

Prof. Dr. Peter Wedde

Direktor der Europäischen Akademie der Arbeit
in der Universität Frankfurt am Main
Professor für Arbeitsrecht und
Recht der Informationsgesellschaft



Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)252 H

Stellungnahme

**für die Öffentliche Anhörung des Innenausschusses
des Deutschen Bundestages am 23. Mai 2011 in Berlin
zum Thema Beschäftigtendatenschutz**

A. Einleitung

Mit dem Entwurf der Bundesregierung zu einem Gesetz zur Regelung des Beschäftigtendatenschutzes vom 15.12.2011 sowie mit den alternativen Entwürfen der SPD vom 25.11. 2009 und des BÜNDNIS 90/DIE GRÜNEN vom 22.2.2011 liegen drei unterschiedliche Regelungskonzepte vor, die sich dem Thema „Beschäftigtendatenschutz“ widmen. Dass eine so intensive Befassung mit dem Thema erfolgt, ist vor dem Hintergrund zahlreicher Praxisprobleme im Bereich des Beschäftigtendatenschutzes ohne Einschränkung zu begrüßen. Besonders positiv zu

bewerten ist das mit allen Gesetzesvorschlägen verfolgte Ziel, die Datenschutzrechte von Beschäftigten klar herauszuarbeiten und zu stärken.

Der Regierungsentwurf hat nach der amtlichen Begründung zum Ziel, praxisgerechte Regelungen für Beschäftigte und Arbeitgeber zu schaffen, die klarstellen, dass nur solche Daten erhoben, verarbeitet und genutzt werden dürfen, die für das Beschäftigungsverhältnis erforderlich sind. Mit den Neuregelungen sollen Beschäftigte an ihrem Arbeitsplatz zudem wirksam vor Bespitzelungen geschützt werden. Gleichzeitig sollen Arbeitgebern verlässliche Grundlagen für die Durchsetzung von Compliance-Anforderungen und für den Kampf gegen Korruption an die Hand gegeben werden.¹ Die auf Beschäftigte bezogenen Elemente dieser Zielsetzung sind ohne Einschränkung zu begrüßen. Nicht zu verkennen ist weiterhin, dass es legitime Informationsinteressen von Arbeitgebern gibt, die normativ geregelt werden müssen. Der vorliegende Gesetzentwurf erfüllt allerdings die selbst gesetzten Anforderungen bezüglich des Schutzes der Beschäftigten nur unzureichend.

Vor diesem Hintergrund beschränkt sich die folgende Stellungnahme auf Themenfelder, in denen Defizite für den Schutz der Beschäftigten bestehen bzw. denen in der betriebspraktischen Debatte eine herausragende Bedeutung zukommt. Sie stellt den Gesetzentwurf der Bundesregierung (im Folgenden: Regierungsentwurf) in den Mittelpunkt der Bewertung.

¹ BT-Drs. 17/4230, S. 1.

B. Stellungnahme

Die Stellungnahme bezieht sich auf die folgenden Themenfelder:

1. Erhebung-, Verarbeitungs- und Nutzungsmöglichkeiten auf der Grundlage von Betriebsvereinbarungen.
2. Zulässigkeit der Erhebung-, Verarbeitungs- und Nutzungsmöglichkeiten auf der Grundlage von Einwilligungen der Beschäftigten.
3. Erhebungsbefugnisse in der Bewerbungsphase.
4. Ärztliche Untersuchungen.
5. Videoüberwachung.
6. Verdeckte Datenerhebung und Auswertung vorhandener Daten.
7. Zugriff auf Telekommunikationsdaten.
8. Compliance.
9. Unternehmensübergreifende Datenverarbeitung in Konzernen.

1. Erhebung-, Verarbeitungs- und Nutzungsmöglichkeiten auf der Grundlage von Betriebsvereinbarungen

Der Regierungsentwurf sieht durch die Ergänzung zu § 4 Abs. 1 BDSG ausdrücklich vor, dass Betriebs- und Dienstvereinbarungen datenschutzrechtliche Erlaubnisnormen für die Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten sein können. Diese normative Klarstellung ist zu begrüßen. Die Präzisierung des datenschutzrechtlichen Schutzbereichs durch kollektivrechtliche Regelungen ist gängige und bewährte Praxis.

Bei der Ausgestaltung von kollektivrechtlichen Regelungen müssen die Betriebsparteien die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer schützen und fördern. Diese Vorgabe ist in § 75 Abs. 2 BetrVG ausdrücklich normiert. Hieraus leitet sich für kollektivrechtliche Regelungen mit Bezug zum Beschäftigtendatenschutz ab, dass sie Eingriffe in Persönlichkeitsrechte

nur ausnahmsweise und nur so schonend wie möglich zulassen dürfen. Die Bewertung des hiernach zulässigen Regelungsrahmens konfrontiert die Betriebsparteien und insbesondere Betriebsräte nach geltendem Recht oft mit der Frage, welche mit Eingriffen in das Persönlichkeitsrecht der Beschäftigten verbundenen Erhebungen, Verarbeitungen und Nutzungen überhaupt noch durch eine Betriebsvereinbarung geregelt werden können. In der Praxis geht es beispielsweise um die Weitergabe von Daten von im Bereich der klinischen Forschung beschäftigten Mediziner an US-amerikanische Zertifizierungsstellen oder um die umfassende Auswertung von Daten im Zusammenhang mit zivilrechtlichen Streitigkeiten in Großbritannien.

