Prof. Dr. Wolfgang Däubler

Informationsbedarf versus Persönlichkeitsschutz – was muss, was darf der Arbeitgeber wissen?

I. Einleitung

Rechtsprechung und Literatur haben sich bislang sehr stark auf das „Fragerecht“ des Arbeitgebers gegenüber Bewerbern konzentriert. Im Wesentlichen besteht hier Konsens in dem Sinne, dass der Arbeitgeber nur solche Fakten ermitteln darf, an deren Kenntnis er ein „berechtigtes, billigenswertes und schutzwürdiges Interesse“ hat.[1] Wie diese Beschränkung angesichts der Informationsmöglichkeiten im Internet faktisch durchgesetzt werden soll, ist bislang eine offene Frage.[2]

Wird ein Bewerber eingestellt, so gilt keine prinzipiell andere Regel. Der Arbeitgeber muss auch jetzt ein „berechtigtes, billigenswertes und schutzwürdiges Interesse“ an der Kenntnis bestimmter Umstände haben; andernfalls läge ein unverhältnismäßiger Eingriff in die Persönlichkeitssphäre des Arbeitnehmers vor.[3] Was sich ändert ist der Kontext, in den dieses Prinzip gestellt ist. Kraft öffentlichen Rechts muss der Arbeitgeber zahlreiche Daten erheben und sie an die Verwaltung weiterleiten oder für diese bereithalten. Auf diese Weise werden etliche Angaben offenkundig, nach denen man in der Bewerbungssituation nicht hätte fragen dürfen: Die Konfession ergibt sich aus der Lohnsteuerkarte, die Gewerkschaftsmitgliedschaft wird offenkundig, wenn der Arbeitgeber eine alte Tradition beibehalten hat, die Beiträge direkt an die Gewerkschaft abzuführen. Viel wichtiger ist aber die Tatsache, dass im Zusammenhang mit der Durchführung der Arbeit zusätzliche berechtigte Informationsinteressen entstehen: Der Arbeitgeber möchte etwa mit Hilfe einer Umfrage herausbekommen, wie die „Stimmung“ im Betrieb beschaffen ist. Manchmal wird er wissen wollen, weshalb die Fehlzeiten in einer bestimmten Abteilung besonders hoch sind oder warum bestimmte Regeln nicht beachtet, z. B. Gäste allzu großzügig bewirtet werden. Wie detailliert dürfen die Informationen sein? Darf ein Bewegungsprofil erstellt oder das

[1] ErfK-*Preis* 17. Aufl. 2017, § 611 BGB Rn. 271; HK-ArbR-*Kreuder/Matthiessen-Kreuder* 4. Aufl. 2017, §§ 611, 611a BGB Rn. 152 ff.
[2] Dazu *Kort* NZA Beilage 2/2016 S. 69; *Weichert* AuR 2010, 100, 104 f.
[3] *BAG* AP Nr. 64 zu § 123 BGB; ähnlich bereits *BAG* NZA 1996, 637.

Verhalten am Computer in allen Einzelheiten aufgezeichnet werden? Dürfen die täglichen und wöchentlichen Arbeitsergebnisse des einzelnen Beschäftigten festgehalten und dem Durchschnitt der Arbeitsgruppe und dem des Betriebes gegenüber gestellt werden? Kontrovers sind weiter die eingesetzten Mittel. Darf das Verhalten bei der Arbeit mit einer Videokamera überwacht werden? Darf jeder Gang ins Internet oder gar jedes Vertippen am Computer festgehalten werden? Inwieweit kann das Führen von Telefongesprächen kontrolliert werden? Schließlich geht es um den Einsatz von Big Data und um die Erstellung eines Abbilds aller Kommunikationsvorgänge im Betrieb, die erst in allerjüngster Zeit zum Problem geworden sind.

Datenschutzrechtlicher Beurteilungsmaßstab ist ab 25. Mai 2018 die DSGVO;[4] zum selben Zeitpunkt tritt das neue BDSG in Kraft,[5] das in § 26 einige Festlegungen zum Beschäftigtendatenschutz enthält, die über den bisherigen § 32 BDSG hinausgehen. Inwieweit auch die Telekommunikation durch die sog. ePrivacy-Verordnung eine unionsrechtliche Neuordnung erfährt, ist derzeit noch nicht absehbar.[6]

II. Unproblematische Fälle

1. Privatsphäre und Konsumverhalten

Das Privatleben des Arbeitnehmers bleibt auch nach der Einstellung für den Arbeitgeber tabu. Mit wem der Einzelne zusammenlebt und welchen Freizeitbeschäftigungen er nachgeht, ist für das Arbeitsverhältnis ohne Belang. Wird im Betrieb ein Spind zur Verfügung gestellt, in dem der Einzelne seine persönlichen Dinge aufbewahren kann, so gehört dieser zur Privatsphäre. Eine heimliche Durchsuchung durch Beauftragte des Arbeitgebers würde nach der Rechtsprechung einen schweren Eingriff in das allgemeine Persönlichkeitsrecht darstellen.[7] Privaten Charakter trägt auch das Verhalten während der Pausen und in der Kantine.[8] Welches Essen der Arbeitnehmer wählt, welche Waren er kauft und wie viel Benzin er erlaubter Weise im Betrieb tankt, hat mit dem Beschäftigungsverhältnis im Sinne des § 32

[4] Offizieller Titel: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl 2016 Nr. L 119/1 ff.
[5] Art. 1 des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) v. 30. Juni 2017, BGBl I S. 2097
[6] *Engeler/Felber* ZD 2017, 251 ff.; *Lurtz* ZD 9/2017 S. IX
[7] *BAG* NZA 2014, 143.
[8] So schon *Zöllner* Daten- und Informationsschutz im Arbeitsverhältnis, 2. Aufl. 1983, S. 42.

Abs. 1 Satz 1 BDSG (ab 25. Mai 2018: § 26 Abs. 1 Satz 1 BDSG-neu) nichts zu tun. Erfasst der Arbeitgeber – ähnlich wie ein Unternehmen im Verhältnis zu seinen Kunden – zu Abrechnungszwecken Daten, sind diese als „verbraucherbezogen" streng von den arbeitsbezogenen zu trennen.[9] Soweit technisch machbar, ist es allerdings vorzuziehen, auf Karten ohne personenbezogene Daten umzustellen, die der Einzelne nach seinen Bedürfnissen an einem Automaten mit bestimmten Beträgen aufladen kann – dies würde dem Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO entsprechen, der durch Art. 25 Abs. 1 DSGVO („privacy by design") konkretisiert wird. Danach ist die Technik so zu gestalten, dass möglichst wenige Daten anfallen. Auch hat der Arbeitgeber nach § 26 Abs. 5 BDSG-neu „geeignete Maßnahmen" zu ergreifen, um sicherzustellen, dass insbesondere die in Art. 5 niedergelegten Grundsätze eingehalten werden.

