IT-Arbeitsrecht

Digitalisierte Unternehmen: Herausforderungen und Lösungen

Bearbeitet von
Herausgegeben von Dr. Stefan Kramer, Rechtsanwalt, Fachanwalt für Arbeitsrecht, Bearbeitet von Dr. Frank Bongers, Rechtsanwalt, Fachanwalt für Arbeitsrecht, Dr. Philipp Byers, Rechtsanwalt, Fachanwalt für Arbeitsrecht, Dr. Mario Eylert, Vorsitzender Richter am Bundesarbeitsgericht, Dr. Christian Hoppe, Rechtsanwalt, Fachanwalt für Arbeitsrecht, Dr. Judith Neu, Rechtsanwältin, Fachanwältin für Arbeitsrecht, Dr. Nathalie Oberthür, Rechtsanwältin, Fachanwältin für Arbeitsrecht, Fachanwältin für Sozialrecht, Dirk Petri, Rechtsanwalt, Fachanwalt für Strafrecht, Fachanwalt für Steuerrecht, Dr. Alexander Raif, Rechtsanwalt, Fachanwalt für Arbeitsrecht, Christian Solmecke, Rechtsanwalt, Dr. Axel Straten, Stellvertretender Direktor des Arbeitsgerichts, Richter am Arbeitsgericht, Dr. Jens Tiedemann, Richter am Arbeitsgericht, und Kathrin Wenzel, Rechtsanwältin, Fachanwältin für Arbeitsrecht

1. Auflage 2017. Buch. XXXVIII, 456 S. In Leinen
ISBN 978 3 406 70715 5
Format (B x L): 16,0 x 24,0 cm
Gewicht: 952 g

ter Berücksichtigung von Billigkeits- und Zumutbarkeitskriterien abhängt.[5] Als solche kommen etwa in Betracht:
– das potenzielle **Risiko** eines Schadenseintritts,
– die **Versicherbarkeit** dieses Risikos,
– die **Einkommenshöhe** des Arbeitnehmers,
– der **Ausbildungsgrad** des Arbeitnehmers,
– die **Leistungsfähigkeit** des Arbeitnehmers,
– das **bisherige Verhalten** des Arbeitnehmers im Betrieb sowie
– die **sozialen Verhältnisse** des Arbeitnehmers.

Bei Vorliegen **grober Fahrlässigkeit** (dh in Fällen „subjektiv schlechthin unentschuldbarer" Fehlleistung) ist auch eine **unumschränkte Haftung** des Arbeitnehmers **grundsätzlich** möglich; diese ist jedoch dann einzuschränken, wenn sein Einkommen in einem deutlichen **Missverhältnis** zum verwirklichten Schadensrisiko seiner Tätigkeit steht.[6] Ein derartiges Missverhältnis kann insbesondere dann vorliegen, wenn die Höhe des geltend gemachten Schadens **drei Bruttomonatseinkommen** des Arbeitnehmers übersteigt. **Vollumfänglich** haftet der Mitarbeiter schließlich bei **vorsätzlicher Handlung,** wobei er insoweit aber auch im Hinblick auf den tatsächlichen Eintritt eines Schadens beim Arbeitgeber zumindest mit Eventualvorsatz handeln muss, also den Schadenseintritt ernsthaft für möglich halten und ihn zugleich billigend in Kauf nehmen sowie damit abfinden muss.[7] 378

2. Anspruchsgrundlagen

Im Zusammenhang mit der IT-Nutzung durch Mitarbeiter stehen zunächst **Schäden an der betrieblichen IT selbst** (etwa in Gestalt eines Datenverlustes oder von Systemausfällen, verursacht durch *Malware* oder schlicht durch Bedienungsfehler des Mitarbeiters) im Vordergrund. Auswirkungen können sich aber aus dem Umgang mit der betrieblichen IT auch auf andere Bereiche ergeben, etwa, wenn der Arbeitgeber, der infolge eines Schadens an seiner IT kurzfristig nicht mehr in der Lage ist, seine vertraglichen Pflichten gegenüber Dritten zu erfüllen, einen gegenwärtigen oder gar künftige **Aufträge verliert** und ggf. Vertragsstrafen oder sonstigen **Regressforderungen Dritter** ausgesetzt ist. 379

