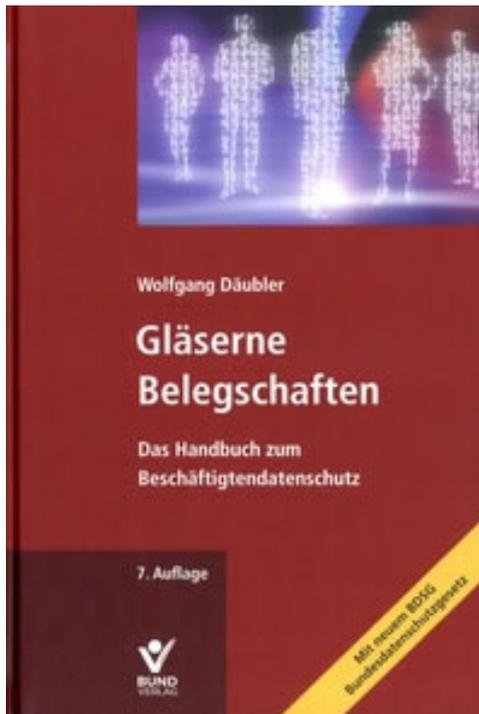


Gläserne Belegschaften

Das Handbuch zum Beschäftigtendatenschutz

Prof. Wolfgang Däubler



"Darf der Chef die E-Mails der Mitarbeiter lesen? Darf er Videokameras installieren? Dürfen Arbeitnehmerdaten irgendwo in der Cloud gespeichert werden? Wie verhalten sich Datenschutz und Compliance zueinander? Diese und andere Praxisfragen werden sich in Kürze nicht mehr nach dem gewohnten BDSG beantworten. Maßgebend ist stattdessen die EU-Datenschutz-Grundverordnung, die dem deutschen Recht vorgeht und die viele ungewohnte Regeln bringt. Glücklicherweise enthält sie auch eine Reihe von Öffnungsklauseln zugunsten des nationalen Gesetzgebers. Von ihnen macht das neue BDSG Gebrauch, das noch rechtzeitig vor den Wahlen verabschiedet wurde. Die „Gläsernen Belegschaften“ erläutern das neue Recht umfassend und in einer Weise,

die auch für den Nicht-Spezialisten nachvollziehbar ist. Das Buch gehört zu den ersten, die das neue BDSG einbeziehen. Insbesondere in § 26 enthält dieses eine Reihe von Vorschriften zum Beschäftigtendatenschutz, die für die Praxis von zentraler Bedeutung sein werden."

Verlagsinfo zum Buch von Wolfgang Däubler im Bund-Verlag (2017, 678 Seiten, gebunden, 7. Aufl., ISBN: 978-3-7663-6620-7, € 59,90).

Siehe [weitere Informationen sowie Vorwort](#) und hier nachfolgend **das Schlusswort "Perspektiven"** als Leseproben im LabourNet Germany - wir danken dem Autor und dem Verlag!

§ 17: Einige Perspektiven

I. Die permanente Reformdiskussion

935

Seit der Volkszählungsentscheidung vom 15. Dezember 1983¹ wurde mit guten Gründen eine Reform des Datenschutzrechts verlangt. Diskussionsgegenstand war dabei **nicht allein das BDSG als Querschnittsgesetz**; vielmehr ging es um die zahlreichen bereichsspezifischen Regelungen, die vom Ausländerzentralregister über die Sicherheitsüberprüfung bis hin zum Sozialdatenschutz und zum Beschäftigtendatenschutz reichen. Der Gesetzgeber hat sich jedoch fast durchweg auf das Nötigste beschränkt. Auch die Weiterentwicklung des BDSG 1977 über das BDSG 1990 hin zum BDSG 2001 und zur Reform 2009 hielt sich in engem Rahmen und vermied fast immer konzeptionell Neues.

936

Die **EG-Datenschutzrichtlinie** wurde **nicht** als **Impulsgeber**, sondern eher als lästiger Zwang wahrgenommen. Dass die Bundesrepublik die großzügig bemessene Umsetzungsfrist von drei Jahren um mehr als zweieinhalb Jahre überzog, vermag dies hinreichend zu illustrieren. Eine gewisse Ausnahme stellen lediglich die gesetzlichen Regelungen im Bereich der Telekommunikation dar.² Auf die Gründe wird zurückzukommen sein.