Derartige Unklarheiten bezüglich der kollektivrechtlichen Regelungsbefugnis werden durch die Vorgabe in § 32I des Regierungsentwurfs vermieden, nach der von den neuen Vorschriften zum Beschäftigtendatenschutz nicht zu Ungunsten der Beschäftigten abgewichen werden darf. Diese Regelung ist grundsätzlich zu begrüßen. Sie ist praktikabel und hindert die Betriebsparteien in der betrieblichen Praxis nicht daran, einzelne Tatbestände aus dem datenschutzrechtlichen Regelungsfeld in Betriebsvereinbarungen bezogen auf die konkrete betriebliche Situation zu präzisieren.

Die Einführung einer Regelung, nach der Betriebsvereinbarungen von den neuen Vorgaben des Beschäftigtendatenschutzes zu Ungunsten der Beschäftigten von den Regelungen des Regierungsentwurfs abweichen könnten, wäre problematisch. Eine solche Öffnungsklausel hätte zur Folge, dass der Grundschutz, der durch das neue Gesetz geschaffen wird, in der betrieblichen Praxis sofort wieder reduziert bzw. unterlaufen werden könnte.

Für Arbeitgeber und Betriebsräte würde zudem aus einer solchen Öffnungsklausel vor dem Hintergrund der komplexen neuen Gesetzessituation eine arbeitsintensive und rechtlich anspruchsvolle Herausforderung folgen. Sie müssen mit Blick auf § 75 Abs. 2 BetrVG bei Verhandlungen einerseits bewerten, welche Ab-

weichungen zu Ungunsten der Beschäftigten noch zulässig sein könnten. Andererseits müssten sie die einschlägige Rechtsprechung berücksichtigen wie etwa die Aussagen des BAG zur fehlenden Auswahlmöglichkeit beim Bestehen mehrerer Kontrollalternativen. Arbeitgeber müssen hiernach die Alternative auswählen, die so wenig wie möglich in Grundrechte der Beschäftigten eingreift.²

Vor diesem Hintergrund ist die Gefahr nicht von der Hand zu weisen, dass es bei der Einfügung einer Öffnungsklausel, die Anpassungen unterhalb des gesetzlichen Standards zulässt, zu betrieblichen Regelungen kommen kann, die unangemessen weit in die Rechte von Beschäftigten eingreifen. Damit würde das erklärte Ziel der Gesetzesnovelle, nämlich der Schutz der Beschäftigten, verfehlt.

Sollte es bezogen auf bestimmte betriebliche Sachverhalte die Notwendigkeit abweichender Regelungen durch Betriebsvereinbarungen geben (etwa im Bereich der betrieblichen Altersversorgung), sollte eine klare Rechtssituation durch abschließende beispielhafte Erlaubnisnormen im neuen Gesetz hergestellt werden statt durch Öffnungsklauseln.

2. Zulässigkeit der Erhebung-, Verarbeitungs- und Nutzungsmöglichkeiten auf der Grundlage von Einwilligungen der Beschäftigten

In der arbeitsrechtlichen Debatte zum Thema Beschäftigtendatenschutz wird bezüglich des Rückgriffs auf Einwilligungen immer wieder darauf verwiesen, dass Freiwilligkeit aufgrund der unterschiedlichen Durchsetzungskraft der Parteien im Regelfall nicht gegeben ist. Probleme werden insbesondere in der Anbahnungsphase gesehen, weil Bewerber hier Einwilligungen praktisch nicht verweigern können, wenn sie ihre Einstellungschancen wahren wollen. Dass die Befürchtung berechtigt ist, dass es zu „unfreiwilligen Einwilligungen“ kommt, ist in den letzten

² Vgl. hierzu etwa BAG vom 26.8.2008 - 1 ABR 16/07, BAGE 127, 276-297

Jahren an zahlreichen Beispielen für unangemessene Gesundheits-, Blut- oder Urintests deutlich geworden.

Nach Abschluss eines Arbeitsvertrags stellt sich die Situation für Beschäftigte vertraglich zwar sicherer, tatsächlich aber in vielen Fällen vergleichbar dar. Um den Arbeitsplatz oder Aufstiegschancen zu sichern, stimmen Beschäftigte entsprechenden Anforderungen ihrer Arbeitgeber oft entgegen eigener Interessen zu. Häufig ist dieses Problem etwa im Zusammenhang mit von Arbeitgeber gewollten Zugriffen auf die persönlichen E-Mail-Accounts von Beschäftigten oder bezüglich der Umleitung eingehender elektronischer Post auf von Arbeitgebern bestimmte Vertreter gegeben.

Vor diesem Hintergrund ist die abschließende Begrenzung in § 32I Abs. 1 des Regierungsentwurfs für die Einholung freiwilliger Einwilligungen als Grundlage für die Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten auf die in den Regelungen der §§ 32 bis 32I genannten Fälle grundsätzlich positiv zu bewerten. Sie stellt einen guten Ansatz dar, um Beschäftigte davor zu schützen, Einwilligungen in die Erhebungen, Verarbeitungen oder Nutzungen ihrer personenbezogenen Daten nur deshalb zu erteilen, weil sie Sorge davor haben, sonst berufliche Nachteile zu erleiden.

