Moderner Datenschutz für die Beschäftigten: Ein Ende der Skandale?

Gutachten zum Regierungsentwurf zur Regelung des Beschäftigtendatenschutzes

im Auftrag des

Hugo Sinzheimer Instituts für Arbeitsrecht, Frankfurt am Main

Erstellt durch:

Prof. Dr. jur. Marita Körner

Professorin für Wirtschafts- und Arbeitsrecht
der Universität der Bundeswehr, München

Frankfurt am Main, 08.11.2010

Prof. Dr. jur. Marita Körner

Begutachtung des Regierungsentwurfs zur Regelung des Beschäftigtendatenschutzes

15.10.2010

Einleitung

Erst zum 1.9.2009 wurde als eilige Reaktion des Gesetzgebers auf mehrere „Datenskandale" in Großunternehmen § 32 ins BDSG aufgenommen und geregelt, dass die Erhebung, Verarbeitung und Nutzung von personenbezogenen Beschäftigtendaten zulässig ist, wenn diese Daten für das Beschäftigungsverhältnis *erforderlich* sind. Damit wollte der Gesetzgeber den bis dahin für Beschäftigungsverhältnisse geltenden § 28 I 1 Nr. 1 BDSG konkretisieren und die Rechtsprechungsgrundsätze zusammenfassen.[1] Eine echte Neuerung brachte die Regelung nicht.[2] Daher will die Regierung bereits ein knappes Jahr später die Reform reformieren und hat am 25.8.2010 den *Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes* vorgelegt (im Folgenden: RegE),[3] der die modifizierte Version des Referentenentwurfs des Bundesministeriums des Inneren darstellt.[4]

Seit zwanzig Jahren ist der Arbeitnehmerdatenschutz ein Thema,[5] wenn auch die öffentliche Wahrnehmung der Probleme erst durch die Fälle bei Telekom, Lidl und der Bahn geschärft wurde und darüber das datenschutzrechtlich noch brisantere Thema *Elena* (Elektronischer Entgeltnachweis) fast in den Hintergrund tritt. Dieses „größte Datensammelprojekt in der Geschichte der Bundesrepublik“[6] wurde zu Beginn des Jahres 2010 von derselben Bundesregierung eingeführt, die jetzt „umfassende gesetzliche Regelungen für den Arbeitnehmerdatenschutz verwirklichen“ will.[7] Der Regierungsentwurf spiegelt die Diskussion der letzten beiden Jahrzehnte allerdings nicht, sondern versucht mit im Kern 13 neuen Paragraphen im BDSG (§§ 32-32l RegE) den aktuellen Datenschutzproblemen im Beschäftigungsverhältnis gerecht zu werden.

---

[1] BT Ds. 16/13657, S. 35.
[2] *Thüsing*, NZA 2009, 865, 870.
[3] Abrufbar unter www.bmi.bund.de
[4] Eine detaillierte Gegenüberstellung der Referentenentwürfe vom 28.5., 28.6. und 11.8.2010 und des Regierungsentwurfs vom 25.8.2010 findet sich im MMR-Forum zum Beschäftigtendatenschutz: http://community.beck.de/system/files/private/SynopseRefE.pdf
[5] Vgl. nur *Däubler*, Gläserne Belegschaften, seit 1990, zuletzt 5. Auflg. 2010.
[6] Süddeutsche Zeitung Nr. 212, 14.9.2010, S. 6.
[7] RegE, S. 1.

I. Struktur des Entwurfs

Eine bereichsspezifische Regelung für den Arbeitnehmerdatenschutz wird seit Jahrzehnten gefordert. Etliche Vorschläge wurden gemacht, auch in jüngster Zeit, u.a. mit dem Entwurf eines Gesetzes zum Datenschutz im Beschäftigungsverhältnis der SPD, die den Arbeitnehmerdatenschutz in einem eigenen Gesetz regeln will[8] oder dem geplanten Gesetzentwurf von Bündnis90/Die Grünen, die ebenfalls ein eigenes Gesetz vorschlagen, das derzeit online diskutiert werden kann[9] und parallel zum Gesetzentwurf der Bundesregierung eingebracht werden soll.
Dagegen hat sich die Bundesregierung für eine kleine Lösung entschieden. Für die Ergänzung des BDSG mögen auf den ersten Blick systematische Gründe sprechen. Die Nachteile aber überwiegen. Zum einen ist das BDSG den Besonderheiten der Rechtsmaterie Arbeitsrecht nicht gewachsen. Die zu regelnden Themen sind zu komplex, um mit wenigen Paragraphen erfasst werden zu können. Zum anderen ist das BDSG selbst veraltet. Seit 1977, dem Jahr seines Erlasses, ist es zwar immer wieder modifiziert und ergänzt worden. Konzeptionell stammt der rechtliche Datenschutz aber noch immer aus dieser Zeit, die geprägt war, von Datenschutzproblemen im öffentlichen Bereich. Mittlerweile hat ein Paradigmenwechsel stattgefunden: massenhafte private Datenerhebung und - verarbeitung ist heute der Hauptbereich für Datenschutzprobleme, weshalb schon länger die grundlegende Modernisierung des Datenschutzrechts insgesamt gefordert wird. Vor diesem Hintergrund ist es kontraproduktiv, einem grundlegend reformbedürftigen Gesetz noch eine hochkomplexe Spezialmaterie aufzupfropfen, zumal dieser Weg dazu führt, dass wesentliche Ziele, die die Bundesregierung mit dem Entwurf verfolgt, nicht erreicht werden können.

