Prof. Dr. Gerrit Hornung

Lehrstuhl für Öffentliches Recht, Informationstechnologierecht und Rechtsinformatik

UNIVERSITÄT PASSAU
Juristische Fakultät

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)252 D

Telefon Prof. Dr. Gerrit Hornung
0851 509-2380

Telefax 0851 509-2382

e-mail gerrit.hornung
@uni-passau.de

Datum 18. Mai 2011

Stellungnahme

zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages zum Gesetzentwurf der Bundesregierung (Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes, BT-Drs. 17/4230), zu weiteren Entwürfen der Fraktionen der SPD (Entwurf eines Gesetzes zum Datenschutz im Beschäftigungsverhältnis, BT-DRs. 17/69) und von BÜNDNIS 90/DIE GRÜNEN (Entwurf eines Gesetzes zur Verbesserung des Schutzes personenbezogener Daten der Beschäftigten in der Privatwirtschaft und bei öffentlichen Stellen, BT-Drs. 17/4852) sowie zweier Anträge zum Beschäftigtendatenschutz (BT-Drs. 17/121 und 17/779)

1 Vorbemerkung

Das grundsätzliche Anliegen des vorliegenden Gesetzesentwurfs der Bundesregierung und der alternativ vorgelegten Entwürfe der Fraktionen der SPD und von BÜNDNIS 90/DIE GRÜNEN ist zu begrüßen. Die gegenwärtige Rechtslage wird maßgeblich durch die arbeitsgerichtliche Rechtsprechung bestimmt, die diese Aufgabe zwar insgesamt sachgerecht bewältigt hat, naturgemäß aber immer nur punktuellen und nachlaufenden Einfluss auf die Rechtsentwicklung nehmen konnte. Der Gesetzgeber sollte deshalb die Gelegenheit nicht verstreichen lassen, Leitlinien für die betriebliche Praxis vorzugeben, die zumindest einige grundlegende Rechtsfragen der Datenverarbeitung in diesem wichtigen Lebensbereich entscheiden.

Die vorgelegten Gesetzentwürfe sind komplex und umfangreich. Im Rahmen dieser Stellungnahme ist es daher nicht möglich, zu allen durch die Entwürfe aufgeworfenen rechtlichen und rechtspolitischen Fragen Stellung zu beziehen. Die folgenden Ausführungen

beschränken sich deshalb auf übergreifende Gesichtspunkte und Anmerkungen zu besonders wichtigen und kontroversen Fragen.

2 Grundsätzliche Gesichtspunkte

Aus grundsätzlicher Sicht sind drei Gesichtspunkte anzumerken.

Erstens fällt das Reformvorhaben in eine Zeit, in der auf europäischer Ebene eine Reform der Datenschutzrichtlinie[1] angestrebt wird (die Kommission hat am 4. November 2010 eine Mitteilung über ein „Gesamtkonzept für den Datenschutz in der Europäischen Union“ vorgelegt,[2] die anschließende Konsultation befindet sich derzeit in der Auswertung). Das relativiert zum einen die Frage der Richtlinienkonformität des nationalen Vorhabens, die im Folgenden bei einigen Punkten relevant wird. Zum anderen verbleibt insgesamt das Risiko, für den Fall weitgehender Neuerungen auf europäischer Ebene das vorliegende Reformvorhaben – und andere, die in den Bereich des Datenschutzrechts fallen – zeitnah überarbeiten zu müssen.

Zweitens weisen die Entwürfe (der Regierungsentwurf noch mehr als die alternativ vorgelegten Entwürfe) eine erhebliche Komplexität auf, die durch Wiederholungen allgemeiner Prinzipien und eine unübersichtliche Verweisungstechnik bedingt ist. Allgemeine Grundsätze des Datenschutzrechts wie das Erforderlichkeitsprinzip werden in einer Vielzahl der Vorschriften explizit normiert, anstatt generalklauselartig vor die Klammer gezogen zu werden.

Drittens enthält der Entwurf an vielen Stellen offene Rechtsbegriffe und Verhältnismäßigkeitsklauseln, was sich angesichts der Unterschiede in der betrieblichen Praxis nicht vermeiden lässt. Gleichzeitig gilt es jedoch zu bedenken, dass die Entscheidung über die Zulässigkeit konkreter Datenverwendungen damit auch weiterhin maßgeblich bei den Gerichten liegen wird.

3 Einzelfragen

Aus dem Regelungsbereich der Entwürfe werden im Anschluss die folgenden besonders wichtigen Problemkomplexe behandelt:

- Abweichende Regelungen durch Betriebsvereinbarungen
- Ausschluss und Möglichkeit der Einwilligung

---

[1] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Abl. EG Nr. L 281 vom 23. November 1995 S. 31.

[2] KOM(2010) 609 endgültig.

- Rechtsschutz (Beschwerderecht, Whistleblower, Verbandsklagerecht)
- Konzerndatenschutz
- Bewerberauswahl und soziale Netzwerke
- Organisatorische und technische Aspekte des Datenschutzes
- Regelungen zu Überwachung und Kontrolle im Betrieb (Compliance, Videoüberwachung, Biometrie, Telekommunikationsüberwachung)

