Ingrid Maas/Karl Schmitz/Peter Wedde

Datenschutz 2014

Probleme und Lösungsmöglichkeiten

HSI-Schriftenreihe
Band 9

Ingrid Maas/Karl Schmitz/Peter Wedde

Datenschutz 2014

Probleme und Lösungsmöglichkeiten

BUND
VERLAG

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der
Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet
über http://dnb.d-nb.de abrufbar.

Herstellung: Kerstin Wilke
Umschlaggestaltung: Neil McBeath, Stuttgart
Satz und Druck: Beltz Bad Langensalza GmbH, Bad Langensalza
Printed in Germany 2014
ISBN 978-3-7663-6386-2

www.bund-verlag.de

Gutachten

Datenschutz 2014

Probleme und Lösungsmöglichkeiten

von

Ingrid Maas
Karl Schmitz
Prof. Dr. Peter Wedde

Januar 2014

Vorwort

Die Diskussion über Datenschutz in der Gesellschaft und im Arbeitsleben hat durch diverse Skandale, wie z. B. die NSA-Aktionen oder die Überwachung von Beschäftigten in großen deutschen Unternehmen, aber auch durch prognostizierte zukünftige Entwicklungen, wie Industrie 4.0, an Brisanz und Bedeutung nochmals erheblich zugenommen.

Das vorliegende Gutachten schildert mit einer Reihe von Beispielen, welche Flut von Daten im Arbeitsverhältnis entsteht und verarbeitet wird. Es zeigt, dass allein normative Regelungen zur Begrenzung und für einen wirksamen Schutz der Persönlichkeitsrechte der Beschäftigten nicht mehr ausreichen. Erforderlich sind auch technische Lösungen, die mit bestimmten Routinen Schutzstandards, wie z. B. Löschfristen, automatisch vorsehen. Damit wird die Richtung für ein zukunftsfähiges Datenschutzrecht deutlich neu definiert. Wir sind sicher, dass das Gutachten die weitere Diskussion über einen wirksameren Arbeitnehmer-Datenschutz wesentlich beeinflussen kann und sollte.

Dr. Thomas Klebe
(Leitung HSI)

Prof. Dr. Marlene Schmidt
(Leitung HSI)

Dr. Johannes Heuschmid
(Stellv. Leitung HSI)

Inhaltsverzeichnis

Vorwort 7

Einleitung 11

I. Anforderungen an ein zeitgemäßes Beschäftigten-Datenschutzrecht 13

- 1. Die veränderte Situation 13
- 2. Lokalisierung 13
  - a) Tablet-PC für einen Außendienst 14
  - b) Customer Relationship Management-Systeme 21
  - c) Flottensteuerung 23
  - d) Gerätetracking 23
- 3. Cloud Computing 25
- 4. Elektronische Kommunikation 28
  - a) Private Nutzung von Mail und Internet 28
  - b) Verbindungsdaten 31
  - c) Internet-Filter 32
  - d) Automatische Mailarchivierung 34
  - e) Telefonie und Videokonferencing 35
  - f) Kollaborationsmanagement 36
  - g) Social Media 37
  - h) Gesichtserkennung 40
  - i) Big Data 41
- 5. Anwendungen im Bereich der Beschäftigtendatenverarbeitung 42
  - a) Kompetenzmanagement 43
  - b) Talent Management und Succession Management 45
  - c) Performance Management 49
  - d) Apps für Personaldaten 52
  - e) Personaldaten und Datenschutz 54
- 6. Security 56
  - a) Konzepte struktureller Sicherheit 57
  - b) Remote Control-Funktionen 59
  - c) Intrusion Detection und Intrusion Prevention 59
  - d) Forensische Software 61

e) Compliance ... 63
f) Die Herausforderung der Computersicherheit an die Gesetzgebung ... 67
7. Ausblick ... 68
a) Die Ungnade des Nicht-Vergessens ... 69
b) Das Internet der Dinge ... 70

II. Rechtliche Rahmenbedingungen ... 73
1. Rechtsrahmen des Beschäftigtendatenschutzes nach dem BDSG ... 77
a) Verbotsgesetz mit Erlaubnisnormen ... 77
b) Datenvermeidung und Datensparsamkeit ... 78
c) Zwecke ... 78
d) Übermittlung von Beschäftigtendaten ... 79
e) Dauer ... 80
2. Kollektivrecht und Beschäftigtendatenschutz ... 80
a) § 75 Abs. 2 BetrVG – Schutz und Förderung von Persönlichkeitsrechten ... 80
b) Überwachung der Regelungen zum Beschäftigtendatenschutz als allgemeine Aufgabe des Betriebsrats ... 83
c) § 87 Abs. 1 Nr. 6 BetrVG – Schutz vor Verhaltens- und Leistungskontrollen durch Mitbestimmung ... 85
d) § 87 Abs. 1 Nr. 7 BetrVG – Gesundheitsschutz als Mittel des Beschäftigtendatenschutzes ... 88
e) Ergänzende Mitwirkungs- und Mitbestimmungsrechte ... 89
f) Probleme ... 90

III. Neue Strategien und Konzepte ... 93
1. Prozessorientierte Betriebsvereinbarungen ... 93
2. Datenschutzaudit ... 97
3. Einbindung betrieblicher Datenschutzbeauftragter ... 102
4. Sanktionsmaßnahmen ... 105
5. IT-Folgeabschätzung ... 107
a) Grundsätzliches ... 107
b) Vernetztes Denken ... 113

IV. Anforderungen an den Arbeitnehmer-Datenschutz ... 114

Literatur ... 119

Einleitung

Kaum eine Technik weist eine solch schnelle Änderungsrate auf wie die Informationstechnik. Wo die Erfindung der Drucktechnik noch jahrhundertelange soziale Anpassungsprozesse zur Folge hatte, zeigte sich bereits beim Telefon eine deutliche Beschleunigung des Tempos. Die Erfindung der Computer benötigte dann nur noch wenige Jahrzehnte, bis sie Prägungen des öffentlichen Lebens erkennen ließ. Heute erleben wir eine Turbobeschleunigung der sozialen Anpassungsprozesse durch das Internet und insbesondere seine mobile Nutzung.

Dem steht eine beachtenswerte Langsamkeit von Politik und Rechtsprechung entgegen, die dieser Entwicklung in keiner Weise angemessen Rechnung trägt. Die Datenschutzgesetze stammen konzeptionell aus einer Zeit, in der Datenverarbeitung in Rechenzentren stattfand und noch weit davon entfernt war, sich quasi in jeden Schritt des alltäglichen Lebens einzumischen, sei es privat oder in der Arbeit. Die derzeitige Situation ist gekennzeichnet durch mangelndes Schritthalten der politischen Willensbildung mit dem technischen Entwicklungstempo. Statt normenklarer, auch für den Bürger verständlicher Gesetze entstand eine unübersichtliche Normenmasse mit vielschichtigen Ablagerungen aus 40 Jahren Datenschutzgesetzgebung. Zur „Lösung“ politischer Probleme werden an das bestehende Datenschutzrecht einfach nur zusätzliche Einschränkungen, Ausnahmen und Rückausnahmen angeklebt. Mit jeder gesetzgeberischen Reaktion auf ein aktuelles Thema wird das Datenschutzrecht nur noch unverständlicher“.[1]

Oft bedarf es öffentlichkeitswirksamer Skandale, wie das systematische NSA-Überwachungs-Projekt PRISM der amerikanischen Regierung,[2] das Mitarbeiter-Screening bei der Deutschen Bahn[3] oder der massive Datendiebstahl bei der Telekom,[4] um wieder ein neues Stück Datenschutz-Flickwerk an den Wust der tausend schon bestehenden Regelungen anzufügen. Politische Entscheidungen

---

[1] Alexander Roßnagel: Nicht mehr zeitgemäß, Gastbeitrag in Frankfurter Allgemeine Zeitung vom 31. 5. 2011.

[2] Vgl. Neue Details zu PRISM, silicon.com vom 1. 7. 2013.

[3] Welt Online vom 27. 3. 2009: Deutsche Bahn ließ Journalisten-Mails überprüfen, Quelle www.welt.de/wirtschaft/article3455243

[4] Telekom bricht Postgeheimnis, Frankfurter Rundschau vom 5. 10. 2008.

werden – wenn überhaupt – erst in verspäteter Reaktion auf die technischen Umwälzungen getroffen. Die Konkretisierung und Interpretation der Gesetze durch die Rechtsprechung, insbesondere in Fragen des Datenschutzes, folgt ebenfalls diesem verspäteten Reaktionsmuster. Es entsteht Handlungsbedarf sowohl für die Gesetzgebung als auch für die Politik.

Aus der rasant voranschreitenden technischen Entwicklung leitet sich eine Fülle praktischer Probleme ab, die im derzeit geltenden Datenschutzrecht nicht abgebildet sind. Welche Anforderungen sich an ein längst überfälliges gesetzgeberisches Handeln hieraus ableiten, wird im Teil I dargestellt.

Mit Blick auf die unbefriedigende gesetzliche Situation wird im anschließenden Teil II der Rechtsrahmen beschrieben, der derzeit im arbeitsrechtlichen Bereich mit dem Ziel des Schutzes der Beschäftigten zur Anwendung kommt.

Hieran schließen sich im Teil III Hinweise auf technische und normative Lösungen an, die es ermöglichen sollen, die Einhaltung des datenschutzrechtlichen Schutzrahmens zu garantieren und Mitbestimmungsrechte von Betriebsräten zu optimieren.

I. Anforderungen an ein zeitgemäßes Beschäftigten-Datenschutzrecht

1. Die veränderte Situation

Die Erfindung des Personal Computers hat die Computer aus ihrem Inseldasein in abgeschirmten Rechenzentren herausgelöst. Ihre Miniaturisierung durch die Notebooks, Tablet-PCs und Smartphones hat sie sozusagen unters Volk gebracht. Doch erst die schnelle Verbreitung der Internetnutzung hat uns die heutige Allgegenwärtigkeit der Computer beschert. Die augenfälligste Eigenschaft des Internet ist die Vernetzbarkeit von allem mit allem. Ein wichtiges Element ist dabei die Funktelefonie, die die Computernutzung nahezu überall und ganz besonders auch außerhalb der Betriebe möglich macht.

Gleichzeitig werden immer mehr Mikroprozessoren in Gerätschaften aller Art eingebaut, seien es Küchengeräte oder die Kfz-Ausrüstung, so dass alltägliches Leben ohne Computer schier undenkbar geworden ist.

Im Folgenden sollen wichtige Anwendungen betrachtet werden, die von der fortgeschrittenen Technik umfassend Gebrauch machen, um anhand ihrer Nutzung alte und neu entstandene Datenschutzrecht-Problematiken zu erörtern. Wir beginnen mit einem Leistungsmerkmal, das den nicht weg zu denkenden Reiz vieler tagtäglicher Nutzungen ausmacht, der Lokalisierung.

2. Lokalisierung

Die Verbindung von Funktelefonie, Internet und miniaturisierter Hardware macht typische Anwendungen möglich, wie zum Beispiel Navigation, Tourenplanung, die Abfrage nach dem nächsten italienischen Restaurant auf dem SmartPhone oder dem Vorkommen seltener Vogelarten. Die meisten Menschen freuen sich darüber, diese schon selbstverständlich gewordenen Dinge für sich privat nutzen zu können. Und damit ist das entscheidende Stichwort gefallen, wenn es um den datenschutzrechtlichen Hintergrund geht: die private Nutzung. Die Neuerung wurde von vielen begrüßt, und niemand hatte damit ein Problem. Dennoch wurde das Thema durch einige Miniskandale in Mitleidenschaft gezogen.

Im Frühsommer 2012 hat die Firma Apple die in den iPhones gespeicherten Lokalisierungsdaten über das Einloggen in die Funktelefonnetz-Zellen aus den Geräten förmlich „abgesaugt“ und nach bis heute nicht widerlegten Gerüchten irgendwo auf ihren eigenen Servern gespeichert. Apple beteuerte, dass die Daten bei den „Verursachern“ für deren eigene Nutzung blieben. Diese hatten dem Vernehmen nach die ausschließliche Verfügungsgewalt über sie.

Eine Menge neuer Probleme tritt auf, wenn die Nutzung nicht mehr nur privat erfolgt, sondern sich mit der beruflichen Verwendung vermischt.

a) Tablet-PC für einen Außendienst

Im folgenden Beispiel werden in anonymisierter Form Entwicklungen aus international tätigen Unternehmen geschildert, die in umfangreicher Form von den technischen Neuentwicklungen Gebrauch machen.[5] Die Außendienstmitarbeiter wurden mit einem Tablet-PC ausgerüstet. Auf diesen Tablets sollte die Anwendung eines führenden Cloud-Anbieters laufen. Mit deren Unterstützung sollten die Außendienstmitarbeiter Arztbesuche planen und diese auch dokumentieren sowie persönliche Einschätzungen über die Kunden eintragen. So sollte z. B. die geschätzte Zahl der Patienten notiert werden, weiter ob der besuchte Arzt gerne viele Medikamente verschreibt, ob er dabei die Produkte des Unternehmens verwendet oder Konkurrenzprodukte vorzieht und ob er eher innovativ eingestellt, eher ein Praktiker oder eher ein Wissenschaftler ist. Das System sollte daraus dann nach einem im Programm hinterlegten Algorithmus eine „Kundenwertsegmentation“ berechnen und eine Klassifizierung in A-, B- oder C-Kunden vornehmen, aus der dann die Vorgaben für die Besuchsfrequenzen der Mitarbeiter abgeleitet würden. Außerdem sollten Daten gesammelt werden, die die „Reputation“ des Arztes beschreiben (z. B. Fachveröffentlichungen, Kongressteilnahmen u. Ä.).

Der Systemanbieter schien die Brisanz solcher Datensammlungen inzwischen auch zu erkennen und präsentierte das System ohne die bisher oft üblichen Freitextfelder, die die Benutzer für beliebig gestaltete Kommentare nutzen konnten. Wenn nur noch die „Options“ der Pull-Down-Menüs oder ankreuzbare Checkboxen zur Beschreibung verfügbar sind, bietet sich wenigstens die Möglichkeit, vor Einsatz des Systems auf datenschutzrechtliche Konformität der

---

[5] In dem Beispiel werden Erfahrungen aus verschiedenen Chemie- und Pharma-Konzernen zusammengefasst. Alle Anwendungen machen von der Miniaturisierung der Computertechnik, den Möglichkeiten zur Lokalisierung der Mitarbeiter-Standorte und der Methode des Cloud Computing sowie Führungsmethoden des Performance Managements Gebrauch.

erlaubten Items zu achten und beispielsweise alle Merkmale zu vermeiden, die diskriminierenden Charakter haben könnten. Hier entsteht eine ähnliche Situation wie bei den Textbausteinen eines Zeugnissystems, bei dem hinter freundlich klingenden, compliance-verträglichen Formulierungen andere Bedeutungen stehen, die von den Insidern, aber in der Regel nicht von den betroffenen Personen decodiert werden können.

Ferner sollten nach dem Wunsch des Unternehmens die Besuche mit einer in die Anwendung integrierten Tourenplanung geplant und später direkt vor Ort dokumentiert werden. Die Mitarbeiterinnen und Mitarbeiter sollten in einer Zielvereinbarung verpflichtet werden, die Produktpräsentationen des Unternehmens den Ärzten auf ihren Tablet-PCs vorzuführen. Dabei sollte die Dauer der Vorführung gemessen werden, um – so die Arbeitgeberseite – die Akzeptanz dieser neuen papierlosen Methode bei den Ärzten zu überprüfen. Die Auswertungen sollten dann im Zusammenhang mit einer persönlichen Beurteilung herangezogen werden, von der ein Teil des Jahresgehalts abhängen würde. Außerdem sollten die Besuche sowie die Verlässlichkeit der Planung ausgewertet werden (durch Vergleich der geplanten mit den stattgefundenen Terminen). Das Unternehmen möchte die jeweiligen Standorte der Außendienstmitarbeiter in der Zentrale abfragen können, um z. B. zur Befriedigung kurzfristig geäußerter Terminwünsche von Kunden den jeweils sich am nächsten befindlichen Mitarbeiter gezielt ansprechen zu können.

Die Anwendung sollte als „Software as a Service“ (SaaS) in der Public Cloud eines Anbieters mit Hauptsitz in den USA betrieben werden. Damit unterläge diese Angelegenheit auch US-amerikanischem Recht. Darüber kommt der Patriot Act[6] zur Anwendung. Das Anbieterunternehmen war zwar dem Safe Harbor-Abkommen, beigetreten, um die Übermittlung personenbezogener Daten überhaupt möglich zu machen.[7] Dabei handelt es sich aber bekanntermaßen nur

---

[6] Der Patriot Act („Gesetz zur Stärkung und Einigung Amerikas durch Bereitstellung geeigneter Instrumente, um Terrorismus aufzuhalten und zu blockieren“) wurde als direkte Reaktion auf die terroristischen Angriffe vom 11. September 2001 erlassen und ermöglicht unter Einschränkung der amerikanischen Grundrechte den amerikanischen Ermittlungsbehörden weitgehenden Zugriff auf sämtliche Kommunikationsdaten.

[7] Die EU-Datenschutzrichtlinie aus dem Jahr 1995 verbietet grundsätzlich die Übermittlung personenbezogener Daten in Länder ohne Datenschutzrecht. Da die USA über kein eigenes Datenschutzrecht verfügen, wurde mit dem sogenannten Safe Harbor-Abkommen Unternehmen die Möglichkeit geschaffen, auch personenbezogene Daten mit Stellen in den USA auszutauschen. In diesem Abkommen verpflichten sich die beigetretenen Unternehmen, der EU-Richtlinie vergleichbare Datenschutzstandards einzuhalten.

um eine freiwillige Verpflichtung.[8] Unabhängig von den Regeln des Safe Harbor-Abkommens bestehen die Mitbestimmungsrechte des Betriebsrats bezogen auf die Verwendung der Software nach dem Territorialitätsprinzip fort, wenn Betriebe und Unternehmen in Deutschland angesiedelt sind (vgl. hierzu Abschnitt II.2.f.).

Wegen der USA-Präsenz des Unternehmens hatte der Betriebsrat gefordert, dass die Anwendung in einer Private Cloud des Unternehmens betrieben werden müsse, d. h. in alleiniger Verantwortlichkeit der deutschen Holding des Konzerns.

Zahlreiche, insbesondere die von US-amerikanischen Herstellern vertriebenen Standard-Softwareprodukte haben die Eigenart, die Aktivitäten ihrer Benutzer für lange Zeitabschnitte sozusagen flächendeckend zu speichern. So erlaubt auch in diesem Fall die Anwendung im Rahmen ihrer eingebauten Kalenderfunktion die Dokumentation der Zeitpunkte aller Aktivitäten. Dies kann „in Echtzeit“ erfolgen, z. B. durch Drücken einer Taste für „Besuch begonnen“ und einer anderen Taste für „Besuch beendet“. Um eine kleinteilige Überwachungsmöglichkeit auszuschließen, hatte der Betriebsrat des Unternehmens gefordert, dass die Planung der Termine nur dem einzelnen Mitarbeiter als elektronisches Hilfsmittel zur Verfügung gestellt werden sollte und dass nur Beginn und Ende der Tagesarbeitszeit mit Uhrzeitangaben manuell erfasst würden, alle weiteren Aktivitäten aber nur ohne Uhrzeit- und Dauerangaben.

Bisher war die Benutzung einer Kalenderfunktion freiwillig. Dies sollte nun aufgegeben werden, damit nach den Vorstellungen der Arbeitgeberseite eine verlässlichere Planung auf Teamebene möglich wäre. Wenn einzelne Kollegen ihre Termine nicht im System notierten, hätten die Teamleiter keine Chance mehr, ihre Führungsaufgabe in diesem Zusammenhang wahrzunehmen, so die Argumentation der Arbeitgeberseite.

Eine über diese Aktivitätenerfassung hinausgehende Tourenplanung mit einem Zugriff auf die einzelnen Geräte von der Zentrale aus würde die Aufzeichnung

---

[8] Aufgrund dieses freiwilligen Charakters verlangt der sogenannte „Düsseldorfer Kreis“, ein Zusammenschluss der staatlichen Datenschutzaufsichtsbehörden in Deutschland, für „Safe Harbor“-zertifizierte Auftraggeber flankierende Maßnahmen; so dürften sich z. B. datenexportierende Unternehmen nicht mehr allein auf die Behauptung verlassen, dass eine solche Zertifizierung vorläge. Sie müssen sich vielmehr nachweisen lassen, dass die Grundsätze des Abkommens vom Anbieter der Software auch eingehalten werden. Vgl. Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover (überarbeitete Fassung vom 23. 8. 2010), elektronisch abrufbar unter www.bfdi.bund.de.

von Bewegungsprofilen ermöglichen und wurde deshalb vom Betriebsrat abgelehnt. Auch hier stand seitens des Betriebsrats die Forderung im Raum, eine Tourenplanung möglichst außerhalb der zentralen Außendienst-Anwendung, beispielsweise nur als eigenständige App, jedem einzelnen Mitarbeiter zur Verfügung zu stellen, mit der Maßgabe, dass nur eine Speicherung von Daten auf dem Gerät des Mitarbeiters erfolgen dürfte und dieser jederzeit die Historie der gespeicherten Tourendaten löschen können müsste.

Das Unternehmen hatte dagegen eingewendet, dass ein zunehmender Bedarf an zeitnaher Disposition entstünde, weil immer mehr Kunden sehr kurzfristige Anfragen stellen würden und man die Kollegen über Telefon nur umständlich erreichen würde. Es wurde ein Kompromiss vorgeschlagen, dass man in der Zentrale nur den augenblicklichen Standort der Außendienstler sehen könne und auf eine Speicherung der Historie verzichtet würde. Der Betriebsrat lehnte diesen Kompromiss ab und begründete seine Haltung mit der Unverhältnismäßigkeit des Eingriffs in die Persönlichkeitsrechte einerseits und der Zumutbarkeit für die Arbeitgeberseite andererseits, die Kommunikation telefonisch durchzuführen.

Die geschilderten Beispiele zeigen deutlich, wie „kleinteilig“ die Auseinandersetzungen um den Technikeinsatz ausfallen können. Seitens der Betriebsräte wurde beklagt, dass das bestehende Datenschutzrecht ihnen kaum Hilfe bot und sie sich allein auf die Gestaltungskompetenz des Mitbestimmungsrechts aus § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG)[9] stützen müssten. Weiter konstatierte der Betriebsrat, dass der Druck auf die Arbeitszeit zugenommen habe und von den Beschäftigten eine Erreichbarkeit weit über die bisher üblichen Arbeitszeiten hinaus erwartet würde. Die neuen Techniken entkoppeln die Arbeit vom Betrieb als Ort der Arbeit immer mehr, insbesondere die durch das Cloud Computing beförderte Nutzbarkeit der Computerleistung an beliebigen Orten. Daher hatte der Betriebsrat verlangt, dass die Beschäftigten nicht gezwungen werden dürften, während ihrer Außendiensttätigkeit die Dokumentation ihrer Kundenbesuche sofort vorzunehmen, sondern selber Ort und Zeitpunkt wählen dürften, wann und wo sie ihre Besuche dokumentieren.

Das Beispiel zeigt den zurzeit nicht gelösten Konflikt beim geplanten Cloud Computing zwischen den allgemeinen Vorgaben in der EU-Datenschutzrichtlinie und den sich hieraus ableitenden Festlegungen im deutschen auf der einen und im US-amerikanischen Recht auf der anderen Seite. Es macht ferner deut-

---

[9] Betriebsverfassungsgesetz (BetrVG) in der Fassung der Bekanntmachung vom 25. September 2001 (BGBl. I S. 2518), zuletzt geändert durch Artikel 3 Absatz 4 des Gesetzes vom 20. April 2013 (BGBl. I S. 868).

lich, dass die betriebliche Regelungsebene die einzige ist, um die bestehenden Probleme angemessen zu lösen. In der betrieblichen Praxis können insbesondere die im BetrVG verankerten Mitbestimmungsrechte dazu genutzt werden, den nach deutschem und europäischem Datenschutzrecht gegebenen Schutz gegen die Praktiken der US-Ermittlungsbehörden abzusichern und die technisch mögliche sehr kleinteilige Überwachung durch gleichzeitige automatische Erfassung von Ort und Zeitpunkt auf ein noch zumutbares Maß zu begrenzen.

Allerdings trifft die Sicherung des Datenschutzes durch Mitbestimmung auf Grenzen. So beinhaltet beispielsweise das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG[10] bezüglich der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten und die Leistung der Arbeitnehmer zu überwachen, keine direkte Möglichkeit, die Beachtung von allgemeinen datenschutzrechtlichen Vorgaben durch den Arbeitgeber sicherzustellen. Da das Mitbestimmungsrecht auf technische Einrichtungen zielt, lassen sich auf dieser Grundlage datenschutzrechtliche Fragen nur mittelbar regeln. Betriebsräte müssen nämlich bei der Wahrnehmung ihres Mitbestimmungsrechts nach § 87 Abs. 1 Nr. 6 BetrVG eine Ausgestaltung technischer Einrichtungen nicht akzeptieren, wenn deren Anwendung oder Einsatz gegen geltendes Datenschutzrecht verstößt. Datenschutzwidrige Ausgestaltungen können von Arbeitgebern auch nicht über eine Einigungsstelle erzwungen werden.[11]

Die Wahrung von Datenschutzrechten wird zudem durch den in § 75 Abs. 2 BetrVG verankerten Grundsatz unterstrichen, nach dem Arbeitgeber und Betriebsrat die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer schützen und fördern sollen. Die Kombination von § 87 Abs. 1 Nr. 6 BetrVG mit der Vorgabe in § 75 Abs. 2 BetrVG schafft damit einen Rahmen, durch den Datenschutzrechte auch ohne einschlägiges Mitbestimmungsrecht gesichert werden können.

Das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG besteht uneingeschränkt fort, wenn Arbeitgeber technische Einrichtungen an Auftragnehmer oder Dritte außerhalb ihres Betriebs oder Unternehmens verlagern. In diesen Fällen muss von Arbeitgebern durch vertragliche Regelungen mit den beauftragten Unternehmen sichergestellt werden, dass die Rechte der Betriebsräte uneingeschränkt ausgeübt werden können und dass der Gehalt von Betriebs-

---

[10] Vgl. ausführlich unter II.2.c

[11] Vgl. DKKW-Berg, § 75 Rn. 125.

vereinbarungen garantiert wird.[12] Auf dieser Grundlage können Betriebsräte für die Fälle, in denen Beschäftigtendaten außerhalb Deutschlands oder außerhalb der EU verarbeitet werden, von Arbeitgebern Regelungen verlangen, durch die datenschutzrechtliche Standards sichergestellt werden.

Darüber hinaus können Vorkehrungen zum Schutz vor Zugriffen staatlicher Überwachungsbehörden eingefordert und in Betriebsvereinbarungen verankert werden. Dies gilt auch, wenn nationales Recht von Staaten, in denen die technischen Einrichtungen vorgehalten werden, entsprechende Überwachungsmaßnahmen legitimiert. Nach der Rechtsprechung des BAG sind ausländische Vorschriften jedenfalls dann keine das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG ausschließenden gesetzlichen Regelungen, wenn es keine völkerrechtlich wirksame Transformation in das deutsche Arbeitsrecht gibt.[13]

Trotz der insoweit klaren juristischen Situation trifft die Sicherung der Mitbestimmung in der Praxis immer wieder auf das Problem, dass Unternehmen zu entsprechenden vertraglichen Vereinbarungen entweder nicht bereit sind oder dass sie getroffene Vereinbarungen nicht oder nur unzureichend durchsetzen. Betriebsräten bleibt in dieser Situation nur der mühsame Weg, Arbeitgeber in Beschlussverfahren dazu zu zwingen, rechtskonforme Zustände herzustellen. Dies macht tatsächlich ein sehr aufwändiges und kostspieliges Verfahren notwendig.

Um die in der Praxis bestehenden Regelungsdefizite zu beheben, sind Politik und Gesetzgebung gefordert, Abhilfe zu schaffen. Politisch ist durchzusetzen, dass auch im Rahmen von Arbeitsbeziehungen im Verhältnis zwischen Arbeitgebern und Arbeitnehmern US-amerikanisches Recht nicht deutsches oder EU-Recht „overrulen“ darf. Notwendig sind in diesem Zusammenhang insbesondere gesetzliche Vorgaben, durch die sichergestellt wird, dass bei der Verarbeitung und Nutzung von Daten innerhalb von Konzernstrukturen sowie in Auftragsverhältnissen ausschließlich Konzepte zum Einsatz kommen dürfen, die den Vorgaben der Europäischen Datenschutzrichtlinie bzw. dem deutschen Datenschutzrecht entsprechen, soweit hier weitergehende Vorgaben enthalten sind. In jedem Fall muss mit Blick auf § 4b Abs. 2 Satz 2 Bundesdatenschutzgesetz (BDSG)[14] ein angemessenes Datenschutzniveau gewährleistet werden.

---

[12] Vgl. etwa BAG vom 27. 1. 2004 – 1 ABR 7/03, NZA 2004, 556; grundlegend DKKW-Klebe, § 87 Rn. 21.

[13] Vgl. BAG vom 22. 7. 2008 – 1 ABR 40/07, NZA 2008, 1248.

[14] Bundesdatenschutzgesetz (BDSG) in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814).

US-Firmen wie Hewlett-Packard haben aus dem sich abzeichnenden Datenschutzproblem und dem hieraus folgenden Vertrauensdefizit längst Konsequenzen gezogen und sich deutsche Partnerfirmen gesucht, um mit deutschem Datenschutzrecht konforme Cloud-Lösungen anzubieten. Allerdings bleibt für Fälle wie diese zu prüfen, ob beispielsweise Zugriffe von Administratoren aus nicht EU-Ländern ausgeschlossen sind, die ihrerseits wiederum den Vorgaben des USA-Patriot-Act unterliegen könnten.

Der geschilderte Fall zeigt einen weiteren regelungsbedürftigen Aspekt auf, der aus den im BDSG enthaltenen Regelungen zur Einwilligung folgt. Das aktuelle Datenschutzrecht setzt durch die grundlegende Regelung in § 4 Abs. 1 BDSG voraus, dass keine Erhebung, Verarbeitung oder Nutzung ohne Vorliegen einer gesetzlichen Grundlage bzw. ohne Einwilligung der betroffenen Personen erfolgen darf. Da es für die vorstehend beschriebene Datenerhebung und -verarbeitung keine gesetzliche Grundlage gibt, ist diese nur auf Basis einer freiwilligen Einwilligung nach § 4a Abs. 1 BDSG möglich. Diese kann jederzeit zurück genommen werden, was aufgrund des Wegfalls des Rechtsgrunds für die Verarbeitung gemäß § 35 Abs. 2 Nr. 1 BDSG die Löschung der Daten zur Folge hat. Eben diese Löschung unterbleibt häufig in den angelegten personenbezogenen Datensammlungen.

Erfolgt die Erhebung, Verarbeitung und Nutzung personenbezogener Daten erstmals, müssen die betroffenen Personen nach § 4 Abs. 3 Nr. 2 BDSG insbesondere über die Zweckbestimmung der Erhebung, Verarbeitung und Nutzung informiert werden. Nach § 28 Abs. 1 Satz 2 BDSG sind darüber hinaus die Zwecke konkret festzulegen. Erfolgen Datenerhebungen ohne Kenntnis der betroffenen Personen, sind diese nach § 33 Abs. 1 Satz 1 BDSG über die Speicherung unter Nennung der Zweckbestimmung zu informieren. Gibt es für die Erhebung, Verarbeitung oder Nutzung keine Rechtsgrundlage nach § 4 Abs. 1 BDSG, können die Betroffenen die Löschung verlangen.

Trotz dieser eindeutigen datenschutzrechtlichen Situation ist zu erkennen, dass die Praxis diesen normativen Vorgaben nicht ausreichend nachkommt. In vielen Fällen wissen die betroffenen Personen von den sie betreffenden Datensammlungen nichts, weil die verantwortlichen Stellen ihren Informationspflichten nicht nachkommen. Um dieses Defizit zu beheben, müsste ein angemessenes Datenschutzrecht die Zulässigkeit der vorstehend beschriebenen Datenerhebungen und -verarbeitungen noch deutlicher als bisher davon abhängig machen, dass eine datenschutzrechtliche Erlaubnisnorm oder eine wirksame Einwilligung der Betroffenen vorliegt. Darüber hinaus müssten in das BDSG Sanktionsmechanismen eingefügt werden, die so schwerwiegend sind, dass verantwortliche Stellen dazu angehalten werden, sich rechtskonform zu verhalten. Neben deutlich erhöhten Bußgeldern und Strafandrohungen ist beispielsweise an eine Veröffentlichung von Datenschutzverstößen oder an einen Ausschluss von öffentlichen Aufträgen zu denken. Hinzukommen könnte eine Festschreibung zivilrechtlicher Schadensersatzansprüche der Betroffenen zu Lasten der verantwortlichen Stellen.

b) Customer Relationship Management-Systeme

Die in dem geschilderten Beispiel erhobenen Informationen sind typisch für Programme zum sog. Customer Relationship Management (CRM). Je detaillierter und je umfangreicher diese Informationen ausfallen, desto filigranere Marktanalysen sind möglich. Im System hinterlegte Algorithmen sollen entscheiden, mit welchem Material die in Zielgruppen eingeteilten Personen beliefert, wie oft sie besucht werden sollen, welches Ansprech-Programm der Außendienstler anzuwenden und was er minuziös zu dokumentieren hat. Das dahinter stehende Paradigma lässt sich nur so beschreiben, dass man den Marktteilnehmern mehr oder weniger standardisiertes Verhalten unterstellt, worauf dann ebenfalls in standardisierten Formen reagiert werden soll.

Solcherart automatisierte Geschäftspraktiken versprechen dann nur noch „Verbesserung“ durch weitere Differenzierung der Datensammelei, die sich von dem in § 3a BDSG proklamierten Grundsatz der Datensparsamkeit immer weiter entfernt.

Die erhobenen Daten stellen tiefe Einbrüche in die Persönlichkeitsrechte der „Zielpersonen“ dar, und es ist schwer vorstellbar, dass diese mit einer Datenerhebung einverstanden sind, die auch Bewertungen und Beurteilungen nicht scheut, zumal diese Bewertungen tendenziell sogar automatisiert erzeugt werden.

Für diese Art der Datenverarbeitung gibt es im Regelfall keine gesetzliche Grundlage. Sie ist nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG für die Begründung oder Durchführung eines rechtsgeschäftlichen Schuldverhältnisses nicht erforderlich. Soweit sie der Wahrung berechtigter Interessen nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG dienen soll, stehen der Zulässigkeit der Verarbeitung die schutzwürdigen Interessen der Betroffenen entgegen, deren Persönlichkeitsrechte durch diese Art des Umgangs mit personenbezogenen Daten in unzulässiger Weise tangiert werden. Problematisch ist, dass die Betroffenen von dieser Form der Datensammlung oft gar nichts wissen bzw. dass die Durchsetzung ihrer Rechte gegen die verantwortliche Stelle oft allein wegen des hiermit verbundenen Aufwands unterbleibt.

Ein künftiges Datenschutzrecht hätte auch darauf zu achten, dass zwischen den Grundsätzen der Zweckbindung und der Datensparsamkeit durch immer differenziertere und umfangreichere Datensammlungen kein Normenkonflikt entsteht. Dies impliziert, dass Verarbeitungszwecke so eng definiert werden müssen, so dass sie keinen Raum für auswuchernde Datensammlungen lassen.

Weiterhin müsste durch verbesserte Sanktionsmechanismen sichergestellt werden, dass unzulässige Datenerhebungen, -verarbeitungen und -nutzungen durch staatliche Stellen angemessen verfolgt und geahndet werden. Bezogen auf den arbeitsrechtlichen Kontext müsste darüber hinaus sichergestellt werden, dass Beschäftigte von ihren Arbeitgebern im Rahmen des Direktionsrechts nicht dazu aufgefordert werden dürfen, datenschutzwidrige Erhebungen, Verarbeitungen oder Nutzungen durchzuführen.

Firmen wie Amazon oder Google haben dazu beigetragen, dass die Sensibilität der Verbraucher gegenüber verhaltensbeschreibenden Daten abgenommen hat, finden es doch die meisten Menschen hilfreich, wenn ihnen bei einer Buchbestellung signalisiert wird, was andere Menschen, die dasselbe Buch gekauft haben, an ähnlichen Büchern auch noch erworben haben. Stutzig wird manch einer allerdings, wenn er daran erinnert wird, welches Buch er schon einmal vorübergehend in den elektronischen Einkaufskorb gelegt und doch nicht gekauft hat.

Den Firmen ist bei der Ausdifferenzierung ihrer auf Überwachung beruhenden Marktstrategien weder durch die Politik noch durch die Gesetzgebung eine Grenze gesetzt worden. So darf nicht verwundern, dass sie selber die Grenzen ausloten, wie weit sie gehen können. Bisher war es eher der Protest der betroffenen Personen, seien es nun die Verbraucher oder die Beschäftigten, der übereifrige Initiativen gestoppt hat. Dies hat z.B. der Widerstand aus der Bevölkerung gegen das Street View-Projekt von Google in Deutschland deutlich gezeigt.

Abhilfe darf erwartet werden, wenn die Datenschutz-Gesetzgebung deutlicher als bisher festlegt, dass die betroffenen Personen über jedwede Art von das Verhalten oder die Persönlichkeit beschreibender Information im Detail vorab zu informieren sind. Weiterhin müsste durch ein eindeutiges Opt-In-Modell abgesichert werden, dass die Erhebung, Verarbeitung und Nutzung von Daten verboten ist, solange keine freiwillige und eindeutige Einwilligung vorliegt. Schließlich müsste eine einfach handhabbare Möglichkeit angeboten werden, die erteilte Zustimmung jederzeit zu widerrufen, mit der automatischen Folge, dass die entsprechenden Daten unverzüglich gelöscht werden. Die geforderten Möglichkeiten müssten eindeutiger und klarer sein als das derzeit in § 28 Abs. 4 BDSG enthaltene Widerspruchskonzept. Zudem müssten Umgehungsmöglichkeiten und Ermessenstatbestände zugunsten der verantwortlichen Stellen ausgeschlossen werden.

c) Flottensteuerung

Ein Unternehmen hatte seine Warenauslieferer mit einer Flottensteuerungssoftware ausgestattet, sodass die Zentrale jederzeit einen Überblick darüber hatte, wo sich die Fahrzeuge gerade befunden haben. Dies traf auf heftigen Widerstand des Betriebsrats. Zur Lösung des Konflikts wurden zwei Modelle erörtert, ein Meilenstein- und ein Broadcasting-Verfahren.

Nach dem Meilenstein-Verfahren sollte das System so eingerichtet werden, dass die permanente Beobachtung durch die Zentrale abgeschaltet blieb und die Mitarbeiter von sich aus an definierten Punkten oder bei definierten Ereignissen (z. B. bei der Ablieferung der Ware beim Kunden) das System aktivieren und eine Statusmeldung absetzen konnten.