937

Besonders krass ist die Divergenz zwischen der Forderung nach modernen, problemadäquaten Lösungen und der **Situation des Beschäftigtendatenschutzes**. Unterschiedliche Bundesregierungen haben gesetzliche Regelungen versprochen.³ Erst im Jahre 2010 wurde ein Entwurf präsentiert, der zu einer Intensivierung der Diskussion führte. Im Frühjahr 2013 stellte sich jedoch weniger Enttäuschung als verbreitete Erleichterung ein, als die Koalition deutlich machte, das Vorhaben nicht weiter verfolgen zu wollen: Für Arbeitnehmer hätte sich eine Verschlechterung der Situation ergeben, aber auch die Arbeitgeberseite hätte Schwierigkeiten gehabt, sich mit einzelnen Bestimmungen wie dem totalen Verbot der heimlichen Videoüberwachung zu arrangieren.

938

Im Auftrag der Bundesregierung hatten schon vor über zehn Jahren drei Autoren ein Gutachten erstattet und eine Grundsatzreform des Datenschutzes vorgeschlagen. Dabei stellten sie auch zahlreiche Überlegungen zur Umsetzung an, so dass nicht von praxisferner Theorie die Rede sein konnte.⁴ Anlass für die Arbeit war, dass das BDSG 2001 als erste Stufe einer Datenschutzreform im Prinzip nur die EG-Richtlinie umsetzen wollte, während eine zweite Stufe eine »**Reform an Haupt und Gliedern**« vornehmen sollte.

939

In der jüngeren deutschen Rechtsentwicklung sind allerdings **keine Beispiele** erkennbar, in denen eine bis in viele Einzelfragen hinein ausdifferenzierte Regelung **durch einen Akt des Gesetzgebers von Grund auf umgestaltet** und auf eine neue Basis gestellt worden wäre. Ob es um ein Umweltgesetzbuch, ein Arbeitsvertragsgesetz oder eben den Datenschutz geht – zu mehr als Einzelregelungen oder systemimmanenten Weiterentwicklungen ist es nie gekommen. Auch die Schuldrechtsmodernisierung war als solche nur möglich, weil verschiedene EG-Richtlinien umzusetzen waren und ihre isolierte Ausführung noch mehr Friktionen in das eh schon alles andere als wertungsmäßig konsistente System hineingebracht hätte.⁵ Eine gewisse **Ausnahme** stellte (und stellt) das **Telekommunikationsrecht** dar, doch reagierte es auf eine im Grunde »ungeregelte« neue Situation, die nach der Auflösung des staatlichen Monopols entstanden war. Inhaltlich kam die Überlegung hinzu, nur durch konsequenten Datenschutz könnten Unternehmen auf Dauer im Bereich des E-Commerce erfolgreich sein. Von einer solchen Ausgangssituation her war es dann möglich, Neues zu schaffen und schon 1997 in § 3 Abs. 4 TDDSG den Systemdatenschutz zu verankern, in § 3 Abs. 3 TDDSG ein Koppelungsverbot bei der Einwilligung vorzusehen und in § 4 Abs. 4 TDDSG Nutzungsprofile nur bei der Verwendung von Pseudonymen zuzulassen.

¹ BVerfG 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1ff. = NJW 1984, 419.

² Oben Rn 325ff.

³ Überblick über die schon vor 2001 proklamierten Absichten bei Simitis, AuR 2001, 430.

⁴ Rossnagel/Pfützmann/Garstka, Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern, o. O., o.J. (2002); zusammenfassende Darstellung durch die Verf. in DuD 2001, 253ff. Zur Vereinbarkeit mit EG-Recht s. Brühann, DuD 2002, 296ff. Vgl. weiter Rossnagel, RDV 2002, 61ff.

⁵ Dazu Däubler-Gmelin, NJW 2001, 2286ff.; Canaris, DB 2001, 1815ff.