3.1 Abweichende Regelungen in Betriebsvereinbarungen

Das Bundesarbeitsgericht geht in einer Entscheidung aus dem Jahre 1986 davon aus, dass durch Betriebsvereinbarungen zuungunsten der Beschäftigten von Regelungen des Datenschutzrechts abgewichen werden darf.[3] Diese Ansicht ist in Teilen der Literatur auf heftige Kritik gestoßen.[4] Dort hat sich weithin die Auffassung durchgesetzt, dass Betriebsvereinbarungen zwar die – notwendige und verdienstvolle – Aufgabe der Präzisierung und Konkretisierung allgemeiner datenschutzrechtlicher Anforderungen auf die jeweilige betriebliche Praxis leisten können, Arbeitgeber und Betriebsrat aber kein Mandat haben, gesetzlich vorgegebene Datenschutzrechte einzuschränken, die weithin grundrechtlich abgesicherten Persönlichkeitsschutz beinhalten. Diese Richtung schlägt § 32l Abs. 4 BDSG-E ein, der es generell untersagt, von den geplanten Neuregelungen zulasten der Beschäftigen abzuweichen. Entgegen der teilweise vorgetragenen Kritik in der Literatur sollte an dieser Vorschrift festgehalten werden. Dass die Abgrenzung des Anwendungsbereichs (Konkretisierung versus „Abweichung zuungunsten der Beschäftigten“) im Einzelfall problematisch sein kann,[5] ist kein Gegenargument, da sich hieran auch durch eine andere Formulierung des Anwendungsbereichs nichts ändern würde.

Allerdings kann nicht übersehen werden, dass Betriebsvereinbarungen bei dieser – auch nach dem Entwurf gewollten – Konkretisierungsleistung in Grenzbereichen operieren, weil sich jedes betriebliche Umfeld und jede Datenverarbeitung anders darstellen kann und deshalb die Konkretisierung datenschutzrechtlicher Prinzipien betriebsbezogen unterschiedlich ausfallen wird. Es ist in jedem Fall zu vermeiden, dass mit der Regelung „in Einzelfällen betriebsnahe, sachgerechte Lösungen ausgeschlossen werden“.[6]

---

3 BAG NJW 1987, 674, 677.

4 *Walz*, in: Simitis, BDSG, 6. Auflage 2006, § 4 Rn. 17; *Gola/Wronka*, Handbuch Arbeitnehmerdatenschutz, 5. Auflage 2009, Rn. 246; *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Auflage 2010, § 4 Rn. 2; a.A. *Wank*, in: Erfurter Kommentar zum Arbeitsrecht, 9. Auflage 2009, § 4 Rn. 3; *Thüsing*, Arbeitnehmerdatenschutz und Compliance, 2010, Rn. 105.

5 Darauf weist *Kort*, MMR 2011, 294, 298 f. hin; kritisch auch *Beckschulze/Natzel*, BB 2010, 2368 f.; *Thüsing*, NZA 2011, 16, 18.

6 So *Tinnefeld/Petri/Brink*, MMR 2010, 727, 729, die den Vorschlag im Grundsatz befürworten.

Gesetzeswortlaut oder Begründung sollten deshalb klarstellen, dass die Präzisierung ausfüllungs- und wertungsbedürftiger Begriffe wie „private Lebensgestaltung“, „schutzwürdige Interessen der Beschäftigten“ oder „betriebliche Gründe“ zulässig ist. Auch auf Basis der aktuellen Fassung des Regierungsentwurfs wäre es beispielsweise zulässig, die näheren Umstände des Einsatzes biometrischer Verfahren im Betrieb durch eine Betriebsvereinbarung zu regeln,[7] weil § 32h BDSG-E insoweit nur sehr allgemeine Vorgaben macht.[8] Die Grundüberlegung der Regelung bleibt aber zutreffend, da durch sie der Gefahr entgegengewirkt werden kann, dass grundrechtliche Schutzpositionen in Verhandlungen zwischen Arbeitgebern und Betriebsräten im Rahmen von Gesamteinigungen zu marginalen Verhandlungsposten werden.

3.2 Ausschluss der Einwilligung

Der weitgehende Ausschluss der Einwilligung in § 32l Abs. 1 BDSG-E[9] wirft zwei Fragen auf: Die nach der europarechtlichen Zulässigkeit und die nach der sachlichen Angemessenheit. Vorwegzuschicken ist, dass die praktische Bedeutung einer echten (das heißt freiwilligen und informierten) Einwilligung in der betrieblichen Praxis eingeschränkt ist. Zum einen wird es vielfach an der Freiwilligkeit fehlen, weil die Verweigerung der Einwilligung zu erheblichen Nachteilen für Beschäftige führen kann. Zum anderen erfordern betriebliche Abläufe im Allgemeinen ein hohes Maß an Einheitlichkeit, das nicht gewährleistet werden kann, wenn einzelne Beschäftigte die Einwilligung verweigern. Bei einer tatsächlich freiwilligen Entscheidung ist dies aber praktisch nie auszuschließen.

Zweifel an der Europarechtskonformität von § 32l Abs. 1 BDSG-E bestehen deshalb, weil Art. 7 lit. a der Datenschutzrichtlinie die Einwilligung als eigenständigen Erlaubnistatbestand nennt. Dies allein reicht −entgegen anderslautender Stimmen[10] − indes noch nicht aus, um die vorgeschlagene Regelung richtlinienwidrig werden zu lassen. Zwar hat der Europäische Gerichtshof der Datenschutzrichtlinie den Charakter einer Vollharmonisierung zugesprochen.[11] Das bedeutet aber lediglich, dass den nationalen Gesetzgebern nur die Spielräume zukommen, die die Richtlinie selbst ihnen gibt. In gewissen Grenzen sind sie daher befugt, Anforderungen zu typisieren, die von der Richtlinie selbst gesetzt werden.

---

7 S. beispielsweise die Orientierungshilfe für eine Betriebsvereinbarung beim Einsatz biometrischer Systeme des TeleTrusT e.V., http://www.teletrust.de/uploads/media/TeleTrusT-AG_Biometrie_BetriebsV_1.2.pdf.