Eine schuldhafte Verletzung der vertraglichen Pflichten durch den Arbeitnehmer eröffnet dem Arbeitgeber einen **vertraglichen Anspruch** auf **Schadensersatz** nach § 280 Abs. 1 BGB, sofern er das Verschulden des Mitarbeiters beweisen kann, § 619a BGB. Das AG Brandenburg[8] bejahte insoweit einen Schadensersatzanspruch in Höhe der Kosten für die Wiederherstellung gelöschter Datenbestände durch einen EDV-Fachmann, nachdem ein Mitarbeiter einer Rechtsanwaltskanzlei bewusst und unbefugt eine Rechtsanwaltsgehilfin veranlasst hatte, Textdateien aus dem IT-System der Kanzlei zu löschen. 380

In Abweichung zur allgemeinen Vorschrift des § 280 Abs. 1 S. 2 BGB, wonach das Verschulden des Anspruchsgegners vermutet wird, wenn er den Entlastungsbeweis nicht erbringen kann, ergibt sich aus § 619a BGB grundsätzlich die **volle Darlegungs- und Beweislast des Arbeitgebers** für sämtliche Voraussetzungen der Haftung des Arbeitnehmers. 381

[5] BAG 18.4.2002 – 8 AZR 348/01, NZA 2003, 37.
[6] BAG 15.11.2001 – 8 AZR 95/01, NZA 2002, 612 mwN.
[7] BAG 18.4.2002 – 8 AZR 348/01, NZA 2003, 37.
[8] AG Brandenburg 22.4.2002 – 32 C 619/99, CR 2002, 721.

382 **Praxistipp**

In Fällen **„expliziter Beweisnot"** des Arbeitgebers hat die Rechtsprechung im Einzelfall eine **abgestufte Darlegungslast** anerkannt, wonach der Arbeitnehmer auf schlüssig vorgetragene Indizien für eine Pflichtverletzung hin diese detailliert und substanziell bestreiten und den Vortrag des Arbeitgebers damit gegebenenfalls entkräften muss.[9]

383 Dieses Haftungssystem für das Arbeitsverhältnis findet sowohl im Rahmen der vertraglichen als auch der sog. **deliktischen Verantwortlichkeit** des Arbeitnehmers Anwendung, also bei Inanspruchnahme des Mitarbeiters nach den gesetzlichen Vorgaben die **Haftung aus unerlaubter Handlung,** §§ 823 ff. BGB. Hier trägt der Arbeitgeber schon nach den allgemeinen deliktsrechtlichen Regelungen die vollständige Darlegungs- und Beweislast für das Vorliegen der Haftungsvoraussetzungen.

384 Einen Schadensersatzanspruch aufgrund Eingriffs in den eingerichteten und ausgeübten Gewerbebetrieb kann der Arbeitgeber etwa bei Betriebsstörungen infolge **virenbedingter Ausfälle** der Hard- oder Software auf § 823 Abs. 1 BGB stützen.[10] Dies gilt auch bei schuldhafter **Zerstörung von Datenbeständen** (in einem durch den BGH[11] entschiedenen Fall durch den zwölfjährigen Sohn eines freien Mitarbeiters, der bei dem Versuch, ein Computerspiel auf dem seinem Vater überlassenen Firmen-PC zu installieren, Pläne für Industrieanlagen unwiederbringlich gelöscht hatte). Darüber hinaus können, je nach Lage des Einzelfalles, auch Ansprüche aus § 823 Abs. 2 BGB iVm § 303a StGB (Datenveränderung) bzw. § 274 Abs. 1 Nr. 2 StGB (Urkundenunterdrückung) in Betracht kommen.[12]

3. Übertragung der Haftungsgrundsätze auf die Mediennutzung

385 Bei der Anwendung dieser grundlegenden Prinzipien über die Haftungsverteilung im Arbeitsverhältnis auf den Umgang mit der betrieblichen IT ist zu berücksichtigen, dass schon der Bezug zur beruflichen Tätigkeit bei der Schadensentstehung nicht immer eindeutig feststellbar ist. Nicht selten gleiten Arbeitnehmers von einer ursprünglich dienstlich motivierten Nutzung bereits durch wenige „Maus-Klicks" auf private Inhalte ab und verlassen dabei unmerklich den betrieblich veranlassten und haftungsrechtlich **privilegierten Nutzungsrahmen.** Infolge dieses Abschweifens in private Sphären **entfällt** der für die Haftungsprivilegierung des Mitarbeiters erforderliche **„nahe Zusammenhang"** mit der betrieblichen Tätigkeit. Dieser fehlt bereits dann, wenn die Art und Weise der Arbeitsausführung durch die Verfolgung eigener Interessen beeinflusst wird – etwa, wenn der Mitarbeiter „bei Gelegenheit" seiner betrieblichen Tätigkeit eine Handlung vornimmt, die auch aus seiner Sicht keinerlei Bezug zur Arbeitsaufgabe hat.[13]

386 Für Arbeitgeber wiederum stellen sich angesichts der technischen Anonymität etwa der Internetnutzung Herausforderungen insbesondere im Rahmen der **Nachweisbarkeit des Verschuldens** eines konkreten Mitarbeiters; dies vor allem, wenn der Firmen-PC regelmäßig von mehreren Beschäftigten genutzt wird oder individualisierte Zugangskennungen im Betrieb bekannt sind.