Das Broadcasting-Modell dagegen sah vor, dass nur bei Bedarf einer Ortung, z. B. bei Ausfall eines Fahrers zur Umdisponierung von Einsatzwagen, die Einsatzzentrale alle im Dienst befindlichen Wagen mit Angabe des Einsatzortes anfunken und – ähnlich einer Taxizentrale – die Fahrer auffordern würde, sich zu melden bzw. den Auftrag anzunehmen.

Die Regelungsidee bestand in beiden Fällen darin, dass die permanente Überwachung durch eine Stichproben-Überwachung ersetzt würde. Dies war bisher auf der betrieblichen Regelungsebene im Wesentlichen nur im Rahmen der Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG durchsetzbar.

Ein künftiges Datenschutzrecht sollte die schon jetzt in § 3a BDSG enthaltene Verpflichtung der Unternehmen verstärken, bei der Auswahl von Systemen nach einer Lösung zu suchen, die eine Minimierung der Überwachungseignung vorsieht. Der durch die Überwachung stattfindende Eingriff in das Persönlichkeitsrecht der betroffenen Personen wäre zusätzlich an die zwei folgenden Restriktionen zu binden:

- Eine im Rahmen der Prüfung der Erforderlichkeit stattfindende Interessenabwägung zwischen einer möglichen Verletzung des Persönlichkeitsrechts auf der einen und dem Erreichen wirtschaftlicher Ziele auf der anderen Seite hat dem Persönlichkeitsrecht Priorität zu gewähren.
- Ist ein Eingriff in das Persönlichkeitsrecht der Beschäftigten unumgänglich, muss dieser so schonend wie möglich sein. Insbesondere ist auszuschließen, dass dauerhafte Überwachungen stattfinden, wo punktuelle Überwachungen ausreichend sind.

d) Gerätetracking

Häufig anzutreffende Anwendungen sind auch der Einbau einer Ortungsfunktionalität in bewegliche Computer, um sie z. B. im Fall eines Diebstahls lokalisieren und auf ihr Innenleben zugreifen zu können. Hier sind jedoch schnell Grenzüberschreitungen möglich, wie die Vorfälle bei einem großen internationalen Elektronikkonzern deutlich machen. Wie in vielen solchen Unternehmen üblich, wurde die Betreuung der kompletten IT-Infrastruktur an einen Dienstleister ausgelagert. Dieses Outsourcing umfasste die Beschaffung und Wartung sämtlicher PCs und Notebooks sowie die Betreuung des kompletten Computernetzes. Die Computer-Herstellerfirma lieferte Notebooks aus, bei der eine verborgen bleibende Software installiert war; es handelte sich um das Produkt Computrance der US-amerikanischen Firma Absolute Software. Der Computerhersteller behauptete, dass normalerweise diese Software zwar installiert aber nicht freigeschaltet sei. Wenn ein Unternehmen ein Abonnement dieser Software kaufe, könne sie erweiterte Informationen wie Seriennummer, IP-Adresse und in regelmäßigen Abständen Lokalisierungsinformationen erfassen und an den Hersteller übermitteln, um die Computer überwachen zu lassen. Das Unternehmen machte gegenüber dem Konzernbetriebsrat die Aussage, dass ein solches Abonnement nicht gekauft worden sei. Weltweit waren davon einige tausend, in Deutschland einige hundert Rechner betroffen. Nach der Androhung gerichtlicher Schritte durch den deutschen Konzernbetriebsrat hatte das Unternehmen nochmals beteuert, dass keine Konzerngenehmigung für den Einsatz vorgelegen hätte und der Hersteller aufgefordert worden sei, alle übermittelten Daten unverzüglich zu löschen.

Es wurde dann vereinbart, dass nach einem zeitlich gestaffelten Stufenplan das Innenleben aller Rechner (sog. Images) korrigiert werden sollte. Dazu war ein Rückruf der Rechner erforderlich, um sie mit einem neuen Betriebssystem auszustatten. Weiter wurde die Einrichtung zusätzlicher Kontrollmaßnahmen vereinbart, um sicherzustellen, dass die Überwachungssoftware nicht in einer zukünftigen Image-Erstellung enthalten ist. Diese Kontrollmaßnahmen beinhalteten eine technische Spezifikation, die eine Überprüfung erlaubte, dass die beanstandete Software auch tatsächlich nicht installiert war.

Die „heimliche“ Installation von Überwachungssoftware ist ein immer wieder auftretendes Problem (wie schon bei dem iPhone-Tracker der Firma Apple im Jahr 2012). Es zeigt sich, wie wichtig die Verpflichtung zu einer Offenlegung solcher Installationen durch die Hersteller ist, deren Fehlen an ein Marktverbot gekoppelt werden sollte.

Die datenschutzrechtliche Fundierung einer solchen Forderung ist relativ unproblematisch, da die Nutzung „heimlicher“ Erhebungs- und Verarbeitungsmöglichkeiten mangels einer einschlägigen Erlaubnisnorm nach § 4 Abs. 1 BDSG schon heute unzulässig ist.

Hilfreich wären auch einfache Programme, die die „Außenverbindungen" eines Rechners für Endbenutzer auf deren Displays verständlich sichtbar machen, verbunden mit einer gesetzlichen Verpflichtung der Hersteller, normierte und allgemein verständliche Klartext-Bezeichnungen für die Verbindungen zusätzlich zu den technischen Spezifikationen zu verwenden.

Das Sanktionspotenzial des Konzernbetriebsrats bestand lediglich in der Drohung, den Unterlassungsanspruch wegen verletzter Mitbestimmungsrechte im Eilverfahren arbeitsgerichtlich durchzusetzen. In allen Fällen, in denen Persönlichkeitsrechte betroffen sind, sollte für den Fall nicht getroffener betrieblicher Regelungen der Unterlassungsanspruch des Betriebsrats gegenüber dem Unternehmen ausdrücklich formuliert werden. Für die normative Verankerung eines solchen Anspruchs bietet sich wegen des Sachzusammenhangs das BetrVG an. Möglich wäre aber auch eine Aufnahme in das BDSG.

Auf der individuellen Ebene ergänzt werden könnte der beschriebene Unterlassungsanspruch durch eine Art Verbandsklagerecht, das Betriebsräten direkt ermöglicht, im Auftrag von Beschäftigten gegen individuelle Verletzungen der Datenschutzrechte von Beschäftigten vorzugehen.

3. Cloud Computing

In den bisher beschriebenen Beispielen wurde schon weitgehend vom Cloud Computing Gebrauch gemacht. Grundsätzlich ist Cloud Computing nichts Neues. Es handelt sich dabei auch nur um eine Serverfarm, die – im Unterschied zu früheren traditionellen Lösungen – für internetfähige Anwendungen zur Verfügung steht und wegen der Verbindungsmöglichkeit über das Internet an beliebigen Orten nutzbar ist.

Es war ein genialer Marketing-Trick der Anbieterfirmen, aus dem Cloud Computing einen allseits bestaunten Hype zu machen. Die weltweite Verfügbarkeit ist wegen des für die Datenübertragung verwendeten Internet-Protokolls (TCP/IP) technisch auch nichts Neues. Wie das Internet selber ein Zusammenspiel aus vorher längst bekannten Technologien ist, werden hier auch längst bekannte Leistungsmerkmale zu einem neuen Service zusammengepackt.

Dabei kann man zwischen Public und Private Cloud-Diensten unterscheiden. Erstere umfassen das Angebot eines Providers, einen solchen öffentlich angebotenen Dienst als Kunde gemäß den Geschäftsbedingungen des Anbieters zu nutzen, wie z. B. der Mail-Dienst Gmail von Google. Die zweite Spielart beschreibt die Organisation eines Cloud Computing durch eine Firma für sich selbst oder die Beauftragung eines Providers, den Dienst nach den eigenen

Vorstellungen und Vorgaben zu installieren. Natürlich existieren dazwischen beliebige Mischformen.

Besondere Probleme gibt es beim Public Cloud Computing durch eine Firma, die US-amerikanischem Recht unterliegt. Hier greift der Patriot Act, der den amerikanischen Ermittlungsbehörden eine nahezu unkontrollierte Zugriffsmöglichkeit auf die gespeicherten Daten erlaubt, einschließlich der strafbewehrten Auflage durch die US-Behörden, über diesen Zugriff Stillschweigen zu bewahren.

Der Microsoft-Europa-Manager Gordon Frazer äußerte sich schon anlässlich der Präsentation des Büro-Paketes Office 365 im Juni 2011 in unverhohlener Deutlichkeit zu diesem Thema. Auf die Frage eines Konferenzteilnehmers „Kann Microsoft garantieren, dass europäische Daten, die in Datenzentren innerhalb Europas abgelegt sind, den EU-Raum unter keinen Umständen verlassen – auch dann nicht, wenn Microsoft gemäß des Patriot Act dazu aufgefordert würde?“ antwortete Frazer, dass Microsoft ein US-basiertes Unternehmen sei und die lokalen Gesetze einzuhalten habe, darunter auch den Patriot Act. Er führte weiter aus, dass niemand glauben solle, andere amerikanische Firmen wie etwa Apple oder Google würden anders verfahren. Auf Anforderung würden sie alle den Behörden die angefragten Daten herausrücken.[15]

Diese damaligen Vermutungen wurden dann zwei Jahre später anlässlich des PRISM-Skandals als Tatsachen bestätigt. Dazu heißt es in dem bereits zitierten Pressedienst: „In einem Bericht der Washington Post werden neue Präsentationsfolien zu PRISM veröffentlicht. Diese zeigen weitere Details über das großangelegte Abhörprogramm der National Security Agency (NSA). Die Folien legen den Schluss nahe, dass NSA und FBI die Möglichkeit haben, E-Mails und andere Inhalte in Echtzeit auszuspähen.“[16] Die nicht entkräfteten Vermutungen gehen sogar so weit, dass die regierungsamtlichen Abhöreinrichtungen sogar auf den Betriebsgrundstücken privater Firmen installiert seien.

Andere Bedenken richten sich gegen den Kontrollverlust der Kunden über ihre eigenen Daten, den sie bei sogenannten Public Cloud-Lösungen zu erleiden haben.[17]

---

[15] Sibylle Glassner: USA haben Zugriff auf europäische Cloud-Daten, silicon.com Pressedienst vom 30. Juni 2011.

[16] silicon.com Pressedienst vom 1. 7. 2013.

[17] Der amerikanische Journalist Mat Honan schildert einen persönlichen Albtraum, den er dank Apples iCloud-Dienst erfahren hat, siehe silicon.com Pressedienst vom 7. 8. 2012: Die Cloud ist für Steve Wosniak ein Albtraum: „Es begann damit, dass sein iPhone ausfiel. Beim Versuch, eine Wiederherstellung über iCloud einzuleiten,

Viele Anbieter haben inzwischen die datenschutzrechtliche Problematik erkannt, weniger aus Einsicht in die Probleme mit dem Datenschutz, sondern wegen der das Geschäft ausbremsenden Bedenken ihrer potenziellen Kunden und bieten neuerdings nach deutschem Datenschutzrecht zertifizierte Lösungen mit Serverstandorten in Deutschland oder zumindest einem Land im EU-Rechtsraum an (z. B. Deutsche Telekom[18], Hewlett-Packard[19]).

Das immer wieder auftauchende Problem des Konflikts mit dem US-Recht macht eine gesetzliche Klarstellung unbedingt erforderlich. In den einschlägigen Rechtsnormen nationaler wie auch europäischer Regelungen zum Datenschutz sollte als Mindestanforderung festgelegt werden, dass ein Eingriff in die elektronische Kommunikation nur nach vergleichbaren Kriterien erfolgen darf, wie sie das Bundesverfassungsgericht in seinem Urteil vom 27. 2. 2008 zum Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme für das Verhältnis zwischen Bürgern und Staat dargelegt hat.[20] Unabhängig hiervon ist zu beachten, dass Mitbestimmungsrechte von Betriebsräten, wie etwa das nach § 87 Abs. 1 Nr. 6 BetrVG, nicht davon abhängen, wie sich die datenschutzrechtliche Situation darstellt. Sie werden nach dem Territorialitätsprinzip allein dadurch ausgelöst, dass es sich um personenbezogene Daten von Beschäftigten in Betrieben handelt, die in Deutschland angesiedelt sind (vgl. hierzu Abschnitt II.2.f.).

---

erhielt er keinen Zugang. Er öffnete sein MacBook – und war auch dort nach einem Reset ausgesperrt, der ohne sein Zutun eingeleitet wurde. Nicht besser erging es ihm bei seinem iPad. Ihm wurde klar, dass sich jemand Zugang zu seinem iCloud-Konto verschafft hatte und damit auch seine Geräte kontrollieren konnte. In der Folge vermochte der Unbekannte auch noch auf sein Gmail-Konto sowie sein Twitter-Konto zuzugreifen und die Passwörter zu ändern. Damit erhielt er Zugriff auf das Twitter-Konto des Gadgetblogs Gizmodo.com, für das Honan früher geschrieben hatte – dessen 415.000 Follower wurden wenig später mit anstößigen und rassistischen Tweets eingedeckt. Inzwischen hatte der Angreifer außerdem die nicht mehr aufzuhaltende Fernlöschung von Honans MacBook eingeleitet, die zu erheblichem Datenverlust führte“.

[18] Die T-Systems-International hatte im Herbst 2011 angeregt, ein Zertifikat für deutsche und europäische Cloud-Betreiber einführen. Nach einem Bericht der Nachrichtenagentur Bloomberg sollen in einer derart zertifizierten Cloud Unternehmen ihre Daten vor der US-Regierung abschirmen können. Quelle: www.blomberg.com/news/2011-09-13/deutsche-telekom-wants-german-cloud-to-shield-data-from-u-s-.html.

[19] Rudi Kulzer: HP baut Cloud für den deutschen Markt, silicon.com Pressedienst vom 22. 2. 2012.

[20] Vgl. BVerfG vom 27. 2. 2008 – 1 BvR 370/07, NJW 2008, 822 zum Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme; hierzu Wedde, AuR 2009, 373; vgl. auch BVerfG vom 11. 3. 2008 – 1 BvR 256/08 zu den Grenzen der Vorratsdatenspeicherung.

4. Elektronische Kommunikation

Die Nutzung von E-Mail, elektronischen Tagebüchern (Weblogs oder Microblogs), Online-Foren und Sozialen Netzwerken sind mit jeweils typischen Zeitverschüben aus dem privaten Bereich in den kommerziellen Bereich vorgedrungen. So alt wie die kommerzielle Mail-Nutzung selbst ist dabei der Streit in den Firmen, ob es den Beschäftigten erlaubt sein soll, die elektronischen Kommunikationsmittel auch persönlich zu nutzen. Die deutschen Telekommunikationsgesetze der 1990er Jahre haben hier mehr für Verwirrung als für Schutz gesorgt.

a) Private Nutzung von Mail und Internet

Erst nach jahrelangen Auseinandersetzungen wurde in einem Medienunternehmen vereinbart, dass neben der geschäftlichen Nutzung eine private bzw. persönliche Nutzung erlaubt sei, unter folgenden Bedingungen:

- Die persönliche Nutzung darf die Arbeitsabläufe nicht beeinträchtigen.
- Ausgeschlossen sind das Abrufen, Speichern oder Verbreiten von Inhalten, die gegen datenschutzrechtliche, persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen. Ebenfalls ausgeschlossen ist das Abrufen, Speichern und Verbreiten von beleidigenden, verleumderischen, rassistischen oder pornografischen Äußerungen oder Abbildungen.
- Die Nutzung darf für das Unternehmen mit keinen zusätzlichen Kosten verbunden sein.

Kernpunkt des langen vorangegangenen Streites war einerseits die These, dass der Arbeitgeber unter den Providerstatus falle, wenn er die private Nutzung zuließe und dann die verschärften datenschutzrechtlichen Bestimmungen des Telemediengesetzes zu beachten hätte und in der Folge jedwede Kontrolle über die Nutzung der elektronischen Kommunikationsmittel verlöre. Diese These fiel bei vielen Arbeitgebern auf fruchtbaren Boden, weil sie die Illusion hegten, dass bei verbotener privater Nutzung ein uneingeschränkter Zugriff beispielsweise auf die Inhalte sämtlicher Mails und die Protokolle der Internetnutzung bestünde.

Doch in den Firmen werden überwiegend personalisierte Mail-Accounts verwendet, was auch mit dadurch erzielter höherer Kundenfreundlichkeit, besserer Kundenbindung und besserem Betriebsklima begründet wird.

Wie wenig sich bei dieser Konstellation Dienstliches und Privates trennen lässt, macht schon ein Blick auf die heute übliche betriebliche Verarbeitung personenbezogener Daten deutlich. Dies beginnt bei der – zunehmend elektronisch abgewickelten – Bewerbung, bei der viele handelsübliche Systeme den Vorgang des Löschens schlicht nicht mehr kennen und für unbestimmte Zeiten die Daten gespeichert halten. In vielen Fällen wandert eine Auswahl der Bewerbungsdaten in einen sog. Talent Pool, um sie für spätere Verwendungen verfügbar zu halten. Die Personalsysteme zumindest der größeren Unternehmen speichern in ihren Stammdaten Angaben über Schulbildung, berufliche Ausbildung und bisherige Tätigkeiten, oft einschließlich der Angaben über Vorarbeitgeber. In den Bewegungsdaten der Systeme findet man bei entsprechender Systemausstattung des Arbeitgebers die komplette Historie der angefallenen Fort- und Weiterbildungsmaßnahmen.

Verfügt das Unternehmen über ein elektronisch unterstütztes Arbeitszeitmanagement, so kommen die Arbeitszeitdaten hinzu: Tägliches Kommen und Gehen, die Pausen, die Urlaube, die Krankheitszeiten und sonstige „Fehlzeiten". Unternehmensparkplätze mit elektronisch gesteuerten Schranken halten auch noch das Ankommen und Verlassen der Parkplätze fest, denn die Schranke öffnet und schließt sich nur nach Lesen eines gültigen Betriebsausweises, was dank Transpondersteuerung berührungslos geht.

Das führende SAP-Personalsystem Human Capital Management (HCM) zum Beispiel bietet darüber hinaus Platz für die jährlichen Mitarbeiterbeurteilungen, für mit den Mitarbeiterinnen und Mitarbeitern vereinbarte Ziele und deren Zielerreichung. Module zum Kompetenzmanagement ergänzen diese Datensammlungen um Informationen über die Fähigkeiten und Fertigkeiten der Beschäftigten, ihre sog. Skills, oft in einer Granularität, die Hunderte von Ausprägungen umfasst.

In den Systemen festgehaltene Qualifikationen beschränken sich keinesfalls auf fachliches und methodisches Wissen. Im Zentrum heute üblicher Systemeinführungen stehen vielmehr die Social Skills, wobei Vorgesetzte dann z. B. die Teamfähigkeit, die Kommunikations- und Konfliktfähigkeit, die Ziel- und Ergebnisorientierung, Lernbereitschaft oder auch die „kreative Problemlösungskompetenz" ihrer Untergebenen zu beurteilen haben, alles „weiche Faktoren", für die es kaum objektive Messkriterien geben dürfte. Die subjektive Sicht auf diese Faktoren kann ausgesprochen unterschiedlich ausfallen.

Viele heute üblichen Arbeitsaufgaben umfassen das Recherchieren im Internet mit Hilfe von Suchmaschinen, die sich bei Auswurf ihrer Ergebnisse nicht dafür interessieren, ob diese für dienstliche oder private Verwendung gebraucht werden. Die Unternehmen schätzen die Neugier ihrer Beschäftigten und können ihnen dann kaum vorschreiben, den geistigen Horizont auf die „dienstliche Nutzung" zu begrenzen. Für die Erledigung vieler Arbeitsaufgaben werden die persönlichen Netzwerke der Beschäftigten auch immer wichtiger, wobei dienstliche und private Erfahrungen kaum noch zu trennen sind. Dies steht einem Verbot der Privatnutzung in der Praxis entgegen. Im Ergebnis sind Arbeitgeber damit aber aus juristischer Sicht gehindert, die Kommunikationsinhalte der Beschäftigten zu kontrollieren.

Die Untrennbarkeit von Dienstlichem und Privatem wird insbesondere deutlich, wenn man das BYOD-Konzept (Bring Your Own Device) betrachtet. Insbesondere renommierte Unternehmensberatungen empfehlen ihrer Kundschaft, sich darauf einzustellen, dass man es in Zukunft hinnehmen müsse, wenn die Mitarbeiter ihre eigenen Geräte mit zur Arbeit bringen. Dies müsse schon deshalb geschehen, weil man im heutigen „war of talents“ die hoffnungsversprechenden Jungtalente nicht mehr als Mitarbeiter gewinnen könne, wenn man ihnen das im Vergleich zur schnelllebigen IT-Mode doch meist veraltete Equipment des Unternehmens anböte. Der Trend hin zur Nutzung von privaten Endgeräten für geschäftliche Zwecke sei nicht mehr aufzuhalten. In den meisten Unternehmen sind die Führungskräfte ja die ersten, die ihre privaten Geräte auch im Unternehmen einsetzen. Die Mitarbeiter werden in Zukunft mit ihren bevorzugten persönlichen Produktivitäts-Tools arbeiten und selbst entscheiden, welche Notebooks, Tablets und Smartphones sie nutzen wollen.

Durch die zunehmende Untrennbarkeit von beruflicher und persönlicher Nutzung muss man heute konstatieren, dass das „Innenleben“ der in der Arbeit genutzten Rechner ein Teil der schutzwürdigen Persönlichkeitssphäre geworden ist. Dies hat das Bundesverfassungsgericht in dem Urteil zur „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“[21] deutlich gemacht, in dem festgestellt wird, dass die Nutzung der Informationstechnik für die Persönlichkeit und die Entfaltung des Einzelnen eine früher nicht absehbare Bedeutung erlangt habe. Sicher ist die Übertragbarkeit aus dem Verhältnis Staat-Bürger in die Arbeitswelt nicht selbstverständlich, dürfte aber in der hier angesprochenen Thematik angebracht sein.

Um Missverständnisse und Unklarheiten zu vermeiden, ist es notwendig, das durch die Rechtsprechung des Bundesverfassungsgerichts begründete Grundrecht auf informationelle Selbstbestimmung[22] normativ in einer Form zu verankern, die sicherstellt, dass es nicht immer wieder mühsam aus den Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz (GG)[23] abgeleitet werden muss. Sinnvollerweise könnte eine solche Verankerung in der Form der Aufnahme eines „Grundrechts auf informationelle Selbstbestimmung“ in das Grundgesetz erfolgen.

---

[21] BVerfG vom 27. 2. 2008 – 1 BvR 370/07, NJW 2008, 822.

[22] BVerfG vom 15. 12. 1983 – 1 BvR 209/83, NJW 1984, 419.

[23] Grundgesetz für die Bundesrepublik Deutschland (GG) vom 23. 5. 1949 (BGBl. I S. 1), zuletzt geändert durch Gesetz vom 11. 7. 2012 (BGBl. I S. 1478).

Künftige gesetzliche Regelungen sollten weiterhin klarstellen, dass bei personalisierten Mail-Accounts der Zugriff des Arbeitgebers auf Nutzungsprotokolle und Mail-Inhalte nicht erfolgen darf. Darüber hinaus müsste sichergestellt werden, dass Zugriffe auf private wie auch auf besonders schutzwürdige bzw. persönliche dienstliche Daten unterbleiben müssen.

b) Verbindungsdaten

Im Rahmen der PRISM-Enthüllungen wurde bekannt, dass der amerikanische Geheimdienst Metadaten über so ziemlich jeden Internetnutzer sammelt. Als Metadaten bezeichnet man die „Verbindungsdaten". Im Falle einer E-Mail sind dies vor allem Absender, Empfänger, Datum und Uhrzeit. All das sind zusätzliche Informationen zu den eigentlichen Daten, nämlich dem Inhalt der Nachricht selbst.

Die MIT-Media-Labs hat eine Web-App entwickelt, mit dem jeder User, der diese App erwirbt, genau diese Metainformationen aus dem eigenen Mail-Postfach abfragen und anhand dieser Daten eine grafische Darstellung aller Kontakte erstellen kann.

„Dabei lässt sich beispielsweise auf einen Blick erkennen, in welcher Beziehung eure Bekannten zueinander stehen. So hat man über manche Kollegen oder Freunde Kontakt zu Dutzenden anderen Menschen, während andere abseits stehen und keinerlei Verbindung zum Rest der Kontaktliste haben. Auch wird auf einen Blick deutlich, mit wem man in einem regen Austausch steht und mit wem man kaum kommuniziert."[24]

Somit wird das Erstellen von Bewegungs- und Beziehungsprofilen für jedermann erschwinglich. Noch[25] sind keine Fälle bekannt, in denen Personalabteilungen von solchen Anwendungen Gebrauch gemacht haben. Mit der zu erwartenden schnellen Ausbreitung dieser oder ähnlicher Techniken ist es eine der großen Herausforderungen an ein zukünftiges Datenschutzrecht, kontrollierbare Barrieren zu schaffen, um einer systematische Durchleuchtung der Beschäftigten mittels solcher Bewegungs- und Beziehungsprofile auch rechtlich einen Riegel vorzuschieben.

---

[24] Kim Rixecker: Das weiß Google über dich: „Immersion" analysiert dein Gmail-Konto, in t3n news vom 8. 7. 2013.

[25] In Anbetracht der Schnelllebigkeit der Informationstechnik ist eine genauere Fixierung des Zeithorizonts angebracht: Das „noch" bezieht sich auf das Ende des Jahres 2013.

Dies stößt auf strukturelle Schwierigkeiten des auf den Schutz der Person ausgerichteten Datenschutzrechts. Ähnlich wie im Immissionsschutzrecht, in dem es nicht mehr darauf ankommt, die Gesundheit der einzelnen Bürger zu schützen, sondern die Luft um ihrer selbst willen sauber zu halten, müsse etwas Ähnliches im Datenschutzrecht geschehen: „Gesetzliche Regelungen müssen nicht nur am drohenden Eingriff in die Rechte einzelner Bürger ansetzen, sondern an der Quelle der Gefahr – und digitale Datenanlagen sowie ihre Programme behandeln wie etwa ein Braunkohlekraftwerk: Datenserver wie beispielsweise die von Google müssten durch normative Schutzregelungen als gefährliche Anlage qualifiziert werden, gegen deren schädliche Auswirkungen Vorsorge getroffen werden muss“.[26] Ein zeitgemäßes Datenschutzrecht hätte also technische und organisatorische Vorgaben und Normen festzulegen, die von Softwaresystemen eingehalten werden müssten. Könnten sich Datenschutz-Audits (vgl. Abschnitt III.2) auf solche rechtlichen Grundlagen beziehen, würden sie weit mehr als auf Freiwilligkeit der betroffenen Firmen beruhende Qualitäts-Zertifikate darstellen.

c) Internet-Filter

Internet-Filter bieten Sperren bestimmter Internetseiten für den Zugriff an. Aus ganzen Katalogen kann ausgewählt werden, welche Inhaltsbereiche gesperrt werden sollen. Man kann Services abonnieren, die „black lists“ zu sperrender Seiten auf einem vom Anbieter als aktuell erklärten Stand halten.[27] Solcherart Software war ursprünglich für amerikanische Eltern zwecks Kontrolle ihrer vor Verwahrlosung zu schützenden Kinder gedacht. Offensichtlich wurde aber schnell die Nützlichkeit für den Einsatz in Firmen erkannt.

Schließt ein Unternehmen einen entsprechenden Vertrag ab, so kann es aus dem Katalog des Diensteanbieters Sachgebiete für zu sperrende Inhalte (z. B. Sport, Sex, Spiele) oder bestimmte Domains, z. B. E-Bay, auswählen. Der Einsatz solche Filter auch für Inhaltsbereiche, die nicht nur den Zugriff auf bekannte „Virenschleuder“-Seiten oder aus Sicherheitsgründen bedenkliche Seiten sperren, z. B. Seiten mit pornographischem Inhalt, lässt sich datenschutzrechtlich insbe-

---

[26] Thomas Darnstädt: Leviathan ohne Hemd. Der Staat ist vom digitalen Zerfall bedroht, in Der Spiegel 30/2013, S. 23.

[27] Einer der Anbieter, entensys.de, wirbt mit einem beeindruckenden Katalog. Auf der Internetseite des Anbieters heißt es: „Regulieren Sie privates Surfen während der Arbeitszeit. Überwachen Sie Ihren kompletten Internet-Traffic. Reglmentieren Sie alle Internetaktivitäten. Filtern Sie unerwünschte Websites und Protokolle. Kontrollieren Sie den Internetzugriff all Ihrer Programme. ... Nutzen Sie umfangreiche und detaillierte Statistiken“. Quelle: www.entensys.de/usergate

sondere aus § 9 BDSG ableiten. Soweit die durch entsprechende Software erhobenen personenbezogenen Daten Zwecken der Datenschutzkontrolle, der Datensicherung oder der Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage dienen, ist ihr Einsatz unter Beachtung der engen Zweckbindung in § 31 BDSG aus datenschutzrechtlicher Sicht nur für eng begrenzte Zwecke zulässig.

Betrachtet man die Auswirkungen auf die Firmenkultur, so kann man durchaus von Zensur sprechen. Ob darin eine Frage der Ordnung im Betrieb gemäß § 87 Abs. 1 Nr. 1 BetrVG zu sehen ist, sei dahin gestellt. Da es sich um eine technische Einrichtung handelt, die zur Verhaltens- und Leistungskontrolle geeignet ist, wird in jedem Fall das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG ausgelöst.[28] Dieses eröffnet den Weg, um diese Thematik zum Regelungsgegenstand einer Betriebsvereinbarung zu machen, etwa im Rahmen einer allgemeinen Vereinbarung zur Internetnutzung.

Weitere Probleme entstehen durch die Protokollierung der Filterung und aufgesetzte Alert-Funktionen, die einen Alarm bei Zugriffen auf gesperrte Seiten auslösen. Solche Alarme erscheinen in der Regel als Zeilen in einer Monitoranzeige und enthalten natürlich auch die Identifizierung der zugreifenden Stelle, sei es die Rechnerkennung oder der Name des Benutzers. Dadurch wird das Instrument zu einem umfassenden Kontrollinstrumentarium ausgeweitet. So lässt sich dann gezielt feststellen und nachweisen, wer auf welche Internet-Seiten zugreifen wollte.

Exzesse in der betrieblichen Praxis wurden bisher hauptsächlich durch betriebsverfassungsrechtliche Regelungen vermieden. In vielen Betriebsvereinbarungen ist festgehalten, dass die Filter nur zum Schutz vor dem Zugriff auf sicherheitsgefährdende und Gewalt verherrlichende oder pornografische Seiten eingesetzt werden und dass sie im Sinne reiner Schlüsselfunktionen arbeiten, also sich damit begnügen, den Zugriff zu sperren und diesen Vorgang nicht in einem Protokoll festhalten.

Es ist unbefriedigend, sich nur auf die Ebene des Gestaltungsspielraums verlassen zu können, der sich aus den Mitbestimmungsregeln des Betriebsverfassungsgesetzes ableitet. Sinnvoller wäre es, die Zwecke von Internet-Filtern normativ zu begrenzen. Dieses Ziel könnte durch eine Erwähnung in § 31 BDSG erreicht werden, in dem eine besondere Zweckbindung für bestimmte Maßnahmen des technischen Datenschutzes verankert ist. Flankierend könnte auf der mitbestimmungsrechtlichen Ebene klargestellt werden, dass die im Rahmen

---

[28] Vgl. DKKW-Klebe, § 87 Rn. 201.

von § 31 BDSG getroffenen Maßnahmen uneingeschränkt dem Mitbestimmungsrecht des Betriebsrats unterfallen.

Bezüglich der Protokollierung wäre eine zwingende datenschutzrechtliche Vorschrift nützlich, dass Hersteller ihre Software mit abgestellter Protokollierung als Default-Einstellung auszuliefern hätten und man nicht aufwändig erst später die Protokollierung abstellen muss.[29]

Natürlich muss der Umfang einer Protokollierung „customizable", d. h. vom anwendenden Unternehmen einstellbar sein, so dass die protokollierten Tatbestände einem Sparsamkeitsgebot unterworfen werden können.

d) Automatische Mailarchivierung

Den Firmen werden mit Verweis auf die Abgabenordnung oder andere steuerrechtliche Vorschriften Systeme angeboten, die alle eingehenden und ausgehenden Mails sofort automatisch archivieren, und zwar eingehende Mails schon, bevor sie dem individuellen elektronischen Postfach des Benutzers zugeteilt sind. Dies mag angehen für Call Center und ähnliche Betriebe, bei denen es auch keine personalisierten Mail-Accounts gibt.

Die meisten dieser Systeme zeichnen sich darüber hinaus noch durch komfortable Suchmethoden für die archivierten Mails mit Volltextsuchen über den Inhalt der Mails aus.[30]

In vielen Betrieben ist die Angelegenheit dann so geregelt, dass die Mails den Adressaten zunächst in ihre persönlichen Postfächer zugeteilt werden, sie dann die Möglichkeit haben, Mails mit persönlichem Inhalt in einen als privat oder persönlich gekennzeichneten Ordner zu verschieben. Nach einer definierten Zeit, z. B. drei Monaten, erfolgt dann eine automatische Archivierung, wobei die persönlichen Ordner von diesem Verfahren ausgenommen bleiben.

Lediglich auf der Regelungsebene wurde bisher wirksam durchgesetzt, dass ein Archivsystem nur wie ein Logbuch funktionieren und dass die Suchfunktion nur auf Datum, Absender und Empfänger anwendbar sein darf. Eine entsprechende datenschutzrechtliche Vorgabe, die Zwecke von Archivsystemen klar beschränkt, lässt sich zwar schon heute aus dem BDSG ableiten, weil auch eine Archivierung das Vorliegen einer gesetzlichen Erlaubnisnorm gemäß § 4 Abs. 1

---

[29] Bei vielen Softwareprodukten muss erst mit großem Aufwand festgestellt werden, welche Vorgänge überhaupt protokolliert werden und an welchen Stellen man Einfluss auf diese Protokollierung nehmen kann.

[30] Mit umfassenden Suchoptionen sind zum Beispiel die Modelle EMA®-S40 bis EMA®-S800 der Firma Artec ausgestattet.

BDSG voraussetzt. Fehlt diese rechtliche Legitimation und gibt es auch keine wirksame Einwilligung der Beschäftigten, muss die Speicherung zu Zwecken der Archivierung unterbleiben. In der Praxis kommen Unternehmen dieser Vorgabe unter Hinweis auf einen nicht zu leistenden Aufwand indes oft nicht nach.

Eine Sonderrolle nimmt dabei die Betreff-Zeile der Mails ein. Sie steht zwar im *Header* der Maildateien und wird demzufolge meist unter Verbindungsdaten subsumiert, liefert aber gleichzeitig Informationen über den Mailinhalt und gehört damit zu den wesentlich schutzbedürftigeren Inhaltsdaten.

Ein Einsatz von automatischen Mailarchiven, die Mails schon vor der Zuteilung an die Adressaten archivieren, sollte gesetzlich verboten werden, zumindest in allen Fällen, in denen es sich um personalisierte Mail-Accounts handelt. Insbesondere bedarf es einer Klarstellung, dass die Betreffzeile zu den Inhaltsdaten gehört und damit einem stärkeren Schutz unterliegen muss als die Verbindungsdaten. Eine datenschutzrechtliche Bewertung führt zwar bereits heute zu diesem Ergebnis. In der Praxis werden die Daten in der Betreffzeile indes oft weniger vor unzulässigen Verarbeitungen geschützt als datenschutzrechtlich angebracht.

e) Telefonie und Videokonferencing

Die IP-fähigen Telefonanlagen sind in der Lage, gesprochenes Wort als Sound Files zu speichern. Diese können wie Textdokumente verschickt werden. Dabei muss man eine höhere Sensibilität des gesprochenen Wortes gegenüber geschriebenem Text konstatieren. Sprachliche Äußerungen zeichnen sich gegenüber geschriebenem Text durch ihre höhere Spontaneität und nicht mehr vorhandene Zurücknehmbarkeit aus. Korrekturmöglichkeiten sind hier nur noch als neue Statements oder Entschuldigungen möglich.

Die Hersteller bieten keine Möglichkeit an, wie das Versenden von solchen SoundFiles unterdrückt werden kann. Dies muss erst durch nachträgliche Eingriffe bewerkstelligt werden.

Die gleiche Thematik ergibt sich beim Videoconferencing bezüglich der Aufzeichnung von Konferenzabläufen, eine Funktion, die von den einzelnen Konferenzteilnehmern gerne zur eigenen Dokumentation genutzt wird, aber eine andere Dynamik entwickelt, wenn solche Videoclips versendet werden.

Als technische Anforderung an die Implementierung solcher Systeme sollte die Anforderung gerichtet werden, dass man das Kopieren von Sound Files und Video Streams unterbinden, mindestens aber an eine gesonderte Berechtigung oder an die technisch eingeholte und dokumentierte Zustimmung aller Teilnehmer binden können muss.

Insbesondere in Call Centern wird von den elektronischen Aufzeichnungen oft in Form des „silent monitoring“ Gebrauch gemacht. Dieses Verfahren beschreibt das heimliche, ohne Kenntnis geschweige denn Einwilligen der Teilnehmer erfolgende sich Aufschalten von dritten Personen auf Gespräche der Call Center Agents, die auf Grund einer Checkliste dann das mitgehörte Gespräch bewerten. Durch Betriebsvereinbarungen wird diese Praxis in der Regel verhindert. Doch tut sich manche Einigungsstelle beachtlich schwer, die datenschutzrechtliche Unzulässigkeit solcher Verfahren zu konstatieren.

Die Hersteller von IP-Telekommunikationsanlagen und Kollaborationsplattformen (wie Microsoft Sharepoint/Lync) sollten verpflichtet werden, Verfahren für den kontrollierbaren Umgang mit Sound Files und Konferenzmitschnitten in ihre Produkte zu implementieren, z. B. durch geeignete Workflows und differenzierte Möglichkeiten der Vergabe von Zugriffsrechten.

Das Einverständnis von Gesprächs- oder Konferenzteilnehmern mit technischen Mitschnitten der elektronischen Sessions könnte ohne hohen Aufwand technisch erzwungen werden, beispielsweise durch Opt-In-Funktionen, die eine Aktivierung der Aufzeichnungsfunktion erst dann ermöglichen, wenn alle Teilnehmer ihre elektronische Zustimmung erteilt haben. Ebenso wäre es sinnvoll, die Opt-In-Funktionen so auszugestalten, dass andere Konferenzteilnehmer nicht erteilte Einwilligungen konkreten Personen nicht zuordnen können. Nur so wäre das Recht auf informationelle Selbstbestimmung wirklich garantiert. Entsprechende Vorgaben bzw. Forderungen könnten dann in datenschutzrechtliche Audits bzw. Zertifizierungen aufgenommen werden.

f) Kollaborationsmanagement

Unter dieser Vokabel verbergen sich technische Plattformen zur Unterstützung von Zusammenarbeit wie z. B. das Microsoft-Produkt Sharepoint. Ein bei vielen Mitarbeitern durchaus beliebtes Leistungsmerkmal ist der Präsenzmanager, eine Echtzeit-Anzeige, in welchem Zustand sich die an der Anlage angemeldeten Benutzer gerade befinden. Hier gibt es in vielen Unternehmen allerdings einen rechten Wildwuchs der Statusmerkmale, die über online – offline durch beliebig viele Ausprägungen hinausgehen (bis hin zu „in Pause“, „bin auf Toilette“).

