Spannungsfeld Datenschutz und Compliance im RegE Beschäftigtendatenschutzgesetz

MICHAEL KORT

I. Einleitung

Compliance ist seit einigen Jahren in aller Munde. Der Begriff „Compliance" wird auch in der Begründung zum Entwurf der Bundesregierung eines Gesetzes zur Regelung des Beschäftigtendatenschutzes vom 25.8.2010 (im Folgenden: RegE Beschäftigtendatenschutzgesetz) verwendet. So heißt es einleitend, mit den Neuregelungen würden Beschäftigte an ihrem Arbeitsplatz wirksam vor Bespitzelungen geschützt; gleichzeitig würden den Arbeitgebern verlässliche Grundlagen für die Durchsetzung von Compliance-Anforderungen und für den Kampf gegen Korruption an die Hand gegeben.[1]

An anderer Stelle in der Begründung zum RegE Beschäftigtendatenschutzgesetz, nämlich bei der Begründung zum geplanten § 32 d Abs. 3 BDSG, findet sich eine knappe und letztlich verkürzte Definition von Compliance: Es heißt dort, Compliance bedeute in diesem Zusammenhang die Einhaltung aller relevanten Gesetze, Verordnungen, Richtlinien und Selbstverpflichtungen durch ein Unternehmen als Ganzes.[2] Diese Definition von Compliance greift insofern zu kurz, als unter Compliance nicht nur die Norm- und Regeleinhaltung im Unternehmen zu verstehen ist, sondern auch die Entwicklung von Strukturen und Verfahren, um diese Regeleinhaltung durch Organmitglieder, durch Führungspersonen (Manager) und durch alle ande-

[1] BR-Drucks. 535/10 vom 3.9.2010, S. 2.
[2] BR-Drucks. 535/10 vom 3.9.2010, S. 35.

ren Mitarbeiter (Arbeitnehmer und freie Mitarbeiter) im Unternehmen zu gewährleisten.[3]

Der RegE Beschäftigtendatenschutzgesetz befasst sich mit dem Spannungsfeld zwischen den Anforderungen an Compliance im Unternehmen auf der einen Seite und datenschutzrechtlichen Anforderungen auf der anderen Seite. Die folgenden Ausführungen werden dieses Spannungsfeld behandeln, und zwar insbesondere, wenn auch nicht ausschließlich, im Hinblick auf die geplante Reform des Beschäftigtendatenschutzes.

II. Bestehen eines Spannungsfelds

Vorab stellt sich die Frage, wodurch überhaupt ein solches Spannungsfeld zwischen der Erfüllung von Compliance-Anforderungen und der Erfüllung datenschutzrechtlicher Anforderungen[4] entstehen kann. Dieses Spannungsfeld entsteht dadurch, dass normative oder sonstige Compliance-Anforderungen existieren, die ein Höchstmaß an Transparenz verlangen und damit dem datenschutzrechtlichen Verbot der Datenerhebung, Datenverarbeitung und Datennutzung mit Erlaubnisvorbehalt zuwiderlaufen können. Das Spannungsverhältnis zwischen Compliance-Anforderungen und datenschutzrechtlichen Anforderungen zeigt etwa eine kündigungsschutzrechtliche Entscheidung des *Arbeitsgerichts Berlin* vom 18.2.2010,[5] bei der es um die Kündigung eines leitenden Mitarbeiters im Bereich Compliance und Korruptionsbekämpfung wegen von ihm veranlasster Überwachungsmaßnahmen und Datenabgleiche ging.

Zu Recht wird beklagt, dass die letzte Novelle des BDSG im Jahr 2009, insbesondere § 32 BDSG in der Fassung von 2009, dieses Spannungsverhältnis zwischen Compliance-Anforderungen und datenschutzrechtlichen Anforderungen nicht gelöst hat.[6]

Wenn deutsche normative Compliance-Regeln, insbesondere bundesrechtliche Normen, soweit sie Compliance-Gebote enthalten, Anwendung

---

[3] So z. B. *Wybitul*, Betriebs-Berater 2009, 1582; ähnlich *Forst*, DuD 2010, 160.

[4] Zu diesem Spannungsfeld *Wybitul*, Betriebs-Berater 2009, 1582; *Heldmann*, Der Betrieb 2010, 1235; *Barton*, RDV 2009, 200; *Forst*, NZA 2010, 1043; zum Spannungsfeld aus anwaltlicher Sicht *Hamm*, NJW 2010, 1332.

[5] ArbG Berlin, ZIP 2010, 1191 = CCZ 2010, 158 mit Anm. *Götz*; dazu auch *Kreienbrock*, GWR 2010, 257.

[6] *Wybitul*, Betriebs-Berater 2009, 1582.

finden, mag wegen § 1 Abs. 3 BDSG das BDSG ausnahmsweise zurücktreten, also das Spannungsverhältnis zugunsten der Compliance aufgelöst werden. Das gilt aber nicht, wenn – wie regelmäßig – die Compliance-Anforderungen nicht aus Normen i. S. von § 1 Abs. 3 BDSG resultieren, sondern etwa aus deutschen Normen, die nicht die spezifischen Voraussetzungen von Normen i. S. von § 1 Abs. 3 BDSG erfüllen, oder aus ausländischen, etwa US-amerikanischen Normen, resultieren, oder sich Compliance-Anforderungen – wie häufig – aus bloßen Generalklauseln oder aus nicht normativen Geboten ergeben, etwa auf der Basis von Corporate Governance-Regeln oder Ethik-Richtlinien. In all diesen Fällen ist eine Datenerhebung und Datenverarbeitung personenbezogener Daten nur zulässig, wenn entweder eine Einwilligung vorliegt oder sich die Zulässigkeit der Datenverarbeitung aus den besonderen Bestimmungen zum Beschäftigtendatenschutz, also zukünftig aus den geplanten §§ 32 ff. BDSG oder aus § 28 BDSG ergibt. In diesem Zusammenhang stellt sich angesichts des zukünftigen Beschäftigtendatenschutzes die bereits nach geltendem Recht strittige Frage des Verhältnisses spezifisch beschäftigtendatenschutzrechtlicher Normen wie bislang § 32 BDSG 2009 zu § 28 BDSG[7] erneut, nunmehr bezogen auf das Verhältnis der geplanten §§ 32 ff. BDSG zu § 28 BDSG.

III. Verhältnis der Normen des Beschäftigtendatenschutzes zu § 28 BDSG

1. Verhältnis von § 32 BDSG 2009 zu § 28 BDSG

Einer der wesentlichen Kritikpunkte von § 32 BDSG 2009 war, dass das Verhältnis dieser Norm zu § 28 BDSG ungeklärt geblieben ist.[8] Zwar enthält die Begründung zu der gesetzlichen Neuregelung von 2009 einige Hinweise zum Verhältnis dieser beiden Normen. So wird betont, dass § 28 Abs. 1 Satz 1 Nr. 1 BDSG neben § 32 Abs. 1 Satz 1 BDSG keine Anwendung mehr finden kann.[9] Jedoch ist ein Teil dieser Ausführungen in den Gesetzesmaterialien nicht eindeutig. So ist insbesondere nicht klar, wie weit der Ausschluss auch von § 28

[7] Dazu z. B. *Joussen* NZA 2010, 254, 257.

[8] Für eine weitgehende Verdrängung von § 28 Abs. 1 BDSG durch § 32 BDSG: *Schmidt*, RDV 2009, 193, 195; *Franzen*, RdA 2010, 257, 260; *Joussen*, NZA 2010, 254, 257.

[9] BT-Drucks. 16/13657, S. 34.

Abs. 1 Satz 1 Nr. 2 und 3 BDSG bei Beschäftigungsverhältnissen reicht. Die Gesetzesbegründung deutet auf einen Totalausschluss hin.[10] Ein solcher Totalausschluss der Möglichkeit einer Anwendung von § 28 Abs. 1 Satz 1 BDSG bei Beschäftigungsverhältnissen lässt sich dem Gesetz selbst aber nicht entnehmen. Er wäre auch nicht zielführend. So muss etwa die Übermittlung bestimmter Beschäftigtendaten bei Durchführung einer *due diligence* auf der Basis von § 28 Abs. 1 Satz 1 Nr. 2 BDSG möglich sein.[11]

Nach zutreffender Auffassung dürfte § 32 BDSG 2009 so zu verstehen sein, dass § 32 Abs. 1 Satz 1 BDSG repressive Compliance-Maßnahmen zur Aufdeckung von Ordnungswidrigkeiten, die nicht von § 32 Abs. 1 Satz 2 BDSG erfasst werden, sowie präventive Maßnahmen zur Verhinderung von Straftaten[12] und Ordnungswidrigkeiten erfasst. Ein „erst-recht-Schluss" in dem Sinn, dass § 32 Abs. 1 Satz 2 BDSG mit seinen strengen Voraussetzungen für die Zulässigkeit repressiver Compliance-Maßnahmen „erst recht" solche strengen Voraussetzungen für die präventiven Compliance-Maßnahmen wie die Verhinderung von Straftaten aufstellt, also gleichsam analog auf solche präventiven Compliance-Maßnahmen Anwendung findet, ist nicht geboten.[13]

Präventive Maßnahmen zur Verhinderung von Straftaten dürften sich nach der *lex lata* eher auf § 32 Abs. 1 Satz 1 BDSG stützen lassen[14] als auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG,[15] da der unmittelbare Zusammenhang solcher präventiver Compliance-Maßnahmen mit dem Beschäftigungsverhältnis evident ist.

Ferner dürfte § 32 Abs. 1 Satz 1 BDSG 2009 auch anwendbar sein, wenn es um die Verhinderung oder um die Aufdeckung von arbeitsvertraglichen Pflichtverletzungen[16] geht. Der Begriff der Er-

---

[10] BT-Drucks. 16/13657, S. 35; dazu auch *Wedde*, in: *Däubler/Klebe/Wedde/Weichert*, BDSG, 3. Aufl., 2010, § 32 Rdn. 8.

[11] Dazu – restriktiv – *Wedde*, in: *Däubler/Klebe/Wedde/Weichert*, BDSG, 3. Aufl., 2010, § 28 Rdn. 51.

[12] Dazu *Zikesch/Reimer*, DuD 2010, 96, 97 f.; *Schmidt*, RDV 2009, 193, 200.

[13] Gegen einen solchen erst-recht-Schluss *Zikesch/Reimer,* DuD 2010, 96 f.

[14] So auch die Gesetzesbegründung BT-Drucks. 16/13657, S. 36 sowie *Thüsing*, NZA 2009, 865, 868; *Barton*, RDV 2009, 200, 203; *Schmidt*, RDV 2009, 193, 196; offengelassen von *Körner*, AuR 2010, 416, 418.

[15] Anders *Vogel/Glas*, Der Betrieb 2009, 1747, 1751; *Götz,* CCZ 2010, 158, 160.

[16] Dazu *Thüsing,* NZA 2009, 865, 867 f.

forderlichkeit der Datenerhebung und Datenverarbeitung für die Durchführung des Beschäftigungsverhältnisses i. S. von § 32 Abs. 1 Satz 1 BDSG 2009 ist nämlich im Ergebnis weit auszulegen.[17] § 32 Abs. 1 Satz 1 BDSG 2009 verlangt entgegen seinem Wortlaut letztlich nicht eine Erforderlichkeit im strengen Sinn, sondern eine Abwägung der Interessen der Beteiligten.[18]

Nach zutreffender Ansicht wird nur § 28 Abs. 1 Satz 1 Nr. 1 BDSG durch § 32 Abs. 1 BDSG 2009 verdrängt,[19] nicht aber auch § 28 Abs. 1 Satz 1 Nr. 2 und 3 BDSG.[20] Allerdings geht es nicht an, die Spezialität von § 32 Abs. 1 Satz 1 BDSG 2009 auszuhebeln. Daher können § 28 Abs. 1 Satz 1 Nr. 2 und 3 BDSG nur Anwendung finden, wenn es nicht direkt um die Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses geht. Ein solcher bloß indirekter Bezug zu Beschäftigungsverhältnissen besteht etwa bei der Weitergabe von Arbeitnehmerdaten im Wege der Durchführung einer *due diligence*.