Die Regelung in § 32I Abs. 1 des Regierungsentwurfs steht nicht im Widerspruch zu Artikel 7 Buchstabe a) der Europäischen Datenschutzrichtlinie. Dort ist nämlich als Verarbeitungsvoraussetzung festgelegt, dass die betroffene Person „ohne jeden Zweifel“ ihre Einwilligung gegeben hat. Genau diese Zweifelsfreiheit besteht im Beschäftigungsverhältnis nicht.

Kritisch fällt eine Auseinandersetzung mit den Einzelregelungen aus, in denen die Einwilligung zugelassen werden soll. Insbesondere in der Bewerbungsphase ist es Beschäftigten, die ihre Einstellungschancen wahren wollen, praktisch unmöglich, eine nach § 32 Abs. 6 Satz 4 des Regierungsentwurfs zulässige Einwilligung in die Erhebung von sonstigen Daten bei Dritten nicht zu erteilen.

Problematisch sind in diesem Zusammenhang auch die durch § 32 Abs. 6 Satz 2 erweiterte Erhebungsbefugnisse von Arbeitgebern bezüglich allgemein zugänglicher Daten. Hieraus folgt, dass Bewerber auch dann um eine Einwilligung gebeten werden könnten, wenn der mögliche Arbeitgeber die bei der nach neuem Recht zulässigen Recherche im Internet gewonnenen Informationen durch Anfragen bei Dritten spezifizieren möchte. Da § 32 Abs. 1 Satz 2 als Erhebungsgrund ganz allgemein die „Eignung des Beschäftigten für die vorgesehene Tätigkeit“ nennt und keine Begrenzung auf berufsspezifischen Fähigkeiten oder Kenntnissen enthält, könnten Bewerber in diesem Zusammenhang um Zustimmung dazu gebeten werden, weitere Daten von einem privaten Ermittler erheben zu lassen. Hieran könnte etwa ein Flughafenbetreiber interessiert sein, der im Internet Hinweise darauf gefunden hat, dass ein Bewerber in einer Initiative gegen ein Erweiterungsvorhaben aktiv sein könnte.

Vergleichbare Probleme bestehen bezüglich der Freiwilligkeit einer Einwilligung bei ärztlichen Untersuchungen (§ 32a Abs. 1) oder bezüglich der Erhebung, Verarbeitung oder Nutzung der Inhalte von Telekommunikationsdiensten, die zu beruflichen Zwecken verwendet werden (§ 32i Abs. 2). Diese Beispiele deuten darauf hin, dass der Regierungsentwurf die Rechte der Beschäftigten in diesen Punkten nicht stärkt.

Die restriktive Regelung in § 32l Abs. 1 des Regierungsentwurfs, die Einwilligungen nur in einer abschließend genannten Zahl von Fällen zulässt, kann in der betrieblichen Praxis zu Problemen führen, wenn es Konstellationen gibt, in denen Einwilligungen unstreitig auf freiwilliger Basis erteilt werden. Beispielhaft sei auf die Übermittlung von Beschäftigtendaten an Dritte im Rahmen internen Aktienkaufprogrammen verwiesen.

Um derartige Einwilligungen auch in Zukunft möglich zu machen, könnte eine Öffnung der Regelung in § 32l Abs. 1 des Regierungsentwurfs zur Vermeidung erfolgen, wenn flankierende Schutzmaßnahmen normativ verankert würden.

Hierzu könnte die verbindliche Vorgabe gehören, dass über den im künftigen BDSG genannten Einwilligungstatbestände weitere Einwilligungen nur zulässig sind, wenn als Ergebnis einer neutralen Bewertung zu Ungunsten der Beschäftigten keine Abweichungen vom Schutzstandard des Beschäftigtendatenschutzes gegeben sind.

Weiterhin könnte normativ zu Lasten der Arbeitgeber für Streitfälle eine Beweislastumkehr vorgesehen werden, wenn sie aus einer Einwilligungen Rechte herleiten wollen. Vorbild für eine solche Regelung könnte § 22 AGG sein. Schließlich könnte die Wirksamkeit einer eingeforderten freiwilligen Einwilligung daran gekoppelt werden, dass im Rahmen eines Mitbestimmungsverfahrens eine Prüfung durch den Betriebsrat erfolgt ist. Wo dieser nicht gewählt ist, könnte die Prüfung stattdessen durch den betrieblichen Datenschutzbeauftragten oder durch die zuständige staatliche Aufsichtsbehörde vorgenommen werden.

3. Erhebungsbefugnisse in der Bewerbungsphase

Die Zulässigkeit der Datenerhebung in der Bewerbungsphase wird grundlegend in § 32 des Regierungsentwurfs geregelt. Die hiernach möglichen Datenerhebungen sind sehr weit gefasst. Dies macht schon die in § 32 Abs. 1 Satz 2 des Regierungsentwurfs zu findende Formulierung deutlich, nach der die Erhebung von Daten in der Bewerbungsphase erlaubt ist, „um die Eignung des Beschäftigten“ festzustellen. Der allgemeine Begriff der Eignung geht über die intendierte Feststellung der fachlichen Eignung hinaus. Hierauf bezogen lässt sich eine Begrenzung der Erkenntnismöglichkeiten des Arbeitgebers zwar aus § 32 Abs. 7 des Regierungsentwurfs herleiten. Hiernach ist die Zulässigkeit der Datenerhebung daran gebunden, dass Art und Ausmaß der Datenerhebung im Hinblick auf den Zweck verhältnismäßig sind. In der Praxis generiert diese normative Unklarheit aber die Notwendigkeit der Präzisierung durch die Rechtsprechung.

