

Auszug aus: Däubler, Gläserne Belegschaften? 5. Aufl., Frankfurt/Main 2010

§ 6: Datenerhebung gegenüber Beschäftigten

I. Gesetzliche Vorgaben

- 253** Wird ein Bewerber eingestellt, so gelten für die von diesem Zeitpunkt an erfolgenden Erhebungen, Verarbeitungen und Nutzungen seiner Daten keine prinzipiell anderen Regeln als in der Bewerbungssituation. Wichtigste **Rechtsgrundlage** ist **auch hier § 32 Abs. 1 Satz 1 BDSG**, wobei lediglich der Zweck „Begründung eines Beschäftigungsverhältnisses“ durch dessen „Durchführung oder Beendigung“ ersetzt wird. Hinzu kommt jetzt allerdings die Besonderheit, dass der **Arbeitgeber kraft öffentlichen Rechts zahlreiche Daten erheben** und an die Verwaltung weiterleiten oder für diese bereithalten muss. Als Beispiel für das eine mag die Abführung von Lohnsteuern und Sozialversicherungsbeiträgen stehen, ein Anwendungsfall des zweiten sind die Vorschriften der §§ 49, 50 JArbSchG, wonach der Arbeitgeber ein Verzeichnis der bei ihm beschäftigten Jugendlichen unter 18 Jahren mit bestimmten Angaben erstellen und dieses der Aufsichtsbehörde auf Verlangen vorzulegen oder einzureichen hat. Das BAG¹ hat im Übrigen das Fragerecht des Arbeitgebers in gleicher Weise wie gegenüber Bewerbern beschränkt: Der Arbeitgeber muss ein **»berechtigtes, billigenwertes und schutzwürdiges Interesse an der Beantwortung«** der Frage haben. Alles, was darüber hinausgeht, würde das Persönlichkeitsrecht des Arbeitnehmers verletzen.²
- 254** Auf der faktischen Ebene ist zu beachten, dass der **Arbeitnehmer** im Laufe eines länger dauernden Arbeitsverhältnisses **außerordentlich vielfältigen Informationsinteressen ausgesetzt** ist, die beim Bewerber noch keine Rolle spielen. Dies gilt nicht nur für Fragen der Entgeltabrechnung, sondern insbesondere für die Kontrolle des Arbeitsverhaltens, bei der heute die Einbeziehung von Telefon und Internet sowie der Einsatz von Videokameras spezifische Probleme aufwirft. Außerdem kann ein Bedürfnis zur Identifikation im Wege **biometrischer Verfahren** entstehen. Weiter tritt der Arbeitnehmer – um mit einem relativ harmlosen Beispiel zu schließen – seinem Arbeitgeber bisweilen auch in der Rolle als Konsument gegenüber, wenn er in der Kantine einkauft oder ein Darlehen in Anspruch nimmt.
- 255** Angesichts der Vielfalt der Informationsinteressen gewinnt § 28 Abs. 1 Satz 2 BDSG erhöhte Bedeutung.¹ Je stärker der Einzelne zum Informationsobjekt wird, um so mehr muss von vorneherein der **»konkrete Zweck«** feststehen, für den die Daten verarbeitet oder genutzt werden sollen. Hier gewinnt die **informationelle Gewaltenteilung** zentrale Relevanz.³
- 256** Nach § 32 Abs.2 BDSG findet das Gesetz nunmehr auch bei **manuell geführten Personalakten** Anwendung. Bei der Ausfüllung allgemeiner Begriffe wie „berechtigtes Interesse“ und „schutzwürdige Belange“ kann jedoch auf allgemeine arbeitsrechtliche Grundsätze zurückgegriffen werden.

II. Privatsphäre und Konsumverhalten

- 257** Die privaten Lebensverhältnisse des Arbeitnehmers müssen für den Arbeitgeber ohne Interesse bleiben; insoweit ist die Situation keine andere als gegenüber einem Bewerber.² Dasselbe gilt für das Verhalten während der Pausen und in der Kantine.⁴ Welches Essen der Arbeitnehmer wählt, welche Waren er kauft und wieviel Benzin er tankt, hat mit dem Beschäftigungsverhältnis als dem maßgebenden Vertragsverhältnis im Sinne des § 32 Abs. 1 Nr. 1 BDSG nichts zu tun. Soweit der Arbeitgeber – ähnlich wie ein Unternehmen im Verhältnis zu seinen Kunden – zu Abrechnungszwecken Daten erfasst, sind diese

¹DB 1996, 634.

²Ebenso in der Literatur MünchArbR-Blomeyer, § 99 Rn. 27; Fitting u. a., § 94 Rn. 16; Gola/Wronka Rn 349 ff.; Klebe, in: Däubler/Kittner/KlebeWedde, § 94 Rn. 12.

³ Zu seiner Anwendbarkeit neben § 32 BDSG s. oben Rn 186

⁴S. oben Rn. 89.

² Oben Rn 211.

⁴Ebenso Zöllner, Daten- und Informationsschutz, S. 42.

als »verbraucherbezogen« streng von den arbeitnehmerbezogenen zu trennen.⁵ Auf die private Telekommunikationsnutzung ist an späterer Stelle einzugehen.⁶ Ob ausnahmsweise eine »zweckwidrige« Verwendung möglich ist, soll gleichfalls unten⁷ behandelt werden.

III. Durchführung des Beschäftigungsverhältnisses

1. Entgeltabrechnung

258 Bei der Entgeltabrechnung ist eine Reihe von persönlichen Merkmalen von Bedeutung, nach denen in der Einstellungssituation nicht gefragt werden darf. So erhält der Arbeitgeber etwa aufgrund der Vorlage der Lohnsteuerkarte automatisch Kenntnis von der Konfession; auch die Gewerkschaftszugehörigkeit lässt sich nicht mehr verbergen, wenn der Arbeitgeber – was allerdings immer seltener vorkommt – die Mitgliedsbeiträge direkt an die Gewerkschaft abführt. Entsprechende Fragen an einen Arbeitnehmer sind daher aus begründetem Anlass (etwa bei abhanden gekommener Lohnsteuerkarte) zulässig.⁸ Auch hier ist entscheidend, dass diese Daten nur zu Abrechnungszwecken verwendet werden; die Absicherung dieses Zwecks bedarf besonderer Schutzmaßnahmen.⁹

259 An diesem Zustand hat sich durch die **Sonderregeln über sensitive Daten** nichts geändert. Zwar fällt sowohl die Konfession als auch die Gewerkschaftszugehörigkeit darunter, doch erlaubt § 28 Abs. 6 Nr. 3 BDSG das Erheben, Verarbeiten und Nutzen, soweit dies zur Geltendmachung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung usw. überwiegt. In beiden hier interessierenden Fällen geht es um die Geltendmachung von Ansprüchen, die nach Wortlaut und Sinn des Gesetzes nicht dem Betroffenen zustehen müssen.¹⁰ Außerdem ist kein schutzwürdiges Gegeninteresse des Betroffenen ersichtlich, das überwiegen würde: Die Angabe über die **Konfession** ergibt sich letztlich aus den Vorschriften über die Erhebung der Kirchensteuer, die eine Information des Arbeitgebers implizieren. Dass der Arbeitgeber Kenntnis von der **Gewerkschaftszugehörigkeit** erhält, ist dann unproblematisch, wenn der Arbeitnehmer der Gewerkschaft gegenüber in die **Einziehung der Gewerkschaftsbeiträge** eingewilligt hat. Letzteres muss allerdings erfolgt sein.¹¹ Ergänzend sei noch darauf hingewiesen, dass nach erfolgter Einstellung auch nach Familienstand und **Kinderzahl**¹² und nach **Gehaltspfändungen** gefragt werden kann.¹³

2. Arbeitszeit und Arbeitsverhalten

260 Der Arbeitgeber ist nach § 32 Abs. 1 Satz 1 BDSG berechtigt, die mit dem Arbeitnehmer vereinbarte Dauer und Lage der Arbeitszeit (**»Soll-Arbeitszeit«**) sowie die tatsächlichen Anwesenheitszeiten im Betrieb zu speichern (**»Ist-Arbeitszeit«**). Auch die **Abwesenheitsgründe** können erfasst werden; inwieweit sie über den Einzelfall hinaus ausgewertet werden dürfen, ist im nächsten Abschnitt¹⁴ zu erörtern. Keine Bedenken bestehen auch dagegen, Verkaufserfolge von Außendienstmitarbeitern selbst dann festzuhalten, wenn sie ohne Einfluss auf die Vergütung sind. Dasselbe gilt selbstredend für die Erreichung der in **Zielvereinbarungen** festgelegten Ergebnisse. Lediglich die betriebsinterne Bekanntmachung von »Rennlisten« kann Probleme aufwerfen.¹⁵

261 Erhält der Arbeitnehmer **eine Beurteilung durch Vorgesetzte** oder andere Personen, so kann auch deren Inhalt gespeichert oder auf andere Weise festgehalten werden, da praktisch keine Fälle denkbar sind, in denen dies ohne jede Auswirkung auf den weiteren Ablauf des Arbeitsverhältnisses bleibt.¹⁶ In welchem Umfang das Verhalten des Arbeitnehmers kontrolliert und damit ein »Leistungsprofil« erstellt werden darf,

⁵Dazu unten § 7 II (Rn. 394ff.).

⁶S. unten VII (Rn. 325ff.).

⁷§ 7 III (Rn. 412ff.).

⁸Fitting, § 94 Rn. 17. Weitergehend BAG DB 1987, S. 1050.

⁹Dazu unten § 7 II 4 (Rn. 401f.), 7 (Rn. 408ff.).

¹⁰Gola, RDV 2001, 127.

¹¹Simitis-Simitis, § 28 Rn. 111.

¹²Ebenso Fitting, § 94 Rn. 20; Klebe, in: Däubler/Kittner/Klebe/Wedde, § 94 Rn. 19, beide m.w.N.

¹³Fitting, § 94 Rn. 21; Klebe, in: Däubler/Kittner/Klebe/Wedde § 94 Rn. 19.

¹⁴§ 7 II 4 (Rn. 401).

¹⁵Dazu unten Rn. 483.

¹⁶Vgl. Tinnefeld/Ehmann/Gerling, S. 555.

soll an späterer Stelle¹⁷ behandelt werden.