Außerdem gilt sowohl für die beiden Sätze von § 32 Abs. 1 BDSG 2009 in ihrem Verhältnis zueinander als auch für § 32 BDSG 2009 und § 28 BDSG in deren Verhältnis zueinander eine Art „Gebot praktischer Konkordanz". Dieses Gebot bewirkt, dass jede der Normen im Lichte der jeweiligen Komplementärnorm auszulegen ist. Vor allem aber ist der in den Gesetzesmaterialien zum Ausdruck kommende Wille des Gesetzgebers der Novelle von 2009 zu berücksichtigen, dass mit § 32 BDSG im Grundsatz nur die bisherige Rechtsprechung normativ wiedergegeben werden sollte, nicht aber gänzlich Neuland betreten werden sollte.[21]

2. Verhältnis der geplanten Neuregelung von §§ 32 ff. BDSG zu § 28 BDSG

Welche Bedeutung haben diese Überlegungen für das Verhältnis der zukünftigen §§ 32 ff. BDSG zu dem gleich bleibenden § 28 BDSG? Eine gesetzliche Klärung dieses Verhältnisses findet sich nicht. Die Begründung zum RegE Beschäftigtendatenschutzgesetz führt zu dem

---

[17] S. etwa *Deutsch/Diller*, Der Betrieb 2009, 1462, 1463.

[18] So auch *Thüsing*, NZA 2009, 865, 867 sowie *Zikesch/Reimer,* DuD 2010, 96, 98; ähnlich auch *Schmidt*, RDV 2009, 193, 198.

[19] *Gola/Schomerus*, BDSG, 10. Aufl., 2010, § 32 Rdn. 1.

[20] *Bierekoven*, CR 2010, 203, 204 ff.

[21] BT-Drucks. 16/12011, S. 53; auch *Schmidt*, RDV 2009, 193.

Verhältnis der geplanten §§ 32 ff. BDSG zu § 28 BDSG lediglich aus:

„Die Regelungen des Unterabschnitts zum Beschäftigtendatenschutz gehen, soweit sie speziellere Regelungen treffen, den übrigen Bestimmungen des dritten Abschnitts vor. Insbesondere gehen die Regelungen dem § 28 Absatz 1 Nummer 1 vor. Gleichzeitig gelten insbesondere die allgemeinen und gemeinsamen Bestimmungen sowie die Vorschriften über die Rechte der Betroffenen grundsätzlich auch für den Beschäftigtendatenschutz."

Immerhin scheint der Gesetzgeber damit davon auszugehen, dass nur § 28 Abs. 1 Satz 1 Nr. 1 BDSG, nicht aber auch § 28 Abs. 1 Satz 1 Nr. 2 und 3 BDSG durch §§ 32 ff. BDSG verdrängt werden.[22]

Was die Diskussion über das Verhältnis von § 32 BDSG 2009 zu § 28 BDSG 2009 betrifft, so findet sie somit ihre Fortsetzung in der Diskussion über das neue Recht.

IV. Repressive Compliance-Maßnahmen

Repressive Compliance-Maßnahmen, insbesondere solche der Korruptionsbekämpfung durch Aufdeckung einschlägiger Straftaten und Ordnungswidrigkeiten, spricht der RegE Beschäftigtendatenschutzgesetz, soweit die Datenerhebung, Datenverarbeitung und Datennutzung *mit* Kenntnis des Beschäftigten erfolgt, nur indirekt an, nämlich in § 32 c BDSG und in § 32 d BDSG.[23]

Eine direkte Behandlung finden repressive Compliance-Maßnahmen nur in § 32 e BDSG, wo es um die Datenerhebung *ohne* Kenntnis des Beschäftigten zur Verhinderung von Straftaten und anderen schwerwiegenden Pflichtverletzungen im Beschäftigungsverhältnis geht.

Die geplante Neuregelung enthält Licht und Schatten: Zu begrüßen ist, dass sie, anders als der noch geltende § 32 Abs. 1 Satz 2 BDSG 2009, die Datenerhebung nicht nur zur Aufdeckung von Straftaten, sondern auch zur Aufdeckung anderer schwerwiegender Pflichtverletzungen erfasst.

Fraglich ist, was unter „schwerwiegenden Pflichtverletzungen" zu verstehen ist. Die geplante gesetzliche Neuregelung gibt in § 32 e

---

[22] *Forst*, NZA 2010, 1043, 1044.

[23] Dazu *Forst*, NZA 2010, 1043, 1046.

Abs. Nr. 1 RegE Beschäftigtendatenschutzgesetz Auskunft, dass damit Pflichtverletzungen gemeint sein sollen, die eine außerordentliche Kündigung nach § 626 BGB rechtfertigen. Eine Bezugnahme auf einen kündigungsschutzrechtlichen und damit arbeitsrechtlichen Begriff (hier: wichtiger Grund für eine Kündigung) ist entgegen kritischen Stimmen[24] im Grundsatz durchaus für eine Norm denkbar, die Compliance-Maßnahmen, nämlich in erster Linie die Korruptionsbekämpfung, zum Gegenstand hat.

Jedoch fragt sich, ob es inhaltlich nicht zu eng ist, nur auf Pflichtverletzungen abzustellen, die einen wichtigen Kündigungsgrund bilden.[25] Repressive Compliance-Maßnahmen in Form der Datenerhebung ohne Kenntnis des Betroffenen können nämlich auch bei Pflichtverletzungen geboten sein, die zwar gravierend sind, aber (noch) nicht einen wichtigen Grund zur außerordentlichen Kündigung bilden.

Auch fragt sich, wieso der RegE Beschäftigtendatenschutzgesetz nur eine umfassende Regelung der *Datenerhebung* ohne Kenntnis des Beschäftigten enthält, aber keine detaillierte Regelung der Datenverarbeitung und der Datennutzung ohne Kenntnis des Beschäftigten. So findet sich etwa zu dem wichtigen Thema des Datenabgleichs (Screening) zwecks Aufdeckung von Straftaten und schwerwiegenden Pflichtverletzungen wenig Konkretes im RegE Beschäftigtendatenschutzgesetz.

V. Präventive Compliance-Maßnahmen

Die Behandlung präventiver Compliance-Maßnahmen im RegE Beschäftigtendatenschutzgesetz enthält ebenfalls Licht und Schatten. Zu begrüßen ist, dass das RegE Beschäftigtendatenschutzgesetz anders als der noch geltende § 32 BDSG 2009 überhaupt die Prävention anspricht. Einer der wesentlichen Kritikpunkte an § 32 BDSG 2009 war die Beschränkung in § 32 Abs. 1 Satz 2 BDSG auf die *Aufdeckung* von Straftaten. Es fragte und fragt sich, wie die Prävention (Verhinderung von Straftaten und anderen schwerwiegenden Pflichtverletzungen) auf der Basis des noch geltenden Rechts zu behandeln ist.

---

[24] *Beckschulze/Natzel*, Betriebs-Berater 2010, 2368, 2372.

[25] *Forst*, NZA 2010, 1043, 1047.

Die Vorschläge reichen von einer mehr oder minder weitgehenden analogen Anwendung von § 32 Abs. 1 Satz 2 BDSG 2009 über die Behandlung präventiver Maßnahmen nach § 32 Abs. 1 Satz 1 BDSG 2009, ggf. unter Berücksichtigung der *ratio legis* von § 32 Abs. 1 Satz 2 BDSG 2009, bis zu einer Behandlung präventiver Maßnahmen nach § 28 BDSG, soweit diese Norm nicht durch § 32 BDSG 2009 als *lex specialis* verdrängt wird. Bisweilen wird angesichts von § 32 Abs. 1 Satz 2 BDSG 2009 sogar die Möglichkeit präventiver Compliance-Maßnahmen als gänzlich ausgeschlossen angesehen.[26]

Vor allem der letztgenannten Auffassung ist entgegenzutreten: § 32 BDSG 2009 sollte keine grundsätzlichen Änderungen der damaligen Rechtslage herbeiführen, sondern die Rechtsprechung zum Beschäftigtendatenschutz normativ fixieren.[27] Ein gänzlicher Ausschluss der datenschutzrechtlichen Zulässigkeit präventiver Compliance-Maßnahmen war aber auf der Basis des bis 2009 allein einschlägigen § 28 BDSG nicht angelegt und ergibt sich auch nicht aus der *ratio legis* von § 32 BDSG 2009.

Der nunmehr geplante § 32 e BDSG schafft nur wenig Klarheit, was die Zulässigkeit präventiver Compliance-Maßnahmen betrifft. Nur für den Bereich der Datenerhebung ohne Kenntnis des Beschäftigten sieht die geplante Neuregelung eine Gleichstellung der *Verhinderung* mit der *Aufdeckung* von Straftaten und anderen schwerwiegenden Pflichtverletzungen vor. Damit scheinen zumindest einige rechtspolitische Wünsche der Kritik am § 32 Abs. 1 Satz 2 BDSG 2009 erfüllt.

Der Teufel steckt jedoch im Detail. Jegliche Präventivmaßnahme setzt nämlich nach dem Wortlaut des geplanten § 32 e Abs. 2 BDSG voraus, dass Tatsachen den Verdacht begründen, dass eine Straftat oder schwerwiegende Pflichtverletzung *bereits begangen worden ist*. Eine nach § 32 e Abs. 2 BDSG zulässige Prävention bezieht sich demgemäß konsequent auch nur auf die Verhinderung von in Zusammenhang mit der Straftat oder schwerwiegenden Pflichtverletzung, hinsichtlich derer bereits ein konkreter Verdacht besteht, stehender Straftaten oder Pflichtverletzungen. Mit anderen Worten ist somit eine Datenerhebung nicht möglich, um Straftaten oder schwerwiegende Pflichtverletzungen zu verhindern, ohne dass der durch

---

[26] *Wedde*, in: *Däubler/Klebe/Wedde/Weichert*, BDSG, 3. Aufl., 2010, § 32 Rdn. 131.

[27] *Gola/Klug*, NJW 2010, 2483, 2485.

Tatsachen begründete Verdacht einer bereits konkret begangenen Straftat oder bereits konkret begangenen schwerwiegenden Pflichtverletzung besteht.

Eine bereits vor der „Ersttat" einsetzende Datenerhebung zu Präventionszwecken, etwa bei durch Tatsachen belegtem Verdacht, dass zukünftig *erstmals* Straftaten oder schwerwiegende Pflichtverletzungen begangen werden, ist somit auf der Basis von § 32 e Abs. 2 BDSG nicht zulässig.[28] Die datenschutzrechtliche Zulässigkeit präventiver Compliance-Maßnahmen setzt vielmehr die Ersttat oder zumindest den konkret belegten Verdacht, dass die Ersttat bereits begangen worden ist, voraus. Eine Prävention im eigentlichen Sinn ist damit nicht möglich.