Bezogen auf die angestrebte Verbesserung des Beschäftigtendatenschutzes ist auch die Regelung in § 32 Abs. 6 Satz 2 des Regierungsentwurfs kritisch zu bewerten. Hiernach können Arbeitgeber allgemein zugängliche Daten über Beschäftigte erheben, wenn sie hierauf vor der Erhebung hingewiesen haben. Ausreichend würde es sein, wenn der entsprechende Hinweis sich etwa in der Stellenausschreibung finden würde. Ist diese Voraussetzung erfüllt, könnten Arbeitgeber Informationen über Bewerber im Internet mittels Suchmaschine legal sammeln. Für Bewerber hat diese normative Situation zur Folge, dass sie nicht wissen, welche der über sie im Internet verfügbaren und möglicherweise von Dritten ohne ihre Kenntnis eingestellten Daten ein Arbeitgeber berücksichtigt hat.

Praktisch lässt sich die Möglichkeit der beschriebenen Internetrecherchen aus technischer Sicht nicht mehr verhindern. Auf der normativen Ebene ist aber trotz dieser Möglichkeiten eine Regulierung der Zulässigkeit dieses Vorgehens vorstellbar. Die Situation gleicht strukturell bezüglich des technisch möglichen Herunterladens etwa der Situation bei urheberrechtlich geschützter Musik und der hierzu erfolgten normativen Regulierung.

Soll Beschäftigtendatenschutz im Angesicht der bestehenden technischen Möglichkeiten trotzdem gesichert werden, könnte die Zulässigkeit von Internetrecherchen über Bewerber mit der Schaffung adäquater Informationsrechte verbunden werden. In diesem Zusammenhang ist zu bedenken, dass Beschäftigte nach geltendem Recht gegenüber einem Arbeitgeber, der entsprechende Internetrecherchen durchführt, gemäß § 33 Abs. 1 Satz 1 BDSG einen Rechtsanspruch auf Benachrichtigung haben über die Art der Daten, die gespeichert wurden, die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Identität der verantwortlichen Stelle. Hieraus können sie einen Informationsanspruch ableiten, der sie im konkreten Fall möglicherweise in die Lage versetzt, Ansprüche nach dem AGG geltend zu machen.

Ein effektiver Beschäftigtendatenschutz durch Schaffung einer Transparenz über das Wissen, das Arbeitgeber über Bewerber im Rahmen von Internetrecherchen erwerben können, würde demnach voraussetzen, dass Beschäftigte konkret über die verwendeten Suchbegriffe und die aufgesuchten Seiten informiert werden. Dies ließe sich etwa durch die Verpflichtung zur Protokollierung der Suchvorgänge und zur Übermittlung der Protokolle an Bewerber realisieren.

4. Ärztliche Untersuchungen

Der Umgang mit ärztlichen Untersuchungen sowie mit der Anforderung von Blut- und Urinproben wurde in zahlreichen Fällen aus den letzten Jahren datenschutzrechtlich als unzulässig oder zumindest als kritisch bewertet. Erinnerung sei nur an Bluttests bei Bewerbern für Tätigkeiten bei Rundfunkanstalten oder Automobilherstellern, die durch die Art der Tätigkeit in Verwaltungsbereichen nicht gerechtfertigt waren. Ähnlich verhält es sich mit „Reihenurinuntersuchungen“ bei Bewerbern um eine Ausbildungsstelle vor Abschluss eines Ausbildungsvertrags wurden in der öffentlichen Debatte kritisch hinterfragt.

Vor diesem Hintergrund ist die Aufnahme einer Regelung zur Zulässigkeit ärztlicher Untersuchungen in § 32a Abs. 1 des Regierungsentwurfs grundsätzlich zu begrüßen. Allerdings zeigt die Norm schon deshalb keine klaren Grenzen der Zulässigkeit auf, weil sie in der zweiten Regelungsalternative von Abs. 1 Satz 1 ärztliche Untersuchungen zur Feststellung der Erfüllung bestimmter gesundheitlicher Voraussetzungen auch bezüglich der Bedingungen der Ausübung einer Tätigkeit zulässt. Dies schafft Auslegungsspielräume, die kontraproduktiv zur angestrebten Verbesserung der datenschutzrechtlichen Situation von Bewerbern sind. Angestrebt werden sollte deshalb eine klarere Begrenzung auf Untersuchungen, die aus objektiver Sicht eine Limitierung auf solche Untersuchungen beinhaltet, die wegen der Art der auszuübenden Tätigkeit eine wesentliche und entscheidende Bedingung für deren Ausübung sind. Gleichzeitig sollte festgeschrieben werden,

dass Arbeitgeber das bezogen auf Persönlichkeitsrechte der Beschäftigten mildeste Mittel der ärztlichen Untersuchung wählen müssen.