2. Arbeitszeit und Arbeitsverhalten

Der Arbeitgeber ist nach § 26 Abs. 1 Satz 1 BDSG n. F. berechtigt, die mit dem Beschäftigten vereinbarte Dauer und Lage der Arbeitszeit („Soll-Arbeitszeit") sowie die tatsächlichen Anwesenheitszeiten im Betrieb („Ist-Arbeitszeit") zu speichern. Auch die Abwesenheitsgründe sind einzubeziehen, da andernfalls Fehlschlüsse naheliegen. Die „Datentransparenz" nach Art. 5 Abs. 1 lit. a DSGVO ist nicht gesichert, solange unklar bleibt, ob die Abwesenheit auf Krankheit, auf einer Weiterbildungsmaßnahme oder auf Urlaub beruhte. Zahlreiche Daten können durch die Arbeit selbst anfallen; relativ aktuelles Beispiel sind Kooperationsplattformen („Sharepoint"), bei denen u. a. für alle Beteiligten sichtbar wird, in welchem Zustand sich andere Nutzer gerade befinden („bin zur Toilette", „schreibe am Projektbericht").[10] Festzuhalten ist auch das Erreichen bestimmter Ergebnisse bei Zielvereinbarungen, ebenso Beurteilungen durch Vorgesetzte, die in der Regel Bedeutung für den weiteren Verlauf des Arbeitsverhältnisses haben.[11]

3. Entgeltabrechnung

Bei der Entgeltabrechnung ist eine Reihe von persönlichen Merkmalen wie z. B. die Konfession von Bedeutung, nach denen in der Einstellungssituation nicht gefragt werden darf. Ihre Berücksichtigung ist nunmehr unproblematisch, soweit sie für die Entgeltzahlung und

[9] Dazu *Däubler* Gläserne Belegschaften, 7. Aufl. 2017, Rn. 394 ff.
[10] *Maas/Schmitz/Wedde* Datenschutz 2014. Probleme und Lösungsmöglichkeiten, 2014, S. 36 f.
[11] Vgl. *Gola/Pötters/Wronka* Handbuch Arbeitnehmerdatenschutz, 7. Aufl. 2016, Rn. 148.

damit für die Durchführung des Arbeitsverhältnisses erforderlich ist. Dasselbe gilt für Familienstand und Kinderzahl.[12] Auch Gehaltspfändungen werden offenbar; ob sie zu erwarten sind, kann nunmehr erfragt werden.[13] Nach der Schwerbehinderung darf jedenfalls dann gefragt werden, wenn das Arbeitsverhältnis sechs Monate gedauert hat und damit der Sonderkündigungsschutz nach §§ 168 ff. SGB IX n. F. (bisher: §§ 85 ff. SGB IX) erreicht ist.[14]

4. Weiterförderung

Arbeitnehmerdaten werden auch in völlig anderem Zusammenhang erhoben: Will der Arbeitgeber eine sog. Potenzialanalyse in Bezug auf einzelne Beschäftigte vornehmen, so ist dies nur mit deren Einwilligung möglich.[15] Diese begegnet – da für den Arbeitnehmer nützlich - keinen inhaltlichen Bedenken.[16] Ähnliches gilt für die Aufnahme in eine sog. Weiterförderungsdatei.

III. Umfragen und Ermittlungen von Regelverletzungen

1. Umfragen

Keine datenschutzrechtlichen Probleme wirft eine Umfrage zur Arbeitszufriedenheit, zum Verhalten der Vorgesetzten, zur Darstellung der Firma in der Öffentlichkeit und zu vergleichbaren Themen auf, wenn die Stellungnahme des Einzelnen anonym bleibt, da in einem solchen Fall keine personenbezogenen Daten entstehen.[17] Die Situation ändert sich, wenn die abgegebene Stellungnahme dem einzelnen Beschäftigten zugerechnet werden kann. Steht ihm die Teilnahme frei und muss er keinerlei Nachteile befürchten, wenn er sich nicht beteiligt, so wird man seine Einwilligung als freiwillig und damit als ausreichende Legitimation für die Speicherung und Weiterverarbeitung der Daten ansehen können.[18]

---

[12] DKKW-*Klebe* 15. Aufl. 2016, § 94 Rn. 20; *Fitting* 28. Aufl. 2016, § 94 Rn. 20, jeweils m.w.N.
[13] DKKW-*Klebe* § 94 Rn. 19; *Fitting*, § 94 Rn. 21.
[14] *BAG* NZA 2012, 555
[15] *Schleswig-Holsteinischer DSB* 12. TB, unter 4.10.2.
[16] Zu den inhaltlichen Wirksamkeitsvoraussetzungen für Einwilligungen s. *Däubler* (Fn. 9) Rn. 135 ff.
[17] *Gola* ZD 2013, 379, 380
[18] *BAG* NZA 2015, 604; *Däubler* (Fn. 9), Rn. 160.

Sehr viel problematischer ist eine Weisung kraft Direktionsrechts, wonach der einzelne Arbeitnehmer an einer nicht-anonymen Umfrage teilnehmen muss. In vielen Fällen würde § 26 Abs. 1 Satz 1 BDSG n. F. keine ausreichende Rechtsgrundlage darstellen, weil eine solche Umfrage für die Durchführung des Beschäftigungsverhältnisses nicht »erforderlich« ist,[19] weil dasselbe Ziel auch mit anonymen Daten erreicht werden könnte. Ist dies nicht der Fall, weil beispielsweise ermittelt werden soll, wie die konkreten Arbeitsabläufe verbessert werden können, so muss der Arbeitgeber sicherstellen, dass dem Einzelnen keine Nachteile entstehen. Dies geschieht am besten dadurch, dass eine Drittfirma mit der Befragung beauftragt und im Vertrag mit ihr festgeschrieben wird, dass der Arbeitgeber keine personenbezogenen oder personenbeziehbaren Daten erfahren darf.[20] Damit wäre »informationelle Gewaltenteilung« realisiert. Für eine solche Lösung spricht zudem eine praktische Erwägung: Ohne eine solche Abschirmung wäre der Wert der Befragung erheblich gemindert, weil sich viele scheuen würden, offen auf Missstände oder auf Fehlverhalten von Führungskräften hinzuweisen.

2. Ermittlung von Regelverstößen

Besteht die nicht ganz fern liegende Möglichkeit, dass es im Unternehmen zu Gesetzesverstößen oder sonstigen Regelwidrigkeiten kommen kann oder bereits gekommen ist, so liegt ein „Compliance-Problem“ vor. Die einfachste Form, „Schwachstellen“ zu identifizieren oder Verstöße aufzudecken, ist die persönliche Befragung der Beteiligten.

Der einzelne Beschäftigte ist nach § 241 Abs. 2 BGB grundsätzlich verpflichtet, auf die Arbeit bezogene Fragen seines Vorgesetzten oder anderer zuständiger Stellen im Betrieb wahrheitsgemäß zu beantworten.[21] Eine solche Form der Datenerhebung wird in aller Regel für die Durchführung des Arbeitsverhältnisses erforderlich sein. Zu denken ist etwa an das Verhalten von Konkurrenten auf einem Auslandsmarkt (»Stehen sie im Ruf, inoffizielle Zahlungen zu gewähren oder anzunehmen?«). Rechtsprobleme ergeben sich lediglich, wenn sich der Beschäftigte selbst belasten müsste, weil eine Pflichtverletzung oder gar eine strafbare Handlung zu Tage treten würde.

[19] *Gola* ZD 2013, 379, 380.
[20] *Gola* ZD 2013, 379, 381.
[21] Für eine analoge Anwendung des § 666 BGB besteht mangels Lücke kein Anlass.

