaltung des Telekommunikationsgeheimnisses befreien und somit auch bei erlaubter Privatnutzung eine Nutzungskontrolle vornehmen könne.[300] Eine gegenläufige Meinung schlägt vor, diese Möglichkeit zumindest insofern einzuschränken, als dass vielmehr einzelfallabhängig ermittelt werden müsse, ob eine entsprechende schriftliche Zustimmungserklärung für die jeweilige Kommunikationsart sowie den konkret anstehenden Kontrollvorgang vorliegt.[301]

Kontrolle von Internet und E-Mail im Anwendungsbereich des TKG

Aus § 88 Abs. 2 TKG folgt nach überwiegender Ansicht für den Arbeitgeber als Dienstleister i.S.d. Norm[302] die Pflicht zur Wahrung des Fernmeldegeheimnisses.[303] Dies hat Auswirkungen auf den Umfang des Schutzes des Arbeitnehmers. So darf der Arbeitgeber den Inhalt der Internetkommunikation grundsätzlich zur Kenntnis nehmen, wenn eine private Nutzung des Internets erlaubt ist.[304] Wie sich aus § 88 Abs. 3 S.1 und S. 3 TKG ergibt, ist eine Einsichtnahme in den Inhalt sowie die näheren Umstände der Telekommunikation und die Weitergabe an Dritte nur dann erlaubt, wenn dies für die genannten Zwecke erforderlich ist und soweit das TKG oder ein anderes Gesetz dies durch Bezugnahme auf Telekommunikationsvorgänge zulässt. Vorrangig muss aber der Anzeigepflicht des § 138 StGB nachgekommen werden, vgl. § 88 Abs. 3 S. 4 TKG. An der Einstufung des Arbeitgebers als TK-Anbieter soll sich

---

[295] D.h. zwischen den Arbeitsvertragsparteien liegt bei erlaubter Privatnutzung ein gesondertes TK-Nutzungsverhältnis vor, das den Arbeitnehmer als außenstehenden Dritten qualifiziert (h.M.; Hoppe/Braun, MMR 2010, 80, 81; Mengel, BB 2004, 1445, 1450; Gola, MMR 1999, 322, 324; Kratz/Gubbels, NZA 2009, 652, 654 f.; Vietmeyer/Byers, MMR 2010, 807, 808). Der Arbeitgeber ist durch die Gestattung der Privatnutzung bereits Access-Provider (Rath/Karner, K&R 2007, 446, 450). Anderer Ansicht sind etwa Thüsing, Arbeitnehmerdatenschutz, Rn. 220 ff. sowie Löwisch, DB 2009, 2782, 2783. Dies widerlegend: de Wolf, NZA 2010, 1206, 1208 f. Zu den Rechtsbegriffen vgl. die Legaldefinitionen in § 3 Nr. 6 TKG (Dienststeanbieter) und § 3 Nr. 10 TKG (geschäftsmäßiges Erbringen von Telekommunikationsdiensten; geschäftsmäßig ist dabei nicht gleichbedeutend mit gewerblich, so dass es nicht auf eine Gewinnerzielungsabsicht ankommt und nachhaltig bedeutet lediglich die auf Dauer angelegte Bereitstellung des Zugangs, Weißnicht, IT-Risikomanagement und Online-Überwachung von Arbeitnehmern im Konzern, S. 161.).

[296] Busse in: Besgen/Prinz, Internet und Arbeitsrecht, § 10 Rn. 74 ff.; Kramer, ArbRAktuell 2010, 164.

[297] Kramer, ArbRAktuell 2010, 164.

[298] Kramer, ArbRAktuell 2010, 164.

[299] Lembke, in: Henssler/Willemsen/Kalb, Arbeitsrecht Kommentar, BDSG Einführung Rn. 92 (m.w.N); Kramer, ArbRAktuell 2010, 164.

[300] Hartmann/Pröpper, BB 2009, 1300, 1300. Hierzu kritisch: Kramer, ArbRAktuell 2010, 164.

[301] Kramer, ArbRAktuell 2010, 164.

[302] Siehe Fn. 296.

[303] Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 221.

[304] Weißnicht, IT-Risikomanagement und Online-Überwachung von Arbeitnehmern im Konzern, S. 164; Rath/Karner, K&R 2010, 469, 470.

nach der Regierungsbegründung[305] auch de lege ferenda nichts ändern.[306] Die Einsichtnahme des Arbeitgebers in E-Mails ist dem Arbeitgeber nicht nur verwehrt, wenn E-Mails in einem externen Postfach gespeichert und bloß über das Internet zu erreichen sind, mithin aufgrund der faktischen Zugriffsmöglichkeit durch den Provider trotz eines Passworts des Nutzers außerhalb seines Machtbereichs liegen.[307] Vielmehr liegt eine vergleichbare Situation vor, wenn – wie üblich – E-Mails von dem E-Mail-Server des Arbeitgebers in das Postfach des Beschäftigten, das als Programm auf seinem Computer installiert ist, heruntergeladen werden.[308] Denn sind die Computer der Mitarbeiter durch ein Firmennetzwerk mit dem E-Mail-Server des Arbeitgebers verbunden, kann der Systemadministrator technisch auf das Postfach des Beschäftigten zugreifen, indem er dessen Passwort zurücksetzt und sich so die Möglichkeit der Kontrolle eröffnet.[309] Darüber hinaus ist zu beachten, dass der Arbeitgeber als Eigentümer jederzeit die Herausgabe der betreffenden Endgeräte (z.B. PC, Notebook, Smartphone) von den Beschäftigten verlangen kann.[310] Diese Gründe sprechen für die grundsätzliche Ausweitung des Schutzes des Art. 10 GG auf E-Mails, die bereits übertragen und geöffnet wurden, solange sie sich im Postfach eines Computer befinden, auf das über das Firmennetzwerk ohne Zustimmung des Beschäftigten zugegriffen werden kann.[311] Zusätzlich ist zu beachten, dass der Arbeitgeber als Dienstleister i.S.d. TKG nach § 109 Abs. 1 Nr. 1 TKG zu angemessenen technischen Vorkehrungen und sonstigen Maßnahmen zum Schutz des Fernmeldegeheimnisses und personenbezogener Daten verpflichtet ist. Neben technischen und organisatorischen Maßnahmen gehören hierzu auch Kontrollmaßnahmen über die Einhaltung der festgelegten Prinzipien.[312] Im Einzelnen dürfen Unbefugte von Verbindungsdaten, die z.B. bei Telefonaten oder der Nutzung einer Datenbank anfallen, keine Kenntnis nehmen können und muss der Kreis der zur Kenntnisnahme Berechtigten so klein wie möglich gehalten werden.[313]

Kontrolle von Internet und E-Mail im Anwendungsbereich des TMG

Da der Arbeitgeber entweder selbst bestimmte Dienste anbietet oder zumindest den Zugang hierzu vermittelt, sind hinsichtlich der Kontrolle der privaten Internetkommunikation die Datenschutzverpflichtungen des TMG zu beachten.[314] Nach § 1 Abs. 1 TMG fallen unter den Begriff des Telemediendienstes sämtliche elektronischen Informations- und Kommunikationsdienste, die nicht als Telekommunikationsdienste oder Rundfunk einzustufen sind.[315] Die

[305] Hintergrundpapier zum Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutz v. 25.8.2010, S. 6; Beckschulze/Natzel, BB 2010, 2368, 2374.
[306] Vietmeyer/Byers, MMR 2010, 807, 807.
[307] De Wolf, NZA 2010, 1206, 1209. Vgl. hierzu BVerfGE 124, 43, 54 unter Rückgriff auf E 120, 274, 341.
[308] De Wolf, NZA 2010, 1206, 1209.
[309] De Wolf, NZA 2010, 1206, 1209.
[310] De Wolf, NZA 2010, 1206, 1209.
[311] De Wolf, NZA 2010, 1206, 1209.
[312] Däubler, Gläserne Belegschaften?, Rn. 370 mit Verweis auf die Vorgängervorschrift des § 109 TKG bei Ehmer, in: Beck'scher TKG-Kommentar, § 87 Rn. 18.
[313] Däubler, Gläserne Belegschaften?, Rn. 370 f.
[314] Däubler, Gläserne Belegschaften?, Rn. 342.
[315] Nicht in den Anwendungsbereich des TMG fallen etwa Mitarbeiterportale, In-House-Informationssysteme oder B2B-Dienste, Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 163 f. (zu der Einschränkung des § 11 Abs. 3 TMG vgl. Rn. 167 f.).

Abgrenzung der Geltungsbereiche von TKG und TMG erfolgt danach, ob der technische Übertragungsvorgang als solcher (TKG) oder die Aufbereitung oder Verwendung der übertragenen Inhalte (TMG) in Frage steht.[316] Hierbei schränkt § 11 Abs. 3 TMG den Anwendungsbereich für Telemedien, die überwiegend[317] in der Übertragung von Signalen über Telekommunikationsnetze bestehen, mithin gleichzeitig dem TKG unterliegen, ein.[318] Als solche Telemedien werden in der Regel auch Angebote von Unternehmen zur privaten Nutzung von E-Mail- und anderen Internet-Anwendungen durch ihre Beschäftigten klassifiziert.[319] Für den Arbeitgeber folgt daraus, dass auf Beschäftigtendaten, die bei einer Privatnutzung anfallen, im Regelfall nicht i.R.e. Kontrolle des Kommunikations- oder Leistungsverhalten der Beschäftigten zurückgegriffen werden darf.[320] Es finden dann nach dem TMG nur noch die Datenschutzvorschriften des § 15 Abs. 8 TMG (Rechtsverfolgung) sowie der entsprechenden Bußgeldvorschrift des § 16 Abs. 2 Nr. 4 TMG hinsichtlich der Erhebung und Verwendung personenbezogener Daten der Nutzer Anwendung, vgl. § 11 Abs. 3 TMG. Zu Abweichungen könne es höchstens im Falle einer freiwilligen ausdrücklichen Einwilligung des Mitarbeiters kommen.[321] Für den Fall, dass der Anwendungsbereich des TMG über den Rahmen des § 11 Abs. 3 TMG eröffnet ist, muss etwa nach dem Grundsatz der Datenvermeidung und Datensparsamkeit darauf geachtet werden, dass bei der Gestaltung und Auswahl technischer Einrichtungen der Dienste keine oder so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt werden.[322] Auch muss der Arbeitgeber den in § 13 Abs. 6 S. 1 TMG niedergelegten Grundsatz der Anonymisierung und Pseudonymisierung beachten, soweit dies technisch möglich und zumutbar ist. Hierüber ist der Nutzer gem. § 13 Abs. 6 S. 2 TMG zu informieren. Die Dauer der Nutzung darf nicht erfasst werden.[323] Zudem verbietet sich eine Kontrolle bei unentgeltlichen Diensten.[324] Nach § 14 Abs. 1 BDSG darf der Diensteanbieter personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen ihm und dem Nutzer über die Nutzung von Telemedien erforderlich sind (sog. Bestandsdaten). Diese Daten betreffen nur den Vertrag als solchen, nicht dessen Durchführung.[325] Zudem schreibt § 15 Abs. 1 TMG vor, dass der Diensteanbieter personenbezogene Daten eines Nutzers nur erheben und verwenden darf, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (sog. Nutzungsdaten).

Präventivkontrolle von E-Mails nach dem BDSG

Neben dem speziellen telekommunikationsrechtlichen Datenschutzregime greifen auch die Regelungen des BDSG. Fraglich ist zunächst, ob § 32 BDSG als Erlaubnissatz für die Prä-

[316] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 166.
[317] Vgl. § 3 Nr. 24 TKG. Eine überwiegende Übertragung in diesem Sinne wird bei einem Anteil von mehr als 50 % angenommen, Wittern/Schuster, in: Beck'scher TKG-Kommentar, § 3 Rn. 48.
[318] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 166.
[319] Moos, in: Taeger/Gabel, BDSG, § 12 TMG Rn. 32; Heidrich, CR 2009, 168, 173; Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 167.
[320] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 167.
[321] Däubler, Gläserne Belegschaften?, Rn. 378.
[322] Däubler, Gläserne Belegschaften?, Rn. 373.
[323] Däubler, Gläserne Belegschaften?, Rn. 377.
[324] Däubler, Gläserne Belegschaften?, Rn. 377; Lindemann/Simson, BB 2001, 1950, 1953.
[325] Däubler, Gläserne Belegschaften?, Rn. 374.

ventivkontrolle von E-Mails herangezogen werden kann. Denkbar ist, hierzu über § 32 Abs. 1 S. 2 BDSG vorzugehen. Wie sich aus dem Wortlaut ergibt, ist hierfür allerdings bereits erforderlich, dass tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat. Bei einer Präventivkontrolle des E-Mail-Verkehrs liegt diese Verdachtslage aber noch nicht vor, so dass § 32 Abs. 1 S. 2 BDSG als Erlaubnissatz ausscheidet.[326] Eine Erlaubnis könnte sich hingegen aus § 32 Abs 1 S. 1 BDSG ergeben. Dann müssten Präventivkontrollen für die Erfüllung des Zwecks des Beschäftigungsverhältnisses erforderlich sein. An dieser Stelle kann erneut auf § 88 TKG verwiesen werden. Laut § 88 Abs. 1 Alt. 1 TKG unterliegt der Inhalt der Kommunikation, also der Text der E-Mail,[327] dem Fernmeldegeheimnis. Als Ausnahme hiervon ermöglicht § 88 Abs. 3 S. 3 Alt. 2 TKG dem Arbeitgeber als Diensteanbieter, sich Kenntnis vom Inhalt der Telekommunikation zu verschaffen, wenn eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. § 32 BDSG fungiert aber gerade nicht als derartige Ausnahmeregelung, so dass diese als Rechtsgrundlage für Präventivmaßnahmen durch E-Mail-Kontrollen ausscheidet.[328]

2.2. Die Überwachung sozialer Netzwerke

Mit den technischen Weiterentwicklungen, vor allem innerhalb der letzten Jahre, geht auch die Entwicklung sozialer Netzwerke einher, die inzwischen als fester Bestandteil des alltäglichen Lebens gesehen werden müssen und sich einer großen Popularität erfreuen.[329] Es stellt sich die Frage, inwieweit das in diesem Zusammenhang auftretende Spannungsverhältnis zwischen Selbstverwirklichung, Meinungsfreiheit und sozialer Interaktion einerseits und informationeller Selbstbestimmung von Nutzern und unbeteiligten Dritten auf der anderen Seite[330] interessengerecht aufgelöst werden kann.

2.2.1. Zu der Natur und Funktionsweise sozialer Netzwerke

Unter sozialen Netzwerken versteht man Internetplattformen, die die Präsentation der eigenen Person ermöglichen.[331] In ihrer Funktionsweise unterscheiden sich die einzelnen Netzwerke kaum. Der Nutzer registriert sich zunächst auf der Plattform, indem er ein eigenes Profil mit Benutzernamen anlegt,[332] das durch Benutzerkennung und Passwort gesichert ist. In diesem Zusammenhang entscheidet der Nutzer auch, welche Daten er in welchem Umfang preisgibt. Je nach Struktur des sozialen Netzwerks können diese Informationen sowohl privater als

[326] De Wolf, NZA 2010, 1206, 1210.
[327] De Wolf, NZA 2010, 1206, 1210.
[328] De Wolf, NZA 2010, 1206, 1210.
[329] So konnte etwa das 2004 gegründete Internetportal Facebook im vergangenen Jahr bereits 500 Millionen Mitglieder verzeichnen, heise online Newsticker vom 21.7.2010, abrufbar unter: http:// www.heise.de/newsticker/meldung/Facebook-meldet-500-Millionen-Mitglieder-1043251.html.
[330] Vgl. Lerch/Krause/Hotho/Roßnagel/Stumme, MMR 2010, 454, 454.
[331] Oberwetter, NJW 2011, 417, 417.
[332] Zumindest bei sozialen Netzwerken mit geschäftlichem Bezug wird dies in aller Regel der bürgerlich-rechtliche Name sein, da der Nutzer gerade intendiert, ein seriöses, den geschäftlichen Gepflogenheiten entsprechendes, adäquates Bild von sich zu erwecken. Im Gegensatz dazu finden sich in privaten Netzwerken häufig Kunst- oder Spitznamen sowie Abwandlungen des eigenen Namens wieder.

beruflicher Natur sein.[333] Während in beruflichen Netzwerken v.a. Angaben zu dem beruflichen Werdegang sowie der ausgeübten Tätigkeit eine Rolle spielen,[334] kommen in privaten Netzwerken auch Informationen wie etwa der Beziehungsstatus hinzu.[335] In der Preisgabe dieser Daten liegt gleichzeitig die datenschutzrechtliche Einwilligung des Betroffenen nach §§ 4 Abs. 1, 4a BDSG.[336] Neben der reinen Präsentation der eigenen Person ermöglichen soziale Netzwerke auch die Interaktion mit anderen Mitgliedern, sei es durch individuelle Kommunikation (Nachrichten, Chats, Posts), durch den Beitritt zu Diskussionsforen oder durch die Vernetzung mit anderen Usern (entweder direkt oder indirekt über den Beitritt zu Interessengruppen).[337] Die aufgrund verschiedener Schnittpunkte entstehende allgemeine Verknüpfung der einzelnen Profile bildet schließlich das Netzwerk.[338]

2.2.2. Die Bedeutung sozialer Netzwerke in der digitalisierten Arbeitswelt

In der digitalisierten Arbeitswelt gewinnen soziale Netzwerke zunehmend an Bedeutung. So wird dem Bereich der Social Media bereits jetzt nicht nur ein enormer Einfluss für die Arbeitswelt beigemessen, sondern fällt auch die Zukunftsprognose über die künftige Relevanz sozialer Netzwerke optimistisch aus.[339] Beispielsweise wird die Verlagerung von Social Network-Funktionen in die Unternehmen hinein als wichtigster Zukunftstrend der Branche herausgehoben.[340] Diese Entwicklung bringt natürlich nicht nur Vorteile mit sich, sondern birgt für den Arbeitnehmer erhebliche Risiken in Bezug auf den Umgang mit seinen personenbezogenen Daten.[341] Um Persönlichkeitsprofile zu erstellen, werden mittels sogenannter Crawler bereits jetzt aus allgemein zugänglichen Quellen Informationen gesammelt.[342] Es sind jedoch vor allem die Daten aus den sozialen Netzwerken, denen besondere Bedeutung zugemessen wird.[343]

---

[333] Oberwetter, NJW 2011, 417, 417. Prominentestes Beispiel eines privaten sozialen Netzwerkes ist zweifelsohne Facebook. In Deutschland erfreuen sich darüber hinaus Netzwerke wie Twitter, studiVZ, meinVZ oder Flickr großer Popolarität. Im Bereich der dienstlichen sozialen Netzwerke können XING, Linkedin und Expeerteer die meisten registrierten Nutzer verbuchen.

[334] Bei XING werden diese Daten beispielsweise unter dem Oberbegriff Businessdaten zusammengefasst.

[335] Oberwetter, NJW 2011, 417, 417. Generell sind aber in beiden Arten sozialer Netzwerke umfassende Angaben beruflicher und privater Art möglich.

[336] Ott, MMR 2009, 158, 161; Weichert, MR-Int. 2007, 188, 189.

[337] Oberwetter, NJW 2011, 417, 417.

[338] Oberwetter, NJW 2011, 417, 417.

[339] Vgl. hinsichtlich der Einzelheiten den aktuellen SID/FIT Social Media Report 2010/2011, abrufbar unter: http://www.softwareinitiative.de/studien/SID-FITSocialMediaReport20102011.pdf.

[340] Zu der Etablierung von Corporate XING vgl. die Pressemitteilung des Fraunhofer-Instituts für Angewandte Informationstechnik (FIT) vom 24.11.2010, abrufbar unter: http://fit.fraunhofer.de/presse/10-11-24_de.html.

[341] Zu Personensuchmaschinen vgl. Ott, MMR 2009, 158 ff. sowie Weichert, MR-Int 2007, 188 ff. Über Search Engines wie Isearch (http://www.isearch.com) oder Intelius (http://www.intelius.com) können bereits heutzutage Personen sog. background checks unterzogen werden. Vgl. hierzu vertiefend Bissels, jurisAnwaltZertifikatOnline Arbeitsrecht 13/2009, Anm. 2.

[342] Hierunter fallen grundsätzlich im Internet, beispielsweise über eine Suchmaschine, abrufbare Daten, BT-Drs. 17/4230, S. 16.

[343] Ott, MMR 2009, 158, 158. In der Literatur wird vertreten, die Einwilligung des Betroffenen so auszulegen, dass Suchmaschinen die Daten zulässigerweise crawlen und nutzen dürfen, vgl. Ott, MMR 2009, 158, 161 sowie auch Weichert, MR-Int 2007, 188, 189.

2.2.3. Fälle aus der Rechtsprechung

Bislang liegen noch keine Gerichtsentscheidungen vor, die die Sanktionierung von Beschäftigten durch deren Arbeitgeber aufgrund der Nutzung des Web 2.0 zum Gegenstand hatten.[344] Gleiches gilt für Sanktionen gegenüber der Überwachung sozialer Netzwerke durch den Arbeitgeber. Aufgrund der wachsenden Beliebtheit der Portale wird eine Auseinandersetzung der Judikative mit der Thematik jedoch als unumgänglich prognostiziert.[345]

2.2.4. Wissenschaftliche Auseinandersetzung[346]

Wie bereits erwähnt, steht es dem Arbeitgeber i.R.s. Direktionsrechts grundsätzlich frei, die Internetnutzung am Arbeitsplatz vollständig zu untersagen. Es entspricht aber weit überwiegend nicht den realen Gegebenheiten, dass hiervon Gebrauch gemacht wird. Vielmehr sowohl die Internetnutzung zu dienstlichen Zwecken als die auch die private Nutzung sind fester Bestandteil der Unternehmenspraxis.[347] Es stellt sich die Frage, in welchem Umfang der Arbeitgeber hinsichtlich der Online-Darstellung der Beschäftigten von seinem Direktionsrecht Gebrauch machen kann. Dies hängt wiederum davon ab, ob es sich um ein privates oder berufliches Netzwerk handelt.

2.2.4.1. Direktionsrecht hinsichtlich der Präsentation in einem privaten sozialen Netzwerk

Grundlegend ist herauszustellen, dass von dem Arbeitgeber grundsätzlich nur solche Weisungen vorgenommen werden dürfen, die in einem Bezug zu der Tätigkeit des Mitarbeiters stehen.[348] Bereits früh hat die Rechtsprechung ausgeführt, dass die persönlichen Verhältnisse eines Mitarbeiters nur offenbart werden müssen, soweit im Zusammenhang mit dem Beschäftigungsverhältnis ein berechtigtes, billigenswertes und schutzwürdiges Interesse des Arbeitgebers vorliegt.[349] Hieraus ergeben sich zwei Einschränkungen für das Direktionsrechts des Arbeitgebers bezüglich der Präsentation von Arbeitnehmern in einem privaten sozialen Netzwerk: Zum einen darf der Arbeitgeber hinsichtlich des privaten Umgangs des Mitarbeiters mit Inhalten sozialer Netzwerke keinerlei Direktiven vorgeben.[350] Zum anderen sind soziale Netz-

---

[344] Raif/Bordet, AuA 2010, 88, 88. Die Thematik wurde aber zumindest schon im Ausland behandelt, vgl. etwa die Kündigung einer Beschäftigten Mitarbeiterin wegen der Bearbeitung ihres Profils bei Facebook während der Krankheitszeit; SPIEGEL ONLINE vom 26.4.2009, abrufbar unter: www.spiegel.de/netzwelt/web/0,1518,621185,00.html.

[345] Bissels, BB 2009, 2197; vgl. auch Raif/Bordet, AuA 2010, 88 und Ege, AuA 2008, 72.

[346] Aufgrund des Umfangs der Darstellung findet vorliegend eine Betrachtung der Vorgänge während des Arbeitsverhältnisses sowie nach dessen Beendigung statt. Zum Stadium des Bewerbungsverfahrens vgl. die Darstellungen bei Oberwetter, NJW 2011, 417 sowie Forst, NZA 2010, 427 und Bissels/Lützeler/Wisskirchen BB 2010, 2433. Vgl. zu dem Ausmaß der im Vorfeld von Bewerbungsgesprächen getätigten Personensuchanfragen die Studie des Bundesverbandes Deutscher Unternehmensberater (BDU) aus dem Jahr 2007, abfrufbar unter: http://www.bdu.de/presse_387.html. Zur Anwendung des § 6a BDSG bei E-Recruiting im Internet vgl. Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 417 f.

[347] Oberwetter, NJW 2011, 417, 418.

[348] Oberwetter, NJW 2011, 417, 418.

[349] BAG, NZA 1986, 739, 739.