Auch fragt sich generell, wieso sich die Zulässigkeit der Datenerhebung zu Präventionszwecken immer nur auf eine Prävention hinsichtlich einer „in Zusammenhang" mit der Ersttat stehenden Straftat oder schwerwiegenden Pflichtverletzung beziehen soll. Offenbar soll damit eine anlassunabhängige Vorratsdatenerhebung oder ein anlassloses Screening verhindert werden. Jedoch ist effektive Prävention nicht möglich, wenn sie eine bereits begangene Ersttat erfordert und zudem voraussetzt, dass sich die Prävention nur auf mit der Ersttat in Zusammenhang stehende Pflichtverstöße bezieht. Überdies ist das Erfordernis eines „in Zusammenhang" mit der Ersttat stehenden potentiellen Pflichtverstoßes völlig konturlos.

VI. Elektronische Kommunikation

1. Email-Verkehr und Internetnutzung

Die für die Praxis außerordentlich bedeutsame Frage, ob und inwiefern die Erlaubnis zur privaten Email- und Internet-Nutzung am Arbeitsplatz oder deren Gestattung dem TKG und dem TMG unterfällt[29]

---

[28] Zu Recht kritisch insofern *Beckschulze/Natzel*, Betriebs-Berater 2010, 2368, 2372.

[29] Dazu etwa *Gola/Schomerus*, BDSG, 10. Aufl., 2010, § 32 Rdn. 17; *Däubler*, Gläserne Belegschaften?, 5. Aufl., 2010 Rdn. 338; *Wedde*, in: *Däubler/Klebe/Wedde/Weichert*, BDSG, 3. Aufl., 2010, § 32 Rdn. 114 f.; *Gola/Wronka*, Handbuch zum Arbeitnehmerdatenschutz, 5. Aufl., 2010, Rdn. 738 ff.; *Vogel/Glas*, Der Betrieb 2009, 1747; *Heldmann*, Der Betrieb 2010, 1235, 1239; *Wolf/Mulert*, Be-

(mit zahlreichen daraus resultierenden Pflichten und möglichen strafrechtlichen Konsequenzen), bleibt leider im RegE Beschäftigtendatenschutzgesetz unbeantwortet.[30] Zwar behandelt der nicht gerade kurze § 32 i BDSG die „Nutzung von Telekommunikationsdiensten". Hierbei geht es aber ersichtlich, wie § 32 i Abs. 1 bis 3 BDSG mit aller Deutlichkeit zeigt, nur um die Nutzung zu „beruflichen oder dienstlichen Zwecken".[31]

Die Rechtsstellung des Arbeitgebers bei der Privatnutzung von Email-Kommunikation am Arbeitsplatz wird nur indirekt angesprochen, nämlich in § 32 i Abs. 4 Satz 2 BDSG. Dort heißt es, der Arbeitgeber dürfe private Daten und Inhalte nur erheben, verarbeiten oder nutzen, wenn dies zur Durchführung des ordnungsgemäßen Dienst- oder Geschäftsbetriebs unerlässlich sei und er den Beschäftigten hierauf schriftlich hingewiesen habe. Zwar wird damit das Zugriffsrecht des Arbeitgebers auf private Daten erweitert. Liest man aber § 32 i Abs. 4 BDSG im Kontext mit § 32 i Abs. 1 bis 3 BDSG, so zeigt sich, dass es auch in Absatz 4 nicht um eine erlaubte private Email-Nutzung und Internetnutzung geht, sondern um die Verhinderung der unerlaubten Privatnutzung bzw. um den Zugriff auf private Daten und Inhalte bei Email-Nutzung und Internet-Nutzung zu ausschließlich beruflichen oder dienstlichen Zwecken.

Bislang offene Fragen der Möglichkeiten des Arbeitgebers zum Zugriff auf private Daten oder Inhalte bei Erlaubnis der „privaten" Email-Nutzung oder Internet-Nutzung, insbesondere Fragen einer Anwendung des TKG und des TMG auf den Arbeitgeber, bleiben damit auch in Zukunft unbeantwortet.

Offen bleibt zudem auch die Frage, ob Rechtsgrundlage für eine Privatnutzung von Email-Systemen und Internet durch die Arbeitnehmer auch das Entstehen einer betrieblichen Übung sein kann.[32] Gegen das Entstehen einer betrieblichen Übung spricht nicht, dass es sich bei der Duldung der Privatnutzung von Email und Internet durch den Arbeitgeber bloß um eine „Annehmlichkeit" und nicht um eine

---

triebs-Berater 2008, 442, 445 f.; *Koch*, NZA 2008, 911, 913; *Schmidt*, Betriebs-Berater 2009, 1295, 1296 f.

[30] Kritisch *Beckschulze/Natzel*, Betriebs-Berater 2010, 2368, 2374; *de Wolf*, NZA 2010, 1206, 1208; *Vietmeyer/Byers*, MMR 2010, 807; *Heinson/Sörup/Wybitul*, CR 2010, 751, 757; *Hanloser*, MMR-Aktuell 2010, 307093.

[31] *Beckschulze/Natzel*, Betriebs-Berater 2010, 2368, 2373.

[32] Dazu etwa *Koch*, NZA 2008, 911.

das Vermögen des Arbeitnehmers bereichernde echte Leistung des Arbeitgebers handelt.

Vielmehr spricht gegen die Möglichkeit des Entstehens einer betrieblichen Übung, dass der Arbeitgeber die private Email-Nutzung und Internet-Nutzung in der wohl überwiegenden Anzahl der Fälle durchaus untersagt hat und die private Nutzung trotz Verbots bloß duldend hinnimmt. Aus der Sicht der Arbeitnehmer besteht dann aber kein Vertrauen in die Beibehaltung dieser Praxis. Vielmehr wissen die Arbeitnehmer, dass sie sich mit der Privatnutzung über ein Verbot des Arbeitgebers hinwegsetzen und ihr Verhalten insofern arbeitsvertragswidrig ist. Die Basis für das Entstehen einer betrieblichen Übung existiert in solchen Fällen nicht. Auch ansonsten ist die Gleichsetzung von Erlaubnis und bloßer Duldung bei der privaten Nutzung betrieblicher Email-Systeme oder des Internets nicht möglich.[33]

Eine betriebliche Übung als Rechtsgrundlage für die private Email-Nutzung und Internet-Nutzung kommt daher allenfalls dann in Betracht, wenn der Arbeitgeber kein Verbot einer privaten Nutzung ausgesprochen hat.

2. Telefonnutzung

Der geplante § 32 i BDSG erfasst ebenso wie beim Email-Verkehr und beim Internet auch beim Telefonieren nur die Nutzung von Telekommunikationsdiensten zu beruflichen oder dienstlichen Zwecken. Die private Nutzung dienstlicher Telefonanlagen wird nicht geregelt.

Das „Mithören" von dienstlichen Telefongesprächen wird in § 32 i Abs. 2 Satz 1 BDSG angesprochen. Dessen Zulässigkeit soll von einer vorherigen Einwilligung beider Partner des Telefonats abhängig sein. Ob sich das Einwilligungserfordernis auch auf Notrufe bezieht, lässt der Gesetzentwurf offen.[34]

Das heimliche Mithören und Aufzeichnen des Inhalts von Telefonaten bleibt nach wie vor[35] grundsätzlich unzulässig und kann nach

---

[33] So zutreffend *Thüsing*, RDV 2010, 147 f.

[34] Kritisch *Beckschulze/Natzel*, Betriebs-Berater 2010, 2368, 2374.

[35] Dazu *BVerfG*, NJW 1992, 815; *BVerfG*, NJW 2002, 3619; BAG, NZA 1988, 307; *Wedde*, in: *Däubler/Klebe/Wedde/Weichert*, BDSG, 3. Aufl., 2010, § 32 Rdn. 112; *Gola/Wronka*, Handbuch zum Arbeitnehmerdatenschutz, 5. Aufl., 2010, Rdn. 770 ff.; *Oberwetter*, NZA 2008, 609, 611; *Wolf/Mulert*, Betriebs-Berater 2008, 442, 444.

§ 201 StGB strafbar sein. Zu bedenken ist, dass nach der Rechtsprechung des BAG das *zufällige* Mithören eines Telefonats nicht das Persönlichkeitsrecht des Gesprächspartners verletzt und insofern kein Beweisverwertungsverbot besteht.[36]

VII. Videoüberwachung

In Ergänzung zu dem geltenden§ 6 b BDSG, der die Videoüberwachung in öffentlich zugänglichen Räumen regelt, soll zukünftig § 32 f BDSG eine Regelung der Videoüberwachung in nicht öffentlich zugänglichen Betriebsstätten enthalten. Es ist im Grundsatz erfreulich, dass die Videoüberwachung, die trotz einiger Judikate des BAG[37] wegen ihrer besonderen Eingriffsqualität nach wie vor ungeklärte Rechtsfragen aufwirft, nunmehr gesetzlich geregelt werden soll.

Jedoch handelt es sich nur um eine Teilregelung. § 32 f BDSG behandelt nur die offene Videoüberwachung. Die geheime Videoüberwachung mit „versteckten" Kameras lässt sich, wie § 32 f Abs. 1 Satz 2 BDSG indirekt zeigt, nicht auf § 32 f BDSG stützen.[38] Als Rechtsgrundlage für den Einsatz verdeckter Kameras kommt bei repressiven und bei präventiven Compliance-Maßnahmen allenfalls § 32 e BDSG in Betracht.[39] § 32 e Abs. 4 Satz 1 Nr. 3 BDSG deutet jedoch darauf hin, dass sogar jegliche versteckte Videoüberwachung zukünftig generell verboten ist.[40]

Ein weiteres Problem stellt die Begrenzung der Einsatzmöglichkeit offener Videoüberwachung im geplanten § 32 f Abs. 1 BDSG dar. Dort werden offenbar enumerativ die Fallgruppen der zulässigen offenen Videokontrolle angesprochen. Ein Einsatz von Videokameras zur allgemeinen Verhaltens- oder zur Leistungskontrolle ist demgemäß nicht zulässig, da nicht als Fallgruppe erwähnt.

---

[36] BAG, NZA 2009, 974.

[37] BAG, NZA 2004, 1278; BAG, AP Nr. 5 zu § 87 BetrVG 1972 Ordnung des Betriebs; s. auch *Däubler*, Gläserne Belegschaften?, 5. Aufl., 2010; Rdn. 297; *Oberwetter*, NZA 2008, 609 f.

[38] So auch *Beckschulze/Natzel*, Betriebs-Berater 2010, 2368, 2373.

[39] *Forst*, NZA 2010, 1043, 1047.

[40] So RegE Beschäftigtendatenschutzgesetz, BR-Drucks. 535/10 vom 3.9.2010, S. 37 sowie *Beckschulze/Natzel*, Betriebs-Berater 2010, 2368, 2373; *Tinnefeld/Petri/Brink*, MMR 2010, 727, 732.

Zwar ist auch schon bislang die Zulässigkeit des Einsatzes von Videokameras zur Leistungskontrolle angesichts des Gebots der Wahrung des Persönlichkeitsrechts des Arbeitnehmers und des datenschutzrechtlichen Verbots der Totalkontrolle[41] im Einzelnen umstritten, jedoch galt bisher auf der Basis der BAG-Rechtsprechung der Grundsatz, dass der Arbeitgeber zur Einführung einer Videoüberwachung berechtigt ist, wenn sie verhältnismäßig ist.[42] Der Einsatz von Videoüberwachung zur Leistungskontrolle dürfte jedoch in Zukunft angesichts von § 32 f Abs. 1 BDSG ausgeschlossen sein.