Im Strafprozess ist Angeklagte nicht verpflichtet, sich durch seine Aussage selbst zu belasten. Dieser sog. Nemo-tenetur-Grundsatz gilt auch für Zeugen, die in einem solchen Fall nach § 55 StPO die Aussage verweigern können.[22] Eine Übertragung dieses Grundsatzes in das Arbeitsrecht wird nur sporadisch erörtert; die vorhandenen Stimmen kommen zu recht unterschiedlichen Ergebnissen.[23] Ohne auf strafprozessuale Grundsätze Bezug zu nehmen, hat das BAG den Standpunkt vertreten, der Arbeitnehmer müsse sich weder selbst belasten noch dem Arbeitgeber Tatsachenmaterial liefern, um dessen Kündigung „schlüssig" zu machen. Durch eine unterlassene Mitwirkung verletze er keine arbeitsvertragliche Nebenpflicht.[24] Dem ist zuzustimmen. Das Recht, sich nicht selbst belasten zu müssen, muss auch im Arbeitsrecht gelten: Die Abhängigkeit ist im Prinzip keine geringere als im Verhältnis des Bürgers zum Staat, zumal staatliche Behörden an das Rechtsstaatsprinzip gebunden sind, was für den Arbeitgeber jedenfalls nicht in gleicher Weise gilt. Hinzu kommt, dass die arbeitsrechtliche Sanktion des Arbeitsplatzverlustes sehr viel stärker ins Gewicht fallen kann als viele strafgerichtliche Verurteilungen. Eine unbeschränkte Auskunftspflicht würde zudem dazu führen, dass die strafprozessualen Vorschriften durch die Offenlegung im Arbeitsverhältnis leicht zu umgehen wären: Niemand könnte den Arbeitgeber daran hindern, im Anschluss an die Aussage des Beschäftigten eine Strafanzeige zu erstatten.

Droht dem Arbeitgeber ein Schaden, der noch verhindert werden kann, so muss der Arbeitnehmer im Rahmen seiner Möglichkeiten den Schaden abwenden; in der Regel wird er die zuständige innerbetriebliche Stelle informieren bzw. im Rahmen einer Befragung einen entsprechenden Hinweis geben. Geht die Gefahr von einem Arbeitskollegen aus oder hat dieser bereits eine Pflichtverletzung begangen, so stellt sich das Problem, ob man diesen durch eine Anzeige „ans Messer liefern" muss. Dies zu tun, könnte den Arbeitnehmer selbst nicht nur moralisch, sondern auch rechtlich in Schwierigkeiten bringen: Die Denunziation von Arbeitskollegen kann nach der Rechtsprechung des BAG eine verhaltensbedingte Kündigung rechtfertigen.[25] Eine Mitteilungspflicht anzunehmen, würde weiter bedeuten, dass im Prinzip jeder den andern überwachen müsste und so ein System des Misstrauens und der

[22] Dazu eingehend *Franck* RDV 2013, 287ff.

[23] Für eine entsprechende Anwendung strafprozessualer Grundsätze *Dann/Schmidt* NJW 2009, 1851ff.; (wohl auch) *Mengel/Ullrich* NZA 2006, 240, 243; differenzierend *Göpfert/Merten/Siegrist* NJW 2008, 1703, 1705; *Wisskirchen/Glaser* DB 2011, 1448 linke Spalte (soweit nicht der eigene Arbeitsbereich betroffen, in Bezug auf den volle Wahrheitspflicht bestehen soll); dagegen *Böhm* Non-Compliance und Arbeitsrecht, 2011, S. 157 ff., der den Arbeitnehmer zu voller Offenlegung verpflichten will, aber ein strafprozessuales Verwertungsverbot des »Geständnisses« annimmt.

[24] *BAG* DB 2009, 1544 = NZA-RR 2009, 362.

[25] *BAG* AP Nr. 5 zu § 1 KSchG Verhaltensbedingte Kündigung

gegenseitigen Bespitzelung entstehen könnte.[26] Eine Ausnahme besteht nur dann, wenn schwere Straftaten drohen, deren Nichtanzeige nach § 138 BGB strafbar ist.[27]

IV. Das Problem der eingesetzten Mittel

Kontroverser als der Informationsbedarf des Arbeitgebers sind häufig die Mittel, die aus diesem Anlass eingesetzt werden können. Zu denken ist dabei insbesondere an die Videokontrolle, aber auch an den Einsatz von Privatdetektiven, an die Erstellung von Bewegungsprofilen sowie an den Einsatz von RFID-Technik und von spezifischen Überwachungsprogrammen.

1. Videokontrolle

Der Einsatz von Videokameras breitet sich nicht nur auf öffentlichen Plätzen, sondern auch in Betrieben aus. Als symptomatisch mag man es ansehen, dass in einem größeren Hannoveraner Modegeschäft insgesamt 128 Videokameras installiert waren, bevor es dem neu gegründeten Betriebsrat gelang, ihre Zahl im Wege der Mitbestimmung auf 67 zu reduzieren.[28] Eine solche Observationstechnik besitzt auch nach Meinung des Gesetzgebers eine „besondere Eingriffsqualität“[29], die bei heimlicher Vorgehensweise noch erheblich gesteigert wird.[30] Der Betroffene wird in seinen Verhaltensweisen einschließlich seiner Bewegungen und seiner jeweiligen Stimmungen weitestgehend erfasst. Die Negativ-Utopie von George Orwell (»Big Brother«) ging nicht ganz zu Unrecht von dem allgegenwärtigen Auge des Großen Bruders aus. Je weiter der Radius dieses Mittels reicht und je mehr die dadurch erfassten Daten verknüpft werden können, umso mehr ist das unbeeinflusste Verhalten des Einzelnen und damit der Lebensnerv einer freien Gesellschaft getroffen.[31] Im Fall Lidl spielten verdeckte Kameras eine zentrale Rolle, doch gab es auch eine Reihe anderer derartiger »Überwachungsskandale«.[32] Entgegen dem Anspruch des BVerfG[33] und dem

[26] So ausdrücklich *ArbG Stuttgart* DB 1982, 1626.
[27] Für Mitbestimmung des Betriebsrats über die Pflicht, Compliance-Verstöße über eine Hotline zu melden, *LAG Düsseldorf DB 2006, 162 = dbr 4/2006* mit Anm. *Däubler.* Aus der Praxis des Compliance Officers bei der Allianz SE berichtet *Mert* CuA 1/2016 S. 18 ff.
[28] Näher *Däubler* CuA 2/2016 S. 29 ff.
[29] So der Bericht des Innenausschusses, BT-Dr. 14/5793 S. 61.
[30] *LAG Hamm* ZD 2014, 204.
[31] *Bäumler* RDV 2001, 67f.
[32] Überblick bei *Däubler* (Fn. 9), Rn 2a ff.
[33] BVerfGE 65, 1, 43.