940

Die **Datenskandale** in zahlreichen bekannten Unternehmen, die seit Frühjahr 2008 ans Licht kamen,⁶ haben zu zahlreichen öffentlichen Forderungen nach einem besseren Beschäftigtendatenschutz geführt. Die **Oppositionsparteien** brachten verschiedene Gesetzesinitiativen ein,⁷ die jedoch an den bestehenden Mehrheitsverhältnissen scheiterten. Kurz vor der zweiten und dritten Lesung des Gesetzentwurfs der Bundesregierung »zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften«⁸ legten die Fraktionen von CDU/CSU und SPD einen gemeinsamen Änderungsantrag vor, der eine Reihe von kleineren Veränderungen zugunsten von mehr Beschäftigtendatenschutz brachte.⁹ Sie sind im Einzelnen oben verarbeitet worden.¹⁰ Bei allen übrigen Fragen werden weiter die Arbeitsgerichte in die Bresche springen und **richterrechtliche Sätze** für die in der Praxis auftauchenden Probleme entwickeln müssen.

II. Die DSGVO als Paukenschlag

941

Die am 18. Mai 2018 in Kraft tretende DSGVO hat weniger im materiellen Recht als **bei den flankierenden Maßnahmen neue Impulse** gesetzt: Die umfassende Dokumentationspflicht, die Datenschutz-Folgenabschätzung, das Gebot der „privacy by device“ und der „privacy by default“ (Art. 25) sowie die bei Verstößen drohenden Sanktionen¹¹ sind im Begriff, die Spielregeln in der Praxis zu verändern. Dazu kommen Einzelregelungen wie die Einbeziehung genetischer und biometrischer Daten in die sensitiven Daten nach Art. 9 DSGVO oder das weitgehende Koppelungsverbot bei der Einwilligung nach Art. 7 Abs. 4 DSGVO. Dazu kommt die Erweiterung des Anwendungsbereichs durch das **Marktortprinzip** des Art. 3 Abs. 2 DSGVO. Auf der anderen Seite existiert eine „**Verlustliste**“ im Verhältnis zum bisherigen deutschen Datenschutz, die z. B. den ausdrücklich garantierten Vorrang der Direkterhebung oder die absolute Zweckbindung der Daten betrifft, die aus der Datenschutzkontrolle und der Datensicherung entstehen (§ 31 BDSG a. F.).¹² In den kommenden Jahren wird außerdem ein **hohes Maß an Unsicherheit** bei allen Beteiligten bestehen, weil die DSGVO viele sehr allgemeine Begriffe verwendet, deren verbindliche Konkretisierung beim EuGH liegt.

942

Was speziell den **Beschäftigtendatenschutz** betrifft, so hat der Gesetzgeber von der Öffnungsklausel des Art. 88 DSGVO in Form des § 26 BDSG n. F. einen etwas umfangreicheren Gebrauch gemacht als zunächst beabsichtigt war. Dennoch ist etwa die Frage der Videoüberwachung in nicht öffentlich zugänglichen Räumen oder die Zulässigkeit der Erstellung von Bewegungsprofilen weiter der Rechtsprechung überlassen. Die Verwendung der Ergebnisse von Big-Data-Analysen in der Personalpolitik von Unternehmen ist durch das „Profiling“ nur angesprochen, nicht aber wirklich geregelt, da über den Extremfall des Art. 22 DSGVO hinaus keine Grenzen deutlich werden, die der Erfassung der menschlichen Persönlichkeit gezogen sind. Insoweit besteht ein hoher Interpretationsspielraum, der die künftigen Diskussionen beherrschen wird. Auch bleibt unklar, inwieweit der in Art. 1 Abs. 3 DSGVO betonte **freie Verkehr der Daten** innerhalb der Union eine Verbesserung des Beschäftigtendatenschutzes entgegensteht, also auch Daten betrifft, die primär die „geschlossene Einheit“ der Beziehung Beschäftigte – Arbeitgeber betrifft. Ihre spezifische Zweckbestimmung könnte einer Anwendung des Art. 1 Abs. 3 DSGVO entgegenstehen.

⁶ S. oben Rn 2a ff.