Das ist misslich und widerspricht letztlich dem Verständnis des BAG, das unter einer Videoüberwachungsanlage eine Anlage versteht, die dazu bestimmt ist, das Verhalten oder die Leistung der Arbeitnehmer zu kontrollieren.[43] Auch betonte noch die Begründung zu § 32 BDSG 2009,[44] dass für die Kontrolle der Leistung oder des Verhaltens eines Beschäftigten § 32 Abs. 1 Satz 1 BDSG 2009 einschlägig sein sollte.[45] Ein Totalverbot der Videoüberwachung zwecks Leistungskontrolle gibt es somit auf der Basis der *lex lata* nicht, und zwar zu Recht nicht. Die zukünftige gesetzliche Regelung geht aber in Richtung eines Totalverbots der Leistungskontrolle durch offene Videoüberwachung.

Eine Regelung der offenen Videoüberwachung zwecks Leistungskontrolle dürfte in Zukunft angesichts von § 32 l Abs. 5 BDSG auch nicht mehr mittels Betriebsvereinbarung möglich sein. Diesem Ausschluss der Möglichkeit zur Regelung der Videoüberwachung als Leistungskontrollinstrument in einer Betriebsvereinbarung steht der betriebsverfassungsrechtliche Grundsatz entgegen, dass eine Leistungskontrolle durch den Arbeitgeber im Grundsatz zulässig ist, wenn auch mitbestimmungspflichtig ist.

---

[41] Dazu *Schmidl*, in: *Hauschka* (Hrsg.), Corporate Compliance, 2. Aufl., 2010, § 29 Rdn. 309.

[42] *Fitting/Engels/Schmidt/Trebinger/Linsenmeier*, BetrVG, 25. Aufl., 2010, § 75 Rdn. 150 f. sowie § 87 Rdn. 247, 253.

[43] BAG, NZA 2004, 1278, 1279; BAG, Betriebs-Berater 2008, 2743, 2745; s. auch *Forst*, RDV 2009, 204, 205.

[44] BT-Drucks. 16/13657, S. 36.

[45] S. auch *Forst*, RDV 2009, 204, 210.

VIII. RFID

Entgegen Forderungen in der Literatur[46] hat der Gesetzgeber nicht vor, RFID (*Radio Frequency Identification*)[47] über den schon bestehenden § 6 c BDSG hinaus gesetzlich zu regeln. Das ist zu begrüßen,[48] da die geplanten Regelungen zum Beschäftigtendatenschutz ohnehin schon sehr detailfreudig sind und andernfalls die Gefahr einer Überregulierung droht.

IX. Datenabgleich (Screening)

Eine wichtige Compliance-Maßnahme zur Bekämpfung von Wirtschaftskriminalität, insbesondere von Korruption, ist der Datenabgleich. Compliance-Anforderungen können daher einen Datenabgleich (Screening), etwa in Form des *Data Mining* oder des Daten-Doubletten-Abgleichs[49] nahelegen.

Auf der Basis der *lex lata* ist die Zulässigkeit eines solchen Datenabgleichs sehr umstritten,[50] weil das Gesetz bislang keine Bestimmungen zum Datenabgleich enthält. Weitgehend Einigkeit besteht, dass verdachtsunabhängige oder andauernde Massenscreenings dem Verbot der Totalüberwachung widersprechen.[51] Massenscreenings zur Aufdeckung von Straftaten unterliegen nämlich den strengen Voraussetzungen des § 32 Abs. 1 Satz 2 BDSG 2009,[52] sie werden dort allerdings nicht als solche thematisiert.

---

[46] *Eisenberg/Puschke/Singelnstein*, ZRP 2005, 9.

[47] Dazu allg. *Gola/Schomerus*, BDSG, 10. Aufl., 2010, § 6 c Rdn. 5 a ff.; *Wedde*, in: *Däubler/Klebe/Wedde/Weichert*, BDSG, 3. Aufl., 2010, § 32 Rdn. 98 ff.; *Däubler*, Gläserne Belegschaften?, 5. Aufl., 2010 Rdn. 324 a ff.; *Gola/Wronka*, Handbuch zum Arbeitnehmerdatenschutz, 5. Aufl., 2010, Rdn. 869 ff.

[48] *Westerholt/Döring*, CR 2004, 710, 715.

[49] Zu Datenabgleichsformen *Bierekoven*, CR 2010, 203; *Brink/Schmidt*, MMR 2010, 592; *Gola/Wronka*, Handbuch zum Arbeitnehmerdatenschutz, 5. Aufl., 2010, Rdn. 847; zur Praxis des Data-Mining *Wilke*, AiB 2006, 155.

[50] Für die weitgehende Zulässigkeit *Diller*, Betriebs-Berater 2009, 438, 439 f.; dagegen *Steinkühler*, Betriebs-Berater 2009, 1294; sehr zurückhaltend auch *Däubler*, Gläserne Belegschaften?, 5. Aufl., 2010 Rdn. 427a ff.; differenzierend *Heldmann*, Der Betrieb 2010, 1235, 1237 f.

[51] *Bierekoven*, CR 2010, 203, 207; *Kock/Francke*, NZA 2009, 646, 648.

[52] *Wybitul*, Betriebs-Berater 2009, 1582, 1584; *Salvenmoser/Hauschka*, NJW 2010, 331, 333.

Soweit ein Datenabgleich zu Präventionszwecken durchgeführt werden soll, ist nach der *lex lata* nicht § 32 Abs. 1 Satz 2 BDSG einschlägig, sondern § 32 Abs. 1 Satz 1 BDSG.[53] Da das Merkmal der Erforderlichkeit der Datenerhebung, Datenverarbeitung und Datennutzung für das Beschäftigungsverhältnis i. S. von § 32 Abs. 1 Satz 1 BDSG nicht eng auszulegen ist, sondern letztlich auch in § 32 Abs. 1 Satz 1 BDSG eine Interessenabwägung „hineinzulesen" ist, besteht auf der Grundlage des noch geltenden Rechts keine Veranlassung, den präventiven Datenabgleich generell skeptisch zu betrachten.[54] Vielmehr kann der Datenabgleich auf der Basis von § 32 Abs. 1 Satz 1 BDSG 2009 durchaus zulässig sein, wenn die Verhältnismäßigkeitsprüfung und die Interessenabwägung zugunsten des Arbeitgebers ausfallen.[55]

Beim Screening kommen dem Email-Screening sowie dem Screening von Internetverkehrsdaten besondere Bedeutung zu. Dabei stellt sich mit aller Brisanz die weder auf der Basis der *lex lata* noch auf der Basis des zukünftigen Rechts gelöste Frage, inwiefern der Arbeitgeber den Bestimmungen des TKG und des TMG unterliegt.[56]

Das Screening soll künftig in § 32 d Abs. 3 und Abs. 5 BDSG geregelt werden. Das geplante Gesetz sieht die Möglichkeit eines zweckgebundenen Datenabgleichs ausdrücklich vor. Der Datenabgleich ist allerdings nur zulässig zur Aufdeckung von Straftaten oder anderen schwerwiegenden Pflichtverletzungen durch Beschäftigte, wie § 32 d Abs. 3 Satz 1 BDSG zeigt.[57] Damit ist die Möglichkeit eines Datenabgleichs nur eröffnet, wenn es um repressive Compliance-Maßnahmen (Aufdeckung) geht. Der Datenabgleich zu *Präventionszwecken* dürfte zukünftig generell ausgeschlossen sein, denn der systematische Zusammenhang von § 32 d Abs. 3 BDSG, d. h. die Einbettung dieses Absatzes in Regelungen zur Zulässigkeit der Datenverarbeitung und der Datennutzung im Beschäftigungsverhältnis, schließt es aus, den Datenabgleich zu Präventionszwecken auf andere Erlaubnisnormen zu stützen. Dieser Totalausschluss der Möglichkeit

---

[53] *Salvenmoser/Hauschka*, NJW 2010, 331, 333.

[54] So aber *Brink/Schmidt*, MMR 2010, 592, 593 f. und S. 596.

[55] *Gola/Wronka*, Handbuch zum Arbeitnehmerdatenschutz, 5. Aufl., 2010, Rdn. 858; *Gola/Schomerus*, BDSG, 10. Aufl., 2010, § 32 Rdn. 25.

[56] Dazu ausführlich *Schmidl*, in: *Hauschka* (Hrsg.), Corporate Compliance, 2. Aufl., 2010, § 29 Rdn. 295 ff.

[57] Kritisch *Beckschulze/Natzel*, Betriebs-Berater 2010, 2368, 2372.

eines Datenabgleichs zu Präventionszwecken ist rechtspolitisch fragwürdig.

Zu begrüßen ist es, dass der geplante § 32 d Abs. 3 Satz 1 BDSG den Datenabgleich in der ersten Ermittlungsstufe nur in anonymisierter oder pseudonymisierter Form zulässt.[58] Auch nach bisheriger Rechtslage gilt für den Datenabgleich, dass er jedenfalls bei Massenscreenings möglichst nicht mit unverschlüsselten Daten stattfinden soll.[59]

Nach § 32 d Abs. 3 Satz 2 BDSG ist eine Personalisierung der Daten im Verdachtsfall möglich. Eine solche Personalisierung dürfte freilich nur bei einer Pseudonymisierung möglich sein, nicht aber bei einer Anonymisierung.[60]

Zu begrüßen ist auch die in § 32 Abs. 3 Satz 3 BDSG enthaltene Dokumentationspflicht.

§ 32 d Abs. 3 Satz 4 BDSG enthält die Pflicht zur Information der Beschäftigten über den Datenabgleich, sobald dessen Zweck durch die Unterrichtung nicht mehr gefährdet wird. Hiermit wird zugleich deutlich, dass ein Datenabgleich ohne Kenntnis der Betroffenen jedenfalls nicht generell ausgeschlossen ist, das Gesetz also über § 32 e BDSG hinaus Fallgruppen der zulässigen Datenerhebung und Datenverarbeitung ohne Kenntnis des Betroffenen kennt.

Erfolgt der Datenabgleich ohne Kenntnis der Beschäftigten, ist schon auf der Basis der *lex lata* eine nachträgliche Unterrichtung geboten, und zwar auf der Grundlage von § 33 BDSG. Hierbei ist § 33 Abs. 3 Nr. 7 BDSG relevant. Demnach kann die Information über den Datenabgleich solange aufgeschoben werden, wie sie die Aufklärung von festgestellten Unregelmäßigkeiten gefährden würde.[61]

Zu begrüßen ist der geplante § 32 d Abs. 5 BDSG, der u. a für den Fall des Datenabgleichs das Verbot der Erstellung eines Persönlichkeitsprofils statuiert.[62] Das entspricht der Einbettung des Datenschutzrechts und insbesondere des Beschäftigtendatenschutzes in die

---

[58] Dazu *Bierekoven*, CR 2010, 203, 207.

[59] *Kock/Francke*, NZA 2009, 646, 648; *Gola/Wronka*, Handbuch zum Arbeitnehmerdatenschutz, 5. Aufl., 2010, Rdn. 859; a. A. *Thüsing*, Arbeitnehmerdatenschutz und Compliance, 2010, Rdn. 154.

[60] *Kock/Francke*, NZA 2009, 646, 648.

[61] *Kock/Francke*, NZA 2009, 646, 650.

[62] *Forst*, NZA 2010, 1043, 1046.

Verfassung. Vor allem Art. 1 GG steht der Erstellung von Persönlichkeitsprofilen in Sinne des „gläsernen Arbeitnehmers" entgegen.[63]

X. Datenübermittlung an externe Ermittler

Die Datenübermittlung an in Deutschland ansässige externe Ermittler sowie die Datenübermittlung durch solche Ermittler lässt sich nach der *lex lata* auf § 28 Abs. 2 Nr. 2 b BDSG stützen,[64] falls nicht sogar eine Auftragsdatenverarbeitung i. S. von § 11 BDSG vorliegt.