Transparenzgebot des Art. 5 Abs. 1 lit. a DSGVO wird für den Einzelnen völlig unklar, wer was und bei welcher Gelegenheit über ihn weiß.[34]

a) Öffentlich zugängliche Räume

Befindet sich der Arbeitsplatz in einem öffentlich zugänglichen Raum (z. B. Laden, Tankstelle, Bankfiliale), so gilt bis 25. Mai 2018 die Spezialvorschrift des § 6b BDSG a. F., die danach durch den weitgehend übereinstimmenden § 4 BDSG n. F. abgelöst wird. Nach beiden Vorschriften ist die Beobachtung durch Videokameras insbesondere dann zulässig, wenn sie zur Wahrnehmung berechtigter Interessen für „konkret festgelegte Zwecke" erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.[35] Inhaltlich geht es meist darum, die Begehung von Diebstählen und anderen strafbaren Handlungen zu vermeiden. Dieser Zweck muss bereits vor dem Einsatz der Anlage konkretisiert (aus welchen Gründen drohen welche Delikte?) und auch dokumentiert sein; andernfalls könnte die Rechtmäßigkeit des Videoeinsatzes nicht überprüft werden.[36]

Trotz Vorliegens derartiger Gründe können schutzwürdige Interessen der Betroffenen überwiegen. So kann etwa der Zweck, strafbare Handlungen zu verhindern, nicht die Überwachung von Toiletten und Umkleideräumen rechtfertigen.[37] Die schutzwürdigen Interessen der betroffenen Personen gebieten es weiter, die überwachten Bereiche auf das Notwendige zu beschränken. So muss etwa den Arbeitnehmern, die in öffentlich zugänglichen Räumen als Verkäufer, Bankangestellte, Museumswärter usw. beschäftigt sind, die Möglichkeit bleiben, sich der Videokontrolle zumindest in den Pausen durch Rückzug in einen nicht überwachten Raum zu entziehen.[38] Der Eingriff in das allgemeine Persönlichkeitsrecht ist dann besonders gravierend, wenn die Überwachung kontinuierlich

[34] *Bäumler* RDV 2001, 69; zu Art. 5 Abs. 1 lit. a DSGVO s. insbesondere Kühling/Buchner-*Herbst* Datenschutz-Grundverordnung, 2017, Art. 5 Rn. 18 ff.; Paal/Pauly-*Frenzel* Datenschutz-Grundverordnung, 2017, Art. 5 Rn. 21 f.

[35] Daneben gibt es die hier nicht weiter interessierenden Gründe der „Aufgabenerfüllung öffentlicher Stellen" und der „Wahrnehmung des Hausrechts".

[36] Hamburger DuD-Kommentierung zum BDSG, DuD 2002, 28; Simitis-*Scholz*, BDSG, 8. Aufl. 2014, § 6b Rn 84 (zum bisherigen Recht). Ab 25. Mai 2018 ergibt sich die Dokumentationspflicht aus Art. 5 Abs. 2 DSGVO.

[37] BT-Dr. 14/5793, S. 62; *Vahle* DSB Heft 2/2002, S. 17; Taeger/Gabel-*Zscherpe* BDSG, 2. Aufl. 2013, § 6b Rn. 58.

[38] Weitergehend mit Recht die Bremer Landesbeauftragte für den Datenschutz, wonach die Kameraeinstellung die Überwachung von Beschäftigten generell ausschließen muss – berichtet bei *Köppen* CuA 5/2012, S. 36.

erfolgt und der Einzelne ihr nicht ausweichen kann.[39] Dies bedeutet, dass ohne eine solche Maßnahme gravierende Nachteile drohen, die durch eine Stichprobenkontrolle nicht verhindert werden können. Generell reicht die generelle Gefahr einer Begehung von Straftaten nicht aus. Vielmehr muss entweder ein konkreter Verdacht gegen eine bestimmte Person bestehen oder es müssen entsprechende Vorfälle bereits eingetreten sein. Fehlt es an beidem, überwiegen die schutzwürdigen Interessen der Betroffenen gegenüber dem Sicherheitsbedürfnis des Betreibers.[40]

Die Anwendung des § 4 Abs. 1 und 2 BDSG n. F. hängt nicht davon ab, dass die Videokamera Aufzeichnungen vornimmt; es genügt, wenn sie lediglich Bilder auf einen Monitor überträgt.[41] Dies ergibt sich aus § 4 Abs. 3 BDSG n. F., der die Speicherung und Verwendung der Daten gesondert regelt und dabei auf die Erforderlichkeit für den verfolgten Zweck und das Fehlen überwiegender schutzwürdiger Belange der betroffenen Personen abstellt. Hätte der Gesetzgeber anders entschieden und nur Filmaufnahmen einbezogen, hätte die Vorschrift einen erheblichen Teil ihres Anwendungsbereichs verloren. Da der Einzelne überdies nicht kontrollieren kann, ob die von der Kamera erfassten Vorgänge effektiv festgehalten werden oder nicht, wären in weitem Umfang Umgehungsmöglichkeiten eröffnet. Auch eine bloße Kameraattrappe ist daher einer realen Kamera gleichzustellen.[42] Die Auffassung des LAG Mecklenburg-Vorpommern,[43] in einem solchen Fall bestehe „offensichtlich“ kein Mitbestimmungsrecht, ist nur dann vertretbar, wenn allen Arbeitnehmern bekannt ist, dass es sich nicht um eine wirkliche Kamera handelt.[44] In allen andern Fällen entsteht ein effektiver »Überwachungsdruck«, was die Anwendung des § 4 Abs. 1 BDSG n. F. und des Mitbestimmungsrechts rechtfertigt.[45]

[39] Zu dem Beispiel einer flächendeckenden Überwachung einer Ausbildungsstätte, um Diebstähle und Vandalismus zu bekämpfen, s. (ablehnend) die Stellungnahme des Landesbeauftragten für den Datenschutz NRW, mitgeteilt bei *Köppen* CuA 10/2013 S. 29.

[40] *Däubler* NZA 2001, 878. Vgl. auch Simitis-*Scholz* (Fn. 36), § 6b Rn. 97.

[41] Hamburger DuD-Kommentierung zum BDSG, DuD 2002, 27; Simitis-*Scholz* (Fn. 36), § 6b Rn 65 unter Bezugnahme auf die amtliche Begründung, BT-Drucksache 14/4329, S. 38; Däubler/Klebe/Wedde/Weichert-*Wedde*, BDSG, 5. Aufl. 2016, § 6b Rn. 13; a.A. *Gola/Schomerus*, BDSG, 11. Aufl. 2012, § 6b Rn. 10; *Königshofen* RDV 2001, 222 (alle zum bisherigen Recht).

[42] *LG Berlin* ZD 2016, 189.

[43] ZD 2015, 185 = NZA-RR 2015, 196

[44] Ebenso *Kort* ZD 2016, 3, 5

[45] Ebenso *LG Berlin* ZD 2016, 189; deshalb griff dann auch § 6b BDSG a. F. ein: *Gola/Pötters/Wronka* (Fn. 11), Rn 1171; Simitis-*Bizer* 6. Aufl., § 6b Rn 39; Däubler/Klebe/Wedde/Weichert-*Wedde* § 6b Rn. 18 und muss nunmehr § 4 BDSG n. F. eingreifen; anders Simitis-*Scholz* 8. Aufl., § 6b Rn. 112.

b) Nicht öffentlich zugängliche Räume

Bei nicht öffentlich zugänglichen Räumen kann § 4 BDSG n. F. keine Anwendung finden.[46] Gegenüber Beschäftigten greift § 26 Abs. 1 BDSG n. F. ein;[47] im Verhältnis zu anwesenden Dritten (etwa geschäftliche Besucher) kann Art. 6 Abs. 1 Buchst. f DSGVO Rechtsgrundlage sein.[48] § 4 erlaubt aber immerhin den Rückschluss, dass angesichts der von vorne herein gegebenen Überschaubarkeit des anwesenden Personenkreises die Zulässigkeitsvoraussetzungen eher restriktiver zu bestimmen sind. Dem tragen Rechtsprechung und Lehre durchaus Rechnung.