II. Umsetzung der Ansprüche des Entwurfs

Schon laut Koalitionsvertrag vom 26.10.2009 soll das BDSG lesbarer, verständlicher und zukunftsfest gemacht werden sowie technikneutral sein.[10] Das greift der RegE auf, der „umfassende, allgemeingültige Regelungen für den Datenschutz am Arbeits-

[8] BT Ds. 17/69, 25.11.2009.
[9] http://beschaeftigen-datenschutz.de
[10] Koalitionsvertrag zwischen CDU, CSU und FDP vom 26.10.2009, S. 105.

platz" schaffen will, die dem „Grundprinzip der Transparenz“ entsprechen.[11] Dem wird der Entwurf nur bedingt gerecht.

1. Schutz der Beschäftigten[12]

Schon das Hauptziel des RegE, dass „die Beschäftigten vor der unrechtmäßigen Erhebung und Verwendung ihrer personenbezogenen Daten besser geschützt werden“ sollen,[13] kann nur partiell erreicht werden, da im Mittelpunkt der Regelungen das Informationsinteresse des Arbeitgebers steht, dem „verlässliche Grundlagen für die Durchsetzung von Compliance-Anforderungen und den Kampf gegen Korruption an die Hand gegeben werden“,[14] wenn auch die Befugnisse des Arbeitgebers im Vergleich zu den BMI-Entwürfen eingeschränkt wurden. Typisch ist dafür gleich der erste Satz im Einstiegsparagraphen § 32 I RegE: „Der Arbeitgeber darf…“, heißt es dort. Dagegen ist der zentrale Grundsatz jeden Datenschutzes und also auch des Beschäftigtendatenschutzes, dass Beschäftigtendaten unmittelbar beim Beschäftigten erhoben werden müssen, versteckt in § 32 VI RegE.

Die Befugnisse für die Datenerhebung und –verarbeitung durch den Arbeitgeber werden offenbar als gerechter Ausgleich für die Datenschutzrechte verstanden, die den Beschäftigten zugestanden werden. Dabei bleibt außer Betracht, dass „Ausgleich“ kein Kriterium für die Zulässigkeit der Erhebung und Verarbeitung von personenbezogenen Daten ist. Maßstab hierfür ist allein das verfassungsmäßig geschützte Recht des Einzelnen auf informationelle Selbstbestimmung,[15] das nur unter engen, klar bestimmten Voraussetzungen eingeschränkt werden darf. Dazu können auch gesetzliche Verpflichtungen des Arbeitgebers gehören, zu deren Erfüllung er bestimmte Informationen erheben und verarbeiten muss.

[11] Hintergrundpapier zum Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes – Kabinettsbeschluss vom 25.8.2010, abrufbar unter: www.bmi.bund.de, S. 1 (zitiert als: Hintergrundpapier).
[12] In § 3 XI BDSG definiert das BDSG seit 1.1.2009 den Begriff des Beschäftigten, der weiter ist als derjenige des Arbeitnehmers. Dennoch werden die Begriffe sowohl im RegE wie in dessen Begründung (und auch durchweg in der Literatur) z.T. synonym gebraucht.
[13] Hintergrundpapier, S. 2.
[14] RegE, Begründung (A.I.).
[15] BVerfGE 65, 1.

a) Einfallstor *compliance*

Der RegE geht aber viel weiter. Durch die bedenkenlose Übernahme des anglo-amerikanischen Begriffs der *compliance* – bezeichnenderweise wird der Begriff weder übersetzt noch definiert – als Türöffner für die Erhebung personenbezogener Informationen von Beschäftigten,[16] kann der Arbeitgeber letztlich selbst bestimmen, welche Daten er für *compliance*-konformes Verhalten benötigt.

Der Begriff der *compliance* ist schillernd. Er ist weder in der Rechtswissenschaft noch in der Betriebswirtschaft eindeutig definiert[17] und reicht von „gesetzeskonformem Verhalten von Unternehmen“[18] über *compliance* als ein „Organisationsmodell mit Prozessen und Systemen, das die Einhaltung von gesetzlichen Bestimmungen, internen Standards sowie die Erfüllung wesentlicher Ansprüche der Stakeholder sicherstellt“[19] bis zur Einschätzung, dass als *compliance* „sämtliche vorbeugenden Maßnahmen bezeichnet werden, die an *irgendwelche* Verhaltensanforderungen für bzw. im Unternehmen anknüpfen“[20]. Der Deutsche Corporate Governance Kodex regelt in Nr. 4.1.3, dass der Vorstand für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen hat. Eine klare Abgrenzung berechtigter Informationsbedürfnisse ist damit nicht möglich. Daher ist es erforderlich, den Begriff der *compliance* jedenfalls im Zusammenhang des Beschäftigtendatenschutzes zu definieren und klarzustellen, dass damit ausschließlich gesetzliche Regelungen gemeint sind. Aber auch bei der Kontrolle der Einhaltung gesetzlicher Anforderungen darf der Arbeitgeber nicht zu einer Art Ersatz-Staatsanwaltschaft werden. Für die Verfolgung von Straftaten ist der Staat zuständig.

b) Einschränkung der Einwilligungsmöglichkeiten

Zu begrüßen ist die Einschränkung der Einwilligung als Rechtfertigungsgrund in § 32 l, Abs. 1 RegE. Abweichend von § 4 I BDSG kann eine Einwilligung im Rahmen der

---

[16] „…und gleichzeitig den Arbeitgebern verlässliche Grundlagen für die Durchsetzung von Compliance-Anforderungen an die Hand gegeben werden.", RegE, Begründung (A.I.).
[17] *Bergmoser/Theusinger/Gushurst*, Corporate Compliance – Grundlagen und Umsetzung, BB Beilage 2008, Nr. 5, S. 1.
[18] *Küttner*, Personalhandbuch 2010, Compliance, Rn 1.
[19] So der Ansatz von PricewaterhouseCoopers, zitiert von *Wolf*, Corporate Compliance – ein neues Schlagwort?, DStR 2006, 1995.
[20] *Mahnhold*, Compliance und Arbeitsrecht, Frankfurt 2004, S. 29 m.w.N. in Anm. 21.