Die Sharepoint-Voreinstellung sieht nach dem Stand aus dem Jahr 2013 vor, dass nach fünf Minuten Inaktivität am Rechner die Präsenzanzeige eines Mitarbeiters ihre Farbe (von dunkelgrün auf hellgrün) ändert. Das Abstellen dieser

Merkmale sowie die Veränderung der Anzeigemöglichkeiten erfordern oft umfangreiche Customizing-Arbeiten.

Bewährt haben sich Einstellungen, denen zu Folge die Mitglieder eines Teams die Möglichkeit haben, untereinander ihre Präsenz zu sehen und darüber hinaus in einer „buddy list“ Personen ihrer Wahl eintragen können, deren Präsenz sie nach Zustimmung dieser Personen ebenfalls sehen können. Diese Zustimmung wird dann durch ein technisches Verfahren unterstützt (elektronisch innerhalb des Systems übermittelte Anfrage mit Opt-In-Möglichkeit durch die angefragte Person und automatischer Freischaltung der Präsenzanzeige nach Zustimmung). Selbstverständlich sollte jedem Benutzer die Möglichkeit offen stehen, eine solche Zustimmung auch wieder zurücknehmen zu können, ohne dass dafür ein Administrator angesprochen werden muss.

Die gängigen Plattformen bieten ein Application Sharing und ein Desktop Sharing an. Dies ermöglicht den Teilnehmern, gemeinsam an einem Dokument zu arbeiten oder gar gemeinsam den Bildschirm eines Rechners zu nutzen. Solche Funktionen sind in jedem Fall an das elektronisch abgefragte Einverständnis aller beteiligten Personen zu binden. Wenn die Plattformen ein elektronisches Mitschneiden der Sessions anbieten, so ist in Analogie zum Mitschneiden von Gesprächen zu verfahren.

Die standardmäßigen Voreinstellungen der Statusmerkmale bei Präsenzmanager-Software sollten nur die Ausprägungen „anwesend“ und „abwesend“ anbieten; weitere Differenzierungen müssten explizit vereinbart werden. Freitextfelder für die Beschreibung der Status-Merkmale sind zu vermeiden, da sie einer in der Praxis schnell unkontrollierbaren Vermehrung sehr differenzierter Abwesenheitsunterscheidungen Vorschub leisten. Defaults, bei denen alle Nutzer die An- bzw. Abwesenheit aller Teilnehmer sehen, sind ebenfalls zu vermeiden.

Das Erfordernis des Einverständnisses aller beteiligten Personen an allen Sharing-Funktionen sollte dagegen gesetzlich verankert und technisch erzwungen werden.

Eine gesetzliche Klarstellung ist vor allem auch deshalb wünschenswert, da es in vielen Betrieben zwischen den Betriebsparteien lange Auseinandersetzungen um diese Thematik gibt.

g) Social Media

Die Unternehmen haben erkannt, dass die traditionellen Strategien des Marketings nicht mehr so wirkungsvoll sind wie früher, weil das Vertrauen der

Verbraucher in herkömmliche Medien nachlässt, die aktive Formen der Beteiligung ausschließen. Zunehmend gewinnen die Social Media, wie Facebook, Twitter, aber auch eher beruflich orientierte Netzwerke wie LinkedIn oder Xing für die Meinungsbildung auch über die klassische Internet-Generation hinaus an Bedeutung. Social Media Marketing erscheint den Unternehmen daher als eine kostengünstige Alternative zum traditionellen Marketing.[31]

Über die Produkte und Services eines Unternehmens wird in Blogs, Online-Foren und sonstigen Social Media-Kanälen geredet, ob die Firmen dies wollen oder nicht. Die Unternehmen sind durch dieses veränderte Szenarium in ihrem Handlungsspielraum eingeschränkt; in weiten Teilen des Marketings sehen sie sich ihrer Verfügungsgewalt beraubt. Dabei scheint eine neue Nomenklatura zu entstehen. Weit über 90 Prozent der Nutzer betätigen sich nur passiv als Leser. Einige stellen hin und wieder eine Frage, und unter einem Prozent der Nutzer sind wirklich aktiv und sorgen für über 90 Prozent der Inhalte. Diese sind gut vernetzt und stellen einen beachtlichen Einflussfaktor dar. Wo früher Unternehmen durch Unterlassungsklagen agieren konnten und so den Verbreitungskreis der „schlechten Schlagzeilen“ und den Kreis der „Wissenden“ reduzieren konnten, bleiben heute diese traditionellen Möglichkeiten wirkungslos. Im Gegenteil, es gibt mittlerweile genügend Beispiele, wo gerade der Versuch, Meinungen im Netz zu zensieren und Autoren unter Druck zu setzen, die Beiträge aus dem Netz zu nehmen, einen „shit storm“ im Internet ausgelöst hat, der dann in Form von Tausenden von Protestmeldungen über diese Firmen hereinbricht.

Dies stellt Unternehmen vor eine neue Herausforderung im Umgang mit unangenehmen Veröffentlichungen, die ihren Ruf und somit den Umsatz nachhaltig schädigen können. Hier kommt nun das “human capital” für viele Unternehmen ins Spiel. Sie entdecken ihre Mitarbeiterinnen und Mitarbeiter als ihnen wohlgesonnene Agenten. Diese sollen nun – was früher misstrauisch beäugt wurde – Beiträge ins Netz stellen und das Unternehmen menschlicher und persönlicher erscheinen lassen. Aber gerade in den Social Media spielt die Authentizität der Beiträge eine wichtige Rolle. Und so muss man die ehrliche Meinungsäußerung der Mitarbeiterinnen und Mitarbeiter zulassen. Kritik von Verbrauchern annehmen und darauf eingehen, aus Fehlern lernen, das sind die neuen Direktiven. Viele Firmen sehen ihre Mitarbeiterinnen und Mitarbeiter dann auch als „Missionare“ in eigener Sache. Hierbei wird die Trennung zwischen beruflicher und privater Sphäre immer unschärfer.

---

[31] Siehe Tamar Weinberg: Social Media Marketing. Strategien für Twitter, Facebook und Co, Köln 2010, S. 7 ff.

Viele Führungskräfte, insbesondere der alten Schule, tun sich mit diesem Paradigmenwechsel schwer. Und so blühen die Konflikte um Äußerungen der Mitarbeiterinnen und Mitarbeiter über Produkte und Services des Unternehmens oder um das Unternehmen selbst regelrecht auf. Derzeit konzentrieren sich die Auseinandersetzungen auf Guidelines oder Richtlinien, die Unternehmen zu dem Thema herausgeben.

Besondere Beachtung muss in diesem Zusammenhang dem „discussion mining“ geschenkt werden. Externe Dienstleister bieten Services an, in denen minuziös verfolgt werden kann, wie die Beschäftigten sich in öffentlichen sozialen Netzwerken, in Online-Foren und Blogs verhalten. Die betroffenen Programme verfügen über Schnittstellen zu den unternehmensinternen Personalsystemen und erlauben so den Abgleich von Äußerungen im Netz mit den Namen entweder aller oder ausgewählter Mitarbeiterinnen und Mitarbeiter, z. B. der Führungskräfte. Diese ursprünglich als Marketinginstrumente konzipierten Verfahren eignen sich daher zu einer weitgehenden Mitarbeiterüberwachung weit über die Grenze unternehmensinternen Verhaltens hinaus.

Hier ist die Forderung nach einer gesetzlichen Grenzziehung wünschenswert, insbesondere nach einem Verbot bestimmter Leistungsmerkmale wie der auf gezielte Personen ausgerichteten Rasterfahndung.

Weiter wird deutlich, dass der Anwendungsbereich des BetrVG räumlich nicht auf die physikalischen Grenzen des Betriebs oder Unternehmens beschränkt ist. Der betriebsverfassungsrechtliche Betriebsbegriff ist funktional zu verstehen und nicht nur räumlich.[32] Damit endet die Regelungskompetenz der Betriebsräte nach dem BetrVG nicht an den Grundstücksgrenzen des Betriebs. Innerhalb Deutschlands sind deshalb Betriebsvereinbarungen möglich, die über die unmittelbaren Betriebsstätten hinaus wirken und beispielsweise häusliche Telearbeitsplätze oder mobile Arbeit mit erfassen.

Problematischer wird die Wahrnehmung und Umsetzung kollektiver Rechte, wenn Aufgaben außerhalb Deutschlands erledigt werden, da das sog. Territorialitätsprinzip Mitwirkungs- und Mitbestimmungsrechte von Betriebsräten auf das Hoheitsgebiet Deutschlands begrenzt. Ein Unterlaufen kollektiver Rechte könnte vor diesem Hintergrund durch eine normative Verpflichtung des Arbeitgebers verhindert werden, nach der die Datenverarbeitungen und -nutzungen nur dann außerhalb der Bundesrepublik Deutschland zugelassen

---

[32] BAG vom 29. 1. 1992 – 7 ABR 27/91, NZA 1992, 894; vgl. auch Fitting, § 5 Rn. 206; DKKW-Trümner, § 5 Rn. 47.

wären, wenn die Einhaltung kollektiver Regelungen sowie individueller Rechte abschließend garantiert wäre (vgl. hierzu Abschnitt II.2.f.).

h) Gesichtserkennung

Facebook-Nutzer bekommen Fotos vorgeschlagen, auf denen Freunde von der ins System eingebauten Gesichtserkennung markiert wurden. Sie können dann entscheiden, ob die Software die Gesichter richtig zugeordnet hat. Das Leistungsmerkmal wurde im Sommer 2011 in den USA eingeführt und wenig später ohne Ankündigung weltweit ausgerollt – und löste einen Protest der Datenschützer aus, worauf es – zumindest vorerst – in Deutschland zurückgezogen wurde. Die weltweit fast eine Milliarde Facebook-Nutzer[33] laden täglich mehrere hundert Millionen Bilder auf die Plattform, die damit längst zu einer der umfangreichsten Bildersammlungen im Netz geworden ist. Es war Facebook 50 bis 100 Millionen Dollar wert, ein auf Gesichtserkennung spezialisiertes israelisches Unternehmen aufzukaufen.[34] Damit soll erreicht werden, dass das Leistungsmerkmal auch auf mobilen Geräten funktioniert, wovon sich Facebook eine enorme Steigerung der Upload-Rate für Bilder erwartet.

Die automatische Gesichtserkennung funktioniert besonders gut, wenn man häufig Personen auf Bildern markiert und später erneut Bilder dieser Personen hochlädt. Der Markierungsalgorithmus merkt sich diese Personen und schlägt sie dann zum Markieren vor, wenn neue Bilder mit diesen Gesichtern hochgeladen werden. Zunächst muss man also selber Hand anlegen, damit das System „lernen“ kann. Später mehren sich die Markierungsvorschläge, und es wird einfacher und schneller. Facebook selbst bewirbt die Gesichtserkennung damit, dass man so seine Erinnerungen und Erlebnisse besser mit Freunden teilen kann und sie auch selbst nicht so leicht vergisst.

Der Protest der Datenschützer hatte bereits vor dem (vorläufigen) Rückzug des Leistungsmerkmals immerhin bewirkt, dass Benutzer, die nicht einverstanden waren, es in den Privatsphäre-Einstellungen deaktivieren können, allerdings auf eine recht umständliche Weise. Man kann dann veranlassen, dass man Markierungsversuche der eigenen Bilder bei anderen Personen erst genehmigen muss. Damit wird natürlich nur das Anzeigen der Namen unterdrückt, die Zuordnung der Namen in der Facebook-Datenbasis allerdings nicht. Die Speicherung biometrischer Muster, die ohne die Einwilligung der Betroffenen angelegt wurden, bleibt rechtswidrig, so der Hamburgische Beauftragte für Datenschutz und

---

[33] Stand Frühjahr 2013.

[34] Quelle: t3n.de/news/facebook-gesichtserkennung-2-396448.

Informationsfreiheit.[35] Begründet wird diese Rechtsauffassung u. a. mit dem immensen Risiko- und Missbrauchspotenzial, das von einer Biometrie-Datenbank ausgeht, die jetzt schon millionenfach Gesichtsabdrücke Betroffener enthält.

Öffentlich angebotene automatisierte Gesichtserkennung ist ein datenschutzrechtliches No Go. Aus dem arbeitsrechtlichen Blickwinkel steht ihr das Recht der Beschäftigten am eigenen Bild entgegen. Der Aufforderung, entweder ein Einwilligungs-Tool, auch für die bereits gespeicherten Daten, einzuführen oder die biometrischen Daten zu löschen, kam Facebook nur teilweise entgegen, indem die weitere Namenszuordnung vorerst für die EU-Länder ausgesetzt wurde.

i) Big Data

SAP, Oracle und weitere führende Firmen versuchen ihre Marktpositionen mit der Einführung sog. In-Memory-Techniken zu verbessern, besser bekannt unter dem Schlagwort Big Data. Darunter hat man zu verstehen, dass Terabyte große Datenmengen direkt in den schnellen Hauptspeicher der Rechner geladen werden. Damit kann die Verarbeitung ungewohnt großer Datenmengen ungemein beschleunigt werden, und man kann beliebige Daten nach eventuell bestehenden Korrelationen untersuchen, ohne stundenlang auf die Ergebnisse warten zu müssen. So steht ein ideales Instrumentarium für Rasterfahndungen aller Art zur Verfügung. Die mit dem PRISM-Skandal bekannt gewordenen Methoden der systematischen Suche nach bestimmten Datenmustern wären ohne diese Technik nicht denkbar.

Die Jagd nach Korrelationen entspricht der anlasslosen Suche nach Zusammenhängen und Abhängigkeiten zwischen beliebigen Daten. Die Anwendung dieser Methode auf personenbezogene Daten verletzt allerdings das Prinzip der Zweckbindung. Technische Barrieren lassen sich hier nicht errichten. Allein normative Regelungen können dieser Art von Datenverarbeitung Grenzen setzen.

An früherer Stelle wurde bereits darauf hingewiesen, dass die Erhebung und Verarbeitung von verhaltensbeschreibenden und persönliche Eigenschaften kennzeichnenden Daten an das Einverständnis der betroffenen Personen zu binden sei. Diese Daten wären damit von den Massendatenverarbeitungsformen des Big Data-Geschäfts automatisch ausgeschlossen. Doch die Anwender beteuern immer wieder die Anonymität der für ihre Analysen verwendeten

---

[35] Vgl. n-tv Ticker vom 16. 8. 2012.

Daten und begründen damit die Zulässigkeit ihrer Erhebung. Zum Zeitpunkt der Erhebung sind die Daten in den meisten Fällen jedoch nicht anonym.

Es ist hinreichend bekannt, wie leicht es in Anbetracht einer Vielzahl erhobener Daten möglich ist, eine Reindividualisierung zu bewerkstelligen, trotz Verzichts auf direkt personenidentifizierende Merkmale. Darüber hinaus stellt sich die Frage, ob eine Zivilisation das allseits überwachte Leben wirklich will. Das strikte Festhalten an dem Einwilligungsgebot würde vielen fragwürdigen Datensammlungen Grenzen setzen.

5. Anwendungen im Bereich der Beschäftigtendatenverarbeitung

Das klassische Feld der Auseinandersetzung um Datenschutz und Mitbestimmung in den Betrieben war die Personaldatenverarbeitung. Hauptsächlich ging es dabei um die Personalinformationssysteme, ein Streit, der bis in die späten Siebziger Jahre des letzten Jahrhunderts zurückreicht und sich vor allem um die Auswertung von Fehlzeiten drehte.

Heute hat sich der Fokus deutlich verschoben. Die Veränderungen in der Arbeitsorganisation von der Zuteilung von Arbeiten durch den Vorgesetzten hin zu Projektstrukturen mit höherer Beteiligung der Mitarbeiterinnen und Mitarbeiter machte für die Unternehmen auch eine Veränderung in den Führungsmethoden notwendig. Autoritäre Führungsstile geraten immer mehr in Misskredit, kooperativere Führungsmethoden mit weniger Kontrolle durch die Vorgesetzten und mehr Eigenkontrolle und -steuerung durch die Mitarbeiterinnen und Mitarbeiter selbst werden zunehmend als erforderlich proklamiert.

Parallel zu dieser Entwicklung lief ein nicht zu übersehender Bedeutungsverlust der klassischen Personalabteilungen, nicht zuletzt verursacht durch die vielen Shared Service-Center, in die man immer mehr Aufgaben der Personalabteilungen ausgelagert hatte.

Die ERP[36]-Anbieter, allen voran SAP, waren aber auch nicht untätig und haben einen bunten Strauß von Softwareinstrumenten in ihre Personalsysteme integriert, vom Recruiting Management über Kompetenz- und Performance Management bis zum Talent und Succession Management. Darin sehen heute viele Personalbereiche ihre Chance, sich verloren gegangene Kompetenz zurückzu-

---

[36] ERP ist das Akronym für Enterprise Resource Planning und meint die Software zur umfassenden Unterstützung nahezu aller im Unternehmen anfallenden Aufgaben.

erobern. Personalentwicklung bzw. Personal Development heißt das neue Tummelfeld. Schlagworte wie „Coaching“, „Motivstrukturanalyse“, „Neurolinguistische Programmierung“ (NLP), „Fördern und Fordern“ bereichern die PowerPoint-Präsentationen. Potenzialkreise werden aus der Taufe gehoben, und spezielle Schulungsblöcke für jedwede Zielgruppe werden angeboten.

Das Damoklesschwert des demographischen Wandels und der beginnende Kampf um die „klugen Köpfe“ macht es für die Unternehmen überlebenswichtig, Mitarbeiterinnen und Mitarbeiter zu gewinnen und vor allem an sich zu binden. Unternehmen, die dies nicht schaffen, laufen Gefahr, vom Markt zu verschwinden.

Immer mehr Unternehmen werben deshalb mit ihren Unternehmensleitbildern auf Hochglanzpapieren, reden über Unternehmens- und Führungskultur, und ganz im Trend der Zeit wird die Vertrauenskultur proklamiert.

Doch leider bleibt festzustellen, dass die technischen Systeme immer noch den Hang der Unternehmen zur Kontrolle ihrer Mitarbeiterinnen und Mitarbeiter widerspiegeln.

Die elektronische Erfassung von Daten, die eigentlich im geschützten Raum zwischen Führungskraft und dem einzelnen Beschäftigten besprochen und dort auch verbleiben sollten, wenn man das Wort Vertrauen ernst nimmt, spiegeln immer noch das vorherrschende Kontrollinteresse der Unternehmen und ihre Urangst vor der Individualität von Menschen wider, vor Menschen, die unkontrollierbar, nicht normierbar, nicht steuerbar und nicht verplanbar sind.

Im Folgenden werden nun exemplarisch einige Instrumente aus dem Instrumentenkasten der Personalentwickler untersucht.

a) Kompetenzmanagement

Zielsetzung des klassischen Kompetenzmanagements ist es, die für das Unternehmen erfolgskritischen Fähigkeiten, sogenannte Skills, festzustellen und aufzulisten, um sie mit den vorhandenen Fähigkeiten der Mitarbeiter und Mitarbeiterinnen zu vergleichen und nach Skill-Level zu bewerten. Besteht eine Diskrepanz zwischen den Anforderungs- und den Mitarbeiterprofilen, so müssen die Skills „entwickelt“ bzw. aufgebaut oder die Mitarbeiter anderweitig eingesetzt werden.

Als vergleichsweise unproblematisch wird dieses Vorgehen bei der Abfrage von Fachwissen gesehen, z. B. bei der Dokumentation von Sprachkenntnissen. Zunehmend kritisch wird es allerdings bei den sogenannten „weichen Faktoren“, den Soft Skills (z. B. Kommunikationsfähigkeit, Selbstvertrauen, Vernetztes

Denken, Initiative, Einsatzbereitschaft). Hier handelt es sich nicht mehr um Fakten, sondern um Beurteilungen. Die in den Systemen erstellten Kompetenzprofile der Beschäftigten umfassen eine Vielzahl solcher Items. Es sind Fälle bekannt, in der hunderte solcher Skills, geordnet nach Skill-Gruppen dokumentiert werden.

Es ist hier nicht der Ort für eine methodische Kritik an diesen Verfahren, aber soviel sei angemerkt: Oft werden die morgen gefragten Fähigkeiten mit den Anforderungen von gestern und vorgestern ermittelt. Da der Aufwand zur Erstellung der Profile beachtlich groß ist, verlieren die dokumentierten Skills schnell ihre Aktualität, und aus vieler Software wird dann „Schrankware“. Praktisch unbrauchbar stehen die Systeme dann schon nach wenigen Jahren in irgendeiner ungepflegten virtuellen Ecke.

Hinzu kommt die neue Herausforderung durch Social Media-Anwendungen, die vermutlich einen Modernisierungsschub traditioneller Systeme auslösen werden. Dies zeigt das Interesse der Firma SAP, die über drei Milliarden Dollar für den Kauf von SuccessFactors aufgewendet hat, einer Firma, die nichts anderes als webfähige Personalanwendungen anbietet.

Im Gegensatz zu der Schwerfälligkeit früherer Skill- oder Kompetenzmanagementsysteme zeichnen sich solche SocialMedia-Anwendungen durch eine gewisse Leichtigkeit der Handhabung aus, z. B. in der Form „meine Interessen“ und „meine Vorlieben“, mit entsprechenden Suchfunktionen nach Personen, die „meinen Interessen“ „ihre Fähigkeiten“ entgegenzusetzen haben.

Die in den Kompetenz-Managementsystemen verwendeten Daten weisen einen hohen Detaillierungsgrad auf und sind nicht durch das Arbeitsverhältnis (§ 32 BDSG) abgedeckt, sondern haben nur dann eine rechtlich haltbare Basis, wenn die Informationen von den Beschäftigten freiwillig gegeben werden. An den Voraussetzungen der Freiwilligkeit darf aber unter den Bedingungen des Beschäftigungsverhältnisses gezweifelt werden. Den meisten Firmen gelingt es auch nicht, den Beschäftigten klar zu machen, welche Vorteile sie vom Betrieb dieser Systeme haben.

Besonders problematisch sind Anwendungen, in denen Vorgesetzte solche Angaben über Qualifikationen und Qualifikationslevel ihrer Mitarbeiterinnen und Mitarbeiter in ein System einstellen und die betroffenen Personen noch nicht einmal erfahren, was ihre Vorgesetzten über ihre Qualifikationen gespeichert haben.

Ein vertretbarer Umgang mit solchen Systemen ist nur möglich, wenn auf betrieblicher Ebene Rahmenbedingungen vereinbart werden, die das System in ernstzunehmender Weise in die viel beschworene Vertrauenskultur einbetten.

Dies macht es beispielsweise erforderlich, dass eine Rückholbarkeit eingegebener Daten und der hiermit verbundenen Prozesse gegeben ist.

Die meisten in solchen Systemen gespeicherten Informationen haben keinen Ewigkeitswert, sondern zeichnen sich durch hohe Veränderungsraten aus. Dem werden die Systeme mit ihren langen Speicherfristen in keiner Weise gerecht.

Der österreichische Informatikprofessor Viktor Mayer-Schönberger plädiert in einem beachtenswerten Buch[37] dafür, alle Dateien mit einem Verfallsdatum auszustatten. Dieses „Recht auf Vergessenwerden“ soll sicherstellen, dass Informationen mit einem Personenbezug nach Ablauf einer bestimmten Frist automatisch gelöscht werden. Die Daten ließen sich in unterschiedliche Kategorien mit verschieden langen Speicherfristen einteilen. Allein der Zwang, bei der Erfassung eines Datums überlegen zu müssen, wie lange es gespeichert sein darf, kann eine wirkungsvolle Methode darstellen, die immer weiter anwachsende Datenflut einzudämmen.

Ähnliche Überlegungen finden sich im Entwurf der Europäischen Union für eine Datenschutzverordnung.[38] Dieser enthält in Artikel 17 ein „Recht auf Vergessenwerden und auf Löschung“. Um dieses zu erfüllen, soll Betroffenen gegenüber verantwortlichen Stellen das Recht eingeräumt werden, die Löschung von sie betreffenden personenbezogenen Daten und die Unterlassung jeglicher weiteren Verbreitung dieser Daten zu verlangen.

In der betrieblichen Praxis könnte ein „Recht auf Vergessenwerden“ dadurch umgesetzt werden, dass von den Anbietern der Personalsysteme gefordert wird, die entsprechenden Datensätze mit einem zusätzlichen Datenfeld für ein Verfallsdatum zu versehen und darüber hinaus Prozeduren zur Verfügung zu stellen, die diese Löschoperationen automatisiert durchführen.

b) Talent Management und Succession Management

Ähnlich verhält es sich mit Systemen zum Talent Management oder zum Succession Management (Nachfolgeplanung), in denen – oft ohne Wissen der betroffenen Personen – nicht nur Optionen für Stellenbesetzungen, sondern auch

---

[37] Viktor Meyer-Schönberger: Delete – Die Tugend des Vergessens in digitalen Zeiten, Berlin University Press, Berlin 2010.

[38] Europäische Kommission: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), Brüssel, 25. 1. 2012, Rn. 53 ff.

Angaben über ihre Qualifikationen, oft vermischt mit Beurteilungen gespeichert sind.

In vielen Unternehmen stehen auch die Führungskräfte unter einem speziellen Fokus und werden sozusagen unter besondere Beobachtung gestellt. Vor allem die unteren und mittleren Führungsebenen sind davon betroffen, da diese direkten Kontakt zu den Mitarbeiterinnen und Mitarbeitern haben und ihnen somit eine besondere Rolle für das Unternehmen zukommt.

Unter dem Anliegen, eine möglichst einheitliche und vergleichbare Führungsqualität im Gesamtunternehmen zu erreichen, werden in manchen Unternehmen auf sog. Führungskonferenzen Qualifikationen und Beurteilungen von Führungskräften erhoben, die anschließend durch die nächsthöhere Managementebene begutachtet werden. Dies geschieht in vielen Fällen nicht nur ohne Beteiligung und ohne Wissen der betroffenen Personen, sondern darüber hinaus wird ihnen – wenn sie dann die Existenz solcher Einrichtungen in Erfahrung gebracht haben – auch die Einsicht verweigert.

Die Praxis, dass die betroffenen Beschäftigten noch nicht einmal erfahren, was ihre Vorgesetzten für Einschätzungen abgeben und speichern lassen, seien es Fähigkeiten, Eigenschaften oder Qualifikationen, steht im Gegensatz zu den wichtigen Grundsätzen des Datenschutzrechts. Diese sehen die Wahrhaftigkeit und Überprüfbarkeit der erhobenen Daten und die Korrigierbarkeit durch die Betroffenen vor, vom Recht auf Einsicht aller Daten, die über eine Person gespeichert werden und der Speicherung der Daten außerhalb der Personalakte einmal abgesehen.

In diesem Zusammenhang ist auch zu berücksichtigen, dass das deutsche Arbeitsrecht davon ausgeht, dass über jeden Beschäftigten nur eine einheitliche Personalakte geführt wird.[39] Zu dieser einheitlichen Personalakte gehören auch Neben- und Sonderakten. Werden sie geführt, muss in der zentralen Personalakte ein Verweis hierauf zu finden sein.[40] Die Führung einer „doppelten Personalakte“ ist unzulässig. Beschäftigte haben nach § 83 Abs. 1 BetrVG einen Rechtsanspruch darauf, alle Bestandteile ihrer Personalakte einzusehen.

Ein Nebeneffekt der Talent und Succession Management-Systeme ist auch die Durchleuchtung und Kontrolle der Mitarbeiter und Führungskräfte (in der Regel der unteren und mittleren Führungsebene) vor dem Hintergrund eines Unternehmensleitbildes. Konformität trägt dabei immer den Sieg über Querdenkertum davon. Die Systeme kennzeichnet häufig die Ausrichtung auf eine

---

[39] Vgl. allgemein Fitting, § 83 Rn. 1 ff.; DKKW-Buschmann, § 83 Rn. 3 ff.

[40] DKKW-Buschmann, § 83 Rn. 3.

Normierung von Leistung und Verhalten. Die Angst der Unternehmen vor der Individualität der Menschen nennt der bekannte Unternehmensberater Reinhard Sprenger[41] dieses Phänomen.

Zu erwähnen sind in diesem Zusammenhang auch die sich in letzter Zeit steigender Beliebtheit erfreuenden Systeme zu einem 360°-Feedback, wobei Führungskräfte sich von ihren Vorgesetzten, ihren Mitarbeiterinnen und Mitarbeitern, gleichgestellten Kollegen und Außenstehenden (z. B. Kunden oder Lieferanten) nach einem vorgegebenen Fragebogen beurteilen lassen.

Die Subjektivität der Datenbasis solcher Systeme steht außer Frage. Es handelt sich bei den gespeicherten Daten selten allein um objektivierbare Fakten, sondern um subjektive Werturteile. Man kann den Standpunkt vertreten, dass solche Daten nichts zu suchen haben in Datenbanken, auf die dann weltweite Zugriffe eingeräumt werden, wie bei vielen multinationalen Unternehmen üblich. Es ist dringend erforderlich, dass von den Softwareanbietern Systeme bereit gestellt werden, die einen verlässlichen Zugriffsschutz für solche hochsensiblen Daten gewährleisten, so dass zweifelsfrei sichergestellt werden kann, dass nur die direkt betroffenen Personen Zugriff auf die Details der Daten haben. So lange diese Voraussetzungen nicht gegeben sind, sollte auf eine datenbankorientierte Speicherung verzichtet werden. Entsprechende IT-Unterstützungen hätten sich dann mit der Terminverwaltung der erforderlichen Gespräche zu begnügen.

Die hohe Sensibilität gerade der in Feedback-Systemen gespeicherten Daten ist den Unternehmen durchaus bewusst. Die Teilnahme ist in der Regel freiwillig, doch ist der von der oberen Führungsebene aufgebaute Erwartungsdruck meist sehr hoch. Viele Firmen sehen eine Lösung dieses Problems darin, die Durchführung solcher Verfahren an externe Dienstleister zu vergeben, die dann zur vertraulichen Behandlung der Daten verpflichtet werden. Doch leider lassen gerade deren Systeme viele Merkmale struktureller Sicherheit vermissen. Die Daten verschiedener Firmen befinden sich oft in ein und derselben Datenbank, nur durch eine Art Buchungskreis voneinander getrennt. Zwar überwiegen hochautomatisierte Auswertungsverfahren, doch machen viele Sonderwünsche der Kunden Administratoreingriffe erforderlich. Auch hier lassen die Dienstleister die wünschenswerte Transparenz über die Vergabe der Berechtigungen vermissen.

Die Unternehmen wären gut beraten, wenn sie interne Richtlinien erstellten, in denen eine Grenzziehung für in Succession Management- oder ähnlichen Sys-

---

[41] Reinhard K. Sprenger: Vertrauen führt, Frankfurt-New York 2007.

temen erlaubte Daten vorgenommen wird. Bei deren Ausgestaltung muss neben der Integration allgemeiner datenschutzrechtlicher Vorgaben auch das Mitbestimmungsrecht des Betriebsrats bezüglich Fragen der Ordnung im Betrieb nach § 87 Abs. 1 Nr. 1 BetrVG beachtet werden.

Soweit auf elektronische Systeme zurückgegriffen wird, ist weiterhin das Mitbestimmungsrecht gemäß § 87 Abs. 1 Nr. 6 BetrVG einschlägig. Werden Personalfragebogen verwendet oder kommen Auswahlrichtlinien zur Anwendung, sind schließlich die in den §§ 94 und 95 BetrVG enthaltenen Mitwirkungs- und Mitbestimmungsrechte zu beachten.

Von den Systemanbietern müssen darüber hinaus schon mit Blick auf § 9 BDSG technische Konzepte eingefordert werden, die sicherstellen, dass Zugriffsrechte lokal eng begrenzt werden können. Viele Systeme erlauben heute keinen schnellen und vor allem verlässlichen Überblick darüber, wer welche Rechte hat. Um den in Nr. 3 der Anlage zu § 9 Satz 1 BDSG enthaltenen Vorgaben zur Zugriffskontrolle gerecht zu werden, muss beispielsweise ein verbindliches, abschließendes und transparentes Rollen- und Berechtigungskonzept zur Verfügung stehen, das die Beachtung der vorstehend genannten Anforderungen ermöglicht. Darüber hinaus muss es das Software-Design der Feedback-Systeme ermöglichen, die Verarbeitungsmöglichkeiten an klar definierten Zwecken zu orientieren. Dies erlaubt – im Gegensatz zum Angebot vieler Dienstleister – die Verwendung freier Abfrage- und Reportmöglichkeiten nur in eng begrenztem Rahmen.

Mit Blick auf bestehende Mitbestimmungsrechte wie § 87 Abs. 1 Nr. 1 und 6 BetrVG haben Betriebsräte Einflussmöglichkeiten auf die Ausgestaltung einschlägiger Systeme. In diesem Rahmen können sie beispielsweise Konzepte verlangen, bei denen Ergebnisse ausschließlich den Teilnehmern am Verfahren zur Verfügung stehen und sie diese mit unabhängigen Coaches besprechen können.

Die verbreitete Beauftragung externer Dienstleister wirft aus datenschutzrechtlicher Sicht weitere Fragen auf. Werden sie als Auftragnehmer nach § 11 BDSG tätig, sind sie an Weisungen des Auftraggebers gebunden und dürfen in diesem Rahmen nur Hilfstätigkeiten ausführen. Dies steht einem eigenständigen Betrieb von Feedbacksystemen entgegen.

Sollen die Diensteanbieter hingegen entsprechende Verfahren nach eigenem Ermessen durchführen, erfolgt eine sog. Funktionsübertragung. Hierbei führt der externe Dienstleister eigenständige Erhebungen, Verarbeitungen und Nutzungen der Daten durch. Die Übermittlung von Daten vom Arbeitgeber an den externen Dienstleister bedarf in diesen Fällen einer gesonderten Rechtsgrundlage, da eine Erforderlichkeit i. S. v. § 32 Abs. 1 Satz 1 BDSG für derartige Auswertungen nicht gegeben ist.[42] Fehlt sie, kann eine Funktionsübertragung auch nicht auf ein berechtigtes Interesse des Arbeitgebers i. S. v. § 28 Abs. 1 Satz 1 Nr. 2 BDSG gestützt werden, da sich allein aus der fehlenden Erforderlichkeit ein Grund zu der Annahme ableitet, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Damit ist die Datenschutzkonformität der Ausgestaltung von Feedback-Systemen in den Fällen der Beauftragung externer Dienstleister fraglich.

Bezüglich der internen Durchführung ist eine datenschutzrechtliche Zulässigkeit nur gegeben, wenn sich die verfolgten Zwecke klar in die Erforderlichkeit i. S. v. § 32 Abs. 1 Satz 1 BDSG einfügen.

c) Performance Management

Die bekanntesten Verfahren aus dem bunten Strauß der Management-by-Objectives-Methoden sind die Zielvereinbarungen, wonach Führungskräfte mit ihren Mitarbeiterinnen und Mitarbeitern in der Regel jährlich Ziele vereinbaren, deren Erreichung dann zu einem späteren Zeitpunkt von denselben Führungskräften bewertet wird. Damit war ursprünglich die Idee verbunden, „unternehmerisches Denken“ bei den Beschäftigten zu fördern. Mit den Mitarbeiterinnen und Mitarbeitern sollten Ziele vereinbart werden, wobei die Wege zu deren Erreichung dann von den Betroffenen selber zu finden seien. Initiative und Kreativität sollten so gefördert werden.

Die betriebliche Praxis weicht in weiten Teilen von diesem Idealbild ab. Oft werden nicht Ziele vereinbart, sondern im Detail die Wege zum Erreichen der Ziele. Dabei handelt es sich um Dinge, die eigentlich der kreativen Phantasie der betroffenen Personen überlassen sein sollten.

Besonders kritisch wird es, wenn sogenannte Soft Skills in das Beurteilungsverfahren einbezogen werden, wie das folgende Beispiel verdeutlicht.[43]

Auf einer sechsstufigen Skala sollten zunächst die Mitarbeiter sich selbst bewerten; anschließend wurde die Beurteilung dann durch den Vorgesetzten vorgenommen. So wurde z. B. das zu bewertende Selbstvertrauen des Mitarbeiters durch die folgenden Items erläutert:

---

[42] Ähnlich Simitis-Seifert, § 32 Rn. 17 ff.; DKKW-Däubler, § 32 Rn. 8; enger Gola/Schomerus, § 32 Rn. 33, die eine Anwendbarkeit von § 28 Abs. 1 zulassen wollen, wenn es um Zwecke außerhalb des Beschäftigungsverhältnisses geht.

[43] Auszüge aus einem Performance Management für einen Außendienst.

- Tritt gegenüber internen und externen Gesprächspartnern angemessen und sicher auf
- Vertritt die firmen- und produktspezifischen Standpunkte auch in kritischen Situationen und gegen Widerstände souverän unter Beachtung der Unternehmenswerte
- Kann mit Rückschlägen und Kritik angemessen umgehen und geht gestärkt daraus hervor.

Unter Teamarbeit und Zusammenarbeit fand man

- Übernimmt aktive Rolle und Verantwortung im Team
- Kooperiert mit Kollegen und Vorgesetzten sowie mit dem Innendienst
- Integriert sich in Teamstrukturen.

Die Antworten wurden mit Punkten bewertet und ergaben dann für die beurteilten Mitarbeiterinnen und Mitarbeiter einen Ort in einer zwischen solchen qualitativen und meist durch Verkaufsergebnisse bestimmten quantitativen Dimension aufgezogenen „Performance-Matrix". Je nach Ergebnis befand man sich dann in der Top-Performer-Zone auf einem „Champions Level" oder etwas bescheidener auf einem „Master" oder „Profi Level" oder man hatte „noch Entwicklungspotenzial" und war auf einem „Development Level" gelandet.

Hier ist nicht der Ort, die Statements solcher Verfahren, die oft völlig unterschiedliche Dinge in ein einziges Item zwängen, methodisch zu kritisieren. Für die Persönlichkeitsrechte der Betroffenen ergibt sich ein schwerwiegendes Problem, denn die Daten stehen in einer Datenbank und sind meist für die komplette Hierarchielinie der direkten Vorgesetzten sowie der teils in anderen Ländern angesiedelten fachlichen Vorgesetzten (entlang der sog. „dotted line") einsehbar. Sie werden in vielen Reports ausgewertet. Die betroffenen Personen vor allem der unteren Hierarchieebene haben keinen Überblick darüber, was mit ihren Daten geschieht.