⁷ Vgl. etwa Antrag der FDP-Fraktion: Schutz von Arbeitnehmerdaten durch transparente und praxisgerechte Regelungen gesetzlich absichern (BT-Drucksache 16/12670); Antrag der Fraktion Bündnis 90/DIE GRÜNEN: Persönlichkeitsrechte abhängig Beschäftigter sichern – Datenschutz am Arbeitsplatz stärken (BT-Drucksache 16/9311); Antrag der Fraktion DIE LINKE: Datenschutz für Beschäftigte stärken (BT-Drucksache 16/11376)

⁸ BT-Drucksache 16/12011

⁹ BT-Drucksache 16/13657

¹⁰ S. etwa zu § 32 BDSG oben Rn 182a ff., zur Stellung des betrieblichen Datenschutzbeauftragten oben Rn. 607a ff. und 614ff.; zu den Befugnissen der Aufsichtsbehörde s. oben Rn. 623a

¹¹ Zu allem s. den Überblick oben in § 12

¹² Weitere Verluste bei Roßnagel-Roßnagel § 1 Rn. 11

III. Datenschutz als Wettbewerbsfaktor

943

In einem Bereich sollte auch unter den gegebenen Umständen eine deutliche Weiterentwicklung möglich sein. Je mehr sich geschäftliche wie private Kommunikation elektronischer Mittel bedient,¹³ umso stärker wird das Bedürfnis der Individuen, zumindest bestimmte Teile ihres Informationsaustausches vertraulich zu gestalten. Wer als Verbraucher nicht sicher sein kann, dass andere seine Kreditkartennummer diskret behandeln, wird sich voraussichtlich dem E-Commerce verweigern (und dabei die einfachste Form des Selbst Datenschutzes praktizieren).¹⁴ Mängel im Datenschutz erweisen sich so als Standortnachteil. **Datenschützer und Unternehmen sehen sich als Verbündete.**

944

Im BDSG 2001 hatte dieser Gedanke einen gesetzlichen Niederschlag gefunden, wenn auch in höchst vorsichtiger Weise. In Anlehnung an das Umwelt-Audit sah § 9a Satz 1 BDSG ein **Datenschutz-Audit** vor: Danach konnten Anbieter von Datenverarbeitungssystemen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zertifizierte Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Ein datenschutzrechtliches Gütesiegel sollte die Kommunikation und damit auch den geschäftlichen Erfolg erleichtern nach dem Motto: **Mit zertifizierten Partnern verhandelt sich's besser.**¹⁵ Auch wird die Auftragsdatenverarbeitung entscheidend erleichtert, wenn der Auftragsverarbeiter von unabhängigen Stellen als seriös und verlässlich eingestuft wurde.¹⁶

945

Dieser Grundsatzentscheidung folgte jedoch in § 9a Satz 2 BDSG eine entscheidende **Einschränkung**: Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie (insbesondere) die Auswahl und Zulassung der Gutachter müssen durch besonderes Gesetz geregelt werden. Einen entsprechenden Entwurf hatte die Bundesregierung im Parlament eingebracht,¹⁷ ließ ihn jedoch 2009 aufgrund zahlreicher nicht unberechtigter Einwände wieder fallen.¹⁸ Seither wird dieses Konzept jedenfalls auf Bundesebene nicht mehr weiterverfolgt. Stattdessen wurde eine »Stiftung Datenschutz« gegründet, die sich (auch) um das Datenschutzaudit kümmern soll, doch ist Näheres derzeit noch nicht entschieden.¹⁹ Die europäische Entwicklung ist unsicher.²⁰

946

In **Schleswig-Holstein** (und in Bremen) existiert allerdings seit vielen Jahren eine Datenschutz-Audit-Regelung,²¹ die Modellcharakter gewinnen könnte. Sie hat dazu geführt, dass am 18. Januar 2002 der Landrat des Kreises Ostholstein erstmalig in Deutschland ein »Datenschutz-Audit-Zertifikat« erhalten hat, das vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein verliehen wurde.²² Auf diesem Wege fortzufahren und so ein wenig mehr Transparenz auf dem Markt zu schaffen, erscheint **nicht nur im Verbraucherinteresse sinnvoll.**²³ Anbieter und Allgemeinheit müssten sich mit solchen Überlegungen ebenfalls anfreunden können.²⁴ In der näheren Zukunft wird es primär darum gehen, wie mit den Zertifizierungsmöglichkeiten nach der DSGVO umgegangen wird.²⁵