387 Zu **differenzieren** ist auch und gerade in Bezug auf Haftungsfragen nach den konkreten betrieblichen Verhältnissen in Bezug auf die **Gestattung** bzw. das **Verbot** privater Nutzung.[14] Auf die Haftungsprivilegierung kann sich der Arbeitnehmer nur dann beru-

[9] BAG 2. 12. 1999 – 8 AZR 386/98, NZA 2000, 715, zur Mankohaftung einer Ladenverwalterin.
[10] *Dickmann* NZA 2003, 1009 (1113).
[11] BGH 9. 12. 2008 – VI ZR 173/07, BeckRS 2009, 05633.
[12] AG Brandenburg 22. 4. 2002 – 32 C 619/99, CR 2002, 721.
[13] BAG 21. 10. 1983 – 7 AZR 488/80, NZA 1984, 83; MHdB ArbR/*Reichold* § 51 Rn. 34.
[14] *Kramer* ArbRAktuell 2010, 164 ff.

fen, wenn ein **funktionaler Zusammenhang** mit dem Aufgabenbereich des Arbeitnehmers gegeben ist, den wiederum der Arbeitgeber selbst im Rahmen seines Weisungsrechts vorgibt.

a) Haftung bei dienstlicher Nutzung sowie bei gestatteter Privatnutzung

388 Verursacht der Mitarbeiter Schäden an der betrieblichen IT im Rahmen **dienstlicher** Nutzung, finden die skizzierten Grundsätze der Haftungsprivilegierung bei **betrieblich veranlasster Tätigkeit** ebenso Anwendung wie bei einer Schadensverursachung im Rahmen eines **gestatteten Privatnutzungsvorgangs.**[15] Während bei dienstlicher Nutzung die Betriebsbezogenheit ohnehin feststeht, gilt im Falle erlaubter Privatnutzung der Grundsatz, dass auch genuin eigenwirtschaftliche Tätigkeiten des Arbeitnehmers mit Zustimmung des Arbeitgebers zu „betrieblichen" Tätigkeiten werden können: durch die Erlaubnis der privaten Nutzung kommt es zu einer **betrieblichen Zurechnung.**[16] Erklärt der Arbeitgeber in Kenntnis des bestehenden Gefahrenpotenzials im Zusammenhang mit der IT-Nutzung sein Einverständnis mit einer Nutzung auch zu privaten Zwecken, scheidet eine Erweiterung der Haftung des Arbeitnehmers auf die Verursachung von Schäden angesichts erlaubter privater Nutzungsvorgänge schon aus Billigkeitsgründen aus.

389 Auch die Haftungsprivilegierung im Rahmen gestatteter Privatnutzung hat indes Grenzen: geht etwa ein Arbeitnehmer im Rahmen grundsätzlich gestatteter Privatnutzung **unkalkulierbare Sicherheitsrisiken** (etwa Download von Musik- oder Filmdateien aus dem Internet) ein, spricht selbst ohne ausdrückliche Nutzungsvorgabe viel für eine Überschreitung des gestatteten Rahmens und damit für eine **unumschränkte Haftung** gegenüber dem Arbeitgeber **nach den allgemeinen Regeln,** wenn im Zuge dieser Nutzungsvorgänge Schäden an den betrieblichen IT-Systemen entstehen.

b) Haftung bei Privatnutzung trotz Verbots

390 Bei unerlaubter Privatnutzung **entfällt** dagegen die Haftungsprivilegierung des Arbeitnehmers vollständig.[17] Auftretende **Schäden** sind dann **nicht** mehr Bestandteil des vom Arbeitgeber zu tragenden **Betriebsrisikos.** Für eine gesteigerte **Schutzwürdigkeit** des Mitarbeiters, die in Anbetracht des hohen Haftungsrisikos als Leitgedanke hinter der Haftungsprivilegierung steht, besteht dann keine Veranlassung mehr.