Methoden des Performance Managements kann man vielleicht so lange vertreten, wie die Daten in einer geschützten Sphäre bleiben, die nur den direkt betroffenen Personen, also den betroffenen Mitarbeiterinnen und Mitarbeitern und ihren unmittelbaren direkten Vorgesetzten, zugänglich ist und alle Beteiligten sich auch auf diesen Schutz verlassen können. Das Bild ändert sich grundlegend, wenn es sich um ein System handelt, das Ziele und Zielerreichung einem weltweit verteilten Personenkreis zugänglich macht, wie das bei vielen multinationalen Unternehmen leider Usus ist.

Manche Softwaresysteme bieten noch über die Beurteilung der Zielerreichung hinaus ein „Kalibrierungs-Tool" für das Performance Management an. Das funktioniert folgendermaßen: Da man ja zu wissen glaubt, dass die Vorgesetzten ihre Mitarbeiterinnen und Mitarbeiter unterschiedlich beurteilen, die einen strenger, die anderen großzügiger, setzt man rechnerisch die Mittelwerte aus den Organisationseinheiten auf einen gleichen Wert, nämlich den Durchschnittswert aller Beurteilungen des ganzen Unternehmensbereichs. Da es nun auch noch Vorgesetzte gibt, deren Beurteilungen eine große Spannbreite zwischen gut und schlecht umfassen, andere ihre Leute alle nur mit geringen Ausschlägen um den Mittelwert herum beurteilen, rechnet man ebenfalls die Streuung der Beurteilungen auf den gleichen Standardabweichungswert um. Das alles verkauft sich dann als Maßnahme zur Herstellung größerer Gerechtigkeit. Die solcherart manipulierten Daten steuern dann bei vielen Unternehmen die Höhe des variablen Gehaltsanteils.[44]

Ein weiterer problematischer Aspekt eröffnet die von vielen Unternehmen in den letzten Jahrzehnten eingeleitete Praxis, ihre Personalbereiche auszulagern oder im Konzern zu bündeln, in der Regel in Form einer Konzerntochter als Shared Service Center. So ist die Frage zu beantworten, ob es nach geltendem Recht überhaupt zulässig ist, dass Personalakten von Personen verwaltet und bearbeitet werden dürfen, die überhaupt nicht Mitarbeiter oder Mitarbeiterinnen des betroffenen Betriebs sind.

Aus dem datenschutzrechtlichen Blickwinkel setzt eine solche Verarbeitung das Vorliegen eines Auftrags nach § 11 BDSG voraus, wenn die zu erledigenden „Hilfsaufgaben“ klar umrissen und begrenzt werden können. Eigenständigen Aufgabenerledigungen im Rahmen einer Funktionsübertragung auf Basis von § 28 Abs. 1 Satz 1 Nr. 2 BDSG steht entgegen, dass bei Personalakten immer Grund zu der Annahme besteht, dass schutzwürdige Interessen der Beschäftigten überwiegen.[45]

Betriebsräte können auf der Grundlage ihrer Mitbestimmungsrechte Regelungen zum Performance Management durchsetzen. Einschlägig sind neben den Mitbestimmungsrechten nach § 87 Abs. 1 Nr. 1 und 6 BetrVG in Abhängigkeit von der konkreten Ausgestaltung des Performance Management im Einzelfall auch die Mitwirkungs- und Mitbestimmungsrechte nach den §§ 94 und 95 BetrVG.

Für das Performance Management-Thema insgesamt gilt, dass auf eine datenbankorientierte Erfassung solcher Daten so lange verzichtet werden muss, bis Rahmenbedingungen geschaffen sind, die den Vertraulichkeitsschutz auch

---

[44] Ein Teilnehmer an einem solchen Verfahren bemerkte mit nicht zu überhörendem Zynismus: Wir sind dann alle „praktisch quadratisch gut“.

[45] Zu den Möglichkeiten und Grenzen einer Funktionsübertragung bei Beschäftigungsverhältnissen Gola/Schomerus, § 11 Rn. 9; Simitis-Petri, § 11 Rn. 22 ff.; DKWW-Wedde, § 11 Rn. 14 ff.

kontrollierbar gewährleisten. Datenschutzrechtlich lässt sich diese Forderung relativ einfach fundieren: Zunächst einmal ist fraglich, ob der Einsatz von Performance Management-Systemen überhaupt nach § 32 Abs. 1 Satz 1 BDSG für die Durchführung eines Arbeitsverhältnisses erforderlich ist. Bejaht man dies, bleibt offen, in welchem Umfang personenbezogene Daten erfasst werden und für welche Zeiträume. Zudem müssen mit Blick auf § 4 Abs. 3 BDSG die Zwecke der Datenverarbeitung bereits bei der Erhebung klar und abschließend feststehen und den Betroffenen vorab mitgeteilt werden. Ist dies nicht der Fall, ist die Speicherung als zweckfreie Vorratsdatenverarbeitung zu bewerten und mangels datenschutzrechtlicher Erlaubnisnorm i. S. v. § 4 Abs. 1 BDSG nicht zulässig.

d) Apps für Personaldaten

Das Problem der „Appisierung“ von bisherigen Zentralanwendungen wie dem SAP-System Human Capital Management wird die Betriebsparteien in den kommenden Jahren gründlich beschäftigen. Bereits im Jahr 2010 hat SAP für sein Personalsystem Apps angekündigt, die es erlauben, beispielsweise Kompetenzprofile von Mitarbeitern anzusehen, Abwesenheitsmitteilungen zu bearbeiten, Urlaubstage anzuzeigen, Zeiten einschließlich Fehlzeiten zu erfassen und anzuzeigen, Benachrichtigungen über Aufträge und Vorgänge zu genehmigen usw.[46] Im Jahr 2011 folgte für 3,4 Milliarden Dollar der Aufkauf der amerikanischen Firma SuccessFactors.[47] In den Bereichen Employee Performance, Succession Planning und Learning Management sah sich die SAP gegenüber Wettbewerbern bis dahin klar im Nachteil. Die SuccessFactors-Technologie soll jedoch nicht nur das bestehende Angebot ergänzen, sondern auch SAP-Cloud-Angebote, wie das schon seit Jahren wenig erfolgreiche Hoffnungsträger-Produkt Business by Design oder das branchenspezifische Sales on Demand aufpeppen. Das viele Geld signalisiert die Wichtigkeit des Themas für den Marktführer. Elektronische Bewerbung, Mitarbeiterbeurteilung sowie die Behandlung von Qualifikations- und Kompetenzprofilen sollen dann als webfähige Anwendungen angeboten werden. Der Ankündigung von SuccessFactors zufolge, immer mehr Personalanwendungen internetfähig zu machen, sollen dann auch Teile davon als Apps angeboten werden.

---

[46] Lutz Pössneck: SAP: „Mobilgeräte sind der neue Desktop“, silicon.com Pressedienst vom 18. 5. 2011.

[47] Mit SuccessFactors kauft SAP Cloud-Lösung für Human Capital Management, silicon.com Pressedient vom 5. 12. 2011.

In früheren Zeiten erfolgte der Zugriff auf Personaldaten in den Räumen der Personalabteilung und damit in einer relativ kontrollierten und geschützten Umgebung. Das ändert sich, wenn via TabletPC oder SmartPhone der Zugriff an jedem beliebigen Ort möglich ist, im ICE, im eigenen Wohnzimmer oder in einem öffentlichen Café. Daraus ist die Forderung abzuleiten, dass bei der Vergabe von Berechtigungen der Übertragungskanal angesprochen werden können muss, so dass für den Remote Access-Zugriff gesonderte Berechtigungen vergeben werden können. Die verantwortliche Stelle muss also auch bei Remote Access-Zugriffen sicherstellen, dass nur Berechtigte auf geschützte personenbezogene Daten zugreifen können. In diesem Sinne steht es weiterhin in der Verantwortung der betrieblichen Regelungsebene, festzulegen, welche Daten für den mobilen Gebrauch freigegeben werden und welche nicht.

Es muss ferner möglich sein, alle Apps, die auf den Datenbestand einer personaldatenverarbeitenden Anwendung zugreifen können, vollständig in einer Dokumentation zu erfassen (beispielsweise durch Eintrag in einer sog. Access Control List). Kriterien für die Unzulässigkeit bestimmter Daten für eine Verarbeitung über mobile Geräte wären sehr hilfreich.

Die „Appisierung“ vieler Anwendungen wirft zudem die Frage auf, was eigentlich die „technische Einrichtung“ im Sinne des Betriebsverfassungsgesetzes ist.[48] Konzepte wie zu Zeiten relativ abgeschlossener Systeme versagen immer mehr. Statt mit einem in einem Handbuch noch komplett beschriebenen System hat man es nun mit einer Art Bienenschwarm kleiner und kleinster „Systemchen“ zu tun. Diese Situation darf natürlich nicht dazu führen, dass bestehende Mitbestimmungsrechte, wie insbesondere das nach § 87 Abs. 1 Nr. 6 BetrVG, nicht mehr zur Anwendung kommen. Arbeitgeber müssen auch bezogen auf die Vielzahl der Apps sicherstellen, dass Betriebsräte über deren geplanten Einsatz rechtzeitig vorab informiert werden und dass eine tatsächliche Anwendung erst nach Abschluss des Mitbestimmungsverfahrens erfolgen kann.

Vor diesem Hintergrund ist beispielsweise das Vorgehen eines IT-Unternehmens unzulässig, bei dem der Betriebsrat während laufender Verhandlungen über die Einführung eines neuen Systems feststellen musste, dass für den Remote-Zugriff bereits solche Apps zur Verfügung standen und weltweit genutzt werden konnten. Der hierauf angesprochene Arbeitgeber zog sich auf die Position zurück, dass die Apps von der Konzernmutter im Ausland programmiert worden waren und dass über deren System auch die Verbindung zum neuen IT-System in Deutschland erfolgten sollte. Erst als der Betriebsrat mit einem

---

[48] Vgl. hierzu DKKW-Klebe, § 87, Rn. 168.

Antrag auf Erlass einer einstweiligen Verfügung drohte, veranlasste der Arbeitgeber eine Sperrung der Zugangsmöglichkeiten über die Apps.

e) Personaldaten und Datenschutz

Die angesprochenen oft immensen Datensammlungen in den Systemen, die das Personalmanagement unterstützen sollen, bedürfen aus datenschutzrechtlicher Sicht einer eindeutigen Erlaubnisnorm. Dies folgt aus der allgemeinen Vorgabe in § 4 Abs. 1 BDSG.[49] Bezogen auf Beschäftigungsverhältnisse steht mit § 32 BDSG eine einschlägige Erlaubnisnorm zur Verfügung, die die Erhebung, Verarbeitung und Nutzung personenbezogener Daten „für Zwecke des Beschäftigungsverhältnisses" erlaubt, „wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist."[50] Der Begriff der Erforderlichkeit ist mit Blick auf das zu schützende Persönlichkeitsrecht der Beschäftigten eng auszulegen. Auf diese Auslegungsvorgabe weist auch die grundlegende Vorgabe zur Datenvermeidung und Datensparsamkeit in § 3a BDSG hin.

Erforderlichkeit im strengen Sinne würde bedeuten, dass ohne die entsprechende Information das Beschäftigungsverhältnis nicht durchführbar ist, etwa in dem Sinne, dass ohne Kenntnis der Bankverbindungsdaten niemandem sein Gehalt überwiesen werden kann. Aber rechtfertigt die Erforderlichkeitsformel auch das Abspeichern von hunderten von Qualifikationsitems, nur weil ein Unternehmen entschieden hat, jederzeit allmögliche Eignungen seiner Mitarbeitenden abfragen zu können? Tatsächlich erfolgen entsprechende Verarbeitungsvorgänge aber, weil die Erforderlichkeit i. S. v. § 32 Abs. 1 Satz 1 BDSG von Unternehmen in der Praxis oft nicht eng und restriktiv, sondern weit ausgelegt wird.

Die Praxis zeigt oft in unverhohlener Deutlichkeit, dass alle systemischen Anstrengungen und Aufwendungen keine Rolle spielen, wenn einer der Entscheidungsträger anderes vorhat. Die Konzernbetriebsratsvorsitzende eines großen Medienunternehmens bringt diesen Sachverhalt wie folgt auf den Punkt: „Da haben wir eine siebenstellige Summe ausgegeben für Assessments, High-Potenzial-Trainings, Coachings, Talentmanagement und Nachfolgeplanung, und dann werden drei Leute von Extern eingestellt, nur weil das der Chef so

---

[49] Vgl. allg. Teil 2 unter Ziffer 1a.

[50] § 32 BDSG Satz 1.

haben will."[51] Statements dieser Art ließen sich in nahezu beliebiger Häufigkeit ergänzen.

Die angesprochenen Beispiele zeigen, dass der unbestimmte Rechtsbegriff der Erforderlichkeit nur begrenzt dazu geeignet ist, datenschutzrechtlich unzulässige Verarbeitungen von Beschäftigtendaten zu verhindern. Damit stellt sich die Frage nach flankierenden Maßnahmen, durch die Verstöße gegen gesetzliche Normen verhindert werden können. Die Erforderlichkeitsklausel im Datenschutzrecht braucht insoweit einschränkende Bestimmungen, damit die „Großzügigkeit" in der Interpretation des betrieblichen Gestaltungsspielraums – sei es in der betrieblichen Entscheidungspraxis oder dem Ermessensspielraum von Einigungsstellen oder Arbeitsgerichten – aus ihrer schieren Grenzenlosigkeit herausgelöst wird.

Ist eine Erforderlichkeit nach § 32 Abs. 1 Satz 1 BDSG nicht gegeben, kann eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten auf der Grundlage von § 4 Abs. 1 BDSG dennoch erfolgen, wenn von Beschäftigten hierfür eine wirksame Einwilligung nach § 4a Abs. 1 BDSG erteilt wurde. Diese muss unter Beachtung der Vorgabe in Satz 1 der Norm freiwillig sein.

Es lässt sich jedoch trefflich darüber streiten, ob unter den Bedingungen des Beschäftigungsverhältnisses die Bedingungen der Freiwilligkeit gegeben sind, denn es stehen sich bei dem mit der Direktionsgewalt ausgestatteten Arbeitgeber und dem abhängig Beschäftigten ja keine gleichartigen Partner gegenüber.

Natürlich sind auf der Regelungsebene andere Lösungen denkbar, bei denen man guten Gewissens behaupten kann, dass die Bedingungen der Freiwilligkeit erfüllt sind, wie das folgende Beispiel zeigt:

Ein Unternehmen richtet ein Skillmanagement-System ein, bei dem den Mitarbeitenden gestattet wird, ihre Qualifikationen in einem Profil zu dokumentieren, auf das allein sie selbst Zugriff haben. Umgekehrt werden weltweit im gesamten Konzern alle Stellen – insbesondere neue Jobs – nach denselben Kriterien beschrieben. Die Mitarbeitenden können einen automatischen Nachrichtendienst abonnieren, der sie aufgrund einer ebenfalls automatisiert erfolgenden Analyse darüber informiert, ob und in welchem Umfang ihr Qualifikationsprofil auf die Anforderungen einer Tätigkeit passt. Es ist dann ihnen überlassen, sich auf die entsprechende Stelle zu bewerben. Sie können aber auch ihr Profil „ruhen" lassen. Außerdem erhalten sie die Möglichkeit, sich ein „Wunschprofil"

---

[51] Aus der Beratungspraxis der tse – Gesellschaft für Technologieberatung und Systementwicklung mbH, März 2013.

einzurichten, in welchem die von ihnen selbst gewünschten Qualifikationen mit den entsprechenden Qualifikationslevel ausgefüllt sind, über die sie gerne verfügen würden. Dieses Wunschprofil können sie dann in den jährlich stattfindenden Mitarbeitergesprächen mit ihrer Führungskraft erörtern und dabei auch feststellen, wozu die Firma bereit ist, wenn es um die Förderung ihrer Karriere geht.[52]

Diese Umorientierung von einem Nachfragemodell auf ein Angebotsmodell lässt den Beschäftigten die in Anonymität geschützte freie Wahl und bietet nicht nur dem Unternehmen, sondern auch seinen Beschäftigten echte Vorteile.

Um ein Ausufern der Erforderlichkeit zu vermeiden und um zu verhindern, dass Beschäftigte zu „freiwilligen Einwilligungen“ gezwungen werden, müsste ein zukünftiges Datenschutzrecht insbesondere

- die Erforderlichkeit einer Datenerhebung und -verarbeitung strikter an die Unverzichtbarkeit binden, d. h., von der verantwortlichen Stelle den Nachweis fordern, dass die vertraglich vereinbarte Arbeitsleistung ohne die gewollte Erhebung, Verarbeitung und Nutzung personenbezogener Daten nicht mehr erbracht werden kann und
- alle weiteren Datenerhebungen, -verarbeitungen und -nutzungen, die nur als zweckmäßig, nicht aber als unverzichtbar erforderlich zu qualifizieren sind, an die Freiwilligkeit zu binden, wobei die Bedingungen der Freiwilligkeit zu konkretisieren wären, dass Beschäftigte Einwilligungen jederzeit ohne das Risiko arbeitsrechtlicher Nachteile verweigern oder widerrufen können.

6. Security

Mit zunehmender Internet-Nutzung sind auch die damit verbundenen Sicherheitsrisiken gewachsen. Seit 1990 hat sich die statistisch festgestellte Computerkriminalität mehr als verzwanzigfacht.[53] Dies betrifft zwar hauptsächlich den Betrugsschwerpunkt Geldautomaten, aber darüber hinaus auch die Informationstechnik der Unternehmen. Die Zeiten, in denen eher sportliche Motive Hacker veranlassten, in die Unternehmensnetze – je stärker geschützt, desto lieber – einzudringen, sind inzwischen Vergangenheit. Zunehmend tritt der kriminelle Charakter dieser Angriffe in den Vordergrund. Dabei geht es nicht

---

[52] Pilotversuch in einem Telekommunikationsunternehmen aus der Beratungserfahrung der tse – Gesellschaft für Technologieberatung und Systementwicklung mbH, Sommer 2007.

[53] Vgl. Polizeiliche Kriminalstatistik 2008, Computerkriminalität, Bundesministerium des Innern, S. 236 ff.

nur darum, einem Unternehmen durch Verletzung seines Computernetzes zu schaden, sondern oft auch handfest um Industriespionage.

Um Bedrohungen durch Viren oder gezielte Hackerangriffe abzuwehren, kommt in den Unternehmen ein ganzes Arsenal unterschiedlichster Schutzprogramme zum Einsatz. Die bekanntesten Instrumente sind Firewalls, Virenscanner, Software zur Unterstützung des sog. Vulnerability Management, Intrusion Detection und Intrusion Prevention-Systeme bis hin zu forensischer Software.

Auf einer Informationsveranstaltung des deutschen Verfassungsschutzes für Security-Fachleute wies ein ungenannt bleiben wollender Experte darauf hin, dass rund 800.000 Chinesen damit beschäftigt seien, in mehr oder weniger heftigem Umfang Computernetze der Firmen zu Industriespionagezwecken anzugreifen und merkte dabei bedauernd an „Verhaften können wir sie ja nicht, wir können sie leider nur aussperren“.[54] So scheinen die in diesem Zusammenhang eingesetzten Filtertechniken wie Firewalls oder Virenscanner unter datenschutzrechtlichen Gesichtspunkten weitgehend unproblematisch zu sein, jedenfalls so lange sie sich darauf beschränken, unerwünschte Zugriffe einfach abzuwehren. Differenzierter gestaltet sich die Situation, wenn man die teils sehr ausführlichen Protokollierungen durch die Programme der Sicherheitssoftware betrachtet.

a) Konzepte struktureller Sicherheit

Es sind in der Regel IT-Administratoren, denen die Aufgabe zufällt, über die Sicherheit der Firmencomputernetze zu wachen. Doch hier liegen auch gleichzeitig die Risiken. Immer noch ist es in vielen Firmen üblich, dass Administratoren uneingeschränkte Zugriffsrechte haben. Dies ist vor allem vor dem Hintergrund brisant, dass viele Unternehmen die Betreuung ihrer IT-Infrastruktur an externe Dienstleister ausgelagert haben und somit firmenfremden Personen solch weitgehende Rechte zugestehen. Die Motive dieser Art von Outsourcing sind meist auf der Kostenseite zu suchen. Wer ein solches Unternehmen ausspionieren will, tut ganz im Sinne einer gängigen Kriminalromanvorlage gut daran, seine Leute als Arbeitskraft mit Zeitvertrag bei einem solchen Dienstleister anheuern zu lassen. Dann braucht man nur noch auf die Sternstunde zu warten, bis der Chefadministrator krank ist und seine Berechtigungen eben diesem eingeschleusten Mitarbeiter übergibt. Das darf er zwar nicht, aber im Interesse eines reibungslosen Ablaufs tut er es dennoch.

Über einen ähnlich gelagerten Skandal hatte vor einigen Jahren ein deutsches Unternehmen zu klagen, als am Vortag von dessen „go-live“-Termin Auszüge

---

[54] Die Veranstaltung fand im Jahr 2012 statt, vor dem Bekanntwerden der NSA-Affäre.

aus Dokumenten, die sich im persönlichen Verzeichnis des Vorstandsvorsitzenden befanden, in einem führenden deutschen Wirtschaftsblatt abgedruckt waren. Auch hier war wieder die typische Managementreaktion zu beobachten, nämlich Aktivwerden im Katastrophenfall. Man besann sich endlich, die Dokumente des Unternehmens nach unterschiedlichen Vertraulichkeitsgraden zu klassifizieren (von „öffentlich“ über „intern“ bis zu „streng vertraulich“) und dafür unterschiedliche Prozesse des Umgangs mit ihnen festzulegen. So entschied man sich für den Einsatz einer speziellen Software für alle vertraulichen und streng vertraulichen Dokumente, die den Zugriff an zwei Personen mit verschiedenen Passwörtern gebunden hat und jeden Zugriff dieser Administratoren-Paare in einem technisch erzwungenen, vor Fälschungen besonders geschützten elektronischen Protokoll festhielt.

Die Festlegung unterschiedlicher Vertraulichkeitsgrade der Informationen und die Strukturierung des Unternehmensnetzes in unterschiedliche, je nach Vertraulichkeitsgrad besonders geschützte Zonen sind wichtige Voraussetzungen einer „strukturellen“ Sicherheit. Dabei eröffnet sich die Chance, zwischen den Zonen Router oder Gateways anzubringen, die beim Übertritt von einer in eine andere Zone eine erneute Überprüfung der Berechtigung erlauben. Nichts ist für einen Hacker leichtere Beute als in ein flach organisiertes Computernetz einzudringen, in dem sich alle Elemente auf einer Ebene befinden.

Nicht oder wenig eingeschränkte Administratorenrechte sind zwar aus Bequemlichkeitsgründen sehr verbreitet, doch unter Sicherheitsgesichtspunkten ein nicht zu unterschätzendes Risiko. Die Administratorenrechte wären also spezifisch für die unterschiedlichen Vertraulichkeitsstufen zu gestalten bis hin zum Vier-Augen-Prinzip für höhere Vertraulichkeitsstufen. Die Bindung der Administratorrechte an eine eng gefasste Zweckbestimmung ist dabei selbstverständlich. Diese Zweckbindung hätte sich auf die Gewährleistung der Systemsicherheit und -verfügbarkeit sowie die Analyse und Korrektur technischer Fehler zu beschränken. Außerdem empfiehlt sich die Festlegung für die Administratoren, die im Rahmen ihrer Aufgaben erlangten Informationen nur innerhalb der verabredeten Zweckbindung zu verwenden und nicht an andere Personen weiterzugeben.

Ein Problem mangelnder struktureller Sicherheit zeigt sich auch in manchen öffentlichkeitswirksamen Datenschutz-Skandalen der Vergangenheit. Wenn es möglich ist, dass große Mengen von Credit-Card-Informationen der Kunden in falsche Hände gelangen, so ist dies sehr unwahrscheinlich auf erfolgreiche Hacker-Einbrüche, sondern eher auf Aktivitäten sog. Innentäter zurückzuführen. Nach der Devise „Prävention vor Verfolgung“ ließen sich solche Aktivitäten beachtlich erschweren, wenn es erstens so gut wie keinen direkten Benutzer-

Zugriff auf die Datenbank mit den Kundendaten gäbe[55] und zweitens die Anwendungsprogramme, die allein über die Zugriffsberechtigung auf die Datenbank verfügten, keine Funktionen anböten, bei denen man sich listenförmig tausende solcher Datensätze mit hochsensiblen Informationen anzeigen lassen kann. Dann nämlich ist es ein Leichtes, die Daten in kurzer Zeit zu kopieren und damit aus dem geschützten Raum der Anwendung herauszubefördern.

Maßnahmen struktureller Sicherheit sollten stets Vorrang vor normativen Regelungen wie v. a. Verpflichtungen und Strafandrohungen haben. Dazu bedarf es Regelungen zur Struktur der Administratorberechtigungen inklusive einer Festlegung der Zweckbindung auf betrieblicher Ebene.

b) Remote Control-Funktionen

Remote Control beschreibt das Aufschalten auf einen entfernten Rechner. Technisch ist dieses Verfahren weitgehend identisch mit dem von der Kollaborationssoftware bekannten Desk Sharing, wie es z. B. das Microsoft-Produkt Sharepoint anbietet. Leider ist es aber eine durchaus noch verbreitete Praxis der Administratoren, von diesen Instrumenten ohne Kenntnis der Benutzer Gebrauch zu machen, zumal viele entsprechenden Softwareprodukte dies nicht nur erlauben, sondern auch noch als Default vorsehen. In Unternehmen mit aufmerksamen Betriebsräten ist dies jedoch durch entsprechende Betriebsvereinbarungen unterbunden. Diese legen meistens fest, dass der externe Zugriff nur auf Anforderung des Benutzers, zumindest aber nicht in Unkenntnis von diesem erfolgen darf, der Zugriff erst nach einer aktiven Bestätigung durch den Benutzer möglich ist, dieser Systemzustand deutlich erkennbar sein muss und der Zugriff jederzeit vom Benutzer beendet werden kann. Dieses Verfahren sollte gesetzlich vorgeschrieben werden.

c) Intrusion Detection und Intrusion Prevention

Kein „security officer“ eines größeren Unternehmens hält heute die Vorstellung noch für ausreichend, dass man nur die Peripherie des Firmennetzes mit Virenscannern und Firewalls abschottet und sich dann darauf verlässt, dass das „Innenleben“ der Firma, vergleichbar einer mittelalterlichen Stadt mit bewehrten Stadtmauern, sicher ist. Infolge des Umgangs mit CDs, DVDs und Sticks sowie

---

[55] Natürlich gibt es auch beim Zugang zu den Datenbanken Administratorzugriffe. Diese wären aber an ein Mehr-Augen-Prinzip und an eine elektronische Zwangsprotokollierung aller Zugriffe zu binden. An dieser Stelle ist auch der Hinweis angebracht, wie problematisch es für ein Unternehmen ist, solche Aufgaben an einen externen Dienstleister auszulagern.

eventuell privater ins Firmennetz eingeklinkter Rechner gibt es unzählige neue potenzielle Quellen für Schadware jedweder Art. Also sehen Unternehmen die wachsende Notwendigkeit, das Netz auch intern zu überwachen. Hierfür eignen sich die Intrusion Detection-Systeme oder besser noch die Intrusion Prevention-Systeme.

Mit der erklärten Absicht, das unberechtigte Eindringen in Anwendungen verhindern zu wollen, lassen sich alle Aktivitäten im Netz beobachten. An Knotenstellen des Netzes werden Sensoren eingerichtet, die den kompletten Datenstrom einer genauen Analyse unterziehen. Dabei werden die Bitmuster der Datenpakete mit von Schadware bekannten Mustern, sog. Signaturen, verglichen. Stimmen die Bitmuster eines Datenstroms mit einem hinterlegten Ereignis überein, so wird ein Angriffsalarm ausgelöst. Alle Ereignisse dieser Art werden minuziös protokolliert. Die Vergleichsmuster werden laufend um neu entdeckte Angriffsmuster erweitert. Dazu gibt es spezielle Dienste, die ein Unternehmen abonnieren kann, so dass es dann über eine topaktuelle Bibliothek der Angriffsmuster verfügt. Über heuristische Verfahren lassen sich auch – zumindest teilweise – Angriffsszenarien erkennen, die den bereits bekannten Mustern ähnlich sind.

Intrusion Prevention-Systeme ergänzen die „Detection“ um sofort ergreifbare Maßnahmen und erlauben es beispielsweise, von zentraler Stelle aus, einen infizierten Rechner direkt vom Netz zu nehmen.

Über diese auf die Security im engeren Sinne konzentrierten Aufgaben hinaus, lassen sich die Datenströme aber auch unter inhaltlichen Gesichtspunkten überprüfen, z. B., von welchem Rechner werden zu verdächtigen IP-Adressen Verbindungen aufgebaut oder welche Datenströme enthalten Wörter aus als hochvertraulich eingestuften Dokumenten? Ein System, das Alarme bei Bitmustern auslösen kann, die sich einem Hackerangriff zuordnen lassen, kann theoretisch auch Alarme beim Entdecken beliebiger anderer Inhalte auslösen. Und hier beginnt das Problem für den Schutz der Persönlichkeitsrechte. Jemand muss vorher definiert haben, was in einem Unternehmen als „normal“ gelten soll. Dieses Unterfangen entbehrt nicht einer beachtlichen Problematik, denn es eröffnet sich eine neue Dimension für die Überwachung der Mitarbeiterinnen und Mitarbeiter, die sich durchaus den Vorwurf der Zensur gefallen lassen muss.

Die Notwendigkeit einer engen Definition, welche Muster und Ereignisse sich dem Thema Security zuordnen lassen, ist nicht mehr zu übersehen. Darauf könnte sich die Vergabe von Testaten für Softwareprodukte stützen, die sich verlässlich auf die Analyse von Sicherheitsproblemen konzentrieren und sich nicht für die inhaltliche Analyse (Zensur) des Netzverkehrs einsetzen lassen.

d) Forensische Software

Will man die „Bösewichte“, die das Computernetz eines Unternehmens von innen attackieren, auch dingfest machen, so braucht man gerichtsverwertbare Beweise. Genau dies ist über die Funktionen der Instrusion Detection oder Intrusion Prevention hinaus die Aufgabe forensischer Systeme.

Die US-amerikanische Firma Guidance bewirbt ihr Produkt EnCase mit der Behauptung, die Software sei in der Lage, für als unberechtigt klassifizierte Aktivitäten „gerichtsfest“ verwertbare Beweise zu liefern.[56] Im Einzelnen heißt es dazu: „Bei jeder forensischen Analyse ist es wichtig, die durchgeführten Schritte jederzeit nachvollziehen zu können und die Ergebnisse der Analyse in verständlicher Weise zu präsentieren. EnCase unterstützt den Ermittler hierbei durch integrierte Reporting-Funktionalität. Dazu werden Listen aller in dem Case enthaltenen Dateien und Ordner genauestens aufgelistet. Eine Liste der Internetadressen (URL) und der Zugriffszeitpunkte von besuchten Webseiten wird ebenfalls von EnCase automatisch erstellt. Detaillierte Informationen über das analysierte Laufwerk werden ebenso hinzugefügt. Bilder können mit Hilfe des integrierten Bildbetrachters auch in einer Galerieansicht dargestellt werden, um die Übersicht zu gewährleisten. In grafischer Darstellung können Aktivitäten anhand einer Zeitlinie dargestellt werden, wodurch Rückschlüsse auf die Abläufe am System leichter nachzuvollziehen sind.“[57]

Darüber hinaus bietet das Leistungsspektrum des auch als Incident Response Software gepriesenen Produkts die Beobachtung ausgewählter Prozesse oder Ports, eine Suche im Code-Text mittels mächtiger Filter-Techniken und diverse Entschlüsselungsmethoden, um auch verschlüsselte Dokumente analysieren zu können. Hervorzuheben ist dabei, dass man nicht nur die Festplatten und sonstigen Speichermedien, sondern auch den Hauptspeicher eines Rechners durchsuchen kann. So kann man z. B. Einsicht in ein Dokument nehmen, das ein Benutzer gerade verfasst, ohne dass er dieses Dokument überhaupt abspeichert oder irgendwo hin verschickt. Man muss nur zur rechten Zeit aktiv sein. Dies kommt faktisch dem Mitlesen der Gedanken eines Benutzers gleich und dürfte schwerlich mit dem vom Bundesverfassungsgericht präzisierten Grundrecht der „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ vereinbar sein.

---

[56] Siehe Internet-Site der Firma Guidance www.guidancesoftware.com/encase-forensic.htm: „Court Vetted: EnCase Forensic preserves data in an evidence file format ... with an unsurpassed record of court acceptance“, Stand September 2012.

[57] Quelle: http://de.wikibooks.org/wiki/Disk_Forensik/ _Beweismittelanalyse/_EnCase.

Um im Zusammenhang mit der IT-Sicherheit die Incident Response-Funktionalität besser nutzen zu können, bietet der Hersteller eine „ereignisgetriebene“ Einsatzmethode an, die viele Analysen automatisierbar macht. So kann man der Software über definierbare Regeln mitteilen, welche Prozesse sie von sich aus überwachen oder bei welchen sicherheitsrelevanten Ereignissen sie Alarme auslösen soll. Dies können Namen von Benutzern sein oder gezielte Korrespondenzen von bestimmten Personen oder an bestimmte Personen.

Spezielle Dienstleister bieten den Firmen eine Auswertung von technischen Log-Daten sämtlicher Serversysteme an. Dies umfasst die Webproxies, die DHCP-Zuordnung[58] und die Intrusion Prevention Systeme. Unter dem Stichwort „Vulnerability Management“ werden Systeme zum Schwachstellen-Scanning eingesetzt; auch deren Log-Daten werden in die Auswertung einbezogen. Außerdem lassen sich die Protokolle der Firewalls sowie der E-Mails auswerten. Alle diese Daten werden in einer speziellen Datenbank gesammelt, um dann Sicherheitsvorfälle „besser zu erkennen und besser darauf zu reagieren“[59]. Natürlich handelt es sich dabei nur um eine nachträgliche Untersuchung. Der Anbieter des Services ist wiederum eine US-amerikanische Firma, die die zu analysierenden Daten auf eigenen Servern speichert und ihren Kunden dann regelmäßige Reports zuschickt. Alle diese Daten sind personenbezogen im Sinne des Datenschutzrechts.

Besondere rechtliche Schwierigkeiten bestehen wiederum bei internationalen Konzernen, deren Konzernzentralen außerhalb der EU-Staaten und damit außerhalb des Wirkungsbereichs des europäischen Datenschutzrechts angesiedelt sind. Problematisch sind hierbei insbesondere US-gesteuerte Konzerne, vor allem, wenn sich die Administrationszentralen in den USA befinden. Bezogen auf die Konzernzentralen fehlt es in der Praxis regelmäßig ein einer belastbaren datenschutzrechtlichen Grundlage, da sich selbst auf der Grundlage von Safe Harbor-Vereinbarungen oder von EU-Standardverträgen eigenständige Verarbeitungen und Nutzungen personenbezogener Daten von Beschäftigten aus Deutschland nicht legitimieren lassen. Von den Rechtsexperten in den Konzernzentralen wird dies allerdings oft nicht oder anders gesehen. Um entsprechende Verarbeitungen und Nutzungen zu verhindern, bedarf es einer gesetzlichen Regelung, die enge Grenzen der Zweckbindung definiert und den Missbrauch deutlich stärker strafbewehrt.

---

[58] DHCP steht für Dynamic Host Configuration Protocol und ermöglicht die Zuweisung von Netzwerk-Konfigurations- und -Identifizierungsdaten an die Benutzer.

[59] Vgl. Internet-Site der Firma Splunk, San Francisco, de.splunk.com/

e) Compliance

Compliance heißt das Stichwort, das viele neue Anwendungen auf den Plan gerufen hat. Sicher gibt es in diesem Zusammenhang sinnvolle Anwendungen, aber leider auch eine Vielzahl solcher Anwendungen, die deutlich übers Ziel hinausschießen.

Eine wichtige Compliance-Regel ist z. B. der Schutz des geistigen Eigentums, wie das folgende Beispiel verdeutlicht.

Unter dem Schlagwort „Data Loss Prevention“ bietet die Firma Symantec eine Software an, die unter anderem den Inhalt von Mails, die die Firma verlassen, nach bestimmten Schlagworten automatisch durchsucht. Die vom Unternehmen vorgeschlagene Lösung sah vor, dass geheimhaltungswürdige Informationen entsprechend gekennzeichnet würden und nur verschlüsselt an vertrauenswürdige Partner verschickt werden dürften, die in einer „white list“ verzeichnet sind. Wenn eine Mitarbeiterin oder ein Mitarbeiter ein entsprechend eingestuftes Dokument unverschlüsselt oder an eine nicht registrierte Adresse verschicken wollte, sollte dieser Vorgang automatisch gestoppt und der Absender aufgefordert werden, sich an die betriebliche Regelung zu halten. Tut er dies nicht, sollte eine Alarmfunktion dafür sorgen, dass ein Mitarbeiter des Personalbereichs damit befasst würde und ggf. Maßnahmen gegen den Absender einleiten sollte.

Erst durch Betriebsvereinbarung wurde geregelt, dass für die in Deutschland ansässigen Betriebe auf die Eskalationsfunktion verzichtet wurde und lediglich die Versendung unterdrückt wird, bis der Absender den Text entweder verschlüsselt oder dafür Sorge getragen hat, dass der Empfänger vom System als vertrauenswürdige Instanz eingetragen wird.

Maßnahmen zur Einhaltung von Compliance-Regeln, die eine Erhebung, Verarbeitung oder Nutzung von Beschäftigtendaten notwendig machen, müssen bei der Bewertung der Erforderlichkeit gegen die mögliche Verletzung von Persönlichkeitsrechten abgewogen werden.

Gegen die Durchführung Compliance-begründeter Maßnahmen spricht in vielen Fällen, dass „Compliance“ selbst keine Rechtsnorm darstellt, die eine Verarbeitung personenbezogener Daten legitimieren könnte. Verbindet sich die Durchführung von Compliance-Maßnahmen mit Verstößen gegen geltendes Datenschutzrecht oder gegen einschlägige Normen des Betriebsverfassungsgesetzes, müssen sie unterbleiben, da dann ja gerade nicht die Rechtskonformität vorliegt, auf die Compliance-Konzepte zielen.

Legitimiert werden können Compliance-Maßnahmen durch kollektivrechtliche Regelungen in den Unternehmen. Betriebsvereinbarungen sind andere Rechtsvorschriften i. S. v. § 4 Abs. 1 BDSG und können Erhebungen, Verarbeitungen und Nutzungen ermöglichen. Allerdings müssen Betriebsräte wie Arbeitgeber mit Blick auf die allgemeine Vorgabe zum Schutz der freien Entfaltung der Persönlichkeit in § 75 Abs. 2 BetrVG sicherstellen, dass durch vereinbarte Compliance-Maßnahmen in das Persönlichkeitsrecht der Beschäftigten nicht unangemessen eingegriffen wird.