3. Weiterförderung

262 Will der Arbeitgeber eine sog. **Potenzialanalyse** in Bezug auf einzelne Beschäftigte vornehmen, so ist dies nur mit deren Einwilligung möglich.¹⁸ Inhaltliche Bedenken gegen eine solche Einwilligung bestehen nicht, da diese Maßnahme in aller Regel auch dem Interesse des Beschäftigten dient und ein unmittelbarer Zusammenhang mit dem Beschäftigungsverhältnis besteht.¹⁹ Ähnliches gilt für die Aufnahme in eine sog. Weiterförderungsdatei.

4. Erhebung zahlreicher persönlicher Umstände im Hinblick auf eine mögliche »soziale Auswahl«?

263 Ein besonderes Maß an »Datenhunger« könnte der Arbeitgeber unter Berufung auf die Tatsache entwickeln, dass bei einer sozialen Auswahl im Sinne des § 1 Abs. 3 KSchG zahlreiche für und gegen die soziale Schutzwürdigkeit sprechenden Umstände bei allen vergleichbaren Arbeitnehmern berücksichtigt werden müssen.²⁰ Dies schließt notwendigerweise auch Daten über Angehörige ein. Problematisch ist dabei nicht die Erhebung der fraglichen Daten, sondern ihr **Zeitpunkt**: Da eine betriebsbedingte Kündigung nie völlig auszuschließen ist, könnte auf diesem Wege der durch den Zweck des Arbeitsvertrags gezogene Rahmen enorm erweitert werden.³

264 Keine Lösung bringt die verbreitete und im Prinzip zutreffende Aussage, wonach **§ 1 Abs. 3 KSchG als Spezialnorm** dem BDSG vorgehe.²¹ **Geregelt** ist dort ausschließlich die Weitergabe der Daten an das Gericht und die Gegenpartei (und ggf. ihre Erörterung in mündlicher Verhandlung), **nicht** aber das **Erhebungsrecht des Arbeitgebers**. Dieses bestimmt sich vielmehr nach allgemeinen datenschutzrechtlichen Grundsätzen. Wenig befriedigend ist es, den Arbeitgeber von eigenen Nachforschungen zu dispensieren und ihn auf die Verwertung derjenigen Informationen zu beschränken, die ihm freiwillig von den in die soziale Auswahl einzubeziehenden Belegschaftsmitgliedern gemacht werden.²² Dies führt im Ergebnis dazu, dass **derjenige** Beschäftigte am ehesten **begünstigt** ist, **der die weitesten Einblicke** in seine Privatsphäre **gestattet** – vorausgesetzt, dabei treten Tatsachen zu Tage, die seine soziale Schutzbedürftigkeit verstärken. Mit dem informationellen Selbstbestimmungsrecht lässt sich ein solcher Zustand **nicht vereinbaren**: Wer sich gegen eine Bekanntgabe entscheidet (weil er vielleicht den Arbeitgeber nicht wissen lassen möchte, dass ein Familienangehöriger behindert oder drogenabhängig ist), hat gravierende Nachteile zu gewärtigen. Ein »Recht zur Lüge«, wie es für die Einstellungssituation eingeräumt wird, hilft hier nicht weiter.

265 Ein **verfassungskonformer Zustand** wäre einmal dadurch herstellbar, dass die privaten Lebensverhältnisse generell aus dem Kreis der Faktoren ausgeklammert würden, die bei der sozialen Auswahl zu berücksichtigen sind. Da die Rechtsprechung diesen Weg richtigerweise nicht gegangen ist, bleibt als zweites nur die Möglichkeit, auch die Privatsphäre offenzulegen, den Arbeitnehmer aber gleichzeitig davor zu schützen, dass der Arbeitgeber damit alle sonstigen Grenzen des Fragerechts einreißt. Anders als bei medizinischen Daten ist dies nicht durch eine Beschränkung seines Erhebungsrechts und durch Geheimhaltung seitens des Werksarztes möglich, da es keinen »Sozialauswahlbeauftragten« gibt. Auch ist die Erhebung ersichtlich für den Zweck „Beendigung des Arbeitsverhältnisses“ erforderlich. Es helfen jedoch zwei Mittel:

266 Zum einen ist die Erhebung **erst dann** zulässig, wenn betriebsbedingte **Kündigungen nicht mehr auszuschließen** sind. Die lediglich abstrakte Möglichkeit reicht nicht aus, weil dann eine Vorratsdatenspeicherung vorliegen würde.²³

267 Zum zweiten muss ein zwingendes Verwertungsverbot in Bezug auf die zu Zwecken der sozialen Auswahl

¹⁷S. unten § 7 II 6 (Rn. 405ff.).

¹⁸Schleswig-Holsteinischer DSB, 12. TB, unter 4.10.2.

¹⁹Zu den inhaltlichen Wirksamkeitsvoraussetzungen für Einwilligungen s. oben § 4 III (Rn. 148).

²⁰Dazu Kittner/Deinert, in: Kittner/Däubler/Zwanziger, § 1 KSchG Rn. 468 ff. m.w.N.

³ Das das KSchG nach herrschender Auffassung nur auf Arbeitnehmer, nicht aber auf arbeitnehmerähnliche Personen und sonstige Beschäftigte Anwendung findet, ist hier nur vom „Arbeitsvertrag“ als einem Spezialfall des „Beschäftigungsvertrags“ die Rede.

²¹So BAG NJW 1984, 79 re. Sp.; Achenbach, NZA 1984, 280; wohl auch Gola, DuD 1984, 33.

²²So aber Kroll, S. 102ff. Wenig erhellend auch Wohlgemuth, Datenschutz für Arbeitnehmer, Rn. 330.

²³Wedde, in: Däubler/Klebe/Wedde/Weichert, § 28 Rn. 35.

erhobenen Daten bestehen, die ja bei den nicht gekündigten Beschäftigten weiter abrufbar vorhanden sind. Dies lässt sich am ehesten in der Weise absichern, dass eine **Separation von den übrigen Arbeitnehmerdaten** erfolgt und ein Zugriff nur für den Fall einer effektiv auszusprechenden betriebsbedingten Kündigung möglich ist.²⁴

5. Umfragen im Betrieb und statistische Auswertungen

268

Keine datenschutzrechtlichen Probleme wirft eine Umfrage zur Arbeitszufriedenheit, zum Verhalten der Vorgesetzten, zur Darstellung der Firma in der Öffentlichkeit usw. auf, wenn die **Stellungnahme** des Einzelnen vergleichbar **anonym** bleibt wie bei einer geheimen Wahl: In einem solchen Fall entstehen keine personenbezogenen Daten. Die Situation ändert sich, wenn der einzelne Beschäftigte z.B. einen Fragebogen ausfüllen oder ein Gespräch führen muss und das Resultat ihm weiter zugerechnet werden kann. Soweit ihm die **Teilnahme freisteht** und er sich der Aktion ohne irgendwelche Nachteile entziehen kann, wird man letztlich eine **Einwilligung als Legitimation** für eine solche Datenspeicherung anerkennen können. Will der Arbeitgeber jedoch die Beteiligung auch gegen den Willen des Einzelnen durchsetzen, überschreitet er sein Erhebungsrecht, da bestimmte Fragen den Einzelnen in einen vermeidbaren Gewissenskonflikt bringen können, den zu provozieren ersichtlich nicht vom Zweck des Beschäftigungsverhältnisses gefordert wird.

Zu denken ist etwa an den Fall, dass nach dem Führungsverhalten von Vorgesetzten gefragt wird und eine noch so berechtigte negative Bewertung möglicherweise „Racheaktionen“ zur Folge haben könnte. Ähnliches gilt, wenn man der Firma ein schlechtes Image bescheinigt oder die Arbeitsatmosphäre als bedrückend beschreibt. Da in solchen Fällen vermutlich die »Ausweichstrategie« unwahrer positiver Einschätzungen gewählt würde, besteht auch betriebswirtschaftlich kein Interesse, eine Umfrage mit derart obligatorischer Beteiligung durchzuführen.

Die Erstellung von Statistiken stellt eine Auswertung personenbezogener Daten dar und ist deshalb im nächsten Abschnitt zu behandeln.

IV. Gesundheitsdaten und Gentests

1. Traditionelle Gesundheitsdaten

a) Die Sonderregeln über sensitive Daten

269

Auf die Gesundheit des Arbeitnehmers bezogene Daten werden von § 3 Abs. 9 BDSG erfasst und unterliegen den spezifischen Verarbeitungsvoraussetzungen nach § 28 Abs. 6–9 BDSG.²⁵ Im bestehenden Beschäftigungsverhältnis kommen als Rechtsgrundlage für die Erhebung entsprechender Daten nur § 28 Abs. 6 Nr. 3 BDSG und § 28 Abs. 7 BDSG in Betracht.

270

Bei Abs. 6 Nr. 3 geht es insbesondere um die **Geltendmachung oder Abwehr von Rechtsansprüchen**, so dass Angaben, die nach dem Entgeltfortzahlungsgesetz vorausgesetzt sind, erfasst werden können. Dies gilt selbst dann, wenn der Entgeltfortzahlungszeitraum überschritten ist; auch die fortdauernde Arbeitsunfähigkeit kann erhoben und (manuell oder EDV-mäßig) gespeichert werden. Dem Arbeitgeber steht es weiter frei, daraus die Konsequenz einer **Kündigung wegen Krankheit** zu ziehen; auch dies ist eine ihm eingeräumte rechtliche Möglichkeit, die von § 28 Abs. 6 Nr. 3 BDSG erfasst wird.²⁶ Sollen Gesundheitsdaten zu dem **Zweck** erhoben werden, **künftigen Erkrankungen vorzubeugen**, indem die Arbeitsbedingungen einschließlich des Betriebsklimas verbessert werden, so scheidet § 28 Abs. 6 Nr. 3 als Rechtsgrundlage aus. In diesem Fall greift **allein § 28 Abs. 7 BDSG** ein, der die Datenerhebung für Zwecke der Gesundheitsvorsorge, der medizinischen Diagnostik und anderer medizinischer Zwecke den Ärzten und ihrem Personal vorbehält. Insoweit kann also (nur) der **Betriebsarzt** tätig werden. Die Einschaltung anderer Personen ist lediglich dann möglich, wenn diese der gleichen Schweigepflicht wie ein Betriebsarzt unterliegen.²⁷ Der Gesetzgeber hat damit Art. 8 Abs. 3 der EG-Datenschutzrichtlinie umgesetzt, wobei bewusst nicht die rein ärztliche Tätigkeit, sondern im Prinzip jede gesundheitsbezogene

²⁴ Vgl. auch Gola, RDV 2002, 109.

²⁵ Dazu bereits oben § 5 I 6b (Rn. 196ff.).