Das zukünftige Recht spricht eine Übermittlung von Beschäftigtendaten nur indirekt an, nämlich in § 32 d Abs. 4 BDSG, der die Zweckbindung der Datenverarbeitung durch denjenigen, an den die Daten übermittelt worden sind, vorsieht. Die Datenübermittlung zu Compliance-Zwecken im Allgemeinen oder zur Korruptionsbekämpfung im Besonderen ist im RegE Beschäftigtendatenschutzgesetz nicht angesprochen; sie dürfte daher, soweit sie nicht § 32 d Abs. 1 und 2 BDSG unterfällt, weiterhin unter den Voraussetzungen des § 28 Abs. 2 Nr. 2 b BDSG zulässig sein.

XI. Probleme grenzüberschreitender Ermittlungen

Der RegE Beschäftigtendatenschutzgesetz lässt einen der wichtigsten Punkte des Spannungsverhältnisses zwischen Compliance und Datenschutz ungeregelt, nämlich Fragen des internationalen Datentransfers und die damit einhergehende Frage des Aufeinanderprallens verschiedener Rechtsordnungen mit Anforderungen, die sich nicht gleichzeitig erfüllen lassen (Dilemma-Problematik).

Das gilt insbesondere für Probleme grenzüberschreitender Ermittlungen im Rechtsverkehr zwischen Deutschland und den USA.[65] Betroffen sind nicht nur deutsche Unternehmen, die in den USA tätig sind, sondern auch deutsche Töchter US-amerikanischer Mutterunternehmen.

---

[63] *Schmidl*, in: *Hauschka* (Hrsg.), Corporate Compliance, 2. Aufl., 2010, § 29 Rdn. 302 ff.

[64] *Vogel/Glas*, Der Betrieb 2009, 1747, 1751.

[65] Dazu *Wybitul*, Betriebs-Berater 2009, 606.

Der Datenfluss zwischen Deutschland und den USA richtet sich nach den sehr strengen Voraussetzungen der §§ 4 b und 4 c BDSG.[66] Wie streng die Voraussetzungen sind, lässt sich exemplarisch am Beispiel der *Pre-Trial Discovery* zeigen: So fallen nach einer bedeutenden Auffassung Datenübermittlungen an US-amerikanische Unternehmen im Wege der *Pre-Trial Discovery* im Vorfeld von Rechtsstreitigkeiten grundsätzlich nicht unter § 4 c Abs. 1 Nr. 4 BDSG, weil es sich nicht um die Ausübung oder Verteidigung von Rechtsansprüchen vor einem Gericht handelt.[67]

XII. Internal Investigations

Internal Investigations (unternehmensinterne Ermittlungen) als Compliance-Maßnahmen können sich u. a. auf Ermittlungsmaßnahmen in Hinblick auf den Email-Verkehr erstrecken. Es fragt sich dann, wie sich die Gestattung privater Nutzung des betrieblichen Email-Systems auf die Möglichkeit auswirkt, Ermittlungen durchzuführen, die den Email-Verkehr betreffen. Folgt man der ihrerseits fragwürdigen, aber verbreiteten Meinung, dass bei Gestattung der privaten Nutzung des betrieblichen Email-Systems das TKG und das TMG Anwendung finden können, so ist im Rahmen von Internal Investigations nicht nur eine Durchsuchung privater Emails, sondern oft auch dienstlicher Emails – wegen praktischer Unmöglichkeit getrennter Durchsuchung – problematisch.[68]

Besteht hingegen ein Verbot der privaten Nutzung des betrieblichen Email-Systems, so können nach der *lex lata* Internal Investigations, die sich auf die dienstlichen Emails beziehen, auf § 32 Abs. 1 Satz 2 BDSG gestützt werden, soweit es um repressive Maßnahmen der Aufdeckung von Straftaten geht, und ansonsten auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG.[69] Auf dieser Basis ist nicht nur die Ermittlung von Verbindungsdaten zulässig, sondern auch eine Analyse des Textinhalts, denn dienstliche Emails ähneln nicht etwa dienstlichen Tele-

---

[66] Dazu *Brisch/Laue*, RDV 2010, 1, 6 f.

[67] *Gola/Schomerus*, BDSG, 10. Aufl., 2010, § 4 c Rdn. 7.

[68] *Vogel/Glas*, Der Betrieb 2009, 1747, 1749, 1753; weniger restriktiv *Behling*, Betriebs-Berater 2010, 892.

[69] Ähnlich *Vogel/Glas*, Der Betrieb 2009, 1747, 1749, 1754.

fonaten, sondern gleichen insofern dienstlicher Briefpost.[70] Auf die Überprüfung des Inhalts dienstlicher Emails sind daher nicht die sehr restriktiven Grundsätze über die Überwachung des Inhalts dienstlicher Telefonate anzuwenden.[71]

Nach zukünftigem Recht kann die Überprüfung des dienstlichen Email-Verkehrs sowohl in Hinblick auf Verbindungsdaten als auch in Hinblick auf Inhaltsdaten auf § 32 e BDSG gestützt werden, soweit es um die Aufdeckung oder Verhinderung von Straftaten und anderen schwerwiegenden Pflichtverletzungen geht, und ansonsten – nach wie vor – auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Der geplante § 32 e BDSG schließt nämlich diesbezüglich die Anwendung von § 28 Abs. 1 Nr. 2 BDSG ebenso wenig aus wie § 32 Abs. 1 Satz 2 BDSG in der Fassung von 2009 die Anwendung von § 28 Abs. 1 Nr. 2 BDSG.

Internal Investigations spielen außerdem eine wichtige Rolle im internationalen Rechtsverkehr,[72] insbesondere bei der *Pre-Trial Discovery* und bei der E-Discovery.[73] Bei dem Versuch ausländischer Rechtsordnungen, deutsche Unternehmen zur Durchführung von Internal Investigations zu verpflichten, sind die deutschen und europäischen datenschutzrechtlichen Grenzen für die Durchführung solcher Internal Investigations zu beachten. Das Datenschutzrecht kann Grenzen setzen, die mit den Internal Investigations-Pflichten meist US-amerikanischer Provenienz kollidieren.[74] Eine Lösung solcher Konflikte strebt der RegE Beschäftigtendatenschutzgesetz nicht an.

XIII. Mitarbeiterbefragung

Datenschutzrechtliche Probleme der Mitarbeiterbefragung als besonderer Form der Internal Investigations sind bislang weitgehend ungelöst.[75] Sie werden auch nicht im RegE Beschäftigtendatenschutzgesetz gesondert angesprochen. § 32 Abs. 2 BDSG 2009 hat mit dem

---

[70] *Gola/Wronka*, Handbuch zum Arbeitnehmerdatenschutz, 5. Aufl., 2010, Rdn. 787; *Wolf/Mulert*, Betriebs-Berater 2008, 442, 443.

[71] So zutreffend *Vogel/Glas*, Der Betrieb 2009, 1747, 1754.

[72] *von Rosen*, Betriebs-Berater 2009, 230; *Wagner*, CCZ 2009, 8.

[73] *Brisch/Laue*, RDV 2010, 1; *Spies/Schröder*, MMR 2008, 275; *Gola/Schomerus*, BDSG, 10. Aufl., 2010, § 4 c Rdn. 7.

[74] *Brisch/Laue*, RDV 2010, 1, 3; *Spies/Schröder*, MMR 2008, 275, 277 ff.

[75] *Vogel/Glas*, Der Betrieb 2009, 1747, 1749.

Verzicht auf das Dateierfordernis das persönliche Mitarbeitergespräch für die Anwendung von § 32 BDSG 2009 datenschutzrechtlich relevant gemacht.[76] Wenn es um die Aufdeckung von Straftaten geht, sind demgemäß auf der Basis der *lex lata* bei der Mitarbeiterbefragung die strengen Voraussetzungen von § 32 Abs. 1 Satz 2 BDSG einzuhalten. Problematisch ist dabei insbesondere, dass nur Ermittlungen bei dem Verdächtigen möglich sind, nicht aber bei anderen Mitarbeitern. Die Möglichkeit eines Rückgriffs auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG für die Befragung nicht verdächtiger Mitarbeiter zur Aufdeckung von Straftaten[77] ist jetzt und auch in Zukunft ungesichert.

Nach dem RegE Beschäftigtendatenschutzgesetz dürfte die Mitarbeiterbefragung ohne Kenntnis des Beschäftigten, um dessen Verhalten es geht, nunmehr bei repressiven und präventiven Maßnahmen dem engen Anwendungsbereich des § 32 e BDSG unterfallen, auf die Mitarbeiterbefragung mit Kenntnis des Betroffenen dürfte § 32 c Abs. 1 Nr. 3 BDSG Anwendung finden. Ausdrücklich angesprochen werden solche Mitarbeiterbefragungen jedoch im RegE Beschäftigtendatenschutzgesetz nicht.

XIV. Fehlen einer datenschutzrechtlichen Regelung des Whistleblowing

Ein wichtiger Aspekt des Spannungsverhältnisses zwischen Compliance und Datenschutz ist das Whistleblowing.[78] Gegenstand des Whistleblowing sind gegen Gesetz und Recht oder sonstige Regeln oder Standards verstoßende Handlungsweisen von unternehmensangehörigen Personen.[79] Es ist bekanntlich zwischen dem internen Whistleblowing als unternehmensinterner Offenlegung dieser Rechts- und Regelverstöße und dem externen Whistleblowing zu unterscheiden, bei dem sich Arbeitnehmer an Behörden oder Medien wenden.[80]

---

[76] *Vogel/Glas*, Der Betrieb 2009, 1747, 1750.
[77] So *Vogel/Glas*, Der Betrieb 2009, 1747, 1750.
[78] Dazu allg. *Bürkle*, Der Betrieb 2004, 2158.
[79] Näher *Kort*, in: FS Kreutz, 2010, S. 247.
[80] Näher *Kort*, in: FS Kreutz, 2010, S. 247 f.; *Weber-Rey*, AG 2006, 406, 407.

Strittig ist, ob eine gesetzliche Regelung des Whistleblowing anzustreben ist.[81] Zur Beantwortung dieser Frage ist es sinnvoll zu differenzieren: Beim Whistleblowing stellen sich zum einen individualarbeitsvertragliche Fragen des Rechts und ggf. der Pflicht des Arbeitnehmers zum Whistleblowing, zum anderen kollektivarbeitsrechtliche Fragen der Mitbestimmung des Betriebsrats bei der Absicht des Arbeitgebers, das Whistleblowing, etwa in Richtlinien[82] oder durch Etablierung einer Whistleblowing-Hotline,[83] kollektiv zu regeln.

Was die betriebsverfassungsrechtliche Seite des Whistleblowing betrifft, ist eine gesetzliche Regelung des Whistleblowing überflüssig. Es bedarf keines neuen Mitbestimmungstatbestands in § 87 BetrVG. Vielmehr ist die Rechtsprechung hierzu bereits wegweisend, insbesondere der *Honeywell*-Beschluss des BAG aus dem Jahr 2008.[84]

Weniger eindeutig zu beantworten ist die Frage, ob die gesetzliche Regelung individualarbeitsrechtlicher Fragen des Whistleblowing Sinn machen würde. Im Jahr 2008 wurde mit einem geplanten neuen § 612 a BGB das Konzept einer inzwischen „auf Eis gelegten" bürgerlichrechtlichen Whistleblowing-Norm präsentiert. Die geplante Norm sah eine recht detaillierte Regelung sowohl des internen als auch des externen Whistleblowing vor. Das Gesetzesvorhaben wurde teilweise heftig mit dem Argument kritisiert, es bedürfe angesichts der klaren Rechtsprechung einer solchen gesetzlichen Regelung nicht.[85]

Dieser Kritik ließ und lässt sich freilich entgegenhalten, dass die Rechtsprechung des BAG[86] und des BVerfG[87] nur unter gewissen Aspekten und überdies in teilweise uneinheitlicher Weise die individualarbeitsrechtlichen Probleme des Whistleblowing behandelt hat.[88]

Im hier interessierenden Zusammenhang soll der Frage nach Sinn oder Unsinn einer umfassenden gesetzlichen Regelung der indivi-

---

[81] Näher *Kort*, in: FS Kreutz, 2010, S. 247, 251 ff.; dezidiert gegen eine gesetzliche Regelung des Whistleblowing *Weber-Rey*, AG 2006, 406, 408 f.