Durch Betriebsvereinbarungen kann insbesondere nicht zu Lasten der Beschäftigten vom Schutzstandard abgewichen werden, der durch das BDSG und andere datenschutzrechtliche Vorschriften begründet wird.[60] Den Regelungsbefugnissen der Betriebsparteien sind insoweit klare Grenzen gesetzt. Auch eine Zustimmung des Betriebsrats bzw. der Spruch einer Einigungsstelle kann Maßnahmen nicht legitimieren, die datenschutzrechtlich unzulässig sind.[61] Diese Vorgabe steht damit der Zulässigkeit von Compliance-Maßnahmen entgegen, durch die beispielsweise datenschutzrechtliche Mindeststandards ausgehöhlt werden.

Trotz dieser klaren kollektivrechtlichen Vorgaben finden sich in der Praxis immer wieder Betriebsvereinbarungen, die inhaltlich hinter den Mindestvorgaben des BDSG zurückbleiben. Grund für diese Situation ist nicht selten, dass Betriebsräte beim Datenschutz Zugeständnisse machen, um Arbeitsplätze zu sichern. Um dieses Problem zu beheben, ist eine Präzisierung der normativen Vorgaben notwendig. Eine klare datenschutzrechtliche Begrenzung für die Durchführung von Compliance-Maßnahmen im BDSG würde nicht nur die Persönlichkeitsrechte von Beschäftigten schützen, sondern auch die Handlungsmöglichkeiten von Betriebsräten stärken. Diese könnten auf der Grundlage bestehender Mitbestimmungsrechte von Arbeitgebern Regelungen verlangen, die die gesetzlichen Vorgaben uneingeschränkt garantieren.

Die Firma Cataphora bietet ein System zum angeblichen Schutz vor Insider-Bedrohungen an. Traditionelle Systeme basieren häufig auf der Überprüfung vordefinierter Regeln und statistischen Techniken, die nicht nur alle möglichen Arten von Fehlverhalten vorausberechnen müssen, sondern auch aufgrund ihrer statischen und somit vorhersagbaren Struktur umgangen werden können. Darüber hinaus konzentrieren sich traditionelle Systeme meist ausschließlich auf die Überwachung von Transaktionssystemen wie z. B. das SAP-System und erfassen nicht die riesigen Datenmengen, die durch die Kommunikation der

---

[60] DKKW-Klebe, § 87 Rn. 195 m. w. N.; a. A. noch BAG vom 27. 5. 1986 – 1 ABR 48/84, NZA 1986, 643.

[61] Vgl. BAG vom 15. 5. 1991 – 5 AZR 115/90, CR 93, 230 mit Anm. Wedde; Däubler, Rn. 781; Fitting, § 87 Rn. 253.

Mitarbeiter untereinander auf verschiedensten Kommunikationskanälen entstehen.

Die Monitoring-Lösungen für Insider-Bedrohungen der Firma Cataphora sollen diese beiden Probleme durch die Analyse der gesamten Bandbreite des elektronischen Datenverkehrs innerhalb eines Unternehmens überwinden.

Cataphora erstellt automatisch ein Modell, welches ein behauptetes „Normalverhalten" der Mitarbeiter abbildet. Dieses Modell beruht auf der Auswertung einer großen Anzahl unterschiedlicher elektronischer Informationen und kann erkennen, wenn etwas Außergewöhnliches – und somit etwas potenziell Problematisches – geschieht. Das System sei in der Lage, Abweichungen von der Norm zu identifizieren. Genau diese Abweichungen sind interessant, denn sie sollen Hinweise auf ein für das Unternehmen gefährliches Fehlverhalten liefern.

Das Modell zeigt, so die Herstellerbehauptung, die „wirklichen" Abläufe und die „wahren" Kommunikations- und Entscheidungsmuster – praktisch die sozialen Netzwerke – eines Unternehmens. Diese Netzwerke unterscheiden sich oft in wichtigen Punkten von den formellen Organigrammen und Prozessbeschreibungen. Das Modell kann jedes Detail in einem Unternehmen umfassen, welches auf irgendeine Art elektronisch gespeichert ist. Es kann nicht nur Aufzeichnungen von Transaktionen, sondern auch andere elektronischen Daten, wie z. B. E-Mails, Dokumente, Kalendereinträge, Einzelverbindungsnachweise oder auch Logdateien für Zugangssysteme beinhalten. Das Modell erfasst außerdem das Verhalten und die Interaktionen von Einzelpersonen und Arbeitsgruppen, inklusive deren elektronischer Kommunikation. Auch elektronische Dokumente und ihre Verteilung im Unternehmen können miteinbezogen werden. Weiterhin können interne und externe Ereignisse im Modell berücksichtigt werden. So werden z. B. in Bezug auf Diskussionen über die Änderungen von Preisen für bestimmte Produkte eines Unternehmens auch die Preise von Mitbewerbern im Modell abgebildet. Mit Hilfe dieses Modells ist es dann unter anderem möglich, verborgene Zusammenhänge zwischen bestimmten Personen aufzudecken. Es könnte sich dabei beispielsweise herausstellen, dass mehrere Personen, die in völlig unterschiedlichen Bereichen eines Unternehmens tätig sind, sich sehr gut kennen – vielleicht, weil sie früher an der gleichen Universität studiert haben. Die Kenntnis von solchen „Schatten-Netzwerken" ist ausschlaggebend, um die Motive und die Loyalität von Schlüsselpersonen anderen gegenüber zu verstehen – und dies kann durchaus zu einem Konflikt mit den Interessen des Unternehmens führen.[62]

---

[62] Internet-Seite der Firma Cataphora de.cataphora.com. Siehe auch: Manfred Dworschak: Im Netz der Späher, Der Spiegel 2/2011 vom 10. 1. 2011.

Da das System für das Erkennen potenzieller Probleme auf Abweichungen von „normalen“ Verhaltensmustern setzt, muss dieses „Normalverhalten“ natürlich vorher definiert werden. Zahlreiche Reports listen dann die Personen mit vom System entdeckten Abweichungen von der Normalität auf. Es können auch Netzwerk-Kontakte sichtbar gemacht werden, die über die fachlichen Zuständigkeiten hinaus gehen. Auf den Top-Rängen solcher Auswertungen steht dann oft das Kommunikationsverhalten der Vorstandssekretärinnen. Auch Zeitreihen über verändertes Kommunikationsverhalten lassen sich dank langer Speicherzeiten erstellen.

Um derartige Effekte zu vermeiden und Beschäftigte vor unzulässigen Ausforschungen zu schützen, ist es notwendig, in das BDSG klare Verbote sowie einschlägige Strafvorschriften einzuführen. Im strafrechtlichen Bereich müssten die bisher in § 44 BDSG vorgesehenen Tatbestände mit dem Ziel deutlich erweitert werden, die vorstehend beschriebenen weitgehenden Auswertungen zu verhindern.

Gesetzlich auszuschließen sind auch alle Regelungen, die aufgrund von in Computersprachen definierbaren Verhaltensregeln Alarme produzieren, die dann zu Kontrollmaßnahmen führen, beispielsweise wenn ein System die Arbeitszeiten eines Mitarbeiters beobachtet und Alarm schlägt, wenn sein Arbeitsverhalten nicht der vom System errechneten Norm entspricht, und er später oder früher als sonst üblich zur Arbeit erscheint.

Hinter diesen Bestrebungen steckt das Missverständnis, Sicherheit allein durch technische Vorkehrungen gewährleisten zu können. Bezogen auf derartige Systeme oder Systemfunktionen ist zu bedenken, dass sie schon heute zumeist ohne datenschutzrechtliche Grundlagen sind. Dies folgt bereits aus der Tatsache, dass es im Regelfall an der Erforderlichkeit dieser Systeme i. S. v. § 32 Abs. 1 Satz 1 BDSG fehlt. Würde deren Vorhandensein unterstellt, wäre es mit Blick auf § 4 Abs. 3 BDSG notwendig, Beschäftigte vor der Erhebung und Verarbeitung auf die damit verfolgten Zwecke hinzuweisen. Heimlichen Erhebungen, Verarbeitungen und Nutzungen personenbezogener Daten steht schließlich das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme entgegen, dass das Bundesverfassungsgericht in seinem Urteil zur „Online-Durchsuchung“ am 27. 2. 2008 begründet hat.[63]

---

[63] BVerfG vom 27. 2. 2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822; allgemein zu den Auswirkungen auf das Arbeitsrecht Wedde, AuR 2009, 373.

f) Die Herausforderung der Computersicherheit an die Gesetzgebung

Generell werden betriebliche Bestrebungen zur Verbesserung der Datensicherheit an Bedeutung gewinnen. Die zunehmende Vernetzung computerunterstützter Systeme erzeugt immanent eine neue Verwundbarkeit aller Einrichtungen, die Computer einsetzen, die längst auch schon in den Fokus militärischen Interesses gerückt ist, wie nicht zuletzt die Erfahrungen mit dem unter anderem zur Sabotage iranischer Atomanlagen eingesetzten Computervirus Stuxnet gezeigt haben.[64]

Softwaresysteme zur Gewährleistung computertechnischer Sicherheit werden in ihrem Umfang immer leistungsfähiger. Diese Leistungssteigerung erhöht zugleich die Gefahr, dass Leistungs- und Verhaltenskontrollen der Beschäftigten zunehmen. Ihr Einsatz lässt den Konflikt mit dem Schutz der Persönlichkeitsrechte unweigerlich an Schärfe gewinnen, eine Entwicklung, die von der Politik bis heute eher rat- und tatenlos hingenommen wird. Auch hier ist Handlungsbedarf geboten. Will man Entwicklungen wie im Umgang mit Waffen in den USA vermeiden, so ist staatliches Handeln angesagt. Wer in Deutschland eine Waffe besitzt oder gar mit ihr umgehen will, benötigt dazu eine besondere Genehmigung. Dabei schreibt das Waffengesetz eine Menge von Einschränkungen vor, insbesondere auch strenge Anforderungen an die Zuverlässigkeit und persönliche Eignung der handelnden Personen. Analog hierzu wäre der Einsatz von Sicherheitssoftware, die geeignet ist, die Persönlichkeitsrechte der überwachten Personen tiefgreifend zu verletzen, an entsprechende Auflagen zu binden, z. B.

- die Genehmigungspflicht zum Einsatz der beabsichtigten Sicherheitssysteme,
- gebunden an die Begründung der Notwendigkeit für den Einsatz, d. h. eine enge Zweckbindung,
- eine zeitliche Befristung der Erlaubnis für den Einsatz mit der Auflage, die Erfordernis nach Ablauf einer gesetzten Frist erneut nachzuweisen,
- den Nachweis struktureller Maßnahmen, die zu einer Begrenzung der Überwachungserfordernisse führen,
- die charakterliche Eignung der mit den Aufgaben betrauten Personen,
- den Nachweis von Mechanismen zur nachträglichen Kontrolle des Einsatzes der Anwendungen.

Missbrauch und Verstoß gegen die Auflagen müssten spürbar sanktioniert werden und sollten neben der Verhängung von Strafen auch den Entzug der Erlaubnis zur Folge haben.

---

[64] Vgl. Wikipedia-Eintrag zu Stuxnet:de.wikipedia.org/wiki/Stuxnet.

Die Bundesregierung arbeitet zurzeit an dem Entwurf für ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme[65] und betont darin die Bedeutung der „verantwortlichen Stelle“, die allein für die Verarbeitung der Daten zuständig sei, unabhängig von der „verarbeitenden Stelle“, also in der Regel dem Standort der Server. Wenn ein Unternehmen als verantwortliche Stelle die Einhaltung der in Deutschland geltenden Normen wegen eines Verarbeitungsstandorts in einem anderen Rechtsraum nicht garantieren kann, dann darf diese Verarbeitung nicht zulässig sein. Damit dies die gebührende Ernsthaftigkeit erfährt, muss die Unzulässigkeit über Bußgelder hinaus strafbewehrt sein. Dabei wird der Begriff der Lokalität wieder ins Zentrum der Überlegungen rücken müssen; wir kommen darauf später nochmals zurück.

7. Ausblick

Vernetzung und Miniaturisierung der Technik werden weiter fortschreiten. Prozessoren werden die Dinge des Alltags erobern. Dabei lassen immer mehr Anwendungen eine Personalisierung zu. Dazu benötigen sie personenbezogene Daten. Diese werden vom Benutzer nahezu unbemerkt eingesammelt,ohne dass jedes Mal nach ausdrücklichem Einverständnis gefragt wird. So lange diese Daten nur dem Benutzer für seinen persönlichen Gebrauch zur Verfügung stehen, wird niemand Einwände erheben. Doch die jeweiligen Diensteanbieter, allen voran Google, aber auch die sozialen Netzwerke wie Facebook oder Xing, sammeln die personenbezogenen Daten nicht nur als Voreinstellungen für die nächste persönliche Nutzung, sondern zu eigenen Zwecken, etwa zur weiteren Optimierung von Suchergebnissen oder zum Erraten von Vorlieben der Nutzer. Zumindest die eigenen Strategien zum Anbieten von Werbung machen ebenfalls Gebrauch von diesen Daten. Die Anbieter halten sich alle bedeckt mit Informationen, was genau sie mit den Daten anstellen und vor allem, wie lange die Daten gespeichert bleiben. Computer kennen keine Gnade des Vergessens. Während das menschliche Gehirn Vergessen sozusagen als mehr oder weniger automatisch verlaufende Selektion nach Relevanz benutzt, bedarf es ausdrücklicher und sehr spezifischer Befehle, wenn ein Computer das Löschen von Daten veranlassen soll. Hinzu kommt noch die rapide Verbreitung von Daten durch Kopieren an für den Verursacher nicht mehr überschaubaren Stellen. Das weiß jeder, der einmal ein Bild auf Facebook eingestellt hat.

---

[65] Christian Raum, Die Informationstechnologie ist in der Wirklichkeit angekommen, Interview mit Martin Schallbruch, IT-Beauftragter des Bundesministeriums des Inneren vom 4. 7. 2013, in: silicon.com Pressedienst vom 5. Juli 2013, www.it-newsletter.de/nl.php?id=545354.

a) Die Ungnade des Nicht-Vergessens

Am 25. Januar 2012 ist der Entwurf der Europäischen Kommission für eine Datenschutzverordnung offiziell von der zuständigen EU-Kommissarin Viviane Redding vorgestellt worden, die die derzeit geltende Datenschutzrichtlinie 95/46/EG ersetzen soll.[66] Artikel 17 dieser Verordnung formuliert ein neues Schutzrecht, das Recht auf Vergessenwerden. Über bekannte Löschungsverpflichtungen hinaus soll die datenverantwortliche Stelle, die ein personenbezogenes Datum öffentlich gemacht hat, bußgeldbewehrt verpflichtet sein, dieses Datum wieder aus dem Internet zu „entfernen“. Hierzu soll sie sämtliche öffentlich zugänglichen Hyperlinks auf dieses Datum sowie sämtliche öffentlich zugänglichen Kopien und Replikationen dieses Datums aus dem Internet entfernen bzw. entfernen lassen. Leider lässt der Entwurf offen, wie dieses Recht technisch durchzusetzen ist.

Der ehemalige Präsident des Welt-Automobilverbandes FIA, Max Mosley, klagte gegen Google, um das Verschwinden der Anzeige von widerrechtlich entstandenen intimen Fotos einer alten Sexparty in den Suchergebnissen löschen zu lassen.[67] Mosley argumentierte, dass ohne Google niemand auf der Welt diese Bilder überhaupt finden würde und dass Google sehr wohl wisse, dass die Fotos allesamt illegal zustande gekommen seien. In dem Streit geht es um den Grundkonflikt, wer das Recht im Internet dominiert, Gerichte oder Konzerne wie Google.

Die Thematik spielt nicht nur eine Rolle auf der weltpolitischen Bühne, sondern schickt sich an, auch den Alltag des Firmenlebens zu erobern. Viele Unternehmen haben bereits damit begonnen, intern ähnliche Systeme wie Facebook aufzubauen, in denen Beschäftigte ihre Vorlieben und Interessen, aber auch ihre besonderen Fähigkeiten darstellen können. Die Systeme erfreuen sich einer zunehmenden Interaktivität, was so viel heißt, wie dass Statements einer Person von anderen kommentiert und weiter verbreitet werden, bei multinationalen Konzernen natürlich über die Grenzen der deutschen Standorte hinweg. Ein Recht auf Zurückholen persönlicher Kommentare erscheint als Illusion.

Bisher bleibt nur der Appell an den sparsamen Umgang mit personenbezogenen Daten, insbesondere solchen Informationen, die die Grenze zwischen Arbeit und Privatsphäre verwischen. Die Forderung, dass ein Unternehmen verpflich-

---

[66] Europäische Kommission, Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM/2012/011 endgültig – 2012/0011 (COD) vom 25. 1. 2012.

[67] Für das Vergessen, Der Spiegel Nr. 35/2012, S. 144 ff.

tet werden sollte, den Links aller eine Person betreffenden Informationen nachzugehen, ist zweischneidig, denn jenseits dieses Zwecks würde ein solches Verfahren natürlich auch ein umfassendes Überwachungsinstrument voraussetzen.

b) Das Internet der Dinge

Das Internet der Dinge, gerne auch die Vierte Industrielle Revolution genannt, bezeichnet die Verknüpfung reell existierender Objekte, seien es wirkliche Dinge oder Menschen, über eine virtuelle Repräsentation und kann sie dann ähnlich behandeln wie das bekannte Internet der Daten. Die „Dinge“ müssen dafür nur eindeutig identifiziert werden, sei es über RFID-Chips[68] oder Barcodes. Dann lassen sich beispielsweise die Daten- und Warenströme direkt miteinander verbinden, vom Design vor der Produktion über die Transportwege und Zwischenhandelsstationen über die Verbraucher bis zur Entsorgung.

Die Fabrik der Zukunft integriert dank sog. Cyber-Physical-Systems (CPS) Produktion, Zulieferer und Kundenwünsche in Echtzeit. Dabei vernetzen sich die Microprozessoren automatisch sowohl untereinander als auch mit dem Internet. Umfassende CPS sollen es ermöglichen, dass Objekte über Anwendungs- und Branchengrenzen hinweg interagieren. Dieses Konzept macht den schon weit vorher erkennbaren Trend des Vermischens der „Cyberwelt“ mit der wirklichen Welt überdeutlich. Weder die Erhebung der Daten noch deren – letztlich weltweite – Verbreitung und Verwendung können von den Betroffenen noch kontrolliert werden. RFID, Biometrie, Sensoren, mobiles Internet, GPS, Geodatenverarbeitung und die vielen noch nur wenig integrierten IT-Systeme im Auto sind heute schon vorhandene Vorboten. Die aus solchen Beispielen entstehende allgegenwärtige Datenverarbeitung erfasst potenziell alle Lebensbereiche und diese nahezu vollständig.

Dadurch verschärft sich das Problem des Datenschutzes radikal, und es wird deutlich, dass es sich nicht durch nochmalige ergänzende Einzelvorschriften lösen lässt, die dem Wust der schon bestehenden vielen Regelungen hinzugefügt werden.

Viele der genannten Beispiele zeigen, dass – trotz aller Globalität – der Lokalität in Zukunft eine ganz entscheidende Rolle zukommen muss. Anwendungen wie im Zusammenhang mit dem Konzept der Cyber-Physical-Systems, die sich durch einen hohen Anteil überaus detaillierter Informationen auszeichnen und

---

[68] RFID-Chips (Radio Frequency Identification) sind Funketiketten und ermöglichen die automatische Identifizierung und Lokalisierung beliebiger Objekte.

darüber hinaus alle zumindest einen mittelbaren Personenbezug aufweisen, werden nur dann einen datenschutzrechtlich noch handhabbaren Schutz bieten können, wenn sie die beiden folgenden Bedingungen erfüllen:

- Anwendungen müssen lokal verkapselt werden können, d. h., die Verarbeitung der lokalen Informationen muss auf einen begrenzbaren Raum einschränkbar sein, so dass die Detailinformationen diesen verkapselten Raum nicht mehr verlassen können.
- Die Kommunikation des verkapselten Systems mit seiner Außenwelt darf nur über definierte Interfaces erfolgen, d. h., kein äußeres System darf direkt auf das „Innenleben“ des verkapselten Systems zugreifen, sondern kann zu diesem nur in Kontakt über das Interface treten.[69]

Bei der Gestaltung dieses Interfaces könnte dann auf die Vermeidung zumindest jeden direkten Personenbezugs geachtet werden, sei es durch Anonymisierung oder durch Aggregierung. So würde sich durchsetzen lassen, dass bei dem Paradebeispiel des sich selbst nachfüllenden Kühlschranks der Lieferant nur die zur Nachlieferung aufgebrauchter Produkte erforderliche Information erhielte und das Konsumverhalten der Kühlschrankbenutzer nicht ausforschbar würde. Der Lieferant könnte dann nur durch Speicherung der an ihn gerichteten „Requests“ lediglich wissen, was sein Kunde von ihm gekauft hat und daraus seine Schlüsse ziehen. Über die Geschäftsbeziehungen zu seinen Konkurrenten erführe er dagegen nichts.

Dieses Prinzip ist generalisierbar. Bei entsprechender Interface-Gestaltung könnten innerhalb einer betriebsinternen Anwendung die mit der Arbeit betrauten Menschen über den Personenbezug ihrer Daten verfügen; außerhalb dieser „verkapselten“ Miniaturwelt wäre der Personenbezug aber nicht mehr erkennbar.

Lokalität wird auch zur sozial verträglichen Lösung des Einsatzes von Sicherheitssoftware eine entscheidende Rolle spielen. Die Dinge lassen sich wesentlich leichter gestalten, wenn sie auf örtlich begrenzte (oder genauer: begrenzbare) Strukturen treffen. Die weltweite Vernetzung von allem mit allem auf gleicher Ebene stellt ein sicherheitstechnisch nur um den Preis einer Totalüberwachung lösbares Problem dar. Dies wäre der Eintritt in eine andere Zivilisation, die wir politisch nicht wollen können.

Das Thema Betriebsdatenverarbeitung, bei der eine Flut von eng maschinenbezogenen Steuerungsdaten mit Informationen über die an Maschinen geleisteter

---

[69] Verkapselung und Einschränkung der Kommunikation nach außen über definierte Interfaces mit eigenen Methoden für das Auslesen und Zurückgeben von Informationen sind aus einer schon seit 20 Jahren bekannten Programmiermethode, der sog. Objekttechnik längst bekannte Phänomene.

Arbeit vermischt wird, stellt ein ähnliches Problem dar. Das Schreckensbild der „gläsernen Arbeit“ bleibt dann verhindert, wenn die Informationen nur den direkt handelnden Personen zur Verfügung gestellt und im laufenden Arbeitsprozess sozusagen „verbraucht“ werden. Lokalität als Regelungsprinzip muss eine neue Bedeutung erlangen.

Für diese neuen Herausforderungen gibt es im Datenschutzrecht noch keine spezifischen Regelungen.[70] Die Bedingungen der Verkapselung und Einschränkung der Kommunikation über personenbezugsfreie Daten via definierter Interfaces sind Anforderungen an die Hersteller, denen gesetzliche Normen Nachdruck verleihen können.

---

[70] Vgl. Alexander Roßnagel: Nicht mehr zeitgemäß, Gastbeitrag in der Frankfurter Allgemeinen Zeitung vom 31. 5. 2011

II. Rechtliche Rahmenbedingungen

Die technischen Möglichkeiten für Kontroll- und Überwachungsmaßnahmen von Beschäftigten, die in ihren vielfältigen Facetten im ersten Teil dieser Darstellung beschrieben werden, sind Realität. Wohin sie sich weiter entwickeln werden, ist derzeit nicht absehbar. Es steht aber außer Frage, dass sie zu- und nicht abnehmen werden.

Die Werkzeuge, die im juristischen Bereich für die rechtliche Bewertung und Bewältigung dieser Situation zur Verfügung stehen, sind zumeist allgemeiner Natur und werden den spezifischen Anforderungen nicht gerecht, die aus der aktuellen Entwicklung der Informationstechnik folgen. Aus datenschutzrechtlicher Sicht bestimmt sich beispielsweise die Zulässigkeit der Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten in Arbeitsverhältnissen nach den allgemeinen Vorgaben des BDSG. Darüber hinaus ist in bestimmten Fällen der Rückgriff auf gesetzliche Spezialregelungen, wie die des Telekommunikationsgesetzes (TKG)[71] oder des Telemediengesetzes (TMG)[72], möglich. Alle genannten Gesetze berücksichtigen aber das besondere Abhängigkeitsverhältnis, in dem Bewerber und Arbeitnehmer sich im Rahmen eines Arbeitsverhältnisses befinden können, ebenso wenig wie hieraus resultierende Zwangslagen.

Bezogen auf konkrete arbeitsrechtliche Themen und Fragestellungen, wie beispielsweise das im ersten Teil beschriebene Kompetenzmanagement, das nur durchgeführt werden darf, wenn es hierfür eine freiwillige Einwilligung der Beschäftigten gibt (vgl. zum Kompetenzmanagement Abschnitt I.5.a), führt weder die Anwendung allgemeiner Rechtsregeln, noch der Rückgriff auf einschlägige Spezialgesetze zu zufriedenstellenden Ergebnissen. Damit obliegt es in der Praxis der Rechtsprechung, in Fortschreibung des geltenden Rechts, praktikable Lösungen zu entwickeln und festzuschreiben.

Bezogen auf technische Kontrollmöglichkeiten besteht im arbeitsrechtlichen Bereich eine ähnlich unklare Situation. Einschlägige gesetzliche Regelungen aus dem Bereich des Individualrechts enthalten keine spezifischen Vorgaben be-

---

[71] Telekommunikationsgesetz (TKG) vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 1 des Gesetzes vom 3. Mai 2012 (BGBl. I S. 958).

[72] Telemediengesetz (TMG) vom 26. Februar 2007 (BGBl. I S. 179), zuletzt geändert durch Artikel 1 des Gesetzes vom 31. Mai 2010 (BGBl. I S. 692).

züglich der Zulässigkeit von technischen Kontrollen der Beschäftigten bzw. der hierfür bestehenden Grenzen. Ebenso fehlen im Individualarbeitsrecht ausdrückliche normative Schutzmechanismen, die die Persönlichkeitsrechte der Beschäftigten vor technischen Kontrollen der Arbeitgeber schützen.

Eine vergleichbare Situation gibt es im kollektivrechtlichen Bereich: Die durch das BetrVG von 1972 garantierten Mitwirkungs- und Mitbestimmungsrechte sind in den letzten 40 Jahren nicht grundlegend an die neuen technischen Entwicklungen angepasst worden. Das Gesetz stammt aus einer Zeit, in der es keine PCs, sondern nur wenige Großrechner gab und zielte damals vorrangig auf die Regelung von Produktographen, Fahrtenschreibern, Filmkameras und ähnlichen aus heutiger Sicht schon fast antiquierten Kontrolleinrichtungen.[73] Folgerichtig enthält es in der Fassung aus dem Jahr 1972 keine spezifischen Mitbestimmungsrechte, die sich auf die erst später entstandene bzw. in Betrieben eingeführte Informations- und Kommunikationstechnik beziehen.

Trotz der stürmischen Entwicklung der Informationstechnik und ihres flächendeckenden Einsatzes in den Betrieben hat es der Gesetzgeber in den letzten vierzig Jahren lediglich bei vorsichtigen Modifikationen des BetrVG belassen, wie etwa der ausdrücklichen Aufnahme der „Informations- und Kommunikationstechnik“ als erforderliches Sachmittel in den Katalog des § 40 Abs. 2 BetrVG im Rahmen der letzten großen Novelle dieses Gesetzes im Jahre 2001. Allerdings bezieht sich diese Berücksichtigung nur auf den Bereich der internen Geschäftsführung des Betriebsrats. Sie hat keine Auswirkungen auf den Katalog der „echten“ Mitbestimmungsrechte.

Für die Bewältigung der im ersten Teil dieser Darstellung beschriebenen Entwicklungen und Fallbeispiele stehen Betriebsräten somit nur die allgemeinen Mitbestimmungstatbestände und die hieraus folgenden kollektiven Rechte zur Verfügung. Spezifische Mitwirkungs- und Mitbestimmungsrechte, die sich etwa auf die Wahrung des Grundrechts der Beschäftigten auf informationelle Selbstbestimmung und seiner Kodifizierungen im BDSG beziehen, fehlen im BetrVG. Vor diesem Hintergrund kommt in der Praxis dem Mitbestimmungsrecht des § 87 Abs. 1 Nr. 6 BetrVG bezüglich der Einführung und Anwendung von technischen Einrichtungen, die zur Verhaltens- und Leistungskontrolle der Arbeitnehmer bestimmt sind, eine besondere Bedeutung zu.

Mangels einer Anpassung der einschlägigen gesetzlichen Grundlagen im kollektivrechtlichen Bereich oblag es parallel zur Ausbreitung der Informations- und Kommunikationstechnik der Rechtsprechung, bestehende Regelungslücken

---

[73] Vgl. hierzu DKKW-Klebe, § 87 Rn. 168.

insbesondere auf der Grundlage von § 87 Abs. 1 Nr. 6 BetrVG auszufüllen. Einschlägige Entscheidungen der letzten 40 Jahre illustrieren bezüglich verschiedener IT-Anwendungen jeweils aktuelle Problemfelder. Von grundlegender Bedeutung ist in diesem Bereich die Entscheidung des Bundesarbeitsgerichts (BAG) vom 6. 12. 1983[74], mit der der Umfang des nach § 87 Abs. 1 Nr. 6 BetrVG bestehenden Mitbestimmungsrechts präzisiert wurde. Das BAG hat verdeutlicht, dass das Mitbestimmungsrecht des Betriebsrats bereits dann besteht, wenn eine technische Einrichtung für eine Überwachung lediglich geeignet ist. Das Mitbestimmungsrecht ist nach der Feststellung des BAG hingegen nicht davon abhängig, dass ein Arbeitgeber eine Überwachung auch durchführen will. Diese Entscheidung prägt den Spielraum, den Betriebsräte bezogen auf die Anwendung der Informations- und Kommunikationstechnik haben, bis heute maßgeblich.

Wichtige Entscheidungen gibt es darüber hinaus bezüglich der Nutzung von Informations- und Kommunikationstechniken durch Betriebsräte für ihre betriebliche Arbeit. In einer Entscheidung hatte das BAG im Jahre 1993[75] Betriebsräten noch den generellen Zugriff auf E-Mail-Verteiler verweigert. Mit dem Vordringen der E-Mail-Kommunikation hat sich die Rechtsprechung zu diesem Thema ebenso verändert wie die einschlägigen normativen Vorgaben im BetrVG. Nach der Aufnahme der Informations- und Kommunikationstechnik in § 40 Abs. 2 BetrVG ist die Erforderlichkeit der Nutzung entsprechender Technik in der Praxis nicht mehr grundsätzlich strittig.[76] Nur wenn es um ausgefallene oder neuartige Technikanwendung geht, bedarf es einer gesonderten Darlegung zur Erforderlichkeit durch Betriebsräte. Im Regelfall kann hingegen vom Vorliegen der Erforderlichkeit ausgegangen werden. Personalcomputer mit Internet-Zugriff sind inzwischen ebenfalls als erforderlich anzusehen.[77] Die Lösung bestehender normativer Defizite durch die Rechtsprechung sollte allerdings nicht darüber hinwegtäuschen, dass sie auf Dauer nicht grundlegende gesetzgeberische Festlegungen ersetzen kann.

Kein Mittel zur Erreichung des Ziels eines besseren Schutzes der Beschäftigten in Arbeitsverhältnissen ist der Regierungsentwurf für ein neues Beschäftigtendatenschutzgesetz, der zum 15. 12. 2010 vorgelegt wurde.[78] Dieser stellt nicht den Schutz der Beschäftigten in den Vordergrund, sondern die gegenläufigen

---

[74] BAG vom 6. 12. 1983 – 1 ABR 43/81, NJW 1984, 1476.

[75] BAG vom 17. 2. 1993 – 7 ABR 19/92, NZA 1993, 1515.

[76] Vgl. DKKW-Wedde, § 40 Rn. 163 ff.

[77] DKKW-Wedde, § 40 Rn. 170 m. w. N.

[78] Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes vom 15. 12. 2010, BT-Drs. 17/4230.

Verarbeitungsinteressen von Arbeitgebern. Deshalb ist es zu begrüßen, dass das Gesetzgebungsverfahren Anfang 2013 nicht wie geplant zu Ende geführt wurde. Unabhängig hiervon ist allerdings festzustellen, dass eine einschlägige gesetzliche Regelung, die den Schutz von Persönlichkeitsrechten der Beschäftigten in den Mittelpunkt stellt, unumgänglich ist.

Wenig hilfreich zur Erreichung dieses Ziels ist auch die EU-Grundschutzverordnung, die am 25. 1. 2012[79] vorgelegt wurde und die derzeit diskutiert wird. Die dort in Art. 82 bereits zu findenden Regelungen für das Beschäftigungsverhältnis sind zur Ausräumung bestehender Probleme ebenso wenig geeignet, wie inzwischen vorgeschlagene Einfügungen zu Einzelthemen, die diese Regelung erweitern sollen.[80]

Mit Blick auf die unbefriedigende gesetzliche Situation und im Angesicht der im ersten Abschnitt beschriebenen Praxisprobleme wird nachfolgend im Abschnitt II.1 der Rechtsrahmen beschrieben, der im arbeitsrechtlichen Bereich mit dem Ziel des Schutzes der Beschäftigten zur Anwendung kommt. Eingeleitet wird die Darstellung mit Hinweisen auf einschlägige Vorschriften des BDSG. Anschließend werden Mitwirkungs- und Mitbestimmungsmöglichkeiten beschrieben, die Betriebsräten auf Grundlage des BetrVG zur Verfügung stehen, um unzulässige oder unangemessene Verhaltens- und Leistungskontrollen der Beschäftigten auszuschließen oder zu regulieren.

Hieran schließen sich im abschließenden Abschnitt III Hinweise auf Lösungswege an, die es ermöglichen würden, bestehende Mitbestimmungsrechte der Betriebsräte zu optimieren und so im Ergebnis die Rechte der Beschäftigten optimal zu wahren. In diesem Darstellungsschritt werden insbesondere die Konzepte prozessorientierter Mitbestimmungsverfahren sowie die Einbindung von Auditverfahren diskutiert.

---

[79] Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), elektronisch abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF

[80] Vgl. zum Diskussionsstand etwa die „Inofficial Consolidated Version after LIBE-Committee Vote provided by the Rapporteur“ vom 22. Oktober 2013 (http://ddma.nl/wp-content/uploads/2013/10/DPR-Regulation-inofficial-consolidated-LIBE.pdf); zu den Auswirkungen Wedde, EU-Datenschutz-Grundverordnung – gut für den Beschäftigtendatenschutz? DANA 2014 148.

1. Rechtsrahmen des Beschäftigtendatenschutzes nach dem BDSG

Mangels einer spezialgesetzlichen Regelung zum Beschäftigtendatenschutz bestimmt sich die datenschutzrechtliche Zulässigkeit der Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten nach den allgemeinen Datenschutzvorgaben, die das BDSG enthält.

a) Verbotsgesetz mit Erlaubnisnormen

Die Zulässigkeit einer Erhebung, Verarbeitung und Nutzung personenbezogener Daten setzt gemäß § 4 Abs. 1 BDSG voraus, dass sie durch das Gesetz selbst oder durch eine andere Rechtsvorschrift erlaubt oder angeordnet wird. Alternativ kann die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch eine individuelle Einwilligung der Betroffenen legitimiert werden.

Soll Datenverarbeitung auf der Grundlage einer Einwilligung erfolgen, muss diese die Voraussetzungen erfüllen, die in § 4a BDSG genannt sind. Nach Satz 1 dieser Norm ist eine Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Bezogen auf die Erteilung einer Einwilligung im Rahmen eines Arbeitsverhältnisses gibt es grundsätzliche Zweifel, ob diese freiwillig erteilt wird.[81]

Bezüglich der Zulässigkeit von Datenverarbeitung im Arbeitsverhältnis ist § 32 BDSG eine gesetzliche Erlaubnisnormen i. S. v. § 4 Abs. 1 BDSG. Nach § 32 Abs. 1 Satz 1 BDSG dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung oder für die Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich ist. Der Begriff „erforderlich“ stellt gegenüber der bis 2009 geltenden Fassung des Gesetzes, die in § 28 Abs. 1 Satz 1 Nr. 1 BDSG das Verb „dienen“ enthält, eine Verengung der Verarbeitungsbefugnisse von Arbeitgebern dar. Die Erforderlichkeit ist nur gegeben, wenn bei der Prüfung die gegenläufigen Interessen von Arbeitgebern und Arbeitnehmern angemessen beachtet werden.[82]

Durch § 32 Abs. 1 Satz 2 BDSG wird Arbeitgebern die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zur Aufdeckung von Straftaten erlaubt, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat.

---

[81] Däubler, Rn. 150 f.; Wedde, DuD 2004, 169.

[82] Vgl. BVerfG vom 23. 10. 2006 – 1 BvR 2027/02, RDV 2007, 20; DKKW-Däubler, § 32 Rn. 14.

Weiterhin müssen die Verarbeitungsprozesse zur Aufdeckung erforderlich sein. Das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung darf nicht überwiegen, und Art und Ausmaß der Erhebung, Verarbeitung und Nutzung dürfen im Hinblick auf den Anlass nicht unverhältnismäßig sein. Die in der Norm genannten Erlaubnisvoraussetzungen sind zu Gunsten der Beschäftigten eng auszulegen. Die Regelung ist insoweit als Ausnahmevorschrift zu verstehen.[83]

Unabhängig vom Vorliegen der in § 32 BDSG genannten Voraussetzungen steht die Zulässigkeit der Datenverarbeitung unter dem generellen Vorbehalt, dass die allgemeinen Begrenzungen, die im Gesetz für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten zu finden sind, eingehalten werden. Diese allgemeinen Vorgaben kommen uneingeschränkt auf alle Beschäftigungsverhältnisse gemäß § 3 Abs. 11 BDSG zur Anwendung.

b) Datenvermeidung und Datensparsamkeit

Jede Erhebung, Verarbeitung und Nutzung personenbezogener Daten muss das in § 3a BDSG enthaltene Gebot der Datenvermeidung und Datensparsamkeit beachten. Nach dieser Vorschrift sind alle Datenverarbeitungsprozesse sowie die Auswahl und Gestaltung von Datenverarbeitungssystemen an dem Ziel auszurichten, so wenig wie möglich personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen. Erforderliche Daten sollen nach Möglichkeit anonymisiert oder pseudonymisiert werden, sobald dies möglich ist. Begrenzt wird die Verpflichtung zur Datenvermeidung und Datensparsamkeit von verantwortlichen Stellen und damit auch von Arbeitgebern durch die in § 3a Satz 2 BDSG angesprochene Verhältnismäßigkeit.

c) Zwecke

Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten muss mit Blick auf den Schutzzweck des BDSG bestimmten, gesetzlich legitimierten Zwecken dienen. Eine zweckfreie Erhebung, Verarbeitung oder Nutzung ist nicht zulässig. Bezogen auf Arbeits- und andere Beschäftigungsverhältnisse leitet sich das Fehlen der Zweckfreiheit bereits aus der gemäß § 32 Abs. 1 Satz 1 BDSG notwendigen Erforderlichkeit ab. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten kann nur erforderlich sein, wenn sie für die Erfüllung oder Umsetzung arbeitsvertraglich geschuldeter Maßnahmen notwendig ist.