§§ 32 ff. RegE nur in den gesetzlich genannten Fällen erfolgen.[21] Zwar dient die Einwilligung des Betroffenen in die Erhebung und Verarbeitung seiner personenbezogenen Daten als Grundprinzip zunächst der informationsrechtlichen Selbstbestimmung des Einzelnen, der selbst entscheiden können soll, wem er seine Daten zur Verfügung stellen will. Grundvoraussetzung der informationellen Selbstbestimmung ist aber gem. § 4a BDSG die „freie Entscheidung des Betroffenen". Wenn es auch in anderen Zusammenhängen Zweifel an der Freiwilligkeit einer Einwilligung geben kann,[22] so wird vor allem der abhängige Arbeitnehmer sehr häufig eine Einwilligung nur notgedrungen erteilen. Daher ist die Regelung in § 32 l, Abs. 1 RegE auch keineswegs europarechtswidrig.[23] Zwar sieht Art. 7 lit. a der Richtlinie 95/46/EG die Einwilligung als Rechtfertigungsgrund vor. Nach Art. 2 lit. h derselben Richtlinie ist eine wirksame Einwilligung aber eine „Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt". Sind diese Voraussetzungen nicht erfüllt, kann eine Einschränkung der Einwilligungsmöglichkeit auch in einer generell-abstrakten Regelung vorgesehen werden, wenn, wie im Arbeitsverhältnis, die Freiwilligkeit typischerweise fehlt.

2. Transparenz und Rechtssicherheit

Der vor der Einführung von § 32 BDSG im Herbst 2009 für den Arbeitnehmerdatenschutz einschlägige § 28 galt als „verwirrend"[24] und „für normale Leser unlesbar"[25].
Ob der RegE seinem Anspruch auf Rechtsklarheit und Rechtssicherheit besser genügt, muss bezweifelt werden. Im Vergleich zu einem eigenen Arbeitnehmerdatenschutzgesetz bedeutet allein schon die Einfügung einer Reihe von Vorschriften – die selbst wieder Verweise enthalten - in ein seinerseits strukturell veraltetes Gesetz nicht mehr, sondern weniger Klarheit. Dieser Befund wird verschärft durch den Umstand, dass der RegE mit einer Mischung aus abstrakt-generellen und kasuistischen Regelungen arbeitet, die in meist sehr langen Paragraphen viele Einzelfälle ansprechen. Wichtiges bleibt dagegen unsicher. So regelt der neue Absatz 3 in § 27

[21] Eine Einwilligung ist u.a. vorgesehen in § 32a (ärztliche Untersuchungen), § 32i II (Nutzung von Internet und E-Mail) oder § 32h (Verwendung eines Lichtbildes des Beschäftigten).
[22] Vgl. dazu *Körner*, Informierte Einwilligung als Schutzkonzept, in: FS für Simitis, Baden-Baden 2000, S. 131 ff.
[23] So aber *Forst*, NZA 2010, 1043, 1044.
[24] *Simits*, Kommentar zum Bundesdatenschutzgesetz 2003, 5. Auflg., § 28, Rn. 61.
[25] *Däubler/Klebe*, BDSG 2007, 2. Auflg., § 28 Rn 5.

BDSG nicht, inwieweit § 28 neben den §§ 32 ff. RegE anwendbar bleibt. Aus der Begründung zum RegE ergibt sich, dass jedenfalls „insbesondere“ § 28 I Nr. 1 verdrängt werden soll.[26] Die übrigen Vorschriften bleiben also wohl anwendbar. Angesprochen wird in der Begründung dagegen die Erhebung und Verarbeitung von Beschäftigtendaten für andere als Beschäftigungszwecke: hierfür sollen die §§ 32 ff. RegE gerade nicht gelten.[27]

Auch beim Fragerecht des Arbeitgebers bleibt etliches unklar. Zwar wird diese Materie in § 32 RegE nun erstmals gesetzlich geregelt. Allerdings wird der Stand der Rechtsprechung nicht vollständig übernommen. So fehlt ausgerechnet das durch den EuGH im deutschen Recht verankerte Verbot der Frage nach der Schwangerschaft. Durch die Verknüpfung mit dem AGG – an sich zu begrüßen -, wird mehr Verwirrung gestiftet als Klarheit geschaffen. Fragen nach AGG-Merkmalen dürfen nur unter den Voraussetzungen von § 8 AGG gestellt werden, die nach Religion oder Weltanschauung gemäß § 9 AGG. Unklar bleibt die Rechtsfolgenseite. Bei unzulässigen Fragen galt bislang das „Recht auf Lüge“ mit dem Ausschluss der Arbeitgeber-Anfechtung.[28] Da das Problem im RegE nicht angesprochen wird, könnte die Regelung eine Verschlechterung für Arbeitnehmer bedeuten, wenn die Rechtsfolge allein im Beschwerderecht des § 32 l, Abs. 4 RegE bestehen sollte. Bei unzulässigen Fragen nach AGG-Merkmalen müsste man allerdings ohnehin auch auf die – wirkungsvolleren - AGG-Sanktionen in §§ 13 ff. AGG zurückgreifen. Das bleibt sowohl im Entwurf wie auch in der Begründung unerwähnt.