391 **Grundsätzlich** hat der Arbeitnehmer daher haftungsrechtlich in vollem Umfang für Schäden einzustehen, die er infolge eines unzulässigen privaten Nutzungsvorgangs verursacht.[18] Setzt er zB unter Verstoß gegen die betrieblichen Sicherheitsvorschriften private, virenverseuchte Datenträger im Betrieb ein und verursacht auf diese Weise einen behebungsbedürftigen Schaden am IT-System des Betriebes, so trifft ihn demnach die **volle Schadensersatzpflicht.** Selbiges gilt für Mitarbeiter, die sich aus Bequemlichkeit nicht an Sicherheitsvorschriften halten und etwa virenverseuchte Anhänge privater E-Mails öffnen oder über den Besuch von Online-Spielportalen – wenngleich ungewollt – *Malware* in das betriebliche Netzwerk einschleusen.

392 Ob im Einzelfall **Einschränkungen** in Bezug auf solche Mitarbeiter angezeigt sind, bei denen die Nutzung der betrieblichen IT nicht unmittelbar zum Berufsbild zählt oder wenn sich in der Schadensentstehung eine Sorgfaltswidrigkeit verwirklicht hat, die dem Arbeitnehmer ebenso gut bei dienstlicher Nutzung hätte unterlaufen können,[19] ist bislang ungeklärt.

---

[15] *Fischer* FA 2004, 165; *Beckschulze/Henkel* DB 2001, 1491 (1498).
[16] *Fischer* FA 2004, 165 (166).
[17] MHdB ArbR/*Reichold* § 51 Rn. 19.
[18] *Dickmann* NZA 2003, 1009 (1012f.).
[19] *Hoppe* ArbRAktuell 2010, 388 (390).

393 **Praxistipp**

Der **nahe Zusammenhang** mit dem Aufgabenbereich bzw. dem betrieblichen Wirkungskreis **fehlt** immer dann, wenn der Mitarbeiter mit der schadensstiftenden Tätigkeit ohne explizite Gestattung **eigene Interessen** verfolgt. Derartige Tätigkeiten sind dem **allgemeinen Lebensrisiko** des Arbeitnehmers zuzuordnen. Der Arbeitnehmer kann sich dann nicht darauf berufen, dass die Grundsätze über die Haftungsprivilegierung zu seinen Gunsten eingreifen.[20]

394 Der **Arbeitgeber** hat nach allgemeinen Grundsätzen darzulegen und zu **beweisen,** dass die **Schadenszufügung** im Rahmen einer verbotenen **Nutzungsweise** erfolgt ist, wenn er sich aus den haftungsrechtlichen Beschränkungen des Arbeitsrechts lösen und den Schaden uneingeschränkt bei seinem Arbeitnehmer geltend machen will. Dies wird ihn in nicht seltenen Fällen im Hinblick auf eine **drohende prozessuale Unverwertbarkeit** insbesondere datenschutz- und damit persönlichkeitsrechtswidrig erlangter **Nutzungsdaten** vor erhebliche Probleme stellen, wenn er in seinem Betrieb keine **klaren Nutzungsvorgaben** für den Umgang mit der IT-Technik aufgestellt hat. Schon aus diesem Grund ist daher die Aufstellung **präziser IT-Nutzungsregeln** (→ Rn. 203) aus Sicht des Arbeitgebers dringend zu empfehlen.[21]

c) Berücksichtigung eines Mitverschuldens des Arbeitgebers

395 Der Arbeitgeber muss sich im Einzelfall den **Einwand des Mitverschuldens** gemäß § 254 BGB entgegenhalten lassen, wenn er etwa trotz der mittlerweile allgemein bekannten Gefahr, dass bei jeder Nutzung vernetzter IT-Systeme durch Computerviren oder Hacker-Angriffe Schäden entstehen können, auf die **Installation gängiger Sicherheitssoftware** (Virenschutzprogramme, Firewalls, Mailfilter etc.) **verzichtet** hat.[22] Unterlassene Sicherheitsvorkehrungen auf Seiten des Arbeitgebers können uU auch Auswirkungen auf die Wirksamkeit arbeitsrechtlicher Maßnahmen gegenüber den betroffenen Mitarbeitern haben.[23]

396 Ein **hoher Mitverschuldensanteil** kommt insbesondere bei eigenen Versäumnissen des Arbeitgebers in Bezug auf zentrale **Organisationsobliegenheiten** in Betracht – etwa dann, wenn im Betrieb keine konkreten Weisungen existieren, die den sachgemäßen Umgang mit den IT-Systemen im Einzelnen festlegen.