---

[83] Vgl. Simitis-Seifert, § 32 Rn. 102.

Dies schließt etwa Erhebungen, Verarbeitungen und Nutzungen für Zwecke des Kompetenzmanagements aus (vgl. hierzu Abschnitt I.5.a.).

Handelt es sich um personenbezogene Daten, verlangt das BDSG an verschiedenen Stellen eine Festlegung der verfolgten Zwecke durch die verantwortliche Stelle, d.h. den Arbeitgeber. Die verantwortliche Stelle muss gemäß § 4 Abs. 3 Nr. 2 BDSG bei der Direkterhebung den Betroffenen die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung mitteilen.

Einschlägige Vorgaben zur Zweckbindung finden sich weiterhin in § 28 Abs. 1 Satz 2 BDSG. Hiernach sind bei der Datenerhebung, -verarbeitung und -nutzung für eigene Zwecke schon bei der Erhebung personenbezogener Daten konkrete Festlegungen zu den Zweckbestimmungen vorzunehmen. Fehlt es an der datenschutzrechtlich notwendigen Zweckbestimmung, steht dies der Annahme einer arbeitsrechtlichen Erforderlichkeit aus datenschutzrechtlicher Sicht entgegen.

Spätere Zweckänderungen sind nach dem BDSG grundsätzlich möglich. So sieht beispielsweise § 28 Abs. 2 BDSG vor, dass sie zur Wahrung berechtigter Interessen der verantwortlichen Stelle erfolgen können. Eingegrenzt wird diese Berechtigung zur Zweckänderung aber dadurch, dass kein Grund zu der Annahme bestehen darf, dass das schutzwürdige Interesse von Betroffenen an der Zweckänderung überwiegt. Ein solches überwiegendes Interesse von Beschäftigten kann gegeben sein, wenn die über TabletPCs erfassten Daten von Vertriebsmitarbeitern für die Herstellung von „Besuchsprofilen“ verwendet werden (vgl. die praktischen Beispiele in Abschnitt I.2.).

Die Notwendigkeit der Abwägung mit den schutzwürdigen Interessen der Betroffenen setzt berechtigten Zweckänderungen von verantwortlichen Stellen und somit auch von Arbeitgebern enge Grenzen.

Bezieht man die vorstehenden allgemeinen Regelungen zur Datenvermeidung oder Datensparsamkeit sowie zur Zweckbindung auf Beschäftigungsverhältnisse, folgt hieraus, dass Arbeitgeber bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten nicht frei sind. Im Gegenteil müssen sich von ihnen gewollte oder durchgeführte Datenverarbeitungen daran messen lassen, dass hierbei so wenige Daten wie möglich anfallen und dass diese ausschließlich vorher definierten Zwecken dienen. Dies steht beispielsweise einer pauschalen Speicherung von Beschäftigtendaten zu Archivierungszwecken entgegen.

d) Übermittlung von Beschäftigtendaten

Normative Begrenzung gibt es auch für die Weitergabe von Daten an Dritte außerhalb der verantwortlichen Stelle. Bedient sich ein Arbeitgeber beispielsweise für die Abwicklung von arbeitsrechtlichen Aufgaben eines Auftragnehmers, muss das gewählte Verfahren den Vorgaben entsprechen, die § 11 BDSG zur Auftragsdatenverarbeitung enthält. Das Vertragsverhältnis zwischen einem Arbeitgeber auf der einen und dem Auftragnehmer auf der anderen Seite muss sich auf die Durchführung von „Hilfsaufgaben“ beschränken.[84]

e) Dauer

Die Dauer zulässiger Verarbeitungen und Nutzungen steht unter dem grundsätzlichen Vorbehalt, dass Daten gemäß § 35 Abs. 2 Nr. 1 BDSG zu löschen sind, wenn es keinen Rechtsgrund für ihre weitere Speicherung mehr gibt. Unter bestimmten Umständen kann an die Stelle einer Löschung gemäß § 35 Abs. 3 BDSG eine Sperrung treten.

Diese normative Vorgabe macht es für den arbeitsrechtlichen Bereich unumgänglich, dass Arbeitgeber bei der Gestaltung von IT-Systemen von Anfang an festlegen, wie lange Daten vorgehalten werden sollen. Dies steht Vorratsdatenspeicherungen wie etwa der Aufbewahrung von Standortdaten entgegen (vgl. die praktischen Beispiele in Abschnitt I.2.a.). Diese Form der zweckfreien Speicherung entspricht zudem nicht den Grundsätzen des § 3a BDSG.

2. Kollektivrecht und Beschäftigtendatenschutz

Die Sicherung des Beschäftigtendatenschutzes, der sich zum Schutz der Persönlichkeitsrechte der Arbeitnehmer aus dem BDSG ableitet, gehört nicht zu den Themen, die das BetrVG Betriebsräten als unmittelbare Mitwirkungs- und Mitbestimmungsrechte zuweist. Insbesondere für die Durchsetzung individueller datenschutzrechtlicher Ansprüche von Beschäftigten fehlt es an einem direkten kollektivrechtlichen Mandat. Trotz dieses normativen Defizits lassen sich einschlägige kollektivrechtliche Handlungsspielräume und Handlungspflichten, die auf den Schutz von Persönlichkeitsrechten zielen, aus unterschiedlichen Vorschriften des BetrVG ableiten.

a) § 75 Abs. 2 BetrVG – Schutz und Förderung von Persönlichkeitsrechten

Die grundlegende Regelung des § 75 BetrVG enthält allgemeine Vorgaben für die Behandlung von Betriebsangehörigen. § 75 Abs. 1 BetrVG zielt darauf ab, unzulässige Benachteiligungen zu vermeiden. Zur Erreichung dieses Ziels wer-

---

[84] Vgl. etwa Simitis-Petri, § 11 Rn. 22 m. w. N.

den beispielhaft Diskriminierungsverbote benannt. Die Regelung in § 75 Abs. 2 Satz 1 BetrVG verpflichtet Arbeitgeber und Betriebsrat gleichermaßen, die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen. Neben dem Schutz beinhaltet die Norm auch die Förderung der freien Entfaltung der Persönlichkeit, mithin also eine Verpflichtung zum aktiven Handeln. Hinzu kommt in § 75 Abs. 2 Satz 2 die Verpflichtung, die Selbständigkeit und Eigeninitiative der Arbeitnehmer und Arbeitsgruppen zu fördern.

Aus § 75 Abs. 2 Satz 1 BetrVG folgt nicht nur eine allgemeine Verpflichtung, die für das gesamte Handeln von Arbeitgebern und Betriebsräten gilt. Sie schränkt gleichzeitig die Handlungs- und Regelungsmöglichkeiten der Betriebsparteien ein. Der von ihnen zu leistende Schutz der Arbeitnehmer beinhaltet die Notwendigkeit, rechtswidrige Eingriffe in die Persönlichkeitssphäre der Beschäftigten zu unterlassen.[85] Für die Praxis bedeutet dies, dass selbst einvernehmlich vereinbarte kollektivrechtliche Regelungen unzulässig und damit unwirksam sind, wenn sie Persönlichkeitsrechte von Beschäftigten in nicht hinnehmbarer Art und Weise verletzen.

Die in § 75 Abs. 2 Satz 1 BetrVG normierte Verpflichtung zum Schutz und zur Förderung der Persönlichkeitssphäre der Arbeitnehmer bezieht sich auf alle betrieblichen Maßnahmen bzw. auf alle Vorgaben und Anweisungen der Arbeitgeber. So sind beispielsweise unmittelbare Kontrollen des Eigentums von Beschäftigten (etwa Taschen- oder Fahrzeugkontrollen) ebenso wie Personenkontrollen nur dann zulässig, wenn sie erforderlich und verhältnismäßig sind und wenn hierbei die Würde der Betroffenen nicht verletzt wird.[86] Nicht erlaubt sind unter Anlegung dieses Maßstabs hingegen Formen von Personenkontrollen, die alle Verkäufer eines Unternehmens erfassen und die vor den Augen von Kunden am Ausgang eines Kaufhauses stattfinden. Das entsprechende Vorgehen bei der Modekette Hollister in Frankfurt wurde erst beendet, nachdem der Betriebsrat ein Beschlussverfahren eingeleitet hatte.[87]

Entsprechendes gilt für Kontrollen von Arbeitnehmern, die unter Einsatz von technischen Mitteln oder Gerätschaften erfolgen. Beispielsweise sind Videokontrollen immer ein schwerwiegender Eingriff in Persönlichkeitsrechte der betroffenen Beschäftigten. Offene Videokontrollen sind deshalb nur zulässig, wenn als Ergebnis einer umfassenden Rechtsgüterabwägung die schutzwürdigen Interessen des Arbeitgebers überwiegen. Etwas anderes gilt für heimliche Videokon-

---

[85] Vgl. DKKW-Berg, § 75 Rn. 115; GK-BetrVG-Kreutz, § 75 Rn. 102.

[86] Vgl. DKKW-Berg, § 75 Rn. 117 m. w. N.

[87] Vgl. www.zeit.de/news/2013-04/04/prozesse-hollister-schraenkt-kontrolle-von-mitarbeiter-taschen-ein-04152618

trollen. Diese sollen zwar nach der Rechtsprechung des 2. Senats des BAG in einer Entscheidung vom 21. 6. 2012 in bestimmten Einzelfällen zulässig sein.[88] Selbst wenn man der Argumentation des BAG folgen würde, wären Betriebsräte nicht verpflichtet, in vom Arbeitgeber gewollte heimliche Kontrollen einzuwilligen, wenn sie Alternativen sehen, die dem Arbeitgeber zumutbar sind.

In keinem Fall zulässig sind Kontrollen von Beschäftigten, die unter Einsatz von Abhörgeräten (etwa sog. „Wanzen“ oder mittels Mikrofon) erfolgen sowie das heimliche Mithören oder Aufnehmen von Telefongesprächen.[89]

Einer besonderen Gefährdung sind die Persönlichkeitsrechte von Arbeitnehmern ausgesetzt, wenn die Arbeit unter Nutzung von unterschiedlichen Anwendungen aus dem IT-Bereich erbracht wird. Diese Gefährdung resultiert daraus, dass dabei praktisch immer personenbezogene Daten anfallen, die genutzt werden können, um Verhaltens- und Leistungskontrollen durchzuführen. Um vor diesem Hintergrund den grundsätzlichen Vorgaben gerecht zu werden, die in § 75 Abs. 2 Satz 1 BetrVG enthalten sind, müssen Betriebsräte bei der Ausübung ihrer Mitwirkungs- und Mitbestimmungsrechte neben den Grundrechten auch die Vorgaben einschlägiger Schutzgesetze beachten. Sie müssen deshalb (wie auch der Arbeitgeber) dafür sorgen, dass die Schutzvorgaben und Rechtspositionen, die das BDSG enthält, bei der Ausübung ihrer Mitbestimmungsrechte umfassend beachtet werden.

Der sich aus dem Grundrecht auf informationelle Selbstbestimmung ableitende Regelungsgehalt des BDSG prägt somit das Handeln des Betriebsrats im Bereich der allgemeinen Aufgaben nach § 75 Abs. 2 Satz 1 BetrVG. Damit stellen die Schutznormen, die das BDSG enthält, einen Rahmen dar, der beim Abschluss von Vereinbarungen, durch die die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten geregelt wird, von Arbeitgebern wie von Betriebsräten zwingend zu berücksichtigen ist. Der Regelungsgehalt des BDSG findet auf diesem Weg als Grenze des Zulässigen von Erhebungen, Verarbeitungen und Nutzungen Eingang in die durch das BetrVG normierten Mitwirkungs- und Mitbestimmungsrechte.

---

[88] BAG vom 21. 6. 2012 – 2 AZR 153/11, NZA 2012, 1025.

[89] BAG vom 23. 4. 2009 – 6 AZR 189/09, NZA 2009, 974; vgl. auch DKKW-Berg, § 75 Rn. 121.

b) Überwachung der Regelungen zum Beschäftigtendatenschutz als allgemeine Aufgabe des Betriebsrats

Nach den allgemeinen Regelungen in § 80 Abs. 1 Nr. 1 BetrVG gehört es zu den Aufgaben des Betriebsrats, darüber zu wachen, dass zugunsten der Arbeitnehmer geltende Gesetze, Verordnungen und Unfallverhütungsvorschriften, Tarifverträge und Betriebsvereinbarungen durchgeführt werden. Die Regelung soll durch die Verankerung von Überwachungsaufgaben einerseits sicherstellen, dass Arbeitgeber Vorschriften einhalten, durch die Arbeitnehmer geschützt werden. Andererseits eröffnet sie Betriebsräten die Möglichkeit, einzelnen Arbeitnehmern bei der Durchsetzung ihrer Rechte gegenüber dem Arbeitgeber zu helfen.[90]

Zu den zugunsten der Arbeitnehmer geltenden Gesetzen i. S. v. § 80 Abs. 1 Nr. 1 BetrVG gehören die Vorschriften des BDSG, die auf Beschäftigungsverhältnisse i. S. v. § 3 Abs. 11 BDSG zur Anwendung kommen.[91] Die Überwachungsverpflichtung des Betriebsrats erstreckt sich damit insbesondere auch auf die Spezialregelung zum Beschäftigtendatenschutz in § 32 Abs. 1 BDSG.

Die Überwachungspflicht des Betriebsrats besteht unabhängig von der, die dem nach § 4f Abs. 1 BDSG zu bestellenden betrieblichen Datenschutzbeauftragten obliegt.[92] Im Ergebnis stehen zur Sicherung des Beschäftigtendatenschutzes zwei unterschiedliche und unabhängige Kontrollinstanzen zur Verfügung.[93]

Das kollektivrechtliche Überwachungsrecht eröffnet Betriebsräten umfassende Informations- und Beratungsmöglichkeiten. Nach § 80 Abs. 2 BetrVG sind sie zur Durchführung ihrer Aufgaben nach diesem Gesetz vom Arbeitgeber rechtzeitig und umfassend zu unterrichten. Darüber hinaus haben sie nach Maßgabe von § 80 Abs. 3 BetrVG einen Rechtsanspruch darauf, nach näherer Vereinbarung mit dem Arbeitgeber Sachverständige hinzuziehen, soweit dies zur ordnungsgemäßen Erfüllung ihrer Aufgaben erforderlich ist.

Das allgemeine Unterrichtungsrecht nach § 80 Abs. 2 Satz 1 BetrVG ist umfassend ausgestaltet.[94] Es ermöglicht Betriebsräten, sich auch im Bereich des Beschäftigtendatenschutzes ein umfassendes Bild von den Maßnahmen, die Arbeitgeber getroffen haben, zu verschaffen. Der gesetzliche Informationsan-

---

[90] Vgl. Fitting, § 80 Rn. 5; DKKW-Buschmann, § 80 Rn. 7.

[91] Vgl. BAG vom 17. 3. 1987 – 1 ABR 59/85, AP Nr. 29 zu § 80 BetrVG 1972.

[92] Vgl. DKKW-Buschmann, § 80 Rn. 15; Fitting, § 80 Rn. 7; Richardi-Thüsing, § 80 Rn. 8 und 57.

[93] Vgl. ähnlich Richardi-Thüsing, § 80 Rn. 8.

[94] Vgl. DKKW-Buschmann, § 80 Rn. 79 m. w. N.

spruch bezieht sich auf alle Detailfragen der Umsetzung des BDSG. Betriebsräte können damit insbesondere Informationen darüber verlangen, auf welcher Erlaubnisgrundlage i. S. v. § 4 Abs. 1 BDSG die Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten beruht. Ist keine Erlaubnisgrundlage erkennbar, steht dies der Zulässigkeit der Datenverwendung schon mit Blick auf § 4 Abs. 1 BDSG entgegen. In diesen Fällen könnte vom Arbeitgeber die Unterlassung der rechtswidrigen Datenverarbeitung gefordert werden. Kommt er dieser Aufforderung nicht nach, könnten die staatlichen Aufsichtsbehörden eingeschaltet werden.

Soweit Arbeitgeber personenbezogene Daten auf der Grundlage von Einwilligungen gemäß § 4a BDSG verarbeiten, können Betriebsräte weiterhin prüfen, ob diese aus datenschutzrechtlicher Sicht wirksam sind. Im Mittelpunkt einschlägiger Prüfungen kann insbesondere eine Bewertung stehen, ob die Einwilligung freiwillig i. S. v. 4a Abs. 1 Satz 1 BDSG ist.

Neben der datenschutzrechtlichen Wirksamkeit können Betriebsräte auf der Grundlage von § 80 Abs. 1 Nr. 1 BetrVG prüfen, ob die Erhebung, Verarbeitung und Nutzung personenbezogener Beschäftigtendaten den Vorgaben des § 3a BDSG genügt. Das dort verankerte Regelungsziel der Datenvermeidung und Datensparsamkeit muss sich nach § 3a Satz 1 BDSG bereits in Auswahl und Gestaltung von Datenverarbeitungssystemen niederschlagen. Betriebsräte können somit vom Arbeitgeber Darlegungen dazu verlangen, ob diese Vorgabe im konkreten Fall eingehalten wurde. Dies beinhaltet unmittelbar Zugang zu den Unterlagen, die der Auswahlentscheidung zugrunde lagen. Weiterhin können Betriebsräte unter Hinweis auf § 3a Satz 2 BDSG vom Arbeitgeber Aussagen dazu verlangen, inwieweit die Vorgaben der Anonymisierung und Pseudonymisierung im konkreten Fall bei der Gestaltung von Datenverarbeitungssystemen umgesetzt worden sind.

Das Informationsrecht gemäß § 80 Abs. 1 Nr. 1 BetrVG beinhaltet auch einen Anspruch auf Aussagen des Arbeitgebers dazu, wie den Vorgaben des § 35 BDSG bezüglich der Berichtigung, Löschung und Sperrung von Daten Genüge getan wird. Auf dieser Grundlage können Betriebsräte beispielsweise Auskunft dazu verlangen, nach welchen Kriterien und innerhalb welcher Zeiträume personenbezogene Daten gelöscht werden.

Informationen lassen sich auf Grundlage von § 80 Abs. 1 Nr. 1 BetrVG weiterhin zum Thema der Benachrichtigung der Betroffenen gemäß § 33 BDSG erlangen. Dieses Informationsrecht beinhaltet mit Blick auf § 33 Abs. 1 Satz 1 BDSG beispielsweise Aussagen dazu, ob Arbeitgeber ergänzend zu diesen im Betrieb vorhandenen Daten Informationen aus dem Internet abrufen (etwa aus sozialen Netzwerken im Zusammenhang mit Bewerbungsverfahren). Weiterhin müssen

Arbeitgeber auf der Grundlage von § 80 Abs. 1 Nr. 1 i. V. m. Abs. 2 BetrVG Betriebsräten darüber Auskunft erteilen, wie Verfahren ausgestaltet sind, die den Anforderungen des § 34 BDSG gerecht werden. Diese Norm zielt durch Auskunftsrechte zugunsten der Betroffenen darauf, Informationen der Beschäftigten darüber sicherzustellen, über welche personenbezogenen Daten ihr Arbeitgeber außerhalb der Direkterhebung verfügt.

Schließlich lassen sich auf der Grundlage von § 80 Abs. 1 Nr. 1 BetrVG Informationen darüber erlangen, welche Formen der Auftragsdatenverarbeitung i. S. v. § 11 BDSG erfolgen. Besonders bedeutsam ist diese Information bezüglich unterschiedlicher Formen der Auftragsdatenverarbeitung im Ausland. Der Informationsanspruch von Betriebsräten erstreckt sich nicht nur auf das Ob der Auftragsdatenverarbeitung, sondern unter Berücksichtigung von § 11 Abs. 2 BDSG auch auf deren genaue Ausgestaltung. Da Aufträge nach § 11 Satz 2 BDSG schriftlich zu erteilen sind, können Betriebsräte die Vorlage entsprechender Verträge vom Arbeitgeber verlangen. Diesem Verlangen kann der Arbeitgeber ein eigenes Geheimhaltungsinteresse nicht entgegenhalten. Diesem steht entgegen, dass Betriebsräte gemäß § 79 BetrVG verpflichtet sind, alle ihnen bekanntwerdenden geheimhaltungsbedürftigen Informationen nicht zu offenbaren und nicht zu verwerten. Soweit sind die Interessen von Arbeitgebern an der Vertraulichkeit entsprechender Unterlagen schon durch die gesetzliche Vorgabe hinreichend geschützt.

c) § 87 Abs. 1 Nr. 6 BetrVG – Schutz vor Verhaltens- und Leistungskontrollen durch Mitbestimmung

Betriebliche IT-Anwendungen verfügen nahezu immer über ein „eingebautes“ Kontrollpotenzial: Bei praktisch allen Eingaben und Verarbeitungs- bzw. Nutzungsvorgängen, die in einem elektronisch gesteuerten System stattfinden, werden Log-Dateien in unterschiedlicher Form erzeugt und regelmäßig auch gespeichert. Diese Dateien sind aus technischen Gründen längerfristig abruf- und auswertbar. Lassen sich Log-Daten auf bestimmte Beschäftigte beziehen, fallen personenbezogene oder personenbeziehbare Daten an. Im Regelfall werden neben der Aktion auch deren Datum und Uhrzeit gespeichert. Aus diesen Daten lassen sich mit geeigneten Programmen Verhaltens- und Leistungsinformationen über die Beschäftigten ableiten. Teilweise zielen erfasste Daten ausdrücklich darauf ab, Eingaben zu dokumentieren.

Diese technischen Möglichkeiten stehen in einem natürlichen Spannungsverhältnis zu Vorgaben des BDSG. So sind entsprechende Speicherungen und Auswertungen gemäß § 4 Abs. 1 i. V. m. § 32 Abs. 1 Satz 1 BDSG nur zulässig, wenn sie für die Durchführung des Beschäftigungsverhältnisses erforderlich sind. Diese datenschutzrechtlich vorausgesetzte Erforderlichkeit ist in vielen Fällen nicht durchgängig nachvollziehbar wie etwa bei den in Abschnitt I angesprochenen Skill-Datenbanken (vgl. insbesondere Abschnitt I.5.a.).

Weiterhin steht eine pauschale Speicherung von personenbezogenen Daten in Log-Files im Widerspruch zu dem in § 3a BDSG normierten datenschutzrechtlichen Grundsatz der Datenvermeidung und Datensparsamkeit. Mit Blick auf diese Vorschrift und auf die Vorgabe zur Datenlöschung in § 35 Abs. 2 BDSG müssten personenbeziehbare und personenbezogene Daten in Log-Files demnach immer dann gelöscht werden, wenn sie aus objektiver Sicht nicht mehr benötigt werden. Dieser Vorgabe stehen Speicherdauern von mehreren Monaten oder Jahren entgegen.

Eine pauschale Speicherung von personenbezogenen bzw. personenbeziehbaren Daten steht schließlich im Widerspruch zum Gebot der Zweckbindung in § 28 Abs. 1 Satz 2 BDSG, das von einer verantwortlichen Stelle verlangt, die Zwecke, für die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen. Eine solche Zweckbindung kann gegeben sein, wenn die Erhebung und Speicherung von personenbezogenen Daten in Log-Files oder vergleichbaren Dateien auf der Grundlage von § 31 BDSG ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherheit oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage erfolgt. In diesen Fällen rein technisch bedingter Erhebungen, Verarbeitungen und Nutzungen dürfen die Daten in Log-Files einerseits nicht für andere Zwecke verwendet werden und andererseits nicht unbefristet vorgehalten werden.

Schließlich steht der Erhebung und Speicherung von personenbezogenen Daten in den angesprochenen Dateien die Vorgabe in § 33 Abs. 1 Satz 1 BDSG entgegen, nach der eine Benachrichtigung der Betroffenen erfolgen muss, wenn erstmals personenbezogene Daten für eigene Zwecke ohne deren Kenntnis gespeichert werden. Bezogen auf eine umfassende oder langfristige Speicherung von personenbezogenen bzw. personenbeziehbaren Beschäftigtendaten sind die zitierten Vorgaben des BDSG insgesamt restriktiv zu interpretieren. Eine entsprechende Erhebung und Verarbeitung darf nach datenschutzrechtlichen Vorgaben nicht die Regel darstellen, sondern muss eine Ausnahme sein, die sich zudem aus einschlägigen Erlaubnistatbeständen herleiten muss. Diese Konzeption zielt unmittelbar auf die Wahrung einschlägiger Persönlichkeitsrechte und insbesondere auf die des Rechts auf informationelle Selbstbestimmung.

Die gleiche Zielrichtung wie in den vorstehend angesprochenen Normen des BDSG, nämlich die Vermeidung von unbeschränkten Datenerhebungen, -verarbeitungen und -nutzungen findet sich im BetrVG in § 87 Abs. 1 Nr. 6 wieder. Das hieraus folgende Mitbestimmungsrecht wird ausgelöst, wenn im Betrieb technische Einrichtungen eingeführt oder angewendet werden sollen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Es zielt auf den Persönlichkeitsschutz der Arbeitnehmer ab und stellt eine unmittelbare Umsetzung der Vorgabe in § 75 Abs. 2 BetrVG dar.[95] Zielrichtung der Vorschrift ist damit die Vermeidung unzulässiger bzw. die Regelung zulässiger Verhaltens- und Leistungskontrollen. Als unzulässig sind alle Kontrollmaßnahmen zu qualifizieren, die die Persönlichkeitsrechte der Beschäftigten in nicht gerechtfertigter Weise verletzen.[96]

Das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG kommt immer zur Anwendung, wenn es sich um Kontrollen durch technische Einrichtungen handelt. Der Mitbestimmungstatbestand wird ausgelöst, wenn technische Einrichtungen eigenständige Kontrollwirkungen entfalten.[97] Persönliche Überwachungen durch Menschen im betrieblichen Zusammenhang werden hingegen nicht erfasst.[98]

Das Mitbestimmungsrecht entsteht einerseits durch die Einführung technischer Einrichtungen, d. h. durch die Entscheidung, bestimmte Gerätschaften oder Systeme einzuführen. Daneben setzt es ein, wenn bereits vorhandene technische Einrichtungen im Betrieb angewendet werden.[99]

Weitere Voraussetzung für das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG ist eine Bestimmung der technischen Einrichtung zur Überwachung. Diese Vorgabe bezieht sich auf die Kontrollmöglichkeiten, die aufgrund der technischen Konzeption bestehen. Erfasst werden beispielsweise auch die schon angesprochenen Log-Dateien. Auf eine Überwachungsabsicht des Anwenders eines technischen Systems kommt es nicht an. Nach der Rechtsprechung ist eine Bestimmung zur Überwachung vielmehr bereits dann gegeben, wenn sie aufgrund der technischen Konzeption objektiv geeignet ist, Verhaltens- und Leistungsdaten von Beschäftigten zu erfassen und auszuwerten.[100]

Das Mitbestimmungsrecht ist weit gefasst und setzt ein, wenn eine technische Einrichtung personenbezogene oder personenbeziehbare Daten enthält, die sich in einer Weise auf konkrete Personen zurückführen lassen, die eine Verhaltens-

---

[95] Vgl. etwa BAG vom 29. 6. 2004 – 1 ABR 21/03, NZA 2004, 1278; ausführlich DKKW-Klebe, § 87 Rn. 166 m. w. N.

[96] Ähnlich Fitting, § 87 Rn. 253.

[97] Vgl. BAG vom 9. 9. 1975 – 1 ABR 20/74, AP Nr. 2 zu § 87 BetrVG 1972 Überwachung; Fitting, § 87 Rn. 227 m. w. N.

[98] Vgl. DKKW-Klebe, § 87 Rn. 16.

[99] Vgl. ausführlich DKKW-Klebe, § 87 Rn. 170 ff.; Fitting, § 87 Rn. 248, jeweils m. w. N.

[100] Vgl. grundsätzlich BAG vom 6. 12. 1983 – 1 ABR 43/81, AP Nr. 7 zu § 87 BetrVG 1972 Überwachung.

und Leistungskontrolle möglich machen würde. Der Auslösepunkt für das Mitbestimmungsrecht ist weit zu interpretieren.

Ein Maßstab für die Zulässigkeit von Verhaltens- und Leistungskontrollen i. S. d. § 87 Abs. 1 Nr. 6 BetrVG ist mit Blick auf die durch § 32 Abs. 1 Satz 1 BDSG vorgegebene Erforderlichkeit die Feststellung, dass entsprechende Überwachungen nicht in unzulässiger Art und Weise gegen einschlägige Grundrechte bzw. Schutznormen in anderen Gesetzen verstoßen. Bezogen auf das BDSG leitet sich ein Zulässigkeitsmaßstab aus den dort enthaltenen Grundsätzen ab. Die Erhebung und Verarbeitung von Daten, die Verhaltens- und Leistungskontrollen ermöglichen, ist überhaupt nur zulässig, wenn es hierfür eine datenschutzrechtliche Grundlage gibt. Mit Blick auf § 4 Abs. 1 BDSG stellt damit die Erforderlichkeit in § 32 Abs. 1 Satz 1 BDSG einen absoluten Maßstab dar. An diesem müssen sich Verhaltens- und Leistungskontrollen messen lassen, die ein Arbeitgeber durchführen will und zu denen er im Rahmen des Mitbestimmungsverfahrens gemäß § 87 Abs. 1 Nr. 6 BetrVG von Betriebsräten eine Zustimmung verlangt.

Entsprechende Vereinbarungen müssen sich im kollektivrechtlichen Bereich an der allgemeinen Vorgabe des § 75 Abs. 2 Satz 1 BetrVG messen lassen. Sie sind damit überhaupt nur zulässig, wenn eine Verletzung der Persönlichkeitsrechte der Beschäftigten ausgeschlossen ist. Ist diese Voraussetzung nicht gegeben, können und dürfen Betriebsräte entsprechenden Erhebungen und Verarbeitungen in Ausübung ihres Mitbestimmungsrechts nach § 87 Abs. 1 Nr. 6 BetrVG nicht zustimmen.

Im Bereich des datenschutzrechtlich Zulässigen sind Betriebsräte und Arbeitgeber damit bei der Ausgestaltung entsprechender Verhaltens- und Leistungskontrollen in Betriebsvereinbarungen nicht frei. Mit Blick auf die Persönlichkeitsrechte der Beschäftigten müssen sie vielmehr solche Verhaltens- und Leistungskontrollen wählen, die so wenig wie möglich in geschützte Persönlichkeitsrechte der Beschäftigten eingreifen. Soweit möglich muss damit das zur Verfügung stehende mildeste Mittel eingesetzt werden.[101]

d) § 87 Abs. 1 Nr. 7 BetrVG – Gesundheitsschutz als Mittel des Beschäftigtendatenschutzes

Ein weiteres Mitbestimmungsrecht, das Auswirkungen auf den Bereich des Beschäftigtendatenschutzes haben kann, enthält § 87 Abs. 1 Nr. 7 BetrVG. Nach dieser Vorschrift hat der Betriebsrat mitzubestimmen bei Regelungen über die

---

[101] Vgl. hierzu etwa BAG vom 14. 12. 2004 – 1 ABR 34/03, AuR 2005, 456.

Verhütung von Arbeitsunfällen und Berufskrankheiten sowie über den Gesundheitsschutz im Rahmen gesetzlicher Vorschriften oder der Unfallverhütungsvorschriften. Das Mitbestimmungsrecht besteht, wenn es Arbeitsschutzvorschriften in Gesetzen oder Verordnungen gibt, die dem Arbeitgeber Gestaltungsspielräume eröffnen. Existieren diese nicht, weil etwa ein Gesetz zwingende Vorgaben macht, entsteht das Mitbestimmungsrecht nicht.

Einschlägige Regelungen, die das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 7 BetrVG auslösen, finden sich in Gesetzen sowie in Rechtsverordnungen aus dem Bereich des Arbeits- und Gesundheitsschutzes.[102] Für den hier zu bewertenden Zusammenhang ist insbesondere die aufgrund von § 19 Arbeitsschutzgesetz (ArbSchG)[103] ergangene Bildschirmarbeitsverordnung (BildscharbV)[104] von Bedeutung.

Nach § 4 Abs. 1 BildscharbV hat der Arbeitgeber geeignete Maßnahmen zu treffen, damit Bildschirmarbeitsplätze den Anforderungen des Anhangs zur Verordnung sowie sonstigen Rechtsvorschriften entsprechen. Im Anhang zur BildscharbV findet sich in Nr. 22 die Vorgabe, dass ohne Wissen der Benutzer keine Vorrichtung zur qualitativen oder quantitativen Kontrolle verwendet werden darf. Aus dieser Vorgabe folgt unmittelbar, dass Beschäftigte vor heimlichen Überwachungen geschützt werden müssen. Dies hat unmittelbaren Einfluss auf die Ausgestaltung von betrieblichen IT-Systemen. Arbeitgeber müssen diese so einrichten, dass jegliche Kontrollmaßnahmen den Betroffenen bekannt sind. Hierauf können Betriebsräte in Wahrnehmung ihres Mitbestimmungsrechts ergänzend zu dem nach § 87 Abs. 1 Nr. 6 BetrVG hinwirken.

e) Ergänzende Mitwirkungs- und Mitbestimmungsrechte

Aus dem BetrVG lassen sich bezogen auf den Beschäftigtendatenschutz ergänzende Mitwirkungs- bzw. Mitbestimmungsrechte aus einer Reihe weiterer Vorschriften herleiten. So kann die Wahrnehmung der Mitbestimmungsrechte nach § 87 Abs. 1 Nr. 2 und 3 BetrVG bzgl. der Lage und Länge der betriebsüblichen Arbeitszeit dazu genutzt werden, die Erhebungsmöglichkeiten des Arbeitgebers auf bestimmte Arbeitszeitfenster zu reduzieren. Ein Beispiel stellen Regelungen wie die bei Volkswagen dar, nach denen E-Mails nur in bestimmten Zeitfenstern

---

[102] Zur Anwendbarkeit bei Rechtsverordnungen vgl. Fitting, § 87 Rn. 282; DKKW-Klebe, § 87 Rn. 211.

[103] Arbeitszeitgesetz vom 6. 6. 1994 (BGBl. I S. 1170, 1171), zuletzt geändert durch Artikel 3 Absatz 6 des Gesetzes vom 20. 4. 2013 (BGBl. I S. 868).

[104] Bildschirmarbeitsverordnung vom 4. 12. 1996 (BGBl. I S. 1843), zuletzt geändert durch Artikel 7 der Verordnung vom 18. 12. 2008 (BGBl. I S. 2768).

abgerufen und versendet werden können.[105] Entsprechende Regelungen können eingesetzt werden, um Kontrollbefugnisse des Arbeitgebers auf die Arbeitszeit zu reduzieren, auch wenn Beschäftigte betriebliche Geräte privat nutzen dürfen.

Datenerhebung erfolgt teilweise über Personalfragebogen. Betriebsräte haben diesbezüglich nach § 94 Abs. 1 BetrVG ein zwingendes Beteiligungsrecht, nach dem der Inhalt der Personalfragebogen ihrer Zustimmung bedarf. Insoweit können sie sicherstellen, dass der Arbeitgeber nur solche Daten erheben darf, die erforderlich i. S. v. § 32 Abs. 1 Satz 1 BDSG sind.

Weitere einschlägige Mitwirkungs- bzw. Mitbestimmungsrechte lassen sich aus Vorschriften wie etwa den §§ 96 ff. BetrVG für den Bereich der Berufsbildung, aus § 99 BetrVG bezüglich personeller Einzelmaßnahmen sowie beim Vorliegen der entsprechenden Anwendungsvoraussetzungen aus § 111 BetrVG bezüglich Betriebsänderungen ableiten.

f) Probleme

Trotz des vorstehend angesprochenen Problems einer fehlenden Anpassung des BetrVG 1972 an die technische Entwicklung stehen Betriebsräten damit im Ergebnis wirksame Mitwirkungs- und Mitbestimmungsmöglichkeiten zur Verfügung, die sie einsetzen können, um den Beschäftigtendatenschutz sicherzustellen. Die Umsetzung bestehender Rechte trifft allerdings auf eine Reihe von praktischen Schwierigkeiten. Ein Kernproblem ist hierbei das hohe Entwicklungstempo im Bereich der Informationstechnik. Die feststellbare Innovations- und Veränderungsgeschwindigkeit führt in der Praxis dazu, dass abgeschlossene Regelungen aufgrund der hiermit einhergehenden Systemveränderungen oftmals mit dem ersten Software-Upgrade leerlaufen. Darüber hinaus sind Betriebsräte teilweise nicht in der Lage, notwendige Veränderungen von Betriebsvereinbarungen, die an die technische Entwicklung angepasst sind, einzuhalten und durchzuführen. Insbesondere zeitlich stoßen engagierte Betriebsräte an ihre Grenzen.

Ein Grundproblem stellt in diesem Zusammenhang die fehlende IT-Fachkunde vieler Betriebsräte dar. Sofern es sich nicht um Beschäftigte handelt, die selbst im IT-Bereich tätig sind, fällt es Betriebsräten oft schwer, technische Innovationen in der ganzen Breite ihrer Auswirkungen zu verstehen und bezüglich ihrer

---

[105] Vgl. etwa Blackberry-Pause: VW-Betriebsrat setzt E-Mail-Stopp nach Feierabend durch, Spiegel-Online vom 23. 12. 2001, http://www.spiegel.de/wirtschaft/service/blackberry-pause-vw-betriebsrat-setzt-e-mail-stopp-nach-feierabend-durch-a-805524.html.

kollektivrechtlichen Wirkung einschätzen zu können. Die nach § 37 Abs. 6 BetrVG bestehenden Möglichkeiten der Aus- und Weiterbildung von Betriebsräten sollen hierfür zwar einen Ausgleich darstellen. In der Praxis ergibt sich immer das Problem, dass die Teilnahme an Schulungsveranstaltungen zu neuen technischen Anwendungen von der Rechtsprechung teilweise noch nicht als erforderlich anerkannt ist.[106]

Gibt es im Betrieb Fachleute für bestimmte technische Anwendungen, können Betriebsräte auf der Grundlage von § 80 Abs. 2 Satz 3 BetrVG auf deren Hilfe als betriebliche Auskunftspersonen zurückgreifen. Die Einbeziehung von Auskunftspersonen setzt allerdings voraus, dass sie das Vertrauen des Betriebsrats genießen. Betriebsräten steht deshalb ein Entscheidungsspielraum bezüglich der Person zu, die hinzugezogen werden soll.[107]

Ähnlich stellt es sich mit der Möglichkeit dar, externen Sachverstand einzusetzen. Betriebsräte haben zwar nach § 80 Abs. 3 BetrVG grundsätzlich einen Anspruch darauf, bei der Durchführung ihrer Aufgaben Sachverständige hinzuziehen, soweit dies zur ordnungsgemäßen Erfüllung ihrer Aufgaben erforderlich ist. Die Hinzuziehung bedarf aber immer einer näheren Vereinbarung mit dem Arbeitgeber. Im Einzelfall kann dies dazu führen, dass über die Erforderlichkeit zeitaufwändig vor den Arbeitsgerichten gestritten werden muss. Diese zeitliche Komponente kann in der Praxis dazu führen, dass die Zuziehung eines Sachverständigen sich im Fall des Erfolgs eines Betriebsrats vor Gericht erledigt haben kann, weil ein neues System inzwischen längst eingeführt oder ein bestehendes verändert wurde.