Nach der Rechtsprechung ist die Beobachtung durch eine versteckte Kamera, deren Existenz den betroffenen Arbeitnehmern nicht bekannt ist, als übermäßiger Eingriff in das allgemeine Persönlichkeitsrecht grundsätzlich unzulässig.[49] Auch eine offen eingesetzte, aber ausschließlich der Kontrolle des Arbeitsverhaltens dienende Videotechnik wird mit Recht als Verstoß gegen die Menschenwürde und damit als unzulässig gewertet.[50] Anders ist die Situation dann, wenn ein überwiegendes schutzwürdiges Interesse des Arbeitgebers für eine Überwachung spricht, weil sich beispielsweise erhebliche Warenverluste nur auf diese Weise aufklären lassen.[51] Dies hat das BAG unter Rückgriff auf § 32 Abs. 1 Satz 2 BDSG a. F. durch Beschluss vom 26.8.2008[52] in der Weise konkretisiert, die Videokontrolle sei nur in Bezug auf solche Arbeitnehmer zulässig, gegen die ein konkreter, auf Tatsachen gestützter Verdacht einer strafbaren Handlung bestehe.[53] Richtet sich der Verdacht gegen ein Gruppenmitglied, so kann vorübergehend die gesamte Gruppe observiert werden, sofern es sich nicht nur um den Verdacht einer relativ geringfügigen Verfehlung handelt.[54] Kommen Gegenstände abhanden, ohne dass sich ein konkreter Verdacht gegen bestimmte Personen

---

[46] *BAG* 29.6.2004 – 1 ABR 21/03, NZA 2004, 1278, 1282; zustimmend *Pötters/Traut* RDV 2013, 132 (für § 6b BDSG a. F.).
[47] Ebenso *Pötters/Traut* RDV 2013, 133 für § 32 BDSG a. F. Für einen weiteren Anwendungsbereich spricht demgegenüber BGH, RDV 2013, 303, der die Vorschrift auf die Einrichtung einer Videoanlage überträgt, die von einer Wohnungseigentümergemeinschaft mit Mehrheit beschlossen wurde.
[48] Das gilt auch für Einbrecher, die durch die Videoanlage beobachtet werden; ihre Persönlichkeitsinteressen müssen immer zurücktreten, soweit es um die Aufklärung ihrer Straftat geht. S. den Fall *AG Köln*, ZD 2016, 383
[49] *LAG Köln* BB 1997, 476; *LAG Baden-Württemberg* BB 1999, 1439; DKKW-*Berg* § 75 Rn. 120; *Schierbaum*, CF 6/2002, S. 28; im Ergebnis übereinstimmend *Pötters/Traut* (RDV 2013, 136), wonach es in diesen Fällen in der Regel an der Erforderlichkeit fehlt, weil durch Kontrolle der Arbeitsergebnisse ein den Arbeitnehmer weniger belastender Weg zur Verfügung steht.
[50] *BAG* NZA 2003, 1193; Fitting (Fn. 12), § 75 Rn. 149. Es geht also nicht nur um die individuelle Meinung des Verfassers, wie *Pötters/Traut* (RDV 2013, 132, 138 Fn. 73) behaupten.
[51] *BAG*, NZA 1988, 92.
[52] NZA 2008, 1187
[53] *BAG* NZA 2008, 1187, 1191 Tz. 31, bestätigt durch *BAG* ZD 2012, 558 = NJW 2012, 3594; dazu *Däubler* CuA 11/2012 S. 30.
[54] Vgl. *BAG* NZA 2012, 1025

ergibt, so kann nicht die ganze Belegschaft unter Beobachtung gestellt werden; vielmehr ist auf die Torkontrolle als milderes Mittel zurückzugreifen.[55] Geht es nicht um eine Straftat, sondern um den gleichfalls auf Tatsachen gestützten Verdacht einer schweren Verletzung arbeitsvertraglicher Pflichten, so ist ein entsprechendes Vorgehen auf der Grundlage des § 32 Abs. 1 Satz 1 BDSG a. F. (= § 26 Abs. 1 Satz 1 BDSG n. F.) möglich.[56]

2. Einsatz von Privatdetektiven

Wird ein Privatdetektiv eingesetzt, so werden die Beobachteten in der Regel bewusst im Unklaren gelassen, dass eine Kontrollmaßnahme stattfindet. Dadurch tritt ein ganz ähnlicher Effekt wie bei einer verdeckten Kamera ein. Ein vergleichbares Phänomen kennt man im Strafprozessrecht, wo man von „verdeckten Ermittlern“ spricht. Ihr Einsatz ist nach § 110a StPO nur bei organisierter Kriminalität zulässig, bei der es insbesondere um terroristische Anschläge, um unerlaubten Drogen- und Waffenhandel sowie um Falschgeldproduktion geht. Will man nicht in Kauf nehmen, dass sich die Rechtsordnung mit sich selbst in Widerspruch setzt, so kann der Einsatz „getarnter“ Personen auch im Betrieb nur zur Aufklärung schwerster Delikte erfolgen; bei irgendwelchen Diebstählen oder gar bei bloßen arbeitsvertraglichen Pflichtverletzungen muss sie als unzulässig behandelt werden. Einen vergleichbaren Fall hatte vor Jahren der VGH Baden-Württemberg[57] zu entscheiden. Der Arbeitgeber hatte die Identität eines anonymen Briefeschreibers dadurch aufgedeckt, dass er die Speichelreste auf dem Briefumschlag analysieren und mit jenen vergleichen ließ, die der Verdächtige bei einer Betriebsfeier auf seiner Kaffeetasse und seinem Weinglas hinterlassen hatte. Das Gericht begründete die Unzulässigkeit dieses Vorgehens u a. damit, dieses sei der öffentlichen Hand vorbehalten, die rechtsstaatliche Prinzipien beachten müsse. Weiter sei der Arbeitnehmer keiner „schweren Straftat“ verdächtig gewesen. Das BAG hat sich mit diesen Argumenten bisher nicht auseinander gesetzt, sondern die Zulässigkeit des Einsatzes von Privatdetektiven dahinstehen lassen.[58] Besteht der Verdacht, der Arbeitnehmer schütze eine Erkrankung nur vor, so steht in Form der Einschaltung des Medizinischen Dienstes der Gesetzlichen Krankenkassen nach § 275 Abs. 1 Nr. 3 lit. b und Abs. 1a SGB V ein kostengünstigeres und weniger belastendes Verfahren zur Verfügung.[59] Beobachtet ein Vorgesetzter zufällig in seiner Freizeit einen krank geschriebenen Mitarbeiter, wie er seinen

[55] *BAG*, NZA 2013, 1433
[56] *BAG* 27.7.2017 – 2 AZR 681/16
[57] AuR 2001, 469
[58] *BAG*, AP Nr. 21 zu § 87 BetrVG 1972 Überwachung
[59] *BAG*, NZA 2009, 1300, 1302

Pkw in der Autowaschanlage reinigt, so kann er dies nach Auffassung des LAG Rheinland-Pfalz[60] mit seinem Fotohandy im Bild festhalten.