[82] Dazu *Kort*, in: FS Buchner, 2009, S. 477.

[83] Dazu *Behrendt/Kaufmann*, CR 2006, 642.

[84] *BAG*, NZA 2008, 1248; dazu *Kort*, NJW 2009, 129; ferner *Fahrig*, NZA 2010, 1223.

[85] Nachweise bei *Kort*, in: FS Kreutz, 2010, S. 247, 252 unter Fn. 22.

[86] BAG, NZA 2004, 427; *BAG*, NZA 2007, 502.

[87] BVerfG, NJW 2001, 3474.

[88] Dazu näher *Kort*, in: FS Kreutz, 2010, S. 247, 253 ff.

dualarbeitsvertraglichen Aspekte des Whistleblowing nicht erneut nachgegangen werden. Vielmehr soll lediglich die Frage angesprochen werden, ob die spezifisch datenschutzrechtliche Behandlung des Whistleblowing im geplanten Beschäftigtendatenschutzgesetz Sinn machen würde.

Whistleblowing wird im RegE Beschäftigtendatenschutzgesetz nicht explizit angesprochen. Das ist sehr bedauerlich, denn die datenschutzrechtliche Behandlung des Whistleblowing ist eine der großen Streitfragen des Spannungsverhältnisses zwischen Compliance und Datenschutz. So liegt etwa auf europäischer Ebene eine Stellungnahme der sog. Artikel-29-Gruppe zu Datenschutzaspekten des Whistleblowing aus dem Jahr 2006[89] vor. Dort wird zutreffend Art. 7 (f) EG-Datenschutzrichtlinie als Grundlage für die Etablierung eines datenschutzrechtlich zulässigen Whistleblowing-Systems genannt. Demgemäß können etwa die Ziele des US-amerikanischen *Sarbanes-Oxley Act* Basis gerechtfertigter Interessen des Arbeitgebers an der Datenverarbeitung beim Whistleblowing sein.[90]

Die Etablierung von Whistleblowing-Systemen und die sonstige Handhabung des Whistleblowing im Unternehmen stoßen auf datenschutzrechtliche Grenzen.[91] Hierbei geht es sowohl um datenschutzrechtliche Belange des Meldenden als auch des Gemeldeten. Auch sind verfassungsrechtlich gewährte Rechtspositionen der Beteiligten bei Etablierung von Whistleblowing-Systemen zu beachten, etwa das Allgemeine Persönlichkeitsrecht des Gemeldeten.[92]

Probleme bereitet die Gewichtung der unterschiedlichen Rechtspositionen etwa bei der Frage, ob die Möglichkeit anonymer Meldungen nur eingeschränkt eingeräumt werden kann[93] oder umgekehrt gerade geboten ist.[94] International kann das Aufeinanderprallen US-amerikanischer Vorgaben, die eine Pflicht zur Etablierung von Whistleblowing-Systemen vorsehen,[95] mit deutschem und europäi-

---

[89] Stellungnahme 1/2006, WP 117; dazu *Schmidl*, DuD 2006, 414.

[90] *Schmidl*, DuD 2006, 414, 418.

[91] Dazu instruktiv *Schmidl*, in: *Hauschka* (Hrsg.), Corporate Compliance, 2. Aufl., 2010, § 29 Rdn. 276 ff., ferner *Mahnhold*, NZA 2008, 737 sowie *Behrendt/Kaufmann*, CR 2006, 642, 645 ff.

[92] *Mahnhold*, NZA 2008, 737, 738 f.

[93] So etwa *Breinlinger/Krader*, RDV 2006, 60, 65.

[94] *Gola/Wro*nka, Handbuch zum Arbeitnehmerdatenschutz, 5. Aufl., 2010, Rdn. 673; *Gola/Schomerus*, BDSG, 10. Aufl., 2010, § 4 Rdn. 27 a.

[95] Dazu *Breinlinger/Krader*, RDV 2006, 60, 61 ff.

schem Datenschutzrecht zu Jurisdiktionskonflikten führen.[96] Insbesondere kann das Whistleblowing dann datenschutzrechtlich problematisch sein, wenn es um Meldungen an die Muttergesellschaft im Ausland geht.[97]

Der RegE Beschäftigtendatenschutzgesetz spricht indes allenfalls indirekt Fragen des Whistleblowing an, und zwar in § 32 d BDSG und § 32 e BDSG. Hieraus lassen sich aber weder für die datenschutzrechtliche Position des Whistleblowers noch für die datenschutzrechtliche Position des Gemeldeten konkrete Schlüsse ziehen, ein großes Manko des RegE Beschäftigtendatenschutzgesetzes!

XV. Fehlen von Neuregelungen zur konzernweiten Datenverarbeitung sowie zur Auftragsdatenverarbeitung

Die Konzernverflechtung deutscher Unternehmen ist ein bekanntes Phänomen, insbesondere auch die internationale Konzernverflechtung. Compliance-Anforderungen enden oft nicht an der Unternehmensgrenze, sondern sind häufig konzernbezogen. Der Konzernbezug von Compliance-Anforderungen legt es nahe, dass zur Erfüllung von Compliance-Pflichten ein unternehmensübergreifender Fluss von Daten im Konzern oder auch eine unternehmensübergreifende, konzernweite Datenerhebung stattfindet.

Bei Konzernsachverhalten gilt angesichts des Fehlens eines datenschutzrechtlichen „Konzernprivilegs" für konzernangehörige Unternehmen, dass der Datenfluss zwischen ihnen im Grundsatz als Datenübermittlung zu betrachten ist. Datenschutzrechtlich werden also die konzernangehörigen Unternehmen als verschiedene „Stellen" angesehen.

Die auch im Konzern bestehende Möglichkeit der Etablierung einer Auftragsdatenverarbeitung gemäß § 11 BDSG hilft nur beschränkt über die Klippe des Fehlens eines Konzernprivilegs hinweg.[98] Zum einen waren die Anforderungen an eine Auftragsdatenverarbeitung nach § 11 BDSG schon immer recht hoch und sind mit der BDSG-Novelle 2009 noch einmal gestiegen, zum anderen ist eine

---

[96] *Mahnhold*, NZA 2008, 737, 741 ff.

[97] *Schmidl*, in: *Hauschka* (Hrsg.), Corporate Compliance, 2. Aufl., 2010, § 29 Rdn. 289.

[98] *Thüsing*, RDV 2010, 147, 149.

Auftragsdatenverarbeitung unter Beteiligung eines US-amerikanischen Unternehmens nach h. M. angesichts von § 3 Abs. 8 Satz 3 BDSG nicht etablierbar.

Die Starrheit der Sicht, dass konzernangehörige Unternehmen datenschutzrechtlich genauso wie voneinander völlig unabhängige Unternehmen behandelt werden, ist insbesondere von der Praxis häufig beklagt worden.

Zwar bestehen Bedenken vor einem ungehemmten konzerninternen Personaldatenfluss, die durchaus berechtigt sind. Jedoch fragt sich, ob nicht eine „Mittellinie", die gewisse Vorkehrungen für den Datenfluss zwischen konzernangehörigen Unternehmen trifft, dennoch aber ein beschränktes Konzernprivileg gewährt, nicht besser wäre als die rigorose *lex lata*. Anhaltspunkte für die gesetzliche Gestaltung einer solchen „Mittellinie" könnte § 11 BDSG bieten, also die Norm über die Auftragsdatenverarbeitung. Allerdings dürften die rigorosen und 2009 noch einmal verschärften Anforderungen an die Auftragsdatenverarbeitung nicht 1:1 auf ein beschränktes Konzernprivileg übertragen werden. Eine gesetzliche Regelung eines beschränkten Konzernprivilegs dürfte auf keinen Fall zu einer bloßen gesetzlichen „Zementierung" des in der Praxis zur Zeit häufig gewählten *exits* führen, die Rechtsfolgen einer Art von Konzernprivileg bereits auf der Basis der *lex lata* dadurch zu erreichen, dass man mehr oder minder „künstlich" ein Auftragsdatenverarbeitungsverhältnis zwischen zwei konzerngebundenen Unternehmen konstruiert.

Eine gesetzliche Regelung der konzernweiten Datenerhebung und des konzernweiten Datenflusses sieht jedoch die geplante Regelung des Beschäftigtendatenschutzes nicht vor. Entsprechende Vorschläge der Praxis und der Wissenschaft wurden nicht aufgegriffen, auch nicht der Vorschlag, wenigstens in § 28 BDSG aufzunehmen, dass bei der Abwägung der beiderseitigen Interessen auch Konzernbelange berücksichtigt werden können.[99]

„Abhilfe" hatten bislang teilweise Konzernbetriebsvereinbarungen geschaffen, die Regelungen zur Datenerhebung und Datenverarbeitung im Konzern zum Gegenstand hatten.[100] Fraglich ist jedoch, ob angesichts des geplanten § 32 l Abs. 5 BDSG, wonach von den Vorschriften des betreffenden Unterabschnitts (d. h. von §§ 32 ff. BDSG) nicht zu Ungunsten der Beschäftigten abgewichen werden

[99] *Thüsing*, RDV 2010, 147, 149.

[100] Dazu etwa *Thüsing*, RDV 2010, 147, 148.

darf, in Zukunft noch im selben Umfang von solchen Konzernbetriebsvereinbarungen Gebrauch gemacht werden kann.

Weitere Fragen stellen sich bei international operierenden Konzernen. Wenn ein Datentransfer in ein Land außerhalb des EU/EWR-Raums stattfindet, unterliegt dieser Datentransfer den besonders strengen datenschutzrechtlichen Vorgaben der §§ 4 b und 4 c BDSG.[101] Auch ist in solchen Fällen § 3 Abs. 8 Satz 3 BDSG zu bedenken.[102]

Angesichts der zunehmenden Internationalisierung von Konzernaktivitäten besteht aber ein Bedürfnis der Praxis, auch diesbezüglich gesetzliche Lockerungen vorzusehen, soweit ein angemessenes Datenschutzniveau in dem betreffenden Land gesichert ist. Allerdings hätte der deutsche Gesetzgeber bei solchen Lockerungen die Vorgaben der EU-Datenschutzrichtlinie zu beachten (Art. 25 und 26).

Neue Regelungen zum internationalen Datentransfer enthalten die geplanten Normen zum Beschäftigtendatenschutz indes nicht.

XVI. Zukünftige Bedeutung von Betriebsvereinbarungen

Zu begrüßen ist, dass § 4 Abs. 1 BDSG ein klarstellender Satz angefügt werden soll, dass auch Betriebsvereinbarungen „andere Rechtsvorschriften" im Sinn des BDSG, also andere datenschutzrechtliche Erlaubnisnormen, sein können.