3. Technikneutrale Ausgestaltung

Schließlich will der Entwurf technikneutral sein und zukünftige technische Entwicklungen mit umfassen.[29] Das ist angesichts des rasanten Veränderungstempos in der Informationstechnologie schon grundsätzlich kaum zu gewährleisten, noch viel weniger aber in einem Entwurf, dessen kasuistische Regelungen zur Videoüberwachung, Telekommunikationsmedien und Ortungssystemen ganz besonders eng den derzeit üblichen Technologien verhaftet sind. Ausgerechnet da, wo es Zukunftsträchtiges mit

[26] RegE, Begründung, S. 8 (zu Nr. 7).
[27] RegE, Begründung, S. 8 (zu Nr. 5).
[28] BAG, 5.10.1995, NZA 1996, 371.
[29] RegE, Begründung, S. 6 (VII).

zu berücksichtigen gäbe, in der Biometrie, fällt die Regelung sehr knapp aus. § 32h RegE mag für derzeit praktizierte biometrische Zugangsverfahren ausreichen, nicht aber für in der Entwicklung befindliche biometrische Verfahren, die die Erstellung kompletter Bewegungsprofile während eines gesamten Arbeitstages erlauben, etwa in sicherheitssensiblen Unternehmen, wie Flughäfen. Die Erstellung von Profilen ist im RegE aber nur in § 32d V angesprochen. Der meint aber ausschließlich die Zusammenführung von Arbeitnehmerdaten aus verschiedenen Erhebungszusammenhängen zur Erstellung von Persönlichkeits- oder Gesundheitsprofilen. Bewegungsprofile sind danach nicht verboten.

Zukunftsfestigkeit fehlt auch in der Regelung über Ortungssysteme. In der Formulierung von § 32g RegE werden die technischen Möglichkeiten von Ortungssystemen zumindest verharmlost. Verknüpft mit telemetrischen Daten, d.h. physikalischen Messwerten aus dem Fahrzeug, die gleichzeitig an den Arbeitgeber übertragen werden – technisch kein Problem – ist damit keineswegs nur die punktuelle „Bestimmung eines geografischen Standortes" möglich, sondern wiederum die Erstellung kompletter Bewegungsprofile. Weitere Verknüpfungen sind denkbar, etwa mit elektronischen Terminkalendern. Eingeschränkt wird in § 32g aber nur der Einsatz des reinen Ortungssystems, also der Datenübermittlung über den geographischen Standort.

III. Kritische Würdigung der Hauptregelungsgegenstände

1. Internetrecherche

Bislang gilt nach § 28 I 1 Nr. 3 BDSG, dass allgemein zugängliche Daten erhoben werden dürfen, also etwa die über eine Suchmaschine abrufbaren Informationen über einen Bewerber, sofern nicht die Interessen des Bewerbers überwiegen. Informationen in sozialen Netzwerken, die nur für registrierte Mitglieder zugänglich sind, sind nicht allgemein zugänglich i.S.v. § 28 I 1 Nr. 3. Allerdings gibt es hier einen erheblichen Graubereich, da auch Arbeitgeber eine Mitgliedschaft leicht erwerben können, ggfs. durch Fantasienamen nicht erkennbar, obwohl insbesondere Freund-

schaftsnetzwerke, wie Facebook oder StudiVZ in ihren AGB Arbeitgeberrecherchen verbieten.[30]

§ 32 VI 2 RegE gestattet weiterhin die Internetrecherche nach allgemein zugänglichen Daten und bringt insoweit nur die Veränderung, dass der Arbeitgeber den Beschäftigten darüber vorab informieren muss. Das wird dem Betroffenen nur bedingt helfen, kann er zwar seinen Internetauftritt „glätten", kaum aber sonstige alte Datenspuren beseitigen. Arbeitgeberrecherchen in sozialen Kommunikations-Netzwerken werden nun in § 32 VI 3 RegE ausdrücklich untersagt, was gemäß § 32c I Nr. 3 RegE auch für die Zeit nach Begründung des Beschäftigungsverhältnisses gilt. Das ist zwar eine begrüßenswerte Klarstellung im Vergleich zur derzeitigen Rechtslage, die aber Beschäftigte noch nicht ausreichend schützt. Zum einen wird es einem Bewerber nahezu unmöglich sein, eine für ihn nachteilige, unzulässige Recherche in sozialen Netzwerken nachzuweisen. Hier wäre an eine Beweiserleichterung, ähnlich wie in § 22 AGG zu denken. Zum anderen müsste nicht nur für diesen Fall, sondern generell bei unzulässig erhobenen Beschäftigtendaten ein Verwertungsverbot für diese Daten in eine gesetzliche Regelung aufgenommen werden.[31]

2. Gesundheitsuntersuchungen

Neu im deutschen Arbeitsrecht – und in der Wirkung verschlechternd für die Arbeitnehmer – wird in § 32c III RegE die Möglichkeit des Arbeitgebers eingeführt, ärztliche Untersuchungen und Eignungstests *während* des Beschäftigungsverhältnisses zu veranlassen. Bisher gibt es eine so generelle Befugnis nicht, sondern nur die vom Gesetz festgelegten arbeitsmedizinischen Untersuchungen durch unabhängige Stellen. Der Zweck der Untersuchung müssen laut Entwurf Zweifel an der fortdauernden Eignung des Beschäftigten oder ein beabsichtigter Tätigkeitswechsel sein, beides Gründe, deren Geltendmachung keiner hohen Hürden bedarf, sodass die Gefahr groß ist, dass auf diesem neuen Wege unliebsame oder leistungsschwächere Beschäftigte unter Druck gesetzt werden können. Nicht einmal eine Dokumentationspflicht für die Anordnungsgründe sieht der Entwurf vor. Ungeklärt ist, was geschieht, wenn der Beschäftigte den Test oder die Untersuchung verweigert. Anders als § 32a