397 **Praxistipp**

Mitarbeiter sollten bereits bei Begründung des Arbeitsverhältnisses darauf hingewiesen werden, dass durch sachfremde Nutzung der betrieblichen IT-Infrastruktur kaum absehbare Schäden entstehen können. Zwar mögen die mit der IT-Nutzung am Arbeitsplatz einhergehenden Risiken heute zunehmend als allgemein bekannt gelten; vielen Arbeitnehmern ist aber auch heute noch nicht das Ausmaß bewusst, in dem über den Betrieb hinaus auch unbeteiligte Dritte durch ihr Verhalten in Mitleidenschaft gezogen werden können. Zur Vorbeugung und zur Vermeidung eines möglichen Mitverschuldens sollten Arbeitgeber daher technische und rechtlich-organisatorische **Maßnahmen zur Schadensprävention** treffen, in deren Mittelpunkt die Aufklärung über drohende Gefahren steht. Dies kann etwa durch **spezielle Schulungen,** im Idealfall mit „Erfolgskontrolle", erfolgen, jedenfalls aber durch **nachvollziehbare Nutzungsvorgaben.**

[20] MHdB ArbR/*Reichold* § 51 Rn. 34.
[21] Beispiele und konkrete Vorschläge zur Ausgestaltung solcher Vorgaben finden sich bei *Kramer* ArbRAktuell 2010, 165 f.
[22] *Altenburg/Reinersdorff/Leister* MMR 2005, 135 (139).
[23] *Trappehl/Schmidl* NZA 2009, 985 (989).

Werden entsprechende organisatorische Vorkehrungen getroffen und wird die Einbeziehung der Mitarbeiter in das **Sicherheitskonzept sorgfältig dokumentiert,** erleichtert dies dem Arbeitgeber im Schadensfall im Rahmen der ihm obliegenden Beweisführung die Darstellung grob **fahrlässigen Verhaltens** des schadensverursachenden Mitarbeiters **erheblich.** 398

4. Schadensersatzanspruch des Arbeitgebers für vertragswidrig verwendete Arbeitszeit?

Von der Rechtsprechung bislang noch ungeklärt ist, ob dem Arbeitgeber im Einzelfall ein Schadensersatzanspruch gegen den Mitarbeiter vor dem Hintergrund „verschwendeter" Arbeitszeit zustehen kann. Das **LAG Köln**[24] hatte im Rahmen einer Zahlungsklage auf ausstehenden Arbeitslohn die Frage zu beurteilen, ob der Arbeitgeber mit einem Gegenspruch aus §§ 611, 280 Abs. 1 BGB auf **Schadensersatz** für die auf unerlaubte Privattelefonate und private Internetnutzung **verwendete Arbeitszeit** aufrechnen kann. Der Arbeitgeber, eine Rechtsanwaltskanzlei, hatte das letzte Monatsgehalt des endenden Arbeitsverhältnisses mit einer Rechtsanwaltsgehilfin wegen umfangreicher Privatnutzung der IT-Mittel (etwa zehn Minuten täglich über einen Zeitraum von 18 Monaten) einbehalten. Das LAG Köln hielt einen solchen Ersatzanspruch zwar für **grundsätzlich möglich,** verneinte diesen jedoch im entschiedenen Fall, da der Arbeitgeber weder eine Pflichtverletzung durch Nichterbringung der Arbeitsleistung noch einen Schaden nachzuweisen vermochte. 399

Praxistipp 400

Ein Anspruch des Arbeitgebers auf **Schadensersatz** nach §§ 611, 280 Abs. 1 BGB wegen schuldhafter Verletzung der arbeitsvertraglichen Hauptpflicht ist damit zwar **prinzipiell denkbar;** hierfür muss jedoch **im Einzelnen dargelegt** werden, zu welchem Zeitpunkt welche **Arbeit** infolge der Verwendung der Arbeitszeit zur Privatnutzung von IT-Mitteln **nicht ausgeführt** wurde und welche **Aufgaben** dem Arbeitnehmer im Einzelnen in den fraglichen Zeiträumen **aufgetragen** worden waren.