3. Bewegungsprofile mit Hilfe von GPS

Von Interesse ist es weiter zu wissen, wer sich zu welchem Zeitpunkt an welchem Ort aufhält. Dies gilt insbesondere für Außendienstmitarbeiter und Fahrer, die ggf. umdirigiert werden können, um einen eben eingegangenen Auftrag zu erledigen. Technisch lässt sich dies unschwer mit Hilfe von GPS und Handy-Ortung bewerkstelligen. Der Preis, den die Beschäftigten dafür zu zahlen haben, ist nicht unerheblich: Vom Effekt her ist die Überwachung des Aufenthaltsorts ähnlich belastend wie die Beobachtung durch eine Videokamera: Jede Pause, jedes Parken am Straßenrand, jeder kurze Besuch in einem Laden wird erfasst und kann Anlass für eine Rückfrage sein. Die relative Autonomie eines Außendienstmitarbeiters geht verloren.

Aufgrund der bisherigen technischen Möglichkeiten bestand wenig Anlass, außer dem gesprochenen und dem geschriebenen Wort und der äußeren Erscheinungsform der Person auch den Aufenthaltsort vor unbefugter Erfassung zu schützen. Ähnlich wie beim verdeckten Ermittler haben sich lediglich im Strafverfahrensrecht gesetzliche Regeln entwickelt. Nach Auffassung des BGH stellt die Aufenthaltsbestimmung zwar einen sehr weitgehenden Eingriff in die Persönlichkeitssphäre dar, doch ist er gerechtfertigt, wenn es um die Aufklärung von Sprengstoffanschlägen und damit von besonders schweren Delikten geht.[61] Das Interesse eines Arbeitgebers an umfassender Kontrolle des Arbeitsverhaltens und an einem erfolgreichen „Flottenmanagement“ ist damit in keiner Weise vergleichbar. Doch davon ganz abgesehen: Derartige Eingriffe in die Persönlichkeitssphäre sind gar nicht erforderlich, weil der Arbeitgeber seine Mitarbeiter verpflichten kann, während der Fahrt auf Handy erreichbar zu sein. Durch ein kurzes Gespräch kann er dann den Standort erfragen und ggf. die Route neu bestimmen, weil es noch Zusätzliches zu erledigen gibt.

Detektive oder andere Personen, die heimlich an Lkws GPS-Sensoren anbringen, um auf diese Weise ein Bewegungsprofil der Fahrer zu erstellen, machen sich strafbar. Der BGH[62] hat eine Verurteilung gemäß § 44 BDSG a. F. bestätigt; nach neuem Recht wäre wegen

[60] RDV 2014, 44
[61] *BGH*, NJW 2001, 1658.
[62] RDV 2013, 297 = ZD 2013, 502 = K&R 2013, 669.

unerlaubter Datenerhebung zumindest ein erhebliches Bußgeld nach Art. 83 DSGVO fällig. In einem Zivilprozess wurde festgestellt, dass die heimliche Überwachung mit Hilfe von GPS einen übermäßigen Eingriff in das Persönlichkeitsrecht der beobachteten Person darstelle und deshalb nicht zu den erstattungsfähigen vorprozessualen Kosten gehöre.[63]

4. RFID

RFID (=Radio Frequency Identification) ist derzeit auf dem Vormarsch. Die Technik besteht aus zwei Komponenten. Auf einer Ware (oder auf der gekauften Kleidung eines Menschen) ist ein »tag«, ein sog. Transponder angebracht. Er enthält einen Microchip, der bestimmte Daten gespeichert hat und sie bei Annäherung an ein Lesegerät (die zweite Komponente) an dieses übermittelt.[64] Anders als bei einem bar-code ist dafür keine unmittelbare Nähe mehr erforderlich[65] – theoretisch könnte man die Lesegeräte so einstellen, dass das Auftauchen von tags noch in 30 Meter Entfernung registriert würde. Bisher wird diese Technik insbesondere zur Verbesserung der logistischen Steuerung (etwa des Warenflusses oder des Koffertransports auf Flughäfen) eingesetzt,[66] doch sind sehr viele andere Anwendungen denkbar. Soweit eine relativ dichte Infrastruktur von Lesegeräten besteht, können über einzelne Mitmenschen, in deren Kleidern sich tags befinden, unschwer Bewegungsprofile erstellt werden. Dies kann in der Regel unbemerkt geschehen, da weder tag noch Lesegerät auffallen, wenn sie der Betroffene nicht systematisch sucht.[67] Der Marburger Bund der angestellten Ärztinnen und Ärzte hat dem BMAS im Rahmen der Diskussion um Arbeit 4.0 mitgeteilt, Dienstkleidung werde zunehmend mit RFID-Technologie ausgestattet, wodurch sich ein detailliertes Bewegungsprofil von Ärzten erstellen lasse.[68] Dies ist genauso unzulässig, wie wenn es mit Hilfe von Videokameras erfolgen würde. Das Problem, ob ID-Nummern auf Produkten personenbezogene Daten sind, stellt sich im überschaubaren Bereich des Betriebes nicht, da der Personenbezug mit Hilfe von Zusatzwissen so gut wie immer herstellbar ist.[69]

---

[63] BGH NJW 2013, 2668.
[64] S. *Holznagel/Schumacher* MMR 2009, S. 3, 4. Er ist also »responder« und dann »transmitter«, was zu dem Ausdruck »Transponder« zusammengezogen wird.
[65] *Löw* ZD 2013, 309
[66] S. auch *Kesten* RDV 2008, 97ff.
[67] *Löw* ZD 2013, 310; dazu auch *Arning/Born* in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 2014, Teil X Kap. 2 Rn. 29 ff.
[68] Mitgeteilt bei *BMAS* (Hrsg.), Weissbuch Arbeiten 4.0, 2017, S. 142
[69] Zur Frage, ob in anderen Zusammenhängen ein besonderes RFID-Datenschutzrecht notwendig ist, weil die tags keine personenbezogenen Daten beinhalten, aber dennoch eine allgemeine Überwachung ermöglichen, s. *Löw* ZD 2013, 309ff.

5. Überwachungssysteme

Auf dem Markt werden Programme angeboten, die in regelmäßigen Abständen Screenshots machen, d.h. den jeweiligen Bildschirminhalt festhalten, und jede Aktivität auf dem PC bis hin zum Tastaturanschlag erfassen.[70] Dies kann durch eingebaute Kameras im PC oder im Laptop ergänzt werden, die sich unbemerkt aktivieren lassen.[71] Weiter kann auch ein Handy in ein Abhörgerät verwandelt werden.[72] Derartige »spyware« hat bereits die Rechtsprechung beschäftigt. Im Falle einer Entscheidung des ArbG Augsburg[73] installierte eine Wartungsfirma im Auftrag des Arbeitgebers im Betriebsratscomputer eine spezifische Software: Sobald eine Verbindung zwischen dem PC und dem Arbeitszeitsystem hergestellt war, aktivierte sie sich und machte fünf Minuten lang jede Sekunde einen Screenshot. Das BAG hatte vor kurzem über einen Fall zu entscheiden, in dem auf dem Dienst-PC des Arbeitnehmers eine Software installiert worden war, die sämtliche Tastatureingaben protokollierte und regelmäßig Screenshots fertigte.[74] Beide Gerichte sahen in den fraglichen Maßnahmen weitreichende Eingriffe in die grundgesetzliche geschützte Persönlichkeitssphäre, die nur durch ein überwiegendes Arbeitgeberinteresse gerechtfertigt werden könnten. Im Fall des ArbG Augsburg scheiterte dies daran, dass zwar der Verdacht eines Arbeitszeitbetrugs bestand; die Aufklärungsmaßnahme war jedoch über den dadurch geschaffenen Informationsbedarf des Arbeitgebers hinausgegangen, weil während der fünf Minuten auch solche PC-Aktivitäten festgehalten wurden, die nichts mit dem Arbeitszeitsystem zu tun hatten. Im Fall des BAG bestand keinerlei Verdacht der Pflichtverletzung, so dass ein überwiegendes Arbeitgeberinteresse nicht ersichtlich war.