²⁶ Gola, RDV 2001, 126; für eine weite Auslegung des Begriffs »rechtlicher Anspruch« in Art. 8 Abs. 2 lit. e der Richtlinie auch Dammann/Simitis, Art. 8 Anm. 17; Gola/Wronka Rn 380. Die Vorschrift muss insgesamt jedoch eng ausgelegt werden: Wedde in: Däubler/Klebe/Wedde/Weichert, § 28 Rn 140.

²⁷ Dammann/Simitis, Art. 8 Anm. 19, wonach Mitarbeiter von Gesundheitsdiensten der Arbeitgeber mit erfasst sind.

Dienstleistung erfasst wird.

271 Inwieweit der Betriebsarzt bzw. gleichgestellte Personen ihre Erkenntnisse betriebsintern weitergeben dürfen, ist keine Frage der Erhebung, sondern der Verwendung und Übermittlung von Daten. Insoweit ist auf spätere Ausführungen zu verweisen.²⁸

272 § 28 Abs. 6 Nr. 3 und § 28 Abs. 7 BDSG eröffnen die grundsätzliche Möglichkeit zur Verarbeitung von Gesundheitsdaten; was dies konkret bedeutet, bestimmt sich nach arbeitsrechtlichen Grundsätzen, die durch das BDSG nicht verändert werden sollten.²⁹

b) Informationspflichten des Arbeitnehmers

273 Ähnlich wie ein Bewerber in der Einstellungssituation ist auch ein Beschäftigter verpflichtet, dem Arbeitgeber mitzuteilen, dass er aus gesundheitlichen Gründen **nicht mehr zur Erfüllung der übernommenen Aufgabe in der Lage ist**. In vielen Fällen hängt dies allerdings von einer individuellen Einschätzung ab; solange das „Weitermachen-Können“ auf nachvollziehbaren Überlegungen beruht, liegt in einer unterbliebenen Mitteilung keine Pflichtverletzung.

274 Wird der Arbeitnehmer nach Ende einer krankheitsbedingten Fehlzeit zu einem »Krankengespräch« gebeten, so ist zunächst das Mitbestimmungsrecht des Betriebsrats bzw. des Personalrats zu beachten.³⁰ Fehlt es an einer betrieblichen Interessenvertretung oder hat diese zugestimmt, so muss zwar der Arbeitnehmer der Aufforderung zu einem Gespräch Folge leisten, doch trifft ihn nach Auffassung des baden-württembergischen Datenschutzbeauftragten³¹ **keine Verpflichtung, über seine Krankheit zu sprechen**: Das EFZG geht bewusst davon aus, dass der Arbeitgeber lediglich Kenntnis vom Vorliegen der Arbeitsunfähigkeit, nicht aber von deren medizinischen Gründen erhält. Schon dies spricht gegen eine Auskunftspflicht des Arbeitnehmers, die den gesetzlichen Schutz unterlaufen würde. Daneben stehen datenschutzrechtliche Bedenken: Die Preisgabe von Gesundheitsdaten ist in dieser Situation nicht zur Geltendmachung oder Abwehr von Ansprüchen erforderlich. Häufen sich Erkrankungen und steht deshalb eine Kündigung wegen Krankheit zur Debatte, gibt es eine Obliegenheit des Arbeitnehmers, den behandelnden Arzt von der Schweigepflicht zu entbinden. Eine »Pflicht«, über die Krankheitsbilder zu berichten, besteht auch dann nicht, doch wird das im Streitfall entscheidende Arbeitsgericht im Kündigungsschutzverfahren bei fehlender Befreiung von der Schweigepflicht eine negative Zukunftsprognose unterstellen.³²

275 Eine **Schwangerschaft** »soll« nach § 5 Abs. 1 MuSchG dem Arbeitgeber mitgeteilt werden. Dies ist eine Empfehlung, keine Rechtspflicht, doch kann sich aus Besonderheiten des Arbeitsverhältnisses (z.B. wegen eines Beschäftigungsverbots für Schwangere) etwas Anderes ergeben.³³ Weiter kann nunmehr unbestrittenermaßen nach der **Schwerbehinderteneigenschaft** gefragt werden.³⁴

c) Pflicht des Arbeitnehmers, sich untersuchen zu lassen?

276 Das Arbeitsschutzrecht sieht in zahlreichen Fällen **Vorsorgeuntersuchungen** vor.³⁵ Ihnen muss sich der Einzelne selbstredend unterziehen. Von ihrem Gegenstand her sind sie auf »arbeitsbezogene« Faktoren beschränkt und dürfen sich deshalb – genau wie Einstellungsuntersuchungen – nicht auf alle denkbaren Aspekte der Gesundheit beziehen.

277 Nach der Rechtsprechung des BAG³⁶ **kann der Arbeitnehmer** auch kraft Tarifvertrags oder kraft arbeitsvertraglicher Nebenpflicht **zur Mitwirkung an einer ärztlichen Untersuchung verpflichtet** sein.³⁷

²⁸S. unten § 7 II 2 (Rn. 396ff.).

²⁹S. die Begründung zum Regierungsentwurf, BT-Dr. 14/4329 S. 43.

³⁰S. unten § 13 III 4 (Rn. 676); vgl. auch Hummel, Krankheit und Kündigung, S. 145f.

³¹18. TB, S. 87.

³²LAG Berlin DB 1990, 1621 m.w.N.; Kittner/Däubler/Zwanziger, § 1 KSchG Rn. 104ff.

³³Schaub-Linck, § 167 Rn.9.

³⁴Klebe, in: Däubler/Kittner/Klebe/Wedde, § 94 Rn. 13.

³⁵Überblick bei Schierbaum/Kiper, AiB 1992, 631; Kittner/Pieper, § 11 ArbSchG Rn. 7.

³⁶DB 1999, 2369.

³⁷Anders noch ArbG Frankfurt/Main AiB 1989, 17 mit Anm. Rothenburg; Wohlgemuth, Datenschutz für Arbeitnehmer, Rn. 144.

Da tarifliche Regelungen hier eine relativ geringe Rolle spielen, kommt es entscheidend darauf an, wann eine entsprechende **Nebenpflicht** angenommen werden kann.

- 278 Das BAG betrachtet eine ärztliche Untersuchung mit Recht als **weitgehenden Eingriff in die Intimsphäre** des Arbeitnehmers; das allgemeine Persönlichkeitsrecht schütze grundsätzlich vor der Erhebung von Befunden über den Gesundheitszustand, die seelische Verfassung und den Charakter des Arbeitnehmers.³⁸ Außerdem sei der Arbeitnehmer regelmäßig nicht verpflichtet, Blutentnahmen zu dulden, da diese einen Eingriff in die körperliche Unversehrtheit darstellten.³⁹ Für die Vornahme einer derartigen Untersuchung müsse daher ein **besonderer Anlass** bestehen; auch müsse sie sich auf die Abklärung des dadurch nahegelegten Krankheitsbildes beschränken.⁴⁰ Dem entspricht eine Entscheidung aus dem Jahre 1964, wonach sich ein Omnibusfahrer aufgrund besonders auffälligen Verhaltens im Straßenverkehr einer psychologischen Untersuchung unterziehen musste.⁴¹
- 279 Praktische Bedeutung haben diese Grundsätze insbesondere in Bezug auf einen **Drogen- und Alkoholtest**. Beide sind nur dann zulässig, wenn Umstände vorliegen, die die **ernsthafte Besorgnis** begründen, bei dem betreffenden Arbeitnehmer könne eine Alkohol- bzw. Drogenabhängigkeit bestehen.⁴² Die Pflicht, einen Test zu dulden, ist daher auf enge Ausnahmefälle beschränkt; eine Durchleuchtung der Belegschaft »auf Verdacht«, um »schwarze Schafe« herauszufiltern, ist nicht zulässig.⁴³
- 280 Ein weiterer – seltener – Anwendungsfall liegt darin, dass ein Arbeitnehmer möglicherweise an **ansteckenden Krankheiten** leidet; hier muss er im Interesse der Arbeitskollegen und ggf. der Kunden eine medizinische Klärung herbeiführen lassen.
- 281 Ein **Aidstest**, genauer: eine Untersuchung, die eine HIV-Infektion abklärt, kommt nur bei Tätigkeiten in Betracht, bei denen eine Ansteckungsgefahr besteht; auch in solchen Fällen sind die Betroffenen vorher zu informieren.⁴⁴ **Psychologische Untersuchungen** unterliegen denselben Grundsätzen,⁴⁵ wobei die Literatur besonders Wert darauf legt, dass der Betroffene nach vorheriger Information über Sinn und Funktionsweise des Tests einwilligt und dieser von einem Fachmann durchgeführt wird.⁴⁶
- 282 In allen Fällen ist die medizinische oder psychologische Untersuchung **auf den jeweiligen engen Zweck beschränkt**; eine im Einzelfall zulässige Untersuchung über Drogenabhängigkeit darf sich nicht auf den gesamten Gesundheitszustand erstrecken.⁴⁷ Nur auf diese Weise ist dem in § 3a BDSG niedergelegten Gedanken der Datensparsamkeit Rechnung getragen, der bei sensitiven Daten im Sinne des § 3 Abs. 9 BDSG erst recht Beachtung verlangt.⁴⁸

d) Weitere Datenerhebung durch den Betriebsarzt

- 283 Soweit nach dem bisher Gesagten keine Pflicht des Arbeitnehmers besteht, sich vom Betriebsarzt oder einem anderen Arzt untersuchen zu lassen, kommt nur eine freiwillige Mitwirkung in Betracht.
- 284 Dem Betriebsarzt ist die **EDV-mäßige Speicherung** der erhobenen Daten **grundsätzlich erlaubt**.⁴⁹ Dies folgt aus der datenschutzrechtlichen Zulässigkeit sowie mittelbar aus der Beweislastregel des § 35 Abs. 2 Satz 2 Nr. 2 BDSG, wonach Daten über gesundheitliche Verhältnisse zu löschen sind, wenn die verantwortliche Stelle ihre Richtigkeit nicht beweisen kann. Eine Reihe von Landesdatenschutzgesetzen lässt die automatisierte Speicherung der Ergebnisse medizinischer und psychologischer Untersuchungen nur zu, wenn dies dem Schutz der Beschäftigten dient,⁵⁰ doch lässt sich daraus kein allgemeiner Rechtsgrundsatz ableiten. Die in § 8 Abs. 1 Satz 3 ASiG bestätigte **ärztliche Schweigepflicht**⁵¹ zwingt den Betriebsarzt, von einer Vernetzung mit anderen Systemen abzusehen und die Datensicherung besonders

³⁸BAG DB 1999, 2370.