5. Zusammenfassung

Verursachen Mitarbeiter im Zusammenhang mit der Nutzung der betrieblichen IT-Infrastruktur Schäden, gelangen die Prinzipien der eingeschränkten Arbeitnehmerhaftung zur Anwendung. Wird ein Schaden im Rahmen **dienstlicher Nutzung** bzw. **erlaubter Privatnutzung** verursacht, bestehen haftungsrechtlich keine Unterschiede; in beiden Fällen besteht der für die Anwendung der **Haftungsprivilegierung** erforderliche betriebliche Bezug. Setzt sich der Arbeitnehmer hingegen bewusst **über** klare **Verbotsvorgaben hinweg,** haftet er ohne Einschränkungen nach den allgemeinen Grundsätzen. 401

Eine **Gestattung** der privaten Internetnutzung geht für Arbeitgeber also mit einer **signifikanten Beschränkung** seiner Möglichkeiten, den Arbeitnehmer auf Schadensersatz in Anspruch zu nehmen, einher; umso wichtiger ist aus Sicht des Arbeitgebers für eine spätere Beweisführung im Schadensfall die Einbeziehung der Mitarbeiter in ein betriebliches Sicherheitskonzept und dessen sorgfältige Dokumentation. 402

[24] LAG Köln 11. 2. 2005 – 4 Sa 1018/04, NZA 2006, 106.

IV. Kontrolle der IT-Nutzung

1. Rechtliche Grundlagen

403 Die Kontrolle von Art und Umfang der IT-Nutzung durch Arbeitnehmer berührt ganz unmittelbar deren individuelles **Recht auf informationelle Selbstbestimmung,** wenn sich aus ihr Rückschlüsse auf das Verhalten oder die Leistung einzelner Arbeitnehmer herleiten lassen. Sobald deshalb bei der Kontrolle der IT-Nutzung personenbezogene Daten von Arbeitnehmern erhoben werden, sind die Restriktionen des gesetzlichen Datenschutzrechts zu beachten.

404 In diesem Zusammenhang ist derzeit vor allem das **Bundesdatenschutzgesetz** (BDSG) einschlägig, für den öffentlichen Dienst der Länder ggf. die jeweiligen Datenschutzgesetze der Länder. Für die Anbieter von Telemedien- und Telekommunikationsdiensten sehen das **Telemediengesetz** (TMG) und das **Telekommunikationsgesetz** (TKG) eigene datenschutzrechtliche Vorgaben vor. Veränderungen in den derzeit bestehenden rechtlichen Grundlagen sind allerdings bereits absehbar. Bereits 2010 stand der Entwurf eines „Gesetzes zur Regelung des Beschäftigtendatenschutzes“[1] zur Diskussion, das Gesetzgebungsverfahren wurde jedoch nach der Bundestagswahl 2013 zunächst nicht weiter betrieben, da abgewartet werden sollte, ob es auf europäischer Ebene zu einer einheitlichen Regelung des Beschäftigtendatenschutzes kommen würde.[2] Dies ist entgegen ursprünglicher Erwartungen nicht der Fall. Zwar tritt am 25.5.2018 die **Europäische Datenschutz-Grundverordnung** (DS-GVO) in Kraft, die an die Stelle der Datenschutz-Richtlinie 95/46/EG treten und als unmittelbar in den Mitgliedstaaten geltende Verordnung das BDSG in weiten Teilen ersetzen wird. Die DS-GVO enthält allerdings keine eigenständigen Regelungen zum Beschäftigtendatenschutz, sondern lediglich eine **Öffnungsklausel** zugunsten mitgliedsstaatlicher Regelungen. Gemäß **Art. 88 DS-GVO** können demnach die Mitgliedstaaten

405 „durch Rechtsvorschriften oder Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, insbesondere für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, des Schutzes des Eigentums der Arbeitgeber oder der Kunden sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses vorsehen.

Diese Vorschriften umfassen angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz.“

406 Es bleibt abzuwarten, ob und in welcher Weise der Gesetzgeber von dieser Öffnungsklausel Gebrauch machen und umfassende Regelungen für einen eigenständigen Beschäftigtendatenschutz schaffen wird. Einstweilen ist zur rechtlichen Bewertung auf die allgemeinen datenschutzrechtlichen Bestimmungen zurückzugreifen.

---

[1] Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes vom 15.12.2010, BT-Drs. 17/4230.
[2] Koalitionsvertrag der Großen Koalition aus CDU, SPD und CSU vom 27.11.2013 (18. Legislaturperiode), abrufbar unter https://www.cdu.de/sites/default/files/media/dokumente/koalitionsvertrag.pdf.