947

Auch auf einer anderen Ebene kann das Wettbewerbsrecht einen gewissen Beitrag zur Verbesserung des Datenschutzes leisten. Angebote, die auf einer Verletzung von Datenschutzrecht beruhen, **verstoßen gegen § 3 UWG** und müssen deshalb über kurz oder lang wieder vom (offiziellen) Markt verschwinden.²⁶ Auch das **OLG**

¹³ S. oben § 2.

¹⁴ Auf den zunehmenden Personalisierungsgrad in der Kundenbetreuung verweist zu Recht Büllesbach, RDV 2002, 55; vgl. weiter Weichert, DuD 2001, 265.

¹⁵ Dazu etwa Bäuml, RDV 2001, 167ff. und DuD 2002, 325ff.; Gerhold/Heil, DuD 2001, 378; Kloepfer, § 8 Rn. 91; Wedde/Schröder, AiB 2001, 284.

¹⁶ Mester DuD 2014, 198

¹⁷ BT-Drucksache 16/12011. Übersicht über die Regelungsinhalte bei Schultze-Melling in: Taeger/Gabel § 9a Rn. 11ff.

¹⁸ BT-Drucksache 16/13657

¹⁹ Mester DuD 2014, 198; Schultze-Melling in: Taeger/Gabel, § 9a En. 10

²⁰ Zu den dabei verfolgten Ansätzen s. Hornung/Hartl ZD 2014, 219ff.

²¹ § 43 Abs. 2 LDSG.

²² Mitgeteilt in DuD 2002, 132.

²³ S. Weichert, DuD 2001, 284: Datenschutz als Verbraucherschutz.

²⁴ Zur (wenig überzeugenden) Alternative eines Rating s. Kladroba, DuD 2002, 335ff.

²⁵ Dazu oben § 12 III 2 (Rn. 585)

²⁶ S. OLG Köln 10.11.2000 – 6 U 105/00, RDV 2001, 103 für den (damals) rechtswidrigen Vertrieb »umgekehrter« Telefonbücher.

Frankfurt/M.²⁷ vertrat den Standpunkt, ein Verstoß gegen das informationelle Selbstbestimmungsrecht mache ein **Informationsangebot sittenwidrig**, so dass es vom Markt verdrängt werden könne. Niemand wird erwarten, dass die **Klagen von Konkurrenten oder Verbraucherverbänden** nach § 8 Abs.3 UWG zu einem zentralen Mittel der konsequenteren Umsetzung des Datenschutzrechts werden; dennoch sollte auch dieser **Weg nicht** von vorne herein **ungenutzt** bleiben.

948

Nach § 2 Abs. 2 Nr. 11 UKlaG zählt das **Datenschutzrecht** zu den **verbraucherschützenden Bestimmungen**, deren Verletzung mit Hilfe einer Unterlassungsklage bekämpft werden kann, zu deren Erhebung u. a. auch ein Verbraucherverband berechtigt ist. Von dieser Möglichkeit sollte mehr als bisher Gebrauch gemacht werden.²⁸