[350] Oberwetter, NJW 2011, 417, 418.

werke, die hauptsächlich der privaten Darstellung des Arbeitnehmers dienen, dem Arbeitgeber gänzlich verschlossen.[351]

2.2.4.2. Direktionsrecht hinsichtlich der Präsentation in einem beruflichen sozialen Netzwerk

Anders stellt sich die Rechtslage bei der Präsentation von Mitarbeitern in beruflichen sozialen Netzwerken dar. Hier ist zunächst zu berücksichtigen, dass die Preisgabe der Beschäftigtendaten nicht nur unternehmensintern, sondern auf einer grundsätzlich allgemein zugänglichen Plattform im Internet erfolgt.[352] Damit hängt die Veröffentlichung dieser Daten grundsätzlich von der Einwilligung des betroffenen Arbeitnehmers ab.[353] Eine Ausnahme ergibt sich, wenn die Daten zur Erfüllung der Arbeitspflicht erforderlich sind oder deren Veröffentlichung üblich ist.[354] Im öffentlichen Bereich ist nach dem BVerwG zumindest dann, wenn keine Sicherheitsbedenken entgegenstehen, die Veröffentlichung von Name, Funktion und dienstlicher Erreichbarkeit all jener Beamter als rechtlich zulässig zu betrachten, die mit Außenkontakten betraut sind.[355] Dem gegenüber weitaus kritischer weisen einige Landesdatenschutzbehörden darauf hin, als dass die Daten grenzüberschreitend auch in Ländern ohne angemessenes Datenschutzniveau verfügbar sind.[356] Letztlich ist dem Arbeitgeber im Ergebnis nur die Anordnung eines lückenhaften Profils in dienstlichen sozialen Netzwerken i.R.s. Weisungsrechts möglich.[357]

2.2.4.3. Inhaltliche Anforderungen an das Direktionsrecht

Der Arbeitgeber ist berechtigt, die Nutzung des Internets auszugestalten, indem er diese untersagt oder beschränkt.[358] Insofern gelten für die rechtliche Bewertung sozialer Netzwerke auch und gerade die Grundsätze, die bei der Kommunikation via E-Mail greifen.[359] Im Gegensatz zu einer reinen Internetnutzung finden innerhalb sozialer Netzwerke Interaktionen zwischen den einzelnen Nutzern statt.[360] Verglichen mit der Versendung rein geschäftlicher E-Mails gestaltet sich die Überwachung der Kommunikation in sozialen Netzwerken für den Arbeitgeber ungleich schwieriger.[361] Neben diesem faktischen Aspekt stellt sich in juristischer Hinsicht die Frage, ob die Ansicht, dienstliche E-Mails der jederzeitigen Kontrollmöglichkeit

---

[351] Oberwetter, NJW 2011, 417, 418.
[352] Oberwetter, NJW 2011, 417, 418
[353] Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 1155 sowie 1166 ff. im Hinblick auf das Einwilligungserfordernis des § 22 KUG bei die Veröffentlichung von Bildnissen von Beschäftigten.
[354] Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 1155.
[355] BVerwG, RDV 2009, 30; zu Angabe von Vornamen in der E-Mail-Adresse LAG Schleswig-Holstein, RDV 2008, 212.
[356] Gola/Wronka, Handbuch des Arbeitnehmerdatenschutzes, Rn. 1166. Die Einwilligung ist ferner auch bereits aus tatsächlichen Gründen vonnöten, da die Registrierung auf Plattformen dienstlicher sozialer Netzwerke regelmäßig auf natürliche Personen zugeschnitten ist, die ihr eigenes Profil erstellen, Oberwetter, NJW 2011, 417, 419. Neben diesen Mitgliederprofilen ist aber auch die Erstellung von Unternehmensprofilen möglich, siehe etwa http://www.xing.com/help/hilfe-und-faq-2/funktionalitaten-auf-xing-53/unternehmensprofile-420 (XING-Features Unternehmen).
[357] Oberwetter, NJW 2011, 417, 419.
[358] S.o., Gliederungspunkt 2.2.1.
[359] Oberwetter, NJW 2011, 417, 419.
[360] Oberwetter, NJW 2011, 417, 419.
[361] Oberwetter, NJW 2011, 417, 419.

durch den Arbeitgeber auszusetzen,[362] auf die Überwachung des Informationsaustauschs innerhalb sozialer Netzwerke übertragen werden kann. Es erscheint sehr fraglich, Nachrichten in sozialen Netzwerken wie geschäftliche E-Mails als Handelsbriefe i.S.d. § 257 HGB zu qualifizieren.[363] Eine Parallele besteht allerdings dahingehend, dass in beiden Fällen die Mitteilung in Textform erfolgt und einen Teil der Unternehmenskommunikation darstellt, mithin dem Unternehmen zusteht.[364] Letztlich liegt aber keine völlige Kongruenz vor, da nicht eindeutig festgestellt werden kann, ob z.B. Äußerungen des Arbeitnehmers in Diskussionsforen im Namen des Unternehmens vorgenommen wurden oder vielmehr eine eigene Meinungsäußerung des Beschäftigten vorliegt.[365] Vorgeschlagen wird, eine Differenzierung anhand der Nähe des Themas zu dem Unternehmen vorzunehmen. Demnach sollen unternehmensferne Themen eher dem privaten Bereich zuzuordnen sein, während ein Auftreten im Namen des Unternehmens bei Äußerungen über dessen Produkte vorliegen soll.[366] Ein eindeutiges Auftreten im Namen des Unternehmens soll aber zumindest bei der Korrespondenz des Beschäftigten mit Kunden vorliegen, wenn diese im Rahmen seiner Tätigkeit erfolgt und projektbezogene Aspekte zum Gegenstand hat.[367]

2.2.4.4. Der Umgang mit Daten des Arbeitnehmers bei Beendigung des Beschäftigungsverhältnisses

Spätestens mit der Beendigung des Beschäftigungsverhältnisses stellt sich die Frage, wem die Rechte an dem Benutzerkonto des sozialen Netzwerks und an den entsprechenden Daten (etwa Geschäftskontakte und Kundenverbindungen) zustehen.[368] Für den Arbeitnehmer besteht nach Ausscheiden aus dem Unternehmen die Pflicht zur Herausgabe sämtlicher ihm zur Verfügung gestellten Arbeitsmittel.[369] Ein Benutzerkonto wird durch die Mitteilung der Zugangsdaten herausgegeben.[370] Hierzu ist der Beschäftigte jedoch nur verpflichtet, wenn die Mitgliedschaft in dem sozialen Netzwerk von dem Arbeitgeber finanziert wurde oder dieser das Benutzerkonto anderweitig zur Verfügung gestellt hat.[371] Durch die bloße Einrichtung eines Benutzerkontos im Netzwerk mit Wissen und Wollen des Arbeitgebers wird ein solcher Herausgabeanspruch noch nicht begründet.[372] Sofern den Beschäftigten eine Herausgabepflicht trifft, hat er das Recht, personenbezogene Daten mit privatem Bezug vor der Übergabe zu löschen.[373] Dies gilt auch dann, wenn der Arbeitgeber lediglich eine rein

---

[362] S.o., Gliederungspunkt 2.1.3.5.2.
[363] Oberwetter, NJW 2011, 417, 419.
[364] Oberwetter, NJW 2011, 417, 419.
[365] Oberwetter, NJW 2011, 417, 419.
[366] Oberwetter, NJW 2011, 417, 419, der gleichzeitig betont, dass es sich um keine allgemeingültige Aussage handelt. Insofern scheint eine einzelfallbezogene Betrachtung unter Würdigung der Gesamtumstände der Äußerung angezeigt.
[367] Oberwetter, NJW 2011, 417, 419.
[368] Bissels/Lützeler/Wisskirchen, BB 2010, 2433, 2438; Oberwetter, NJW 2011, 417, 420.
[369] Schaub/Linck, ArbeitsR-Handbuch, S. 1584. Dies folgt entweder aus einer ausdrücklichen vertraglichen Bestimmung oder, falls eine solche nicht vorliegt, aus §§ 861 f., 677, 985 BGB, Bissels/Lützeler/Wisskirchen, BB 2010, 2433, 2438.
[370] Oberwetter, NJW 2011, 417, 420.
[371] Oberwetter, NJW 2011, 417, 420; ähnlich Bissels/Lützeler/Wisskirchen, BB 2010, 2433, 2438.
[372] Oberwetter, NJW 2011, 417, 420.
[373] Oberwetter, NJW 2011, 417, 420.

dienstliche Nutzung erlaubt hat.[374] Denn selbst bei dem rein geschäftlichen Umgang mit Kunden kann ein Austausch von Inhalten mit privatem Bezug stattfinden, an denen der Arbeitgeber kein wirtschaftliches Interesse geltend machen kann.[375] Könnte der Arbeitgeber von diesen Daten Kenntnis nehmen, läge hierin ein unzulässiger Eingriff in das Persönlichkeitsrecht der Mitarbeiter.[376] Im Gegensatz dazu kann den Beschäftigten aber auch dann, wenn kein Anspruch des Arbeitgebers auf Herausgabe der Zugangsdaten vorliegt, die Verpflichtung treffen, bestimmte Dateninhalte seines Benutzerkontos zur Verfügung zu stellen.[377] So müssen solche Daten an den Arbeitgeber herausgegeben werden, die von diesem zur Weiterführung der Geschäfte des Arbeitnehmers benötigt werden, mithin etwa eine von dem Beschäftigten angelegte Kundenkartei[378] oder Kundendaten.[379] Darüber hinaus erstreckt sich die Herausgabepflicht auf wirtschaftlich relevante Geschäftskorrespondenz, sei es hinsichtlich aktueller Projekte oder solcher Unterlagen, derer der Arbeitgeber ipso iure bedarf.[380]

2.3. Die Überwachung des Brief- und Telefonverkehrs

Fraglich ist, ob und in welchem Umfang der Arbeitgeber den Brief- und Telefonverkehr seiner Mitarbeiter überwachen darf.

2.3.1. Die Überwachung des Briefverkehrs

Geht es um die Überwachung des Briefverkehrs der Mitarbeiter, stellt sich die Frage, ob in ungerechtfertigter Weise in das Recht am geschriebenen Wort[381] eingegriffen wurde.

2.3.1.1. Grundrechtliche Dimension des Schutzes des geschriebenen Wortes

Ausgehend von dem Normzweck des Art. 10 Abs. 1 Alt. 1 GG, die Vertraulichkeit des brieflichen Kommunikationsvorgangs zu schützen, fallen unter den Begriff des Briefes sämtliche schriftliche Nachrichten zwischen Absender und individuellem Empfänger in Form individueller Kommunikation.[382] Nach herrschender Meinung kommt es nicht darauf an, dass der Brief verschlossen ist, so dass sich der Schutz auch etwa auf Postkarten erstreckt.[383]

2.3.1.2. Fälle aus der Rechtsprechung

Die Rechtsprechung hatte sich mit der Frage zu beschäftigen, ob Dienstpost seitens des Arbeitgebers geöffnet werden darf. Diesbezüglich wurde ausgeführt, dass eine Verletzung des

---

[374] Oberwetter, NJW 2011, 417, 420.
[375] Oberwetter, NJW 2011, 417, 420.
[376] Oberwetter, NJW 2011, 417, 420.
[377] Bissels/Lützeler/Wisskirchen, BB 2010, 2433, 2438; Oberwetter, NJW 2011, 417, 420.
[378] LAG Hamm, ARSt 1991, 182, 182 f.
[379] Preis, in: ErfK zum Arbeitsrecht, § 611 BGB Rn. 754; vgl. BGH, NJW 1993, 1786 für einen Handelsvertreter.
[380] Oberwetter, NJW 2011, 417, 420.
[381] Der Schutz des Briefverkehrs wird – abgesehen von der verfassungsrechtlichen Dimension – insbesondere durch § 202 StGB sichergestellt.
[382] Durner, in Maunz/Dürig, GG, Art. 10 Rn. 68.
[383] Durner, in Maunz/Dürig, GG, Art. 10 Rn. 68. A.A. etwa Evers, JZ 1965, 661, 662; Marxen, Das Grundrecht des Brief-, Post und Fernmeldegeheimnisses, S. 22 ff.; Groß, in: Berliner Kommentar GG, Art. 10 Rn. 21; Pagenkopf, in: Sachs, GG, Kommentar, Art. 10 Rn. 12 und Oehler, GR II, 605, 608, der ein bloßes Umschlossensein fordert.

Briefgeheimnisses nicht vorliege, wenn eine Dienststelle im Rahmen ihrer Büroordnung an Mitarbeiter und zugleich an die Dienststelle adressierte Sendungen, welche nicht als persönlich oder vertraulich gekennzeichnet sind, öffnet und mit Eingangsstempel versehen an einen betreffenden Mitarbeiter weiterleitet.[384]

2.3.1.3. Wissenschaftliche Auseinandersetzung

In der Literatur wird auf die Ausführungen der Rechtsprechung zu dem Umgang mit Dienstpost zurückgegriffen. So wird ebenfalls auf das Kriterium der Kennzeichnung als vertraulich beziehungsweise persönlich abgestellt und bei dessen Vorliegen dem Persönlichkeitsrecht des Arbeitnehmers der Vorrang eingeräumt.[385] Im Gegensatz zu Dienstpost, auf die der Arbeitgeber zugreifen darf,[386] müssen schriftliche Mitteilungen, die erkennbar für den Mitarbeiter persönlich bestimmt sind, diesem verschlossen zugestellt werden.[387]

2.3.2. Die Überwachung des Telefonverkehrs[388]

Auch kann der Arbeitgeber ein Interesse an der Überwachung des Telefonverkehrs seiner Beschäftigten haben.

2.3.2.1. Fälle aus der Rechtsprechung

In grundlegenden höchstrichterlichen Entscheidungen des BAG[389] und des BVerwG[390] wurde dem Arbeitgeber bei ausgehenden dienstlichen Telefonaten grundsätzlich ein Recht auf Erhebung, Speicherung und Nutzung von Telefondaten etwa zu Zwecken der Kostenkontrolle und Kostenrechnung zugestanden.[391] Möchte der Arbeitgeber ein Telefongespräch zwecks späterer Beweisführung mithören, ist hierzu in der Regel die Einwilligung des externen Gesprächspartners vonnöten.[392] In der besonderen Arbeitssituation in Call Centern ist zudem

---

[384] LAG Hamm, NZA-RR 2003, 346, 347. Vgl. auch BAG, NZA-RR 2011, 15 (außerordentliche Kündigung eines Betriebsratsmitglieds); RDV 2000, 23 (Angabe von Vornamen in Geschäftsbriefen) und BVerwG, RDV 2006, 124 (LS) zu der Behandlung handschriftlicher Aufzeichnungen eines Vorgesetzten über seine Mitarbeiter.

[385] Sassenberg/Bamberg, DuD 2006, 226, 228 f., Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 17.

[386] Pröpper/Römermann: MMR 2008, 514, 514; Wolf/Mulert, BB 2008, 442, 443 (m.w.N); Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 17.

[387] Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 17.

[388] Auf Aspekte der Internettelefonie (Voice over IP, VoIP), die Telefonie oder Bildttelefonie über den normalen Internetanschluss ermöglicht, wird nicht separat eingegangen, da die auftretenden Fragen sich mit denen im Zusammenhang mit herkömmlicher Telefonie sowie derer Verknüpfung mit anderen Medien decken, Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 281 ff. mit Verweis auf TBS NRW, VoIP – Telefonieren übers Internet – Handlungshilfen für die betriebliche Interessenvertretung, abrufbar unter: http://www.tbs-nrw.de/cweb/cgi-bin-noauth/cache/VAL_BLOB/789/789/290/UmschlTBSBroschVoIP.pdf.

[389] DB 1986, 2086; NZA 1987, 515.

[390] NJW 1982, 840; RDV 1990, 24; DuD 1990, 426.

[391] Diese Auffassung wird von Seiten der Datenschutzbehörden mitgetragen, vgl. z.B. Aufsichtsbehörde Baden-Württemberg, Hinweis zum BDSG Nr. 3, Staatsanzeiger vom 1.7.1978, Nr. 52, S.4 Nr. 8.1. Unterschiedliche Meinungen von Rechtsprechung und Aufsichtsinstanzen bestehen dagegen hinsichtlich der Frage, ob die komplette Zielrufnummer gespeichert werden darf, vgl. BAG, DRV 1991, 7; Wohlgemuth/Mostert, ArbuR 1986, 138.

[392] BVerfG, RDV 2003, 23; 1992, 121; BGH, RDV 2003, 237. Vgl. zu der Berechtigung des Mithörens von Telefongesprächen ferner BVerfG, NJW 1992, 815; RDV 2008, 18; BAG, NJW 1998, 307 sowie Grosjean, DB 2003, 2650, 2650 f.

offenes Mithören zum Zweck einer Leistungskontrolle nach der Rechtsprechung nur soweit zulässig, wie es dem Anlernprozess dient und in der schonendsten Art, mithin auf die Probezeit beschränkt, erfolgt.[393]

2.3.2.2. Wissenschaftliche Auseinandersetzung

Bezüglich der Zulässigkeit der Erfassung und Kontrolle von Telefonaten und Telefonverbindungsdaten gelten überwiegend die Ausführungen hinsichtlich der Überwachung von E-Mail- und Internet-Nutzung.[394] Die Beurteilung der Rechtmäßigkeit der Überwachungsmaßnahmen hängt daher von der Frage ab, ob der Arbeitgeber auch die private Nutzung von dienstlichen Festnetz- und Mobiltelefonen gestattet.

2.3.2.2.1. Erlaubte Privatnutzung

Ein Anspruch des Arbeitnehmers auf Privatnutzung dienstlicher Telefone besteht nicht.[395] Sollte der Arbeitgeber die private Nutzung erlaubt haben, finden wiederum die Regelungen des TKG mit der Folge Anwendung, dass die arbeitgeberseitigen Überwachungsmöglichkeiten nur in deutlich restriktiverem Umfang möglich sind.[396] Telefonverbindungsdaten (Zielrufnummer, Uhrzeit und Dauer des Telefonats, Anzahl der angefallen Gebühreneinheiten) dürfen gem. § 96 Abs. 1 TKG[397] nur erhoben und kontrolliert werden, wenn sie zu Abrechnungszwecken erforderlich sind,[398] vgl. § 97 TKG. Dies ist denkbar, wenn die Privatnutzung nur entgeltlich erlaubt ist,[399] in der Praxis üblicherweise allerdings nicht der Fall.[400] Hinsichtlich des Umfangs der erfassten und genutzten Daten ist nicht die vollständige Zielrufnummer für die Kostenberechnung notwendig, sondern genügt bereits die Vorwahl für die Bestimmung der Gebührenzone.[401] Kann der Beschäftigte Diensttelefone unentgeltlich nutzen, darf der Arbeitgeber die Verbindungsdaten i.d.R. nur auswerten, wenn ein Fall der Störungsbeseitigung vorliegt (§ 100 Abs. 1 TKG) oder ein begründeter Missbrauchsverdacht besteht (§ 100 Abs. 3 TKG).[402] Hingegen darf an die Erhebung der Verbindungsdaten keine Leistungskontrolle des Arbeitnehmers gekoppelt werden.[403] Sowohl das Mithören als auch Aufzeichnen des Inhalts von Telefongesprächen ist als Eingriff in das Recht am gesprochenen Wort grundsätzlich unzulässig.[404] Zudem genießen Privatgespräche des Arbeitnehmers den Schutz durch das Fernmeldegeheimnis des § 88

---

[393] BAG, RDV 1986, 30. Vgl. zu dem Einsatz von Silent Monitoring und Voice Recording Jordan/Bissels/Löw, BB 2008, 2626.
[394] Wellhöner/Byers, BB 2009, 2310, 2312.
[395] Mengel, BB 2004, 1445, 1446; Altenburg/v. Reinersdorff/Leister, MMR 2005, 135, 135.
[396] Wellhöner/Byers, BB 2009, 2310, 2312.
[397] Vietmeyer/Byers, MMR 2010, 807, 809.
[398] Wellhöner/Byers, BB 2009, 2310, 2312; Vietmeyer/Byers, MMR 2010, 807, 809.
[399] Wellhöner/Byers, BB 2009, 2310, 2312; Heldmann, DB 2010, 1235, 1239; Vietmeyer/Byers, MMR 2010, 807, 809.
[400] Wellhöner/Byers, BB 2009, 2310, 2312.
[401] Mengel, BB 2004, 1445, 1451; Gola, MMR 1999, 322, 327; Altenburg/v. Reinersdorff/Leister, MMR 2005, 135, 137; Wank, in: ErfK zum Arbeitsrecht, § 28 BDSG, Rn. 19.
[402] Heldmann, DB 2010, 1235, 1239; Vietmeyer/Byers, MMR 2010, 807, 809; Mengel, BB 2004, 1445, 1451; Oberwetter, NZA 2008, 609, 611.
[403] Gola, MMR 1999, 322, 327; Oberwetter, NZA 2008, 609, 611.
[404] Wellhöner/Byers, BB 2009, 2310, 2312; Oberwetter, NZA 2008, 609, 611; Mengel, BB 2004, 1445, 1451; Moll, Münchener Anwaltshandbuch Arbeitsrecht, § 100 TKG Rn. 46.

TKG.[405] Die Kontrolle des Gesprächsinhalts ist auf seltene Ausnahmefälle beschränkt. Denkbar ist hier etwa das Vorliegen eines begründeten Verdachts einer Straftat gegen den Beschäftigten, der sich erheblich auf das Beschäftigungsverhältnis auswirkt (beispielsweise Verrat von Geschäftsgeheimnissen oder sexuelle Belästigung von Arbeitskollegen).[406] Bezüglich der Erfassung und Kontrolle der Telefonate und Verbindungsdaten bei erlaubter Privatnutzung dienstlicher Mobilfunkgeräte bestehen keine Unterschiede zu der Rechtslage bei der Überwachung von Festnetztelefonen.[407] Zu beachten ist, dass der Arbeitgeber auf dem Mobiltelefon des Beschäftigten anrufen darf, um dessen derzeitigen Aufenthaltsort zu erfragen.[408]

2.3.2.2.2. Ausschließlich dienstlich erlaubte Nutzung

Sofern dem Arbeitnehmer ausschließlich die dienstliche Nutzung von Festnetz und Mobiltelefonen erlaubt ist, ist der Anwendungsbereich des TKG nicht eröffnet und die Zulässigkeit der Überwachungsmaßnahmen an den Bestimmungen des BDSG zu messen.[409] Da der Arbeitgeber nicht als TK-Anbieter auftritt, kommen Verstöße gegen das Fernmeldegeheimnis nicht in Betracht.[410] Grundsätzlich zulässig ist die Erfassung und Kontrolle der Telefonverbindungsdaten.[411] Mangels Überwachung des Gesprächsinhalts liegt kein Eingriff in das Recht am eigenen Wort vor.[412] Jedoch wird in das Recht des Arbeitnehmers auf informationelle Selbstbestimmung eingegriffen.[413] Im Rahmen des Abwägungsvorgangs werden aber die berechtigten Interessen des Arbeitgebers an der Kosten- und Missbrauchskontrolle regelmäßig schwerer ins Gewicht fallen.[414] Wiederum braucht nicht die gesamte Zielrufnummer erfasst werden, hier genügt der Anfang der Rufnummer zur Kostenkontrolle.[415] Abweichungen hiervon können bei der Missbrauchskontrolle bestehen, um den Nachweis der Privatnutzung erbringen zu können.[416] Im Gegensatz dazu dürfen Telefonverbindungsdaten zur allgemeinen Leistungskontrolle auch bei einem Verbot der privaten Telefonnutzung nicht erfasst werden.[417] Die Überwachung von Gesprächsinhalten dienstlicher Telefonate betreffend, wird ein strengerer Maßstab als bei der Inhaltskontrolle von E-Mails angelegt.[418] Das Mithören und Aufzeichnen von Telefonaten ist grundsätzlich als unzulässiger Eingriff in das Recht am eigenen Wort zu werten.[419] Allenfalls in äußersten

---

[405] Oberwetter, NZA 2008, 609, 611; Altenburg/v. Reinersdorff/Leister, MMR 2005, 135, 137; Wank, in: ErfK zum Arbeitsrecht, § 28 BDSG, Rn. 19; Gola, MMR 1999, 322, 325.
[406] Altenburg/v. Reinersdorff/Leister, MMR 2005, 135, 137; Mengel, BB 2004, 1445, 1451.
[407] Wellhöner/Byers, BB 2009, 2310, 2312.
[408] Oberwetter, NZA 2008, 609, 612; Gola, NZA 2007, 1139, 1142.
[409] Altenburg/v. Reinersdorff/Leister, MMR 2005, 135, 136; Mengel, BB 2004, 1445, 1447.
[410] Wellhöner/Byers, BB 2009, 2310, 2313.
[411] Wellhöner/Byers, BB 2009, 2310, 2313.
[412] Mengel, BB 2004, 1445, 1448; Altenburg/v. Reinersdorff/Leister, MMR 2005, 135, 136.
[413] Wellhöner/Byers, BB 2009, 2310, 2313.
[414] Oberwetter, NZA 2008, 609, 611; Altenburg/v. Reinersdorff/Leister, MMR 2005, 135, 136; Mengel, BB 2004, 1445, 1448; Gola, MMR 1999, 322, 326 f.
[415] Gola, MMR 1999, 322, 326.
[416] BAG, NJW 1987, 674, 677; Simitis, in: Simitis, BDSG, § 28 Rn. 107; Oberwetter, NZA 2008, 609, 611; Altenburg/v. Reinersdorff/Leister, MMR 2005, 135, 136.
[417] Gola, MMR 1999, 322, 327; Oberwetter, NZA 2008, 609, 611. Zu den Besonderheiten in Call Centern vgl. Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 758 ff.
[418] Wellhöner/Byers, BB 2009, 2310, 2313.
[419] Oberwetter, NZA 2008, 609, 611; Mengel, BB 2004, 1445, 1451.

Ausnahmefällen kann sich eine Rechtfertigung ergeben, wie etwa bei Vorliegen eines begründeten Straftatverdachts, der sich auf das Arbeitsverhältnis auswirkt.[420] Dies ergibt sich zuletzt auch aus dem Wortlaut von § 32 Abs. 1 S. 2 BDSG,[421] der als Rechtfertigungsgrund für die Aufdeckung einer im Arbeitsverhältnis begangenen Straftat fungieren kann.[422] Anders stellt sich die Rechtslage in Bezug auf offenes Mithören von dienstlichen Telefonaten dar.[423] Diese Maßnahme kann aufgrund von Ausbildungs- und Kontrollzwecken zulässig sein.[424] Eine umfassende Arbeitnehmerkontrolle ist wiederum ungerechtfertigt.[425] Diese Ausführungen beanspruchen ebenso für den dienstlichen Gebrauch von Mobilfunkgeräten Geltung.[426] Da regelmäßig keine Einwilligung des Anrufers vorliegt, bestimmt sich bei Einsatz von ISDN-Technik die Speicherung von dessen Rufnummer sowie weiterer Daten nach Maßgabe des § 28 Abs. 1 S.1 Nr.2 BDSG.[427] Sollten eingehende Telefongespräche privaten Charakter haben, führt dies nicht zu einer Anwendung des TKG.[428]

2.4. Die Videoüberwachung

Findet eine Videoüberwachung von Mitarbeitern statt, stellt dies ebenfalls einen Eingriff in deren allgemeines Persönlichkeitsrecht dar. Aufgrund der mit der Videoüberwachung einhergehenden permanenten Drucksituation für den Arbeitnehmer ist dessen Persönlichkeitsrecht am Arbeitplatz im besonderen Maße gefährdet.[429]

2.4.1. Fälle aus der Rechtsprechung

In mehreren Entscheidungen[430] hat die Rechtsprechung aufgezeigt, dass der Persönlichkeitsschutz der Arbeitnehmer grundsätzlich Vorrang vor Sicherheitsinteressen des Arbeitgebers genießt.[431]

---

[420] Oberwetter, NZA 2008, 609, 611; Altenburg/v. Reinersdorff/Leister, MMR 2005, 135, 136; Mengel, BB 2004, 1445, 1449; Dann/Gastell, NJW 2008, 2945, 2948. Denkbar ist auch das Abhören bei Verdacht des Verrats von Geschäftsgeheimnissen, vgl. Dann/Gastell, NJW 2008, 2945, 2948; Oberwetter, NZA 2008, 609, 611.
[421] Wellhöner/Byers, BB 2009, 2310, 2313.
[422] Deutsch/Diller, DB 2009, 1462, 1464; von Steinau-Steinrück/Mosch, NJW-Spezial 2009, 450, 451; Wybitul, BB 2009, 1582, 1583.
[423] Wellhöner/Byers, BB 2009, 2310, 2313.
[424] Wellhöner/Byers, BB 2009, 2310, 2313. Als Beispiel kommt hier etwa die Einarbeitung neuer Beschäftigter in Telefonzentralen oder Call Centern in Betracht, Dann/Gastell, NJW 2008, 2945, 2948; Mengel, BB 2004, 1445, 1449; Gola, MMR 1999, 322, 325. Im Bereich der Schulungszwecke ist allerdings die Einwilligung der betroffenen Arbeitnehmer erforderlich, Dann/Gastell, NJW 2008, 2945, 2948; Oberwetter, NZA 2008, 609, 611. Vgl. zu einer ausnahmsweise zulässigen heimlichen Aufzeichnung Gola,/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 785.
[425] Wellhöner/Byers, BB 2009, 2310, 2313.
[426] Wellhöner/Byers, BB 2009, 2310, 2313.
[427] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 202.
[428] Gola, MMR 1999, 332, 324 f.; Däubler, K&R 2000, 323, 327; Post-Ortmann, RDV 1999, 102.
[429] BAG, NZA 1988, 92; NZA 2003, 1193, 1194; NZA 2004, 1278, 1281.
[430] BAG, RDV 1988, 137; NZA 1988, 92 RDV 1992, 178; NJW 2003, 3436; NJW 2005, 313; RDV 2005, 216; RDV 2008, 238.
[431] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 65.

2.4.2. Wissenschaftliche Auseinandersetzung[432]

Im Bereich der Videoüberwachungsmaßnahmen ist eine Differenzierung zwischen Videoüberwachungen öffentlich und nicht öffentlich zugänglicher Räume angebracht sowie zwischen offenen und heimlichen Maßnahmen zu unterscheiden.