Bezüglich zulässige ärztlicher Untersuchungen innerhalb von Beschäftigungsverhältnissen enthält § 32c Abs. 3 Nr. 2 des Regierungsentwurfs die Möglichkeit, dass ärztliche Untersuchungen auch im Zusammenhang mit dem beabsichtigten Wechsel einer Tätigkeit oder eines Arbeitsplatzes verlangt werden können. Diese Regelung eröffnet Arbeitgebern Handlungsspielräume, die arbeitsrechtlich nicht nachzuvollziehen sind. Aus Blick des Beschäftigtendatenschutzes ist bezogen auf § 32c Abs. 3 des Regierungsentwurfs insgesamt eine Begrenzung auf die Fälle notwendig, in denen ärztliche Untersuchungen gesetzlich vorgeschrieben sind. Darüber hinausgehende Untersuchungsverlangen könnten durch ein Verfahren der Vorprüfung einer von Arbeitgebern gewollten Einwilligung durch Betriebsräte, betriebliche Datenschutzbeauftragte oder staatliche Aufsichtsbehörden rechtlich flankiert werden.³

5. Videoüberwachung

Die Fälle unzulässiger Videoüberwachung von Beschäftigten bei einem großen Lebensmitteldiscounter waren im April 2008 der Ausgangspunkt einer sich schnell intensivierenden Debatte um die Notwendigkeit einer Verbesserung des Beschäftigtendatenschutzes. In der Folgezeit gab es zahlreiche weitere Beispiele unzulässiger Videoüberwachung, etwa bei einem Lebensmittelproduzenten. Die arbeits- und datenschutzrechtliche Bewertung dieser Fälle hat das Fehlen einer gesetzlichen Regelung zur Videoüberwachung in nicht öffentlich zugänglichen Betriebsstätten verdeutlicht. Vor diesem Hintergrund ist die Aufnahme von § 32f in den Regierungsentwurf zu begrüßen.

³ Vgl. hierzu die Ausführungen zu Kapitel 2 / Seite 8.

Kritisch ist anzumerken, dass durch § 32f des Regierungsentwurfs die Handlungsmöglichkeiten von Arbeitgebern gegenüber denen aus § 6b BDSG erweitert werden. Dies wird am Beispiel der durch § 32f Abs. 1 Nr. 7 möglichen Erhebung von Beschäftigtendaten zur Qualitätskontrolle deutlich. Unter dieses Tatbestandsmerkmal ließe sich etwa auch die permanente Beobachtung von Produktionsmitarbeitern subsumieren, wenn etwa ein Zulieferbetrieb mit einem Abnehmer ein „Null-Fehler-Konzept“ vereinbart hat und diesem gegenüber durch Videoaufzeichnung im Streitfall nachweisen können will, dass alle Beschäftigten jeden Handgriff richtig gesetzt haben. Gemessen an der Rechtsprechung des BAG zur Videoüberwachung, die permanente „Totalkontrollen“ für den Regelfall ausschließt⁴, wäre ein solches Vorgehen derzeit unzulässig. Es könnte vor dem Hintergrund der neuen Rechtsgrundlage von der Rechtsprechung künftig als zulässig erachtet werden, wenn das überwiegende schutzwürdige Interesse der Betroffenen am Ausschluss der Datenerhebung, das im letzten Halbsatz von § 32f Abs. 1 Satz 1 des Regierungsentwurfs ausdrücklich genannt ist, im konkreten Fall negiert würde.

In der betrieblichen Praxis wird weiterhin die in § 32f Abs. 1 Satz 2 des Regierungsentwurfs enthaltene Verpflichtung des Arbeitgebers zur Kenntlichmachung der Videoüberwachung durch geeignete Maßnahmen zu Problemen führen. Mit Blick auf die Rechtsprechung, die Beschäftigten zur Wahrung ihrer Persönlichkeitsrechte auch im Betrieb kontrollfreie Bereiche zuspricht⁵, wird es nicht ausreichend sein, nur pauschal auf den Umstand der Videoüberwachung hinweisen. Ergänzend muss in Situationen, in denen die Abgrenzung von berechtigt kontrollierten Bereichen und kontrollfreien Zonen für Beschäftigte nicht eindeutig ist, durch weitere Maßnahmen wie beispielsweise farbliche Kennzeichnung auf dem Fussboden einer Halle oder eines Büros verdeutlicht werden, wo gefilmt wird und wo nicht.

⁴ Vgl. etwa BAG vom 14.12.2004 - 1 ABR 34/03, RDV 2005, 216

⁵ Vgl. BAG vom 14.12.2004, a.a.O.

Abschließend sei die Bemerkung erlaubt, dass das vielfach formulierte Ziel des Gesetzgebers, heimliche Videoüberwachungen ausschließen zu wollen, sich derzeit gesetzestechnisch noch dezent im Hintergrund hält. Das Verbot heimlicher Videoüberwachung wird in § 32f selbst nämlich nicht ausdrücklich genannt, sondern muss aus § 4e Abs. 4 Nr. 3 i.V.m. Abs. 2 des Regierungsentwurfs hergeleitet werden, weil die Videoüberwachung als ein sonstiges besonderes technisches Mittel zu qualifizieren ist, mit dem die Erhebung ohne Kenntnis der Betroffenen unzulässig ist.