8 Dazu noch unten 3.7.3.

9 Der Entwurf von BÜNDNIS 90/DIE GRÜNEN enthält eine vergleichbare Regelung in § 4 Abs. 1 Satz 1.

10 Mit diesem Argument *Forst*, RDV 2010, 150; *ders*., NZA 2010, 1043, 1044; *Thüsing*, RDV 2010, 147,148 f.; *ders*., NZA 2011, 16, 18 f.; *Rasmussen-Bonn/Raif*, GWR 2011, 80; ähnlich *Kort*, MMR 2011, 294, 299; für die Zulässigkeit *Tinnefeld/Petri/Brink*, MMR 2010, 727, 729.

11 EuGH, Urteil vom 6.11.2003 - Rs. C-101/01 (Lindqvist/Schweden), MMR 2004, 95, 98 f.

Hierzu gehört auch die Freiwilligkeit der Einwilligung, an die die Datenschutzrichtlinie hohe Anforderungen stellt. Demzufolge muss es zulässig sein, wenn nationale Gesetzgeber in Konkretisierung des durch die Richtlinie vorgeschriebenen „hohen Schutzniveaus“[12] in bestimmten Lebensbereichen, in denen von einer Freiwilligkeit typischerweise nicht ausgegangen werden kann, die Möglichkeit einer Einwilligung generell ausschließen. Eine solche Situation ist im Arbeitsverhältnis weithin gegeben.

Aus den vorstehenden Erwägungen folgt allerdings auch, dass der nationale Gesetzgeber dort keine Einschränkungen machen darf, wo typischerweise gerade keine Unfreiwilligkeit vorliegt. Gemessen an diesem Kriterium erscheinen die ausdrücklich zugelassenen Einwilligungstatbestände des Entwurfs[13] zu eng. Dort, wo Beschäftigte gerade keinem starken Druck ausgesetzt sind, spricht auch kein sachlicher Grund für einen Ausschluss der Einwilligung. In der Literatur finden sich denn auch Beispiele wie das Angebot zum Abschluss einer betrieblichen Altersvorsorge[14] oder die Internetpräsentation von Wissenschaftlern und ihren Arbeitsergebnissen,[15] bei denen der Ausschluss der Einwilligung nicht angemessen wäre. Für derartige Fälle bedarf es einer Generalklausel, die die Einwilligung in bestimmten Fällen zulässt – allerdings nur bei Vorliegen bestimmter Mittel zur Sicherung der Freiwilligkeit. Dies könnte eine Beschränkung auf Fälle sein, in denen Beschäftigte selbst initiativ werden, oder ein freiwilliges Koppelungsverbot seitens des Arbeitgebers.

3.3 Rechtsschutzfragen

Der Regierungsentwurf bedarf hinsichtlich des Komplexes der Rechtsschutzfragen in mehreren Punkten der Überarbeitung.

3.3.1 Beschwerderecht

§ 32l Abs. 4 BDSG-E verlangt von Beschäftigten, sich vor einer Eingabe an die Datenschutzaufsichtsbehörde mit einer Beschwerde an den Arbeitgeber zu wenden. Dies ist eine Verschlechterung der Rechtsposition der Beschäftigten, sachlich nicht zu rechtfertigen und darüber hinaus europarechtswidrig. Es ist nicht zutreffend, dass der Entwurf ein Beschwerderecht neu einführt.[16] Nach aktueller Rechtslage hat jedermann gemäß § 38 Abs. 1 Satz 8 i.V.m. § 21 Satz 1 BDSG das Recht, sich an die Datenschutzaufsichtsbehörde zu wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung

---

12 Erwägungsgrund 10.

13 Die Einwilligung wird in § 32 Absatz 6 Satz 4, § 32a Absatz 1 Satz 2, Absatz 2 Satz 2, § 32b Absatz 3, § 32c Absatz 3, § 32h Absatz 1 Satz 2, § 32i Absatz 2 Satz 1, § 32i Absatz 2 Satz 2 BDSG-E explizit zugelassen.

14 S. *Thüsing*, NZA 2011, 16, 19; kritisch auch *Beckschulze/Natzel*, BB 2010, 2368, 2374.

15 S. bei *Tinnefeld/Petri/Brink* (die die Regelung im Grundsatz befürworten), MMR 2010, 727, 729.

16 So aber *Beckschulze/Natzel*, BB 2010, 2368, 2374

seiner personenbezogenen Daten in seinen Rechten verletzt worden zu sein. Das gilt auch für Beschäftigte.[17]

Inhaltlich ist nicht einzusehen, warum Beschäftige selbst bei schweren Pflichtverletzungen des Arbeitgebers zunächst bei diesem um Abhilfe nachsuchen sollen.[18] In derartigen Fällen besteht das Risiko, dass die Beschäftigten von der Wahrnehmung ihrer datenschutzrechtlich garantierten Betroffenenrechte (die gemäß § 6 Abs. 1 BDSG nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden können) abgeschreckt werden. Europarechtlich sieht Art. 28 Abs. 4 der Datenschutzrichtlinie ein vorheriges internes Beschwerdeverfahren nicht vor, sondern gibt jedermann das Recht, sich zum Schutz der die Person betreffenden Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten an jede Kontrollstelle mit einer Eingabe wenden.[19]

§ 32l Abs. 4 BDSG-E sollte folglich ersatzlos gestrichen werden.