IV. Transparenz des Datenschutzrechts

949

Die **DSGVO** wie das **BDSG n. F.** sind zwar dem Grundsatz der Datentransparenz verpflichtet, von ihrer äußeren Erscheinungsform her jedoch das exakte **Gegenteil eines transparenten, bürgerfreundlichen Gesetzes**. Schon die Formulierungen des alten BDSG wurden als überkompliziert, scheinpräzise und widersprüchlich qualifiziert²⁹, eine Einschätzung, der man schwerlich widersprechen kann. Hinzu kommt, dass es zwar ein alle Bereiche umfassendes »Querschnittsgesetz« war, dass seine Grundsätze jedoch keineswegs in allen Einzelbereichen galten. Die oben genannten Vorschriften zur Sicherheitsüberprüfung, bei denen die Individualrechte des Betroffenen weithin auf der Strecke bleiben,³⁰ sind dafür ebenso ein Beispiel wie die Sonderregeln im TMG, die in vieler Hinsicht den Einzelnen stärker als das **BDSG** schützen. Letzteres war deshalb **nicht** mit einem »**Allgemeinen Teil**« zu verwechseln; es stellte vielmehr eine **Auffangordnung** dar. Für jedes konkrete Problem war daher zunächst nach bereichsspezifischen Regeln zu suchen, ehe man sich dem BDSG mit seinen Interpretationsproblemen zuwenden konnte. Auch dies ist keine Normsetzungstechnik, die sich durch besondere Bürgerfreundlichkeit auszeichnet.

950

Trotz eines weitreichenden Konsenses in diesem Punkt³¹ war es nicht möglich, irgendwelche substanziellen Fortschritte zu machen. Eine rein **redaktionelle Überarbeitung** hätte zwar die Verständlichkeit erhöht, wäre jedoch immer dem Verdacht ausgesetzt, unter der Hand inhaltliche Änderungen vorzunehmen. Auch wäre das BDSG sehr viel umfangreicher geworden, hätte man einzelne Bestimmungen wie z. B. § 28 a. F. »entzerrt« und jede Phase der Datenverarbeitung der Transparenz wegen gesondert geregelt.

951

Die **DSGVO** hat die Dinge noch **weiter kompliziert**. An zahlreichen Stellen finden sich sprachliche Unschönheiten (um es höflich auszudrücken).³² Dazu kommt eine ungewohnte Terminologie, die sich oft durch **wenig trennscharfe Begriffe** auszeichnet. So ist etwa – um ein ganz einfaches Beispiel zu nennen – recht unklar, wann eine Regelung im „Beschäftigungskontext“ steht. Betrifft dieser auch den verbilligten Kauf eines Autos durch einen VW-Mitarbeiter, steht auch das Abitur im „Beschäftigungskontext“, weil es Voraussetzung für den Zugang zu bestimmten Berufen ist? Noch gravierender ist die Tatsache, dass viele konkrete Sachgebiete **sowohl in der DSGVO als auch im BDSG n. F. geregelt** sind. Grenzen der Informationspflicht des Verantwortlichen finden sich z. B. bei (indirekter) Erhebung sowohl in Art. 14 Abs. 3 DSGVO als auch in § 33 BDSG n. F. Die Regeln über die Einwilligung sind in der DSGVO an verschiedenen Stellen untergebracht, doch ist bei Beschäftigten zusätzlich noch § 26 Abs. 2 BDSG n. F. zu beachten. Hinzu kommt, dass die **DSGVO** anders als das BDSG a. F. kein susidiäres, nur hilfsweise eingreifendes Gesetz ist; Als Teil des Unionsrechts **geht sie dem gesamten nationalen Datenschutzrecht vor**. Dies schafft bei bereichsspezifischen Datenschutznormen wie z. B. dem Sozialdatenschutz oder dem Melderecht ein **erhebliches Maß an Anpassungsbedarf**, dem der Gesetzgeber mit einem besonderen Gesetz Rechnung tragen will.³³ Gegenüber

²⁷ 13.12.2000 – 13 U 204/98, RDV 2001, 131.

²⁸ Näher oben § 12 IX 3 (Rn. 624 ff.)

²⁹ Rossnagel/Pfitzmann/Garstka, DuD 2001, 254.

³⁰ S. oben § 16 (Rn. 882ff.).

³¹ S. bereits Tauss/Özdemir, RDV 2000, 143ff.

³² Beispiele: Oben Rn 42d und § 10 Fn. 60

³³ So heißt es in der Begründung zum BDSG n. F. (BT-Drucksache 18/11325 S. 69: „Weiterer gesetzlicher Anpassungsbedarf ergibt sich hinsichtlich der betehenden bereichsspezifischen Datenschutzregelungen des Bundes infolge der Änderungen im allgemeinen

diesen zu erwartenden bereichsspezifischen Regelungen kommt dem BDSG n. F. seinerseits nur subsidiäre Bedeutung zu (§ 1 Abs. 2 Satz 1 BDSG n. F.). Auch ein Index „Beschäftigtendatenschutz“ wie er im Weissbuch Arbeiten 4.0 vorgeschlagen wird,³⁴ könnte ein nützlicher Beitrag in dieser Richtung sein.

