



Anette Kramme

Mitglied des Deutschen Bundestages

11/2009

**Arbeitnehmerdatenschutz:
Rechtslage und wesentliche Änderungsvorschläge im
Diskussionsentwurf des BMAS für ein Beschäftigtendatenschutzgesetz**

Seit letztem Jahr häufen sich aufsehenerregende Berichte in den Medien über gravierende Eingriffe in das informationelle Selbstbestimmungsrecht von Mitarbeitern insbesondere durch große Konzerne. Die Deutsche Bahn, Lidl, Siemens, die Deutsche Post, die Telekom, die Deutsche Bank, Burger King, Bauhaus, Ikea und mehrere kleinere Unternehmen haben auf verschiedene Weise ihre Mitarbeiter und teilweise sogar deren persönliches Umfeld überwacht oder Mitarbeiter-Daten zweckwidrig verwendet. Bekannt wurde beispielsweise, dass Mitarbeiter durch Kameras überwacht wurden, die eigentlich zur Diebstahlsvermeidung installiert waren, und dass umfassende Persönlichkeitsprofile von den Beschäftigten angelegt wurden, in denen von den Inhalten von Pausengesprächen bis hin zur Anzahl der Tätowierungen jedes Detail festgehalten wurde. Ein Unternehmen überwachte ohne Wissen der Beschäftigten Pausen- und Umkleideräume sowie Toiletten durch Videokameras. Ein weiteres Unternehmen hat Betriebsrats-Wahlen und Vorbereitungstreffen hierfür heimlich per Video aufgezeichnet, um Erkenntnisse über die „Rädelsführer“ und das Abstimmungsverhalten der Mitarbeiter zu erhalten. Geschäftsleitungen lasen heimlich bei den E-Mails ihrer Beschäftigten mit oder verhinderten die Zuleitung unliebsamer Mails wie z.B. von Gewerkschaften. Detektive wurden auf Mitarbeiter angesetzt, um zu erfahren, mit wem diese in ihrer Freizeit Umgang haben. Mitarbeiter wurden nach Fehltagen aufgefordert, über Art und Schwere ihrer Krankheit Auskunft zu geben. Die Bankverbindungen von Mitarbeitern wurden für groß angelegte Nachforschungen zur Aufdeckung von potentiell durchgeführtem Betrug am Unternehmen benutzt.

Obwohl die große Koalition beendet ist, besteht der Handlungsbedarf fort. Datenschutz am Arbeitsplatz betrifft zutiefst die Würde der Arbeitnehmer und Arbeitnehmerinnen. Der Diskussionsentwurf des BMAS sollte Grundlage des weiteren Handelns der SPD-Fraktion sein. Ein eigenständiges Arbeitnehmerdatenschutzgesetz wird durch Schwarz-Gelb abgelehnt. Konkrete Inhalte für die Änderung des Bundesdatenschutzgesetzes sind nicht genannt.

Der Arbeitnehmerdatenschutz ist im Recht auf informationelle Selbstbestimmung begründet, das wiederum Teil des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 GG iVm. Art. 1 Abs. 1 GG ist. Regelungen, die für den Datenschutz im Beschäftigungsverhältnis relevant sind, finden sich im BDSG, BetrVG/PersVG, im TKG, in Tarifverträgen und Betriebsvereinbarungen und im Europarecht. Die Regelungen im BDSG und in den anderen Gesetzen geben aber nur grobe Vorgaben. Das allgemeine Persönlichkeitsrecht muss vielfach zur Auslegung des BDSG herangezogen werden. Das Ergebnis eines Rechtsstreits hängt daher immer davon ab, als wie schwerwiegend das Gericht das Ausforschungsinteresse des Unternehmens einschätzt im Verhältnis zum informationellen Selbstbestimmungsrecht des Beschäftigten. Die Rechtsprechung hat bisher nur punktuelle Fragen geklärt, die wegen der jeweils nötigen Interessenabwägung in der Regel nur für den Einzelfall



Anette Kramme

Mitglied des Deutschen Bundestages

Gültigkeit haben. Zudem ist die Rechtsprechung auch teilweise uneinheitlich. Hinzu kommt, dass sowohl die Strafen als auch die Schadensersatzforderungen, die den Unternehmen drohen, wenig abschreckend sind bzw. für die Beschäftigten wenig Anreiz zu gerichtlichem Vorgehen geben.