3.3.2 Whistleblower

Der Regierungsentwurf enthält keine ausdrückliche Regelung für „Whistleblower". Das hat zur Folge, dass sich die Einrichtung einer Stelle für anonyme Beschwerden als rechtlich problematisch erweist, da keine Datenerhebungs- und -verarbeitungsbefugnis für die so erhobenen Daten existiert.

Rechtspolitisch wäre eine solche Regelung wünschenswert,[20] auch wenn – oder gerade weil – über den konkreten Inhalt unterschiedliche Auffassungen herrschen. Die Bedeutung hat sich gerade bei den so genannten Datenskandalen der letzten Jahre gezeigt, die zum Teil durch Whistleblower aufgedeckt wurden.[21] Für die USA sind entsprechende Regelungen nach dem Sarbanes-Oxley Act vorgeschrieben. Daneben hat auch die Art. 29-Gruppe ausdrücklich festgestellt, dass Whistleblower-Regelungen mit der Datenschutzrichtlinie vereinbar sind.[22] Eine entsprechende Norm sollte dabei auch diejenigen Daten erfassen, die im Betrieb über Dritte (insbesondere Kunden) verarbeitet werden.

---

17 S. *Petri*, in: Simitis (Fn. 4), § 38 Rn 3 m.w.N.; *Tinnefeld/Petri/Brink*, MMR 2010, 727, 735.

18 Kritisch auch *Wybitul*, Handbuch Datenschutz im Unternehmen, 2011, 523.

19 S.a. Stellungnahme der Neuen Richtervereinigung (abrufbar unter http://www.nrv-net.de/downloads_stellung/89.pdf), S. 9; Stellungnahme des ULD Schleswig-Holstein (abrufbar unter https://www.datenschutzzentrum.de/arbeitnehmer/20101012-stellungnahme.html).

20 Ebenso z.B. *Gola*, RDV 2010, 97, 99; *Tinnefeld/Petri/Brink*, MMR 2010, 727, 735; *Kort*, MMR 2011, 294, 296 f.; § 24 des Entwurfs von BÜNDNIS 90/DIE GRÜNEN enthält einen entsprechenden Vorschlag.

21 S. *Tinnefeld/Petri/Brink*, MMR 2010, 727, 728.

22 S. Art. 29-Gruppe, WP 117, Stellungnahme 1/2006 zur Anwendung der EU-Datenschutzvorschriften auf interne Verfahren zur Meldung mutmaßlicher Missstände in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität, abrufbar unter

3.3.3 Verbandsklagerecht

Im Konfliktfall ist das betriebliche Umfeld ein typisches Beispiel eines Machtgefälles, welches das Risiko birgt, dass Betroffene von Rechten, die ihnen zustehen, keinen Gebrauch machen. Selbstverständlich muss dem Einzelnen die subjektive Verfolgung von Rechten erhalten bleiben. Dies wird jedoch kaum je (und in Zukunft noch weniger)[23] zur Durchsetzung des Datenschutzrechts in größeren Zusammenhängen wie betrieblichen Abläufen führen. Hier bedarf es der Unterstützung durch professionelle Institutionen und Organisationen. Dies wird durch die Datenschutzbehörden in Teilen geleistet; diese arbeiten aber weithin an der Kapazitätsgrenze.

Zur Lösung bietet sich ein Rückgriff auf das Verbandsklagerecht an, das etwa im Verbraucher- und Umweltschutzrecht seit vielen Jahren ein anerkanntes Instrument zur kollektiven Wahrnehmung von Interessen ist. Ein derartiges Recht (etwa für Betriebsräte und Gewerkschaften) sollte auch bei Verstößen gegen die Datenschutzvorschriften im Betrieb gesetzlich verankert werden.[24] Zur Absicherung könnte ein Zulassungsverfahren eingeführt werden, in dem – ähnlich wie im Umweltrecht – Nachhaltigkeit, Zielrichtung und Dauerhaftigkeit der Tätigkeit überprüft werden.

3.4 Konzerndatenschutz

Die fehlende Regelung einer Verarbeitungs- und Übermittlungsbefugnis im Konzern und die Frage nach dem Verhältnis zur Auftragsdatenverarbeitung sind zwei der drängendsten Probleme des betrieblichen Datenschutzes, insbesondere weil die binäre Trennung zwischen Auftragsdatenverarbeitung und Funktionsübertragung in weiten Teilen nicht mehr der betrieblichen Wirklichkeit entspricht.

Insofern ist es einerseits zwar misslich, dass der Entwurf hierzu keine Regelung enthält.[25] Anderseits ist jedoch zu bedenken, dass nicht nur Zweifel an der europarechtlichen Zulässigkeit eines derartigen Vorhabens bestehen,[26] sondern die eigentlichen Probleme zudem bei solchen internationalen Konzernen bestehen, denen selbständige Unternehmen mit Sitz außerhalb des Geltungsbereichs der europäischen Datenschutzrichtlinie angehören. Abhilfe kann hier daher wohl nur auf europäischer Ebene geleistet werden.

---

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_de.pdf: Basis ist Art. 7 (f) der Datenschutzrichtlinie.

23 S. perspektivisch *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, 198 f.

24 Vergleichbar dem Entwurf von BÜNDNIS 90/DIE GRÜNEN, § 23.

25 S.a. *Kort*, MMR 2011, 294, 297 f.; aus Perspektive der Aufsichtsbehörden s. den Arbeitsbericht der ad-hoc-Arbeitsgruppe „Konzerninterner Datentransfer“, abrufbar unter http://www.rp-darmstadt.hessen.de/?cid=f8a680608c6fea87bbe406d0cc8eb0d0.