V. Die nicht (voll) bewältigten Probleme

949

Das eigentliche Dilemma des Persönlichkeitsschutzes und einer wirksamen Gesetzgebung liegt nicht in diesen »Alltagsproblemen« einer nicht zustande kommenden Reform. Viel wichtiger ist, dass es eine wachsende Zahl von Phänomenen gibt, für die noch keine spezifischen rechtlichen Lösungen entwickelt wurden. Die wichtigsten Stichworte seien genannt.³⁵

1. Cloud Computing

950

Cloud Computing ist mit einem **Kontrollverlust des Nutzers** verbunden: Er weiß nicht mehr, auf welchem Server sich seine Daten befinden und er kann erst recht nicht kontrollieren, ob von ihnen ein missbräuchlicher Gebrauch gemacht wird.³⁶ Liegt wie in der Regel ein Fall von Auftragsdatenverarbeitung vor, so gilt **Art. 28 DSGVO**, der die Einschaltung von Subunternehmern ,von bestimmten Voraussetzungen abhängig macht.³⁷ Ob diese effektiv zu einem sorgsamem Umgang mit den Daten führen, ist aus Sicht des Betroffenen reichlich unklar. Die Anwendungsfälle von cloud computing sind höchst vielfältiger Art; als Beispiel sei „Office 365“ genannt.³⁸ Der Zugriff US-amerikanischer Behörden ist im Regelfall selbst dann nicht ausgeschlossen, wenn der Speicherort in der EU liegt.³⁹

2. Big Data

951

Bestimmten Akteuren wie z.B. sozialen Netzwerken stehen riesige Datenmengen zur Verfügung. Aber es geht nicht nur um die Quantität von (Benutzer-)Daten. Vielmehr verfügen bestimmte Institutionen über die unterschiedlichsten Informationen, die vom Arbeitsverhalten über die Freizeit- und Kaufgewohnheiten bis hin zu politischen Präferenzen reichen. Hier lassen sich **beliebige Verknüpfungen** herstellen, die das Verhalten des Einzelnen umfassend abbilden. Dies mag zwar alles mit dem Zweckbindungsgrundsatz, dem informationellen Selbstbestimmungsrecht und Bestimmungen des Datenschutzrechts unvereinbar sein.⁴⁰ Gegen eine in irgendeinem Teil der Welt vorgenommene Auswertung lässt sich damit nicht ankämpfen; der **Anwendungsbereich des deutschen** (und des europäischen) **Datenschutzrechts** ist **begrenzt**.⁴¹ Von informationeller Gewaltenteilung ist man bei »Big Data« weit entfernt. Ein starker Betriebsrat kann möglicherweise in einem Unternehmen mit deutscher Spitze eine »Abkoppelung« der Beschäftigtendaten von solchen Auswertungsmöglichkeiten durchsetzen.⁴² Sobald sich die Spitze im Ausland befindet⁴³ (oder soweit es nicht mehr um Beschäftigtendaten geht), sind noch keine ausreichenden Konzepte entwickelt, wie man die

Datenschutzrecht durch die Verordnung (EU) 2016/679 und das sie ergänzende neu gefasste BDSG. Die hierzu erforderlichen Änderungen werden im Rahmen eines gesonderten Gesetzesvorhabens umgesetzt.“

³⁴ S. 150

³⁵ Zur Problematik des Datenschutzes unter den Bedingungen von Arbeit 4.0 s. oben § 14 V 6 (Rn. 837a ff.) sowie insbesondere Däubler, Internet und Arbeitsrecht, 5. Aufl. 2015 (6. Aufl. in Vorbereitung)

³⁶ Dazu oben Rn 7a und 507r

³⁷ Oben § 8 I (Rn. 436 ff.)