³⁹BAG, a.a.O., auch zum Folgenden.

⁴⁰Ähnlich Fitting, § 94 Rn. 16, der ein überwiegendes berechtigtes Interesse des Arbeitgebers gegenüber dem Schutz des Arbeitnehmers verlangt.

⁴¹BAG AP Nr. 1 zu Art. 1 GG.

⁴²BAG DB 1999, 2369, 2370; zum Drogenscreening vgl. Heilmann/Wienemann/Thelen, AiB 2001, 465.

⁴³Ebenso Fitting, § 94 Rn. 25; Klebe, in: Däubler/Kittner/Klebe/Wedde § 94 Rn. 38; Diller/Powietzka, NZA 2001, 1227.

⁴⁴Fitting, § 94 Rn. 25a.

⁴⁵BAG AP Nr. 1 zu Art. 1 GG.

⁴⁶Fitting, § 94 Rn. 26; Grunewald NZA 1996, 15; Klebe, in: Däubler/Kittner/Klebe/Wedde, § 94 Rn. 38; Däubler, Arbeitsrecht 2, Rn. 72 f..

⁴⁷So vom Ansatz her auch BAG DB 1999, 2370.

⁴⁸Dies schließt nicht aus, dass der untersuchende Arzt dem Arbeitnehmer einen Hinweis gibt, sich auch um seine sonstigen Erkrankungen und Risiken zu kümmern.

⁴⁹Hilla/Goldenbohm, CR 1992, 180; Schmidt-Beck, NJW 1991, 2335.

⁵⁰S. etwa § 29 Abs. 5 DSG-NRW, § 29 Abs. 4 DSG-Brandenburg, § 31 Abs. 4 DSG-Saarland. Eine ähnliche Regelung findet sich in § 28 Abs. 5 des DSG-Hamburg.

⁵¹Zu ihr Däubler, BB 1989, 282ff.

ernst zu nehmen.⁵² Soweit möglich, sind die **Befunddaten zu anonymisieren**, was z.B. dann in Betracht kommt, wenn es nur noch um epidemiologische Forschung, nicht aber um konkrete Maßnahmen am Arbeitsplatz geht. Zu den speziellen Problemen des **Eingliederungsmanagements**, das primär vorhandene Informationen auswertet, s. unten Rn 399a ff.

2. Zulässigkeit von Gentests?

285 Die grundsätzliche Unzulässigkeit gentechnischer Untersuchungen gegenüber Bewerbern⁵³ gilt in gleicher Weise auch gegenüber bereits Beschäftigten. Auf die obigen Ausführungen kann daher verwiesen werden.⁴

286 **Auch zur Feststellung der Identität sind gentechnische Verfahren nicht erlaubt.** Dies gilt auch dann, wenn es um die Aufklärung einer schweren Pflichtverletzung oder einer Straftat im Betrieb geht. Mit Recht hat der VGH Baden-Württemberg in der im Eingangskapitel genannten Entscheidung⁵⁴ den Standpunkt vertreten, dass in einem solchen Fall ein überwiegendes Interesse des Arbeitnehmers bestehe, von einer DNA-Analyse seiner Körperzellen verschont zu bleiben. Dies gelte trotz des berechtigten und schutzwürdigen Informationsinteresses des Arbeitgebers. Die im Strafverfahrensrecht vorgesehenen Eingriffsmöglichkeiten stünden Privaten nicht zur Verfügung.^{54a} Im Ergebnis wurde daher mit Recht ein **Verwertungsverbot** angenommen, was der beabsichtigten Kündigung des Personalratsmitglieds die Grundlage entzog.⁵⁵

V. Erfassung biometrischer Merkmale

287 In der Praxis gibt es den Versuch, Arbeitnehmer mit Hilfe bestimmter körperlicher Merkmale zu identifizieren. Dies kann ein **Fingerabdruck** sein, eine bestimmte Form und Farbe der **Iris** oder auch ein bestimmter Zuschnitt des Gesichts. Daneben wird bisweilen auf die **Stimme** oder auf die Schrift abgehoben.⁵ In allen Fällen lässt sich eine wirksame Identitätskontrolle durchführen, die insbesondere beim Zugang zum Betrieb, aber auch zu Informationssystemen (Fingerabdruck statt Passwort beim PC) zum Einsatz gelangt.⁶ Zusammenfassend ist von biometrischen Merkmalen die Rede. Im Arbeitsleben kommt ihnen wachsende Bedeutung zu.⁷

288 Die Erfassung derartiger Daten bringt **erhebliche Risiken** mit sich. Nicht nur, dass in manchen Fällen die »Gesichtskontrolle« ohne Wissen des Betroffenen erfolgen kann – viel wichtiger ist die **Dauerhaftigkeit der erhobenen Daten**. Da sie den betreffenden Menschen ein Leben lang charakterisieren, kann auf sie noch nach 30 oder 50 Jahren zurückgegriffen werden. In vielen Fällen ergeben sich überdies sog. **überschießende Informationen**; dem Gesichtsausdruck oder der Stimme kann der körperliche Zustand wie auch die psychische Verfassung zu entnehmen sein. Von daher haben derartige Daten einen hoch sensiblen Charakter.⁵⁶ Um sensitive Daten im Sinne des § 3 Abs. 9 BDSG handelt es sich nur, wenn im Einzelfall Rückschlüsse auf die Rasse oder den Gesundheitszustand möglich sind. Sofern dies wie beim Fingerabdruck von vorneherein ausscheidet, gelten lediglich die allgemeinen Regeln.

289 Das BDSG enthält **kein Verbot**, derartige Daten zu erfassen. Bemerkenswert ist allerdings, dass der österreichische Oberste Gerichtshof den Standpunkt vertritt, durch biometrische Kontrollverfahren sei die Menschenwürde berührt, so dass der Betriebsrat über das normale Mitbestimmungsrecht hinaus ein (im Gesetz vorgesehenes) Vetorecht habe, das auch durch den Schlichtungsausschuss nicht ausgeräumt werden könne.⁸ Insofern muss auf die allgemeinen Erhebungsvoraussetzungen nach § 32 Abs. 1 Satz 1 BDSG zurückgegriffen werden. Dabei ist zu beachten, dass **nur im Rahmen des Erforderlichen** in das informationelle Selbstbestimmungsrecht des Einzelnen eingegriffen werden darf.⁵⁷ Diese Voraussetzung ist

⁵²Zur Separierung der arbeitsmedizinischen Daten näher unten § 7 II 2 (Rn. 396ff.).

⁵³Dazu oben § 5 IV (Rn. 234 ff.).

⁴Oben Rn. 234 ff.

⁵⁴VGH Baden-Württemberg AuR 2001, 469, auch zum Folgenden.

^{54a}Zu den auch dort bestehenden Grenzen s. § 81h StPO sowie LVerfG Brandenburg DSB 5/2002, S. 21.

⁵⁵Dazu auch die Anm. von Roos AuR 2001, 470ff.

⁵Einzelheiten bei Tinnefeld/Ehmann/Gerling S. 658 ff.

⁶Weitere Verwendungsmöglichkeiten bei Hornung/Steidle AuR 2005, 201, 203

⁷Hornung AuR 2007, 400

⁵⁶Näher hamburgischer DSB, 18. TB, S. 3, 17ff.

⁸OGH AuR 2007, 398 mit Anm. Hornung/Steidle

⁵⁷S. oben § 3 IV 2 b (Rn. 115ff.).

nicht gegeben, wenn die **Fingerabdrücke** der Beschäftigten allein zu dem Zweck gespeichert werden, **im Falle von Straftaten** bessere Erkenntnismöglichkeiten zu haben.⁹ Auch das Ziel „Erfassung der Arbeitszeit“ kann keinen so weitreichenden Eingriff rechtfertigen.¹⁰ Auf der anderen Seite ist es ohne Bedeutung, wenn die Identifizierung per Fingerabdruck bei einem ganz kleinen Teil der Beschäftigten nicht funktioniert, weil die Betroffenen deshalb keine Nachteile zu befürchten haben.¹¹

Legt man dies zugrunde, so ist in erster Linie die Frage zu stellen, ob auch eine **andere Technik, die** nicht oder **weniger** in das informationelle Selbstbestimmungsrecht **eingreift**, denselben oder einen vergleichbaren Zweck erreichen könnte. Auch verpflichtet § 3a BDSG die verantwortliche Stelle, sich um die schonendste Form von Technik zu bemühen. Dabei ist auch danach zu fragen, welche Nachteile entstehen könnten, weil beispielsweise nur mit Zugangsausweisen (die natürlich verloren gehen oder gestohlen werden können) oder mit Passwörtern (die „verraten“ werden können) gearbeitet wird. Dies hängt von den jeweiligen Umständen ab, so dass sich eine generelle Aussage verbietet; nur im Einzelfall können maschinenlesbare Ausweise als milderes Mittel in Betracht kommen. Ist die Erfassung biometrischer Merkmale im Einzelfall unvermeidbar, ist in erster Linie daran zu denken, das **Referenzmaterial zu anonymisieren** und so beispielsweise beim Fingerabdruck nur zu überprüfen, ob eine Entsprechung in der Gesamtdatenbank aller zugangsberechtigten Personen gespeichert ist.¹² Außerdem ist auf alle Fälle zu vermeiden, dass die Betroffenen die Datenerfassung nicht bemerken, z. B. eine „Gesichtskontrolle“ im Vorbeigehen erfolgt.¹³ Weiter ist zu prüfen, ob die biometrische Zugangskontrolle nur für einen beschränkten besonders sensiblen Bereich praktiziert wird, im Übrigen (z. B. bei der Erfassung der Arbeitszeit) aber weniger eingreifende Methoden verwendet werden.¹⁴

291

Ein unzulässiges Übermaß stellt es auf alle Fälle dar, wenn die Erfassung der Merkmale so organisiert ist, dass automatisch auch **überschießende Informationen** z.B. über die Stimmungslage anfallen. Die Abgleichung der Gesichtsförmigkeit führt überdies dazu, dass in vielen Fällen die (vermeintliche) Rasse und damit ein sensibles Datum erfasst wird, was nur mit ausdrücklicher und freiwilliger Einwilligung des Betroffenen zulässig ist.¹⁵ Da dieser Effekt vom Zweck der Maßnahme her nicht geboten, sondern überflüssig ist, wäre diese daher insgesamt rechtswidrig.¹⁶ Ein besonderes Gefährdungspotenzial für die Betroffenen enthalten die sog. **Referenzdaten**, mit denen das Merkmal der konkreten Person abgeglichen wird. Bei ihnen ist die Datensicherung besonders ernst zu nehmen;¹⁶ auch darf eine Verknüpfung mit anderen Dateien nicht in Betracht kommen. Dem Betriebsrat steht bei allen Fragen der Anwendung biometrischer Verfahren ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG, aber auch nach § 87 Abs.1 Nr. 1 BetrVG zu.^{58a}

VI. Überwachung des Arbeitsverhaltens: Verdeckte Ermittler, Videokontrolle, Überwachungsprogramme, Bewegungsprofile

1. Nichttechnische Formen von Kontrolle

291
292

Dem Arbeitgeber steht es **grundsätzlich** frei, **die** Einhaltung der arbeitsvertraglichen Pflichten zu kontrollieren. Dies kann nicht nur durch einen »Blick über die Schulter«, sondern auch durch Rückfrage, Anfordern von Unterlagen, Konfrontation mit Fehlern usw. erfolgen. Eine solche Form von Datenerhebung liegt ohne jeden Zweifel innerhalb des durch § 32 Abs. 1 Satz 1 BDSG gezogenen Rahmens.