26 Z.B. *Thüsing*, NZA 2011, 16, 19, der allerdings nationale Spielräume bejaht.

Entscheidend gegen eine Regelung spricht im vorliegenden Zusammenhang schließlich, dass es beim Konzerndatenschutz zwar auch, aber nicht nur um die Verwendung von Daten der Beschäftigten geht – betroffen sind vielmehr auch die Daten von Kunden, Vertragspartnern, Behörden und sonstigen Dritten. Dass der Konzerndatenschutz einer Lösung bedarf, steht somit außer Frage, eine entsprechende Regelung sollte aus den genannten Gründen aber nicht gesondert in einem Abschnitt über den Beschäftigtendatenschutz erfolgen.

3.5 Bewerberauswahl und soziale Netzwerke

§ 32 Abs. 6 Satz 2 und Satz 3 BDSG-E bemühen sich um eine sachgerechte Lösung des Problems der sozialen Netzwerke. Die Norm ist aber in mehrfacher Hinsicht zweifelhaft. Soweit sie an schutzwürdige Interessen des Beschäftigten anknüpft, stellt sich das Problem, dass sich das Vorliegen derartiger Interessen jenseits des gesetzlich geregelten Falles der nicht-beruflichen sozialen Netzwerke regelmäßig erst aus der Information ergeben wird, die im Internet verfügbar ist. In diesem Fall hat der Arbeitgeber die relevante Information jedoch bereits zur Kenntnis genommen.

Soweit § 32 Abs. 6 Satz 3 BDSG-E dem Arbeitgeber untersagt, Daten aus privaten sozialen Netzwerken zu erheben, ist die Norm de facto unkontrollierbar[27] und wird deshalb mutmaßlich Placebo bleiben. Ein Effekt könnte höchstens insoweit eintreten, als entsprechende Informationen in gerichtlichen Verfahren nicht verwertet werden dürfen[28] oder Mitarbeiter in Personalabteilungen sich unter Berufung auf die Vorschrift gegen Anweisungen zur Erhebung von Daten aus privaten sozialen Netzwerken zur Wehr setzen können.

Insgesamt sendet § 32 Abs. 6 Satz 3 BDSG-E angesichts seiner fehlenden Durchsetzbarkeit ein falsches Signal an die Betroffenen: Es wird suggeriert, man könnte die Verwendung von Informationen dauerhaft kontrollieren, die sich einmal im Internet befinden. Dies wird zunehmend unrealistisch, und das gilt auch für die vorgeblich geschützten Räume „privater“ sozialer Netzwerke, in denen häufig hunderte von Kontakten Zugriff auf die Daten haben und diese weitergeben können.

3.6 Organisatorische und technische Seiten des Datenschutzes

Der Bereich der organisatorischen und technischen Aspekte des Datenschutzes ist im Regierungsentwurf deutlich zu schwach ausgeprägt. Erwägenswert erscheint der weitere Ausbau folgender Aspekte:

---

[27] Ebenso Stellungnahme des ULD Schleswig-Holstein (Fn. 19).
[28] S. *Raif*, ArbRAktuell 2010, 617.

- Die Dokumentationspflichten, die derzeit lediglich in § 32d Abs. 3 Satz 2, § 32e Abs. 5 Satz 2 und Satz 3 BDSG-E gesetzlich verankert sind. Derartige Verpflichtungen sollten auch bei anderen eingriffsintensiven Maßnahmen vorgesehen werden.
- Die Vorabkontrolle nach § 4d Abs. 5 BDSG wird nur in ausgewählten Bereichen angeordnet und begegnet in der Art der Anordnung weiteren Bedenken. Der Anwendungsbereich der Norm beschränkt sich nämlich auf besondere Risiken, die etwa bei heimlicher Kontrolle oder bestimmten technisch elaborierten Maßnahmen wie „intelligenter" Videoüberwachung vorliegen.[29] Das wird beispielsweise in den Fällen des § 32e Abs. 5 BDSG-E nicht zwingend der Fall sein. Außerdem dürfte im Betrieb häufig die Ausnahmeregelung des § 4d Abs. 5 Satz 2 2. HS Var. 2 BDSG greifen.[30] Beide Aspekte werden die Verweisung substantiell beschränken. Wenn insoweit eine Rechtsfolgenverweisung beabsichtigt war, sollte dies entsprechend dem Vorschlag des Bundesrates[31] klargestellt werden. Vorzugswürdig wäre es demgegenüber allerdings, eine allgemeine Vorschrift zur Vorabkontrolle einzuführen.[32]

Schließlich gibt es einen Aspekt, der im Regierungsentwurf nicht beachtet wird, nämlich die Frage besonderer Datensicherheitsmaßnahmen. Bei einer Einfügung der Regelungen zum Beschäftigtendatenschutz in das Bundesdatenschutzgesetz greift insoweit die allgemeine Vorschrift des § 9 BDSG mit der entsprechenden Anlage. Die Anforderungen dieser Norm (und damit die Regelungstechnik über eine Generalklausel, die jede Form der Verarbeitung personenbezogener Daten erfasst) hat das Bundesverfassungsgericht allerdings in der Entscheidung zur Vorratsdatenspeicherung als nicht hinreichend beurteilt.[33] Die Anforderungen, die das Gericht insoweit aufgestellt hat, sind zwar nicht direkt auf den Umgang mit Daten im Betrieb anwendbar. In beiden Fällen geht es aber um die Speicherung von Daten mit erheblicher Sensibilität und von vielen Betroffenen (Streubreite), teilweise (bei der Speicherung von Telekommunikations-Verkehrsdaten) sogar um identische Datenarten. Insofern sind auch an die Maßnahmen der Datensicherheit im Bereich der nur mittelbaren Wirkung der Grundrechte (wie im Betrieb) hohe Anforderungen zu stellen. In der Folge der Entscheidung des Bundesverfassungsgerichts darf sich der Gesetzgeber