2. Personenbezug der Kontrolldaten

Kontrollmaßnahmen sind rechtlich unbedenklich, wenn sie Rückschlüsse lediglich auf ein allgemeines anonymes Nutzerverhalten erlauben; erst die Erhebung und Verarbeitung personenbezogener oder personenbeziehbarer Daten berührt das Recht der Arbeitnehmer auf informationelle Selbstbestimmung. 407

Personenbezogene Daten sind nach der Definition des **§ 3 Abs. 1 BDSG** „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person". Informationen über die Nutzung von IT-Systemen besitzen deshalb immer dann Personenbezug zu einem Arbeitnehmer, wenn sie Rückschlüsse auf dessen Leistung oder Verhalten zulassen. So ist die Information, dass der Arbeitnehmer zu einer bestimmten Zeit ein Telefongespräch von bestimmter Länge geführt hat, ein personenbezogenes Datum,[3] ebenso die Aufzeichnung von Arbeitszeiten und Pausen.[4] Auch bei den in der Chronik eines Internetbrowsers erfolgenden Protokollierungen handelt es sich um personenbezogene Daten, da sie ausweisen, welche Seiten im Internet mit welchem Titel von dem Nutzer aufgerufen wurden.[5] Informationen darüber, wann, mit welchem zeitlichen Umfang und in welcher Art ein bestimmter Arbeitnehmer IT-Systeme des Arbeitgebers genutzt hat, sind deshalb personenbezogene Daten. 408

Nutzungsdaten sind nur dann nicht personenbezogen, wenn ihre Zuordnung zu einzelnen Arbeitnehmern nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. Bei Vorliegen einer dokumentierten Zuordnung bestimmter IT-Geräte zu bestimmten Arbeitnehmern ist die Person des Nutzers in aller Regel zumindest bestimmbar im Sinne von § 3 Abs. 1 BDSG.[6] Zugangsgeräte, seien es PCs, Notebooks oder Smartphones, sind regelmäßig durch individuelle Passwörter geschützt, eine Begrenzung des Zugangs ist bereits aus Gründen der Datensicherheit gemäß § 9 BDSG erforderlich. Die Kontrolle der IT-Nutzung wird deshalb in aller Regel personenbezogene Daten zum Gegenstand haben.[7] Sofern eine IT-Einrichtung demgegenüber von einer größeren Gruppe von Arbeitnehmern genutzt wird, ohne dass das Nutzerverhalten einzelnen Arbeitnehmern zugeordnet werden könnte, fehlt es an einem Personenbezug, wenn die Gruppe ausreichend groß ist.[8] **Gruppendaten** sind nur dann personenbezogen, wenn sie auf einzelne Personen „durchschlagen". 409

3. Kontrollmaßnahmen bei untersagter Privatnutzung

Datenerhebung ist gemäß § 3 Abs. 3 BDSG das **Beschaffen von Daten** über den Betroffenen. Feststellungen über Art und Inhalt der IT-Nutzung durch Arbeitnehmer unterliegen deshalb dem Anwendungsbereich des BDSG. Im Rahmen eines Beschäftigungsverhältnisses gilt dies gemäß § 32 Abs. 2 BDSG in der seit dem 1.9.2009 geltenden Fassung nicht nur für die automatisierte Datenverarbeitung iSv § 3 Abs. 2 BDSG; vielmehr ist jede erdenkliche Art der auch nicht automatisierten Erhebung, Nutzung oder Verarbeitung personenbezogener Beschäftigtendaten durch den Arbeitgeber datenschutzrechtlich zu bewerten.[9] 410

[3] BAG 13.1.1987 – 1 AZR 267/85, NZA 1987, 515.
[4] EuGH 30.5.2013 – C-342/12, NZA 2013, 723.
[5] LAG Berlin-Brandenburg 14.1.2016 – 5 Sa 657/15, BB 2016, 891.
[6] LAG Berlin-Brandenburg 14.1.2016 – 5 Sa 657/15, BB 2016, 891.
[7] Ausführlich zu den technischen Aspekten WHW Arbeitnehmerdatenschutz/*Broy* Teil B. IX Rn. 1ff.
[8] Vgl. BAG 26.7.1994 – 1 ABR 6/94, NZA 1995, 185: mindestens 6–8 Arbeitnehmer; ebenso § 12 Abs. 3 S. 2 EntgTranspG: mindestens 6 Beschäftigte.
[9] ErfK/*Franzen* BDSG § 32 Rn. 2.