³⁸ Dazu Ruchhöft/Mösinger CuA Heft 9/2016 S. 8 ff. und Ruchhöft CuA Heft 9/2016 S. 13 ff.

³⁹ Maas/Schmitz/Wedde, S. 26

⁴⁰ Vgl. Schaar RDV 2013, 223ff.

⁴¹ Dazu oben § 9 II (Rn. 493ff.).

⁴² Brandt CuA 11/2013 S. 11. Zu darüber hinaus gehenden Ansätzen bei der Telekom s. Ulmer RDV 2013, 227ff.

⁴³ S. das Beispiel oben § 7 II 8 (Rn. 411a)

Persönlichkeit des Einzelnen schützen könnte.⁴⁴ Audits und Zertifizierungen sowie der Grundsatz der Datensparsamkeit⁴⁵ werden bei den »Systemherren« nur ein müdes Lächeln auslösen. Inwieweit sich auch im Unternehmen ein Wandel vollzieht, der die »Abkoppelung« von Beschäftigendaten erschwert oder ausschließt, ist derzeit nicht absehbar. Das Reden von der »**Industriearbeit 4.0**« ist erst wenig mit konkreten Inhalten verbunden und steht deshalb (wohl zu Unrecht) im Verdacht, ähnlich wie vor 15 Jahren CIM (=Computer Integrated Manufacturing) über eine Schlagwortexistenz nicht hinauszukommen.⁴⁶ Klar ist jedoch, dass durch die Digitalisierung der Arbeitsabläufe immer mehr Beschäftigendaten anfallen, die sich für die unterschiedlichsten Zwecke auswerten lassen. Da die Vernetzung mit anderen Unternehmen zunimmt, sind Beschäftigendaten auch nicht mehr auf das „Internum“ des Arbeitgeberunternehmens beschränkt.⁴⁷

3. Datenschutz im Internet

952

Die Diskussion um das »**Recht auf Vergessenwerden**« hat die Sensibilität der Öffentlichkeit für Datenschutz im Internet vergrößert. Dass es dabei immer nur um einzelne Schritte gehen kann, dass beispielsweise bestimmte Eintragungen nicht insgesamt aus dem Internet getilgt werden können, ist bereits betont worden.⁴⁸ Der Wegfall nationaler Grenzen im Internet bringt einerseits Informationsmöglichkeiten, die vor 30 Jahren undenkbar waren. Auf der anderen Seite entsteht eine Art rechtsfreier Raum, weil in vielen Teilen der Welt keine Staatsgewalt vorhanden ist, die bestimmte Regeln (so es sie denn gibt) durchsetzen würde.⁴⁹ Dies kann zu erheblichen Verletzungen der Persönlichkeitssphäre führen.⁵⁰ Dasselbe gilt für staatliche Zugriffe auf die Internet-Kommunikation, in Bezug auf die selbst die Vereinbarung eines internationalen Abkommens (»no spy«) verweigert wird. In der Zukunft kann die Frage nicht mehr ausgeklammert werden, dass wirksamer Datenschutz auf internationaler Ebene nur erreichbar ist, wenn mächtige Akteure auf einen Teil ihrer Privilegien verzichten.

Das Vertrauen in den Datenschutz ist eine wichtige Voraussetzung für die Akzeptanz der Digitalisierung in Wirtschaft und Arbeitswelt – dieser Feststellung im Weissbuch Arbeiten 4.0⁵¹ wird man schwerlich widersprechen können.

⁴⁴ Praktische Anwendungsfälle oben § 7 VII (Rn. 429 ff.)

⁴⁵ Weitere Vorschläge bei Roßnagel/Richter/Nebel ZD 2013, 103ff.

⁴⁶ Vgl. C. Kurz CuA 5/2014 S. 8ff.

⁴⁷ Vgl. auch Däubler, SR 2016 (Sonderheft) S. 3, 28 ff.

⁴⁸ Oben § 11 IV (Rn. 561b ff.)

⁴⁹ Weichert RDV 2013, 8, 10.

⁵⁰ Vgl. auch Weichert RDV 2013, 8, 14 zur Notwendigkeit internationaler Regelungen.

⁵¹ S. 147