Isoliert betrachtet handelt es sich bei diesem Zusatz bloß um eine normative Festschreibung der Rechtsprechung und einhelligen Auffassung in der Literatur, dass Betriebsvereinbarungen diese Qualität zukommt. Jedoch hat der geplante Zusatz in § 4 Abs. 1 BDSG im Kontext mit dem geplanten § 32 l Abs. 5 BDSG Bedeutung.

U. a. Betriebsvereinbarungen sind nämlich gemeint, wenn es in § 32 l Abs. 5 BDSG heißt, dass von den Vorschriften der §§ 32 ff. BDSG nicht zu Ungunsten der Beschäftigten abgewichen werden kann.

Diese neue Bestimmung ist nicht unproblematisch. 1986 hatte das BAG[103] entschieden, dass Betriebsvereinbarungen von den Bestimmungen des BDSG auch *zu Ungunsten* der Arbeitnehmer abweichen

---

[101] *Vogel/Glas*, Der Betrieb 2009, 1747, 1748 f.

[102] So etwa *Vogel/Glas*, Der Betrieb 2009, 1747, 1748.

[103] BAG, NZA 1986, 643, 646 f.

können. Diese Entscheidung des BAG wurde und wird in der Literatur zu Recht kritisiert,[104] insbesondere, weil sie dem Betriebsrat eine Art von Ersatzgesetzgeberfunktion auf dem Gebiet des Datenschutzrechtsrechts einräumt, die ihm nicht zukommt.

Seit 1986 hat das BAG nicht mehr zu dieser strittigen Thematik Stellung genommen. Die Literatur hat im Lauf der Zeit herausgearbeitet, dass Betriebsvereinbarungen angesichts von § 75 BetrVG nicht in das Persönlichkeitsrecht der Arbeitnehmer eingreifen dürfen und demgemäß das Schutzniveau des BDSG jedenfalls nicht wesentlich unterschreiten dürfen.[105] Es entspricht heute h. M., dass Betriebsvereinbarungen zwar Einzelheiten der Datenverarbeitung abweichend vom BDSG regeln können, aber nicht in grundsätzlicher Weise die datenschutzrechtliche Position der Beschäftigten beeinträchtigen dürfen.

Modifikationen sind also erlaubt, wesentliche Unterschreitungen des datenschutzrechtlichen Niveaus hingegen nicht. Die Crux besteht darin, Modifikationen von solchen wesentlichen Unterschreitungen abzugrenzen. Auf der Basis der Rechtsprechung des BAG durfte man bislang den Betriebspartnern eine Einschätzungsprärogative zubilligen, was noch als Modifikation der Bestimmungen des BDSG und noch nicht als Niveauunterschreitung gelten kann.

Fraglich ist, ob der geplante § 32 l Abs. 5 BDSG mit seiner pauschalen Aussage: „...darf nicht zu Ungunsten der Beschäftigten abgewichen werden..." generell auch noch so geringfügige Unterschreitungen des Datenschutzniveaus des BDSG durch eine Betriebsvereinbarung ausschließt. Das dürfte trotz des Wortlauts der Norm nicht der Fall sein, da eine Zusammenschau des geplanten § 4 Abs. 1 Satz 2 BDSG und des geplanten § 32 l Abs. 5 BDSG zeigt, dass Betriebsvereinbarungen durchaus datenschutzrechtliche Maßnahmen erlauben können, die ohne die entsprechende Betriebsvereinbarung nicht zulässig wären.

Es dürfte sich daher am bisherigen Verständnis der Funktion einer Betriebsvereinbarung für den Beschäftigtendatenschutz nichts ändern, auch wenn der Wortlaut von § 32 l Abs. 5 BDSG Anderes nahelegt. Angesichts des geplanten § 4 Abs. 1 Satz 2 BDSG zeigt sich bei näherer Betrachtung, dass die bislang offene Frage der Zulässig-

---

[104] Kritisch in jüngerer Zeit etwa *Brandt*, DuD 2010, 213.

[105] *Gola/Schomerus*, BDSG, 10. Aufl., 2010, § 4 Rdn. 10; im Ergebnis auch *Brandt*, DuD 2010, 213, 215.

keit einer modifzierend-moderaten Unterschreitung des BDSG-Datenschutzniveaus durch eine Betriebsvereinbarung[106] weiterhin offen ist.

So dürfte nach wie vor etwa zulässig sein, die betriebliche und private Nutzung betrieblicher Kommunikationstechniken in einer Betriebsvereinbarung[107] derart zu regeln, dass die Regelung der Kontrollmöglichkeiten des Arbeitgebers die diesbezüglichen Vorgaben des BDSG zwar im Sinn einer Erweiterung der Kontrollmöglichkeiten modifizieren, gesichert ist das freilich angesichts des geplanten § 32 l Abs. 5 BDSG nicht.[108]

Zu beachten ist insbesondere, dass schon nach bisherigem Verständnis von § 4 Abs. 1 BDSG und erst recht angesichts des zukünftigen Wortlauts von § 4 Abs. 1 BDSG Betriebsvereinbarungen als datenschutzrechtlicher Erlaubnistatbestand in Betracht kommen können. Es fragt sich, wie eine solche Möglichkeit bestehen soll, wenn die Betriebsvereinbarung nicht – wenn auch nur geringfügig – das vorgegebene datenschutzrechtliche Niveau des BDSG unterschreiten kann. Jeder Erlaubnistatbestand unterschreitet nämlich insofern das Niveau des BDSG, als ohne den Erlaubnistatbestand ein Verbot der Datenverarbeitung bestünde. Aus einer Gesamtschau des geplanten § 4 Abs. 1 BDSG und des geplanten § 32 l Abs. 5 BDSG dürfte sich daher ein einschränkendes Verständnis von § 32 l Abs. 5 BDSG ergeben.

XVII. Einwilligung

Die Einwilligung des Beschäftigten kann bei datenschutzrechtlich relevanten Compliance-Maßnahmen von Bedeutung sein.[109] Die Funktion der Einwilligung des Beschäftigten für die datenschutzrechtliche Zulässigkeit der Datenerhebung und Datenverarbeitung war bislang schon umstritten. Zwar sieht das geltende Recht die Einwilligung in §§ 4 und 4 a BDSG ausdrücklich vor. Jedoch ist die Einwilligung beim Beschäftigungsverhältnis auf der Basis der *lex*

---

[106] Dazu *Thüsing*, RDV 2010, 147.

[107] Dazu *Gola/Wronka*, Handbuch zum Arbeitnehmerdatenschutz, 5. Aufl., 2010, Rdn. 796 ff.; BT-Drucks. 16/13657, S. 34.

[108] Zu Recht kritisch gegenüber § 32 l Abs. 5 BDSG *Beckschulze/Natzel*, Betriebs-Berater 2010, 2368 f.; *Franzen*, RdA 2010, 257, 260; *Thüsing*, NZA 2011, 16, 18; anders hingegen *Tinnefeld/Petri/Brink*, MMR 2010, 727, 729.

[109] *Vogel/Glas*, Der Betrieb 2009, 1747, 1748.

lata besonders problematisch. Dies betrifft insbesondere die Freiwilligkeit der Einwilligung des Arbeitnehmers sowie die praktische Bedeutung der Einwilligung für den Arbeitgeber, der regelmäßig auf eine *durchgängige Einwilligungserteilung* durch sämtliche Beschäftigte angewiesen ist. Letzteres ist gerade angesichts der Freiwilligkeit der Einwilligung sowie ihrer praktisch jederzeitigen Widerruflichkeit sehr problematisch. Selbst wenn dem Arbeitgeber jedoch durchgängig eine Einwilligung erteilt wird, besteht die Gefahr, dass die Einwilligung unwirksam ist.

Teilweise wurde und wird die Einwilligung daher als völlig untaugliches Instrument im Bereich des Beschäftigtendatenschutzes angesehen.

Die geplante gesetzliche Neuregelung der Einwilligung beim Beschäftigungsverhältnis hinterlässt einen zwiespältigen Eindruck. § 32 l Abs. 1 BDSG geht wie selbstverständlich davon aus, dass es eine datenschutzrechtlich relevante Einwilligung auch beim Beschäftigungsverhältnis gibt. Allerdings soll die Einwilligung nicht generell als Erlaubnistatbestand i. S. von § 4 BDSG in Betracht kommen, sondern abweichend von § 4 BDSG nur dann, soweit sie in den Normen zum Beschäftigtendatenschutz ausdrücklich zugelassen ist. Es handelt sich also um einen *numerus clausus* von Einwilligungsfällen. Es fragt sich, ob dieser Kreis einwilligungsfähiger Fälle nicht zu klein ist, etwa bei konzernweiter Datenverarbeitung.[110]

Angesichts der praktischen Bedenken, die schon bislang gegen die Einwilligung als Erlaubnistatbestand sprechen, und angesichts der engen Voraussetzungen für die Einwilligung in der geplanten gesetzlichen Regelung kommt die Einwilligung zukünftig allenfalls subsidiär als Erlaubnistatbestand in Betracht. Die Einwilligung ist als Erlaubnistatbestand in Art. 7 (a) der EU-Datenschutzrichtlinie ausdrücklich genannt. Es bestehen daher Bedenken, ob die nunmehr vorgesehene Beschränkung der Einwilligung beim Beschäftigungsverhältnis auf bestimmte Fallgruppen europarechtskonform ist.[111]

Gegenüber einer Einengung der Einwilligung auf bestimmte Fallgruppen wäre es vorzugswürdig, im Gesetz beschäftigungsverhältnisspezifische inhaltliche und formale Voraussetzungen für die Beschäftigten-Einwilligung aufzustellen, die in Umsetzung der EU-Daten-

---

[110] So *Beckschulze/Natzel*, Betriebs-Berater 2010, 2368, 2374.

[111] *Forst*, RDV 2010, 150; *ders.*, NZA 2010, 1043, 1044; *Thüsing*, RDV 2010, 147, 148 f.; *ders.*, NZA 2011, 16, 18.

schutzrichtlinie dafür sorgen, dass zumindest eine gewisse Gewähr für die Freiwilligkeit der Beschäftigten-Einwilligung besteht.[112]

XVIII. Erstreckung des Beschäftigungsdatenschutzes auf nicht automatisierte Daten

Der geplante § 27 Abs. 3 BDSG erstreckt zukünftig sämtliche Normen des Beschäftigtendatenschutzes auch auf nicht automatisierte Daten, also z. B. auch auf den Umgang mit papierbezogenen Beschäftigungsdaten. Das ist angesichts des Persönlichkeitsschutzes der Beschäftigten, wie er etwa in § 75 Abs. 2 BetrVG zum Ausdruck kommt, insgesamt eine positiv zu bewertende Fortschreibung von § 32 Abs. 2 BDSG 2009.[113]

XIX. Erfüllung rechtspolitischer Forderungen durch die geplante Neuregelung des Beschäftigtendatenschutzes?

In summa stellt sich die Frage, ob die geplante Neuregelung des Beschäftigtendatenschutzes den rechtspolitischen Forderungen nach Auflösung des Spannungsverhältnisses von Compliance-Anforderungen und einem ausreichenden Beschäftigtendatenschutz gerecht wird.

1. Berücksichtigung beider Pole des Spannungsverhältnisses

Teilweise betonen die rechtspolitischen Forderungen zu stark nur *einen* Pol dieses Spannungsverhältnisses. So tritt das *Eckpunktepapier* der Datenschutzbeauftragten für eine Modernisierung des Datenschutzrechts aus dem Jahr 2010 zwar für eine umfassende Verstärkung des Datenschutzes ein. Hinweise, wie zunehmenden Compliance-Anforderungen Genüge getan werden kann, finden sich dort aber nicht. Vielmehr heißt es sehr pauschal und allgemein, es sei höchste Zeit, den Bürger wieder zum „Herrn seiner Daten" zu machen.[114] Der

[112] Dazu im einzelnen *Forst*, RDV 2010, 150, 154 sowie *Thüsing*, RDV 2010, 147, 148 f.