⁹ Gola/Wronka Rn 764; sie sprechen insoweit von einer unzulässigen Vorratsdatenspeicherung

¹⁰ Ebenso Hornung AuR 2007, 401 im Anschluss an den österreichischen OGH AuR 2007, 398

¹¹ Gola/Wronka Rn 766

¹² Ebenso Hornung/Steidle AuR 2005, 201, 206; Gola/Wronka Rn 765.

¹³ Hornung/Steidle AuR 2005, 201, 206

¹⁴ Hornung/Steidle AuR 2005, 201, 206

¹⁵ Hornung/Steidle AuR 2005, 201, 206

^{58a} Klebe, in: Däubler/Kittner/Klebe, § 94 Rn. 38.

^{58a} BAG AuR 2004, 106, 238 = DuD 2004, 433; ebenso ArbG Frankfurt/M. CF 6/2002, S. 29.

¹⁶ Hornung/Steidle AuR 2005, 201, 207

- 293 Keine Probleme ergeben sich auch dann, wenn sich Kontrollmaßnahmen nicht auf einzelne Arbeitnehmer oder einzelne Gruppen von Beschäftigten beziehen, sondern nur die »**Dienstleistungsqualität**« im **Allgemeinen** zum Gegenstand haben. Wird etwa die „Kundenorientierung“ einer Bank durch eine Drittfirma an zufällig ausgewählten Schaltern überprüft, ohne dass diese in dem fraglichen Bericht namhaft gemacht würden, ist der Persönlichkeitsschutz nicht im Spiel.⁵⁹
- 294 Die Situation ändert sich, wenn **der Betroffene bewusst im Unklaren gelassen wird, dass eine Kontrollmaßnahme stattfindet**. Dies gilt etwa beim Einsatz von **Detektiven**, der in der Praxis immer wichtiger wird.⁶⁰
- Die Rechtsprechung des BAG vermittelt **Anschauungsmaterial**. BAG DB 1986, 2187: Warenhausdetektiv stellt eine Arbeitnehmerin, die angeblich einen Lippenstift gestohlen hat; BAG DB 1987, 2420: Überprüfung, ob das Alkoholverbot im Betrieb eingehalten wird; BAG DB 1991, 1834: Als Kunden getarnte Detektive erscheinen mit nicht verkehrssicheren Autos beim TÜV, wo angeblich zu großzügig verfahren wurde.⁶¹
- Für die Beschäftigten tritt durch eine solche **heimliche Observation** ein ganz ähnlicher Effekt wie bei einer versteckten Kamera ein. Auch kennt man dasselbe Phänomen aus dem Strafprozessrecht, wo man diese Menschen als „**verdeckte Ermittler**“ bezeichnet. Ihr Einsatz ist nach § 110a StPO nur bei organisierter Kriminalität zulässig, bei der es insbesondere um terroristische Anschläge, um unerlaubter Drogen- und Waffenhandel sowie um Falschgeldproduktion geht.
- Der verdeckte Ermittler zeichnet sich gerade dadurch aus, dass er eine falsche Identität annimmt, sich wie die beobachteten Gruppenmitglieder verhält, dadurch im Rahmen des Möglichen ein Vertrauensverhältnis zu ihnen aufbaut und die so erlangten Informationen an die Strafverfolgungsbehörden weitergibt.¹⁷ Wenn berichtet wird, dass in einem Einzelhandelsunternehmen zwei Detektive als „Praktikanten“ eingeschleust wurden und heimlich zahlreiche Fotos von Beschäftigten machten, die sie dann samt ihren Berichten an die Firmenleitung weitergaben¹⁸ - wo besteht da ein prinzipieller Unterschied zu „verdeckten Ermittlern“?
- Will sich die Rechtsordnung nicht mit sich selbst in Widerspruch setzen, kann der Einsatz „getarnter“ Personen zur Aufklärung irgendwelcher kleiner Diebstähle oder arbeitsrechtlicher Unkorrektheiten nur als unzulässig behandelt werden. Die Situation ist insoweit keine andere als beim „betrieblichen Speicheltest“.⁶² Gäbe es den § 110a StPO nicht, könnte man solche Maßnahmen bei einem überwiegenden Arbeitgeberinteresse zulassen, dem auf keinem anderen Weg entsprochen werden kann. Dies wäre etwa dann der Fall, wenn dieses Vorgehen die einzige Möglichkeit wäre, weitere Straftaten erheblichen Umfangs zu verhindern.
- In den oben genannten Fällen war weder im Fall des Alkoholverbots noch in dem der möglicherweise großzügigen TÜV-Prüfer der Einsatz zu rechtfertigen.
- Das **BAG** hat die **Zulässigkeit** bisher **dahinstehen lassen**.⁶³
- 295 Nur unter Abwägung der beteiligten Interessen lässt sich die Frage entscheiden, ob der Arbeitgeber zu Kontrollzwecken dem Arbeitnehmer **eine »Falle« stellen** darf: Es wird beispielsweise unbemerkt Geld in die Kasse gelegt, um auf diese Weise die Ehrlichkeit der Kassiererin zu überprüfen.⁶⁴ Auch dies kommt nur dann in Betracht, wenn der Arbeitnehmer Anlass zu einer solchen Maßnahme gegeben hat, wenn beispielsweise unerklärbare Fehlbeträge in der Kasse aufgetreten sind.
- Beispiel:**
Im Betrieb ist einem bestimmten Mitarbeiter zwei Mal Geld gestohlen worden. Um den Täter, der aus dem Kollegenkreis stammen muss, zu überführen, werden die Geldscheine des »Opfers« mit einer chemischen Substanz präpariert, die sich von der Diebeshand nicht mit normalen Mitteln abwaschen lässt.⁶⁵
- 296 In praktisch allen Fällen unzulässig ist das **heimliche Mithörenlassen** einer anderen Person bei einem Personalgespräch;⁶⁶ allenfalls bei einer drohenden Erpressung könnte Anderes gelten.

⁵⁹S. den Fall BAG AP Nr. 33 zu § 87 BetrVG 1972 Überwachung.

⁶⁰Linnemann/Göpfert, DB 1997, 374ff.

⁶¹S. weiter ArbG Frankfurt und LAG Hamm AiB 1986, 212 mit Anm. Grimberg.

¹⁷ S. etwa als Anschauungsmaterial den Fall BVerwG NJW 1997, 2534, wo der Ermittler ein „freundschaftliches Vertrauensverhältnis“ zu den (zu Unrecht observierten) Personen aufgebaut hatte.

¹⁸ S. den Bericht in DANA 2008, 123.

⁶²S. oben Rn 286. Zur versteckten Kamera s. unten VI 2 b (Rn. 312).

⁶³BAG AP Nr. 21 zu § 87 BetrVG 1972 Überwachung = DB 1991, 1834.

⁶⁴S. der Fall BAG AP Nr. 32 zu § 626 BGB Verdacht strafbarer Handlung.

⁶⁵So der Fall BAG AP Nr. 5 zu § 87 BetrVG 1972 Ordnung des Betriebs.

⁶⁶BAG DB 1998, 371.

^{66a}Nach einer Pressemitteilung der Konferenz der Datenschutzbeauftragten von Bund und Ländern vom Okt. 2000 waren bereits zu diesem Zeitpunkt über 400 000 betriebliche Videoüberwachungsanlagen installiert – mitgeteilt bei Kloepfer, § 8 Fn 92 und bei Simitis-Bizer § 6b Rn.2. Von 500 000 Geräten spricht Schierbaum, CF 5/2002, S. 24. Inzwischen dürfte die Zahl weitaus höher liegen.