a) Gesetzliches Verbot mit Erlaubnisvorbehalt

411 Gemäß § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Das BDSG postuliert damit ein gesetzliches **Verbot mit Erlaubnisvorbehalt,**[10] nach dem jeder Umgang mit personenbezogenen Daten einer Rechtfertigungsgrundlage bedarf. Liegt keine Einwilligung des Betroffenen vor, ist die Datenverarbeitung nur zulässig, wenn eine Rechtsvorschrift dies erlaubt.[11]

b) Rechtsgrundlage: Einwilligung des Arbeitnehmers

412 Der gesetzliche Datenschutz ist eine Ausprägung des verfassungsrechtlich verankerten **Rechts auf informationelle Selbstbestimmung.** Art. 2 Abs. 1 GG iVm Art. 1 Abs. 1 GG verleiht jedem Menschen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[12] In besonderer Weise schützt dieses Grundrecht vor dem Verlangen, Informationen preiszugeben, die den Betroffenen selbst belasten.[13] Jeder soll selbst entscheiden können, wann und innerhalb welcher Grenzen seine persönlichen Lebenssachverhalte offenbart werden und welche persönlichen Daten preisgegeben und verwendet werden dürfen. Dieses Recht auf informationelle Selbstbestimmung ist gewährleistet, wenn der Betroffene wirksam in die Erhebung und Nutzung seiner personenbezogenen Daten eingewilligt hat.

aa) Freiwilligkeit der Einwilligungsentscheidung

413 Gemäß **§ 4a BDSG** ist eine wirksame **Einwilligung** in datenschutzrelevante Vorgänge nur möglich, wenn diese auf der **freien Entscheidung des Betroffenen** beruht. Aufgrund der regelmäßig bestehenden strukturellen Unterlegenheit des Arbeitnehmers im Rahmen eines Arbeitsverhältnisses[14] ist lange Zeit streitig gewesen, ob die Erteilung einer datenschutzrechtlichen Einwilligung durch einen Arbeitnehmer überhaupt auf dessen freien Willen beruhen kann.[15] Dies ist höchstrichterlich mittlerweile bejaht worden, so dass von einer **grundsätzlichen Einwilligungsfähigkeit** des Arbeitnehmers auszugehen ist; auch im Rahmen eines Arbeitsverhältnisses können sich Arbeitnehmer grundsätzlich „frei entscheiden", wie sie ihr Grundrecht auf informationelle Selbstbestimmung ausüben wollen.[16] Ob die Einwilligung allerdings tatsächlich auf dem freien Willen des Arbeitnehmers beruht, ist jeweils im Einzelfall zu prüfen, wobei es konkreter Anhaltspunkte dafür bedarf, dass der Arbeitnehmer die Einwilligung im Einzelfall nicht ohne Zwang abgegeben hat.[17]

414 Auch durch eine freiwillig erteilte Einwilligung kann sich der Arbeitnehmer allerdings nicht vollständig seines Grundrechts auf informationelle Selbstbestimmung begeben.[18] Auch Kontrollmaßnahmen, die auf einer Einwilligung des betroffenen Arbeitnehmers beruhen, müssen deshalb ein angemessenes Maß an Persönlichkeitsschutz gewährleisten, so

[10] ErfK/*Franzen* BDSG § 4 Rn. 1; Tschöpe HdB ArbR/*Grimm* Teil 6 F Rn. 27.
[11] BAG 20.6.2013 – 2 AZR 546/12, NZA 2014, 143; LAG Sachsen vom 29.1.2015 – 1 Sa 407/14, ZD 2016, 90.
[12] BVerfG 15.12.1983 – 1 BvR 209/83, NJW 1984, 419.
[13] BVerfG 4.8.1998 – 1 BvR 2095/97, NZA 1998, 1329.
[14] BVerfG 23.11.2006 – 1 BvR 1909/06, NZA 2007, 85; BAG 15.4.2016, 4 AZR 796/13, NZA 2015, 1388.
[15] Bejahend zB HWK/*Lembke* Vorb. BDSG Rn. 60; Tschöpe HdB ArbR/*Grimm* Teil 6 F Rn. 44; abl. zB NK-BDSG/*Simitis* § 4a Rn. 62; *Gola/Schomerus* § 4a Rn. 7.
[16] BAG 19.2.2015 – 8 AZR 1011/13, MMR 2015, 544.
[17] VG Saarlouis 29.1.2016 – 1 K 1122/14, RDV 2016, 101; aA DKWW/*Däubler* BDSG, § 4a Rn. 23, der für den Regelfall eine Vermutung der Unfreiwilligkeit annimmt.
[18] DKWW/*Däubler* BDSG, § 4a Rn. 29.