Bezogen auf die Möglichkeiten zur Internationalisierung von Arbeit, die IT-Anwendungen bieten, stellt sich für Betriebsräte zudem das Problem, dass ihre kollektivrechtlichen Möglichkeiten durch das Territorialitätsprinzip[108] geografisch auf den Anwendungsbereich des BetrVG und damit auf die Bundesrepublik Deutschland beschränkt sind. Hieraus leitet sich einerseits die Feststellung ab, dass die gesetzlichen Mitwirkungs- und Mitbestimmungsrechte immer bestehen, wenn Daten von Beschäftigten durch Arbeitgeber in der BRD erhoben, verarbeitet und genutzt werden. An diesen Rechten ändert sich nichts, wenn eine vom Arbeitgeber veranlasste Datenverarbeitung durch Unternehmen erfolgt, die in anderen Staaten angesiedelt sind. Insbesondere innerhalb von grenzüberschreitenden Konzernstrukturen ergibt sich aber in diesen Fällen die

---

[106] Vgl. zu Schulungsansprüchen und ihren Grenzen etwa DKKW-Wedde, § 37 Rn. 131.

[107] Vgl. DKKW-Buschmann, § 80 Rn. 152.

[108] Vgl. hierzu etwa BAG vom 22. 3. 2000 – 7 ABR 34/98, NZA 2000, 1119; BAG vom 22. 7. 2008 – 1 ABR 40/07, NZA 2008, 1248.

Gefahr, dass bestehende Mitwirkungs- und Mitbestimmungsrechte und hierauf basierende verbindliche Vereinbarungen ausgehöhlt werden, wenn etwa bestimmte IT-Aufgaben von Konzernunternehmen im Ausland wahrgenommen werden. Damit steigt das Risiko, dass es dort zu unzulässigen Leistungs- und Verhaltenskontrollen kommen kann. Allenfalls lassen sich für diese Fälle Kontrollrechte durch die Ausgestaltung von Betriebsvereinbarungen vorsehen. Dieses Problem gilt insbesondere, wenn Konzerne ihre IT-Systeme, die personenbezogenen Daten enthalten, europa- oder weltweit zentral aufstellen und betreiben. Es stellt sich aber gleichermaßen bei Konzepten wie CloudComputing oder Offshoring. Auch in diesen Fällen sind bestehende Mitwirkungs- und Mitbestimmungsrechte praktisch nicht mehr in der Lage, Regelungen entlang der vom Arbeitgeber geschaffenen Verarbeitungsstränge zu schaffen. Damit laufen bestehende Mitwirkungs- und Mitbestimmungsrechte in vielen Fällen leer.

III. Neue Strategien und Konzepte

Die Bestandsaufnahme der aktuellen technischen Entwicklungen und praktischen Probleme im ersten Teil dieser Darstellung verdeutlicht, dass es auf der individual- wie auf der kollektivrechtlichen Ebene für Beschäftigte und für Betriebsräte eine Fülle neuer Herausforderungen gibt. Für deren Bewältigung stehen nur die vorstehend beschriebenen allgemeinen gesetzlichen Anspruchsgrundlagen und begrenzte Mitwirkungs- und Mitbestimmungsrechte aus dem BetrVG zur Verfügung. Um vor diesem Hintergrund Handlungsmöglichkeiten zu garantieren, ist es notwendig, über neue Ansätze und Konzepte zu diskutieren, die es auf der Grundlage des bestehenden Rechts ermöglichen, negative Effekte zulasten der Beschäftigten auszuschließen oder zumindest begrenzen zu können. Wie entsprechende Ansätze aussehen, wird im folgenden Teil angesprochen. Vorgestellt werden Lösungsansätze, die es, ausgehend vom geltenden Rechtsrahmen, ermöglichen würden, identifizierte Regelungsprobleme bezüglich neuer IT-Anwendungen auf der Grundlage organisatorischer und/oder technischer Verfahren zu reduzieren.

Untersucht werden insbesondere die Möglichkeiten von prozessorientierten Regelungskonzepten, von Audits und Zertifizierungsverfahren, von Sanktionsmechanismen sowie Ansatzpunkte für eine kollektivrechtliche IT-Folgenabschätzung.

1. Prozessorientierte Betriebsvereinbarungen

Die in Abschnitt I beschriebenen Fallbeispiele und Entwicklungstrends verdeutlichen, dass Anforderungen, die sich Betriebsräten im Zusammenhang mit neuen IT-Trends oder IT-Anwendungen stellen, sich längst nicht mehr auf die Einführung einer abschließend definierten Software oder eines abgrenzbaren IT-Systems beschränken. Tatsächlich sind Betriebsräte in vielen Fällen damit konfrontiert, dass im IT-Bereich komplexe Gesamtanwendungen geschaffen werden, deren einzelne Komponenten oft nicht mehr abgrenzbar und identifizierbar sind. Hinzu kommt, dass es insbesondere bei Anwendungen aus dem Bereich „Software as a Service“ (SaaS) nur noch schwer möglich ist, einen Einführungs- bzw. Veränderungspunkt für Softwareanwendungen zeitlich vorab exakt zu bestimmen. Grund hierfür ist die, als ein Vorteil von SaaS gepriesene ständige automatische Aktualisierung der Systeme. Diese Situation führt dazu, dass die mit der Einführung konkreter Anwendungen zusammenhängenden Mitbestimmungsrechte von Betriebsräten oft leerlaufen. Dies zeigt sich beispielsweise an Betriebsvereinbarungen, bei denen etwa zulässige Datenfelder, Reports oder Berechtigungen in Anlagen aufgeführt werden. Um diese Anlagen aktuell zu halten, ist ein hoher Pflege- und Kontrollaufwand notwendig. Kann dieser nicht erbracht werden, werden Betriebsvereinbarungen als Folge der Veränderungen nach kurzer Zeit entwertet.

Abzusehen ist das angesprochene Leerlaufen insbesondere bei SaaS-Angeboten, die für Unternehmen zentral in der Cloud vorgehalten werden. Derzeit wird beispielsweise von großen Software-Anbietern angeboten, komplexe HR-Systeme auf SaaS-Basis direkt aus der Cloud zu betreiben. Versprochen werden erhebliche Performance-Steigerungen und Kostensenkungen.

Umgesetzt werden derartige Konzepte in größeren Konzernen auf der Grundlage komplexer IT-Verträge und Regelwerke, die teilweise weltweit Gültigkeit haben. Änderungen der Vertragswerke aufgrund nationaler oder unternehmensspezifischer Anforderungen sind zumeist schwierig. Betriebsräten wird es bei derartigen Angeboten praktisch unmöglich, bestehende Mitbestimmungsrechte, wie insbesondere das nach § 87 Abs. 1 Nr. 6 BetrVG, noch wirksam und nachhaltig einzufordern und durchzusetzen. Die Unmöglichkeit resultiert daraus, dass der lokale Arbeitgeber in der Praxis oft nicht mehr weiß, welche Versionen einer Software im Auftrag verwendet werden, wann Veränderungen technischer oder grundlegender Art anstehen und welche generellen Auswertungs- und Kontrollmöglichkeiten in SaaS-Anwendungen integriert sind. Hinzu kommen teilweise weitgehende und unternehmensübergreifende Reporting-Möglichkeiten. Bezogen auf das angeführte Beispiel einer SaaS-Lösung (vgl. Abschnitt I.2.c.) führt dies dazu, dass der zuständige Betriebsrat die von ihm vertretenen Beschäftigten nicht mehr wirksam davor schützen kann, dass neue Reporting-Möglichkeiten zu ihren Lasten eingeführt werden.

Probleme würden sich auch aus einer Kombination vorhandener Systeme mit SaaS-Lösungen ableiten, wenn etwa Informationen aus der Flottensteuerung und dem Geräte-Tracking mit vorhandenen Daten in einer Cloud verknüpft würden (vgl. Abschnitt I.3.).

Aber auch im „konventionellen" Rahmen, das heißt bei der Anwendung bisher üblicher betrieblicher Systeme, tritt allein aufgrund der hohen Innovationsgeschwindigkeit von IT-Anwendungen immer wieder das Problem auf, dass Betriebsräte weder die Einhaltung abgeschlossener Vereinbarungen wirksam und effektiv kontrollieren können, noch dass sie deren Regelungsinhalt zeitnah und effektiv an technische Veränderungen anpassen können.

Aber selbst wenn der notwendige Anpassungsprozess in der betrieblichen Praxis geleistet wird, bedeutet dies nicht, dass der Regelungsgehalt von Vereinbarungen tatsächlich rechtskonform umgesetzt wird. Auch für diese Fälle lassen sich vielmehr Anpassungsprobleme erkennen. Dies macht beispielsweise ein Blick auf Betriebsvereinbarungen deutlich, die es in einer Reihe von Unternehmen zu Personalinformationssystemen bzw. zu HR-Systemen gibt. Teilweise enthalten diese Betriebsvereinbarungen bezüglich bestehender Auswertungsmöglichkeiten die Vorgabe, dass alle zulässigen Reports vollständig und abschließend in einer Anlage dokumentiert werden müssen. In der Praxis führt diese Vorgabe häufig dazu, dass einerseits Arbeitgeber Probleme damit haben, die Anlagen aktuell zu halten. Andererseits sind Betriebsräte aufgrund der Fülle von Informationen zu beabsichtigten neuen Auswertungen oft nicht mehr in der Lage, effektiv zu bewerten, ob diese zulässig sind oder nicht.

Die vorstehend angesprochenen Formen von IT-Betriebsvereinbarungen, die eine bestimmte Anwendung in einer Kombination von „statischer“ Betriebsvereinbarung und „flexibler“ Anlagen regeln, geraten bezogen auf komplexe und vernetzte IT-Anwendungen an ihre Grenzen. Betriebsräte sind schon aus zeitlichen Gründen oft nicht mehr in der Lage, permanente Veränderungen der Systeme aus mitbestimmungsrechtlicher Sicht qualifiziert einschätzen und regelungstechnisch begleiten zu können. Hinzu kommt eine zunehmende Komplexität technischer Veränderungen und Weiterentwicklungen.

Aus dieser Situation resultieren Regelungsdefizite, die im Ergebnis bestehende Mitbestimmungsrechte beschränken oder aushöhlen. Diese negativen Effekte könnten durch eine Ausgestaltung von Betriebsvereinbarungen ausgeschlossen oder zumindest begrenzt werden, die bei ihrer Konzeption absehbare Veränderungen von Anfang an berücksichtigen. Regelungstechnisch müssten sie einerseits garantieren, dass bestehende Mitbestimmungsrechte gewahrt werden. Andererseits müssten sie es Anwendern bzw. Arbeitgebern ermöglichen, notwendige Anpassungen (insbesondere im technischen Bereich) kurzfristig durchführen zu können.

Letztlich geht es damit um eine inhaltliche Ausgestaltung von Betriebsvereinbarungen, die Veränderungsprozesse in ihren Regelungsmechanismus integrieren. Umsetzbar ist diese Anforderung durch Ausgestaltungen, die einerseits notwendige technische Anpassungen ohne nachhaltigen Mitbestimmungsbedarf im Rahmen eines Automatismus zulassen und die andererseits sicherstellen, dass relevante Veränderungen im Einklang mit Vorgaben des BetrVG erfolgen. Für Betriebsräte hätte ein solches Konzept den Vorteil, dass nicht permanent alle Veränderungen darauf überprüft werden müssten, ob hierdurch einschlägige Mitbestimmungsrechte ausgelöst werden. Für den Arbeitgeber beinhalten derartige Konzepte einen erheblichen Zeitgewinn und damit ein großes Einsparungspotenzial.

Die auf den ersten Blick gegensätzlichen Anforderungen einer solchen Konzeption können dadurch aufgelöst werden, dass in einer Betriebsvereinbarung zunächst verschiedene Klassen von Veränderungen nebst den hieraus folgenden kollektivrechtlichen Mitbestimmungsverfahren festgelegt werden. Dazu ist es notwendig, jeden Veränderungsschritt im Voraus strukturiert zu skizzieren und an Anforderungen zu messen, die beide Betriebsparteien gemeinsam festgelegt haben. Wird im Rahmen einer solchen Konzeption festgestellt, dass bezüglich einer Veränderung nur ein geringer Mitbestimmungsbedarf besteht (etwa für eine technisch notwendige Störungsbehebung) und hat diese keinen Einfluss auf mögliche Verhaltens- und Leistungskontrollen, wäre eine unmittelbare Befassung des Betriebsrats obsolet.

Anders stellt sich die Situation dar, wenn Veränderungen das Funktionsspektrum einer Software erweitern, indem etwa neue Auswertungsmöglichkeiten oder Schnittstellen geschaffen werden. Ist dies der Fall, müsste sichergestellt werden, dass die Einführung erst erfolgt, wenn das Mitbestimmungsverfahren abgeschlossen ist.

Zwischen diesen beiden Extremen gibt es eine Kategorie weiterer Veränderungen, bei denen nicht auf den ersten Blick klar ist, ob Mitbestimmungsbedarf besteht oder nicht. Für diese dritte Kategorie von Daten müsste ein Informations- und Konsultationsmechanismus sichergestellt werden, der Betriebsräten die Möglichkeit gibt, wirksam über das weitere Vorgehen und die Notwendigkeit von kollektivrechtlichen Regelungen zu entscheiden.

Anknüpfend an die vorstehende Einteilung nach technischen Veränderungen in die Kategorie

- „Veränderungen ohne Mitbestimmungsbedarf“,
- „Veränderungen mit möglichem Mitbestimmungsbedarf“ und
- „Veränderungen mit klarem Mitbestimmungsbedarf“

können weitere Verfahrensschritte in einer Rahmenbetriebsvereinbarung festlegt werden. Insbesondere zeitliche Abläufe bis hin zur Beschlussfassung durch den Betriebsrat können ausgehend von der Regelungsnotwendigkeit präzisiert werden.

Das vorstehend beschriebene Konzept setzt einerseits voraus, dass eine klare Verantwortlichkeit des Arbeitgebers für die zutreffende Klassifizierung von Veränderungen besteht. Andererseits ist es notwendig, Konsequenzen festzulegen, die aus einer unrichtigen Klassifizierung folgen würden. Da Veränderungen der technischen Systeme vom Arbeitgeber durchgeführt bzw. verantwortet werden, ist es notwendig, dass er diese Verantwortung uneingeschränkt trägt. Dies setzt eine funktionierende Vertrauensbasis voraus. Daneben muss durch flankierende Maßnahmen sichergestellt werden, dass Betriebsräte keine wichtigen Mitbestimmungsrechte aufgeben oder verlieren (vgl. zu Sanktionen Abschnitt III.4.).

Funktioniert das skizzierte Verfahren einer Klassifikation und sich hieraus ableitender Mitbestimmungsabläufe, beinhaltet es für Betriebsräte den Vorteil der besseren Anpassung abzuschließender oder abgeschlossener Regelungen an technische Veränderungen und damit eine Arbeitsentlastung. Für Arbeitgeber resultiert hieraus eine Vereinfachung bei der Durchführung technisch notwendiger Maßnahmen außerhalb von unmittelbaren Mitbestimmungsnotwendigkeiten.

Um bestehende Kollektivrechte von Betriebsräten zu erhalten, ist es, bezogen auf die vorstehend skizzierte Konzeption, notwendig, dass Veränderungen, die unter Verstoß gegen eine Betriebsvereinbarung erfolgt sind, „rückholbar" sind. Am einfachsten wäre es, wenn die unter Verstoß gegen die Betriebsvereinbarung eingeführten Veränderungen auf Verlangen des Betriebsrats rückgängig gemacht würden. Dies wäre ein optimaler Schutz vor Nachteilen, die sich auf kollektivrechtlicher Ebene zulasten von Betriebsräten ergeben könnten. Technisch ist diese Konzeption allerdings gerade bei komplexeren Software-Anwendungen nicht möglich, weil durchgeführte Modifikationen oft nicht zurückgenommen werden können.

Zur Wahrung von Betriebsratsrechten kommen vor diesem Hintergrund alternative Konzeptionen in Betracht, die nach einer unzutreffenden Einordnung für den Arbeitgeber zu Erschwernissen führen, wie etwa eine Verlängerung der Zeitabläufe für die Zustimmung durch den Betriebsrat bzw. die Aussetzung automatisierter Einführungsverfahren. Darüber hinaus ist es wichtig, zugunsten der betroffenen Beschäftigten einen Nachteilsschutz festzuschreiben, der sie vor unzulässigen Verhaltens- und Leistungskontrollen schützt. Gegebenenfalls sollte dieser mit einer Beweislastumkehr gekoppelt werden. Schließlich ist an Sanktionsmaßnahmen zu denken (vgl. den nachstehenden Abschnitt 6).

2. Datenschutzaudit

Das Problem, das abgeschlossene Betriebsvereinbarungen oft schon nach kurzer Zeit von der technischen Entwicklung im IT-Bereich überholt werden, kann wenigstens teilweise dadurch begrenzt werden, dass die Einhaltung der vereinbarten Regelungen regelmäßig durch standardisierte Verfahren überprüft wird.

Diese können einerseits bereits in der Betriebsvereinbarung vereinbart und ausgestaltet werden. Andererseits kann es in Abhängigkeit von der betrieblichen Situation sinnvoll sein, auf im Betrieb bereits etablierte qualitätssichernde Verfahren zurückzugreifen, die es im Datenschutzbereich gibt.

Unabhängig von der Integration in Betriebsvereinbarungen oder von einer möglichen Bezugnahme müssen qualitätssichernde Verfahren sicherstellen, dass bestehende Mitwirkungs- und Mitbestimmungsrechte unangetastet bleiben. Zudem muss es sich um Konzepte handeln, die aus Sicht der Betriebsräte vertrauenswürdig sind und zur Wahrung bzw. Stärkung ihrer Rechte beitragen. Damit scheiden beispielsweise Verfahren aus, die allein vom Arbeitgeber beeinflusst werden können oder die einseitig deren Rechtspositionen berücksichtigen.

Im datenschutzrechtlichen Bereich kommen als geeignete Verfahren Datenschutzaudits in Betracht. Das BDSG sieht Datenschutzaudits seit der Novelle im Jahr 2001 nach der Regelung in § 9a Satz 1 BDSG als Instrument zur Verbesserung des Datenschutzes und der Datensicherheit vor. Um dieses Ziel zu erreichen, können Anbieter von Datenverarbeitungssystemen und -programmen sowie datenverarbeitende Stellen ihre Datenschutzkonzepte sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen.

Datenschutzaudits zielen von ihrer Grundkonzeption her darauf ab, die Verbreitung datenschutzfreundlicher Produkte und Verfahren zu fördern. Erreicht werden soll dieses Ziel dadurch, dass externe und unabhängige Gutachter bestehende Datenschutzkonzepte bzw. eingesetzte technische Einrichtungen prüfen und bewerten.[109]

Attraktiv werden sollen Datenschutzaudits nach der Intention des Gesetzgebers durch die Möglichkeit, dass erfolgreichen Datenschutzaudits Auszeichnungen in Form von Siegeln, Zertifikaten usw. vergeben werden können und dass diese zu Werbezwecken genutzt werden dürfen.[110]

Datenschutzaudits und die dazugehörigen Zertifizierungskonzepte sollen sich nicht darauf beschränken, die Einhaltung eines gesetzlich vorgeschriebenen Datenschutzminimums festzustellen. Sie sollen vielmehr darauf abzielen, die

---

[109] Vgl. Simitis-Scholz, § 9a Rn. 3; vgl. BT-Drs. 14/4329, S. 30 und 38.

[110] Vgl. Simitis-Scholz, § 9a Rn. 3; grundlegend Roßnagel/Pfitzmann/Garstka, Seite 132 ff.; Wedde/Schröder (Hrsg.), Seite 16 ff.

Fähigkeit einer verantwortlichen Stelle auszuzeichnen, auf Veränderungen in der IT-Landschaft schnell und flexibel reagieren zu können.[111]

Datenschutzaudits zielen darauf ab, die Einhaltung eines vorab definierten Qualitätsstandards festzustellen. Ihre Durchführung ist darauf ausgerichtet, die Eigenverantwortlichkeit einer verantwortlichen Stelle zu fordern und zu fördern.[112] Für ihre Durchführung besteht nach derzeitiger Rechtslage jedoch keine Verpflichtung einer verantwortlichen Stelle. Der Einsatz von Datenschutzaudits beruht damit auch in Anbetracht der Regelung in § 9a BDSG ausschließlich auf Freiwilligkeit.

Nach außen können Datenschutzaudits von verantwortlichen Stellen als Werbefaktor verwendet werden.[113] Herausragend guter Datenschutz kann als Werbeargument verwendet werden, um sich gegenüber Mitbewerbern positiv abzusetzen. Datenschutz wird damit zu einem Wettbewerbsfaktor.[114] Bedeutsam kann ein herausragend guter Datenschutz insbesondere für Unternehmen sein, die mit sensiblen Kundendaten arbeiten, wie etwa Telekommunikationsunternehmen, Versicherungen, Finanzdienstleister und Banken sowie Auskunfteien.[115]

Die Konzeption von Datenschutzaudits gemäß § 9a BDSG ist vor gut zehn Jahren zwar in der wissenschaftlichen Diskussion und auch bei Praktikern aus Unternehmen grundlegend positiv aufgenommen worden.[116] In der Praxis haben sich externe Datenschutzaudits aber bisher nicht durchsetzen können. Eine nennenswerte Verbreitung haben sie bisher nur im öffentlichen Bereich des Landes Schleswig-Holstein gefunden. Dort sind auf der Basis des entsprechenden Landesdatenschutzgesetzes seit 2002 zahlreiche Produkte und Verfahren vom unabhängigen Landeszentrum für Datenschutz (ULD) auditiert und zertifiziert worden.[117]

Eine weitere Verbreitung haben demgegenüber verschiedenste individuelle Auditkonzepte in Konzernen und Unternehmen gefunden. Datenschutzaudits sind dort teilweise als autonome Konzepte ausgestaltet. Teilweise fügen sie sich in umfassendere Konzepte des Qualitätsmanagements ein. Interne Datenschutzaudits zielen sowohl auf die Verbesserung der datenschutzrechtlichen Situ-

---

[111] Simitis-Scholz, § 9a Rn. 4; Wedde/Schröder, Seite 18.

[112] Simitis-Scholz, § 9a Rn. 5.

[113] Vgl. Simitis-Scholz, § 9a Rn. 4.

[114] Vgl. Bizer/Petri, DuD 2001, 97; Bäumler, DuD 2002, 325 f.; Wedde/Schröder, Seite 20.

[115] Vgl. DKWW-Weichert, § 9a Rn. 4.

[116] Vgl. zum Meinungsstand Simitis-Scholz, § 9a Rn. 8 (Fußnote 23); Wedde/Schröder, Seite 38.

[117] Vgl. DKWW-Weichert, § 9a Rn. 8 m. w. N.

ation, als auch auf eine Erhöhung der Datensicherheit. Sie sind in einer Reihe von Fällen Bestandteile umfassender Compliance- oder Risikomanagement-Systeme.[118]

Unternehmensinterne Audits sind in der Regel als sog. Verfahrensaudits ausgestaltet und zielen darauf ab, festgelegte IT-Prozesse zu prüfen, zu bewerten und im Ergebnis zu verbessern. Sie stellen so die Prüfung und Beurteilung bestehender Datenschutzkonzepte einer verantwortlichen Stelle in den Mittelpunkt. Denkbar sind auch die Prüfung von Teilaspekten sowie die Einbeziehung der Umsetzung von Konzepten.[119]

Im Rahmen von Datenschutzaudits wird abgeprüft, ob eine verantwortliche Stelle die Maßstäbe, die in Form eines Datenschutzkonzeptes vorliegen, selbst einhält. Dabei wird vorausgesetzt, dass eine Übereinstimmung mit gesetzlichen Mindeststandards besteht. Die Feststellung eines herausragenden Datenschutzes im Rahmen eines Audits, der auch werbewirksam eingesetzt werden kann, setzt jedoch im Regelfall voraus, dass das bestehende Datenschutzniveau über den gesetzlichen Standard deutlich hinausgeht.[120] Prüfmaßstab ist damit in der Regel mehr als das datenschutzrechtliche Minimum, das sich aus einschlägigen gesetzlichen Regelungen ableitet.[121]

Im Rahmen von Wiederholungsaudits kann darüber hinaus festgestellt werden, ob Schwachstellen von der verantwortlichen Stelle verbessert worden sind. Datenschutzaudits tragen damit zur Qualitätsverbesserung und damit auch zu einer Steigerung des Datenschutzes bei.

Neben dem Verfahrensaudit ist die Durchführung von Produktaudits im betrieblichen Rahmen möglich. Produktaudits zielen auf die (in der Regel einmalige) Überprüfung der Datenschutzeigenschaften eines bestimmten IT-Produkts ab. Bezogen auf die hier zu bewertende Frage der Einbeziehung in Betriebsvereinbarungen stellen sie eine Ausnahme dar.

Werden in Betrieben oder Unternehmen Datenschutzaudits durchgeführt, die für den Betriebsrat nachvollziehbar, transparent und vertrauenswürdig sind, können diese zu Bestandteilen von Betriebsvereinbarungen gemacht werden. Es könnte beispielsweise festgelegt werden, dass der Prüfmaßstab für Datenschutzaudits nicht nur die Anforderungen aus Datenschutzkonzepten ist, sondern auch solche aus Betriebsvereinbarungen. Ein solches Verfahren würde sicher-

---

[118] Vgl. Scholz-Simitis, § 9a Rn. 10; Ulmer/Zwick, DuD 2004, Rn. 85 ff.

[119] Vgl. Bizer, DuD 2006, 5.

[120] Hammer/Schuler, DuD 2007, 81.

[121] Ähnlich Simitis-Scholz, § 9a Rn. 29.

stellen, dass durch eine von Arbeitgebern und Betriebsräten akzeptierte Auditinstanz Diskrepanzen festgestellt werden könnten. Ist dies der Fall, könnten Verfahren vereinbart werden, die sicherstellen, dass schnelle Reaktionen erfolgen mit dem Ziel, betriebsvereinbarungskonforme Zustände wiederherzustellen.

Wie entsprechende Gesamtkonzepte aussehen könnten, lässt sich am Beispiel der „Konzernbetriebsvereinbarung Beschäftigtendatenschutz“ im DB-Konzern (KBV BDS) vom 24. 11. 2010 verdeutlichen.[122] Diese Vereinbarung gilt als Rahmenregelung im gesamten DB-Konzern.

In § 23 KBV BDS wird unter der Überschrift „Audits“ in § 23 Abs. 3 festgelegt:

> „Die Organisationseinheit Konzerndatenschutz-Audit (CDA) prüft auf Basis der anwendbaren datenschutzrechtlichen Bestimmungen, insbesondere gesetzlicher Grundlagen, kollektivrechtlicher Vereinbarungen und Richtlinien (RiL) die Rechtmäßigkeit von Datenerhebungen, -verarbeitungen und -nutzungen. Hierbei werden auf Grundlage der kollektivrechtlichen und unternehmenspolitischen Vorgaben besonders hohe Anforderungen an das Datenschutzniveau im Allgemeinen und die Datensparsamkeit und die Transparenz der Verfahren im Besonderen gestellt.“

Für die Durchführung von Datenschutzaudits wird nach § 23 Abs. 3 KBV BDS ein Jahres-Audit-Plan erstellt. Für die Durchführung von Audits können nach § 23 Abs. 5 KBV BDS auch Betriebsräte Themen einbringen. Diese Vorschläge werden nach dem Text der KBV

> „geprüft, mit der Audit-Planung von CDA und der Konzernrevision abgeglichen und möglichst zeitnah berücksichtigt.“

Nach § 23 Abs. 7 KBV BDS wird

> „Zu jedem durchgeführten Audit (…) ein Bericht gefertigt, der folgende Darstellung beinhaltet:
> - den Ist-Zustand des Datenschutzniveaus,
> - die diesbezügliche Risikoabschätzung,
> - Hinweise auf mögliche Lücken und/oder Optimierungspotenziale,
> - daraus abgeleitete Umsetzungsmaßnahmen mit Terminsetzung (Maßnahmenplan).“

---

[122] Die Konzernbetriebsvereinbarung findet sich unter http://www.evg-online.org/Arbeitswelt/Mitbestimmung/Betriebsverfassung/.Aktuelles/13_04_10_KBV_BDS/.

Den entsprechenden Bericht erhalten auch die jeweils zuständigen Betriebsräte. Soweit datenschutzrechtliche Mängel erkannt wurden, gilt:

> „Ab Erhalt des Abschlussberichts sind die Maßnahmen durch die verantwortliche Stelle zum festgelegten Termin umzusetzen, soweit wie sie datenschutzkonform sind."

Damit besteht im Ergebnis eine Verpflichtung der verantwortlichen Stelle, alle identifizierten Mängel zu beseitigen. Dies kommt dem Regelungsgehalt der KBV insgesamt zugute, da damit ein „Automatismus" geschaffen wurde, der sicherstellt, dass Lücken und Optimierungspotenziale identifiziert werden und dass entsprechende Verbesserungen oder Optimierungen umgesetzt werden.

Als Alternative für den Rückgriff auf bestehende Audit-Konzepte können Audit-Maßnahmen auch in Betriebsvereinbarungen selbst verankert werden. In der Praxis finden sich beispielsweise Regelungen zu Datenschutzaudits, die darauf zielen, vereinbarte Rollen- und Berechtigungskonzepte zu prüfen. Diese werden teilweise durch externe Auditoren durchgeführt und ermöglichen es, die Übereinstimmung der vereinbarten Rollen und Berechtigungen, die Zugriffe auf personenbezogene Daten haben, mit den tatsächlichen Systemeinstellungen zu vergleichen.

3. Einbindung betrieblicher Datenschutzbeauftragter

In Betrieben und Unternehmen, die personenbezogene Daten automatisiert verarbeiten, muss gemäß § 4f Abs. 1 Satz 2 BDSG innerhalb eines Monats nach Aufnahme der Datenverarbeitung ein betrieblicher Datenschutzbeauftragter verpflichtet werden. Ausgenommen von dieser Verpflichtung sind lediglich Unternehmen, die in der Regel höchstens neun Personen mit automatisierter Datenverarbeitung beschäftigen. In Betracht kommt diese Ausnahme mit Blick auf allgegenwärtige Varianten der automatischen Verarbeitung personenbezogener Daten nur für kleine Betriebe und Unternehmen.

Die Aufgaben der betrieblichen Beauftragten für Datenschutz sind in § 4g BDSG benannt. Nach Abs. 1 Satz 1 dieser Vorschrift wirken sie auf die Einhaltung des BDSG und anderer Vorschriften über den Datenschutz hin. Primäres Schutzziel ist damit die Wahrung des durch das Gesetz garantierten Persönlichkeitsrechts der Betroffenen. Diese gesetzliche Zielvorgabe ist bezogen auf den Schutz der Persönlichkeitsrechte von Beschäftigten strukturell deckungsgleich mit der Vorgabe, die in § 75 Abs. 2 Satz 1 BetrVG enthalten ist. Danach haben Arbeitgeber und Betriebsrat die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern. Mit Blick auf das Grundrecht auf informationelle Selbstbestimmung, das eine unmittelbare Umsetzung der verfassungsrechtlich geschützten Persönlichkeitsrechte ist, obliegt es in diesem Rahmen Arbeitgebern und Betriebsräten, dafür Sorge zu tragen, dass unter Berücksichtigung des BDSG alles unterbleibt, was Persönlichkeitsrechte von Beschäftigten beeinträchtigen könnte.[123]

Damit hat die Arbeit von betrieblichen Datenschutzbeauftragten und Betriebsräten bezüglich des Schutzes von Persönlichkeitsrechten, der Einhaltung des Grundrechts auf informationelle Selbstbestimmung und damit im Ergebnis der Umsetzung der Schutzvorgaben des BDSG eine identische Zielrichtung. Dies weist den Weg für eine Zusammenarbeit.

In der Praxis findet sich bezüglich dieser Zusammenarbeit ein differenziertes Bild. Teilweise ist eine gute Zusammenarbeit zwischen betrieblichen Datenschutzbeauftragten und Betriebsräten zu identifizieren. Diese äußert sich beispielsweise darin, dass Betriebsräte die vom betrieblichen Beauftragten für Datenschutz gemäß § 4d Abs. 5 und 6 Satz 1 BDSG durchzuführende Vorabkontrolle als Grundlage für die Ausgestaltung von Betriebsvereinbarungen verwenden. In einer Reihe von Fällen werden notwendige Kontrollen nach dem Abschluss von Betriebsvereinbarungen bezogen auf die geregelten Systeme gezielt vom betrieblichen Datenschutzbeauftragten durchgeführt. In derartigen Konstellationen ergänzen sich die unterschiedlichen Kontrollaufgaben von betrieblichen Datenschutzbeauftragten und Betriebsräten.

Derartig positive Konstellationen und konstruktive Gestaltungen setzen jedoch ein Vertrauensverhältnis des Betriebsrats zum betrieblichen Datenschutzbeauftragten voraus. Dieses kann insbesondere dadurch gefördert werden, dass eine Beteiligung des Betriebsrats bei der Bestellung des betrieblichen Datenschutzbeauftragten bis hin zum Einvernehmen über die Besetzung besteht. Eine solche Konstellation geht allerdings über die gesetzlichen Anforderungen hinaus, die weder im BDSG, noch im BetrVG spezifische Mitwirkungs-, Mitbestimmungs- oder Widerspruchsrechte bezogen auf die Position des betrieblichen Datenschutzbeauftragten vorsehen. Betriebsräte können auf der Grundlage von § 99 BetrVG lediglich ihre Zustimmung zu den mit der Bestellung eines betrieblichen Datenschutzbeauftragten verbundenen personellen Einzelmaßnahmen verweigern, wenn die in Abs. 2 dieser Norm genannten Voraussetzungen vorliegen.

Das Widerspruchsrecht bleibt in der Qualität hinter einem echten Mitbestimmungsrecht weit zurück. Wählt der Arbeitgeber einen betrieblichen Daten-

---

[123] Vgl. DKKW-Berg, § 75 Rn. 125.

schutzbeauftragten aus, der nicht das Vertrauen des Betriebsrats genießt, steht dies einer wirksamen Zusammenarbeit entgegen. Um dieses Problem auszuräumen, bedarf es eines echten Mitbestimmungsrechts bei der Bestellung des betrieblichen Datenschutzbeauftragten. Vorbild für die Verankerung eines echten Mitbestimmungsrechts könnte § 9 Abs. 3 ASiG[124] sein. Nach Satz 1 dieser Regelung bedarf die Bestellung oder Abberufung von Betriebsärzten und von Fachkräften für Arbeitssicherheit der Zustimmung der Betriebsräte.

Den vorstehend beschriebenen positiven Gestaltungen stehen Fälle gegenüber, in denen die Zusammenarbeit zwischen betrieblichen Datenschutzbeauftragten und Betriebsräten nicht optimal ist. So finden sich einzelne Betriebsräte in einer Situation wieder, in denen betriebliche Datenschutzbeauftragte den Schutz von Persönlichkeitsrechten (soweit datenschutzrechtlich möglich) wirtschaftlichen Interessen von Arbeitgebern unterordnen. Darüber hinaus sind Fälle bekannt, in denen betriebliche Datenschutzbeauftragte Kontrollrechte von Betriebsräten, die in Betriebsvereinbarungen vereinbart wurden, unter Hinweis auf ihre datenschutzrechtliche Unzulässigkeit konterkarieren. Im Einzelfall wurden beispielsweise Kontrollen unter Hinweis darauf nicht zugelassen, dass Betriebsräte nicht befugt seien, personenbezogene Daten im Betrieb einzusehen.

Datenschutzrechtlich ist eine derartige Position nicht zu fundieren. Betriebsräten stehen als Teil der verantwortlichen Stelle die per Betriebsvereinbarung wirksam vereinbarten Kontrollrechte zu. Ihnen stellt sich allerdings das Problem, in derartigen Fällen per Betriebsvereinbarung geregelte Kontrollrechte in Beschlussverfahren gegen den Arbeitgeber durchsetzen zu müssen, da sie selbst keine unmittelbaren Klagebefugnisse gegen den betrieblichen Datenschutzbeauftragten haben. Und selbst wenn Arbeitgeber betriebliche Datenschutzbeauftragte auffordern, entsprechende Kontrollen zuzulassen, können sich diese auf ihre gesetzlich garantierte Unabhängigkeit bei der Ausübung ihrer Fachkunde berufen und ihre Position aufrecht erhalten.

Die vorstehend skizzierten Probleme resultieren teilweise daraus, dass betriebliche Datenschutzbeauftragte von der normativen Konstruktion des BDSG nicht wirklich unabhängig sind. Gemäß § 4f Abs. 3 Satz 2 BDSG sind sie zwar in Ausübung ihrer Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Gemäß § 4f Abs. 3 Satz 3 BDSG dürfen sie wegen der Erfüllung ihrer Aufgaben nicht benachteiligt werden. Darüber hinaus besteht nach § 4f Abs. 3 Satz 4 BDSG ein Schutz vor ordentlichen Kündigungen. Trotz dieses arbeitsrechtlichen Mindest-

---

[124] Gesetz über Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit (ASiG) vom 12. Dezember 1973 (BGBl. I S. 1885), zuletzt geändert durch Artikel 3 Absatz 5 des Gesetzes vom 20. April 2013 (BGBl. I S. 868).

schutzes besteht aber schon allein deshalb keine Weisungsfreiheit, weil sie einseitig durch den Arbeitgeber bestellt werden können.

Das Fehlen eines Mitbestimmungsrechts des Betriebsrats bei der Bestellung eines betrieblichen Datenschutzbeauftragten hat beispielsweise das BAG in einer Entscheidung vom 11. 11. 1997[125] zum Anlass genommen, an der Unabhängigkeit zu zweifeln und insbesondere Kontrollen des Betriebsratsbüros durch den betrieblichen Datenschutzbeauftragten für unzulässig zu halten. Das BAG hat das Betriebsratsbüro damit nicht als datenschutzrechtlich kontrollfrei gesehen. Es hält im Gegenteil das BDSG auch für die Datenverarbeitung durch Betriebsräte uneingeschränkt für anwendbar. Das Gericht hat aber ausgeschlossen, dass ein möglicherweise nicht ausreichend unabhängiger betrieblicher Datenschutzbeauftragter auf vertrauliche Unterlagen von Betriebsräten Zugriff nehmen kann.