---

29 Dazu *Hornung/Desoi*, K&R 2011, 153, 158.
30 Stellungnahme des ULD Schleswig-Holstein (Fn. 19)
31 BT-Drs. 17/4230, S. 34.
32 Z.B. entsprechend dem Vorschlag von BÜNDNIS 90/DIE GRÜNEN, § 29.
33 BVerfGE 125, 260; zur Frage der Datensicherheit s. *Roßnagel/Bedner/Knopp*, DuD 2009, 536 ff.; *Hornung/Schnabel*, DVBl. 2010, 824, 829.

insoweit nicht auf die betriebliche Praxis verlassen, sondern hat vielmehr selbst Vorgaben zu machen.[34]

3.7 Der Regelungskomplex der Überwachung und Kontrolle

Es ist zu begrüßen, dass sich die Entwürfe mit der besonders konfliktträchtigen Frage der Überwachung und Kontrolle der Beschäftigten im Detail auseinandersetzen und dabei auch relevante Fragen aus der Praxis entscheiden. Allerdings sollte man sich nicht der Hoffnung hingeben, dass damit ein Maß an substantieller Rechtsklarheit geschaffen wird, das die Ausfüllung durch die Arbeitsgerichtsbarkeit überflüssig macht. An vielen Stellen enthält der Regierungsentwurf etwa wertungs- und ausfüllungsbedürftige Begriffe wie „betriebliche Gründe", „schwerwiegende Pflichtverletzung", „erforderlich", „unerlässlich", „Kernbereich privater Lebensgestaltung", „Anhaltspunkte für schutzwürdige Interessen der Betroffenen" etc. Dies wird dazu führen, dass die Festlegung wichtiger Grundlinien für die Praxis schließlich doch Aufgabe der Gerichte sein wird. So bleibt etwa die genaue Bedeutung des Kernbereichsschutzes offen: § 32e Abs. 7 BDSG-E nennt nur den Begriff, und die Begründung[35] enthält keine weiteren Erläuterungen. Die relativ enge Definition des Bundesverfassungsgerichts[36] wird jedenfalls nur selten einschlägig sein.

Im Folgenden sollen einige Problempunkte dieses Regelungskomplexes bewertet werden.

3.7.1 Compliance und Screening

Die Regelung in § 32d Abs. 3 BDSG-E stellt eine Gewichtungsverschiebung zulasten des Schutzes der Beschäftigendaten dar. Die Gesetzesbegründung betont zwar zu Recht, dass sich Pflichten der Unternehmen zur Korruptionsbekämpfung und Compliance teilweise aus Spezialgesetzen ergeben.[37] Bislang ist aber offen – und wird vielfach bestritten – ob diese Verpflichtungen den datenschutzrechtlichen Pflichten der Arbeitgeber gegenüber den Beschäftigen vorgehen, oder ob umgekehrt das Datenschutzrecht gerade Grenzen für derartige Compliance-Vorschriften enthält. Der Entwurf gibt hier auf Seiten des Beschäftigendatenschutzes nach. Die in der Öffentlichkeit bekannt gewordenen Missbrauchsfälle zeigen indes, dass dieser Komplex einer deutlich einengenderen Regelung bedarf als der Entwurf dies bislang vorsieht.

Zunächst ist die Regelung in § 32d Abs. 3 BDSG-E nicht konsistent mit den Begrifflichkeiten und Zielrichtungen der datenschutzrechtlichen Konzepte der Anonymität und Pseudo-

---

[34] S. etwa die Vorschläge im Entwurf der SPD (§ 16 und § 17) und von BÜNDNIS 90/DIE GRÜNEN (§ 5).
[35] BT-Drs. 17/4230, S. 19.
[36] Verweis bei *Tinnefeld/Petri/Brink*, MMR 2010, 727, 732.
[37] BT-Drs. 17/4230, S. 18.

nymität.[38] Gemäß § 3 Abs. 6 BDSG bedeutet „anonymisieren“ das „Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können“. Ausweislich § 32d Abs. 3 Satz 2 BDSG-E ist dies aber gerade nicht gemeint, da die Daten offenbar so behandelt werden sollen, dass eine Re-Personalisierung noch möglich ist. Pseudonymisieren meint gemäß § 3 Abs. 6a BDSG das „Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren“. Bei der Regelung in § 32d Abs. 3 BDSG-E wird indes weder das eine noch das andere beabsichtigt. Es kann deshalb keine Rede davon sein, dass die Pflicht zur Anonymisierung die Rechte der Beschäftigten hinreichend wahrt.[39] Die Begrifflichkeiten suggerieren vielmehr eine datenschutzfreundliche Lösung, die de facto nicht erreicht wird.

Der Regierungsentwurf enthält überdies keine definierte Anlassbeschreibung oder Verdachtsschwelle. Dies ist ausweislich der Gegenäußerung auch so beabsichtigt,[40] das heißt die Norm ist so zu lesen, dass das beschriebene Vorgehen anlasslos und dauerhaft zulässig ist. Dies ist eine potentiell außerordentlich weitreichende Verarbeitungsbefugnis, da – wie beschrieben – das Verfahren gerade weder eine Anonymisierung noch eine Pseudonymisierung im Rechtssinn beinhaltet und deshalb auch keinen echten Schutz bietet.