2. Videokontrolle

- 297 Der Einsatz von Videokameras ist nicht nur auf öffentlichen Plätzen eine immer häufigere Erscheinung; auch in den Betrieben breitet sich diese Technologie aus.^{66a} Eine solche Observationstechnik besitzt eine »besondere Eingriffsqualität«⁶⁷. Der Einzelne wird in seinen Verhaltensweisen einschl. seiner Bewegungen und seiner jeweiligen Stimmungen total 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, um so mehr ist das freie Verhalten des einzelnen und damit der Lebensnerv der Demokratie getroffen.⁶⁸ Auch vor der Intimsphäre wird bisweilen nicht Halt gemacht; so wird berichtet, dass die Videokontrolle in Schwimmbädern bis in die Umkleidekabinen hineinreiche.⁶⁹ Im Fall Lidl spielten verdeckte Kameras eine zentrale Rolle, doch gab es auch eine Reihe anderer derartiger „Überwachungsskandale“.¹⁹ Entgegen dem Anspruch des BVerfG⁷⁰ wird für den Einzelnen völlig unklar, wer was und bei welcher Gelegenheit über ihn erfahren hat.⁷¹
- 298 Der 2001 eingeführte § 6b BDSG regelt einen Teil der Probleme, nämlich die **Videouberwachung in öffentlich zugänglichen Räumen** und erfasst dabei auch den Einsatz durch nicht öffentliche Stellen. Für andere als öffentlich zugängliche Räume bleibt es bei einer „ungeregelten“ Situation, die de facto durch richterrechtliche Grundsätze ausgefüllt wird.⁷²
- a) Öffentlich zugängliche Räume
- 299 Die Regeln des § 6b BDSG sind nur anwendbar, wenn die Räume wie z.B. Ladenpassagen, Kaufhäuser, Gaststätten, Tankstellen und Bankfilialen öffentlich zugänglich sind. Die Tatsache, dass wie im Museum ein **Eintrittsgeld** bezahlt werden muss, ist **ohne Bedeutung**.⁷³ Irrelevant ist auch, wem das Gelände gehört, doch fehlt es ersichtlich an der öffentlichen Zugänglichkeit, wenn wie bei einem großen Mietshaus oder einem Bürogebäude üblicherweise nur Besucher aus besonderem Anlass kommen.⁷⁴
- 300 Eine Beobachtung solcher Räume mit »optisch-elektronischen Einrichtungen« (so die gesetzliche Umschreibung für Videouberwachung und sonstigen Kameraeinsatz²⁰) ist nach § 6b Abs. 1 BDSG **nur zulässig**, soweit (1) sich der Betreiber auf **bestimmte Gründe stützen** kann und (2) **keine Anhaltspunkte** bestehen, **dass schutzwürdige Interessen der Betroffenen überwiegen**. **Ohne Bedeutung** ist, ob **digitale oder analoge** Technik eingesetzt wird: Die Wirkung ist dieselbe, der Betroffene kann die Art der eingesetzten Technik nicht erkennen.²¹
- 301 § 6b Abs. 1 BDSG nennt in Nr. 1 die hier nicht näher interessierende »Aufgabenerfüllung öffentlicher Stellen«. Nr. 2 lässt alternativ dazu die »**Wahrnehmung des Hausrechts**« genügen, was dann praktische Bedeutung gewinnt, wenn ein Hausverbot auf andere Weise nicht durchgesetzt werden kann. Gibt es weniger einschneidende Mittel wie z. B. die Beobachtung der Eingänge durch Menschen, scheidet Nr. 2 aus.⁷⁵
- 302 Dritter und wichtigster Grund ist die Wahrnehmung berechtigter Interessen »**für konkret festgelegte Zwecke**«. Diese erst im Ausschuss eingefügte Formulierung will insbesondere ausschließen, dass schon eine Vermarktungsabsicht in Bezug auf die Videobilder oder die Wahl des Geschäftszwecks »Videouberwachung« zu einem »berechtigten Interesse« erklärt wird.⁷⁶ Inhaltlich geht es insbesondere

⁶⁷So der Bericht des Innenausschusses, BT-Dr. 14/5793 S. 61.

⁶⁸Bäumler, RDV 2001, 67f.

⁶⁹Hamburgischer DSB, 18. TB, S. 11.

¹⁹ S. oben Rn 2a ff.

⁷⁰Oben § 3 I (Rn. 78).

⁷¹Bäumler, RDV 2001, 69.

⁷²Christians, RDV-Sonderheft (BDSG-Novellierung) 2000, 15.

⁷³Königshofen, RDV 2001, 220.

⁷⁴Königshofen, RDV 2001, 220. Anders, wenn dort eine Ausstellung stattfindet: Schierbaum CF 6/2002, S. 26.

²⁰ Dazu Wedde, in: Däubler/Klebe/Wedde/Weichert § 6b Rn. 16 ff.

²¹ Simitis-Bizer § 6b Rn 36 unter Bezugnahme auf die amtliche Begründung. Selbst wenn es bei analoger Technik an der Entstehung einer Datei fehlen sollte, würde doch aus § 32 Abs.,2 deutlich, dass auch dieser Fall erfasst sein muss: Es wäre widersinnig, würde zwar eine handschriftliche Notiz, nicht aber ein analoger Videofilm dem BDSG unterliegen.

⁷⁵Tinnefeld, NJW 2001, 3082: Videokontrolle nur, wenn keine tauglichen Alternativen bestehen.

⁷⁶Gerhold/Heil, DuD 2001, 380; Hamburger DuD-Kommentierung zum BDSG, DuD 2002, 28, beide unter Bezugnahme auf BT-Dr. 14/5793 S. 61.

darum, die **Begehung von Diebstählen** oder anderen **strafbaren Handlungen** zu verhindern.⁷⁷ 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.⁷⁸

303 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.⁷⁹ Die schutzwürdigen Interessen der Betroffenen gebieten es weiter, die überwachten Bereiche nicht mehr als notwendig auszudehnen. 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. Um einen Zustand dauernden Überwachtseins zu vermeiden, will man selbst den Benutzern öffentlicher Verkehrsmittel das Recht einräumen, U-Bahn-Wagen ohne Kamera zu besteigen.⁸⁰

304 Der Eingriff in das allgemeine Persönlichkeitsrecht ist dann besonders gravierend, wenn die **Überwachung kontinuierlich** erfolgt und der Einzelne ihr nicht ausweichen kann. Am Beispiel eines Weges, der den alleinigen Zugang zu zwei Häusern vermittelte und der von einem der Nachbarn mit einer Videokamera permanent überwacht wurde, hat der BGH die damit verbundenen Auswirkungen einleuchtend geschildert:⁸¹

»Derartige Maßnahmen der Beklagten (kontinuierliche Videoaufnahmen – W. D.) bewirken eine schwerwiegende Beeinträchtigung des allgemeinen Persönlichkeitsrechts der Kläger. Diese müssen sich praktisch stets, wenn sie, von ihrem Haus kommend oder zu ihrem Haus gehend, den öffentlichen Zugangsweg benutzen, in einer jede ihrer Bewegungen geradezu dokumentierenden Weise kontrolliert fühlen. Auf dem jeweiligen Videofilm ist nicht nur festgehalten, wann, wie oft und in welcher Begleitung sie den Weg begangen haben, sondern auch in welcher Stimmung, mit welchem Gesichtsausdruck etc. sie dies getan haben. Die hierin liegende Beeinträchtigung der Kläger wird nicht dadurch gemindert, dass die Beklagte ihrem unwidersprochenen Vorbringen nach die Videoaufzeichnungen nach Überprüfung wieder löscht. Es kann nicht dem – für den Betroffenen letztlich gänzlich unkontrollierbaren – Belieben eines Anderen überlassen bleiben, wie er mit derart hergestellten Bildaufzeichnungen verfährt.«

Im Folgenden bleibt dann mangels ausreichender Anhaltspunkte dahinstehen, ob ein solches Vorgehen ausnahmsweise deshalb gerechtfertigt sein könnte, weil die Beobachteten im Verdacht stehen, regelmäßig Unrat auf das Grundstück des Beobachters zu werfen. Die Schilderung macht **schon auf der Grundlage des bisherigen Rechts** zwei Dinge deutlich:

305 Zum einen ist eine kontinuierliche Überwachung besonders belastend und deshalb **allenfalls dann zulässig, wenn sonst gravierende Nachteile** eintreten würden. Im Einzelfall wird daher meist nur eine stichprobenweise Kontrolle in Betracht kommen. Auch praktizieren Bankfilialen ihre Videoanlage meist in der Weise, dass sie erst in einer Bedrohungssituation durch Knopfdruck aktiviert wird.

306 Zum zweiten reicht ersichtlich die **abstrakte Gefahr der Begehung von Diebstählen** und anderen **Straftaten nicht** aus. Vielmehr muss entweder ein konkreter Verdacht gegen eine bestimmte Person bestehen oder aber müssen entsprechende Vorfälle bereits aufgetreten sein. Fehlt es an beidem, so überwiegen die schutzwürdigen Interessen der Betroffenen gegenüber dem Sicherheitsbedürfnis des Betreibers.⁸²

306a

Das **BDSG 2009** hat durch den neuen **§ 32 Abs.1 Satz 2** jeder Form der **Ermittlung von Straftaten** (und damit auch mit Hilfe der Videokontrolle) **engere Grenzen gezogen**. Zur „Aufdeckung“ von strafbaren Handlungen dürfen Beschäftigtendaten nur erhoben werden, „wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat.“ Voraussetzung ist weiter, dass die Erhebung zur Aufdeckung **erforderlich** ist und dass das **schutzwürdige Interesse des Betroffenen nicht überwiegt**, weil etwa Art und Ausmaß der Kontrolle im Hinblick auf den Anlass unverhältnismäßig sind. Dies bedeutet, dass ein abstrakter Verdacht („hier könnte geklaut werden“), aber auch eine konkrete Erfahrung („in diesem Raum sind Diebstähle vorgekommen“) als solche nicht ausreichen; vielmehr kann die Kamera nur eingesetzt werden, wenn es einen durch Tatsachen untermauerten **konkreten Verdacht gegen eine bestimmte Person** gibt. Damit ist § 6b Abs.1 Nr. 3 BDSG auf die Fälle reduziert, wo der Betroffene Anlass für eine solche Maßnahme gegeben hat und

⁷⁷Hamburger DuD-Kommentierung zum BDSG, DuD 2002, 28.

⁷⁸Hamburger DuD-Kommentierung zum BDSG, DuD 2002, 28. Vgl. auch Simitis-Bizer § 6b Rn 53.

⁷⁹BT-Dr. 14/5793, S. 62; Vahle, DSB Heft 2/2002, S. 17.

⁸⁰Hamburger DuD-Kommentierung zum BDSG, DuD 2002, 28.

⁸¹BGH NJW 1995, 1955, 1957.

⁸²Däubler, NZA 2001, 878.

die Videokontrolle ultima ratio ist. Erst recht muss ein solches Mittel ausscheiden, wenn es nur um **die Verletzung arbeitsvertraglicher Pflichten** wie langsames Arbeiten oder Unfreundlichkeit gegen Kunden geht.

307 Im Interesse eines Minimums an **Transparenz** schreibt § 6b Abs. 2 BDSG vor, dass der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen sind.⁸³ Der Hinweis kann durch Anbringung eines Piktogramms (also eines symbolischen Abbilds einer Kamera) und durch Benennung der verantwortlichen Stelle (»Kaufhaus GmbH«) erfolgen. Letzteres ist nur notwendig, wenn es nicht schon den Umständen nach evident ist.⁸⁴ § 6b Abs. 2 kennt keine Ausnahmen, was die hohe Bedeutung unterstreicht, die der Gesetzgeber dem Transparenzprinzip einräumen wollte.