2.4.2.1. Videoüberwachung öffentlich zugänglicher Räume, § 6b BDSG

Nach der Neueinführung des § 6b BDSG findet sich im deutschen Recht eine Rechtsgrundlage für die Videoüberwachung öffentlich zugänglicher Räume. § 6b Abs. 1 BDSG regelt die Frage der Zulässigkeit der Erhebung personenbezogener Daten mittels optisch-elektronischer Einrichtungen.[433] Wie sich aus der Gesetzesbegründung ergibt, zielt das Telos der Norm auf die Wahrung des informationellen Selbstbestimmungsrechts durch einen angemessenen Interessensausgleich ab.[434] Hierbei sollte eine Regelung geschaffen werden, die auf Seiten der Anlagenbetreiber eine einschränkende Verwendungspraxis dergestalt vorsieht, dass eine Videoüberwachung auf schützenswerte Beobachtungszwecke beschränkt wird.[435] Aufgrund des Umstands, dass schon die Beobachtung selbst erfasst ist, kommt es hinsichtlich der datenschutzrechtlichen Relevanz nicht darauf an, ob das Bildmaterial im Anschluss gespeichert wird.[436] Normadressat der Regelung in § 6b BDSG sind alle öffentlichen und nicht-öffentlichen Stellen i.S.d. § 2 BDSG in dem von der Vorschrift gesetzten Rahmen. Wird die Videoüberwachung nicht selbst durchgeführt, sondern im Auftrag durch einen Auftragnehmer, bleibt bei einer Auftragsdatenverarbeitung gem. § 11 BDSG die entsprechende Stelle Normadressat.[437]

2.4.2.1.1. Anwendungsbereich

Der Anwendungsbereich des § 6b BDSG ist auf öffentlich zugängliche Räume beschränkt. Vom Wortsinn her ist der Begriff Raum dreidimensional zu verstehen, d.h. es ist neben dem Boden auch der Raum über dieser Fläche erfasst.[438] Im Übrigen ist strittig, welchen Anforderungen ein „öffentlich zugänglicher Raum“ genügen muss. Einerseits wird vertreten, bei dem Raum müsse es sich um einen baulich abgrenzbaren, umbauten Raum handeln.[439] Andere wiederum verzichten auf dieses Kriterium.[440] Begründet wird dies damit, dass weder aus dem Wortlaut des § 6b BDSG noch aus der Gesetzesbegründung ein entsprechendes Erfordernis abgeleitet werden kann.[441] Entscheidend sei vielmehr, dass der Raum nach dem Willen des rechtlichen Besitzers für die Öffentlichkeit zugänglich oder für den öffentlichen Verkehr gewidmet ist.[442] Damit fallen solche Räume in den Anwendungsbereich, die ihrem Zweck nach dazu bestimmt sind, von einer unbestimmten Zahl oder nach nur allgemeinen

---

[432] Zu der rechtlichen Bewertung von Kamera-Attrappen vgl. näher Kirsch, MMR-Aktuell 2011, 317919.
[433] Zscherpe, in:Taeger/Gabel, BDSG, § 6b Rn. 21.
[434] BT-Drs. 14/4329, S. 38.
[435] Zscherpe, in: Taeger/Gabel, BDSG, § 6b Rn. 5; Gola/Schomerus, BDSG, § 6b Rn. 1.
[436] BT-Drucks. 14/4329, S. 38.
[437] Zscherpe, in: Taeger/Gabel, BDSG, § 6b Rn. 19.
[438] Zscherpe, in: Taeger/Gabel, BDSG, § 6b Rn. 31.
[439] So die ganz h.M., vgl. nur Bizer, in: Simitis, BDSG, § 6b Rn. 36.
[440] Zscherpe, in: Taeger/Gabel, BDSG, § 6b Rn. 32; Gola/Schumerus, BDSG, § 6b Rn. 8.
[441] Zscherpe, in: Taeger/Gabel, BDSG, § 6b Rn. 32.
[442] Bizer, in: Simitis, BDSG, § 6b Rn. 37; Gola/Schumerus, BDSG, § 6b Rn. 12; Zscherpe, in: Taeger/Gabel, BDSG, § 6b Rn. 32

Merkmalen bestimmten Personen betreten und genutzt zu werden.[443] Maßgeblich ist danach allein die durch den Berechtigten eröffnete tatsächliche Nutzungsmöglichkeit durch die Allgemeinheit.[444] Laut der Gesetzesbegründung fallen hierunter etwa Bahnsteige, Ausstellungsräume eines Museums, Verkaufsräume[445] oder Schalterhallen.[446] Bei der Beurteilung, ob Arbeitsplätze als öffentliche Räume zu qualifizieren sind, ist eine differenzierte Betrachtung vorzunehmen.[447] Oft wird es bei diesen an der öffentlichen Zugänglichkeit fehlen.[448] § 6b BDSG ist deshalb nur Maßstab für die Zulässigkeit einer Videoüberwachung öffentlich zugänglicher Räume, wenn Arbeitnehmer in Räumlichkeiten mit Publikumsverkehr ihre Tätigkeit verrichten.[449] Im Einzelfall kann die Abgrenzung zwischen öffentlich zugänglichen und nicht öffentlichen Räumen Schwierigkeiten bereiten. Teilweise wurde etwa versucht, den Kassenbereich eines Supermarktes als dem Publikumsverkehr nicht unmittelbar zugängliche Enklave innerhalb des öffentlichen Verkaufsraums dem Anwendungsbereich der Vorschrift zu entziehen.[450] Jedoch ist es bereits aufgrund der technischen Gegebenheiten unvermeidbar, dass eine Videokamera, die auf den nicht für Kunden zugänglichen Kassenbereich ausgerichtet ist, nicht auch Teile des öffentlich zugänglichen Bereichs filmt oder Kunden – z.B. beim Bezahlvorgang anlässlich der Eingabe der PIN-Nummer ihrer EC-Karte – in den Aufnahmebereich der Kamera geraten.[451] Mithin ist der Kassenbereich nicht als eigenständiger, abgrenzbarer Raum im öffentlich zugänglichen Raum zu klassifizieren.[452] Festzuhalten bleibt, dass § 6b BDSG allein Erlaubnisnorm für die Beobachtung öffentlich zugänglicher Räume sein kann; eine Überschreitung von Grenzen zwischen öffentlichen und nicht-öffentlichen Räumen wird hingegen gerade nicht gestattet.[453] Somit müssen Kameras so aufgestellt sein, dass einzig und allein der öffentliche Raum beobachtet wird.[454]

2.4.2.1.2. Offene Videoüberwachung

Fraglich ist, wie die offene Videoüberwachung öffentlich zugänglicher Räume rechtlich zu bewerten ist.

---

[443] BAG, NZA 2004, 1278, 1282; NJOZ 2005, 2708, 2713; Zscherpe, in: Taeger/Gabel, BDSG, § 6b Rn. 32.
[444] Gola/Schumerus, BDSG, Rn. 9.
[445] Wie etwa Ladengeschäfte oder Kaufhäuser, Bayreuther, NZA 2005, 1038, 1038, der darüber hinaus noch Bankfilialen, Tankstellen und Gaststätten als Beispiele nennt.
[446] BT-Drucks. 14/4329, S. 38.
[447] Zscherpe, in: Taeger/Gabel, BDSG, § 6b Rn. 37.
[448] Meyer, K&R 2009, 14, 15; Zscherpe, in: Taeger/Gabel, § 6b BDSG Rn. 37; Grimm/Schiefer, RdA 2009, 329, 331.
[449] Grimm/Schiefer, RdA 2009, 329, 331; Däubler, NZA 2001, 874; Wiese, in: Festschr. f. E. Lorenz, 2004, S. 915, 923; Gola/Klug, RDV 2004, 67, 72.
[450] LAG Mecklenburg-Vorpommern – 1 Sa 387/03; Helle, JZ 2004, 340, 346.
[451] Grimm/Schiefer, RdA 2009, 329, 331.
[452] ArbG Frankfurt, RDV 2006, 314; Wank, in: ErfK zum Arbeitsrecht, § 6b BDSG Rn. 1; Bayreuther, NZA 2005, 1038, 1038 f.; Grimm/Brock/Windeln, ArbRB 2006, 179, 180; Wilke, AiB 2006, 31, 33; Grimm/Schiefer, RdA 2009, 329, 331. Zu weiteren strittigen Fällen vgl. Zscherpe, in: Taeger/Gabel, BDSG, § 6b Rn. 36. Vgl. ferner Bayreuther, 1038, 1039 zu der Einordnung von Filialen in Einkaufszentren.
[453] Zscherpe, in: Taeger/Gabel, BDSG, § 6b Rn. 38.
[454] Zscherpe, in: Taeger/Gabel, BDSG, § 6b Rn. 38; a.A. noch BGH, NJW 1995, 1955, 1956.

Einzelheiten der Zulässigkeitsprüfung

Nach § 6b Abs. 1 BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie zur Aufgabenerfüllung öffentlicher Stellen (Nr. 1), zur Wahrnehmung des Hausrechts (Nr. 2) oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (Nr. 3) erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Geht es um die Beurteilung der Zulässigkeit der Videoüberwachung, sind mithin mehrere Schritte durchzuführen.

Legitime Beobachtungszwecke, § 6b Abs. 1 Nrn. 1, 2 und 3 BDSG

Um eine rechtmäßige Videoüberwachung nach § 6b Abs. 1 BDSG durchzuführen, bedarf es zunächst eines zulässigen Beobachtungszwecks.[455] Im Bereich des Beschäftigtendatenschutzrechtes hat der Zweck nach Nr. 1 nur geringe Bedeutung und wird auch die Wahrnehmung des Hausrechts (Nr. 2) nur selten als Legitimationsgrundlage für eine Videoüberwachung dienen.[456] So umfasst das Hausrecht die zivilrechtlichen Ansprüche des Eigentümers (§§ 903 f., 1004 BGB) beziehungsweise berechtigten Besitzers (§§ 859 ff. BGB), die darauf gerichtet sind, Störer aus einem Raum zu verweisen und ihnen zukünftig ebenfalls den Zutritt zu untersagen.[457] Beschäftigte müssen hingegen gerade Zutritt zu der Arbeitsstelle erhalten, um ihre Arbeitsleistung erbringen zu können.[458] Somit liegt in der Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (Nr. 3)[459] der bedeutendste Zweck für eine Videoüberwachung öffentlich zugänglicher Räume.[460]

Geeignetheit und Erforderlichkeit, § 6b Abs. 1 letzter HS. BDSG

In einem zweiten Schritt muss die Geeignetheit und Erforderlichkeit der Maßnahme (§ 6b Abs.1 letzter HS. BDSG) überprüft werden. Dabei ist eine Maßnahme erforderlich, wenn sie zur Erreichung des angestrebten Erfolges das mildeste unter mehreren zur Verfügung stehenden, gleich geeigneten Mitteln darstellt.[461] In diesem Zusammenhang ist zu klären, ob und wie der Zweck der Beobachtung erreicht werden kann und ob die gewählte Videoüberwachung hierzu überhaupt objektiv geeignet ist.[462] Ferner ist zu prüfen, ob der verfolgte Zweck auch mit einem milderen, d.h gleich effektiven, aber das Persönlichkeitsrecht der Mitarbeiter weniger einschränkenden,[463] Mittel hätte erreicht werden können.[464] Vom Umfang her muss sich die Videoüberwachung folglich sachlich und räumlich auf ein

[455] Zscherpe, in: Taeger/Gabel, BDSG, § 6b Rn. 51.
[456] Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 353 f.
[457] Bizer, in: Simitis, BDSG, § 6b Rn. 48; Müller, Die Zulässigkeit der Videoüberwachung am Arbeitsplatz, S. 456. Sollte dennoch das Bedürfnis des Arbeitgebers an einer Überwachung (z.B. um angetrunkene Beschäftigte aus den Räumlichkeiten zu verweisen) bestehen, liegt i.d.R. keine Erforderlichkeit der Überwachungsmaßnahme (s. hierzu sogleich) vor, vgl. Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 354.
[458] BAG, NZA 2004, 1278, 1283; NJOZ 2005, 2708, 2714.
[459] Der Zweck nach Nr. 3 gilt laut BT-Drs. 14/5793, S. 61 nur für nicht-öffentliche Stellen.
[460] Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 355.
[461] Bizer, in: Simitis, BDSG, § 6b Rn. 56.
[462] Zscherpe, in: Taeger/Gabel, BDSG, § 6b Rn. 51; Bizer, in: Simitis, BDSG, § 6b Rn. 56.
[463] Wedde, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 6b Rn. 39; Bayreuther, NZA 2005, 1038, 1040.
[464] Zscherpe, in: Taeger/Gabel, BDSG, § 6b Rn. 51.

notwendiges Maß beschränken.[465] Hierbei ist insbesondere in die Erwägungen einzubeziehen, ob der verstärkte Einsatz von Sicherheitspersonal oder die Verwendung von anderen Sicherheitseinrichtungen (z.B. Schlösser, Sicherheitskontrollen) den Zweck ebenfalls erfüllen würden, mithin auf eine Videoüberwachung verzichtet werden könnte.[466] Soweit dies der Fall ist, wäre die Videoüberwachung dann bereits mangels Erforderlichkeit unzulässig. Hinsichtlich der Durchführung der Überwachungsmaßnahmen ist u.a. auch auf das in § 3a BDSG statuierte Prinzip der Datenvermeidung und Datensparsamkeit zu verweisen.[467] Meist ist die Videoüberwachung unter mehreren gleich geeigneten Mitteln das eingriffsintensivere.[468] Ferner sind Kameras möglichst so zu installieren, dass so wenig personenbezogene Daten wie möglich erhoben werden, indem beispielsweise Videoaufnahmen nur dann gemacht werden, wenn dies wirklich erforderlich ist (z.B. während Bank- oder Ladenöffnungszeiten) und räumlich nur der Bereich erfasst wird, der für den verfolgten Zweck erforderlich ist.[469] Steht die Aufklärung von Inventurdifferenzen in Frage, darf eine Videoüberwachung der Arbeitnehmer erst dann durchgeführt werden, wenn im Vorfeld Maßnahmen der Innenrevision und Überprüfungen des Warenwirtschaftsystems sowie weitere Untersuchungen der Arbeitsabläufe im Ergebnis zu keinem Erfolg geführt haben.[470] Bei der Beurteilung der Frage, ob andere technische Alternativen vorliegen, muss erwogen werden, ob gespeicherte Aufzeichnungen notwendig sind oder ob ein Fernsehmonitoring ausreicht.[471] Letzteres wurde von der Rechtsprechung jedoch insbesondere für die Aufklärung von Diebstählen als nicht in gleicher Weise effizient eingestuft wie eine Aufzeichnung.[472] Der Ansatz, in die Erwägungen die Alternative einer menschlichen statt technischen Beobachtung durch Vorgesetzte und Kollegen einzubeziehen,[473] begegnet praktischen Bedenken. So wird kritisiert, dass eine gleiche Eignung des eingesetzten Mittels tendenziell eher nicht vorliegen wird, vor allem wenn das aufzuklärende Fehlverhalten auf Heimlichkeit angelegt ist.[474] Anzuzweifeln sei im Übrigen, ob eine betriebsinterne Bespitzelung die Persönlichkeitsrechte der Arbeitnehmer weniger tangiert als eine offene Videoüberwachung.[475]

---

[465] BAGE 127, 276 Rn. 20; BAG, NZA 2004, 1278, 128; Bergmann/Möhrle/Herb, BDSG, § 6b Rn. 27.
[466] Zscherpe, in: Taeger/Gabel, BDSG, § 6b Rn. 55 i.V.m. Rn. 51.
[467] Zscherpe, in: Taeger/Gabel, BDSG, § 6b Rn. 56; Wedde, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 6b Rn. 41.
[468] Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 356.
[469] Zscherpe, in: Taeger/Gabel, BDSG, § 6b Rn. 56
[470] BAG, NZA 2003, 1193, 1195; ArbG Düsseldorf, NZA-RR 2004, 345, 346.
[471] BAGE 127, 276 Rn. 27; BAG, NZA 2004, 1278, 1283.
[472] BAGE 127, 276 Rn. 27.
[473] BAG, NZA 2003, 1193, 1195; NZA 2004, 1278, 1283. Dies könne nach Ansicht des BAG durch eigens mit Überwachungsaufgaben befasste Mitarbeiter und unter Einbeziehung der Möglichkeit von Ausgangs- und Personenkontrollen geschehen, NZA 2004, 1278, 1283. Betriebsparteien sollen im Rahmen ihrer Einschätzungsprärogative aber auf solche Maßnahmen verzichten dürfen, wenn Diebesgut „nicht ohne weiteres als solches erkennbar ist", BAGE 127, 276 Rn. 27.
[474] BAG 2003, 1193, 1195; Grimm/Brock/Windeln, ArbRB 2006, 179, 180.
[475] Bayreuther, NZA 2005, 1038, 1040.

Angemessenheit,[476] § 6b Abs. 1 letzter HS. BDSG

Als finaler Schritt muss, wie sich aus § 6b Abs. 1 letzter HS. BDSG bereits ergibt, eine Angemessenheitskontrolle stattfinden. Hier hat eine Abwägung zwischen den mit der Videoüberwachung verfolgten Interessen des Arbeitgebers sowie den Überwachungszwecken einerseits und den schutzwürdigen Interessen der von der Beobachtung Betroffenen andererseits zu erfolgen.[477] Diesbezüglich kann es häufig zu Kollisionen von Verfassungsrechten kommen, wie etwa dem Recht auf informationelle Selbstbestimmung und dem Persönlichkeitsrecht auf der einen Seite und dem Schutz des Eigentums und der körperlichen Unversehrtheit (beispielsweise im Fall drohender Angriffe) auf Seiten des Arbeitgebers.[478] Welches Gewicht den Interessen der Beobachteten innerhalb der Abwägung zukommt, hängt maßgeblich von der Intensität des Eingriffs in das allgemeine Persönlichkeitsrecht ab.[479] Im Einzelnen können räumliche, zeitliche, personelle und technische Aspekte bei der Beurteilung eine Rolle spielen.[480] Bedeutsam für die Klassifizierung der Schwere des Eingriffs ist zum einen der Ort, an dem die Videoüberwachung stattfindet.[481] In jedem Fall unzulässig sind Beobachtungen, die die unantastbare Intimsphäre der beobachteten Menschen verletzen, so etwa die Observierung von Toiletten und Umkleidekabinen zur Diebstahlsprävention.[482] In der Regel wird sich die Beobachtung nicht auf die besonders schutzwürdige Privatsphäre auswirken, sondern vielmehr in die weniger schutzbedürftige Sozialsphäre eingreifen.[483] Hierbei muss beachtet werden, dass sich Arbeitnehmer in öffentlich zugänglichen Räumen in einem Umfeld befinden, in dem sie nicht davon ausgehen können, ständig unbeobachtet zu sein.[484] Darüber hinaus ist für das Ausmaß des von der Videoanlage ausgehenden Überwachungsdrucks die zeitliche Komponente bedeutsam.[485] Maßgeblich ist zum einen, ob die Überwachungsmaßnahme auf einen bestimmten Zeitraum begrenzt ist oder dauerhaft durchgeführt wird.[486] Zum anderen ist von Bedeutung, über wie viele Zeitstunden die Beobachtung wöchentlich erfolgt und ob die Arbeitnehmer Kenntnis von den Betriebszeiten der Anlage haben.[487] In quantitativer Hinsicht spielt die Anzahl der von der Überwachung betroffenen Personen eine Rolle.[488] Ferner ist bedeutend, ob der Betroffene einen zurechenbaren Anlass für die Überwachung geschaffen hat (z.B. durch eine Rechtsverletzung)

[476] Sog. Verhältnismäßigkeit im engeren Sinne, BVerfG, NJW 2008, 1505, 1515; BAGE 127, 276 Rn. 31.
[477] Grimm/Schiefer, RdA 2009, 329, 331. Gegebenenfalls müssen auch Grundrechte Dritter berücksichtigt werden. So hat das BAG mit Blick auf Videoüberwachungen von Postverteilungszentren neben dem Briefgeheimnis (Art. 10 GG) auch die Eigentumsrechte (Art. 14 GG) der potentiell von Postdiebstählen betroffenen Kunden in die Abwägung miteinbezogen, BAG, NZA 2004, 1278, 1283; E 127, 276 Rn. 21, 24.
[478] Zscherpe, in: Taeger/Gabel, BDSG, § 6b Rn 59.
[479] BAGE 127, 276 Rn. 21; Grimm/Schiefer, RdA 2009, 329, 331.
[480] Grimm/Schiefer, RdA 2009, 329, 331 f.
[481] Grimm/Schiefer, RdA 2009, 329, 331.
[482] BT-Drs. 14/5793, S. 62; Zscherpe, in: Taeger/Gabel, BDSG, § 6b Rn. 60.
[483] BAG, NZA 2003, 1193, 1195; ausführlich zu der vom BVerfG entwickelten Sphärenabstufung innerhalb des Persönlichkeitsrechts Wank, in: ErfK zum Arbeitsrecht, Art. 2 GG Rn. 60 (m.w.N.); Grimm/Schiefer, RdA 2009, 329, 331.
[484] BAG, NZA 2003, 1193, 1195.
[485] BAG, NZA 2004, 1278, 1281.
[486] BAG, NZA 2004, 1278, 1281.
[487] BAG, NZA 2004, 1278, 1284.
[488] BAGE 127, 276 Rn. 39; BAG, NZA 2004, 1278, 1284.

oder ob diese anlasslos vorgenommen wurde.[489] Jedoch kann zu berücksichtigen sein, dass diese Betroffenen durch die Überwachung die Möglichkeit der Entlastung vom Verdacht einer Straftat oder eines Fehlverhaltens erhalten.[490] In technischer Hinsicht ist für die Abwägung von Einfluss, ob der Arbeitgeber eine analoge oder digitale Aufzeichnungstechnik verwendet.[491] Mittels digitaler Videoaufzeichnung ist es möglich, das gewonnene Bildmaterial automatisiert zu verarbeiten, also auch vor allem einzelne Personen zu vergrößern und herausfiltern zu können.[492] Entsprechend intensiv kann der Eingriff in das Persönlichkeitsrecht ausfallen.[493] Noch kritischer ist der Einsatz sog. Thinking Cameras zu bewerten, die imstande sind, Bilder selbstständig nach vorgegebenen Mustern auszuwerten und bei Auffälligkeiten Alarm auszulösen.[494] Es kann auch der Fall vorliegen, dass der Betroffene vergleichsweise gering in seinen Interessen beeinträchtigt wird, wenn er für den Beobachtenden nicht erkennbar ist, vor allem weil die optisch-elektronische Einrichtung mit einer zu niedrigen Auflösung arbeitet.[495] Im Ergebnis verbieten sich jedoch pauschale Aussagen hinsichtlich der Interessenabwägung.[496]

Die gezielte Überwachung von Mitarbeitern

Als Beweggrund für eine gezielte Überwachung von Arbeitnehmern kommt der Verdacht einer Straftat oder eines sonstigen Fehlverhaltens in Betracht.[497]

Offene Videoüberwachung bei konkreter Verdachtslage

Maßgebend für die Beurteilung der Zulässigkeit der Videoüberwachungsmaßnahme ist der Grad und die Konkretisierung der Verdachtslage.[498] Laut BAG ist dieser anhand einer Würdigung der Gesamtumstände unter Abwägung der Intensität des Eingriffs und des Gewichts der ihn rechtfertigenden Gründe zu ermitteln.[499] Eine heimliche Videoüberwachung eines Arbeitnehmers[500] ist danach zulässig, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft sind, die verdeckte Videoüberwachung praktisch das einzig verbleibende Mittel darstellt und insgesamt

[489] BAGE 127, 276 Rn. 21.
[490] BAG, NZA 2003, 1193, 1195.
[491] Grimm/Schiefer, RdA 2009, 329, 332. Videoüberwachung unter Einsatz von Digitaltechnik stellt ein Verfahren automatisierte Verarbeitung i.S.d. § 3 Abs. 2 S. 1 BDSG dar, Wedde, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 6b Rn. 7; Bergmann/Möhrle/Herb, BDSG, § 6b Rn. 5. Für derartige Verfahren begründet § 4d Abs. 1 BDSG eine Meldepflicht nach Maßgabe des § 4e BDSG. Regelmäßig wird bei Videoüberwachungen zudem eine Vorabkontrolle i.S.d. § 4d Abs. 5 BDSG geboten sein, Scheja, in: Taeger/Gabel, BDSG, § 4d Rn. 65.
[492] Grimm/Schiefer, RdA 2009, 329, 332.
[493] BAG, NZA 2004, 1278, 1284.
[494] Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 844; Oberwetter, NZA 2008, 609, 610. Zu Smart Cameras und automatischer Verhaltensanalyse vgl. Hornung/Desoi, K&R 2011, 153.
[495] Zscherpe, in: Taeger/Gabel, BDSG, § 6b Rn. 65
[496] Auch so: Grimm/Schiefer, RdA 2009, 329, 332.
[497] Grimm/Schiefer, RdA 2009, 329, 332.
[498] Grimm/Schiefer, RdA 2009, 329, 332.
[499] St. Rspr. des BVerfG (NJW 2008, 1505, 1505 mit Verweis auf E 109, 279); BAG, NZA 2004, 1278, 1280 f.; NZA, 2008, 1187, 1190.
[500] Im konkreten Fall ging es um die Überwachung des Kassenbereichs eines Supermarktes.

nicht unverhältnismäßig ist.[501] Der für die offene Videoüberwachung notwendige Anfangsverdacht muss in persönlicher, räumlicher und funktionaler Hinsicht ausreichend konkret sein.[502] Als Maßstab wird vorgeschlagen, es vorauszusetzen, aber auch gleichzeitig genügen zu lassen, dass das behauptete Fehlverhalten fassbar, eingrenzbar und insgesamt wahrscheinlich ist.[503] Aus dem bloßen Umstand, dass sich der Verdacht nicht einzig und allein auf den beobachteten Mitarbeiter beschränkt, ergibt sich noch nicht die Unverhältnismäßigkeit einer Überwachung.[504] Diesbezüglich liegt eine Verhältnismäßigkeit in diesem Sinne vor, wenn die Überwachung dazu dient, den bereits räumlich und funktional konkretisierten Verdacht auf eine Person einzugrenzen.[505] Gleichzeitig kann eine derartige Überwachung das einzige Mittel darstellen, die übrigen Arbeitnehmer aus dem engen Kreis der Verdächtigen auszuschließen.[506] In den Beschlüssen zu den Briefverteilungszentren hat das BAG ebenfalls auf die Verdachtslage abgestellt.[507] Von der Grundaussage her lässt sich den Entscheidungen entnehmen, dass eine Videoüberwachung zumindest dann verhältnismäßig sein kann, wenn sie von einem auf konkrete Personen bezogenen Verdacht einer strafbaren Handlung abhängig gemacht und räumlich auf den Bereich des verdachtsauslösenden Vorfalls sowie zeitlich auf die Aufklärung des Vorfalls beschränkt wird.[508] Regelungen ohne jegliche räumliche, zeitliche und personelle Einschränkungen seien hingegen unzulässig, da ein weit größerer Kreis unbeteiligter Arbeitnehmer in die Überwachung einbezogen wird, mithin in die Persönlichkeitsrechte von sehr viel mehr Arbeitnehmern eingegriffen wird, ohne dass diese hierzu Anlass gegeben hätten.[509] Insofern darf auch keine Videoüberwachung zur bloßen Kontrolle des Leistungs- und Ordnungsverhaltens stattfinden.[510]

Gezielte Videoüberwachung unterhalb der Schwelle einer konkreten Verdachtslage

Nach wie vor von der Rechtsprechung unbeantwortet ist die Frage, ob eine gezielte Mitarbeiterüberwachung auch dann durchgeführt werden darf, wenn die Schwelle der hinreichend persönlich, räumlich und funktional konkretisierten Verdachtslage noch nicht erreicht wurde. Im Schrifttum wird vorgeschlagen, ein derartiges Vorgehen zumindest bei einer verdachtsunabhängigen Kontrolle des Leistungs- und Ordnungsverhaltens als unzulässig zu erachten.[511] Das Interesse des Arbeitgebers, die Arbeitsleistung des Arbeitnehmers im besonderen Maße qualitativ zu kontrollieren und damit in Relation zu dem zu entrichtenden Entgelt setzen zu können, vermag den durch den permanenten Überwachungsdruck intensiven Eingriff in das Persönlichkeitsrecht der Arbeitnehmer nicht zu rechtfertigen.[512]

[501] BAG NZA 2003, 1187, 1193.
[502] Bayreuther, NZA 2005, 1038, 1039.
[503] Bayreuther, NZA 2005, 1038, 1039.
[504] BAG, NZA 2003, 1193, 1195.
[505] BAG, NZA 2003, 1193, 1195.
[506] BAG, NZA 2003, 1193, 1195.
[507] BAG, NZA 2004, 1278; NZA, 2008, 1187, 1190.
[508] BAG, NZA, 2008, 1187, 1191.
[509] BAG, NZA, 2008, 1187, 1191.
[510] Bayreuther, NZA 2005, 1038, 1039.
[511] Bayreuther, NZA 2005, 1038, 1039; Grimm/Schiefer, RdA 2009, 329, 332.
[512] Grimm/Schiefer, RdA 2009, 329, 332.