[30] *Forst*, NZA 2010, 427, 428 f.
[31] So auch das BAG in: BAG 23.4.2009 – 6 AZR 189/08, NZA 2009, 974 (rechtswidriges Abhören von Telefongesprächen).

für die Situation vor der Einstellung, sieht § 32c nicht einmal ein Einwilligungserfordernis des Beschäftigten vor. Für Eignungstests vor wie nach der Einstellung höchst problematisch ist der Umstand, dass diese Tests nur dann nach wissenschaftlich anerkannten Methoden durchzuführen sind, „sofern solche bestehen“ (§ 32a II3). Das scheint zu bedeuten, dass ansonsten Tests nach laienhaften Kriterien durchgeführt werden dürfen.

3. Aufdeckung und Verhinderung von Straftaten und Pflichtverletzungen

a) Videoüberwachung

Die noch im Referentenentwurf enthaltene Regelung zur Zulässigkeit heimlicher Videoüberwachung von Beschäftigten (§ 32f II RefE) wurde zwar gestrichen. In der Begründung zum RegE heißt es nun, die heimliche Videoüberwachung sei unzulässig.[32] Aus dem Wortlaut von § 32e IV RegE ergibt sich das aber nicht ohne weiteres. In den dort angeführten zeitlichen Grenzen – planmäßige verdeckte Beobachtung über 24 Stunden ohne Unterbrechung oder an mehr als vier Tagen – bleibt die heimliche Videoüberwachung offenbar zulässig. Hier bedarf es einer Klarstellung, wenn das in der Begründung angegebene Ziel – Verbot der heimlichen Videoüberwachung – tatsächlich gewollt ist.

Offene Videoüberwachung ist für nicht öffentlich zugängliche Betriebsstätten allerdings in § 32f I RegE ausdrücklich erlaubt. Für die offene Videoüberwachung öffentlich zugänglicher Räume (z.B. Kassenbereiche) soll laut RegE-Begründung auch weiterhin § 6b BDSG gelten.[33] Die Video-Überwachung in nicht öffentlich zugänglichen Betriebsstätten wird zwar in § 32f I RegE an sieben abschließend geregelte Zwecke gebunden, die aber alle, bis auf einen (Sicherheit des Beschäftigten) im Interesse des Arbeitgebers liegen. Im Vergleich zum Referentenentwurf ist mit Nr. 7 die Qualitätskontrolle als Überwachungsgrund dazu gekommen. Dieser Zweck wie auch Nr. 3 (Schutz des Eigentums), Nr. 2 (Wahrnehmung des Hausrechts) oder Nr. 6 (Abwehr von Gefahren für die Sicherheit des Betriebes), ist derart weit, dass eine offene

[32] RegE, Begründung, S. 19 (zu Abs. 4).
[33] RegE, Begründung, S. 20 (zu Abs. 1).

Videoüberwachung so gut wie immer in Betracht kommen wird. Das hat schon das BAG ausgeschlossen. Zwar dürfen die Betriebsparteien grundsätzlich Videoüberwachung einführen. Die muss aber verhältnismäßig sein, wobei es insbesondere auf die Intensität des Eingriffs ankommt. Eine verdachtsunabhängige Totalüberwachung ist danach unwirksam.[34] Der Umstand, dass der Arbeitgeber die Videoüberwachung nach dem Entwurf „durch geeignete Maßnahmen erkennbar machen muss“ schützt die Betroffenen nicht vor Dauerüberwachung, die, gerade wenn sie offensichtlich ist, mit besonders hohem Leistungsdruck einhergeht. Selbst die Regelung über die Einschränkung der Überwachung für private Rückzugsräume in § 32f II RegE ist nicht eindeutig, denn laut Begründung sollen z.B. Raucherzimmer nicht darunter fallen.[35]

Ganz fehlen klare Regelungen zur Einschränkung des Einsatzes von Detektiven (wie bei Lidl praktiziert) und von Systemen zur Mitteilung von Korruptionsverdächtigen durch Beschäftigte (internes Whistleblowing). Einen Anhaltspunkt enthält nur § 32d IV RegE, wonach die Übermittlung von Beschäftigtendaten an Dritte – etwa Detekteien - einer auf das Beschäftigungsverhältnis beschränkten Zweckbindung unterliegt. Damit ist aber nicht gesagt, unter welchen Voraussetzungen die Detektive selbst zur Überwachung von Beschäftigten überhaupt tätig werden dürfen.

b) Überwachung der Telekommunikationsmedien

Bei der Überwachung der vom Arbeitnehmer genutzten Telekommunikationsmedien durch die Arbeitgeber ergeben sich die größten Probleme daraus, dass dienstliche und private Kommunikation über dieselben Kommunikationsmedien erfolgen. Besonders heikel ist die Überwachung der gestatteten oder geduldeten privaten Nutzung. Hier führen bislang die Grundsätze der Rechtsprechung zu den allgemeinen Regeln des BDSG sowie zu § 88 TKG dazu, dass bei Privatnutzung Verbindungsdaten nur in engen Grenzen (etwa zu Abrechnungszwecken) und Inhaltsdaten nur ganz ausnahmsweise (z.B. bei konkretem Verdacht auf Straftaten oder Pflichtverstöße) erhoben werden dürfen. Die Unterscheidung zwischen dienstlicher und privater Nutzung greift der Entwurf in dem ausführlichen § 32i zwar auf, stellt aber eine Verschlechterung der derzeitigen Lage dar, denn der RegE enthält nahezu keine Einschränkung