6. Verdeckte Datenerhebung und nachträgliche Auswertung vorhandener Daten

Eine Reihe bekannter Fälle unzulässiger Datenerhebung und Datenverarbeitung der letzten Jahre erfolgte mit dem Ziel der Aufdeckung von Straftaten oder schwerwiegender Pflichtverletzungen ohne Kenntnis der Beschäftigten und teilweise auch ohne gesetzeskonforme Einschaltung der zuständigen Betriebsratsgremien. Herausragende Aufmerksamkeit fanden insbesondere entsprechende Vorgänge bei der Telekom AG und der Bahn AG.

Neben der unzulässigen heimlichen Videoüberwachung hat die Reihe heimlicher Datenerhebungen und Datenverarbeitungen die Notwendigkeit einer Verbesserung des Schutzes der Beschäftigten verdeutlicht. Vor diesem Hintergrund überrascht es, dass der Gesetzentwurf Arbeitgebern durch § 32d Abs. 3 weitgehende Befugnisse zugesteht, vorhandene Daten mit dem Ziel der Aufdeckung von Straftaten oder anderen schwerwiegenden Pflichtverletzungen zu verarbeiten. Der Regierungsentwurf bleibt damit hinter dem Stand der geltenden Regelung in § 32 Abs. 1 Satz 2 BDSG zurück, die zum 1. September 2009 als erste Reaktion auf die zahlreichen Fälle von Datenmissbrauch in das Gesetz eingefügt wurde. Voraussetzung einer Erhebung, Verarbeitung oder Nutzung ist nach dieser Norm, dass *„zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass*

der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat“. Die geplante Regelung stellt aus Sicht der Beschäftigten damit nur eine Verschlechterung gegenüber der bisherigen Gesetzessituation dar.

An dieser Feststellung ändert sich auch durch das vorgesehene Verarbeitungsverfahren nichts, das zunächst einen anonymen oder pseudonymen Abgleich vorsieht und erst im Verdachtsfall eine Personalisierung vorsieht. Die Durchführung entsprechender Datenabgleiche steht nach dem derzeitigen Gesetzesvorschlag im alleinigen Ermessen des Arbeitgebers. Insoweit ist eine ausgewogene Inhaltskontrolle nicht garantiert.

Die in § 32d Abs. 3 des Regierungsentwurfs enthaltenen Tatbestandsvoraussetzungen, durch die eine „Personalisierung“ gerechtfertigt würde, sind nicht präzise gefasst. Diese Aussage gilt insbesondere hinsichtlich der Zulässigkeit eines Datenabgleichs mit dem Ziel der Aufdeckung schwerwiegender Pflichtverletzungen. Der Gesetzestext zielt diesbezüglich wohl auf das Vorliegen der Voraussetzungen einer Kündigung aus wichtigem Grund gemäß § 626 BGB ab. Diesbezüglich ist zu bedenken, dass die Schwelle für eine solche Kündigung auch nach der im *„Fall Emmely“* zu Gunsten der gekündigten Klägerin ergangenen Entscheidung des BAG⁶ nicht übermäßig hoch ist.

Im Ergebnis gesteht die Regelung in § 32d Abs. 3 des Regierungsentwurfs Arbeitgebern weitergehende Rechte zu als die bisherige Rechtssituation. Sie gefährdet damit in der Praxis auch funktionierende Betriebsvereinbarungen, die mit dem Ziel getroffen wurden, einerseits Arbeitgeber vor Straftaten und schwerwiegenden Pflichtverletzungen zu schützen und andererseits die Rechte von Beschäftigten zu wahren.

Besonders kritisch ist in diesem Zusammenhang die Regelung in § 32e Abs. 2, nach der Arbeitgeber in den dort abschließend genannten Fällen Beschäftigten-

⁶ BAG vom 10.06.2010 - 2 AZR 541/09, NZA 2010, 1227.

daten auch ohne Kenntnis der Beschäftigten erheben dürfen. Voraussetzung ist auch hier, dass Tatsachen den Verdacht begründen, dass im Beschäftigungsverhältnis eine Straftat oder eine andere schwerwiegende Pflichtverletzung begangen wurde. Diese Regelung ist durch den letzten Halbsatz von Abs. 2 sowohl „repressiv“ bezüglich der Aufdeckung begangener Straftaten oder Pflichtverletzungen als auch „präventiv“ bezüglich der Verhinderung weiterer ausgestaltet. Die neue Vorschrift bleibt bezüglich der tatbestandlichen Voraussetzungen hinter den bereits angesprochenen weitergehenden Anforderung in § 32 Abs. 1 Satz 2 BDSG zurück.

Die Erhebung von Daten zu Zwecken der Aufdeckung oder Verhinderung von Straftaten und anderen schwerwiegenden Pflichtverstößen im Beschäftigungsverhältnis steht gemäß § 32e Abs. 3 des Regierungsentwurfs unter dem Vorbehalt der Verhältnismäßigkeit. Weiterhin muss die Erforschung auf andere Weise erschwert oder weniger erfolgversprechend sein. Diese Regelung nimmt die Vorgaben der Rechtsprechung des BAG zum Persönlichkeitsschutz nur unzureichend auf.

Das propagierte Ziel, den Beschäftigtendatenschutz zu verbessern, wird durch die §§ 32d Abs. 3 und § 32e Abs. 2 des Regierungsentwurfs weit verfehlt. Arbeitgebern werden nach dieser Norm vielmehr zu Zwecken der Ermittlung und Identifikation von Straftaten und schwerwiegenden Pflichtverletzungen datenschutzrechtliche Kompetenzen eingeräumt, die weitreichender sind als bisher.