Videoüberwachung bei besonderer Gefährdungslage

Es sind Fallgestaltungen denkbar, in denen zwar noch kein hinreichend konkreter Straftatverdacht gegen Arbeitnehmer vorliegt, das Bedürfnis nach Straftatprävention aufgrund der besonders hohen Gefahr der Begehung von Straftaten am Arbeitsplatz allerdings besteht. In derartigen Konstellationen sind die Arbeitgeberinteressen weniger stark gefährdet, mit der Folge, dass eine abstrakt-präventive Beobachtung nur ausnahmsweise in Betracht gezogen werden kann.[513] Voraussetzung hierfür ist das Vorliegen einer besonderen Gefährdungslage,[514] d.h. einer Gefahrenlage, die über die generell und überall bestehende Gefahr der Begehung von Straftaten hinausgeht.[515] Dies muss seitens des Arbeitgebers substantiiert dargelegt werden,[516] wobei die Darlegung hohen Anforderungen gerecht werden muss.[517] Neben der Höhe der Wahrscheinlichkeit von Straftatbegehungen kann auch ein etwaig zu erwartender Schaden ein zu würdigendes Kriterium darstellen.[518] Vorgeschlagen wird daher, die Abwägung zugunsten des Präventionsinteresses des Arbeitgebers und somit zu Lasten des Persönlichkeitsrechts der Mitarbeiter zu entscheiden, wenn schon vereinzeltes Fehlverhalten enorme Schäden verursachen kann.[519]

Die Videoüberwachung betriebsfremder Dritter

Meist steht in Unternehmen mit Publikumsverkehr nicht die gezielte Mitarbeiterüberwachung im Vordergrund, sondern stellt diese eine mehr oder minder erwünschte Reflexwirkung dar.[520] Primär wird es den Betreibern der optisch-elektronischen Einrichtungen darum gehen, ihr Hausrecht innerhalb der Grundstücksgrenzen[521] zu wahren und die Videoüberwachung zu präventiven Zwecken[522] oder als repressives Mittel zur Verfolgung von Straftätern einzusetzen.[523] Bislang ungeklärt ist, ob und inwieweit die von der Rechtsprechung aufgestellten Grundsätze gelten, wenn Mitarbeiter lediglich mit überwacht werden. Teilweise wird vorgeschlagen, die Konstellation genauso zu behandeln wie bei einer gezielten Mitarbeiterüberwachung.[524] Diese Ansicht stößt jedoch auf faktische Grenzen, da dann die inzwischen üblichen, verdachtsunabhängigen Videoüberwachungen zur Straftatprävention in Supermärkten, Banken, Museen oder auf Bahnsteigen unzulässig sind, sobald Mitarbeiter ins Aufnahmefeld der Kamera geraten, was praktisch nicht zu vermeiden ist.[525] So müssen etwa in Supermärkten das Sortiment überprüft und aufgefüllt sowie auf Bahnsteigen Abfallbehälter

[513] Bayreuther, NZA 2005, 1038, 1039.
[514] BAG, NZA 2004, 1278, 1283 f.
[515] Grimm/Schiefer, RdA 2009, 329, 332.
[516] BAG, NZA 2004, 1278, 1283.
[517] Grimm/Schiefer, RdA 2009, 329, 332.
[518] Grimm/Schiefer, RdA 2009, 329, 333.
[519] Grimm/Schiefer, RdA 2009, 329, 333 unter Rückgriff auf das bei Bayreuther (NZA 2005, 1038, 1039 Fn. 7) genannte Beispiel der Überwachung von Mitarbeitern einer Diamantschleiferei und dem zutreffenden Hinweis, dass generell sicherheitsrelevante Bereiche regelmäßig nicht öffentlich zugänglich sind.
[520] Grimm/Schiefer, RdA 2009, 329, 333.
[521] BGH, NJW 1995, 1955, 1957; Gola/Schomerus, BDSG, § 6b Rn. 16 (m.w.N.).
[522] Präventive Zwecke liegen insbesondere in der Vermeidung von Diebstählen, Sachbeschädigungen oder Störungen, BAG NZA 2008, 1187, 1193.
[523] Wedde, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 6b Rn. 33.
[524] Roloff, in Besgen/Prinz, Neue Medien und Arbeitsrecht, 2006, § 5 Rn. 39.
[525] Grimm/Schiefer, RdA 2009, 329, 333.

entleert werden. Eine andere Ansicht vertritt den Standpunkt, die Videoüberwachung sei immer dann als arbeitsplatzimmanent hinzunehmen, wenn sie gegenüber Dritten nach § 6b BDSG zulässig ist.[526] Dies wird als unzureichend empfunden,[527] da bei § 6b BDSG die schutzwürdigen Interessen aller Betroffenen, folglich auch die der beobachteten Mitarbeiter, zu berücksichtigen seien.[528] Gleichwohl wird herausgestellt, dass bei der Überwachung betriebsfremder Dritter als Hauptmotiv des Arbeitgebers ein präventiver Zweck als grundsätzlich legitim gewertet werden könne.[529] In diesem Punkt unterscheide sich die Interessenlage von der bei einer gezielten Mitarbeiterüberwachung.[530]

Zeitliche Grenzen des hinzunehmenden Überwachungs- und Anpassungsdrucks

Bislang ungeklärt bleibt die Frage, wie lange Arbeitnehmer den Überwachungs- und Anpassungsdruck ertragen müssen. In der Literatur werden Bestrebungen vorgenommen, in diesem Kontext zwischen den unterschiedlichen Betriebsbereichen zu differenzieren.[531] Bei der Überwachung des Außen- und Eingangsbereichs ist der genannte Druck dadurch, dass die Mitarbeiter dort selten ihre Arbeit verrichten, als eher gering zu klassifizieren.[532] Anders stellt sich die Lage bei dem öffentlich zugänglichen und für den Arbeitgeber sensibleren Innenbereich dar.[533] Auch wenn die Situation für den Arbeitnehmer einem ständigen Überwachungsdruck sehr nahe kommt, sollen die Interessen des Arbeitgebers im Verhältnis zu denen der Betroffenen zumindest dann als gewichtiger einzustufen sein, wenn die Videoüberwachung im Innenbereich das einzige erfolgversprechende Mittel, um präventiv gegen Straftaten von Kunden vorgehen zu können.[534] Dies wird zumindest für öffentlich zugängliche Unternehmen, in denen sich die Begehung bestimmter Straftaten[535] als geschäftstypisches Risiko darstellt, angenommen.[536] Einer Realisierung der Gefahr bedarf es dabei gerade nicht. Vielmehr sei es für den Betriebsinhaber unzumutbar, mit der Installation einer Videokamera so lange abzuwarten, bis er selbst erstmalig Opfer einer solchen Straftat wird.[537] Der Betriebsinhaber sieht sich bei der Straftatgefahr durch Kunden einem deutlich größeren, typischerweise anonymen potentiellen Täterkreis ausgesetzt als dies im Fall der Straftatbegehung von Beschäftigten der Fall wäre.[538] Das von Art. 14 GG geschützte Interesse des Arbeitgebers an der Wahrung seines Hausrechts und Schutz seines Eigentums wiegt entsprechend schwer.[539] Im Gegensatz dazu handelt es sich auf Arbeitnehmerseite um einen

[526] Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 816. Vgl. ferner SG München RDV 1992, 85.
[527] Grimm/Schiefer, RdA 2009, 329, 333.
[528] Bayreuther, NZA 2005, 1038, 1039; Grimm/Schiefer, RdA 2009, 329, 333.
[529] Bayreuther, NZA 2005, 1038, 1039; Grimm/Brock/Windeln, ArbRB 2006, 179, 180; Grimm/Schiefer, RdA 2009, 329, 333.
[530] So Grimm/Schiefer, RdA 2009, 329, 333 unter Rückgriff auf die Rechtsprechung des BAG (NZA 1187, 1193).
[531] Grimm/Schiefer, RdA 2009, 329, 333.
[532] Grimm/Schiefer, RdA 2009, 329, 333.
[533] Grimm/Schiefer, RdA 2009, 329, 333.
[534] Grimm/Schiefer, RdA 2009, 329, 333.
[535] Z.B. Ladendiebstähle in einem Kaufhaus oder Überfälle in einer Bankfiliale, Bayreuther, NZA 2005, 1038, 1039.
[536] Bayreuther, NZA 2005, 1038, 1039; Wiese, in: Festschr. f. E. Lorenz , S. 915, 925.
[537] Bayreuther, NZA 2005, 1038, 1039.
[538] Grimm/Schiefer, RdA 2009, 329, 333.
[539] Grimm/Schiefer, RdA 2009, 329, 333; ähnlich auch BAG, NZA, 1193, 1195.

relativ geringfügigen Eingriff in das Persönlichkeitsrecht, wenn deren Überwachung nicht Zweck, sondern nur unbeabsichtigte Nebenfolge einer präventiven Videoüberwachung ist.[540] Meist werden sich Arbeitnehmer nur vorübergehend im Fokus der Kamera aufhalten.[541] Ferner ist zu beachten, dass bspw. bei der Überwachung von Bankfilialen die Überwachung auch letztlich ihrer eigenen Sicherheit dient.[542] Vor dem Hintergrund, in das Persönlichkeitsrecht so gering wie möglich einzugreifen, dürfen Videoanlagen gerade nicht zweckwidrig eingesetzt werden, um Mitarbeiter gezielt zu überwachen.[543] Zur Prävention von Kaufhausdiebstählen reicht es bspw. aus, die Kamera auf den Kassengang auszurichten, anstatt mittels Ausrichtung auf die Registrierkasse das Verhalten des Arbeitnehmers zu beobachten.[544] Hierzu müsste vielmehr wiederum eine konkrete Verdachtslage vorliegen.[545]

2.4.2.1.3. Heimliche Videoüberwachung in öffentlich zugänglichen Räumen trotz § 6b Abs. 2 BDSG?

Das BAG hat eine heimliche Videoüberwachung in öffentlich zugänglichen Räumen bei einem konkreten Verdacht einer Straftat oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers für zulässig erachtet, wenn weniger einschneidende Aufklärungsmaßnahmen ausgeschöpft waren, die verdeckte Videoüberwachung somit für die Betriebspraxis das einzige verbleibende Mittel darstellte und insgesamt nicht unverhältnismäßig war.[546] Aufgrund der Tatsache, dass bei einer heimlichen Videoüberwachung vorheriger Rechtsschutz faktisch verwehrt und nachträglicher Rechtsschutz erschwert werden, wiegt diese nach der Rechtsprechung schwerer als eine offene Überwachung.[547] Ob hieran trotz der Einführung des § 6b BDSG und dem damit verbundenen Erfordernis, den Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen (§ 6b Abs. 2 BDSG), festgehalten werden kann, ist umstritten. Telos der Norm ist vor allem die Sicherstellung von Transparenz.[548] Der Betroffene soll sein Verhalten danach ausrichten können, dass es möglicherweise beobachtet wird, oder der Beobachtung ausweichen.[549] Damit ist die Erkennbarkeit Rechtmäßigkeitsvoraussetzung von Videoüberwachungen öffentlich zugänglicher Räume.[550] Welche Anforderungen an die Erkennbarkeit zu stellen sind, wird uneinheitlich beantwortet. Einerseits soll bereits die Installation der Kamera, die beim Betreten des öffentlichen Raumes erkannt wird, ausreichend sein, andererseits wird das Aufhängen eines Schildes oder sogar die Kennzeichnung, ob gerade nur beobachtet oder aufgezeichnet wird, verlangt.[551] Andere sehen zwar kein

[540] Grimm/Schiefer, RdA 2009, 329, 333.
[541] Grimm/Schiefer, RdA 2009, 329, 333.
[542] Grimm/Schiefer, RdA 2009, 329, 333 f.
[543] Grimm/Schiefer, RdA 2009, 329, 334.
[544] Grimm/Schiefer, RdA 2009, 329, 334; vgl. hierzu auch BAG, NZA, 1193, 1195.
[545] Grimm/Schiefer, RdA 2009, 329, 334; vgl. hierzu auch BAG, NZA, 1193, 1195.
[546] BAG, NZA 2003, 1193, 1195; offen gelassen von LAG Sachsen-Anhalt – 11 Sa 522/07.
[547] BVerfG, NJW 2008, 1505, 1507 f.; BAG, NZA 2008, 1187, 1190.
[548] BT-Drucks. 14/4329, S. 38.
[549] Zscherpe, in: Taeger/Gabel, BDSG, § 6b Rn. 66.
[550] AG Frankfurt – 7 Ca 3342/05 Rn. 53; Bayreuther, NZA 2005, 1038, 1040, Roloff, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 5 Rn. 38; Maschmann, NZA 2002, 13, 17; zweifelnd: Gola/Schomerus , BDSG, § 6b Rn. 28.
[551] Zum Meinungsbild vgl. Gola/Schomerus, BDSG, § 6b Rn. 25 f.; Bizer, in: Simitis, BDSG, § 6b Rn. 68, 70.

Erfordernis einer detaillierten Information über die Art und Weise der Überwachung, verlangen aber zumindest einen erkennbaren Hinweis auf die Kamera, was eine verdeckte Vorgehensweise ausschließt.[552] Wie sich aus dem Wortlaut ergibt,[553] handelt es sich bei der Kenntlichmachung der Beobachtung um eine Verpflichtung der verantwortlichen Stelle.[554] Entsprechend wird teilweise vertreten, dass heimliche Videoüberwachung per se und ausnahmslos unzulässig ist, und dies trotz der damit verbundenen Folge, dass Arbeitgebern das im Einzelfall einzige effektive Mittel zur Aufklärung von Straftaten genommen wird, wenn deren Begehung gerade auf Heimlichkeit angelegt ist.[555] So wird sich gegen die Anerkennung von Ausnahmen vom Verbot der heimlichen Videoüberwachung über einen Rückgriff auf die allgemeinen Rechtfertigungs- und Entschuldigungsgründe[556] ausgesprochen.[557] Dem steht eine Vielzahl von Vertretern gegenüber, die die Anwendbarkeit der allgemeinen Rechtfertigungs- und Entschuldigungsgründe bejahen.[558] Angeführt wird für letztgenannte Ansicht insbesondere, dass, wenn der Gesetzgeber die Anwendbarkeit dieser rechtsgebietsübergreifenden Prinzipien ausnahmsweise für das Gebiet des Datenschutzrechts hätte ausschließen wollen, es hierfür einer ausdrücklichen Ausschlussregelung bedurft hätte.[559] Lässt man diese Argumentation gelten, ist in Ausnahmekonstellationen die Durchführung einer heimlichen Videoüberwachung in öffentlich zugänglichen Räumen trotz § 6b Abs. 2 BDSG möglich und kann an der Rechtsprechung des BAG festgehalten werden.

2.4.2.1.4. Rechtmäßigkeit der weiteren Verwendung, § 6b Abs. 3-5 BDSG

Aus der Zulässigkeit der Beobachtung nach § 6b Abs. 1 BDSG folgt nicht automatisch die Zulässigkeit der Verarbeitung oder Nutzung gewonnener personenbezogener Daten nach Abs. 3, sondern bedarf diese einer separaten Prüfung.[560] Nach § 6b Abs. 3 S.1 BDSG ist die Verarbeitung oder Nutzung von nach Abs. 1 erhobenen Daten zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Als Folge muss für jeden Verarbeitungsschritt der durch die Kamerabeobachtung gewonnen Daten eine eigenständige Interessenabwägung vorgenommen werden.[561] Sind die Daten zur Erreichung des Zwecks nicht mehr erforderlich oder stehen schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegen, sind sie unverzüglich,[562] d. h. in der Regel innerhalb von ein bis zwei

---

[552] Bizer, in: Simitis, BDSG, § 6b Rn. 67; Grimm/Schiefer, RdA 2009, 329, 334.
[553] „Sind“, vgl. § 6b Abs. 2 BDSG.
[554] Zscherpe, in: Taeger/Gabel, BDSG, § 6b Rn. 66; Grimm/Schiefer, RdA 2009, 329, 334.
[555] Bayreuther, NZA 2005, 1038, 1040 f.; Grimm/Schiefer, RdA 2009, 329, 334.
[556] Als Rechtfertigungstatbestände können sowohl Notwehr (§§ 227 BGB, § 32 StGB) als auch Notstand (§ 34 StGB) in Betracht kommen, Grimm/Schiefer, RdA 2009, 329, 334.
[557] Bayreuther, NZA 2005, 1038, 1040 f.
[558] ArbG Freiburg – 4 Ca 128/04; Grosjean, DB 2003, 2650, 2651; Grimm/Brock/Windeln, ArbRB 2006, 179, 181. Zu den weiteren Einzelheiten vgl. Grimm/Schiefer, RdA 2009, 329, 334 f.
[559] Grosjean, DB 2003, 2650, 2651; Grimm/Brock/Windeln, ArbRB 2006, 179, 181, Grimm/Schiefer, RdA 2009, 329, 334.
[560] BT-Drs. 14/5793, S. 62; Schaffland/Wiltfang, BDSG, § 6b Rn. 5; Bizer, in Simitis, BDSG, § 6b Rn. 75; Zscherpe, in: Taeger/Gabel, BDSG, § 6b Rn. 76.
[561] Bizer, in: Simitis, BDSG, § 6b Rn. 75.
[562] Folglich ohne schuldhaftes Zögern, vgl. § 121 Abs. 1 S.1 BGB, Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 359.

Arbeitstagen,[563] zu löschen (§ 6b Abs. 5 BDSG). Am wirksamsten wird dem Löschungsgebot durch eine automatisierte periodische Löschung, etwa durch Selbstüberschreiben zurückliegender Aufnahmen, entsprochen.[564] Wiederum kommt dem Grundsatz der Datenvermeidung und Datensparsamkeit (§ 3a BDSG) in diesem Zusammenhang entscheidende Bedeutung zu.[565] Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, besteht eine Benachrichtigungspflicht bezüglich der Verarbeitung oder Nutzung entsprechend den §§ 19a und 33 BDSG, vgl. § 6b Abs. 4 BDSG. Besondere Bedeutung erhält die in § 6b Abs. 3 S. 1 BDSG genannte Zweckbindung, die einzelfallabhängig ermittelt werden muss.[566] Die Zulässigkeit jeder weiteren Verarbeitung der Aufnahmen orientiert sich streng an dem nach § 6b Abs. 1 BDSG festzulegenden konkreten Zweck der Beobachtung.[567] Eine Verarbeitung oder Nutzung der Daten zu anderen Zwecken ist nur unter den in § 6b Abs. 3 S. 2 BDSG genannten Voraussetzungen möglich, d.h. soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

2.4.2.2. Videoüberwachung nicht öffentlich zugänglicher Räume

Nach welchen Maßstäben sich die Videoüberwachung in nicht öffentlich zugänglichen Räumen richtet, ist ebenfalls ungeklärt.[568] Unter nicht öffentlich zugänglichen Räumen sind sämtliche Räumlichkeiten zu verstehen, die nur von einem bestimmten Personenkreis betreten werden dürfen.[569]

2.4.2.2.1. Rechtfertigung durch Einwilligung

Wiederum ausgehend von dem in § 4 Abs. 1 BDSG statuierten präventiven Verbot mit Erlaubnisvorbehalt kann sich die Zulässigkeit der Videoüberwachung nicht öffentlich zugänglicher Räume aus einer Einwilligung der Arbeitnehmer ergeben, sofern man eine solche Rechtfertigungsmöglichkeit im Beschäftigungskontext zulässt.[570]

2.4.2.2.2. Keine analoge Anwendung des § 6b BDSG

Angedacht werden könnte, § 6b BDSG als andere Rechtsvorschrift i.S.d. § 4 Abs. 1 BDSG analog für die Videoüberwachung nicht öffentlich zugänglicher Arbeitsplätze heranzuziehen. Voraussetzung für eine Analogie ist das Vorliegen einer planwidrigen Regelungslücke sowie einer vergleichbaren Interessenlage.[571] Es liegt aber bereits keine planwidrige Regelungslücke vor.[572] So fand seitens des Gesetzgebers eine bewusste Beschränkung des Anwendungsbereichs des § 6b BDSG auf öffentlich zugängliche Räume statt und wurde die

---

[563] BT-Drs.14/5793, S. 63.
[564] BT-Drs.14/5793, S. 63.
[565] BT-Drs.14/5793, S. 63.
[566] Zscherpe, in: Taeger/Gabel, BDSG, § 6b Rn. 77.
[567] Grimm/Schiefer, RdA 2009, 329, 335.
[568] Grimm/Schiefer, RdA 2009, 329, 335. Maßnahmen zur reinen Schikane der Beschäftigten verbieten sich hingegen (§ 226 BGB), Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 361.
[569] Bizer, in: Simitis, BDSG, § 6b Rn. 43.
[570] Siehe bereits oben, Gliederungspunkt 1.3.2.4.1.
[571] Vgl. etwa das Sondervotum der Richterin Haas, BVerfGE 115, 51, 74: „Eine Analogie setzt voraus, dass eine vom Gesetzgeber unbeabsichtigt gelassene Lücke vorliegt und diese Planwidrigkeit auf Grund konkreter Umstände positiv festgestellt werden kann."
[572] BAG NZA 2004, 1278, 1282; Maties, NJW 2008, 2219, 2221.

Erforderlichkeit besonderer Regelungen betont, etwa im Rahmen eines separaten Arbeitnehmerdatenschutzgesetzes.[573] Auch fehlt eine vergleichbare Interessenlage. Im Gegensatz zu öffentlich zugänglichen Orten handelt es sich nicht um einen überwiegend anonymen Personenkreis, der nur kurzfristig von der Kamera erfasst wird; vielmehr sind die überwachten Arbeitnehmer dem Arbeitgeber an nicht öffentlich zugänglichen Arbeitsplätzen bekannt.[574] Da die Arbeitnehmer über einen längeren Zeitraum an ihrem jeweiligen Arbeitsplatz verweilen und aufgrund der vertraglichen Verpflichtung regelmäßig keine Möglichkeit haben, einer Überwachung auszuweichen, sind sie einem ungleich größeren Überwachungs- und Anpassungsdruck ausgesetzt.[575] Die Tatsache, dass die Eingriffsintensität in öffentlich zugänglichen Räumen im Einzelfall höher sein kann als in nicht öffentlich zugänglichen Räumen,[576] steht nicht im Widerspruch dazu, dass bei der Schaffung des § 6b BDSG eher weniger intensive Eingriffe im Fokus des Gesetzgebers lagen.[577]

2.4.2.2.3. Eingriffsnormen der §§ 28, 32 BDSG

Soweit § 6b BDSG – wie im Fall von Videoüberwachungsmaßnahmen im nicht öffentlich zugänglichen Raum – unanwendbar ist, bestimmt sich die Zulässigkeit der Videoüberwachungsmaßnahmen in Abhängigkeit von dem mit der Überwachungsmaßnahme verfolgten Zweck nach den §§ 28, 32 BDSG.[578]

Offene Überwachung

Für repressive Zwecke findet § 32 Abs. 1 S. 2 BDSG bei der offenen Videoüberwachung nicht öffentlich zugänglicher Räume zwar Anwendung, dürfte aber in der Regel zur Überführung des Täters unbrauchbar sein.[579] Andere Fälle sind an § 32 Abs. 1 S. 1 BDSG und nach Auffassung der Regierungsbegründung auch an § 28 Abs. 1 Nr. 2 BDSG zu messen.[580] Wie bei § 6b BDSG muss die Maßnahme nicht nur geeignet und erforderlich, sondern ebenfalls angemessen sein, was wiederum einer vom Einzelfall abhängigen Rechtsgüterabwägung bedarf.[581] Laut Regierungsbegründung sind dieser Abwägung die vom BAG entwickelten datenschutzrechtlichen Grundsätze zugrunde zu legen,[582] wobei hier wiederum insbesondere dem Verhältnismäßigkeitsgrundsatz Rechnung zu tragen ist.[583] Unter engen Voraussetzungen kann eine Interessenabwägung zu Lasten der Arbeitnehmer ausfallen,[584] wenn es sich bei der Mitarbeiterüberwachung in nicht-öffentlichen Räumen um einen Nebeneffekt anderer Überwachungszwecke handelt[585] und die Maßnahme auch dem

[573] BT-Drs. 14/4329, S. 38.
[574] Grimm/Schiefer, RdA 2009, 329, 336.
[575] BAG, NZA 2004, 1278, 1282.
[576] Bayreuther, NZA 2005, 1038, 1041.
[577] Grimm/Schiefer, RdA 2009, 329, 336.
[578] Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 347 f.
[579] Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 360.
[580] Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 361, der weiterhin (a.a.O., Rn. 348) ausführt, ob überhaupt noch Raum für eine Anwendung des § 28 Abs. 1 S. 1 Nr. 2 BDSG bleibt.
[581] Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 362.
[582] BT-Drs. 16/13657, S. 35.
[583] BAGE 127, 276 Rn. 17; vgl. zu der Rechtsgüterabwägung im Einzelnen die überblicksartige Darstellung bei Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 362 ff.
[584] BAG, NZA 2004, 1278, 1283.
[585] Grimm/Schiefer, RdA 2009, 329, 337.

Schutz der dort beschäftigten Arbeitnehmer dient oder ein schützenswertes arbeitgeberseitiges Sicherheitsinteresse besteht.[586]

Heimliche Überwachung

Im Bereich nicht öffentlich zugänglicher Räume tritt das Problem, ob § 6b Abs. 2 BDSG eine Sperrwirkung entfaltet, nicht auf.[587] Nach der Regierungsbegründung ist vielmehr eine spezialgesetzliche Regelung für die heimliche Überwachung vonnöten.[588] Hinsichtlich der Interessenabwägung ist wiederum zu beachten, dass die Abwehrmöglichkeiten der Arbeitnehmer bei einer heimlichen Überwachung erschwert sind.[589] Letztere kann aufgrund der hohen Eingriffsintensität nur als ultima ratio in Betracht kommen.[590] Ferner darf in dem Bereich der Intimsphäre (also beispielsweise in Duschen, Umkleidekabinen oder Toiletten) keine Videoüberwachung stattfinden.[591]

2.5. Mitarbeiterüberwachung via Zugangskontrollsystemen[592]

Eine gängige Methode, um den Zugang unbefugter Dritter zu dem Betriebsgelände sowie zu sensiblen Firmenbereichen zu unterbinden, ist die Verwendung von Zugangskontrollsystemen.[593] Je nach Ausgestaltung der verwendeten Systeme können Mitarbeiter u.U. nur zu bestimmten Bereichen Zugang erhalten.[594]

2.5.1. Darstellung der gängigen Systeme

Im Einzelnen lässt sich mit Blick auf die technische Ausgestaltung zwischen mehreren gebräuchlichen Systemtypen differenzieren.

2.5.1.1. Einsatz von Transpondersystemen[595]

Zum einen kann der Zugang mithilfe von Transpondern[596] und Lesefeldern kontrolliert werden.[597] Um Zutritt zu einem Bereich zu erhalten, muss der Transponder vor ein Transponderfeld gehalten werden, um so die auf dem Transponder hinterlegten Daten (bspw. ID-Nummer eines Angestellten) an das System zu übermitteln.[598] Sofern der Besitzer des

---

[586] LAG Mannheim, RDV 2000, 27, 27 f.; LAG Köln, BB 1997, 475, 476. Ein Bedürfnis zur Überwachung von Maschinen oder produzierenden Anlagen kann sich in z.B. in der Kernenergie- oder Chemiebranche ergeben, Roloff, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 5 Rn. 29.
[587] Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 368.
[588] BT-Drs. 14/4329, S. 38.
[589] Siehe bereits oben, Gliederungspunkt 2.4.2.1.4.
[590] BAG, NZA 2003, 1193, 1195; Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 175.
[591] Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 175.
[592] Eine Videoüberwachung kann ebenfalls zum Zweck der Zugangskontrolle eingesetzt werden. Aufgrund des Umfangs und im Sinne einer übersichtlicheren Darstellung wird dieses Thema separat behandelt, vgl. Gliederungspunkt 2.4. An dieser Stelle erfolgt eine Auseinandersetzung mit Transpondersystemen, biometrischen Systemen und der RFID-Technologie.
[593] Meyer, K&R 2009, 14, 16.
[594] Meyer, K&R 2009, 14, 16.
[595] Der Begriff „Transponder“ setzt sich aus den Wörtern „transmitter“ (Sender) und „responder“ (Antwortsender) zusammen, Däubler, Gläserne Belegschaften?, S. 184 Fn. 141.
[596] Entweder via Chipkarte oder Coin, vgl. Roloff, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 5 Rn. 53.
[597] Meyer, K&R 2009, 14, 16.
[598] Meyer, K&R 2009, 14, 16.