[34] Vgl. BAG, Beschl. v. 26.8.2008 – 1 ABR 16/07, NZA 2008, 1187; BAG, Beschl. v. 29.6.2004 – 1 ABR 21/03, NZA 2004, 1278.
[35] RegE, Begründung, S. 21 (zu Abs. 2).

für die Kontrollbefugnisse des Arbeitgebers bei der erlaubten oder geduldeten privaten Nutzung von Telekommunikationsdiensten durch die Beschäftigten. Gemäß § 32 i IV 2 RegE soll die Erhebung, Nutzung und Verarbeitung privater Daten und Inhalte zulässig sein, wenn es „zur Durchführung des ordnungsgemäßen Dienst- oder Geschäftsverkehrs unerlässlich ist und (der Arbeitgeber) den Beschäftigten hierauf schriftlich hingewiesen hat". § 32 i IV 2 RegE ermächtigt damit den Arbeitgeber, im Grunde jede private Kommunikation, inklusive der Inhalte zu kontrollieren, wenn er das für unerlässlich hält. Das ist ein Verstoß gegen das Recht auf informationelle Selbstbestimmung, denn an privater Kommunikation hat der Arbeitgeber i.d.R. kein berechtigtes Interesse und bei einem konkreten Verdacht auf eine Straftat oder schwere Pflichtverletzung gilt ohnehin § 32e RegE.

Es dürfte wegen dieser Lücke die bisherige Rechtslage weiter gelten und damit auch der Streit, ob das TKG überhaupt anwendbar ist.[36] In der Entwurfsbegründung geht die Regierung aber davon aus, dass das Fernmeldegeheimnis in § 88 TKG ohnehin nicht mehr eingreift, wenn der Übermittlungsvorgang abgeschlossen ist. Dann kann sich der Arbeitgeber für Mails auf dem Arbeitsplatzcomputer des Beschäftigten auf §§ 32c, d RegE stützten[37] und die Mail-Daten erheben, verarbeiten und nutzen, wenn die Erhebung für die Durchführung, Beendigung oder Abwicklung des Beschäftigungsverhältnisses erforderlich ist.

c) Datenscreenings

Bislang war die „Rasterfahndung" im Betrieb nicht klar geregelt. Jetzt soll mit § 32d III RegE die Befugnis dazu geschaffen und die Beschäftigten erst nachträglich über Inhalt, Umfang und Zweck unterrichtet werden. Automatisierte Datenscreenings ohne konkreten Verdacht und ohne Wissen der Beschäftigten, wie bei der Bahn praktiziert, werden durch den Entwurf nicht etwa verboten, aber in der zulässigen technischen Ausgestaltung begrenzt.

Auch nach derzeitiger Rechtslage war das Vorgehen der Bahn allerdings schon unzulässig. Das ergibt sich nicht zuletzt aus dem noch jungen Grundrecht auf Vertraulichkeit und Integrität in informationstechnischen Systemen, das das BVerfG in seiner Entscheidung zur „Online-Überwachung" anerkannt hat[38] und das heimliche Zugriffe

[36] Ablehnend z.B. *Löwisch*, DB 2009, 2782.
[37] RegE, Begründung, S. 26 f. (Abs. 4).
[38] BVerfG 27.2.2008 – 1 BvR 370/07 und 595/07, AuR 2008, 152.

auf personenbezogene Daten in vernetzten IT-Systemen zu reinen Präventionszwecken nicht erlaubt, sondern nur, wenn eine konkrete Gefahr für ein überragend wichtiges Rechtsgut besteht.[39]

Nach § 32d III RegE darf der Abgleich von Beschäftigtendaten mit vom Arbeitgeber geführten Dateien zur Aufdeckung von Straftaten, wie Untreue, Bestechung oder Bestechlichkeit sowie anderer schwerwiegender Pflichtverletzungen durchgeführt werden, wenn auch in anonymisierter und pseudonymisierter Form. Das ist zwar ein gewisser Schutz für die Beschäftigten, aber trotzdem problematisch, weil nicht klar geregelt ist, wer unter welchen Voraussetzungen wann die Daten entschlüsseln darf. In § 32d III heißt es nur: „Ergibt sich ein Verdachtsfall, dürfen die Daten personalisiert werden“. Der Arbeitgeber hat laut Gesetzestext lediglich die Umstände, die ihn zum Abgleich veranlassen, zu dokumentieren. Über die Bedingungen der Personalisierung enthält auch die Begründung nichts. Wer stellt also den Verdachtsfall fest? Hier wäre eine betriebliche Kontrollinstanz erforderlich – der Betriebsrat oder zumindest der betriebliche Datenschutzbeauftragte.