Ergebnis dieser Regelung wäre, dass die Zahl von Datenschutzverstößen gegenüber Beschäftigten abnimmt. Dies aber nur deshalb, weil sich Zahl und Umfang erlaubter Eingriffe in die Persönlichkeitsrechte der Beschäftigten erhöhen.

7. Zugriff auf Telekommunikationsdaten

Die Zugriffsmöglichkeiten von Arbeitgebern auf die Daten, die bei der Nutzung von betrieblichen Telekommunikationseinrichtungen anfallen, ist in der betrieblichen Praxis ein zentrales und oft auch kontroverses Diskussionsthema für Arbeitgeber, Betriebsräte und Arbeitnehmer.

Debattiert wird zunächst über die Notwendigkeit und Zulässigkeit des Zugriffs auf dienstliche Daten. Einvernehmen besteht in diesem Punkt zumeist dazu, dass Arbeitgeber bestimmte Daten aus gesetzlichen oder betrieblichen Gründen benötigen. Hierzu gehören insbesondere Geschäftsdaten, die nach steuerrechtlichen Grundsätzen vorgehalten werden müssen.

Das Einvernehmen endet, wenn es um die Verwendung anderer Daten wie insbesondere der geschriebenen und empfangenen E-Mails geht. Soweit die private Nutzung betrieblicher Systeme verboten ist, wird teilweise die Auffassung vertreten, dass dann Arbeitgebern die Einsicht in die E-Mails zusteht. Vor diesem Hintergrund wird teilweise auch eingefordert, bei Abwesenheit alle eingehenden E-Mails an einen Vertreter umzuleiten. Dieser Auffassung wird entgegen gehalten, dass es auch im dienstlichen Rahmen persönliche Kommunikationsvorgänge gibt, die sich der Kenntnis des Arbeitgebers oder direkter Vorgesetzter entziehen müssen wie etwa die Korrespondenz zwischen einem Arbeitnehmer und dem Betriebsrat, dem betrieblichen Datenschutzbeauftragten oder der Personalabteilung in einer individuellen Einkommenssteuerangelegenheit.

Verschärft wird die Diskussion um die Zulässigkeit der Zugriffe auf Daten aus dem Bereich der Nutzung von Telekommunikationsdiensten, wenn die private Nutzung betrieblicher Systeme erlaubt bzw. nicht ausdrücklich verboten ist. In diesen Fällen setzen insbesondere die anwendbaren Vorgaben des TKG Zugriffen der Arbeitgeber auf Inhaltsdaten praktisch absolute Grenzen, sofern keine wirksame Einwilligung der Beschäftigten besteht.

Die vorstehend skizzierten Fragen löst § 32i des Regierungsentwurfs nicht oder nur begrenzt, da es sich auf die ausschließlich dienstliche Nutzung beschränkt. Aber auch in diesem Rahmen wird keine Rechtsklarheit bezüglich des besonders zu schützenden Bereichs der „persönlichen dienstlichen Kommunikation“ geschaffen. Das Verbot der Erhebung, Verarbeitung und Nutzung der persönlichen Daten, die etwa aus einem E-Mail-Verkehr mit einem Betriebsrat oder dem zuständigen Personalreferenten resultieren, muss im Einzelfall aus der Abwägung zwischen den Interessen des Arbeitgebers und den schutzwürdigen Interessen der Beschäftigten abgeleitet werden. Diese Abwägung findet sich in § 32i des Regierungsentwurfs mehrfach wieder.

Die Bewertung der zutreffenden Durchführung der notwendigen Interessenabwägung obliegt damit im Ergebnis ebenso der Rechtsprechung wie das Setzen von notwendigen Begrenzungen. Rechtsklarheit wird damit nicht erzeugt.

8. Compliance

Teile der Neuregelungen des Regierungsentwurfs sind dazu bestimmt, die Grundlagen für die Durchsetzung von Compliance-Anforderungen der Arbeitgeber zu sein. Insbesondere die Regelung in § 32d Abs. 3 des Regierungsentwurfs soll eine Grundlage für die Korruptionsbekämpfung und die Durchsetzung von Compliance-Anforderungen darstellen.⁷

Unklar bleibt allerdings, wofür dieser Begriff steht. Zum Regierungsentwurf findet sich in den Materialien die folgende Definition: *„Compliance bedeutet in diesem Zusammenhang die Einhaltung aller relevanten Gesetze, Verordnungen, Richtlinien und Selbstverpflichtungen durch ein Unternehmen als Ganzes.“*⁸

⁷ Vgl. BT-Drs. 17/4230, S. 18.

⁸ Vgl. a.a.O.

Setzt man diese Definition bei der Interpretation der Vorschrift voraus, werden Arbeitgebern im Rahmen von Compliance-Aktivitäten weitgehende Befugnisse eingeräumt, um Datenerhebungen und Datenverarbeitungen gemäß § 32d Abs. durchzuführen. Unter den Voraussetzungen von § 32e Abs. 2 des Regierungsentwurfs könnte dies ggf. auch ohne Kenntnis der Beschäftigten, also „heimlich“ erfolgen.