308 Die Anwendung des § 6b Abs. 1 und 2 BDSG hängt nicht davon ab, dass die Videokamera Aufzeichnungen vornimmt; es genügt, wenn sie **lediglich Bilder auf einen Monitor** überträgt.⁸⁵ Wollte man anders entscheiden und nur Filmaufnahmen einbeziehen, würde die Vorschrift einen erheblichen Teil ihres Anwendungsbereichs verlieren. Da der Einzelne überdies nicht kontrollieren kann, ob die von der Kamera erfassten Vorgänge effektiv festgehalten werden oder nicht, wären Umgehungsmöglichkeiten in weitem Umfang eröffnet. Ein „Überwachungsdruck“ entsteht in beiden Fällen, ja sogar dann, wenn lediglich eine Attrappe aufgestellt wird.²²

309 Soweit personenbezogene Daten festgehalten werden, muss ihre **Verarbeitung und Nutzung** den Voraussetzungen des § 6b Abs. 3 Satz 1 BDSG entsprechen. Dabei ist erneut zu prüfen, ob Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. In Abweichung von § 28 Abs. 2 BDSG lässt überdies § 6b Abs. 3 Satz 2 eine Zweckänderung nur noch engeren Voraussetzungen zu: Sie ist nur möglich, soweit es »zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.«

Beispiel:

Die Überwachung der Ladenpassage hat den Zweck, das Erscheinen von bestimmten Personen mit »Hausverbot« sofort sichtbar zu machen und Gegenreaktionen auszulösen. Im Videofilm wird nun auch ein Raubüberfall festgehalten. Nach § 6b Abs. 3 Satz 2 ist eine Weitergabe an die Polizei zulässig.

310 § 6b Abs. 4 BDSG schreibt die **Benachrichtigung des Betroffenen** vor, wenn erhobene Daten einer bestimmten Person zugeordnet werden, wenn etwa festgestellt wird, dass der X zu einem bestimmten Zeitpunkt in der Bankfiliale Y war.

§ 6b Abs. 5 BDSG sieht unter erleichterten Voraussetzungen die **Löschung** einmal gespeicherter Daten vor.

b) Nicht öffentlich zugängliche Räume

311 Bei nicht öffentlich zugänglichen Räumen kann § 6b BDSG keine Anwendung finden, doch erlaubt er immerhin den Rückschluss, dass angesichts der von vorneherein gegebenen Überschaubarkeit des anwesenden Personenkreises die **Zulässigkeitsvoraussetzungen eher restriktiver** zu bestimmen sind. Dem tragen arbeitsrechtliche Rechtsprechung und Lehre in weitem Umfang Rechnung.

312 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 **generell unzulässig**.⁸⁶ Dasselbe gilt dann, wenn die Existenz der Kamera zwar bekannt, wenn sie jedoch **ohne konkreten Anlass jederzeit eingeschaltet** werden kann.⁸⁷ 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.⁸⁸ **Anders** ist die Situation nur dann, wenn ein **überwiegendes schutzwürdiges Interesse des Arbeitgebers** für eine solche Überwachung spricht, weil sie beispielsweise die einzige Möglichkeit darstellt, um erhebliche Warenverluste aufzuklären.⁸⁹ Dies hat das BAG durch Beschluss vom 26.8.2008²³ in der Weise konkretisiert, dass die

⁸³Gerhold/Heil, DuD 2001, 380.

⁸⁴Hamburger DuD-Kommentierung zum BDSG, DuD 2002, 29.

⁸⁵Hamburger DuD-Kommentierung zum BDSG, DuD 2002, 27; Simitis-Bizer § 6b Rn 37 unter Bezugnahme auf die amtliche Begründung, BT-Drucksache 14/4329, S. 38; a. A. Königshofen RDV 2001, 222.

²²Weshalb auch dann § 6b eingreift: Gola/Wronka Rn 731; Simitis-Bizer § 6b Rn 39; Wedde, in: Däubler/Klebe/Wedde/Weichert § 6b Rn. 18.

⁸⁶LAG Köln BB 1997, 476; LAG Baden-Württemberg BB 1999, 1439; Berg, in: Däubler/Kittner/Klebe/Wedde, § 75 Rn. 56; Schierbaum, CF 6/2002, S. 28.

⁸⁷BAG AP Nr. 15 zu § 611 BGB Persönlichkeitsrecht = NZA 1988, 92.

⁸⁸BAG AP Nr. 36 zu § 87 BetrVG 1972 Überwachung; Fitting, § 75 Rn. 149.

⁸⁹BAG AP Nr. 15 zu § 611 BGB Persönlichkeitsrecht = NZA 1988, 92.

Videokontrolle nur in Bezug auf solche Arbeitnehmer zulässig ist, gegen die **ein konkreter, auf Tatsachen gestützter Verdacht einer strafbaren Handlung** besteht.²⁴ Eine rein präventive Überwachung ist ausgeschlossen. Dies entspricht inhaltlich der neuen Regelung des **§ 32 Abs.1 Satz 2 BDSG**, die gleichfalls „tatsächliche Anhaltspunkte“ dafür verlangt, dass der Betroffene eine strafbare Handlung begangen hat.²⁵

313 Die unerlaubte Videoüberwachung⁹⁰ kann wegen Verletzung des allgemeinen Persönlichkeitsrechts zum **Schadensersatz** verpflichten. Das ArbG Frankfurt⁹¹ hat einem betroffenen Arbeitnehmer ein »**Schmerzensgeld**« in Höhe von 1300,00 DM zugesprochen, weil knapp zwei Monate lang ein Teil seines Arbeitsbereichs im Lebensmittellager (nicht aber sein Büro) von einer versteckten Videokamera überwacht worden war, von der weder er noch der Betriebsrat etwas wusste.⁹² Die Beschäftigten von Lidl, die von Überwachungsaktionen erfasst waren,²⁶ erhielten Presseberichten zufolge pro Person eine Entschädigung von 300 Euro.

c) Mitbestimmung

314 Unabhängig von der datenschutzrechtlichen Zulässigkeit einzelner Maßnahmen greift bei der Videokontrolle das Mitbestimmungsrecht des Betriebsrats nach **§ 87 Abs. 1 Nr. 6 BetrVG** bzw. das Mitbestimmungsrecht des Personalrats nach **§ 75 Abs. 3 Nr. 17 BPersVG** ein.⁹³ Dabei wird nicht zwischen öffentlich zugänglichen und nicht öffentlich zugänglichen Räumen unterschieden.

314a

Geht es um eine ausnahmsweise legale Aufklärung strafbarer Handlungen durch eine versteckte Kamera, so darf der **Betriebsrat** die Ermittlungen nicht dadurch unterlaufen, dass er **dem Verdächtigen einen „Tipp“** gibt. Dies würde auf einen Verrat eines Betriebs- und Geschäftsgeheimnisses nach **§ 78 BetrVG** hinauslaufen. Das Mitbestimmungsrecht ist deshalb nicht etwa suspendiert, weil es im Betriebsrat eine „undichte“ Stelle geben könnte. Richtet sich der **Verdacht gegen ein Betriebsratsmitglied**, kann auch dies die gesetzlichen Rechte des Organs als solches nicht beeinträchtigen. Will der Arbeitgeber einen „Warneffekt“ vermeiden, kann er Polizei und Staatsanwaltschaft einschalten; soweit diese einzelne Maßnahmen ergreifen, steht dem Betriebsrat kein Mitbestimmungsrecht zu.²⁷

3. Überwachungsprogramme

315 Auf dem Markt werden eine Reihe von Programmen angeboten, die es unschwer ermöglichen, in regelmäßigen Abständen **Screenshots** zu machen, d.h. den jeweiligen Bildschirminhalt festzuhalten, und **jeden Tastaturanschlag** zu erfassen. Dies kann durch eingebaute Kameras im PC oder im Laptop ergänzt werden.⁹⁵ Außerdem gibt es sog. **Trojanische Pferde**, die nach ihrer »Einnistung« das Mikrofon im PC aktivieren und so ein unproblematisches Mithören ermöglichen.⁹⁶ Durch ein kleines Zusatzgerät, das sich unschwer übers Internet beschaffen lässt, kann schließlich auch ein **Handy in ein Abhörgerät verwandelt** werden.⁹⁷

316 Soweit dies alles unbemerkt geschieht, dann aber doch irgendwie zu Tage kommt, ist die Rechtslage einfach: **§ 202a StGB** stellt das **Ausspähen von Daten** unter Strafe, **§ 201 Abs. 2 Satz 1 Nr. 1 StGB** tut dasselbe mit dem **unerlaubten Abhören**.

317 Die Strafsanktionen versagen jedoch dann, wenn der Beobachtete von den Maßnahmen informiert ist und – aus welchen Gründen auch immer – sein **Einverständnis** erklärt hat. In diesen Fällen stellt sich allein das Problem, ob eine Einwilligung einen so schweren Eingriff in die Persönlichkeitssphäre rechtfertigen kann.

²³ NZA 2008, 1187

²⁴ BAG NZA 2008, 1187, 1191 Tz. 31.

²⁵ S. oben Rn. 306

⁹⁰ Beispiel auch bei LAG Hamm RDV 2001, 288.

⁹¹ RDV 2001, 190.

⁹² Zur Bemessung des Schmerzensgelds bei Eingriffen in das allgemeine Persönlichkeitsrecht s. Däubler, BGB kompakt, Kap. 30 Rn. 83ff.

²⁶ S. oben Rn. 2a ff.

⁹³ Zum Mitbestimmungsrecht des Betriebsrats s. Klebe, in: Däubler/Kittner/Klebe, § 87 Rn. 123ff.; Tammen, RDV 2000, 15.

²⁷ BAG AP Nr. 5 zu § 87 BetrVG 1972 Ordnung des Betriebes

⁹⁵ Darstellung bei Bernhard/Ruhmann, CF Heft 12/2001 S. 13f.

⁹⁶ Beispiel in CF Heft 4/2001 S. 26.

⁹⁷ Mitgeteilt in CF Heft 3/2002 S. 3.

Die Frage ist eindeutig zu verneinen, da es sich entgegen den oben⁹⁸ dargelegten Anforderungen um **keinen** auch nur annäherungsweise **angemessenen Interessenausgleich** handelt. Selbst wenn der Arbeitgeber sich die Totalkontrolle einiges kosten lassen wollte, wäre eine solche „Kommerzialisierung der Person“ nicht hinnehmbar.