Transponders legitimiert ist, wird ihm der Zugang gewährt.[599] Dabei kann das System so eingestellt werden, dass die Transponder den Zutritt nur zu bestimmten Bereichen oder Zeiten zulassen,[600] mithin in raumzeitlicher Hinsicht. Jedenfalls komplexere Transpondersysteme weisen eine zentrale, rechnerbasierte Steuerung auf, die die systematische Erfassung der Verwendung der Transponder und somit die Erstellung von Bewegungsprofilen ermöglicht.[601] Da die Mitarbeiter regelmäßig ihren persönlichen Transponder erhalten und diesen auch bei sich führen müssen, wird – abhängig von der sich aus der Anzahl der Transponderfelder ergebenen Kontrolldichte – eine verhältnismäßig präzise Mitarbeiterortung ermöglicht.[602] Hierdurch können unter Einsatz von entsprechender Software beispielsweise Rückschlüsse auf den Aufenthaltsort eines Mitarbeiters oder dessen Kontakt zu anderen Mitarbeitern gezogen werden.[603]

2.5.1.2. Einsatz biometrischer Systeme

Eine Realisierung von Zugangskontrollen kann auch über den Abgleich biometrischer Daten erfolgen. Als biometrische Charakteristika können physiologische beziehungsweise passive (z.B. Fingerabdruck, Gesichts- Iris- oder Venenerkennung) oder verhaltensbedingte beziehungsweise aktive (z.B. Stimmerkennung, Unterschrift, Tippmuster bei Eingabe eines Passwortes) dienen.[604] Durch den Einsatz biometrischer Techniken wird die Identifikation von Personen somit allein aufgrund ihrer persönlichen und individuellen Körpermerkmale ermöglicht.[605] Dem Einsatz derartiger Zugangskontrollsysteme werden insbesondere deshalb Bedenken entgegengesetzt, weil die biometrischen Informationen über die Arbeitnehmer in einer zentralen Datenbank gespeichert werden.[606] Biometrische Daten können einzelfallbezogen und in Abhängigkeit von der konkreten Nutzungsart[607] als besondere Art personenbezogener Daten i.S.d. § 3 Abs. 9 BDSG qualifiziert werden.[608] Während dies nicht der Fall ist, wenn die bloße Überprüfung der Zutrittslegitimation eines Mitarbeiters in Frage steht, würden etwa Rückschlüsse auf das Gesundheitsbild eines Mitarbeiters unter Zuhilfenahme gewonnener biometrischer Daten rechtlich anders zu beurteilen sein.[609] Festzuhalten ist aber zumindest, dass biometrische Daten sensible Informationen darstellen.[610] Entsprechend vorsichtig und zurückhaltend muss mit ihnen umgegangen werden, um einen Datenmissbrauch zu verhindern. Setzt man Transpondersysteme und biometrische Abgleiche in Verhältnis zueinander, ist ersteren aufgrund der geringeren Eingriffsintensität bei Mitarbeiterkontrollen der Vorzug einzuräumen.[611]

---

[599] Meyer, K&R 2009, 14, 16.
[600] Meyer, K&R 2009, 14, 16.
[601] Meyer, K&R 2009, 14, 16.
[602] Meyer, K&R 2009, 14, 16.
[603] Meyer, K&R 2009, 14, 16.
[604] Gola/Wronka, Handbuch des Arbeitnehmerdatenschutzes, Rn. 874; Bartmann/Wimmer, DuD 2007, 199.
[605] Raif, ArbRAktuell 2010, 359.
[606] Meyer, K&R 2009, 14, 17.
[607] Vgl. exemplarisch zu dieser h.M. Gola/Schomerus, BDSG, § 3 Rn. 56.
[608] Meyer, K&R 2009, 14, 17.
[609] Meyer, K&R 2009, 14, 17 mit der Feststellung, dass § 6a BDSG keine Anwendung findet.
[610] Meyer, K&R 2009, 14, 17.
[611] Meyer, K&R 2009, 14, 17; ähnlich Roloff, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 5 Rn. 66.

2.5.1.3. Einsatz von RFID-Technik[612]

RFID-Systeme ermöglichen eine im Vergleich zu den zuvor genannten Maßnahmen wesentlich genauere Kontrolle von Arbeitnehmern, indem mittels Funketiketten (sog. RFID-Tags) auf einem Chip gespeicherte Informationen berührungslos abgerufen werden können.[613] Aufgrund der geringen Größe können die Tags problemlos für Hausausweise oder andere Anwendungen verwendet,[614] im Extremfall sogar auf der Kleidung angebracht werden.[615] Mithilfe von RFID-Technolgie werden personenbezogene Daten verarbeitet, wenn Informationen auf einem RFID-Tag mit den Identifizierungsdaten einer Person (Foto, Name, Anschrift, wiederkehrende Kennnummer) verknüpft werden beziehungsweise werden können.[616] Die Lesereichweite befindet sich je nach RFID-Anwendung im zweistelligen Meterbereich.[617]

2.5.2. Fälle aus der Rechtsprechung

Rechtsprechung mit Bezug zu Zugangskontrollsystemen liegt bisher erst in geringem Umfang vor,[618] RFID-Systeme waren bislang noch nicht Gegenstand gerichtlicher Entscheidungen. Vorgeschlagen wird aber, auf die Ausführungen der Rechtsprechung zu der Videoüberwachung zurückzugreifen.[619]

2.5.3. Wissenschaftliche Auseinandersetzung

Wie bereits dargestellt, wird die datenschutzrechtliche Zulässigkeit danach beurteilt, ob der Datenumgang von einer Einwilligung des Betroffenen[620] oder einem gesetzlichen Erlaubnistatbestand gedeckt ist. Bei der Verwendung personalisierter Transponder werden personenbezogene Daten erhoben und verarbeitet, so dass sich die rechtliche Bewertung des Einsatzes derartiger Systeme nach dem BDSG beurteilt.[621] Findet hingegen durch das System lediglich ein Abgleich dergestalt statt, dass die Zugehörigkeit eines Mitarbeiters zu einer Gruppe von Zugangsberechtigten im Zentrum steht und damit die einzelne Person an sich nicht erfasst wird, wird der für die Anwendbarkeit des BDSG vorauszusetzende

---

[612] Häufig spricht man in diesem Zusammenhang auch von sog. Ubiquitous Computing (allgegenwärtige Datenverarbeitung), vgl. Buchner, in: Taeger/Gabel, BDSG, § 3 Rn. 18.

[613] Vgl. zur Funktionsweise von RFID Gräfin von Westerholt/Döring, CR 2004, 710, 710; Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutzrecht, Rn. 870. Allgemein zu den Grundlagen der RFID-Technologie, zu dem Aufbau der Systeme aus Transponder (Tag), Schreib-/Lesegerät (Reader) und RFID-Middleware sowie zu der Differenzierung zwischen aktiven und passiven Tags vgl. John, in: Kilian/Heussen/Computerrechts-Handbuch, 3. Abschnitt, Teil 300 Rn. 1 ff.

[614] Gola/Schomerus, BDSG, § 6c Rn. 2a; Gräfin von Westerholt/Döring, CR 2004, 710, 711.

[615] Däubler,Gläserne Belegschaften?, Rn. 324a.

[616] Art-29-Datenschutzgruppe, RFID, S. 29, abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_de.pdf; Buchner, in:Taeger/Gabel, BDSG, § 3 Rn. 18.

[617] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 78 mit Verweis auf die Ausführungen zu der Technik bei Hansen/Wiese, DuD 2004, 109. John, in: Kilian/Heussen, Computerrechts-Handbuch, 3. Abschnitt, Teil 300 Rn. 9 nennt eine Reichweite bei Long-Range-Systemen von bis zu 30m bei Einsatz aktiver Tags.

[618] Z.B. BAG, RDV 2004, 122 (Mitbestimmung bei biometrischem Zugangskontrollsystem).

[619] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 82.

[620] Sofern man diese Möglichkeit zulässt, siehe Gliederungspunkt 1.3.2.4.1.

[621] Meyer, K&R 2009, 14, 17.

Personenbezug gerade nicht hergestellt.[622] Im Geltungsbereich des BDSG richtet sich die Bewertung der Rechtmäßigkeit der Maßnahmen wiederum nach Maßgabe der Eingriffsnormen der §§ 28, 32 BDSG unter Zugrundelegung der genannten Prüfungskriterien. Denkbar ist zunächst die Erfassung von Anwesenheitszeiten durch die Zugangskontrollsysteme, wenn die entsprechenden Daten zur Ermittlung von Arbeitszeit und Vergütung benötigt werden.[623] Ebenfalls wird die Zulässigkeit einer Arbeitnehmerortung auf dem eigenen Betriebsgelände für den Fall befürwortet, dass auf Seiten des Arbeitgebers besondere Gründe für die Nutzung eines weitreichenden Zugangskontrollsystems vorliegen, z.B. aufgrund eines besonderen Sicherungsbedürfnisses oder wegen der Eigenart des Betriebes.[624] Hierunter sollen etwa Betriebe fallen, die mit besonders gefährlichen Materialien umgehen oder deren internes Firmenwissen besonders schützenswert ist.[625] Ohne Vorliegen eines entsprechenden Sicherungsbedürfnisses sollen zumindest keine biometrischen Techniken eingesetzt werden dürfen.[626] Ferner ist zu beachten, dass biometrische Verfahren die Kenntnis des Arbeitnehmers von deren Einsatz voraussetzt.[627] Einem heimlichen Abgleich biometrischer Daten dürfte zudem entgegenstehen, dass der Arbeitgeber Kenntnis von Eigenschaften i.S.d. § 1 AGG erhalten kann,[628] beispielsweise in Bezug auf den Gesundheitszustand oder die Herkunft des Arbeitnehmers.[629] Eine Speicherung solcher Merkmale sowie sensibler Daten i.S.v. § 3 Abs. 9 BDSG ist regelmäßig an die Einwilligung des Mitarbeiters geknüpft.[630] Eine Rechtfertigung des Speicherns kann sich ebenfalls nicht aus einer Betriebsvereinbarung ergeben, da sich die Zulässigkeit der Verarbeitung von sensitiven Daten gem. § 28 Abs. 6 BDSG nur aus einer Einwilligung des Betroffenen oder bei Vorliegen eines der Ausnahmetatbestände nach § 28 Abs. 6, 7 oder 9 BDSG in Betracht kommt.[631] Aus datenschutzrechtlicher Sicht noch skeptischer muss der Einsatz von RFID-Systemen betrachtet werden.[632] Im Gegensatz zu den o.g. Techniken gestaltet sich der Einsatz der Tags für Arbeitnehmer oft nicht ausreichend transparent.[633] Werden etwa RFID-Lesegeräte flächendeckend auf dem Betriebsgelände installiert, können präzise und lückenlos Bewegungsprofile von Mitarbeitern erstellt werden, ohne dass diese hieran mitwirken müssten.[634] Aufgrund der erhöhten Missbrauchsgefahr der RFID-Systeme müssen im Vergleich zu anderen Techniken erhöhte Schutzanforderungen bei deren Nutzung gestellt

---

[622] Roloff, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 5 Rn. 55. Zu denken ist hier beispielsweise an den Einsatz von Transpondern ohne individuelle ID, Meyer, K&R 2009, 14, 17.
[623] Zöll, in: Taeger/Gabel, BDSG, § 32 Rn. 22; Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 885.
[624] Meyer, K&R 2009, 14, 17.
[625] Roloff, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 5 Rn. 68.
[626] Roloff, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 5 Rn. 71.
[627] Raif, ArbRAktuell 2010, 359.
[628] Raif, ArbRAktuell 2010, 359.
[629] Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 875; Steinkühler/Raif, AuA 2009, 213, 217.
[630] Raif, ArbRAktuell 2010, 359. Vertreter einer strengeren Ansicht (Oberwetter, NZA 2008, 609, 612, vgl. ferner Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 875 m.w.N.) gehen sogar von eine generellen Unzulässigkeit der Authentifizierung mittels sensibler Daten i.S.d. § 3 Abs. 9 BDSG bzw. Merkmale i.S.d. § 1 AGG aus.
[631] Raif, ArbRAktuell 2010, 359.
[632] Vgl. auch Schmitz/Eckhardt, CR 2007, 171, 172 zu verschiedenen Anwendungsmöglichkeiten und diesbezüglicher Bedenken.
[633] Meyer, K&R 2009, 14, 18.
[634] Meyer, K&R 2009, 14, 18.

werden.[635] Zumindest bzgl. aktiver RFID-Tags[636] greift § 6c BDSG,[637] der den Umgang mit mobilen personenbezogenen Speicher- und Verarbeitungsmedien[638] (§ 3 Abs. 10 BDSG) regelt. Darunter fallen grundsätzlich alle Medien, die über einen eigenen Prozessorchip verfügen.[639] Etwas anderes gilt, wenn wie bei üblichen Zugangskontrollsystemen lediglich unveränderbare Informationen wie eine ID-Nummer gespeichert sind.[640] Für den Verwender konstituiert § 6c BDSG diverse Aufklärungspflichten wie etwa die Pflicht, dem Betroffenen seine Identität zu offenbaren oder diesen über die Funktionsweise der Technik sowie die Ausübung seiner Rechte zu unterrichten, soweit dieser nicht bereits Kenntnis erlangt hat. Daneben besteht, abhängig vom Einzelfall, bei jeder konkreten Verwendung der RFID-Technik eine zusätzliche Informationspflicht nach § 6c Abs. 3 BDSG, die allerdings nicht näher ausgestaltet ist.[641] Vorgeschlagen wird, hieraus eine Hinweispflicht bezüglich der Datenerfassung (etwa mittels akustischem Hinweiston) abzuleiten.[642] Der Einsatz von RFID-Techniken ist an die Information der Mitarbeiter gekoppelt, wobei diese u.U. auch darüber in Kenntnis gesetzt werden müssen, inwieweit durch systematische Auswertung der einzelnen Lesevorgänge ein Bewegungsprofil erstellt wird.[643] Im Übrigen gelten die gleichen allgemeinen Denkansätze wie für die bereits genannten Zugangskontrollsysteme.[644] Was die Überwachung des Aufenthaltsortes eines Mitarbeiters unter Zuhilfenahme technischer Mittel (wie eben etwa RFID) zum Zweck der Leistungskontrolle angeht, wird dies regelmäßig unzulässig sein.[645] Etwas anderes kann sich in speziellen Fällen wie beispielsweise der Erfassung bereits passierter Kontrollpunkte bei Rundgängen von Wachpersonal ergeben.[646]

2.6. Mitarbeiterüberwachung außerhalb des Betriebsgeländes

Eine Mitarbeiterüberwachung ist auch außerhalb des Betriebsgeländes denkbar.[647] Um den Kontrollbereich derart auszuweiten, bedarf es dem Einsatz diverser technischer Hilfsmittel wie GPS oder GSM. Stellt der Arbeitgeber dem Arbeitnehmer Betriebsmittel zur Verfügung,

---

[635] Meyer, K&R 2009, 14, 18.

[636] Aktive RFID-Tags sind solche, die aufgrund einer eigenen Energiequelle (Batterie oder Solarzelle) in der Lage sind, Informationen auszusenden, sobald sie von einem Lesegerät einen Aktivierungsimpuls erhalten, John, in: Kilian/Heussen, Computerrechts-Handbuch, 3. Abschnitt, Teil 300 Rn. 3.

[637] Gräfin von Westerholt/Döring, CR 2004, 710, 714; differenzierter Schmitz/Eckhardt, CR 2007, 171, 173.

[638] Wie sich aus § 3 Abs. 10 BDSG ergibt, handelt es sich bei mobilen personenbezogenen Speicherungs- und Verarbeitungsmedien um Datenträger, die an den Betroffenen ausgegeben werden, auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebenden oder eine andere Stelle automatisiert verarbeitet werden können und bei denen die Betroffenen diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

[639] Gola/Schomerus, BDSG, § 3 Rn. 58; Gola, in: Hümmerich/Boecken/Düwell, Anwalt-Kommentar Arbeitsrecht, § 6b BDSG Rn. 2, § 3 BDSG Rn. 20.

[640] Zscherpe, in: Taeger/Gabel, BDSG, § 6c Rn. 52; Meyer, K&R 2009, 14, 18.

[641] Gola, in: Hümmerich/Boecken/Düwell, Anwalt-Kommentar Arbeitsrecht, § 6c BDSG Rn. 3.

[642] Meyer, K&R 2009, 14, 18.

[643] Meyer, K&R 2009, 14, 18, der heraushebt, dass durchaus ein Bedürfnis für die Erstellung von Bewegungsprofilen bestehen kann, beispielsweise bei Wachpersonal.

[644] Schmitz/Eckhardt, CR 2007, 171, 175.

[645] Wank, in: ErfK zum Arbeitsrecht, § 6c BDSG Rn 19.

[646] Wank, in: ErfK zum Arbeitsrecht, § 6c BDSG Rn 19; Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 885.

[647] So etwa bei Außendienstmitarbeitern oder Kurierfahrern, vgl. Däubler, CR 2005, 767, 770.

kann er regelmäßig den Standort der Arbeitnehmer ermitteln sowie deren Aktivität kontrollieren.[648]

2.6.1. Fälle aus der Rechtsprechung

Da Ortungssysteme bislang noch nicht Gegenstand von Entscheidungen im Zusammenhang mit dem Beschäftigtendatenschutz waren, wird wiederum ein Rückgriff auf die Ausführungen der Judikative zur Videoüberwachung vorgeschlagen.[649]

2.6.2. Wissenschaftliche Auseinandersetzung

Häufig werden mittels GPS-Ortung von Dienstwagen und Dienstmobiltelefonen Bewegungsprofile von Mitarbeitern erstellt.[650]

2.6.2.1. GPS-Ortung von Dienstwagen[651]

Ist der Arbeitgeber lediglich an einer Überwachung der Arbeitszeiten seiner Arbeitnehmer interessiert, kann dies mitunter schon durch die Auswertung der Daten des digitalen Tachografen des Dienstwagens erreicht werden.[652] Soll hingegen zusätzlich eine Standortbestimmung durchgeführt werden, um die Nutzung des Dienstwagens zu kontrollieren, wird regelmäßig ein GPS-Sender im oder am Fahrzeug installiert.[653] Technisch gesehen ermöglichen die GPS-Sender dabei grundsätzlich eine Positionsbestimmung sämtlicher Gegenstände oder Personen, wobei der Einsatz hauptsächlich im Bereich der Fahrzeugortung stattfindet.[654] Von der Funktionsweise her findet dabei zuerst eine Bestimmung der eigenen Position des Senders durch Datenabgleich mit den GPS-Satelliten statt.[655] Im Anschluss werden die Standortdaten für eine bestimmte Zeit gespeichert und komprimiert übertragen.[656] Dies geschieht durch den Aufbau einer Mobilfunkverbindung zu einem zuvor festgelegten Empfänger.[657] Zur Auswertung und Aufbereitung der Daten wird spezielle Software eingesetzt, die etwa die Visualisierung der gefahrenen Route auf einer Landkarte ermöglicht.[658] Ermöglichen die Systeme die Zuordnung von Positionsdaten zu einer bestimmten natürlichen Person, ist deren Einsatz wiederum an § 6c BDSG zu messen.[659] Ein solcher direkter Personenbezug liegt immer dann vor, wenn es nicht mehr allgemein um die Ermittlung der Fahrzeugposition geht, sondern einem Mitarbeiter ein bestimmter

---

[648] Meyer, K&R 2009, 14, 18.
[649] Raif, ArbRAktuell 2010, 359; Meyer, K&R 2009, 14, 19; Gola/Schomerus, BDSG, § 32 Rn. 19.
[650] Vogt, NJOZ 2009, 4206, 4212; Meyer, K&R 2009, 14, 18; Raif, ArbRAktuell 2010, 359.
[651] Da GPS-Sender hauptsächlich zur Ortung von Fahrzeugen eingesetzt werden (Meyer, K&R 2009, 14, 18), beschränken sich die folgenden Ausführungen auf diesen Bereich.
[652] Gola, NZA 2007, 1140, 1142.
[653] Meyer, K&R 2009, 14, 18.
[654] Meyer, K&R 2009, 14, 18. Zu den verschiedenen, aufgrund der geringen Größe vielseitigen Einsatzmöglichkeiten der GPS-Sender vgl. weiterführend Gola, NZA 2007, 1140, 1143.
[655] Roloff, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 5 Rn. 72. Hierin besteht der Unterschied zu Navigationssystemen, bei denen die Positionsdaten weder aufgezeichnet noch weitergegeben werden, Meyer, K&R 2009, 14, 18.
[656] BVerfGE 112, 304, 308; Roloff, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 5 Rn. 72. Bei entsprechender technischer Ausgestaltung kann die Datenübertragung sogar in Echtzeit stattfinden, Meyer, K&R 2009, 14, 18 f.
[657] Meyer, K&R 2009, 14, 19.
[658] Meyer, K&R 2009, 14, 19.
[659] Meyer, K&R 2009, 14, 19.

Dienstwagen zugeordnet wird, der nur von ihm gefahren werden darf.[660] Ähnlich wie bei RFID-Systemen werden auch hier Daten von einem Medium selbstständig verarbeitet und übermittelt, wobei der Mitarbeiter nicht nachvollziehen kann, wann und in welchem Umfang mit seinen personenbezogenen Daten umgegangen wird.[661] Dementsprechend muss der Arbeitgeber wiederum den Informationspflichten des § 6c BDSG nachkommen.[662] Ferner ist die Erhebung und Speicherung der Daten abhängig von der Einwilligung des Arbeitnehmers oder einem Erlaubnistatbestand. In Ermangelung besonderer gesetzlicher Vorschriften für Ortungssysteme hat hierbei ein Rückgriff auf die allgemeinen datenschutzrechtlichen Regelungen zu erfolgen.[663] Damit stehen wiederum §§ 28, 32 BDSG im Zentrum der datenschutzrechtlichen Zulässigkeitsprüfung. Insofern kommt es maßgeblich auf die zuvor erwähnten Prüfungskriterien an. In der Literatur wird dabei eine Parallele zur Videoüberwachung entwickelten Rechtsprechung[664] gezogen und bei Kenntnis des Arbeitnehmers von der Überwachung gefordert, dass der Einsatz einen legitimen Zweck verfolgt und eine hinreichende Abwägung von Arbeitgeber- und -nehmerinteressen stattgefunden hat.[665] Vorgeschlagen wird hierbei, dem Umstand, dass die Ortung via GPS bislang seitens der Gerichte als nicht besonders intensiven Eingriff in das allgemeine Persönlichkeitsrecht eingestuft wurde, Rechnung zu tragen.[666] Zumindest in Relation zu Videoüberwachungen oder Aufzeichnung von Telefongesprächen, die weitreichende Kontrollmöglichkeiten eröffnen, liegt bei der GPS-Ortung eine geringere Eingriffsintensität vor, da hier lediglich eine ungefähre Positionsbestimmung stattfindet und von daher höchstens indirekt Rückschlüsse auf das Verhalten eines Arbeitnehmers ermöglicht werden.[667] Aber auch hier verbieten sich pauschale Aussagen. Vielmehr muss die Bewertung der Rechtslage einzelfallabhängig erfolgen. Dabei kann im Hinblick auf den Zeitpunkt der Kontrolle und deren Ausgestaltung unterschieden werden. Als grundsätzlich zulässige Interessen des Arbeitgebers werden neben stichprobenartigen Kontrollen des Mitarbeiterverhaltens auch die Effizienzsteigerung des Außendienstes[668] sowie der Verlust des Dienstwagens in Erwägung gezogen.[669]

2.6.2.1.1. GPS-Ortung während der Dienstzeit

Erfolgt die Ortung lediglich während der Arbeitszeit, so soll bei dem Vorliegen eines berechtigten Interesses des Arbeitgebers sogar eine ständige und verdachtsunabhängige Mitarbeiterkontrolle anzuerkennen sein.[670] Begründet wird dies damit, dass privaten

[660] Meyer, K&R 2009, 14, 19.
[661] Meyer, K&R 2009, 14, 19.
[662] Meyer, K&R 2009, 14, 19. Ebenso Schmitz/Eckhardt, CR 2007, 171, 173 Fn. 22.
[663] Raif, ArbRAktuell 2010, 359; Gola/Schomerus, BDSG, § 6c Rn. 5.
[664] Vgl. zu der Zulässigkeit von Videoüberwachungsmaßnahmen ausführlich Gliederungspunkt 2.4.
[665] Raif, ArbRAktuell 2010, 359.
[666] Roloff, in: Besgen/Prinz, Multimedia und Arbeitsrecht, § 5 Rn. 81 (m.w.N.).
[667] Vgl. hierzu die Ausführungen in BVerfGE 112, 304, 308, 317.
[668] Vgl. nur Raif, ArbRAktuell 2010, 359, der ein Verhalten von Außendienstmitarbeitern, die entgegen der vertraglichen Vereinbarung, nicht auf dem Weg zum Kunden sind, als schwerwiegende Vertragsverletzung des qualifiziert.
[669] Vogt, NJOZ 2009, 4206, 4212 mit dem Hinweis, dass im Gegensatz dazu eine lückenlose Überwachung des Mitarbeiters als unzulässig erachtet wird (so auch Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 908, die sich explizit gegen eine Rundumkontrolle aussprechen).
[670] Roloff, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 5 Rn. 83, zustimmend Meyer, K&R 2009, 14, 19.

Erledigungen mit dem Dienstwagen grundsätzlich nicht nachgekommen werden darf.[671] Ist hingegen die Privatnutzung des Fahrzeugs erlaubt, müsse die Lokalisierung in dieser Zeit deaktiviert werden können, um dem Vorrang des Interesses des Arbeitnehmers, nicht in seinem privaten Bereich überwacht zu werden, gegenüber dem arbeitgeberseitigen Interesse an der Kontrolle seines Eigentums an dem Fahrzeug Rechnung zu tragen.[672] In den Freizeitbereich der Arbeitnehmer darf die Ortung jedoch nicht ausstrahlen.[673]

2.6.2.1.2. Verdeckter Einsatz der GPS-Ortung

§ 6c BDSG sieht den Einsatz einer heimlichen GPS-Ortung nicht vor.[674] Aufgrund der vorzunehmenden Unterrichtung des Arbeitnehmers durch den Arbeitgeber nach § 4 Abs. 3 BDSG und § 98 Abs. 1 TKG[675] vertritt eine strenge Ansicht, den heimlichen Einsatz der GPS-Ortung zur Gewinnung von Aufenthaltsdaten nicht zu ermöglichen.[676] Andere wiederum erwägen, insofern liberaler, eine verdeckte Ortung zumindest für den Fall zu legitimieren, dass ein bestimmter Arbeitnehmer der Begehung einer Straftat oder schwerwiegenden Verfehlung verdächtig ist und keine anderweitigen Möglichkeiten zur Aufdeckung des Verdachts bestehen.[677] Folglich könnte an dieser Stelle eine Parallele zu heimlicher Videoüberwachung gezogen werden. Sollte man diese zulassen, so müsse a maiore ad minus die GPS-Überwachung aufgrund der vergleichsweise geringen Eingriffsintensität als zulässig erachtet werden.[678]

2.6.2.2. Ortung von Mobiltelefonen

Eine weitere Maßnahme der Mitarbeiterkontrolle ist die Ortung von Mobiltelefonen.

2.6.2.2.1. GPS-Ortung

Auch per Mobilfunkgerät ist eine GPS-Ortung möglich.[679] Dafür muss entweder in dem Endgerät selbst ein GPS-Empfänger eingebaut sein oder das Gerät eine Verbindung zu einem externen GPS-Empfänger herstellen können.[680] Mittels auf dem Telefon installierter Software kann dann in bestimmten Intervallen die GPS-Position abgefragt und über das Mobilfunknetz übertragen werden, wobei das Mobiltelefon als GPS-Sender fungiert.[681] Hinsichtlich der Zulässigkeit einer solchen Ortung gelten die oben stehenden Ausführungen.

2.6.2.2.2. GSM-Ortung

---

[671] Meyer, K&R 2009, 14, 19.
[672] Meyer, K&R 2009, 14, 19; Vogt, NJOZ 2009, 4206, 4212.
[673] Vogt, NJOZ 2009, 4206, 4212.
[674] Meyer, K&R 2009, 14, 19.
[675] § 98 TKG behandelt den Umgang (siehe zu der erweiterten Auslegung des Begriffs der Verarbeitung Munz, in: Taeger/Gabel, BDSG, § 98 TKG Rn. 4) mit Standortdaten. Nach § 3 Nr. 19 TKG sind hierunter Daten zu verstehen, die in einem Telekommunikationsnetz erhoben oder verwendet werden und die den Standort des Endgeräts eines Endnutzers eines Telekommunikationsdienstes für die Öffentlichkeit angeben.
[676] Vogt, NJOZ, 4206, 4212.
[677] Steinkühler/Raif, AuA 2009, 213, 216.
[678] Meyer, K&R 2009, 14, 19 mit Verweis auf Roloff, in: Besgen/Prinz, Multimedia und Arbeitsrecht, § 5 Rn. 87.
[679] Gola, NZA 2007, 1141, 1143.
[680] Meyer, K&R 2009, 14, 19.
[681] Meyer, K&R 2009, 14, 19.