[113] Kritisch hingegen *Beckschulze/Natzel*, Betriebs-Berater 2010, 2368: Unnötiges Hinausgehen über die europäische Datenschutzrichtlinie; kritisch schon zu § 32 Abs. 2 BDSG *Deutsch/Diller*, Der Betrieb 2009, 1462.

[114] Eckpunktepapier, RDV 2010, 189.

RegE Beschäftigtendatenschutzgesetz hingegen bemüht sich, beide Pole des Spannungsverhältnisses zu berücksichtigen.

2. Beziehung des Beschäftigtendatenschutzes zum allgemeinen Datenschutz

Zu Recht nimmt der RegE Beschäftigtendatenschutzgesetz davon Abstand, den Beschäftigtendatenschutz in einem eigenen Gesetz zu behandeln. Aufgrund der engen Verzahnung des Beschäftigtendatenschutzes mit anderen datenschutzrechtlichen Gebieten und Themen ist die Einbettung des Beschäftigtendatenschutzes in das allgemeine Datenschutzrecht eine richtige gesetzgeberische Entscheidung.[115]

Allerdings bestehen erhebliche Zweifel, ob diese Einbettung im Einzelnen gelungen ist. Insgesamt erwecken die geplanten §§ 32 ff. BDSG den Eindruck zu vieler und zu langer Normen. Auch wird der Bezug zum allgemeinen Datenschutz nicht immer deutlich. So richten sich berechtigte rechtspolitische Forderungen etwa auf eine zukünftige Klarstellung des Verhältnisses von § 28 BDSG zum Beschäftigtendatenschutz,[116] und zwar sowohl für präventive als auch für repressive Compliance-Maßnahmen, soweit diese datenschutzrechtlich relevant sind. Diese Klarstellung ist, wie aufgezeigt, nicht oder jedenfalls nicht ausreichend genug erfolgt.

3. Whistleblowing

Besonders bedauerlich ist, dass das Gesetzesvorhaben keinerlei Aussage zur datenschutzrechtlichen Zulässigkeit des Whistleblowing enthält, obwohl das ein Kernbestandteil des Spannungsverhältnisses von Compliance und Datenschutz ist. Rechtspolitische Forderungen nach Regelung des Whistleblowing[117] bleiben somit unerfüllt. Hingegen sieht etwa der DGB-Entwurf für ein Arbeitnehmerdatenschutzgesetz von 2010 eine wenn auch zu knapp geratene und damit letztlich nicht befriedigende Regelung des externen Whistleblowing vor.[118]

---

[115] *Thüsing*, RDV 2010, 147.
[116] *Gola*, RDV 2010, 97, 98.
[117] *Gola*, RDV 2010, 97, 99.
[118] DGB-Entwurf, AuR 2010, 315, 317, § 9.

4. Mitarbeiterüberwachung

Forderungen nach einer umfassenden und einheitlichen Regelung der offenen und der verdeckten Mitarbeiterüberwachung[119] erfüllt der RegE Beschäftigtendatenschutzgesetz nur teilweise. So sind repressive und präventive Compliance-Maßnahmen nur partiell in § 32 e BDSG angesprochen, die Videoüberwachung ist in § 32 f BDSG ebenfalls nicht umfassend geregelt.

Zu begrüßen ist, dass sich der RegE Beschäftigtendatenschutzgesetz nicht für ein rechtspolitisch vorgeschlagenes umfassendes Verbot von Video- und Tonbandaufnahmen[120] ausgesprochen hat. Videoaufzeichnungen unter Wahrung des Gebots der Verhältnismäßigkeit dienen einer Erfüllung von Compliance-Anforderungen. Dies gilt insbesondere für die in § 32 e Abs. 3 BDSG angesprochene Aufdeckung und Verhinderung von Straftaten und schwerwiegenden Pflichtverstößen.

5. Beweisverwertungsverbote

Rechtspolitischen Forderungen nach gesetzlicher Festschreibung von Beweisverwertungsverboten bei unrechtmäßiger Datenerhebung oder Datenverarbeitung[121] kommt die geplante gesetzliche Neuregelung zu Recht nicht nach. Im Einzelfall mögen sich auf der Basis der Rechtsprechung des BAG aus schweren Verstößen gegen datenschutzrechtliche Normen, die zugleich einen schwerwiegenden Eingriff in das Persönlichkeitsrecht des betroffenen Arbeitnehmers bilden, Beweisverwertungsverbote ergeben. Dabei macht die Rechtsprechung aber zutreffend deutlich, dass weder aus bloßen datenschutzrechtlichen Verstößen (ohne schwerwiegenden Eingriff in das Persönlichkeitsrecht) noch aus dem bloßen Fehlen der betriebsverfassungsrechtlichen Mitbestimmung ein prozessuales Beweisverwertungsverbot resultiert.[122]

---

[119] *Gola*, RDV 2010, 97, 99.

[120] So die *Deutsche Vereinigung für Datenschutz und andere*, Kritik am Eckpunktepapier der *Bundesregierung*, AuR 2010, 314.

[121] So die Kritik der *Deutschen Vereinigung für Datenschutz und anderer*, Kritik am Eckpunktepapier der *Bundesregierung*, AuR 2010, 314; auch *Tinnefeld/Petri/Brink*, MMR 2010, 727, 732.

[122] BAG, NZA 2008, 1008; *LAG Hamm*, RDV 2005, 170; s. auch *Kock/Francke*, NZA 2009, 646, 651 sowie *Bayreuther*, NZA 2005, 1038, 1043; *Dzida/Grau*, NZA 2010, 1201.

Eine umfassende gesetzliche Anordnung von Beweisverwertungsverboten wäre nicht sachdienlich.

6. Privatnutzung von Telekommunikationseinrichtungen

Das der Praxis auf den Nägeln brennende Thema der Stellung des Arbeitgebers bei der erlaubten Privatnutzung von E-Mail und Internet ist im RegE Beschäftigtendatenschutzgesetz ebenfalls nicht geregelt, obwohl es diesbezüglich deutliche rechtspolitische Forderungen gibt.[123] Es wäre sinnvoll gewesen, wenn der Gesetzesentwurf entgegen der heute auf der Basis des geltenden Rechts gebildeten h. M. klarstellen würde, dass der Arbeitgeber kein Diensteanbieter im Sinn der Telekommunikationsgesetzgebung ist, wenn er die private Email-Nutzung oder die private Internetnutzung erlaubt.[124]

7. Konzernverbindungen

Ferner fehlt im RegE Beschäftigtendatenschutzgesetz trotz entsprechender rechtspolitischer Forderungen jegliche Regelung des praxisrelevanten Personaldatenflusses bei Konzernverbindungen.[125]

Hingegen ist die rechtspolitische Forderung nach *gesetzlicher Präzisierung* der berechtigten Interessen des Arbeitgebers an einer konzernweiten Verarbeitung von Beschäftigungsdaten[126] im RegE Beschäftigtendatenschutzgesetz zu Recht nicht erfüllt worden. Eine solche Präzisierung von Arbeitgeberinteressen ist wegen ihrer starken Einzelfallorientierung im Gesetz nicht möglich.

8. Auftragsdatenverarbeitung und DV-Outsourcing

Wie bereits ausgeführt, wäre eine gesetzliche *Erweiterung* der Möglichkeit zur Auftragsdatenverarbeitung durchaus sinnvoll. Hierzu schweigt der RegE Beschäftigtendatenschutzgesetz leider.

---

123 *Gola*, RDV 2010, 97, 99.

124 So der Vorschlag der *Deutschen Vereinigung für Datenschutz und anderer*, Kritik am Eckpunktepapier der *Bundesregierung*, AuR 2010, 314.

125 Dazu *Gola*, RDV 2010, 97, 99; *Forst*, NZA 2010, 1043, 1048; ferner dazu das BDA-Positionspapier „Datenschutz im Arbeitsverhältnis ausgewogen und rechtssicher gestalten" von Februar 2010.

126 *Deutsche Vereinigung für Datenschutz und andere*, Kritik am Eckpunktepapier der *Bundesregierung*, AuR 2010, 314.

Zu begrüßen ist, dass der RegE Beschäftigtendatenschutzgesetz nicht umgekehrt auf eine weitere *Verengung* der Möglichkeit zur Auftragsdatenverarbeitung eingeht, wie sie für die Auftragsdatenverarbeitung im Konzern etwa von der *Deutschen Vereinigung für Datenschutz und anderen* vorgeschlagen worden ist.[127]

Auch ist es richtig, dass der RegE Beschäftigtendatenschutzgesetz nicht der ihrerseits unklaren Forderung nachkommt, bei Einschaltung eines externen Dienstleisters sollten Verbote und Informationspflichten, die für den Arbeitgeber gelten, auch beim Einsatz externer Diensteanbieter einzuhalten sein.[128] Ist der externe Diensteanbieter Auftragnehmer im Sinn von § 11 BDSG, bleibt im Wesentlichen der Auftraggeber verantwortlich. Liegt hingegen ein Datenverarbeitungs-Outsourcing vor, ohne dass die Voraussetzungen der Auftragsdatenverarbeitung gegeben sind, z. B. bei einer Funktionsausgliederung, so ist der externe Diensteanbieter ohnehin neben dem Arbeitgeber verantwortlich.

9. Fehlen einer Regelung des grenzüberschreitenden Informationsaustausches

Forderungen nach einer Regelung des grenzüberschreitenden Informationsaustausches bei der Korruptionsbekämpfung,[129] etwa zur Ermöglichung von *Cross Border Investigations*, werden im RegE Beschäftigtendatenschutzgesetz leider nicht erfüllt.

10. Betriebsvereinbarungen

Nicht zufriedenstellend gelöst ist im RegE Beschäftigtendatenschutzgesetz die rechtspolitisch aufgeworfene Frage, ob Betriebsvereinbarungen zum Nachteil der Arbeitnehmer vom BDSG abweichen können.[130]

---

[127] *Deutsche Vereinigung für Datenschutz und andere*, Kritik am Eckpunktepapier der *Bundesregierung*, AuR 2010, 314.

[128] So aber *Deutsche Vereinigung für Datenschutz und andere*, Kritik am Eckpunktepapier der *Bundesregierung*, AuR 2010, 314.

[129] *Wybitul*, Betriebs-Berater 2009, 1582, 1584.

[130] *Gola*, RDV 2010, 97, 99; *Forst*, NZA 2010, 1043, 1044.

11. Einwilligung

Die Beschränkung der Möglichkeit zur Einwilligung in die Datenerhebung und Datenverarbeitung als Erlaubnistatbestand beim Beschäftigungsverhältnis auf einzelne Fallgruppen im RegE Beschäftigtendatenschutzgesetz ist fragwürdig.

12. Erfassung nicht automatisierter Dateien

Positiv zu bewerten ist im RegE Beschäftigtendatenschutzgesetz hingegen die konsequente Fortschreibung von § 32 Abs. 2 BDSG 2009 im zukünftigen § 27 Abs. 3 BDSG.[131]

13. Fazit

Insgesamt zeigt sich, dass der RegE Beschäftigtendatenschutzgesetz zwar das Spannungsverhältnis zwischen Datenschutz und Compliance thematisiert, aber nicht in jeder Hinsicht befriedigend löst.

[131] Dazu *Gola,* RDV 2010, 97, 99.