Wenn die Norm beibehalten wird, sollte sie enger gefasst werden. Hierfür bieten sich mehrere Möglichkeiten an:

- Um eine ubiquitäre, anlasslose und dauerhafte Kontrolle zu verhindern, sollte entsprechend dem Vorschlag des Bundesrates das Vorliegen tatsächlicher Anhaltspunkte verlangt[41] und die Variante der schweren Pflichtverletzung gestrichen werden. Keinesfalls sollte Stimmen gefolgt werden, die den Anwendungsbereich sogar noch über den der schweren Pflichtverletzung hinaus und in den präventiven Bereich hinein erweitern wollen.[42]
- Falls die anlasslose Datenerhebung beibehalten wird, sollte sie zumindest insoweit beschränkt werden, dass sie nur für besonders gefahrgeneigte Arbeitsbereichen wie Beschaffungsabteilungen zugelassen wird. Man kann dies aus Gesichtspunk-

---

38 S. *Heinson/Sörup/Wybitul*, CR 2010, 751, 755; *Schuler*, DuD 2011, 126, 127 f.; Stellungnahme des ULD Schleswig-Holstein (Fn. 19).
39 So aber *Forst*, NZA 2010, 1043, 1046 f.
40 BT-Drs. 17/4230, S. 40.
41 BT-Drs. 17/4230, S. 32; ebenso *Rasmussen-Bonn/Raif*, GWR 2011, 80; Stellungnahme des ULD Schleswig-Holstein (Fn. 19).
42 So aber *Kort*, Der Betrieb 2011, 651, 652 f.

ten der Verhältnismäßigkeit auch aus dem aktuellen Entwurf herauslesen.[43] Es sollte aber explizit geregelt werden.

- Ein allgemeines und verdachtsloses Screening von Beschäftigtendaten ist allenfalls dann zu rechtfertigen, wenn effektive technische und organisatorische Sicherungsmittel sowie eine Vorabprüfung[44] eingesetzt werden. Diese Anforderung erfüllt der Entwurf nicht.
- Eine echte Pseudonymisierung kann nur erreicht werden, wenn die Daten bei Dritten ausgewertet werden und der Arbeitgeber weder faktische noch rechtliche Möglichkeiten des Zugriffs auf die Zuordnungsregel hat und sicherstellt, dass lediglich konkrete Verdachtsfälle in den Verantwortungsbereich des Arbeitgebers gelangen.[45] Insofern wäre die Einbeziehung vertrauenswürdiger Dritter zu erwägen.
- Eine echte Anonymisierung kann ebenfalls eingesetzt werden, aber nicht in dem Sinne, in dem der Entwurf dies vorsieht. Anonyme Daten können – etwa zur Bestimmung korruptionsgefährdeter Arbeitsbereiche – analysiert werden, wenn keine Möglichkeit der Re-Individualisierung besteht. Stattdessen können im Fall von Auffälligkeiten (pseudonyme) Stichproben erfolgen.[46]

3.7.2 Videoüberwachung

Die Absicht einer Regelung der Videoüberwachung nicht öffentlich zugänglicher Bereiche ist zu begrüßen, weil es bislang an einer gesetzlichen Normierung hierzu fehlt.[47] Besonders positiv zu werten ist dabei die Anwendung auch auf Attrappen (§ 32f Ab s. 1 Satz 3 BDSG-E), deren subjektive Wirkung auf die Beschäftigten vielfach mit der einer echten Kamera identisch sein wird.

An einigen Stellen bedarf der Regierungsentwurf jedoch der Überarbeitung. Bei den Zulässigkeitsalternativen sollten § 32f Abs. 1 Satz 1 Nr. 2 und Nr. 7 BDSG-E gestrichen werden. Die Wahrnehmung des Hausrechts (Nr. 2) betrifft typischerweise nicht das Beschäftigtenverhältnis, sondern Dritte. Hinsichtlich Nr. 7 ist zumindest eine Präzisierung dahin geboten, dass eine Videoüberwachung nicht etwa standardmäßig zur Kontrolle der Arbeitsqualität zulässig ist. Dies wäre mit den Persönlichkeitsrechten der Beschäftigten nicht zu vereinbaren.[48] Dass die Gesetzesbegründung von den sieben Alternativen der Zulässigkeit lediglich eine (Nr. 3) etwas näher erläutert, ist wenig hilfreich. Als Ergänzung der

---

43 S. *Heinson/Sörup/Wybitul*, CR 2010, 751, 755.
44 Stellungnahme des ULD Schleswig-Holstein (Fn. 19).
45 In diese Richtung *Heinson/Sörup/Wybitul*, CR 2010, 751, 755.
46 S. *Brink*/*Schmidt*, MMR 2010, 592, 594 f.
47 6b BDSG betrifft nur öffentlich zugängliche Bereiche.
48 Kritisch auch *Viotto*, AuR 2010, 433, 433; ULD Schleswig-Holstein (Fn. 19); *Seifert*, DuD 2011, 98, 103.

Zulässigkeitstatbestände wäre ein expliziter Ausschluss des Einsatzes zur Leistungskontrolle angemessen.[49]

Die Auflistung überwachungsfreier Räume in § 32f Abs. 2 BDSG-E sollte um einen expliziten Schutz auch von Pausenräumen ergänzt werden.[50] Hiergegen spricht jedenfalls nicht, dass derartige Räume von mehreren Personen genutzt werden;[51] selbstverständlich kann auch in diesem Fall ein so großes Schutzbedürfnis bestehen, dass der Ausschluss der Kontrolle gerechtfertigt ist. Keinesfalls sollten umgekehrt die Varianten der Sanitär-, Umkleide- und Schlafräume gestrichen werden.[52]

Zu der kontrovers diskutierten Frage des Verbots einer heimlichen Videoüberwachung ist zu bemerken: Dieses Verbot gilt nur für den Arbeitgeber. Soweit der Verdacht auf eine entsprechende Straftat vorliegt, kann dieser sich selbstverständlich an Staatsanwaltschaft und Polizei wenden. Bei Vorliegen eines entsprechende Anfangsverdachts dürfen dann gemäß § 100h Abs. 1 Satz 1 Nr. 1 StPO auch ohne Wissen der Betroffenen Bildaufnahmen hergestellt werden.