Dies ist in der betrieblichen Praxis immer dann höchst problematisch, wenn Richtlinien oder Selbstverpflichtungen von Arbeitgebern einseitig gestaltet und vorgegeben werden. So sieht sich beispielsweise derzeit der zuständige Betriebsrat in einem großen europäischen Unternehmen mit einem Code of Compliance konfrontiert, der Beschäftigten weitgehende Verhaltensvorgaben macht. Diese Vorgaben sind wiederum maßgeblich durch Regeln der europäischen Konzernspitze geprägt, die ihren Sitz in einem anderen europäischen Land hat. Die Einhaltung der Vorgaben soll auch durch Auswertungen personenbezogener Daten in den verwendeten elektronischen Systemen kontrolliert werden. Die beabsichtigten Kontrollen haben nach der übereinstimmenden Meinung von Arbeitgeber und Betriebsrat derzeit in Deutschland keine Rechtsgrundlage. Die Konzernspitze hat dem Betriebsrat deshalb gerade mitgeteilt, dass die Einführung zur Vermeidung rechtlicher Unklarheiten erst nach Verabschiedung des hier zu diskutierenden Gesetzes erfolgen soll. Auf der Grundlage von § 32d Abs. 3 des Regierungsentwurfs hält sie die geplanten Kontrollen für zulässig.

9. Verarbeitungsregeln in Konzern

Der Regierungsentwurf enthält derzeit keine Erweiterung zur Zulässigkeit der unternehmensübergreifenden Verarbeitung in Konzernen. Eine solche Regelung wird indes in der Diskussion immer wieder gefordert.

Für eine solche Regelung spricht aus Sicht von Unternehmen und Konzernen die Vereinfachung von Verarbeitungsvorgängen gerade in Großkonzernen wie bei-

spielsweise eine Zentralisierung der Verarbeitung von Finanz-, Vertriebs- oder Personaldaten in zentralen Systemen. Derartige Zentralisierungen sind indes nach dem geltenden BDSG schon heute zulässig, beispielsweise auf der Grundlage von Aufträgen gemäß § 11 BDSG. Sie finden auf dieser Basis auch in vielen Fällen rechtskonform statt. Insoweit gibt es grundlegende Zweifel an der Notwendigkeit einer solchen Ergänzung.

Ein Sinn für eine solche Erweiterung erschließt sich aber aus der Praxis: Betriebsräte und betriebliche Datenschutzbeauftragte, die im Rahmen ihrer Aufgaben mit der Bewertung unternehmensübergreifender Systeme befasst sind, stellen in einer nicht geringen Zahl von Fällen fest, dass innerhalb von Konzernen eine unternehmensübergreifende Datenverarbeitung erfolgt, ohne dass die nach § 11 BDSG notwendigen Aufträge vertraglich abgesichert sind. Liegen entsprechende Verträge vor, erfüllen sie teilweise nicht die zwingenden Formvorgaben des § 11 BDSG oder sind aus anderen Gründen rechtsfehlerhaft.

Betriebsräte haben am Abschluss von Verträgen nach § 11 BDSG mit Blick auf den im Rahmen ihrer gesetzlichen Mitbestimmungsrechte angestrebten Persönlichkeitsschutz von Beschäftigten ein großes Interesse. Nur auf diesem Weg können sie bei unternehmensübergreifenden Verarbeitungen überprüfen und sicherstellen, ob etwa der Regelungsinhalt von Betriebsvereinbarungen zu IT-Systemen auch für Auftragnehmer verpflichtend ist. Sind etwa bestimmte Auswertungen nach einer Betriebsvereinbarung im Betrieb oder Unternehmen verboten, muss dies vertraglich auch mit einem Auftragnehmer vereinbart werden. Entsprechende Gestaltungen können Betriebsräte auf der Basis bestehender Mitbestimmungsrechte derzeit noch durchsetzen.

Würde die Schaffung einer konzernweiten Berechtigung zur Verarbeitung von Daten zum Wegfall der Notwendigkeit des Abschlusses von Aufträgen nach § 11 BDSG führen, hätte dies aus kollektivrechtlicher Sicht zur Folge, dass Betriebsräte das vorstehend beschriebene Regelungsinstrument ersatzlos verlieren. Betriebs-

vereinbarungen, die mit dem Ziel des Persönlichkeitsschutzes getroffen werden, könnten vor diesem Hintergrund leerlaufen, wenn es innerhalb von Konzernen keine wirksamen Begrenzungen auf zulässige Verarbeitungen gibt. Erfolgt die unternehmensübergreifende Verarbeitung grenzüberschreitend, hätten Betriebsräte in Konzernen noch nicht einmal mehr die Möglichkeit der Einbindung eines Konzernbetriebsrats.

Die Schaffung der Möglichkeit, innerhalb von Konzernstrukturen unternehmensübergreifende Erhebung-, Verarbeitungs- und Nutzungsmöglichkeiten einzuführen, würde damit unmittelbar die Mitwirkungs- und Mitbestimmungsrechte von Betriebsräten schwächen, ohne dass es vor dem Hintergrund der Möglichkeiten nach § 11 BDSG für eine solche Novelle einen zwingenden Grund gibt. Auch in diesem Punkt wird damit das Regelungsziel eines besseren Beschäftigtendatenschutzes verfehlt.