Unzulässige Überwachungssysteme müssen sich nicht auf den Gang der Arbeit als solchen beziehen. Vielmehr ist es auch denkbar, dass die Arbeitsergebnisse in einer so detaillierten Weise erfasst und mit einem Durchschnittswert abgeglichen werden, dass ein vergleichbar intensiver Druck für die Beschäftigten entsteht. Wird beispielsweise bei den Schadenssachbearbeitern einer Versicherung jeden Tag und jede Woche die Zahl der bearbeiteten Vorgänge, die Anzahl und Dauer der Rückstände, die Zahl der Telefongespräche, die Nachbearbeitungszeit je Gespräch und eine Reihe weiterer Faktoren erfasst, so stellt diese

[70] Instruktiv *Heidemann* CuA 9/2010 S. 18ff.
[71] Darstellung bei *Bernhard/Ruhmann* CF Heft 12/2001 S. 13f.; s. auch *Heidemann* CuA 9/2010 S. 19
[72] CF Heft 3/2002 S. 3.
[73] LAGE Art. 2 GG Persönlichkeitsrecht Nr. 16; dazu *Däubler* CuA 1/2013 S. 13ff.
[74] *BAG* Urt. v. 27.7.2017 – 2 AZR 681/16, Pressemitteilung Nr. 31/17 („keylogger“)

„Statistik“ einen schwerwiegenden Eingriff in das Persönlichkeitsrecht der Arbeitnehmer dar, der nicht durch überwiegende schutzwürdige Belange des Arbeitgebers gedeckt war.[75]

6. Telekommunikation

Darf der Arbeitgeber Telefongespräche, Mails und die Internetnutzung kontrollieren? Hier ist zu unterscheiden.

Handelt es sich um erlaubte private Kommunikation, so ist das Telekommunikationsgeheimnis des § 88 TKG zu wahren. Es bezieht sich nicht nur auf den Inhalt des Gesprochenen oder Geschriebenen, sondern auch auf die näheren Umstände der Kommunikation. Bezogen auf Telefongespräche bedeutet dies, dass lediglich die Daten festgehalten und verwertet werden dürfen, die für die Abrechnung erforderlich sind.

Bei dienstlicher Kommunikation verhält es sich anders. Die äußeren Daten, etwa Zeitpunkt und Dauer eines Telefongesprächs oder Eingangszeitpunkt eines E-Mails kann erfasst und gespeichert werden.[76] Das eigentliche Problem liegt im Zugriff auf die Inhalte. Nach der Rechtsprechung des BVerfG[77] kann sich ein Arbeitnehmer auch dann auf sein Recht am eigenen Wort berufen, wenn er Dienstgespräche führt. Das Mithören durch Dritte würde einen Eingriff in seine Persönlichkeitssphäre darstellen, die mit einer heimlichen Tonbandaufnahme vergleichbar sei.[78] Allerdings kann ein solcher Eingriff im Einzelfall wegen überwiegender schutzwürdiger Interessen des Arbeitgebers gerechtfertigt sein. Das BAG hat sich dieser Rechtsprechung angeschlossen[79] und die Rechtfertigungsgründe näher eingegrenzt. Danach hat das Arbeitgeberinteresse nur dann den Vorrang, wenn der Eingriff nach Inhalt, Form und Begleitumständen erforderlich ist. Wer seine Probezeit in einem Reservierungszentrum eines Luftfahrtunternehmens absolviere, müsse sich ein gelegentliches Mithören gefallen lassen, weil sich der Arbeitgeber andernfalls kein Bild von der Qualität seiner Arbeit machen könne.[80] Dies wird man auf den Fall übertragen können, dass nach Ende der Probezeit verschiedentlich Beschwerden eingehen, die Zweifel an der „Dienstleistungsqualität“

[75] So *BAG* NZA 2017, 1205.
[76] *BAG* AP Nr. 15 zu § 87 BetrVG 1972 Überwachung
[77] DB 1992, 786, bestätigt durch *BVerfG* NJW 2002, 3619
[78] Zu deren Unzulässigkeit BVerfGE 34, 238, 245
[79] *BAG* NZA 1996, 218; BAG DB 2003, 2230
[80] *BAG* NZA 1996, 218, 221

aufkommen lassen. Regelmäßige „Stichproben“, wie sie in vielen Call Centern üblich sind, lassen sich damit aber nicht rechtfertigen.

Ob E-Mails genauso wie Telefongespräche zu behandeln sind, wird unterschiedlich beurteilt.[81] Letztlich kommt es aber allein auf das Vorliegen eines überwiegenden Arbeitgeberinteresses an. Ein heimliches Mitlesen durch den Vorgesetzten kommt allenfalls dann in Betracht, wenn der auf Tatsachen gegründete Verdacht einer strafbaren Handlung oder einer schweren Pflichtverletzung besteht. Im Normalfall muss der Arbeitnehmer gebeten werden, die Mail weiterzuleiten oder sie auszudrucken und dem Vorgesetzten zur Verfügung zu stellen. Bei der Internetnutzung geht es typischerweise um die Frage, ob Dateien angeschaut oder heruntergeladen wurde, die nichts mit den dienstlichen Zwecken zu tun haben. Ist dies der Fall, liegt darin eine Verletzung der Arbeitspflicht, doch ändert dies nicht den privaten Charakter des Vorgangs: Der Arbeitgeber kann selbstredend die Löschung der Datei verlangen, doch hat er kein überwiegendes Interesse daran, auch von ihrem Inhalt Kenntnis zu nehmen. Um festzustellen, ob privat gesurft wurde, gibt das LAG Berlin-Brandenburg[82] dem Arbeitgeber das Recht, in die „Chronik“ des Internet-Browsers Einblick zu nehmen und alle Internetkontakte nachzuvollziehen.