Neben GPS ist im Zusammenhang mit Mobilfunkgeräten auch die GSM-Ortung eine mögliche Maßnahme der Mitarbeiterkontrolle. Bei Verwendung dieser Technik wird die Position des Mobilfunkgerätes dadurch bestimmt, dass der zelluläre Aufbau des Mobilfunknetzes zur Ermittlung des Standortes genutzt wird.[682] Im Einzelnen wird zunächst die jeweilige Funkzelle, in der sich das Gerät befindet, ermittelt, wobei jeder Zelle eine spezifische Cell-ID zugeordnet ist.[683] In Abhängigkeit von der Dichte der Funkzellen kann eine Lokalisierung mit einer Genauigkeit von bis zu ca. 100 m erreicht werden.[684] Exaktere Positionsbestimmungen können zwar unter Zuhilfenahme ergänzender Maßnahmen wie Laufzeitberechungen erfolgen,[685] jedoch bleibt die GSM-Ortung letztlich in puncto Genauigkeit deutlich hinter der GPS-Ortung zurück.[686] Der Einsatz der Technik gestaltet sich hingegen durchaus einfach. So ist für die Durchführung der Maßnahme lediglich ein für die Positionsbestimmung freigeschaltetes und innerhalb des GSM-Mobilfunknetzes betriebenes Mobiltelefon notwendig.[687] Die Freischaltung selbst erfolgt dabei meist nicht über die Mobilfunkanbieter, sondern über externe Dritte.[688] Je nach Vorgehensweise der Dienstleister reicht dabei entweder pauschal die Übersendung einer einmaligen SMS oder der Betroffene wird vor jeder Standortbestimmung per SMS informiert beziehungsweise um seine Einwilligung gebeten.[689]

2.6.2.2.3. Telekommunikationsdatenschutz

Die Bestimmungen zum Telekommunikationsdatenschutz verlangen von Dienstleistern, bereits im Vorfeld eine Freigabe für die zu erfolgende Positionsbestimmung einzuholen.[690] Der Umgang mit Standortdaten wird in § 98 TKG geregelt.[691] Nach der Begründung zum Regierungsentwurf soll der voranschreitenden Entwicklung der Telekommunikation Rechnung getragen werden, die die Nutzung von Telekommunikationsdiensten standortbezogen möglich macht (Location Based Services, LBS).[692] Diesbezüglich ist ein Umgang mit Standortdaten von der Einwilligung des Teilnehmers[693] als Vertragspartner des Dienstleisters abhängig.[694] Sofern zwischen Teilnehmer und Nutzer des Mobilfunkgerätes keine Personenidentität vorliegt, sieht § 98 Abs. 1 S. 2 TKG eine Unterrichtung des Nutzers über die erteilte Einwilligung vor.[695] Hieraus folgt, dass es rechtlich unzulässig ist, wenn der Arbeitgeber ein dienstliches Mobilfunkgerät zunächst für die Standortbestimmung freischalten lässt und dieses dem Arbeitnehmer überlässt, ohne ihn auf die Möglichkeit der

[682] Meyer, K&R 2009, 14, 19.
[683] Meyer, K&R 2009, 14, 19.
[684] Meyer, K&R 2009, 14, 19.
[685] Meyer, K&R 2009, 14, 19.
[686] Wittern, in: Beck'scher TKG-Kommentar, § 98 TKG Rn. 4.
[687] Meyer, K&R 2009, 14, 19.
[688] Meyer, K&R 2009, 14, 19.
[689] Meyer, K&R 2009, 14, 19.
[690] Gola, NZA 2007, 1141, 1143.
[691] Siehe bereits oben, Fn. 678. Vgl. zum Einwilligungserfordernis nach § 98 TKG Jandt, MMR 2007, 74.
[692] Munz, in: Taeger/Gabel, BDSG, § 98 TKG Rn. 1 unter Rückgriff auf BT-Drs. 15/2316, S. 89.
[693] Teilnehmer ist nach § 3 Nr. 20 TKG jede natürliche oder juristische Person, die mit einem Anbieter von Telekommunikationsdiensten einen Vertrag über die Erbringung derartiger Dienste geschlossen hat.
[694] Meyer, K&R 2009, 14, 20.
[695] Wittern, in: Beck'scher TKG-Kommentar, § 98 TKG Rn. 7.

ständigen Lokalisierung zu informieren.[696] Sofern die Voraussetzungen des § 98 TKG vorliegen, indiziert dies keine Erlaubnis des Arbeitgebers, jederzeit eine Standortbestimmung vornehmen zu können.[697] Vielmehr ist weitergehend – und insofern über den Bereich des Telekommunikationsdatenschutzes hinaus – fraglich, ob nicht ein unzulässiger Eingriff in das allgemeine Persönlichkeitsrecht des Mitarbeiters stattfindet, wenn diesem ein freigeschaltetes Mobilfunkgerät überlassen wird.[698] In der vorzunehmenden Interessenabwägung spielen mehrere Aspekte eine Rolle. Vergleicht man die Ortung des Mobiltelefons mit der oben erwähnten Lokalisierung eines Dienstwagens mit erlaubter Privatnutzung, so hat der Arbeitnehmer bei erstgenannter Maßnahme zumindest grundsätzlich die Möglichkeit, der Positionsbestimmung zu entgehen, indem er das Gerät ausschaltet.[699] Dem gegenüber dürfte ein unzulässiger Eingriff in das Persönlichkeitsrecht des Mitarbeiters vorliegen, wenn für diesen die Verpflichtung besteht, das Gerät auch außerhalb der regulären Arbeitszeit bei sich zu führen und hierüber erreichbar zu sein.[700] Sofern ein berechtigtes arbeitgeberseitiges Interesse vorliegt, wird der Beschäftigte aber zumindest – insofern parallel zu der GPS-Ortung von Dienstwagen – die Standortbestimmung während der Dienstzeit zu dulden haben.[701] Als Mindestvoraussetzung wird man dann aber vom Arbeitgeber fordern dürfen, Kriterien für die Durchführung von Standortbestimmungen aufzustellen und den Mitarbeiter hierüber zu informieren.[702] Unabhängig von der Reichweite des § 98 TKG folgt dies aus § 6c BDSG, der ebenfalls auch für die SIM-Karte eines Mobilfunkgerätes anwendbar ist.[703]

2.7. Besonderheiten bei Mitarbeiterscreenings

Bei einem sog. Mitarbeiterscreening werden bereits beim Arbeitgeber vorhandene oder zu diesem Zweck erhobene Arbeitnehmerdaten Prüfrastern unterworfen, um anhand erzielter Treffer gewisse Schlüsse ziehen zu können.[704] In Deutschland findet das Screening inzwischen weitreichend Anwendung, wobei in Hinblick auf den Persönlichkeitsrechtsschutz am Arbeitsplatz dem Bereich der Korruptionsbekämpfung besonderes Augenmerk geschenkt werden soll.[705]

2.7.1. Erscheinungsformen des Mitarbeiterscreenings

Das Mitarbeiterscreening tritt, sofern eine Anordnung durch Rechtsvorschrift nach § 4 Abs. 2 BDSG nicht vorliegt, insbesondere in zwei Formen in Erscheinung: einerseits, wenn die Prävention von Korruption und anderen Compliance-Verletzungen im Mittelpunkt steht und andererseits, wenn es repressiv um die Verfolgung von Straftaten und anderen Compliance-

[696] Meyer, K&R 2009, 14, 20; Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 897.
[697] Gola, NZA 2007, 1141, 1143.
[698] Meyer, K&R 2009, 14, 20.
[699] Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 905; Meyer, K&R 2009, 14, 20.
[700] Meyer, K&R 2009, 14, 20.
[701] Meyer, K&R 2009, 14, 20.
[702] Meyer, K&R 2009, 14, 20.
[703] Gräfin von Westerholt/Döring, CR 2004, 710, 714; Gola/Schomerus, in Gola/Schomerus, BDSG, § 6c Rn. 2a.
[704] Brink/Schmidt, MMR 2010, 592, 592.
[705] Zu weiteren Screeningmaßnahmen wie etwa dem Abgleich von Terrorlisten oder der Zugangskontrolle bei staatlichen Zulassungs- bzw. Vergünstigungsverfahren vgl. exemplarisch Brink/Schmidt, MMR 2010, 592, 595 f.

Verstößen geht.[706] Präventivscreenings kennzeichnen sich vor allem dadurch, dass auf Seiten des Arbeitgebers zwar noch keine Anhaltspunkte für das Vorliegen konkreter Rechtsverstöße bestehen, die Rechtskonformität aber dennoch vorbeugend überprüft und umgesetzt werden soll.[707] Im Gegensatz dazu weiß der Arbeitgeber bei repressivem Screening von Compliance-Verletzungen und versucht, durch die Maßnahmen Rückschlüsse auf den Ursprung des Verstoßes ziehen zu können.[708]

2.7.2. Fälle aus der Rechtsprechung

Noch liegt wenig Judikatur im Bereich des Mitarbeiterscreenings vor, auf die zurückgegriffen werden könnte.[709] Daher sollen wiederum die Kriterien der Rechtsprechung im Zusammenhang mit der Videoüberwachung Anwendung finden.[710]

2.7.3. Wissenschaftliche Auseinandersetzung

Für die Beurteilung der Zulässigkeit von Mitarbeiterscreenings nach der aktuellen Rechtslage kommen wiederum die §§ 28, 32 BDSG als Erlaubnistatbestände in Betracht.[711] Hinsichtlich der Möglichkeit der Einwilligung steht bei Mitarbeiterscreenings die Freiwilligkeit aus zweierlei Gesichtspunkten besonders in Frage: Es ist einerseits nicht nur sehr zweifelhaft, ob ein Mitarbeiter bei Massenscreenings wirklich keinen Zwang zur Teilnahme verspürt.[712] Vielmehr müssen andererseits auch die eventuell auftretenden Konsequenzen bedacht werden, wenn man nicht an einem Verfahren partizipiert, das auf sämtliche Betroffene einheitlich angewandt werden soll.[713] In Bezug auf die Prüfung der Zulässigkeit von Maßnahmen i.R.d. Mitarbeiterscreening ist die bereits oben vorgenommene Differenzierung zwischen präventiven und repressiven Screeningmaßnahmen beizubehalten.

2.7.3.1. Präventive Screeningmaßnahmen, § 32 Abs. 1 S. 1 BDSG

Zunächst könnte § 32 Abs. 1 S. 1 BDSG Legitimationswirkung entfalten. Dies scheitert jedoch in der Regel am Erforderlichkeitskriterium. Das Beschäftigungsverhältnis ist auch ohne ein Screening durchführbar, so dass die Maßnahme nicht notwendig ist.[714] Das bloße, wenn auch nachvollziehbare, arbeitgeberseitige Interesse an präventiver Korruptionsbekämpfung rechtfertigt im Fall des § 32 Abs. 1 S. 1 BDSG noch keinen Zugriff auf personenbezogene Daten von Arbeitnehmern.[715] Selbst wenn es darum ginge, die Beschäftigten über potentielle Compliance-Verstöße innerhalb des Unternehmens aufzuklären, bedarf es hierfür keiner Bezugnahme auf früheres Fehlverhalten, ggf. sogar unter

---

[706] Brink/Schmidt, MMR 2010, 592, 592; Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 857.
[707] Brink/Schmidt, MMR 2010, 592, 592.
[708] Brink/Schmidt, MMR 2010, 592, 592.
[709] Vgl. z.B. die Ausführungen des BVerfG zu einer staatsanwaltschaftlichen Datenerhebung bei einem Kreditkarteninstitut, RDV 2009, 113.
[710] Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 856; Mähner, MMR 2010, 379, 381.
[711] Eine Rechtfertigung über Konsensualvereinbarungen scheidet nach Brink/Schmidt, MMR 2010, 592, 593 hingegen regelmäßig aus. A.A. Vogt, NJOZ 2009, 4206, 4214, der eine Betriebsvereinbarung als gesetzliche Befugnisnorm anerkennt.
[712] Brink/Schmidt, MMR 2010, 592, 593.
[713] Brink/Schmidt, MMR 2010, 592, 593.
[714] Brink/Schmidt, MMR 2010, 592, 593; Thüsing, NZA 2009, 865, 867.
[715] Brink/Schmidt, MMR 2010, 592, 593 f.

Namensnennung der Verantwortlichen.[716] Gleiches gilt im Übrigen bei der Behandlung von Vertragsbrüchen seitens der Arbeitnehmer, wobei die Tatsache, dass es lediglich allein der Arbeitgeber sein wird, der eine derartige Aufklärung initiiert, keine andere rechtliche Bewertung nach sich zieht.[717] Letztlich scheidet § 32 Abs. 1 S. 1 BDSG damit grundsätzlich als Legitimationsgrundlage für ein präventives Mitarbeiterscreening aus.[718]

2.7.3.2. Repressive Screeningmaßnahmen (Aufklärungsmaßnahmen), § 32 Abs. 1 S. 2 BDSG

Wie sich aus der Gesetzeslektüre ergibt, muss der Umgang mit Arbeitnehmerdaten zur Aufdeckung von Straftaten hohen Anforderungen genügen. Eine Rechtfertigung von Aufklärungsmaßnahmen über § 32 Abs. 1 S. 2 BDSG käme höchstens bei Vorliegen eines konkreten Straftatverdachts in Betracht.[719] Bloße Anhaltspunkte, dass eine beliebige Person aus dem Kreis der Beschäftigten eine Straftat begangen hat, reichen noch nicht für die Rechtfertigung repressiver Screeningmaßnahmen aus.[720] Letztlich ist der Geltungsbereich des § 32 Abs. 1 S. 2 BDSG daher sehr eng umgrenzt.

2.7.3.3. § 28 Abs. 1 S. 1 Nr. 2 BDSG

Sofern man neben der Anwendung des § 32 BDSG einen Rückgriff auf § 28 Abs. 1 Nr. 2 BDSG zulässt, kommt eine Rechtfertigung über diesen Erlaubnistatbestand nur ausnahmsweise in Betracht. [721] Denkbar ist dies beispielsweise, wenn sich die Zulässigkeit des Screenings nicht nach § 32 BDSG richtet, etwa wenn Beschäftigte im Verhältnis zum Arbeitgeber nur als beliebige Dritte zu qualifizieren sind.[722]

2.8. Beteiligungsrechte der Interessenvertretungen

Möchte ein Arbeitgeber Mitarbeiterüberwachungsmaßnahmen durchführen, bedarf es hierzu regelmäßig der Beteiligung der Interessenvertretungen der Beschäftigten (Betriebs- beziehungsweise Personalrat).[723] § 32 Abs. 3 BDSG schreibt insofern vor, dass die Beteiligungsrechte der Interessenvertretungen unberührt bleiben.[724] Dies führt dazu, dass bei kollektiven Maßnahmen und damit auch etwa bei einheitlich durchgeführten Überwachungsmaßnahmen, dem Gestaltungsspielraum des Arbeitgebers Grenzen gesetzt sind.[725] Mitbestimmungserfordernisse sind nicht nur bei der formalisierten Erhebung von Personaldaten (§ 94 BetrVG, §§ 75 Abs. 3 Nr. 8, 76 Abs. 2 Nr. 1 BPersVG) sowie datenschutzrelevanten Fragen der betrieblichen Ordnung und des Verhaltens (§ 81 Abs. 1 Nr.

---

[716] Brink/Schmidt, MMR 2010, 592, 594.
[717] Brink/Schmidt, MMR 2010, 592, 594. A.A. Thüsing, NZA 2009, 865, 868 f.
[718] I.E. ebenso Mähner, MMR 2010, 379, 381.
[719] Brink/Schmidt, MMR 2010, 592, 594; ebenso Rasmussen-Bonne/Raif, GWR 2011, 80.
[720] Brink/Schmidt, MMR 2010, 592, 594; Mähner, MMR 2010, 379, 381.
[721] Brink/Schmidt, MMR 2010, 592, 594; Bierekoven, CR 2010, 205 unter Hinweis auf BT-Drs. 16/13657, S. 35.
[722] Schmidt, DuD 2010, 207, 209; Brink/Schmidt, MMR 2010, 592, 594, wobei beispielsweise durch die Übermittlung von Daten i.R.e. Unternehmenstransaktion der Beschäftigte dem Arbeitgeber als beliebiger Dritter gegenüber tritt.
[723] Zöll, in: Taeger/Gabel, BDSG, § 32 Rn. 48.
[724] Die Regierungsbegründung nennt beispielsweise § 87 Abs. 1 Nr. 6 BetrVG und § 75 Abs. 3 Nr. 17 BPersVG, BT-Drs. 16/13657, S. 37.
[725] Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 531 ff.

1 BetrVG, § 75 Abs. 3 Nr. 15 BPersVG) zu beachten, sondern insbesondere auch bei dem durch automatisierte Personaldatenverarbeitung verwirklichten Einsatz technischer Überwachungseinrichtungen (§ 87 Abs. 1 Nr. 6 BetrVG, § 75 Abs. 3 Nr. 17 BPersVG).[726] Nach der von dem BAG[727] entwickelten und insoweit herrschenden[728] Theorie der Wirksamkeitsvoraussetzung ist die Mitbestimmung der Interessenvertretungen notwendig für die Wirksamkeit einer Maßnahme. Individualvertraglich folgt hieraus, dass bei einem Verstoß gegen Mitbestimmungsrechte Weisungen, für Beschäftigte nachteilige Vertragsänderungen oder die Ausübung von Gestaltungsrechten unwirksam sind und demzufolge nicht beachtet werden müssen.[729] Zu beachten ist in diesem Kontext, dass sich das Mitbestimmungsrecht nicht auf die Frage der Erlaubnis der Privatnutzung an sich erstreckt.[730]

[726] Gola/Schomerus, in: Gola/Schomerus, BDSG, § 32 Rn. 43.
[727] BAG, NZA 1992, 749, 759; NZA 2004, 331, 333.
[728] Vgl. zu der Gegenansicht Richardi, in: Richardi: BetrVG, § 87 Rn. 104 ff.; Worzalla, in: Hess/Schlochauer/ Worzalla/Glock/Nicolai, BetrVG, § 87 Rn. 83 ff.
[729] BAG, NZA-RR, 469, 471; Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 564.
[730] LAG Hamm, NZA-RR 2007, 20, 21 f.; Ernst, NZA 2002, 585, 586; Lindemann/Simon, BB 2001, 1950, 1954.

3. ARBEITNEHMERDATENSCHUTZ AUS SICHT DER DATENSCHUTZBEHÖRDEN UND WEITERGEHENDES INFORMATIONSMATERIAL

3.1. Stellungnahme des HmbBfDI zum Thema Persönlichkeitssrechtsschutz im Berufsleben[731]

Hinsichtlich der Frage des Persönlichkeitsrechtsschutzes von Arbeitnehmern begrüßt man von Seiten der Aufsichtsbehörden zwar grundsätzlich das Tätigwerden des Gesetzgebers, jedoch wird dem geplanten Gesetzesvorhaben auch Kritik entgegengeworfen sowie Regelungs- und Nachbesserungsbedarf im Bereich des Arbeitnehmerdatenschutzes angemeldet. Die Schaffung des § 32 BDSG als Generalklausel für den Umgang mit Arbeitnehmerdaten sei hierbei nicht nur eine unzureichende, politisch motivierte und symbolische Gesetzgebung, um den Druck aus der aktuellen Diskussion zu nehmen. Vielmehr bringe sie auch in der Praxis erhebliche Probleme mit sich, gerade mit Blick auf das unzureichend geklärte Konkurrenzverhältnis zu § 28 BDSG. Dem hieraus resultierenden großen Maß an Rechtsunsicherheit müsse dadurch entgegen getreten werden, dass ein klarer gesetzlicher Rahmen geschaffen werde, der den nötigen Praxisbezug nicht außer Betracht lässt. Hierbei müsse nicht nur der Abwägung von Kapital und lohnabhängiger Arbeit Rechnung getragen werden, sondern sei weitergehend zu berücksichtigen, dass die Gesellschaft immensen Innovationszyklen unterliege und tendenziell zu einer Ökonomisierung von Daten übergegangen werde. Damit werde zusätzlich das Problem des Verhältnisses von Recht und Technik auf den Plan gerufen. Geht es etwa um die Frage, wo der Einsatz von Technik mit Blick auf das informationelle Selbstbestimmungsrecht der Beschäftigten aus rechtsethischen Gründen an seine Grenzen stößt, befindet man sich auf politischer Ebene in einem sehr schwierigen Abwägungsprozess. Eine Auflösung der Kollisionslage lasse sich dabei gerade nicht über regulierte Selbstregulierung erreichen. Ein solches Modell sei in Bereichen interessant, in denen Datenschutz als Maßnahme zur Wettbewerbsverbesserung eingesetzt werden kann, um ein Eigeninteresse der Betriebsleitung an der Optimierung bestimmter Prozesse zu verfolgen. Wenig Sinn mache es dort, wo unterschiedliche Interessen entschieden oder Rechtseingriffe festgelegt werden sollen. Von gesetzgeberischer Seite sei man dem Bedürfnis nach einer interessengerechten Abwägung der kollidierenden Positionen nur bedingt nachgekommen, so etwa mit der Entscheidung, sich konsequent gegen heimliche Videoüberwachungen auszusprechen. Kritikfähig sei hingegen, im Gegenzug dafür offene Videoüberwachungsmaßnahmen weitgehend zuzulassen. Derartige Maßnahmen dürften nicht dazu führen, dass letztlich jeder Handschlag eines Arbeitnehmers digitalisiert und rekonstruierbar wird. Gerade mit Blick auf die Möglichkeit, neue Technologien einzusetzen und technische Maßnahmen miteinander zu kombinieren sowie Abläufe innerhalb betrieblicher Sphären jederzeit zu rekonstruieren, sei das informationelle

[731] Die Ausführungen basieren auf einem Interview mit dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, Herrn Prof. Dr. Johannes Caspar. Der Volltext ist in einem separaten Dokument verfügbar, s. Fn. 205.

Selbstbestimmungsrecht großen Gefahren ausgesetzt. Natürlich werde es auch weiterhin Fälle geben, in denen der Arbeitgeber ein legitimes Interesse an dem Einsatz moderner Technologien habe, etwa zur Sicherung seines Eigentums. Dies müsse aber in einer menschengerechten Weise erfolgen und dürfe gerade nicht zu einer totalen Überwachung am Arbeitsplatz führen. Neben der grundsätzlichen Vermeidung der Erhebung von Vorratsdaten und dem grundsätzlichen Verbot heimlicher Maßnahmen müsse ferner auch ein Höchstmaß an Transparenz sichergestellt werden. Aber nicht nur von legislativer Seite sei ein sorgsamer Umgang mit personenbezogenen Daten angezeigt. Dadurch, dass sich die Gefahren in der digitalisierten Arbeitswelt, angefangen bei der Bewerberauswahl, über den gesamten Bereich der Arbeitsrechtsverhältnisse erstrecken, müssten auch Arbeitgeber und -nehmer ein entsprechendes Verhalten an den Tag legen. Während auf Arbeitnehmerseite bereits früh, d.h. auch schon während seiner Schulzeit, angezeigt sei, selbstreflektiert und im Hinblick auf die etwaigen Konsequenzen vorausschauend mit seinen personenbezogenen Daten umzugehen, sollten Arbeitgeber auch ein gewisses Maß an Liberalität an den Tag legen. Dies impliziere letztlich beispielsweise auch, Menschen, die sich möglicherweise digital tätowieren, ja stigmatisiert haben, nicht aufgrund des sorglosen Umgangs mit ihren Daten aus dem Kreis von Bewerbern auszuschließen. Im Ergebnis bleibe festzuhalten, dass Ziel der Kontrollinstanzen sein muss, Wissen zu etablieren und klare Vorgaben zu schaffen. Neben der angesichts der zu erwartenden steigenden Eingaben bei den Datenschutzbehörden hierfür erforderlichen Umschichtung und Umstrukturierung der Behörden sei eines klar: Moderner Datenschutz erfordere auch zukünftig einen hohen Bedarf an Eigenverantwortung.

3.2. Weitergehendes Informationsmaterial des BfDI

Auf der Homepage des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit[732] ist diverses Informationsmaterial abrufbar, das sich u.a. auch mit Aspekten befasst, die im Zusammenhang mit dem Persönlichkeitsrechtsschutzes von Beschäftigten Bedeutung erlangen können. Im Übrigen gelangt man hier auch zu wichtigen datenschutzrechtlichen Gremien,[733] zum Datenschutzforum, den Landesdatenschutzbeauftragten, den Aufsichtsbehörden für den nicht-öffentlichen Bereich, den Rundfunkdatenschutzbeauftragten, zum virtuellen Datenschutzbüro sowie zu diversen anderen interessanten Websites, die Informationen im Bundesbereich und im europäischen und internationalen Kontext liefern.[734]

[732] Abrufbar unter http://www.bfdi.bund.de.

[733] Z.B. Nationale Datenschutzkonferenz, Düsseldorfer Kreis, Europäische Datenschutzkonferenz und Internationale Datenschutzkonferenz.

[734] Darüber hinaus gibt es natürlich eine Vielzahl anderer Websites [etwa von Interessenvertretungen wie dem Bundesverband Digitale Wirtschaft (BVDW) e.V. oder dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) e.V.], die die Thematik des Arbeitnehmerdatenschutzes aufgreifen. Angesichts des immensen Angebots kann hierauf i.R.d. hiesigen Ausführungen nicht eingegangen werden.

4. SANKTIONEN BEI DATENSCHUTZVERSTÖßEN

Wird von Arbeitgebern und -nehmern gegen Gesetze verstoßen, kann dies datenschutz- und arbeitsrechtliche sowie andere Sanktionen nach sich ziehen.

4.1. Sanktionen im Bereich des Datenschutzrechtes

Abgesehen von einer großen Auswahl an Sanktionsmaßnahmen in bereichsspezifischen Datenschutzregelungen (vgl. etwa exemplarisch die Straf- und Bußgeldvorschriften der §§ 148, 149 TKG) statuiert das Bundesdatenschutzgesetz beispielsweise, dass Verstöße gegen das Datenschutzrecht als Ordnungswidrigkeiten bußgeldbewehrt sind. Der Katalog des § 43 BDSG bietet hierfür eine Vielzahl von Möglichkeiten, die Nichteinhaltung der gesetzlichen Vorgaben zu sanktionieren. So können nach § 43 Abs. 3 S. 1 BDSG etwa Verstöße gegen Benachrichtigungs- und Auskunftspflichten (vgl. § 43 Abs. 1 Nr. 8 und Nr. 8a BDSG) mit bis zu 50.000 Euro, bei Verstößen in den Fällen des Absatzes 2 sogar mit einer Geldbuße bis zu 300.000 Euro geahndet werden.[735] Über § 44 BDSG werden bestimmte Handlungen sogar unter Strafe gestellt.[736] Die Verpflichtungen des BDSG treffen dabei die verantwortliche Stelle (§§ 1 Abs. 2, 2 BDSG), mithin den Leiter der Dienststelle oder die Unternehmensleitung.[737] In manchen Fällen haben ferner die Betroffenen die Möglichkeit, neben den ihren in § 6 Abs. 1 BDSG genannten Rechten Löschungs- oder Schadensersatzansprüche wegen unzulässiger oder unrichtiger Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten nach § 7 BDSG geltend zu machen.[738] Die Verletzung einer Benachrichtigungspflicht etwa eröffnet diese Möglichkeit hingegen nicht.[739] Für öffentlich-rechtliche Arbeitgeber kann sich beispielsweise eine verschuldensunabhängige Haftung aus § 8 BDSG ergeben.[740]

4.2. Sanktionen im Bereich des Arbeitsrechts

Prozessual gesehen besteht als beweisrechtliche Folge mitbestimmungswidrigen Handelns die Möglichkeit, Beweisverwertungsverbote aufgrund unzulässiger Mitarbeiterüberwachung zu verhängen.[741] Im Zivilprozess sind rechtswidrig erlangte Beweismittel nicht generell unverwertbar, sondern dann, wenn ein Verwertungsverbot nach dem Schutzzweck der bei der

---

[735] Vgl. auch § 43 Abs. 3 S. 2 und 3 BDSG: Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden.

[736] Oft werden aber Spezialnormen einschlägig sein, vgl. Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 1296.

[737] Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutzrecht, Rn. 1292.

[738] § 7 BDSG ist Anspruchsgrundlage für eine Haftung aus vermutetem Verschulden, Däubler, Gläserne Belegschaften?, Rn. 574.

[739] Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutzrecht, Rn. 338.

[740] Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutzrecht, Rn. 1370. Vgl. ferner Rn. 1371 ff. zu der Haftung bei hoheitlicher Tätigkeit aus Art. 34 GG i.V.m. § 839 BGB sowie im fiskalischen Bereich aufgrund etwaiger vertraglicher oder deliktischer Haftung nach §§ 31, 89 beziehungsweise § 831 BGB sowie § 839 BGB.

[741] Thüsing Arbeitnehmerdatenschutz und Compliance, Rn. 564.