Auch wenn die Entscheidung des BAG noch zu der vor der Novellierung des Jahres 2001 geltenden Fassung des BDSG erfolgt ist, kann aus ihr bis heute abgeleitet werden, dass eine Unabhängigkeit der betrieblichen Datenschutzbeauftragten qua Gesetz nicht gegeben ist. Diese Situation ist bedauerlich. Wäre eine Unabhängigkeit der betrieblichen Datenschutzbeauftragten etwa dadurch garantiert, dass sie nur im Einvernehmen mit dem Betriebsrat berufen oder abberufen werden könnten, ließe sich die Arbeit der Datenschutzbeauftragten mit der von Betriebsräten besser verzahnen. Insbesondere könnte vereinbart werden, dass Kontrollmaßnahmen des betrieblichen Datenschutzbeauftragten nach dem BDSG Berücksichtigung in Betriebsvereinbarungen finden. So könnte beispielsweise festgelegt werden, dass die Ergebnisse von Vorabkontrollen zu neuen IT-Verfahren einen Maßstab für die Regelungstiefe von Betriebsvereinbarungen generieren könnten. Entsprechendes gilt für die Ergebnisse von Datenschutzaudits, die von betrieblichen Datenschutzbeauftragten durchgeführt werden. Besteht bezüglich deren Gehalt und Qualität Einvernehmen zwischen betrieblichen Datenschutzbeauftragten und Betriebsräten, könnte vereinbart werden, dass positive Auditergebnisse die Regelungstiefe bzw. Regelungsnotwendigkeiten reduzieren würden.

4. Sanktionsmaßnahmen

Das im vorstehenden Abschnitt III.1. skizzierte Konzept von prozessorientierten Betriebsvereinbarungen erleichtert Arbeitgebern und Betriebsräten den Umgang mit Veränderungen von IT-Systemen. Es schafft aber auch das Risiko, dass

---

[125] Vgl. BAG vom 11. 11. 1997 – 1 ABR 21/97, BAGE 87, 64.

Veränderungen von IT-Systemen, bezüglich derer Betriebsräte eigentlich Mitbestimmungsbedarf hätten, vom Arbeitgeber unter der Überschrift der reinen „Fehlerkorrektur" in einem erleichterten Verfahren ohne explizite Beachtung von Mitbestimmungsrechten eingeführt werden können. Wird etwa zur Fehlerbehebung eine neue Schnittstelle zu einem System eröffnet, die im Ergebnis Verhaltens- und Leistungskontrollen ermöglicht, tritt in der Praxis oft die Schwierigkeit auf, dass die Veränderungen nicht rückholbar sind. Selbst wenn das der Fall ist, argumentieren Arbeitgeber häufig mit dem unzumutbaren wirtschaftlichen Schaden, der durch notwendige Anpassungen entsteht. Diese Argumentation findet im gerichtlichen Verfahren nicht selten Gehör.

Aus Sicht von Betriebsräten liegt es mit Blick auf diese Situation nahe, Betriebsvereinbarungen mit „Sanktionsregelungen" zu versehen, die abschreckende Wirkung auf Arbeitgeber haben könnten. Zeitweise wurde dieses Ziel dadurch realisiert, dass Arbeitgeber durch Betriebsvereinbarungen verpflichtet wurden, im Falle der Verletzung von Mitbestimmungsrechten bzw. von Regelungen in Betriebsvereinbarungen Vertragsstrafen an einen (gemeinnützigen) Dritten zu zahlen. Dieses Vorgehen hat das BAG allerdings unter Verweis auf das Fehlen einer erforderlichen Vermögens- und Rechtsfähigkeit von Betriebsräten für unzulässig erklärt.[126] Damit sind entsprechenden Vereinbarungen Grenzen gesetzt. Um dennoch die Einhaltung geschlossener Regeln sicherstellen zu können, auch wenn Arbeitgebern weitergehende Handlungsspielräume eingeräumt werden, bieten sich andere Regelungsmechanismen an.

Kommt es zu Verstößen, die der Arbeitgeber zu vertreten hat, ist weiter daran zu denken, dass vorgesehen wird, dass Betriebsräten „Reißleinen" in Form eines kollektivrechtlich vereinbarten Unterlassungsanspruchs zur Verfügung gestellt werden, deren Betätigung zur Abschaltung bestimmter Systemteile oder zur Reduzierung der Systemperformance führt. Die Maßnahmen müssen auf Verlangen der Betriebsräte so lange aufrechterhalten werden, bis eine einvernehmliche Lösung gefunden wird. Ergänzend kann vorgesehen werden, dass Bearbeitungsfristen beim Betriebsrat zeitlich verlängert werden (vgl. hierzu Abschnitt III.1.).

Alternativ oder ergänzend kann vereinbart werden, dass nach festgestellten Verstößen Betriebsräte ein erhöhtes Freistellungskontingent in Anspruch nehmen können, um künftige Systemänderungen zu bewerten. Darüber hinaus kann vereinbart werden, dass in derartigen Fällen die Zuziehung von internem

---

[126] Vgl. BAG vom 29. 9. 2004 – 1 ABR 30/03, BAGE 112, 96; BAG vom 19. 1. 2010 – 1 ABR 62/08, BAGE 133, 69.

oder externem Sachverstand nach § 80 Abs. 3 BetrVG ohne weitere Vereinbarungen möglich wird.

Für den Arbeitgeber haben derartige Regelungen den Nachteil, dass Veränderungen von IT-Systemen erschwert werden. Deshalb ist davon auszugehen, dass sie im Regelfall ein Interesse daran haben werden, dass eine betriebsvereinbarungskonforme Einführung erfolgt.

5. IT-Folgeabschätzung

a) Grundsätzliches

Die in Abschnitt II. beschriebenen Mitwirkungs- und Mitbestimmungsrechte sind bisher zumeist interpretiert und eingesetzt worden, um jeweils bestimmte und abgrenzbare Hardware oder Software zu regeln. Diese Beschränkung auf abgrenzbare IT-Systeme oder -Anwendungen leitet sich aus den kollektivrechtlichen Gegebenheiten ab: Nach dem Wortlaut von § 87 Abs. 1 Nr. 6 BetrVG besteht beispielsweise das Mitbestimmungsrecht bei der Einführung und Anwendung von technischen Einrichtungen. Unter einer technischen Einrichtung wird in der Regel eine bestimmte Einheit von Rechnern und Programmen verstanden.[127] Ob sich das Mitbestimmungsrecht darüber hinaus auch pauschal auf ganze Systemlandschaften beziehen lässt, die aus unterschiedlichen Einzelanwendungen und Systemen bestehen und die zu unterschiedlichen Zeiten und möglicherweise in unterschiedlichen Unternehmen eines Konzerns eingeführt werden, ist eine naheliegende Frage. Sie wäre mit Blick auf die Rechtsprechung nur zu bejahen, wenn sich ein Gesamtsystem mit der Einführung und Anwendung einer bestimmten technischen Einrichtung in Zusammenhang bringen ließe. Darüber hinaus lassen sich weitere Mitbestimmungsrechte, die sich etwa aus § 87 Abs. 1 Nr. 7 BetrVG bezüglich Regelungen zum Arbeits- oder Gesundheitsschutz oder aus § 111 BetrVG für den Fall von Betriebsänderungen ebenfalls auf die gesamte Systemlandschaft beziehen. Schließlich lassen sich auch die Mitwirkungs- und Mitbestimmungsrechte, die nach den §§ 96 bis 98 BetrVG bezüglich der Berufsbildung bestehen, auf das Gesamtsystem beziehen.

Das Fehlen übergreifender Mitbestimmungsrechte setzt systemübergreifenden Regelungsmöglichkeiten von Betriebsräten oft Grenzen. Die kollektivrechtliche Beeinflussung von Systemlandschaften bzw. von vernetzten Einzelsystemen auf der kollektivrechtlichen Ebene wird erschwert und teilweise unmöglich gemacht.

---

[127] Vgl. DKKW-Klebe, § 87 Rn. 169 m. w. N.

Wie einschlägige Problemfelder aussehen, kann an einem Beispiel aus der Vergangenheit illustriert werden:

Bei der Einführung betrieblicher E-Mail-Systeme, die flächendeckend ab Beginn der 1990er Jahre erfolgte, standen für Betriebsräte im kollektivrechtlichen Bereich Themen im Vordergrund, wie beispielsweise

- Gleichbehandlung beim Zugang zu betrieblichen E-Mail-Systemen,
- Ausschluss und Begrenzung von Kontrollen der E-Mails,
- Zulässigkeit und Grenzen von Weiterleitungen,
- Ausschluss von zwingenden Reaktionszeiten,
- Nachteilsschutz für Beschäftigte,
- Recht zur Privatnutzung usw.

In zahlreichen Betriebsvereinbarungen wurden diese Themenfelder in unterschiedlicher Qualität geregelt. Über die Jahre haben sich diesbezüglich „Mindeststandards“ herausgebildet.[128]

Nicht bei der kollektivrechtlichen Regelung von E-Mail-Systemen berücksichtigt wurden weitere erkennbare Risiken bezüglich der Nutzung von E-Mails, wie insbesondere die Möglichkeit zur Übermittlung vertraulicher Informationen oder von Geschäfts- bzw. Betriebsgeheimnissen. Absehbare Kontrollansprüche von Arbeitgebern, die diese Übermittlungen aufdecken können, spielten bei der kollektivrechtlichen Regelung von E-Mail-Systemen keine Rolle. Entsprechende Regelungen, die bestimmte Verarbeitungen und Auswertungen begrenzen bzw. verbieten, sind in früheren Betriebsvereinbarungen deshalb eine absolute Ausnahme. Hätten Betriebsräte entsprechende Regelungen zu Beginn der E-Mail-Zeit angemahnt, um Beschäftigte vor „Spätfolgen“ der Technik zu schützen, hätten sie wahrscheinlich nur ungläubiges Staunen von Arbeitgebern erfahren.

Heute sind E-Mails aus der betrieblichen Kommunikation nicht mehr wegzudenken. Und heute realisieren sich Risiken und Kontrollpotenziale, die dieser Technik schon immer immanent waren. So wird beispielsweise aus steuerlichen Archivierungsvorgaben für Geschäftsbriefe, die sich nunmehr auch auf elektronische Post erstrecken, von Arbeitgebern die Anforderung abgeleitet, alle E-Mails zu archivieren und nicht nur steuerlich relevante. Für Beschäftigte leitet sich aus einer vollständigen Archivierung das Risiko ab, dass persönliches Fehlverhalten, das arbeitsrechtlich relevant sein kann, damit auch bis zu zehn Jahre später noch identifiziert werden kann. Darüber hinaus sehen sich Betriebsräte unter Hinweis auf „IT-Compliance“ mit der Anforderung konfrontiert, dass

---

[128] Vgl. etwa die Nachweise zum Inhalt von Betriebsvereinbarungen bei Böker, E-Mail-Nutzung und Internetdienste, Frankfurt 2008-

E-Mail-Inhalte vor der Archivierung umfassend ausgewertet werden müssen, um die Rechtskonformität des Firmenhandelns sicherzustellen.

Eine Beschränkung der Archivierung auf reine Geschäftsbriefe erfolgt heute regelmäßig deshalb nicht, weil eine Trennung zwischen geschäftlichen und persönlichen bzw. privaten Inhalten für Arbeitgeber technisch zu aufwendig ist. Dass diese fehlende Trennung verschiedener Inhalte sowohl ein organisatorischer, wie auch ein datenschutzrechtlicher Mangel ist, wird von Arbeitgebern regelmäßig ebenso ignoriert, wie Aussagen der Finanzbehörden, nach denen Arbeitgeber zu einer entsprechenden Trennung verpflichtet sind. So heißt es beispielsweise in den „Fragen und Antworten zum Datenzugriffsrecht der Finanzverwaltung“ des BMF vom 22. 1. 2009 in Abschnitt 6 auf Seite 3:

> „Nach dem GDPdU ist es Aufgabe des Steuerpflichtigen, die steuerrelevanten Daten von den anderen abzugrenzen. Er wird sich dabei auch an datenschutzrechtlichen bzw. besonderen berufsspezifischen Gesichtspunkten orientieren müssen.“[129]

Mängel bei der Ausgestaltung von E-Mail-Systemen, die von Arbeitgebern zu vertreten sind, führen damit im Ergebnis dazu, dass von Beschäftigten und Betriebsräten verlangt wird, umfassende Speicherungen ebenso zu akzeptieren, wie die hieraus resultierenden Gefährdungen für Persönlichkeitsrechte der Beschäftigten.

Kollektivrechtliche Reaktionen auf derartige schleichende Zweckänderungen sind schwierig. Arbeitgeber halten Anforderungen von Betriebsräten, die Speicherung der Daten zu beschränken, regelmäßig das Argument entgegen, dass eine entsprechende Umstellung der E-Mail-Systeme technisch nicht machbar oder zu aufwändig sei. Besonders mit Hilfe des letzten Arguments versuchen Arbeitgeber, die Verhandlungsspielräume von Betriebsräten in der Praxis einzuschränken. An dieser Stelle rächt es sich, dass entsprechende Verarbeitungsnotwendigkeiten bei der Einführung und grundlegenden Gestaltung von E-Mail-Systemen in den entsprechenden Betriebsvereinbarungen nicht ausreichend berücksichtigt worden sind. Wäre dies geschehen, hätte beispielsweise eine sinnvolle Trennung von Geschäftsbriefen und anderen E-Mails bei der Einführung des Systems von Anfang an festgelegt werden können. Diese Tren-

---

[129] Vgl. zur Verpflichtung von Steuerpflichtigen, steuerrelevante Daten von den anderen abzugrenzen, die Ausführungen im Schreiben des BMF Referat IV A 4 vom 22. Januar 2009, online unter http://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Steuern/Weitere_Steuerthemen/Abgabeordnung/Datenzugriff_GDPdU/GdPdU-faq-anl.pdf?__blob=publicationFile&v=3

nung wäre zwar theoretisch auch in bestehenden Systemen noch möglich. Sie scheitert aber praktisch daran, dass eine Veränderung der Systeme und der hier bereits vorhandenen Unterlagen sehr aufwändig ist.

Eine vergleichbare Entwicklung bezogen auf E-Mail-Systeme zeichnet sich derzeit bezüglich der sog. DLP-Systeme (vgl. Abschnitt I.5.e.),[130] ab, die ein umfassendes Kontrollpotenzial und die Möglichkeit zu individualisierten Verhaltens- und Leistungskontrollen beinhalten.

Der Einsatz entsprechender Systeme wird von Arbeitgebern angesichts der Tatsache, dass E-Mail-Systeme ein Standard-Kommunikationsmittel sind, in vielen Fällen als „alternativlos“ dargestellt. Von Betriebsräten wird verlangt, den Einsatz dieser Systeme zu akzeptieren mit dem Hinweis darauf, dass der Einsatz einerseits „Industriestandard“ sei und dass andererseits die Risiken für Unternehmen unübersehbar seien. Auch hier wiederum realisieren sich Grundprobleme, die auch bei der Einführung von E-Mail-Systemen vor über 20 Jahren schon erkennbar waren, aber in Betriebsvereinbarungen nicht thematisiert wurden. Darüber, dass das Risiko der Übersendung von vertraulichen Unterlagen weniger aus E-Mail-Systemen resultiert, als vielmehr aus unzureichenden Maßnahmen der Datensicherung in der gesamten Systemlandschaft, wird hingegen nicht diskutiert. In der Konsequenz werden damit durch neue Kontrollmechanismen nur Symptome bekämpft, nicht aber die Ursachen.

Im Ergebnis ist festzustellen, dass Beschäftigte und Betriebsräte im Bereich von E-Mail-Systemen mit weiteren Kontrollanwendungen konfrontiert werden, deren Entstehen sich aus dem System selbst und dessen Möglichkeiten zu ergeben scheint. Wären entsprechende Kontrollmöglichkeiten bereits bei Einführung der Systeme klar thematisiert worden, wären kollektive Regelungen hierzu möglicherweise ebenso anders ausgefallen, wie Anforderungen von Betriebsräten an die technische Ausgestaltung. Problematisch ist, dass im E-Mail-Bereich der nächste Schritt bereits vorprogrammiert ist. Neue Möglichkeiten der Verhaltens- und Leistungskontrollen werden sich ergeben, wenn E-Mail-Daten zusammen mit Kalenderdaten, Standortdaten oder Geräteinformationen ausgewertet werden. Auch hierfür lassen sich aus Arbeitgebersicht Argumente ableiten, wie etwa die Sicherung von Firmeneigentum oder der Schutz vor Arbeitszeitmanipulationen. Die nächste Runde der Kontrollen ist damit eingeläutet.

Die beschriebenen Effekte, wie etwa die Schwierigkeiten bei der Trennung von elektronischen Geschäftsbriefen von anderen Inhalten waren schon bei der Einführung von E-Mail-Systemen ebenso absehbar, wie Gefahren für vertrauli-

---

[130] Zur technischen Ausgestaltung vgl. Höller, CuA 7-8-2013, S. 9.

che Informationen, die auf diesem Wege unzulässig übermittelt werden können. Dass sich absehbare Risiken jetzt realisieren, hat in der Konsequenz eine Verschärfung von Kontrollmaßnahmen zur Folge.

Entsprechende Entwicklungen, die mittelfristig ebenfalls zu mehr Kontrollen führen werden, wiederholen sich derzeit in anderen Bereichen wie etwa zum Thema „Bring Your Own Device“ (BYOD). Dieser Begriff steht für Konzepte, bei denen Arbeitnehmer ihre eigene Hardware (insbesondere Notebooks oder Mobiltelefone) für die Erbringung ihrer beruflichen Arbeitsleistung verwenden (vgl. Abschnitt I.4.a.). Argumentativ wird die Einführung entsprechender Konzepte von Arbeitgebern damit untermauert, dass die Nutzung privater Geräte von Beschäftigten gewünscht wird. Aus betriebswirtschaftlicher Sicht verbindet sich mit BYOD die Hoffnung auf Einsparungen.

Aus dem Blickwinkel der Datensicherheit beinhalten BYOD-Konzepte für Arbeitgeber das Risiko, dass Firmendaten auf privaten Geräten abgespeichert werden. Um das Risiko zu minimieren, setzen viele Sicherheitskonzepte darauf, dass die Informationen auf Geräten von Beschäftigten und damit die Hardware selbst von Firmenseite überwacht werden. So hat etwa Jeanette Horan, IT-Chefin bei IBM, darauf verwiesen, dass Sicherheitsaspekte von der IBM dadurch gewahrt werden, dass die privaten Geräte von der Firma nach eigenen Vorgaben konfiguriert und angepasst werden.[131] Damit ist absehbar, dass betriebliche Kontrollmethoden das private Eigentum der Beschäftigten erfassen werden.

Für Betriebsräte schafft diese Situation neue Herausforderungen: Sie haben zwar bezüglich der privaten Hardware ein Mitbestimmungsrecht, das sich insbesondere aus den Regelungen in § 87 Abs. 1 Nr. 6 und 7 BetrVG ableitet. Diesbezüglich ist zu beachten, dass Mitbestimmungsrechte nicht dadurch ausgeschlossen werden, dass Arbeitgeber ein der Mitbestimmung unterliegendes Geschäft Dritten überlassen.[132] In derartigen Fällen müssen Arbeitgeber in ihren vertraglichen Vereinbarungen mit Dritten sicherstellen, dass der Inhalt von Betriebsvereinbarungen oder anderen kollektivrechtlichen Vereinbarungen dort Berücksichtigung findet.

Auf der Grundlage der angesprochenen Mitbestimmungsrechte können Betriebsräte beispielsweise bestimmte Nutzungsformen verhindern oder mögliche Verhaltens- und Leistungskontrollen ausschließen. Auch ergonomische Min-

---

[131] Vgl. Bergstein, IBM Faces the Perils of „Bring Your Own Device“, MIT Technology Review, 21. 5. 2012, http://www.technologyreview.com/news/427790/ibm-faces-the-perils-of-bring-your-own-device/

[132] Vgl. hierzu etwa DKKW-Klebe, § 87 Rn. 21.

destanforderungen wie etwa das Verbot von für berufliche Tätigkeiten ungeeigneten Geräten kann auf diesem Weg erreicht werden. Dennoch ist zu befürchten, dass die Standards bei der Nutzung privater Hardware tatsächlich hinter denen im Betrieb zurückbleiben, weil Kontrollmöglichkeiten bezüglich privater Geräte schon mit Blick auf den Grundrechtsschutz der Beschäftigten hinter denen zurück bleiben, die es bezogen auf betriebliche Geräte gibt. Im Spannungsfeld zwischen Interessen von einzelnen Beschäftigten, Interessen von Arbeitgebern und kollektivrechtlichen Vorgaben ist derzeit nicht abzusehen, zu welchen Ergebnissen dies führen wird.

Eine weitere problematische Entwicklung, die ebenfalls zu unkalkulierten Risiken führen könnte, zeichnet sich derzeit im Bereich der Nutzung sogenannter „sozialer Medien“ ab. Dieser Begriff steht einerseits für die Nutzung von Kommunikationsnetzwerken, wie etwa Facebook oder Twitter. Andererseits zeichnet sich derzeit weiterhin ab, dass Unternehmen eigene Kommunikationsplattformen einführen, die sich am Beispiel sozialer Netzwerke orientieren. Auf diesen Plattformen werden Nachrichtenforen, Möglichkeiten zur gemeinsamen Bearbeitung von Dokumenten, Kalender und allgemeine Informationsforen zusammengefasst. Betriebsräte werden auch in diesem Bereich oft damit konfrontiert, dass Beschäftigte entsprechende Nutzeroberflächen fordern.

Der Einsatz von sozialen Medien in den vollständig beschriebenen unterschiedlichen Ausgestaltungen generiert aus individual- und kollektivrechtlicher Sicht Probleme. So ist beispielsweise derzeit rechtlich noch weitgehend ungeklärt, was geschieht, wenn ein Beschäftigter, der in sozialen Netzwerken persönliche Accounts auch zu beruflichen Zwecken genutzt hat, das Unternehmen verlässt. Bezogen auf betriebsinterne Social-Media-Plattformen zeichnet sich ab, dass hier eine Fülle von Suchfunktionen vorgesehen ist, die es beispielsweise ermöglichen, jeden Eintrag eines bestimmten Beschäftigten zu erfahren. Dies erzeugt eine völlig neue Qualität von möglichen Verhaltens- und Leistungskontrollen.

Betriebsräte, die vom Arbeitgeber eingeführte interne Anwendungen regeln wollen, stoßen auf das Problem, dass die Auswirkungen und damit auch die möglichen Verhaltens- und Leistungskontrollen kaum absehbar sind. Gleiches gilt für das Ansinnen von Arbeitgebern, Beschäftigten die individuelle Nutzung persönlicher Accounts für berufliche Zwecke zuzugestehen. Es ist aber ohne viel Fantasie absehbar, dass sowohl interne Lösungen, wie auch die Nutzung individueller Accounts zu einer Fülle von Kontrollmöglichkeiten führen werden, die zu Nachteilen von Beschäftigten verwendet werden können. Bezogen auf individuelle Accounts in sozialen Netzwerken sei in diesem Zusammenhang nur auf erste Entscheidungen der Arbeitsgerichte verwiesen, die aus persönlichen Einträgen in öffentlich zugängigen sozialen Netzwerken Abmahnungen bzw. Kündigungen abgeleitet haben.[133]

b) Vernetztes Denken

Um den vorstehend skizzierten neuen Risiken zu begegnen, ist es zur langfristigen Sicherstellung von Mitwirkungs- und Mitbestimmungsrechten aus Betriebsratssicht sinnvoll, nicht nur neu einzuführende bzw. zu verändernde Systeme selbst zu bewerten und zu regeln, sondern darüber hinaus auch Folgen und Wechselwirkungen mit in die Überlegungen und Vereinbarungen einzubeziehen. Notwendig ist eine IT-Folgenabschätzung, die insbesondere auch die Wechselwirkungen und Entwicklungsperspektiven von IT-Systemen berücksichtigt und die darauf abzielt, denkbare negative Effekte und Auswirkungen neuer IT-Anwendungen bereits vor oder spätestens bei deren Einführung zu identifizieren. Auf diesem Weg wäre es Betriebsräten möglich, vorsorgende Schutzregeln in Betriebsvereinbarungen aufzunehmen. Um entsprechende Regelungen durchsetzbar zu machen, ist der Ausbau bestehender oder die Schaffung eines neuen Mitbestimmungsrechts notwendig.

Diese Erkenntnis ist keinesfalls neu. Im kollektivrechtlichen Bereich wird eine neue Denkweise vielmehr schon seit längerer Zeit gefordert.[134] Dieser Bereich ist aber bisher in der Praxis immer noch schlecht entwickelt. Dies liegt möglicherweise daran, dass entsprechende direkte Mitbestimmungstatbestände und damit auch Handlungsmöglichkeiten für Betriebsräte fehlen. Allerdings lassen sich einschlägige Handlungs- und Mitbestimmungsmöglichkeiten von Betriebsräten schon heute aus einer Reihe von kollektivrechtlichen Regelungen wie etwa den Mitbestimmungsrechten in § 87 Abs. 1 Nr. 6 und 7 BetrVG ableiten (vgl. dazu Abschnitt II.2.c. und d.).

Allerdings ist Streit über die Erforderlichkeit von entsprechenden Handlungen bzw. Maßnahmen der Betriebsräte vorprogrammiert. Verweigert der Arbeitgeber entsprechende Ressourcen, so ist Betriebsräten anzuraten, Betriebsvereinbarungen zu Systemen statisch auszugestalten und hierbei bestimmte Weiterentwicklungen auszuschließen.

In positiven Fällen, in denen Arbeitgeber an einer entsprechenden Regelung interessiert sind, sind gemeinsame Bewertungen denkbar mit der Folge, dass Schutzstandards geschaffen und garantiert werden.

---

[133] Vgl. etwa ArbG Bochum vom 26. 9. 2012 – 5 Ca 949/12, DuD 2013, 255; ArbG Paderborn vom 1. 6. 2012 – 3 Ca 93/12, Die Mitbestimmung 2013, 1/2, 8; LAG Hamm vom 10. 10. 2012 – 3 Sa 644/12, DuD 2013, 251.

[134] Vgl. hierzu etwa DKKW-Klebe, § 87 Rn. 162 ff. mit zahlreichen Nachweisen.

IV. Anforderungen an den Arbeitnehmer-Datenschutz

Wenn eine künftige gesetzliche Regelung zum Arbeitnehmerdatenschutz sowie auch das BetrVG mit der veränderten IT-Technik Schritt halten sollen, so erscheinen die im Folgenden aufgeführten normativen Anforderungen und Festlegungen als unverzichtbar:

- Verstöße gegen die derzeit im BDSG enthaltenen gesetzlichen Verbote bezüglich unzulässiger Erhebungen, Verarbeitungen und Nutzungen personenbezogener Daten müssen deutlich schwerer sanktioniert werden, als dies bisher der Fall ist. Dies darf sich nicht auf die Verhängung von Bußgeldern beschränken, sondern muss auch den Entzug der Betriebserlaubnis für betroffene Anwendungen vorsehen.
- Die Bedingungen für die Erforderlichkeit einer Verarbeitung personenbezogener Daten bedürfen einer Konkretisierung und Verschärfung. Dem Schutz der Persönlichkeitsrechte muss Vorrang vor der Erforderlichkeit gewährt werden. Das Grundrecht der informationellen Selbstbestimmung bedarf einer datenschutzrechtspezifischen Fundierung.
- Wenn Arbeitgeber, als Ergebnis einer Abwägung zwischen Erforderlichkeit und Verletzung der Persönlichkeitsrechte, Eingriffe in die Persönlichkeitsrechte von Beschäftigten vornehmen wollen, muss der Nachweis erbracht werden, dass sie dafür den schonendsten Weg wählen.
- Die Anforderungen an die Zweckbindung der Verarbeitung personenbezogener Daten bedürfen einer Konkretisierung. Ein Normenkonflikt zwischen Zweckbindung und Sparsamkeit bei der Datenverwendung ist so weit wie möglich zu vermeiden.
- Ähnliches gilt für die Anforderungen an die Freiwilligkeit unter Bedingungen des Beschäftigungsverhältnisses bzw. des Tätigseins für ein Unternehmen. Die Verarbeitung aller nicht zwingend erforderlichen persönlichen Daten muss an die vorab zu erteilende Einwilligung der betroffenen Person gebunden werden. Eine diskriminierungsfreie Widerrufung einer solchen Einwilligung muss technisch und organisatorisch gewährleistet sein.
- Ein Transparenzgebot sollte von allen Herstellern fordern, alle über die Systembenutzer erfassten Daten – auch im Detail – offen zu legen, insbesondere die Übermittlung solcher Daten an andere Systeme.
- Softwaresysteme, die in der Lage sind, das Benutzerverhalten in differenzierter Weise zu erfassen und zu dokumentieren, sollten an eine staatliche Genehmigungspflicht gebunden werden. Die Kriterien sollten deutlich machen, dass die Einsatzzwecke präzise und überprüfbar beschrieben sind

und dass die persönliche Eignung der betreibenden Personen nachgewiesen werden muss.
- Nur Unternehmen, die ihre Dienste auch öffentlich anbieten, sollten als Provider gelten; somit könnten sie ihren Mitarbeiterinnen und Mitarbeitern die private Nutzung ihrer Kommunikationsmittel ohne die mit dem Providerstatus verbundenen gesetzlichen Restriktionen erlauben.
- Es muss ausgeschlossen werden, dass eine Verarbeitung personenbezogener Daten in einem Rechtsraum möglich ist, in dem dort geltende Rechtsnormen das deutsche Datenschutzrecht verletzen.
- Die bisherige Praxis in den Betrieben lässt erkennen, welch hohe Bedeutung der durch die Mitbestimmungsrechte der Arbeitnehmerinteressenvertretung gegebenen Gestaltung zukommt. Im BetrVG enthaltene Mitbestimmungstatbestände sollten daraufhin überprüft werden, ob sie die genannten Themen erfassen. Wo dies nicht der Fall ist, müssen Ergänzungen des BetrVG erfolgen.
- Die Verarbeitung personenbezogener Daten erfolgt in einer zunehmenden Zahl von Fällen unabhängig von konventionellen betrieblichen Strukturen und von geografischen Grenzen. Um in dieser Situation Mitwirkungs- und Mitbestimmungsrechte auf dem heutigen Niveau zu sichern, sind ergänzende kollektivrechtliche Regelungen notwendig, die es ermöglichen, dass Betriebsräte ihre Rechte nach dem BetrVG entlang der gesamten Verarbeitungskette wirksam wahrnehmen können.

Um der Aushöhlung bestehender Informations-, Mitwirkungs- und Mitbestimmungsrechte entgegenzuwirken, ist die Einführung von verbesserten Sanktionsmechanismen in das BetrVG angebracht. Nicht rechtskonformes Verhalten von Arbeitgebern wie etwa die Einführung neuer IT-Anwendungen ohne vorherige Information der Betriebsräte muss kollektivrechtliche Folgen haben. Deshalb sollte Betriebsräten, flankierend zu einer Verschärfung datenschutzrechtlicher Sanktionen, im BetrVG Handlungsmöglichkeiten zur Verfügung gestellt werden wie etwa ein wirksamer kollektivrechtlicher Unterlassungsanspruch, der bei Verstößen gegen vereinbarte Verarbeitungsregeln zur Anwendung kommen kann. Darüber hinaus könnte vorgesehen werden, dass Betriebsräten zur Bewältigung derartiger Verstöße erhöhte Freistellungskontingente zur Verfügung gestellt werden.

- Datenschutzaudits könnten dazu genutzt werden, sowohl die Einhaltung geltender Datenschutzvorschriften als auch abgeschlossener Betriebsvereinbarungen zu überprüfen. Voraussetzung ist aber, dass Auditverfahren entsprechende Prüfschritte explizit enthalten. Dies setzt voraus, dass die Ausgestaltung von Audits durch Betriebsräte aktiv mitgestaltet werden kann. Insoweit ist ein explizites Mitbestimmungsrecht bezüglich des Inhalts und der Durchführung von Audits notwendig.
- Betriebliche Datenschutzbeauftragte könnten bezüglich der vorstehend angesprochenen Sicherung abgeschlossener Betriebsvereinbarungen eben-

falls eine wichtigere Rolle spielen als bisher. Voraussetzung hierfür wäre jedoch neben der Optimierung ihrer Arbeitsbedingungen, dass nur Personen bestellt werden, die einerseits fachlich qualifiziert sind und die andererseits auch das Vertrauen der Betriebsräte genießen. Um dieses Ziel zu erreichen, ist die Verankerung eines Mitbestimmungsrechts bezüglich der Bestellung und ggf. auch der Abberufung von betrieblichen Datenschutzbeauftragten notwendig.

Wenn es in Zukunft gelänge, die über viele verschiedene Gesetze verstreuten datenschutzrechtlichen Normen in einem Gesetzeswerk zusammenzufassen, so würde dies mit an Sicherheit grenzender Wahrscheinlichkeit von allen handelnden Instanzen begrüßt werden.

Allerdings werden die vorgeschlagenen normative Anforderungen und Festlegungen wohl nicht ausreichen, um mit den Möglichkeiten und Risiken Schritt zu halten, die sich aus der fortschreitenden technischen Entwicklung ableiten. Deshalb ist es notwendig, den Arbeitnehmerdatenschutz ergänzend durch technische Vorkehrungen abzusichern. In Betracht kommen hierfür beispielsweise folgende Maßnahmen:

- Neben den auf den Schutz der Personen gerichteten Regelungen müssen neue datenschutzrelevante Normen sich auf die „Objekte“ beziehen, welche die Probleme verursachen, also die Softwaresysteme und technischen Einrichtungen selber. Sie müssen einerseits Verbote aussprechen für Leistungsmerkmale, die das Persönlichkeitsrecht verletzen und andererseits unverzichtbar zu erfüllende Anforderungen enthalten, denen Softwaresysteme genügen müssen. So muss es z. B. Verbote geben für die Erfassung und Auswertung von Bewegungs- und Beziehungsprofilen sowie das Anlegen weltweit zugänglicher Datenbasen mit besonders schutzwürdigen personenbezogenen Daten. Die Bindung von Funktionen an eine vorher erfolgte Einwilligung muss auch technisch erzwungen werden, um nur einige Beispiele zu nennen.
- Das „Recht auf Vergessenwerden“ muss in personaldatenverarbeitenden Systemen auch technisch umgesetzt werden, etwa durch Einführen von Verfallsfristen für bestimmte Daten. Darüber hinaus muss vorgeschrieben werden, dass ein automatisiertes Löschen solcher Daten erfolgt und dass die hierfür notwendigen Prozeduren und Programme bereitgestellt werden müssen.
- Mögliche Sicherheitseinstellungen in Systemen, die dem Schutz personenbezogener Daten dienen, müssen standardmäßig aktiviert sein. Die Veränderung bzw. Deaktivierung dieser Einstellungen mit dem Ziel einer Zunahme von Erhebungen, Verarbeitungen und Nutzungen personenbezogener Daten muss in einer Form protokolliert werden, die für Betriebsräte einfach nachvollziehbar und prüfbar ist.
- Jedes umfangreichere Software-Tool sollte eine Visualisierung der für seine Nutzung vergebenen Berechtigungen anbieten müssen.

- Das Lokalitäts- und Verkapselungsprinzip sollte als Anforderung an Softwaresysteme formuliert werden, die personenbezogene Beschäftigtendaten mit hohem Detaillierungsgrad verarbeiten. Es muss technisch verlässlich überprüfbar sein, dass die betroffenen Daten nur eine lokal begrenzte Verbreitung erfahren können und dass die Vermeidung des Personenbezugs bei Verlassen von Daten aus dem betroffenen System gewährleistet werden kann.

Literaturverzeichnis

Böker, E-Mail-Nutzung und Internetdienste, Frankfurt 2008

Däubler, Gläserne Belegschaften?, 5. Auflage Frankfurt 2010

Däubler/Kittner/Klebe/Wedde, Betriebsverfassungsgesetz, 14. Auflage Frankfurt 2014 (im Folgenden: DKKW-Bearbeiter).

Däubler/Klebe/Wedde, Weichert, Bundesdatenschutzgesetz, 4. Auflage Frankfurt 2014 (im Folgenden: DKWW-Bearbeiter)

Fitting/Engels/Schmidt/Trebinger/Linsenmaier, Betriebsverfassungsgesetz, 26. Auflage München 2012 (im Folgenden: Fitting)

Gola/Schomerus, Bundesdatenschutzgesetz, 10. Auflage München 2012

Meyer-Schönberger, Delete – Die Tugend des Vergessens in digitalen Zeiten, Berlin 2010

Richardi (Hrsg), Betriebsverfassungsgesetz, 13. Auflage München 2012 (im Folgenden: Richardi-Bearbeiter),

Roßnagel/Pfitzmann/Garstka, Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Inneren, ohne Ort, 2001

Simitis (Hrsg.), Bundesdatenschutzgesetz, 7. Auflage Baden-Baden 2012 (im Folgenden: Simitis-Bearbeiter)

Sprenger, Vertrauen führt, Frankfurt-New York 2007

Wedde/Schröder (Hrsg.): Das Gütesiegel für Qualität im betrieblichen Datenschutz, Frankfurt am Main 2001

Weinberg, Social Media Marketing. Strategien für Twitter, Facebook und Co., Köln 2010

Wiese/Kreutz/Oetker/Raab/Weber/Franzen, Gemeinschaftskommentar zum Betriebsverfassungsgesetz, 9. Auflage Köln 2010 (im Folgenden: GK-BetrVG-Bearbeiter)

Weitere Veröffentlichungen aus der Schriftenreihe des Hugo Sinzheimer Instituts für Arbeitsrecht:

Band 8 *Thorsten Kingreen,* Universität Regensburg
Der Vorschlag des Europäischen Gewerkschaftsbundes für ein Soziales Fortschrittsprotokoll

Band 7 *Ulrike Wendeling-Schröder,* Leibniz Universität Hannover
Kritik der Lehre vom fehlerhaften Tarifvertrag unter besonderer Berücksichtigung der Tarifverträge tarifunfähiger Gewerkschaften in der Leiharbeit

Band 6 *Jens Schubert*
Der Vorschlag der EU-Kommission für eine Monti-II-Verordnung – eine kritische Analyse unter Einbeziehung der Überlegungen zu der Enforcement-Richtlinie

Band 5 *Wolfgang Däubler*, Universität Bremen
Die Unternehmerfreiheit im Arbeitsrecht – eine unantastbare Größe?

Band 4 *Bernd Waas,* Goethe-Universität Frankfurt a. M.
Betriebsrat und Arbeitszeit – Pauschale Abgeltung und Freistellungen über das Gesetz hinaus

Band 3 *Bernd Waas*, Goethe-Universität Frankfurt a. M.
Geschlechterquoten für die Besetzung der Leitungsgremien von Unternehmen – Bewertung der aktuellen Entwürfe aus unionsrechtlicher und rechtsvergleichender Sicht

Band 2 *Rüdiger Krause,* Georg-August-Universität Göttingen
Tarifverträge zur Begrenzung der Leiharbeit und zur Durchsetzung von Equal Pay

Band 1 *Britta Rehder/Olaf Deinert/Raphaël Callsen*
Arbeitskampfmittelfreiheit und atypische Arbeitskampfformen – Rechtliche Bewertung atypischer Arbeitskampfformen und Grenzen der Rechtsfortbildung