Insgesamt ist es erstaunlich, dass mit § 32d III RegE überhaupt anlasslose, verdachtsfreie Abgleiche ermöglicht werden sollen, denn es waren doch gerade derartige Massensceenings, u.a. bei der Bahn AG, die den vorliegenden Regierungsentwurf zum Beschäftigtendatenschutz veranlasst haben. Klargestellt wird jetzt, dass Massendatenabgleiche zulässig sind.[40]

4. Neuer Rechtsbehelf/Kontrolle

Problematisch ist der neue Rechtsbehelf für den Arbeitnehmer in § 32 l, Abs. 4 RegE. Zwar ist es zu begrüßen, dass dem Betroffenen ein individuelles Beschwerderecht gegenüber der zuständigen Datenschutzbehörde eingeräumt wird. Kontraproduktiv ist aber die Verpflichtung, zunächst den Arbeitgeber einzuschalten. Es darf bezweifelt werden, ob hier § 612a BGB den Arbeitnehmer schützt.[41] Außerdem bleibt offen, ob der Arbeitnehmer seinen Arbeitsvertrag verletzt, wenn er sich doch unmittelbar mit der Aufsichtsbehörde in Verbindung setzt, etwa wenn der Datenschutz-

[39] Zur Wirkung dieses Grundrechts im Arbeitsrecht vgl. *Wedde*, Das Grundrecht auf Vertraulichkeit und Integrität in informationstechnischen Systemen aus arbeitsrechtlicher Sicht, AuR 2009, 373.
[40] So auch *Tinnefeld/Petri/Brink*, Aktuelle Fragen um ein Beschäftigtendatenschutzgesetz, MMR 2010, 727, 731.
[41] So auch *Forst*, a.a.O.

verstoß so gravierend war, dass der Arbeitnehmer mit Abhilfe durch den Arbeitgeber nicht rechnen kann und/oder Nachteile befürchten muss. Darüber hinaus verlangt Art. 28 IV der EU-Datenschutzrichtlinie 95/46, dass jedermann das Recht einzuräumen ist, sich beim Verdacht auf Verstöße gegen Datenschutzbestimmungen direkt an unabhängige Kontrollbehörden zu wenden.

Schließlich steht die in Deutschland zuständige Aufsichtsbehörde seit einem Urteil des EuGH vom März 2010 selbst auf rechtlich problematischen Füßen. Der EuGH hat das Kontrollsystem in Deutschland wegen der mangelnden Unabhängigkeit der Datenschutzkontrolleure im privaten Bereich für europarechtswidrig gehalten.[42] Damit hat das Gericht das zentrale Problem der Datenschutzkontrolle in Deutschland mit der Trennung in Landesdatenschutzbeauftrage und den Bundesdatenschutzbeauftragen, die für den öffentlichen Bereich zuständig sind und Kontrolle des privaten Bereichs, also auch der Unternehmen, durch Verwaltungsbehörden aufgegriffen. Selbst wenn die materielle Datenschutzrechtslage in befriedigender Weise den Schutzbedürfnissen von Arbeitnehmern entspräche, bliebe es bei dem Problem der mangelnden Unabhängigkeit der Datenschutzbehörden im privaten Bereich. Die Bundesregierung sieht offenbar keinen Handlungsbedarf, was angesichts der klaren Aussagen aus Luxemburg erstaunt.

IV. Rolle des Betriebsrats

Der RegE kann zu einer Schwächung des Betriebsrats auf dem Gebiet des Arbeitnehmerdatenschutzes führen, da es bislang zahlreiche Betriebsvereinbarungen zu § 87 I Nr. 6 BetrVG gibt. Zwar bleiben gemäß § 32 l, Abs. 3 RegE die Rechte der Interessenvertretungen der Beschäftigten unberührt und stellt § 4 I 2 RegE klar, dass Betriebs- und Dienstvereinbarungen Rechtsvorschriften i.S.v. § 4 I 1, 2. Alt. BDSG sind und folglich eine Datenerhebung, -nutzung und –verarbeitung rechtfertigen können. Die bisherige Sichtweise der Rechtsprechung, wonach durch Betriebsvereinbarungen Arbeitnehmerdatenschutz auch unterhalb der Gesetze geregelt werden darf,[43] ist mit § 32 l, Abs. 5 RegE aber nicht mehr vereinbar. Danach darf von den Vorschriften zum Beschäftigtendatenschutz nicht zu Ungunsten der Beschäftigten

[42] EuGH, Urt. v. 9.3.2010 – C-518/07 (Kommission/Deutschland), NJW 2010, 1265.
[43] BAG, Beschl. v. 25.5.1986 – 1 ABR 48/84, NJW 1987, 774, 777.

abgewichen werden. Das ist auch schon deshalb sachgerecht, weil anderenfalls Beschäftigte in Betrieben mit Betriebsrat ggfs. schlechter geschützt wären als Beschäftigte in betriebsratslosen Betrieben. Allerdings ist die Begründung zum RegE in diesem Punkt nicht widerspruchsfrei. Zu § 4 I 2 RegE heißt es, der neue Satz 2 solle „gegenüber der jetzigen, durch die Rechtsprechung geprägten Rechtslage“ weder eine Einschränkung noch eine Erweiterung der Möglichkeiten und Grenzen sein, durch Betriebs- oder Dienstvereinbarungen abweichende Vereinbarungen zu treffen.[44] Dagegen heißt es zu § 32 l, Abs. 5, dass „solche Vereinbarungen (BV) zulässig sind, soweit sie von den gesetzlichen Regelungen nicht zum Nachteil der Beschäftigten abweichen“[45]. Der Betriebsrat bleibt dennoch für den Arbeitnehmerdatenschutz wichtig, etwa für die Ausfüllung der zahlreichen unbestimmten Rechtsbegriffe im RegE (insbesondere: Erforderlichkeit, Verhältnismäßigkeit) durch Betriebsvereinbarung. Das hatte offenbar auch der Gesetzgeber im Sinn, denn in der Begründung zum RegE heißt es: „Damit wird nicht ausgeschlossen, dass Tarifverträge, Betriebs- oder Dienstvereinbarungen die gesetzlichen Regelungen konkretisieren oder Alternativen gestalten, um den jeweiligen betrieblichen Besonderheiten Rechnung zu tragen“.[46]