Beweiserhebung verletzten Norm angezeigt ist.[742] Dies ist vor allem der Fall, wenn durch die Beweiserlangung verfassungsrechtlich geschützte Grundpositionen verletzt wurden,[743] mithin auch, wenn der Arbeitgeber Persönlichkeitsrechte seiner Beschäftigten verletzt hat.[744] In diesem Zusammenhang ist zu beachten, dass Arbeitgeber und Betriebsrat nach § 75 Abs. 2 S. 1 BetrVG eine Fürsorgepflicht trifft,[745] die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern. Doch auch Arbeitnehmer müssen bei pflichtwidrigem Verhalten mit Konsequenzen rechnen. Nutzen sie beispielsweise unbefugt die betriebliche Informations- und Kommunikationstechnik, drohen ihnen Abmahnungen, ordentliche bzw. ggf. sogar fristlose Kündigungen[746] sowie Entgeltkürzungen.[747] Auch können sie u.U. in die Haftung für rechtswidrig verursachte Schäden genommen werden.[748] Bezüglich vermögensrechtlicher Folgen ist jedoch zu beachten, dass im Beschäftigungsverhältnis Haftungsprivilegierungen bestehen, die in Abhängigkeit von dem Grad des Verschuldens und der Schadenshöhe eine Haftung eingrenzen beziehungsweise sogar ausschließen können.[749] Dies gilt allerdings nur für Schäden, die im Zusammenhang mit der betrieblichen Tätigkeit des Beschäftigten eingetreten sind, nicht hingegen für Schäden aufgrund unerlaubter Privatnutzung.[750]

4.3. Sonstige Sanktionen

Die Sanktionen des deutschen Rechts beschränken sich aber keineswegs nur auf den arbeits- und datenschutzrechtlichen Bereich. Gerade wenn unzulässige Überwachungsmaßnahmen in Frage stehen, läuft der Arbeitgeber Gefahr, nach den Vorschriften des StGB bestraft zu werden. Der Schutz von Informationen im weitesten Sinne kann insbesondere durch § 202a StGB (Ausspähen von Daten), § 202b StGB (Abfangen von Daten), § 202c StGB (Vorbereiten des Ausspähens und Abfangens von Daten), § 203 (Verletzung von Privatgeheimnissen), § 263a (Computerbetrug), § 268 StGB (Fälschung technischer Aufzeichnungen), § 269 StGB (Fälschung beweiserheblicher Daten), § 270 (Täuschung im

[742] BVerfGE 117, 202, 214. Vgl. zu den beweisrechtlichen Folgen der Wirksamkeitstheorie, der Differenzierung zwischen Beweiserhebung und -verwertung sowie dem Streit, wann ein Verwertungsverbot im Einzelnen angenommen werden kann, Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 564 ff.
[743] BGH, NJW 2005, 497, 498 f.
[744] St. Rspr. seit BGHZ 27, 284, 286; vgl. hierzu BVerfG, NJW 2002, 3619, 3624; NZA 1992, 307, 308; BAGE 105, 356, 358. Vgl. zu dem diesbezüglichen Streitstand Kratz/Gubbels, NZA 2009, 652, 655. Vgl. ferner Lunk, NZA 2009, 457, 459 ff. Der Schutz des Persönlichkeitsrechts von Mitarbeitern gehört zu den Schutz- bzw. Nebenpflichten des Arbeitgebers i.S.v. § 241 Abs. 2 BGB, BAG, NZA 1988, 53, 53; Preis, in ErfK zum Arbeitsrecht, Rn. 615, 620. Zu der Fürsorgepflicht (vor allem mit Blick auf § 75 Abs. 2 S. 1 BetrVG) sowie allgemein zu den Adressaten datenschutzrechtlicher Verpflichtungen vgl. Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 1292 ff.
[745] Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutzrecht, Rn. 1292.
[746] Vgl. hierzu Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 364 ff., Trappehl/Schmidl, NZA 2009, 985, 987 ff. sowie Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 1383 ff.
[747] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 361.
[748] Vgl. hierzu etwa Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 1343 ff.
[749] Grundlegend BAG, DB 1993, 939.
[750] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 384, der auch auf die Anrechnung eines etwaigen Mitverschuldens des Arbeitgebers i.S.d. § 254 BGB eingeht.

Rechtsverkehr bei Datenverarbeitung) § 274 StGB (Unterdrücken beweiserheblicher Daten), § 303a StGB (Datenveränderung) und § 303b StGB (Computersabotage) realisiert werden.[751]

Sofern der Arbeitgeber rechtswidrig auf Verbindungsdaten zugreift oder Telefonate in unzulässiger Weise kontrolliert, kann er sich wegen der Verletzung des Fernmeldegeheimnisses (§ 88 TKG) nach § 206 StGB strafbar machen.[752] Losgelöst von der Eigenschaft als Telekommunikationsanbieter kommt zudem eine Strafbarkeit nach § 201 StGB aufgrund der Verletzung der Vertraulichkeit des Wortes in Betracht.[753] Die Verletzung des Rechts am geschriebenen Wort kann darüber hinaus auch eine Strafbarkeit nach § 202 StGB (Verletzung des Briefgeheimnisses) nach sich ziehen.[754] Der Versand von Botschaften auf dem elektronischen Wege ist hiervon jedoch nicht erfasst.[755] Insofern fehlt es am Merkmal des Verschlossenseins des Schriftstücks.[756] Hier greift wiederum § 206 StGB,[757] der auch den Schutz von E-Mail-Verkehr umfasst.[758] Auf Seiten des Arbeitnehmers kann etwa ein Betrug (§ 263 StGB) begangen werden, wenn aufgrund unerlaubter Privatnutzung verursachte Kosten als dienstlich notwendig vorgespiegelt werden.[759] Darüber hinaus besteht die Möglichkeit, die Verletzung spezieller Geheimhaltungspflichten zu pönalisieren, z.B. über § 17 UWG (Verrat von Geschäfts- und Betriebsgeheimnissen) oder § 67 BBG (Verschwiegenheitspflicht).[760] Ferner kann in dem Abrufen und Verbreiten von Inhalten aus dem Internet ebenfalls ein Verstoß gegen straf- oder urheberrechtliche (vgl. die Straftatbestände der §§ 106 ff. UrhG)[761] Bestimmungen liegen.[762] Da die Datenschutzhaftungsnormen der §§ 7, 8 BDSG keine abschließenden Regelungen darstellen,[763] bleibt ein Rückgriff auf die allgemeinen zivilrechtlichen Ansprüche möglich.[764] Unzulässige Überwachungsmaßnahmen können dadurch z.B. empfindliche Entschädigungsforderungen nach sich ziehen.[765]

---

[751] Trappehl/Schmidl, NZA 2009, 985, 990; Schmidl, NJW 2010, 476, 479; Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 1341.
[752] Vgl. hierzu Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 103 ff.
[753] Vgl. zu der Unzulässigkeit heimlichen Mithörens BVerfG, NJW 2002, 3619 und BGH, RDV 2003, 237. Zu dem strafbaren Einsatz von Mithörtechnik vgl. Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 244 ff.
[754] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 51.
[755] So etwa Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 51.
[756] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 52.
[757] Verletzung des Post- oder Fernmeldegeheimnisses.
[758] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 52 sowie hinsichtlich der Einzelheiten Rn. 103 ff. Bezüglich des Schutzbereiches des Fernmeldegeheimnisses vgl. ferner Durner, in Maunz/Dürig, GG, Art. 10 Rn. 67.
[759] Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 378.
[760] Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 1296.
[761] Der Arbeitgeber kann dann Unterlassungs- und Beseitigungsansprüche geltend machen, vgl. Trappehl/ Schmidl, NZA 2009, 985, 990.
[762] Z.B. können § 86 StGB (Verbreiten von Propagandamitteln verfassungswidriger Organisationen), § 184 StGB (Verbreitung pornographischer Schriften) oder § 184b StGB (Verbreitung, Erwerb und Besitz kinderpornographischer Schriften) verletzt sein, Gola, Datenschutz und Multimedia am Arbeitsplatz, Rn. 197 Fn. 26 f.
[763] BT-Drs. 14/4458, S. 2.
[764] Gabel, in: Taeger/Gabel, BDSG, § 7 Rn. 23, § 8 Rn. 2. Vgl. zu der Darstellung der wesentlichen Anspruchsgrundlagen Gabel, in: Taeger/Gabel, BDSG, § 7 Rn. 24 ff. sowie Grimm/Schiefer, RdA 2009, 329, 343 f. und Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 503 ff.
[765] Vgl. etwa jüngst die Verurteilung eines Arbeitgebers zur Zahlung einer Entschädigung von 7.000 Euro wegen unzulässiger Videoüberwachung, LAG Hessen, MMR 2011, 346.

5. ZUSAMMENFASSUNG

Wie aufgezeigt, ist der Bereich des Persönlichkeitsrechtsschutzes von Arbeitnehmern aktuell sehr im Fluss. Die Regelungen de lege lata erweisen sich als größtenteils unzureichend, auch und gerade um den neuen Anforderungen der digitalisierten Arbeitswelt effektiv entgegenzutreten. Zwar gibt es – vor allem auch mit Blick auf die seitens des BAG entwickelte Rechtsprechung hinsichtlich des Abwägungsvorgangs – durchaus Ansätze, deren Intention begrüßenswert ist. Hingegen kann nach dem derzeitigen Stand der Dinge nicht davon gesprochen werden, über ausreichende Mittel zur Verwirklichung eines Beschäftigtendatenschutzes zu verfügen, der sich sowohl für Arbeitgeber als auch Arbeitnehmer als interessengerechte Lösung darstellt. Es bleibt abzuwarten, inwieweit der Gesetzgeber für Kritik offen, zu der Beseitigung von Schwachstellen des aktuellen Entwurfs gewillt[766] und zudem fähig ist, ausgewogene und mit Blick auf die Praxis auch sinnvolle Regelungen zu schaffen, die den Anforderungen an Rechtssicherheit und Rechtsklarheit in ausreichendem Maße gerecht werden. Bis es soweit ist, bleibt den Beteiligten gleichermaßen vor allem eines zu raten: „Abundans cautela non nocet“![767]

[766] Vgl. etwa Tinnefeld/Petri/Brink, MMR 2010, 727; Wybitul, MMR 2011, 313091 oder auch die Sachverständigenkritik vom 23.5.2011 (FD-ArbR 2011, 318249).

[767] Zu viel Vorsicht schadet nicht (aus dem Lateinischen übersetzt von Lauterbach, Latein – Deutsch: Zitaten-Lexikon, S. 135).

LITERATUR- UND QUELLENVERZEICHNIS

Albrecht, Florian/Maisch, Michael Marc: Bluttests und Verhaltensanalysen bei Bewerbern, Datenschutz-Berater 3/2010, S. 11-18.

Altenburg, Stephan/von Reinersdorff, Wolfgang/Leister, Thomas Betriebsverfassungsrechtliche Aspekte der Telekommunikation am Arbeitsplatz, Multimedia und Recht 2005, S. 135-138.

Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe „Protokollierung“, 2009, http://www.bfdi.bund.de/SharedDocs/Publikationen/Orientierungshilfen/OHProtokollierung.pdf?__blob=publicationFile. [01.04.2011]

Art-29-Datenschutzgruppe, RFID, 2005, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_de.pdf. [18.04.2011]

Aufsichtsbehörde Baden-Württemberg, Hinweis zum BDSG Nr. 3, Staatsanzeiger vom 1.7.1978, Nr. 52.

Backes, Volker/Eul, Harald/Guthmann, Markus/Martwich, Robert/Schmidt, Mirko: Entscheidungshilfe für die Übermittlung personenbezogener Daten in Drittländer, Recht der Datenverarbeitung 2004, S.156-163.

Bartmann, Dieter/Wimmer, Martin: Kein Problem mehr mit vergessenen Passwörtern: Webbasiertes Password Reset mit dem psychometrischen Merkmal Tippverhalten, Datenschutz und Datensicherheit 2007, S. 199-202.

Bausback, Winfried: Fesseln für die wehrhafte Demokratie?, Neue Juristische Wochenschrift 2006, S. 1922-1924.

Bayreuther, Frank: Videoüberwachung am Arbeitsplatz, Neue Zeitschrift für Arbeitsrecht 2005, S. 1038-1044.

Beckschulze, Martin: Internet-, Intranet- und E-Mail-Einsatz am Arbeitsplatz – Rechte der Beteiligten und Rechtsfolgen bei Pflichtverletzungen, Der Betrieb 2003, S. 2777-2786.

Beckschulze, Martin: Internet- und E-Mail-Einsatz am Arbeitsplatz, Der Betrieb 2009, S. 2097-2103.

Beckschulze, Martin/Henkel, Wolfram: Der Einfluß des Internets auf das Arbeitsrecht, Der Betrieb 2001, S. 1491-1506.

Beckschulze, Martin/Natzel, Ivo: Das neue Beschäftigtendatenschutzgesetz, Betriebs-Berater 2010, S. 2368-2375.

Behling, Thorsten B.: Compliance versus Fernmeldegeheimnis, Betriebs-Berater 2010, S. 892-896.

Beisenherz, Gerhard/Tinnefeld, Marie-Theres: Sozialdatenschutz – eine Frage des Beschäftigtendatenschutzes?, Datenschutz und Datensicherheit 2010, S. 221-224.

Bergmann, Lutz/Möhrle, Roland/Herb, Armin: Datenschutzrecht, Boorberg, Stuttgart, München, Hannover, 2011.

Besgen, Nicolai/Prinz, Thomas: § 1 Dienstliche Nutzung von Internet, Intranet und E-Mail, in: Besgen, Nicolai/Prinz, Thomas (Hrsg.): Handbuch Internet: Arbeitsrecht: Rechtssicherheit

bei Nutzung, Überwachung und Datenschutz, Deutscher Anwaltsverlag, Bonn, 2009.

Bierekoven, Christiane: Korruptionsbekämpfung vs. Datenschutz nach der BDSG-Novelle, COMPUTER UND RECHT 2010, S. 203-208.

Bissels, Alexander: Background Checks bei der Begründung des Arbeitsverhältnisses – Was darf der Arbeitgeber?, juris AnwaltZertifikatOnline Arbeitsrecht 13, Anm. 2 2009.

Bissels, Alexander: Standpunkt Twitter & Co.: Neue Herausforderungen an das Arbeitsrecht, Betriebs-Berater 2009, S. 2197.

Bissels, Alexander/Lützeler, Martin/Wisskirchen, Gerlind: Facebook, Twitter & Co.: Das Web 2.0 als arbeitsrechtliches Problem, Betriebs-Berater 2010, S. 2433-2439.

Bizer, Johann, in: Simitis, Spiros (Hrsg.): Bundesdatenschutzgesetz, Nomos, Baden-Baden, 2011.

Bloesinger, Hubert: Grundlagen und Grenzen privater Internetnutzung am Arbeitsplatz, Betriebs-Berater 2007, S. 2177-2184.

Bonn, Heinz Paul: BITKOM Presseinformation vom 6.4.2011, http://www.bitkom.org/files/documents/RFID_PIA_06_04_2011.pdf. [06.04.2011]

Braun, Frank/Spiegl, Katarina: E-Mail und Internet am Arbeitsplatz – Was ist erlaubt? Was ist verboten?, Arbeitsrecht im Betrieb 2008, S. 393-397.

Brink, Stefan/Schmidt, Stephan: Die rechtliche (Un-)Zulässigkeit von Mitarbeiterscreenings – Vom schmalen Pfad der Legalität, MultiMedia und Recht 2010, S. 592-596.

Buchner, Benedikt, in: Taeger, Jürgen/Gabel, Detlev (Hrsg.): Kommentar zum BDSG und den Datenschutzvorschriften des TKG und TMG, Verlag Recht und Wirtschaft, Frankfurt a.M., 2010.

Büllesbach, Alfred, in: Roßnagel, Alexander (Hrsg.): Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, Beck, München, 2003.

Bundesministerium des Innern: Hintergrundpapier zum Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes: Kabinettbeschluss vom 25.8.2010, http://www.bmi.bund.de/SharedDocs/Downloads/DE/Kurzmeldungen/pressepapier_beschaeftigtendatenschutz.pdf;jsessionid=875DDC94DFC4D74B5F2EF98355FF1A07.1_cid165?__blob=publicationFile. [01.04.2011]

Busse, Julia: § 10 Datenschutz, in: Besgen, Nicolai/Prinz, Thomas (Hrsg.): Handbuch Internet: Arbeitsrecht: Rechtssicherheit bei Nutzung, Überwachung und Datenschutz, Deutscher Anwaltsverlag, Bonn, 2009

Callies, Christian, in: Calliess, Christian/Ruffert, Matthias (Hrsg.): EUV, AEUV: Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, Beck, München, 2011.

Caspar, Johannes: Interview mit Dipl.-Jur. Falk Hagedorn vom 18.5.2011, http://pawproject.eu/de/dokumente. [18.05.2011]

CDU/CSU/FDP: Wachstum. Bildung. Zusammenhalt, Koalitionsvertrag zwischen CDU, CSU und FDP, 2009, http://www.cdu.de/doc/pdfc/091026-koalitionsvertrag-cducsu-fdS.pdf. [01.04.2011]

Dammann, Ulrich, in: Simitis, Spiros (Hrsg.): Bundesdatenschutzgesetz, Nomos, Baden-Baden, 2011.

Dann, Matthias/Gastell, Roland Gastell: Geheime Mitarbeiterkontrollen: Straf- und arbeitsrechtliche Risiken bei unternehmensinterner Aufklärung, Neue Juristische Wochenschrift 2008, S. 2945-2949.

Däubler, Wolfgang: Nutzung des Internet durch Arbeitnehmer, Kommunikation und Recht 2000, S. 323-327.

Däubler, Wolfgang: Grundrechte-Charta und kollektives Arbeitsrecht, Arbeit und Recht 2001, S. 380-384.

Däubler, Wolfgang: Das neue Bundesdatenschutzgesetz und seine Auswirkungen im Arbeitsrecht, Neue Zeitschrift für Arbeitsrecht 2001, S. 874-881.

Däubler, Wolfgang: Internet und Arbeitsrecht, Bund-Verlag, Frankfurt a.M., 2004.

Däubler, Wolfgang: Arbeitsrecht und Informationstechnologien – Vom Umgang eines traditionellen Rechtsgebiets mit neuen Herausforderungen, COMPUTER UND RECHT 2005, S. 767-772.

Däubler, Wolfgang: Gläserne Belegschaften?: Das Handbuch zum Arbeitnehmerdatenschutz, Bund-Verlag, Frankfurt a.M., 2010.

De Maizière, Thomas: Bundesministerium des Innern, 14 Thesen zu den Grundlagen einer gemeinsamen Netzpolitik der Zukunft, 2010, http://www.bmi.bund.de/cae/servlet/contentblob/1099988/publicationFile/88667/thesen_netzpolitik.pdf. [26.05.2011]

Deutsch, Markus/Diller, Martin: Die geplante Neuregelung des Arbeitnehmerdatenschutzes in § 32 BDSG, Der Betrieb 2009, S. 1462-1465.

De Wolf, Abraham: Kollidierende Pflichten: Zwischen Schutz von E-Mails und "Compliance" im Unternehmen, Neue Zeitschrift für Arbeitsrecht 2010, S. 1206-1210.

Dickmann, Roman: Inhaltliche Ausgestaltung von Regelungen zur privaten Internetnutzung im Betrieb, Neue Zeitschrift für Arbeitsrecht 2003, S. 1009-1013.

Di Fabio, Udo, in: Maunz, Theodor/Dürig, Günter (Hrsg.): Grundgesetz, Beck, München, 2009.

Dieterich, Thomas, in: Dieterich, Thomas/Hanau, Peter/Schaub, Günter: Erfurter Kommentar zum Arbeitsrecht, Beck, München, 2011.

Durner, Wolfgang, in: Maunz, Theodor/Dürig, Günter (Hrsg.): Grundgesetz, Beck, München, 2011.

Düsseldorfer Kreis: Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 8. April 2011, http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/08042011lDatenschutzKodex.pdf;jsessionid=E00DA804E1E079427B96060617D5C96F.1_cid136?__blob=publicationFile. [08.04.2011]

Ege, Andreas: Arbeitsrecht und Web 2.0 – Online-Tagebücher, Corporate Blogging, Wikis, Arbeit und Arbeitsrecht, 2008, S. 72-74.
Ehmann, Horst: Zur Struktur des Allgemeinen Persönlichkeitsrechts, Juristische Schulung 1997, S. 193-203.

Ehmer, Jörg, in: Geppert, Martin/Piepenbrock, Hermann-Josef/Schütz, Raimund/Fabian Schuster (Hrsg.): Beck'scher TKG-Kommentar, Beck, München, 2006.

Erler, Andreas: Die private Nutzung neuer Medien am Arbeitsplatz, Utz, München, 2003.

Ernst, Stefan: Der Arbeitgeber, die E-Mail und das Internet, Neue Zeitschrift für Arbeitsrecht 2002, S. 585-591.

Evers, Hans-Ulrich: Verletzung des Postgeheimnisses (Art 10 GG) und Beweisverwertungsverbot im Strafprozeß – Zugleich Besprechung des Beschlusses des LG Stuttgart vom 1964-09-29 IV QS 117/64, JuristenZeitung 1965, S. 661-666.

Fleck, Ulrike: Brauchen wir ein Arbeitnehmerdatenschutzgesetz?, Betriebs-Berater 2003, S. 306-310.

Forst, Gerrit: Der Regierungsentwurf zur Regelung des Beschäftigtendatenschutzes, Neue Zeitschrift für Arbeitsrecht 2010, S. 1043-1048.

Franzen, Martin: Arbeitnehmerdatenschutz – rechtspolitische Perspektiven, Recht der Arbeit 2010, S. 257-263.

Fraunhofer-Institut für Angewandte Informationstechnik (FIT): Pressemeldung vom 24. November 2010, http://www.fit.fraunhofer.de/presse/10-11-24_de.html. [01.04.2011)

Friedrich, Hans-Peter, Gastkommentar in der Financial Times Deutschland vom 26.5.2011, http://www.ftd.de/it-medien/medien-internet/: gastkommentar-des-innenministers-das-internet-braucht-nicht-immer-gleich-gesetze/60056634.html. [26.05.2011]

Gabel, Detlev, in: Taeger, Jürgen/Gabel, Detlev (Hrsg.): Kommentar zum BDSG und den Datenschutzvorschriften des TKG und TMG, Verlag Recht und Wirtschaft, Frankfurt a.M., 2010.

Gastell, Dann: Geheime Mitarbeiterkontrollen: Straf- und arbeitsrechtliche Risiken bei unternehmensinterner Aufklärung, Neue juristische Wochenschrift 2008, S. 2945-2949.

Gerhards, Julia: (Grund-)Recht auf Verschlüsselung?, Nomos, Baden-Baden, 2010.

Gola, Peter: Neuer Tele-Datenschutz für Arbeitnehmer? – Die Anwendung von TKG und TDDSG im Arbeitsverhältnis, MultiMedia und Recht 1999, S. 322-330.

Gola, Peter: Die Einwilligung als Legitimation für die Verarbeitung von Arbeitnehmerdaten, Recht der Datenverarbeitung 2002, S. 109-116.

Gola, Peter: Datenschutz bei der Kontrolle „mobiler" Arbeitnehmer – Zulässigkeit und Transparenz, Neue Zeitschrift für Arbeitsrecht 2007, S.1139-1144.

Gola, Peter: Datenschutz und Multimedia am Arbeitsplatz: Rechtsfragen und Handlungshilfen für die betriebliche Praxis, Datakontext, Heidelberg, 2010.

Gola, Peter, in: Hümmerich, Klaus/Boecken, Winfried/Düwell, Franz Josef (Hrsg.): AnwaltKommentar Arbeitsrecht, Deutscher Anwaltverlag, Bonn, 2010.

Gola, Peter/Klug, Christoph: Videoüberwachung gemäß § 6b BDSG – Anmerkungen zu einer verunglückten Gesetzeslage, Recht der Datenverarbeitung 2004, S. 65-74.

Gola, Peter/Schomerus, Rudolf: Bundesdatenschutzgesetz: Kommentar, Beck, München, 2010.

Gola, Peter/Wronka, Georg: Handbuch zum Arbeitnehmerdatenschutz: Rechtsfragen unter Berücksichitgung der BDSG-Novellen, Datakontext, Heidelberg, 2010.

Grentzenberg, Verena/Schreibauer, Markus/Schuppert, Stefan: Die Datenschutznovelle (Teil II) – Ein Überblick zum "Gesetz zur Änderung datenschutzrechtlicher Vorschriften", Kommunikation und Recht 2009, S. 535-543.

Grimm, Detlef/Brock, Martin/Windeln, Norbert: Video-Überwachung am Arbeitsplatz, Der

Arbeits-Rechts-Berater 2006, S. 179-182.

Grimm, Detlef/Schiefer, Jennifer: Videoüberwachung am Arbeitsplatz, Recht der Arbeit 2009, S. 329-344.

Grobys, Marcel: Wir brauchen ein Arbeitnehmerdatenschutzgesetz!, Betriebs-Berater 2003, S. 682-683.

Grosjean, Sascha R.: Überwachung von Arbeitnehmern – Befugnisse des Arbeitgebers und mögliche Beweisverwertungsverbote, Der Betrieb 2003, S. 2650-2654.

Groß, Thomas, in: Friauf, Karl Heinrich/Höfling, Wolfgang (Hrsg.): Berliner Kommentar zum Grundgesetz, Erich Schmidt Verlag, Berlin, 2011.

Hanau, Peter/Hoeren, Thomas: Private Internetnutzung durch Arbeitnehmer: Die arbeits- und betriebsverfassungsrechtlichen Probleme, Beck, München, 2003.

Hansen, Marit/Wiese, Markus: RFID – Radio Frequency Identification, Datenschutz und Datensicherheit 2004, S. 109.

Hartmann, Daniel/Pröpper, Martin (2009): Internet und E-Mail am Arbeitsplatz – Mustervereinbarung für den dienstlichen und privaten Zugang, Betriebs-Berater 2009, S. 1300-1302.

Heckmann, Dirk, in: Taeger, Jürgen/Gabel, Detlev (Hrsg.): Kommentar zum BDSG und den Datenschutzvorschriften des TKG und TMG, Verlag Recht und Wirtschaft, Frankfurt a.M., 2010.

Heidrich, Joerg: Rechtliche Fragen bei der Verwendung von DNS-Blacklisting zur Spam-Filterung, COMPUTER UND RECHT 2009, S. 168-173.

Heise online: Newsticker vom 21.07.2010, http://www.heise.de/newsticker/meldung/Facebook-meldet-500-Millionen-Mitglieder-1043251.html. [21.07.2010]

Heldmann, Sebastian: Betrugs- und Korruptionsbekämpfung zur Herstellung von Compliance – Arbeits- und datenschutzrechtliche Sicht, Der Betrieb 2010, S. 1235-1239.

Helle, Jürgen: Die heimliche Videoüberwachung – zivilrechtlich betrachtet, JuristenZeitung 2004, S. 340-347.

Hesse, Konrad: Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland, Müller, Heidelberg, 1985.

Hilber, Marc D.: Die datenschutzrechtliche Zulässigkeit intranet-basierter Datenbanken internationaler Konzerne, Recht der Datenverarbeitung 2005, S. 143-152.

Hillgruber, Christian: Der Staat des Grundgesetzes – nur bedingt abwehrbereit? Plädoyer für eine wehrhafte Verfassungsinterpretation, JuristenZeitung 2007, S. 209-218.

Hoeren, Thomas/Sieber, Ulrich: Handbuch Multimedia-Recht, Beck, München, 2010.

Hold, Dieter: Arbeitnehmer-Datenschutz – Ein Überblick, Recht der Datenverarbeitung 2006, S. 249-259.

Holzner, Stefan: Neues zur Regelung der Nutzung von E-Mail und Internet am Arbeitsplatz?, Zeitschrift für Rechtspolitik 2011, S. 12-15.

Hoppe, Christian: Arbeitnehmerhaftung und ihre Auswirkungen auf die Nutzung betrieblicher Kommunikationsmittel, Arbeitsrecht Aktuell 2010, S. 388.

Hoppe, René/Braun, Frank: Arbeitnehmer-E-Mails: Vertrauen ist gut – Kontrolle ist schlecht –

Auswirkungen der neuesten Rechtsprechung des BVerfG auf das Arbeitsverhältnis, MultiMedia und Recht 2010, S. 80-84.

Hornung, Gerrit/Desoi, Monika: "Smart Cameras" und automatische Verhaltensanalyse – Verfassungs- und datenschutzrechtliche Probleme der nächsten Generation der Videoüberwachung, Kommunikation und Recht 2011, S. 153-158.

Jandt, Silke: Datenschutz bei Location Based Services – Voraussetzungen und Grenzen der rechtmäßigen Verwendung von Positionsdaten, MultiMedia und Recht 2007, S. 74-78.