Schwer lösbare Probleme ergeben sich dann, wenn dienstliche und erlaubte private Kommunikation per E-Mail technisch nicht getrennt sind und der Arbeitnehmer ausgeschieden oder vorübergehend nicht erreichbar ist. Im Regelfall wird einvernehmlich eine Person bestimmt, an die die Mails weitergeleitet werden oder die jedenfalls auf sie zugreifen darf. Fehlt es daran, wird häufig ein dringendes Bedürfnis des Arbeitgebers entstehen, von der dienstlichen Korrespondenz Kenntnis zu erhalten. Gleichzeitig ist jedoch wegen der Privaten Mails das Telekommunikationsgeheimnis zu wahren. Dem kann am besten dadurch Rechnung getragen werden, dass ein neutraler Dritter wie z. B. ein Rechtsanwalt oder der Datenschutzbeauftragte Einblick nimmt und dem Arbeitgeber die ersichtlich dienstlichen Mails zugänglich macht.[83]

[81] Für Gleichbehandlung *Balke/Müller* DB 1997, 326; *Raffler/Hellich* NZA 1997, 863; anders Simitis-*Seifert* § 32 Rn. 91 mwN
[82] BB 2016, 891
[83] Dafür im Grundsatz auch *de Wolf*, NZA 2010, 1206, 1211

V. Zukunftsperspektiven

Big Data, genauer: Erkenntnisse, die aus einer unübersehbaren Menge von Daten gewonnen werden, können in Zukunft bei Personalentscheidungen eine erhebliche Rolle spielen. Man kann verschiedene Erscheinungsformen unterscheiden.

- Der Arbeitgeber bezieht von einer Drittfirma „Erfahrungssätze", die diese durch Auswertung von Big Data gewonnen hat. Wer sich beispielsweise in bestimmter Weise verhält, ist auf dem Absprung zu einem anderen Unternehmen; will man ihn halten, ist Angebote fällig. Oder umgekehrt: Wer fünf Jahre lang nicht befördert wurde, hat kein Entwicklungspotential mehr und sollte am besten das Unternehmen verlassen. Wendet man einen derartigen Grundsatz an, so ist dies ein Kriterium für die Personalbeurteilung, das nach § 94 BetrVG der Mitbestimmung unterliegt.[84] Wird der „Erfahrungssatz" auf eine konkrete Person bezogen und diese beispielsweise als „ohne Zukunftsaussichten" qualifiziert, so kommt der Datenschutz ins Spiel. Dies hat zur Folge, dass die betroffene Person nach Art. 14 DSGVO über die Existenz dieser Einordnung informiert werden muss. Weiter ist sie über die Kriterien aufzuklären, die zu dieser Beurteilung geführt haben. Dies verlangt auch der in Art. 5 Abs. 1 Buchst. a DSGVO niedergelegte Transparenzgrundsatz; nur auf dieser Grundlage kann sich die betroffene Person zur Wehr zu setzen. Ist die Bewertung negativ, lassen sich die Grundsätze über das Arbeitszeugnis entsprechend anwenden, wonach der Arbeitgeber für alle Angaben beweispflichtig ist, die einer unterdurchschnittlichen Beurteilung des Arbeitnehmers zugrunde liegen.[85] Dabei steht auch der „Erfahrungssatz" zur Disposition, dessen korrekte Gewinnung im Zweifelsfall nicht belegt werden kann. Dafür spricht u. a., dass die Datenbasis in US-amerikanischen Unternehmen gewonnen wurde, wo möglicherweise völlig andere Verhaltensstandards gelten als in Deutschland.
- Erkenntnisse (oder Pseudoerkenntnisse), die auf Big Data beruhen, müssen nicht von außen importiert werden. So wird etwa von einem Programm berichtet, das bei der US-Investmentbank JP Morgan im April 2015 eingesetzt wurde: Daten unterschiedlichster Art wurden gesammelt, kombiniert und analysiert, um ein wahrscheinliches Fehlverhalten von Angestellten voraussagen zu können.[86] Dabei wurden u. a. Telefongespräche, Mails, Teilnahme an Compliance-Kursen sowie persönliche Bemerkungen in Bezug auf die einzuhaltenden Regeln einbezogen. Auf diese Weise werden „Risikopersonen"

[84] Dazu *Däubler*, Gläserne Belegschaften (Fn. 9) Rn. 486
[85] *BAG* NZA 2004, 843; Däubler/Deinert/Zwanziger-*Däubler*, Kündigungsschutzrecht, 10. Aufl. 2017, § 109 GewO Rn. 98
[86] *Schröder*, Die digitale Treppe, 2017, S. 132, auch zum Folgenden

herausgefiltert. Sie müssen damit rechnen, auf einen schlechteren Arbeitsplatz versetzt oder für den nächsten Personalabbau vorgesehen zu werden. In Deutschland ließe sich ein solches Vorhaben nicht realisieren, da die Erkenntnismöglichkeiten des Arbeitgebers (etwa in Bezug auf Telefongespräche) beschränkt sind und eine solche „Totalerfassung" des Arbeitsverhaltens, das bis zur Prognose künftigen (Fehl-)Verhaltens geht, gegen das Verbot zur Erstellung eines Persönlichkeitsprofils verstoßen würde.[87] Umsichtiger ist der Vorschlag, aus dem Verhalten der erfolgreichsten Führungskräfte oder Vertriebsmitarbeiter Algorithmen zu entwickeln, mit denen Bewerber abgeglichen werden. Anders ausgedrückt: Nur wer dem firmeneigenen Mitarbeiterideal nahe kommt, wird eingestellt.[88] Ein Problem liegt darin, dass die Daten der Führungskräfte für andere Zwecke als die Durchführung ihres Arbeitsverhältnisses verwendet werden, ein weiteres besteht in mangelnder Transparenz: Wie soll ein Bewerber nachvollziehen können, weshalb einzelne Personen zur Bestimmung des „Leitverhaltens" ausgesucht wurden und wie dieses im Einzelnen erarbeitet wurde.

- Ein immer größerer Tel der innerbetrieblichen Kommunikation erfolgt über soziale Netzwerke, in Arbeitsgruppen und durch sonstigen Austausch von Informationen. Dies macht es möglich, „Netze" im Betrieb abzubilden und „Außenseiter" mit wenig Kommunikation zu identifizieren. Die Informatiker sprechen vom „Social Graph" des Unternehmens,[89] das sehr viel mehr Einsichten in das innerbetriebliche Geschehen als traditionelle Methoden eröffnet. Bis auf weiteres stehen dem allerdings datenschutzrechtliche Bedenken entgegen,[90] weil die Erforderlichkeit für die Durchführung des einzelnen Arbeitsverhältnisses nicht erkennbar ist.

VI. Fazit

Der Arbeitgeber kann sich alle Informationen verschaffen, die er für die Begründung, Durchführung und Beendigung des Arbeitsverhältnisses benötigt. Der dabei anzuwendenden Mittel wollen sorgfältig bedacht sein. Auch wenn der Einsatz einer Videokamera oder eines verdeckten Ermittlers ein einfacher und Erfolg versprechender Weg wäre, ist er deshalb noch lange nicht zulässig. Dasselbe gilt für die Erstellung von Bewegungsprofilen und für den Einsatz von Überwachungsprogrammen. Erhebliche Eingriffe in die Persönlichkeitssphäre sind im Grundsatz nur dann gerechtfertigt, wenn ein durch Tatsachen begründeter Verdacht einer Straftat oder einer schweren Pflichtverletzung besteht. Aus Big Data gewonnene

[87] Ablehnend zur Anwendung von Big-Data-Analysen bei Personalentscheidungen auch *Niklas/Thurn*, BB 2017, 1589 ff.
[88] Näher *Dzida*, NZA 2017, 541 ff.
[89] Einzelheiten bei *Höller* CuA 5/2016 S. 9 ff.
[90] *Wedde* CuA 5/2016 S. 14 ff.

Erkenntnisse sind grundsätzlich kein taugliches Mittel, das bei Personalentscheidungen Verwendung finden kann.