4. Erstellung eines Bewegungsprofils

- 318 Kontrolle über das soziale Verhalten eines Menschen kann nicht nur über Videokameras, über das Öffnen von Briefen oder das Mithören von Telefongesprächen erfolgen. Nicht weniger wichtig sind Informationen darüber, wer sich zu welchem Zeitpunkt an welchem Ort aufgehalten hat. Wollte man das Tun des Einzelnen nachträglich rekonstruieren, wäre dieses Element nicht weniger wichtig als die andern. Dies gilt auch für das Arbeitsleben: Die **relative Autonomie eines Außendienstmitarbeiters** geht verloren, wenn sich sein jeweiliger Aufenthaltsort präzise bestimmen lässt. Dies ist mit Hilfe von GPS oder Handy-Ortung unschwer möglich.²⁸ Theoretisch wäre auch denkbar, RFID-Technik in diesem Zusammenhang einzusetzen,²⁹ doch sind die anderen Wege bislang bei weitem vorherrschend. Auch die **Mitarbeiter in einem sicherheitsempfindlichen Betrieb** wie z. B. einem Kernkraftwerk können sich einer intensiven Kontrolle ausgesetzt sehen, wenn der Gang von Sicherheitszone 1 in Sicherheitszone 2 und von dort zur außerhalb der Sicherungsbereiche gelegenen Kantine sekundengenau erfasst und dasselbe für den Rückweg geschehen würde. Unschwer könnte ein Betroffener mit dem Vorhalt konfrontiert werden, er habe sich ein wenig lange im Sicherheitsbereich 2 aufgehalten.oder sei den Weg zur Kantine allzu gemächlich gegangen.
- 319 Aufgrund der bisherigen technischen Möglichkeiten bestand kein Anlass, außer dem gesprochenen Wort und der äußeren Erscheinungsform der Person auch den Aufenthaltsort vor unbefugter Erfassung zu schützen. **Durch moderne Techniken** wie GPS und die geschilderten Zugangskontrollsysteme hat sich jedoch die **Situation verändert**. Kann es auch jetzt noch erlaubt sein, den Aufenthaltsort des Einzelnen als relativ uninteressantes Datum zu behandeln?
- 320 Die Frage war lange Zeit wenig erörtert. Der hamburgische Datenschutzbeauftragte verwies als erster auf das Problem und schlug einen Schutz durch Einbeziehung in das Fernmeldegeheimnis vor.⁹⁹ Soweit ersichtlich, existiert Rechtsprechung nur im **Strafverfahrensrecht**, das als erstes die neuen technischen Möglichkeiten verarbeitet hat. Dort hält es der **BGH** auf der Grundlage des § 100c Abs. 1 Nr. 1b StPO a. F. für zulässig, dass der Standort und die Bewegung von Fahrzeugen mit Hilfe von GPS festgestellt werden; dies gelte auch dann, wenn daneben weitere technische Überwachungsmaßnahmen wie der Einsatz von Videokameras und die Telefonkontrolle nach § 100a StPO eingesetzt würden.¹⁰⁰ Der unantastbare Kernbereich der Privatsphäre und des informationellen Selbstbestimmungsrechts sei im konkreten Fall nicht berührt, da es um die Aufklärung von Sprengstoffanschlägen, und damit von besonders schweren Delikten gehe. Dies wurde vom BVerfG bestätigt.³⁰ Auch der **Standort eines Mobiltelefons** darf nach § 100i Abs. 1 Nr. 2 StPO ermittelt werden.¹⁰¹ Dies wurde vom BVerfG gleichfalls als gerechtfertigter Eingriff in das informationelle Selbstbestimmungsrecht gebilligt.³¹ Außerhalb dieses Bereichs ist die Erfassung von Standortdaten eines Mobilfunkgeräts nach § 98 Abs.1 Satz 1 TKG nur zulässig, wenn sie anonymisiert wurden oder der Betroffene einwilligt. Mitbenutzer müssen nach § 98 Abs.1 Satz 2 TKG von der Einwilligung in Kenntnis gesetzt werden.³² Entsprechende Einschränkungen für die Nutzung des GPS-Systems bestehen nicht.³³ Auf der Grundlage des hessischen Polizeirechts hat das VG Darmstadt eine Ortungsmaßnahme für rechtswidrig erklärt.¹⁰²
- 321 Wie in anderen Fällen steht auch hier ein Abwägungsproblem zur Debatte. Der vom BGH zu Recht konstatierte sehr weitgehende Eingriff in die Persönlichkeitssphäre mag im Interesse der Aufklärung von Sprengstoffdelikten und anderen Verbrechen gerechtfertigt sein, das **Interesse an der umfassenden Kontrolle des Arbeitsverhaltens reicht dafür bei weitem nicht aus**.

⁹⁸ § 3 IV (Rn. 117f.).

²⁸ Kiesche/Wilke CuA Heft7/2009. Man spricht insoweit von Location Based Services – dazu Steidle MMR 2009, S. 167 ff.

²⁹ Dazu unten Rn. 324a ff.

⁹⁹ Hamburgischer DSG 18. TB unter 1.1.3.

¹⁰⁰ BGH DSB Heft 3/2001 S. 17.

³⁰ BVerfG NJW 2005, 1338

¹⁰¹ Zur Möglichkeit, dies als Teil der Telefonüberwachung zu tun, s. BGH DSB Heft 4/2001 S. 19. Zur Technik des sog. IMSI-catchers s. Fox, DuD 2002, 212.

³¹ BVerfG NJW 2007, 351 ff.

³² Zu weiteren Einschränkungen s. die Informationen in RDV 2009, 136.

³³ Kiesche/Wilke CuA Heft 7/2009

¹⁰² VG Darmstadt NJW 2001, 2273.

- 322 Was zunächst die **Außendienstmitarbeiter** betrifft, so kann es ein legitimes Interesse geben, ihre jeweilige Erreichbarkeit sicherzustellen. Hierfür genügt, dass sie auf ihrem Handy angerufen werden können. Dabei kann ggf. auch der jeweilige Aufenthaltsort erfragt werden. Darüber hinaus wie mit einer im Weltraum stationierten Videokamera jeden Teil des Fahrverhaltens und jede Pause am Straßenrand oder auf einem Parkplatz zu erfassen, wäre eine **unzulässige »Totalkontrolle«**, die den Einzelnen zum Beobachtungsobjekt degradiert.³⁴ Die Situation ist insoweit keine andere als beim direkten Einsatz einer Videokameras, die ausschließlich das Arbeitsverhalten überwachen soll.¹⁰³ Was dort unzulässig ist, kann hier nicht akzeptabel sein. Der Eingriff in die Persönlichkeitssphäre ist unverhältnismäßig und deshalb rechtswidrig. Daraus kann man den Grundsatz herleiten, dass dem Einzelnen ein „**Aufenthaltsgeheimnis**“ zusteht, das nur in singulären Ausnahmefällen wie bei einem konkreten Verdacht einer strafbaren Handlung durchbrochen werden kann.³⁵ Auch die Möglichkeit, die Überwachungsgeräte auszuschalten, ändert an dieser Situation nichts, da der Arbeitnehmer Rückfragen gewärtigen muss, weshalb er so lange »abgetaucht« sei.
- 323 Im Prinzip gilt bei **betrieblichen Bewegungsprofilen** nichts Abweichendes. Anders sind lediglich die eingesetzten Techniken, wie das Beispiel der innerbetrieblichen Sicherheitszonen und der Überschreitung der Grenzen zwischen ihnen zeigt. Ähnliches könnte mit Hilfe der »Rufweitschaltung« beim Telefon erreicht werden, wenn ihre Aktivierung beim Verlassen des Büros obligatorisch ist und zugleich die Weisung besteht, sich grundsätzlich nur in Räume zu begeben, wo man auf Grund dieser Funktion erreichbar ist. Eine Ausnahme gilt insoweit allerdings für die Rundgänge der Wachpersonals, die für bestimmte Zeiten vorgeschrieben sind und die dokumentierbar sein müssen.
- 324 Unabhängig von der datenschutzrechtlichen Zulässigkeit besteht ein **Mitbestimmungsrecht** des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG bzw. des Personalrats nach § 75 Abs. 3 Nr. 17 BPersVG.

5. Kontrolle mit Hilfe von RFID-Technik

324a

RFID (=Radio Frequency Identification) ist derzeit auf dem Vormarsch. Die Systeme bestehen aus **zwei Komponenten**. Auf einer Ware (im Extremfall auch auf der Kleidung eines Menschen) ist ein „tag“, ein sog. Transponder angebracht. Es enthält einen Microchip, der bestimmte Daten gespeichert hat und sie bei Annäherung an ein Lesegerät (die zweite Komponente) an dieses übermittelt.³⁶ Anders als bei einem barcode ist dafür keine unmittelbare Nähe mehr erforderlich – 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) angewandt.³⁷

324b

Bisher ist der Einsatz von RFID vorwiegend im Zusammenhang mit dem Schutz des Verbrauchers diskutiert worden.³⁸ Der Metro-Konzern hat vor einigen Jahren einen **Supermarkt erprobt**, bei dem die gekauften Waren – ähnlich wie das Gepäck bei der Kontrolle am Flughafen – durch ein Band an einem Lesegerät vorbeitransportiert wurden, wo der Preis „ausgelesen“ und die Karte des Kunden belastet wurde.³⁹ Gleichzeitig wurde eine **Gesamtbetriebsvereinbarung** geschlossen, die betriebsbedingte Kündigungen verbot, auch wenn Kassiererinnen aufgrund der Bedienung des Systems durch Kunden überflüssig werden sollten.⁴⁰ Da **Kontrolle** über die Beschäftigten **möglich** ist (wenn beispielsweise der Warenfluss rekonstruiert wird und gleichzeitig bekannt ist, wer für einzelne Abschnitte verantwortlich war), unterliegt die Einführung und Anwendung von RFID-Systemen der Mitbestimmung des Betriebsrats. Dass sie gezielt als Kontrollmittel eingesetzt werden, ist im Moment nicht erkennbar. Allerdings kann es durchaus Fälle geben, in denen Mitarbeiter eines Wachdienstes bestimmte Punkte passieren müssen und dies nicht mehr durch Bedienung eines Schlüssels oder eines Knopfes, sondern mit Hilfe der RFID-Technik dokumentiert wird.⁴¹

³⁴ Ähnlich Gola NZA 2007, S. 1139, 1144.

¹⁰³ S. oben VI 2b (Rn. 312).

³⁵ Eingehender Däubler CF 7-8/2005 S. 42 ff.

³⁶ S. Holznapel/Schumacher MMR 2009, S. 3, 4. Er ist also „responder“ und dann „transmitter“, was zu dem Ausdruck „Transponder“ zusammengezogen wird.

³⁷ S. auch Kesten RDV 2008, 97 ff.

³⁸ S. neben Holznapel/Schumacher etwa Schmitz/Eckhardt CR 2007, 171 ff.

³⁹ Dazu Däubler dbr 6/2005, S. 30 ff.

⁴⁰ Die Betriebsvereinbarung ist abgedruckt in dbr 6/2005, S. 32 mit Einschätzungen von Mattheßen-Kreuder und Köster.

⁴¹ Gola NZA 2007, S. 1139, 1142.