Jenau, Jens: Private Nutzung von Internet und Firmen-E-Mail-Adresse am Arbeitsplatz, Arbeitsrecht im Betrieb 2010, S. 88-92.

John, Dana, in: Kilian, Wolfgang/Heussen, Benno (Hrsg.): Computerrechts-Handbuch: Informationstechnologie in der Rechts- und Wirtschaftspraxis, Beck, München, 2011.

Jordan, Christopher/Bissels, Alexander/Löw, Christine: Arbeitnehmerkontrolle im Call-Center durch Silent Monitoring und Voice Recording, Betriebs-Berater 2008, S. 2626-2631.

Kamp, Meike/Körffer, Barbara: Auswirkungen des § 32 BDSG auf die Aufgabenerfüllung und die strafrechtliche Verantwortung des Compliance Officers, Recht der Datenverarbeitung 2010, S. 72-76.

Kania, Thomas: Gleichbehandlung, in: Küttner, Wolfdieter/Roller, Jürgen (Hrsg.): Personalbuch 2011: Arbeitsrecht, Lohnsteuerrecht, Sozialversicherungsrecht, Beck, München, 2011.

Kempf, Dieter: Statement „Datenschutz im Internet“ vom 08.02.2011, http://www.bitkom.org/files/documents/BITKOM_Statement_Datenschutz_Prof_Kempf_08_02_2011.pdf. [01.04.2011]

Kinast, Karsten, in: Taeger, Jürgen/Gabel, Detlev (Hrsg.): Kommentar zum BDSG und den Datenschutzvorschriften des TKG und TMG, Verlag Recht und Wirtschaft, Frankfurt a.M., 2010.

Kirsch, Markus: Die datenschutzrechtliche Beurteilung von Kamera-Attrappen im Betrieb; MultiMedia und Recht-Aktuell 2011, 317919.

Kliemt, Michael: Vertrauen ist gut, Kontrolle ist besser? Internet- und E-Mail-Nutzung von Mitarbeitern, Arbeit und Arbeitsrecht 2011, S. 532-538.

Klug, Christoph: Beispiele richtlinienkonformer Auslegung des BDSG, Recht der Datenverarbeitung 2001, S. 266-274.

Koch, Frank A.: Rechtsprobleme privater Nutzung betrieblicher elektronischer Kommunikationsmittel, Neue Zeitschrift für Arbeitsrecht 2008, S. 911-916.

Kort, Michael: Lückenhafte Reform des Beschäftigtendatenschutzes – Offene Fragen und mögliche Antworten in Bezug auf die geplanten §§ 32 ff. BDSG, MultiMedia und Recht 2011, S. 294-299.

Kramer, Ernst A., in: Säcker, Franz Jürgen/Rixecker, Roland (Hrsg.): Münchener Kommentar zum Bürgerlichen Gesetzbuch: BGB: Band 2: Schuldrecht Allgemeiner Teil: §§ 241-432, Beck, München, 2007.

Kramer, Philipp: Dix in Hamburg: „§ 32 BDSG ist Baustellenschild“, Datenschutz-Berater 5/2010, S. 14-16.

Kramer, Stefan: Internetnutzung als Kündigungsgrund, Neue Zeitschrift für Arbeitsrecht 2004, S. 458-467.

Kramer, Stefan: Gestaltung betrieblicher Regelungen zur IT-Nutzung, Arbeitsrecht Aktuell 2010, S. 164.

Kratz, Felix/Gubbels, Achim: Beweisverwertungsverbote bei privater Internetnutzung am Arbeitsplatz, Neue Zeitschrift für Arbeitsrecht 2009, S. 652-656.

Kunst, Heiko: Individualarbeitsrechtliche Informationsrechte des Arbeitnehmers, 2003 Individualarbeitsrechtliche Informationsrechte des Arbeitnehmers: Ein Beitrag zur Informationsordnung im Arbeitsverhältnis, Lang, Frankfurt a.M., 2003.

Langrock, Marc/Samson, Erich: Bekämpfung von Wirtschaftskriminalität im und durch Unternehmen, Der Betrieb 2007, S. 1684-1689.

Lembke, Mark, in: Henssler, Martin/Willemsen, Josef/Kalb, Heinz-Jürgen (Hrsg.): Arbeitsrecht Kommentar, Verlag Dr. Otto Schmidt, Köln, 2010.

Lerch, Hana/Krause, Beate/Hotho, Andreas/Roßnagel, Alexander/Stumme, Gerd: Social Bookmarking-Systeme – die unerkannten Datensammler – Ungewollte personenbezogene Datenverabeitung?, MultiMedia und Recht 2010, S. 454-458.

Lindemann, Achim/Simon, Oliver: Betriebsvereinbarungen zur E-Mail, Internet- und Intranet-Nutzung, Betriebs-Berater 2001, S. 1950-1956.

Löwisch, Manfred: Fernmeldegeheimnis und Datenschutz bei der Mitarbeiterkontrolle, Der Betrieb 2009, S. 2782-2786.

Lunk, Stefan: Prozessuale Verwertungsverbote im Arbeitsrecht, Neue Zeitschrift für Arbeitsrecht 2009, S. 457-464.

Mähner, Nicolas: Neuregelung des § 32 BDSG zur Nutzung personenbezogener Mitarbeiterdaten – Am Beispiel der Deutschen Bahn AG, MultiMedia und Recht 2010, S. 379-382.

Marxen, Horst: Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses (Art. 10 GG): Unter besonderer Berücksichtigung der gesetzlich zulässigen Ausnahmen, without obligation, Kiel, 1958

Maschmann, Frank: Zuverlässigkeitstest durch Verführung illoyaler Mitarbeiter?, Neue Zeitschrift für Arbeitsrecht 2002, S. 13-22.

Maties, Martin: Arbeitnehmerüberwachung mittels Kamera?, Neue Juristische Wochenschrift 2008, S. 2219-2225.

Mattl, Tina: Die Kontrolle der Internet- und E-Mail Nutzung am Arbeitsplatz, Verlag Dr. Kovaĉ, Hamburg, 2008.

Mengel, Anja: Kontrolle der Telefonkommunikation am Arbeitsplatz, Betriebs-Berater 2004, S. 1445-1453.

Mengel, Anja: Kontrolle der E-Mail- und Internetkommunikation am Arbeitsplatz, Betriebs-Berater 2004, S. 2014-2021.

Mengel, Anja: Alte arbeitsrechtliche Realitäten im Umgang mit der neuen virtuellen Welt, Neue Zeitschrift für Arbeitsrecht 2005, S. 752-754.

Meyer, Sebastian: Ortung eigener Mitarbeiter zu Kontrollzwecken, in: Taeger, Jürgen/Wiebe, Andreas (Hrsg.): Von AdWords bis Social Networks: Neue Entwicklungen im Informationsrecht: Tagungsband Herbstakademie 2008, Edewecht, Oldenburg, 2008.

Ders.: Mitarbeiterüberwachung: Kontrolle durch Ortung von Arbeitnehmern, Kommunikation und Recht 2009, S. 14-20.

Moll, Wilhelm: Münchener Anwaltshandbuch Arbeitsrecht, Beck, München, 2009.

Mozek, Martin/Zendt, Marcus, in: Hoeren, Thomas/Sieber, Ulrich (Hrsg.): Handbuch Multimedia-Recht: Rechtsfragen des elektronischen Geschäftsverkehrs, Beck, München, 2011.

Müller-Glöge, Rudi, in: Säcker, Franz Jürgen/Rixecker, Roland (Hrsg.): Münchener Kommentar zum Bürgerlichen Gesetzbuch: BGB: Band 4: Schuldrecht Besonderer Teil II §§ 611-704 EFZG, TzBfG, KSchG, Beck, München, 2009.

Munz, Martin, in Taeger, Jürgen/Gabel, Detlev (Hrsg.): Kommentar zum BDSG und den Datenschutzvorschriften des TKG und TMG, Verlag Recht und Wirtschaft, Frankfurt a.M., 2010.

Müller, Arnold: Die Zulässigkeit der Videoüberwachung am Arbeitsplatz: In der Privatwirtschaft aus arbeitsrechtlicher Sicht, Nomos, München, 2008.

Moos, Flemming, in Taeger, Jürgen/Gabel, Detlev (Hrsg.): Kommentar zum BDSG und den Datenschutzvorschriften des TKG und TMG, Verlag Recht und Wirtschaft, Frankfurt a.M., 2010.

Nägele, Stefan/Meyer, Lars: Internet und E-Mail am Arbeitsplatz: Rechtliche Rahmenbedingungen der Nutzung und Kontrolle sowie der Reaktion auf Missbrauch, Kommunikation und Recht 2004, S. 312-316.

Naujock, Anja: Internet-Richtlinien – Nutzung am Arbeitsplatz – Ein Plädoyer für eine klare Regelung, Datenschutz und Datensicherheit 2002, S. 592-596.

Oberwetter, Christian: Arbeitnehmerrechte bei Lidl, Aldi & Co., Neue Zeitschrift für Arbeitsrecht 2008, S. 609-613.

Oberwetter, Christian: Soziale Netzwerke im Fadenkreuz des Arbeitsrechts, Neue Juristische Wochenschrift 2011, S. 417-421.

Oehler, Dietrich: Postgeheimnis, in: Neumann, Franz L./Nipperdey, Hans Carl/Scheuner, Ulrich (Hrsg.): Die Grundrechte: Handbuch der Theorie und Praxis der Grundrechte: Band 2, Duncker & Humblot, Berlin, 1954.

Orantek, Kerstin: Datenschutz im Informationszeitalter: Herausforderungen durch technische, politische und gesellschaftliche Entwicklungen, GUC-Verlag, Lößnitz, 2008.

Ott, Stephan: Stephan Das Internet vergisst nicht – Rechtsschutz für Suchobjekte?, MultiMedia und Recht 2009, S. 158-163.

Pagenkopf, Martin, in: Sachs, Michael (Hrsg.): Grundgesetz, Kommentar, Beck, München, 2009.

Pauly, Stephan/Osnabrügge, Stephan: § 6 Überlassung und Nutzung von Arbeitsmitteln, in: Besgen, Nicolai/Prinz, Thomas (Hrsg.): Handbuch Internet: Arbeitsrecht: Rechtssicherheit bei Nutzung, Überwachung und Datenschutz, Deutscher Anwaltsverlag, Bonn, 2009.

Petri, Thomas: Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, in: Kartmann, Norbert/Ronellenfitsch, Michael (Hrsg.): Vorgaben des Bundesverfassungsgerichts für eine zeitgemäße Datenschutzkultur in Deutschland: 17. Wiesbadener Forum Datenschutz, Der Hessische Datenschutzbeauftragte, Der Präsident des Hessischen Landtags, Wiesbaden, 2009.

Petri, Thomas: Compliance und Datenschutz, in: Schweighofer, Erich/Geist, Anton/Staufer, Ines (Hrsg.): Globale Sicherheit und proaktiver Staat – Die Rolle der Rechtsinformatik: Tagungsband des 13. Internationalen Rechtsinformatik Symposions IRIS 2010, OCG books, Wien, 2010.

Post-Ortmann, Karin: Der Arbeitgeber als Anbieter von Telekommunikations- und Telediensten, Recht der Datenverarbeitung 1999, S. 102-109.

Preis, Ulrich, in: Dieterich, Thomas/Hanau, Peter/Schaub, Günter: Erfurter Kommentar zum Arbeitsrecht, Beck, München, 2011.

Pröpper, Martin/Römermann, Martin: Nutzung von Internet und E-Mail am Arbeitsplatz (Mustervereinbarung), MultiMedia und Recht 2008, S. 514-518.

Raffner, Andrea/Hellich, Peter: Unter welchen Voraussetzungen ist die Überwachung von Arbeitnehmer-E-Mails zulässig?, Neue Zeitschrift für Arbeitsrecht 1997, S. 862-868.

Raif, Alexander: Beschäftigtendatenschutz: Wird alles neu bei der Arbeitnehmerkontrolle?, Arbeitsrecht Aktuell 2010, S. 359.

Raif, Alexander/Bordet, Katharina: Twitter, Facebook & Co. – Arbeitrechtliche Fragen im Web 2.0, Arbeit und Arbeitsrecht 2010, S. 88-90.

Rasmussen-Bonne, Hans-Eric/Raif, Alexander: Neues beim Beschäftigtendatenschutz – Worauf sich Unternehmen einstellen müssen, Gesellschafts- und Wirtschaftsrecht 2011, S. 80.

Rath, Michael/Karner, Sophia: Private Internetnutzung am Arbeitsplatz – rechtliche Zulässigkeit und Kontrollmöglichkeiten des Arbeitgebers, Kommunikation und Recht 2007, S. 446-452.

Rath, Michael/Karner, Sophia: Internetnutzung und Datenschutz am Arbeitsplatz, Kommunikation und Recht 2010, S. 469-475.

Richardi, Reinhard/Kortstock, Ulf: BAG: Videoüberwachung am Arbeitsplatz – allgemeines Persönlichkeitsrecht – Grundsatz der Verhältnismäßigkeit – Besprechung des Beschlusses BAG v. 29. 6. 2004 - 1 ABR 21/03, Recht der Arbeit 2005, S. 381-384.

Richardi, Reinhard: Betriebsverfassungsgesetz: BetrVG mit Wahlordnung, Beck, München, 2010.

Roloff, Sebastian: § 5 Überwachungseinrichtungen, in: Besgen, Nicolai/Prinz, Thomas (Hrsg.): Handbuch Internet: Arbeitsrecht: Rechtssicherheit bei Nutzung, Überwachung und Datenschutz, Deutscher Anwaltsverlag, Bonn, 2009.

Roßnagel, Alexander: Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, Beck, München, 2003.

Sachverständigenkritik, 23.5.2011, Fachdienst Arbeitsrecht, 318249.

Salvenmoser, Steffen/Hauschka, Christoph E.: Korruption, Datenschutz und Compliance, Neue Juristische Wochenschrift 2010, S. 331-335.

Sassenberg, Thomas/Bamberg, Niclas: Betriebsvereinbarung contra BDSG?, Datenschutz und Datensicherheit 2006, S. 226-229.

Schaar, Peter: Dokumentation der Festveranstaltung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder aus Anlass des 25. Jahrestages der Verkündung des Volkszählungsurteils des Bundesverfassungsgerichts am 15. Dezember 2008 im Bürgersaal des Karlsruher Rathauses, 2008, http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/Dokumentation25JahreV

olkszaehlungsurteil.pdf?__blob=publicationFile. [01.04.2011]

Schaar, Peter, Gespräch mit der Projektgruppe Datenschutz der Enquete-Kommission "Internet und digitale Gesellschaft" vom 21.2.2011, http://www.bundestag.de/dokumente/textarchiv/2011/33500340_kw08_pa_schaar/index.html . [01.04.2011]

Schmidt, Bernd: Arbeitnehmerdatenschutz gemäß § 32 BDSG – Eine Neuregelung (fast) ohne Veränderung der Rechtslage, Recht der Datenverarbeitung 2009, S. 193-200.

Schmidt, Bernd: Vertrauen ist gut, Compliance ist besser, Betriebs-Berater 2009, S. 1295-1299.

Schmidt, Bernd: Beschäftigtendatenschutz in § 32 BDSG – Perspektiven einer vorläufigen Regelung, Datenschutz und Datensicherheit 2010, S. 207-209.

Schmidt, Walter: Die bedrohte Entscheidungsfreiheit, JuristenZeitung 1974, S. 241-250.

Schmitt-Rolfes, Günther: Kontrolle von Internet- und E-Mail-Nutzung am Arbeitsplatz, Arbeit und Arbeitsrecht 2008, S. 391.

Schaffland, Hans-Jürgen/Wiltfang, Noeme: Bundesdatenschutzgesetz (BDSG): Ergänzbarer Kommentar nebst einschlägigen Rechtsvorschriften, Erich Schmidt Verlag, Berlin, 2010.

Schaub, Günter/Linck, Rüdiger, in: Schaub, Günther: ArbeitsR-Handbuch: Systematische Darstellung und Nachschlagewerk für die Praxis, Beck, München, 2009.

Scheja, Gregor, in: Taeger, Jürgen/Gabel, Detlev (Hrsg.): Kommentar zum BDSG und den Datenschutzvorschriften des TKG und TMG, Verlag Recht und Wirtschaft, Frankfurt a.M., 2010.

Schmidl, Michael: Aspekte des Rechts der IT-Sicherheit, Neue Juristische Wochenschrift 2010, S. 476-481.

Schmidt, Bernd, in: Taeger, Jürgen/Gabel, Detlev (Hrsg.): Kommentar zum BDSG und den Datenschutzvorschriften des TKG und TMG, Verlag Recht und Wirtschaft, Frankfurt a.M., 2010.

Schmitz, Peter/Eckhardt, Jens: Einsatz von RFID nach dem BDSG, COMPUTER UND RECHT 2007, S. 171-177.

Schrader, Hans-Hermann: 18. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten – zugleich Tätigkeitsbericht der Aufsichtsbehörde für den nicht öffentlichen Bereich 2000/2001, 2002.

Schuster, Friederike: Die Internetnutzung als Kündigungsgrund, Verlag Dr. Kovaĉ, Hamburg, 2009.

Seitz, Walter, in: Hoeren, Thomas/Sieber, Ulrich (Hrsg.): Handbuch Multimedia-Recht: Rechtsfragen des elektronischen Geschäftsverkehrs, Beck, München, 2011.

SID/FID: SID/FIT Social Media Report 2010/2011, 2011, http://www.softwareinitiative.de/studien/SID-FITSocialMediaReport20102011.pdf. [01.04.2011]

Simitis, Spiros: Schutz von Arbeitnehmerdaten, Regelungsdefizite, Lösungsvorschläge, Gutachten erstattet im Auftrag des Bundesministers für Arbeit und Sozialordnung, Bundesminister für Arbeit u. Sozialordnung, Referat Presse- u. Öffentlichkeitsarbeit, Bonn, 1981.

Simitis, Spiros: Zur Mitbestimmung bei der Verarbeitung von Arbeitnehmerdaten – Eine Zwischenbilanz, Recht der Datenverarbeitung 1989, S. 49-60.

Simitis, Spiros: Zur Internationalisierung des Arbeitnehmerdatenschutzes – Die verhaltensregeln der Internationalen Arbeitsorganisation, in: Hanau, Peter/Heither, Friedrich/Kühling, Jürgen (Hrsg.): Richterliches Arbeitsrecht: Festschrift für Thomas Dieterich zum 65. Geburtstag, Beck, München, 1999.

Simitis, Spiros: Arbeitnehmerdatenschutzgesetz – Realistische Erwartung oder Lippenbekenntnis?, Arbeit und Recht 2001, S. 429-433.

Simitis, Spiros: Zu den erwarteten Auswirkungen auf das deutsche Recht, Recht der Datenverarbeitung 2003, S. 43-49.

Simitis, Spiros: Bundesdatenschutzgesetz, Nomos, München, 2010.

SPIEGEL ONLINE, Netzwelt 26.4.2009, http://www.spiegel.de/netzwelt/web/0,1518,621185,00.html. [01.04.2011]

Steffen, Till/Weichert, Thilo: Gehört der private Datenschutz ins BGB?, Zeitschrift für Rechtspolitik 2009, S. 95.

Steinkühler, Bernhard/Raif, Alexander: Big brother am Arbeitsplatz: Arbeitnehmerüberwachung auf neustem technischem Stand, Arbeit und Arbeitsrecht 2009, S. 213-217.

Stück, Volker: LAG Rheinland-Pfalz: Nutzungsverbot für privates Handy während Arbeitszeit, Arbeitsrecht Aktuell 2010, S. 432.

TBS: Technologieberatungsstelle beim DGB NRW e.V.: VoIP – Telefonieren übers Internet – Handlungshilfen für die betriebliche Interessenvertretung, 2006, http://www.tbs-nrw.de/cweb/cgi-bin-noauth/cache/VAL_BLOB/789/789/290/UmschlTBSBroschVoIS.pdf. [01.04.2011]

Thon, Horst: Datenschutz im Arbeitsverhältnis, in: Bauer, Jobst-Hubertus/Beckmann, Paul Werner/Lunk, Stefan/Meier, Hans-Georg/Schütte, Reinhard (Hrsg.): 25 Jahre Arbeitsgemeinschaft Arbeitsrecht im DAV, Deutscher Anwalt-Verlag, Bonn, 2006.

Thüsing, Gregor: Datenschutz im Arbeitsverhältnis – Kritische Gedanken zum neuen § 32 BDSG, Neue Zeitschrift für Arbeitsrecht 2009, S. 865-870.

Thüsing, Gregor: Arbeitnehmerdatenschutz und Compliance: Effektive Compliance im Spannungsfeld von reformiertem BDSG, Persönlichkeitsschutz und betrieblicher Mitbestimmung, Beck, München, 2010.

Tinnefeld, Marie-Theres/Petri, Thomas/Brink, Stefan: Aktuelle Fragen um ein Beschäftigtendatenschutzgesetz – Eine erste Analyse und Bewertung, MultiMedia und Recht 2010, S. 727-735.

Trappehl, Bernhards/Schmidl, Michael: Arbeitsrechtliche Konsequenzen von IT-Sicherheitsverstößen, Neue Zeitschrift für Arbeitsrecht 2009, S. 985-990.

Trittin, Wolfgang/Fischer, Esther D.: Datenschutz und Mitbestimmung – Konzernweite Personaldatenverarbeitung und die Zuständigkeit der Arbeitnehmervertretung, Neue Zeitschrift für Arbeitsrecht 2009, S. 343-346.

Uecker, Andre: Private Internet- und E-Mail-Nutzung am Arbeitsplatz – Entwurf einer Betriebsvereinbarung, Der IT-Rechts-Berater 2003, S.158-162.

Vehslage, Thorsten: Privates Surfen am Arbeitsplatz, Anwaltsblatt 2001, S. 145-149.

Vietmeyer, Katja/Byers, Philipp: Der Arbeitgeber als TK-Anbieter im Arbeitsverhältnis – Geplante BDSG-Novelle lässt Anwendbarkeit des TKG im Arbeitsverhältnis unangetastet, MultiMedia und Recht 2010, S. 807-810.

Vogel, Florian/Glas, Vera: Datenschutzrechtliche Probleme unternehmensinterner Ermittlungen, Der Betrieb 2009, S. 1747-1754.

Vogt, Volker: Compliance und Investigations – Zehn Fragen aus Sicht der arbeitsrechtlichen Praxis, Neue juristische Online Zeitschrift 2009, S. 4206-4220.

Von Steinau-Steinrück, Robert/Mosch, Ulrich (2009): Datenschutz für Arbeitnehmer – Bestandsaufnahme und Ausblick, Neue Juristische Wochenschrift-Spezial, S. 450-451.

Von Westerholt, Gräfin Margot/Döring, Wolfgang: Datenschutzrechtliche Aspekte der Radio Frequency Identification – Ein virtueller Rundgang durch den Supermarkt der Zukunft, COMPUTER UND RECHT 2004, S. 710-716.

Waltermann, Raimund: Anspruch auf private Internetnutzung durch betriebliche Übung?, Neue Zeitschrift für Arbeitsrecht 2007, S. 529-533.

Wank, Rolf, in: Dieterich, Thomas/Hanau, Peter/Schaub, Günter (Hrsg.): Erfurter Kommentar zum Arbeitsrecht, Beck, München, 2011.

Wedde, Peter, in: Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert (Hrsg.): Bundesdatenschutzgesetz: Kompaktkommentar zum BDSG, Bund-Verlag, Frankfurt a.M., 2009.

Weichert, Thilo: Datenschutz bei Suchmaschinen, MEDIEN und RECHT International 2007, S. 188-194.

Weichert, Thilo/Kilian, Wolfgang, in: Kilian, Wolfgang/Heussen, Benno (Hrsg.): Computerrechts-Handbuch: Informationstechnologie in der Rechts- und Wirtschaftspraxis, Beck, München, 2011.

Weißnicht, Elmar: Die Nutzung des Internet am Arbeitsplatz, MultiMedia und Recht 2003, S. 448-453.

Weißnicht, Elmar: IT-Risikomanagement und Online-Überwachung von Arbeitnehmern im Konzern, in: Krimphove, Dieter (Hrsg.): Reihe: Europäisches Wirtschaftsrecht, EUL Verlag, Lohmar, 2008.

Wellhöner, Astrid/Byers, Philipp: Datenschutz im Betrieb – Alltägliche Herausforderungen für den Arbeitgeber?, Betriebs-Berater 2009, S. 2310-2316.

Wiese, Günther: Videoüberwachung von Arbeitnehmern durch den Arbeitgeber und Persönlichkeitsschutz, in: Wandt, Manfred/Reiff, Peter/Looschelders, Dirk/Bayer, Walter (Hrsg.): Kontinuität und Wandel des Versicherungsrechts: Festschrift für Prof. Dr. Egon Lorenz zum 70. Geburtstag, Verlag Versicherungswirtschaft, Karlsruhe, 2004.

Wilke, Matthias: Videoüberwachung - Dürfen Arbeitgeber ihre Angestellten mit Videoanlagen beobachten?, Arbeitsrecht im Betrieb 2006, S. 31-37.

Wittern, Felix/Schuster, Fabian, in: Geppert, Martin/Piepenbrock, Hermann-Josef/Schütz, Raimund/Fabian Schuster (Hrsg.): Beck'scher TKG-Kommentar, Beck, München, 2006

Wohlgemuth, Hans H.: Datenschutz für Arbeitnehmer, Luchterhand, Neuwied, 1988.

Wohlgemuth, Hans H./Mostert, Michael: Rechtsfragen der betrieblichen Telefondatenverarbeitung, Arbeit und Recht 1986, S. 138-146.

Wolf, Thomas/Mulert, Gerrit: Die Zulässigkeit der Überwachung von E-Mail-Korrespondenz am Arbeitsplatz, Betriebs-Berater 2008, S. 442-447.

Worzalla, Michael, in: Hess, Harald/Schlochauer,Ursula/Worzalla, Michael/Glock, Dirk/Nicolai, Andrea (Hrsg.): BetrVG – Kommentar zum Betriebsverfassungsgesetz, Luchterhand, Köln, 2008.

Wybitul, Tim: Das neue Beschäftigtendatenschutzgesetz: Verschärfte Regeln für Compliance und interne Ermittlungen – Vertrauen ist gut, Kontrolle verboten?, Betriebs-Berater 2009, S. 1582-1585.

Wybitul, Tim: Bundestag: Streit um den neuen Beschäftigtendatenschutz, MultiMedia Aktuell 2011, 315091.

XING (2011), XING AG Unternehmensprofil,

https://companyprofile.xing.com/de_index.html. [01.04.2011]

Zöll, Oliver, in: Taeger, Jürgen/Gabel, Detlev (Hrsg.): Kommentar zum BDSG und den Datenschutzvorschriften des TKG und TMG, Verlag Recht und Wirtschaft, Frankfurt a.M., 2010.

Zöllner, Wolfgang: Daten- und Informationsschutz im Arbeitsverhältnis, Carl Heymanns Verlag, Köln, 1983.

Zscherpe, Kerstin A., in: Taeger, Jürgen/Gabel, Detlev (Hrsg.): Kommentar zum BDSG und den Datenschutzvorschriften des TKG und TMG, Verlag Recht und Wirtschaft, Frankfurt a.M., 2010.

Anmerkungen zu Drucksachen und Gerichtsentscheidungen

Im Bereich des Persönlichkeitsrechtsschutzes an Arbeitsplätzen gewinnen diverse Drucksachen an Bedeutung:

- BT-Drs.
  - 14/4329 [13.10.2000]
  - 14/4458 [31.10.2000]
  - 14/5793 [4.4.2001]
  - 15/2316 [9.1.2004]
  - 16/13657 [1.7.2009]
  - 17/69 [25.11.2009]
  - 535/10 [5.11.2010].
  - 17/4230 [15.12.2010]
  - 17/4853 [22.2.2011]
- BR-Drs. 535/10 (B) [5.11.2010]
- LT-Drs. Schleswig-Holstein 16/2439 [3.3.2009]

Darüber hinaus gibt es eine Vielzahl relevanter Gerichtsentscheidungen zu Fragen des Beschäftigtendatenschutzes. Die wesentlichen höchstrichterlichen Entscheidungen sind

abrufbar unter:

- http://www.bundesverfassungsgericht.de/entscheidungen.html
- http://juris.bundesarbeitsgericht.de/cgi-bin/rechtsprechung/list.py?Gericht=_bag&Art=en
- http://www.servat.unibe.ch