IV. **Schlussfolgerungen**

Die oben genannten drei Datenskandalfälle wären durch die Neuregelungen im RegE, Rechtstreue der Handelnden vorausgesetzt, nur partiell verhindert worden:

- Zur reinen Prävention sind zwar verdeckte Datenscreenings nur noch anonymisiert und pseudonymisiert möglich. Die Daten können aber im Verdachtsfall vom Arbeitgeber entschlüsselt werden. Der Bahn-Fall wäre also zulässig gewesen, wenn die Rasterfahndung im Betrieb zunächst anonymisiert durchgeführt worden wäre.
- Die Führung geheimer Krankenakten ist schon nach gegenwärtiger Rechtslage unzulässig (Lidl-Fall).

[44] RegE, Begründung, S. 7.
[45] A.a.O., S. 29 (zu Abs. 5).
[46] A.a.O.

- Zur zweiten Facette der Datenschutzverstöße bei Lidl – die Einschaltung externer Detekteien - regelt der Entwurf nichts.
- Ob der Telekom-Fall mit der Neuregelung verhindert worden wäre, ist zweifelhaft, da die Kontrolle der Telekommunikation der Beschäftigten auch bei gestatteter Privatnutzung zulässig sein soll, wenn sie „zur Durchführung des ordnungsgemäßen Dienst- und Geschäftsverkehrs unerlässlich“ ist. Neu ist, dass dem Beschäftigten ein schriftlicher Hinweis erteilt werden muss.

Aber selbst wenn alle Skandalfälle mit dem Entwurf entschärft werden könnten, bliebe er ein verfehlter Versuch, „Arbeitnehmer umfassend zu schützen“, auch wenn der Entwurf den Anspruch erhebt, nicht nur diese wenigen, wenn auch spektakulären, konkreten Fälle einer Lösung zuzuführen, sondern den Beschäftigtendatenschutz insgesamt zu regeln. Das gelingt nicht, weil große Teile des Entwurfs Kataloge für Datenerhebungsbefugnisse des Arbeitgebers sind. Z.T. werden sogar neue Befugnisse geschaffen (z.B. Erhebung von Gesundheitsdaten während des Beschäftigungsverhältnisses), wichtige Bereiche, die bislang zumindest durch Rechtsprechung, wenn auch nicht eindeutig, so doch im Wesentlichen arbeitnehmerschützend geregelt sind (Umgang mit privaten Telekommunikationsdaten bei gestatteter oder geduldetet Privatnutzung) nun arbeitgeberfreundlich geregelt, etliches im Unklaren gelassen (Verhältnis zum AGG, insbesondere zu dessen Rechtsfolgen) oder Wichtiges nicht angesprochen (Verwertungsverbot, Rechtsfolge bei unzulässiger Arbeitgeberfrage im Bewerbungsverfahren, Frage nach der Schwangerschaft).

Zusammengefasst gibt es Änderungs- bzw. Regelungsbedarf vor allem zu Folgendem:

1. Die Einfügung von zahlreichen Einzelfallregelungen ins BDSG bleibt lückenhaft und macht den Arbeitnehmerdatenschutz intransparent und schwer les- und anwendbar. Ein eigenes Beschäftigtendatenschutzgesetz könnte diesen Defiziten wesentlich besser abhelfen.
2. Wegen der kasuistischen Regelungen ist baldiger Änderungsbedarf absehbar (Stichwort: Biometrie).

3. Regelungsbedarf besteht allein im Hinblick auf die im RegE angesprochenen Bereiche nach wie vor zu
    - einer Definition des Begriffes *compliance*,
    - dem Schutz der Arbeitnehmerdaten bei erlaubter oder gestatteter privater Internet- und Telefonnutzung,
    - einem Verwertungsverbot für zu Unrecht erhobene Daten,
    - einer Beweiserleichterung für den Beschäftigten bei (unzulässigen) Internetrecherchen des Arbeitgebers.
4. Klarstellungen sind erforderlich bei
    - den Rechtsfolgen bei Verstößen, insbesondere beim Fragerecht des Arbeitgebers,
    - der Aufnahme des Verbotes der Frage nach der Schwangerschaft in den Katalog der unzulässigen Fragen vor der Einstellung,
    - der heimlichen Videoüberwachung, die nur nach der Begründung zum RegE, nicht aber nach dem Wortlaut des § 32e IV eindeutig verboten ist.
5. Änderungen sind notwendig für
    - die Einschränkung der Erhebung von Gesundheitsdaten auf die gesetzlich geregelten Fälle,
    - der Ausschluss von nicht wissenschaftlich anerkannten Methoden für Eignungstests,
    - die Einschränkung der offenen Videoüberwachung auf klar abgegrenzte Fälle, um eine Dauerüberwachung der Beschäftigten zu verhindern.

Insgesamt müssen Regelungen zum Beschäftigtendatenschutz erkennen lassen, dass das verfassungsmäßig gewährleistete Recht auf informationelle Selbstbestimmung des Beschäftigten der Leitgedanke der Gesetzgebung ist. Berechtigte Informationsinteressen des Arbeitgebers müssen daneben an klare, abgrenzbare und vorhersehbare Kriterien gebunden werden. Die pauschale Rechtfertigung von Informationsansprüchen mit dem undefinierten und daher nahezu beliebig ausdehnbaren Begriff der *compliance* verstößt gegen Art. 2 I 1 GG.