Sollte eine Änderung des absoluten Verbots erwogen werden, so wären aus verfassungsrechtlicher Sicht jedenfalls hohe Anforderungen zu formulieren: Zum einen für die materiellen Eingriffsvoraussetzungen (konkrete Anhaltspunkte für eine Straftat),[53] zum anderen für organisatorische Absicherungen: Beteiligungen des Betriebsrats, Dokumentationspflichten (Vorabkontrolle, Dokumentation des Überwachungsanlasses und der Durchführung der Überwachung) sowie für den Fall der Nichteinhaltung der materiellen und prozessualen Anforderungen ein explizites Beweisverwertungsverbot sowie die Aufnahme einer besonderen Sanktionsvorschrift in den Katalog des § 43 BDSG.

Abschließend bleibt anzumerken, dass bei Umsetzung dieser Anforderungen im Wesentlichen Anwendungsfälle verbleiben, die in den Zuständigkeitsbereich von Staatsanwaltschaft und Polizei fallen. Da insofern auch eine Durchführung der Maßnahme durch diese staatlichen Stellen möglich (und unter rechtsstaatlichen Gesichtspunkten sogar vorzugswürdig) ist, erscheint eine Veränderung des Entwurfs insgesamt verzichtbar.

---

[49] S. Stellungnahme der Neuen Richtervereinigung (Fn. 19), S. 7; ebenso der Entwurf von BÜNDNIS 90/DIE GRÜNEN, § 10 Abs. 1 Satz 1; a.A. *Kort*, MMR 2011, 294, 296.

[50] Ebenso der Vorschlag des Bundesrates, BT-Drs. 17/4230, S. 34.

[51] S. *Seifert*, DuD 2011, 98, 104 f.

[52] So aber *Heinson/Sörup/Wybitul*, CR 2010, 751, 757.

[53] Diese Verengung gegenüber der Rechtsprechung des BAG erscheint geboten. Das Gericht hat – zu weitgehend – die heimliche Überwachung auf Basis der bisherigen Rechtslage auch bei schweren Pflichtverletzungen für zulässig erklärt, s. BAG NJW 2003, 3436, 3437.

3.7.3 Biometrie

§ 32h BDSG-E ist so weit und generisch gefasst, dass auf ihn in der Form des Entwurfs verzichtet werden kann. Er bietet gegenüber den Regelungen der §§ 32c, 32d BDSG-E de facto keine präziseren Leitlinien Die Komplexität der verschiedenen biometrischen Charakteristika, Systeme und Verfahren und der mit ihnen verbundenen Rechtsfragen im Betrieb[54] ist so groß, dass mit einer derart allgemein gefassten Norm wenig gewonnen ist. Zumindest müssten bestimmte zulässige oder unzulässige Einsatzfelder oder Einsatzmodalitäten beschrieben und Regeln für den Umgang mit biometrischen Daten vorgegeben werden.

3.7.4 Telekommunikationsdienste

§ 32i BDSG-E befasst sich nur mit einer Hälfte des schwierigen Problems der Kontrolle von Telekommunikationsdiensten am Arbeitsplatz, und zwar mit der weniger problematischeren.

Der Fall der ausschließlich beruflichen oder dienstlichen Nutzung ist zwar ebenfalls komplex, im Ergebnis aber unproblematischer als die Überwachung von Diensten, wenn eine private Nutzung gestattet ist. Der von § 32i BDSG-E geregelte Fall ist in der Praxis der bei weitem leichter zu bewältigende, der aber insbesondere bei der Internetnutzung immer unrealistischer wird. Die eigentlichen Probleme und kontroversen Rechtsfragen entstehen dann, wenn eine private Nutzung ganz oder in Grenzen zugelassen ist. Hierzu schweigt der Entwurf.[55] Auch die Gesetzesbegründung enthält noch nicht einmal Anhaltspunkte zur Lösung des Problems. Die Gegenäußerung[56] verweist (de lege lata zutreffend) auf das Telekommunikationsgesetz, dessen Regelungen aber ersichtlich für das Problem der privaten Nutzung betrieblicher Telekommunikationsanlagen nicht geschaffen wurden und für dieses Problem auch nicht adäquat sind.

§ 32i Abs. 4 Satz 2 BDSG-E sollte gestrichen werden. Weder aus dem Gesetz noch aus der Begründung ist ersichtlich, was genau mit „private Daten“ gemeint ist. Ein anerkennenswertes Interesse von Arbeitgebern an der Kenntnisnahme privater Daten und Inhalte der Telekommunikation ist nicht ersichtlich.[57]

---

[54] S. z.B. *Hornung/Steidle*, AuR 2005, 201 ff.; *Hornung*, AuR 2007, 398 ff.; allgemein zu den Verhältnismäßigkeitskriterien *Hornung*, Die digitale Identität, 2005, 178 ff.

[55] Kritisch dazu z.B. *Heinson/Sörup/Wybitul*, CR 2010, 751, 757 ff.; *Kort*, MMR 2011, 294 f.; *Wybitul* (Fn. 18), 503.

[56] BT-Drs. 17/4230, S. 42.

[57] Ebenso *Forst*, NZA 2010, 1043, 1048.