Seit der Verabschiedung des § 32 BDSG im Juli 2009 im Rahmen des Datenschutzauditgesetzes besteht eine speziell für Beschäftigungsverhältnisse geltende Datenschutzregelung. Laut Gesetzesbegründung macht die Neuregelung ein Beschäftigtendatenschutzgesetz *nicht* entbehrlich – die neue Regierungskoalition scheint dies allerdings anders zu beurteilen. Das BMAS hat im August 2009 einen Entwurf für ein Beschäftigtendatenschutzgesetz vorgelegt (E-BDatG), dessen wichtigste Änderungsvorschläge hier vorgestellt werden. Im Zuge einer Verabschiedung des E-BDatGs wäre damit zu rechnen, dass § 32 BDSG ebenso wie einige andere dann im BDatG zusammengefasste Regelungen aufgehoben würde.

Inhalt des folgenden Papiers:

1. Definition der geschützten Daten
2. Definition der geschützten Personengruppen
3. Erlaubnistatbestände für Datenerhebungen/-nutzungen/-verwendungen
4. Voraussetzungen der Erlaubnistatbestände
5. Datensparsamkeit
6. Kontrollrechte des Beschäftigten über die über ihn erhobenen und gespeicherten Daten
7. Zulässige Datenerhebungen und -speicherungen im Rahmen von Bewerbungen
8. Auskunftseinholung bei Dritten (z.B. ehemaliger Arbeitgeber)
9. Zulässigkeit ärztlicher Untersuchungen und psychologischer Tests
10. Zulässigkeit von graphologischen Gutachten
11. Zulässigkeit von genetischen Untersuchungen
12. Zulässigkeit der Videoüberwachung von Betriebsgelände und Beschäftigten
13. Zulässigkeit der Überwachung von Telefon-, E-Mail- und Internetnutzung
14. Zulässigkeit des Einsatzes von Ortungssystemen
15. Zulässigkeit der Erhebung, Speicherung und Verwendung biometrischer Daten
16. Zulässigkeit der Überwachung durch Privatdetektive
17. *Whistleblowing*
18. Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten
19. Schadensersatzansprüche der Beschäftigten
20. Unterlassungsansprüche der Beschäftigten/des Betriebsrats
21. Ansprüche der Beschäftigten auf Löschung, Berichtigung und Sperrung von Daten
22. Ordnungswidrigkeits-/ Straftatbestände
23. Zulässigkeit der prozessualen Verwertung unzulässig erhobener Daten



Anette Kramme

Mitglied des Deutschen Bundestages

1. Definition der geschützten Daten

Bis Juli 2009 galt das BDSG in privatwirtschaftliche Unternehmen im Prinzip nur bei einer Datenerhebung, -nutzung oder -verarbeitung unter Einsatz von Datenverarbeitungsanlagen oder in/aus Dateien. Nicht vom Schutz umfasst waren insbesondere alle Unterlagen, die nicht systematisch geordnet sind, wie in der Praxis z.B. häufig bei Bewerbungsunterlagen der Fall. Der neue § 32 BDSG gilt dagegen einschränkungslos für alle personenbezogenen Daten, sofern sie *für Zwecke des Beschäftigungsverhältnisses* erhoben, genutzt oder verarbeitet werden.

Der **E-BDatG** bezieht sich laut § 3 Nr. 1, 2 allgemein auf Beschäftigtendaten iSv. Einzelangaben über persönliche oder sachliche Verhältnisse.

2. Definition der geschützten Personengruppen

§ 3 Abs. 11 BDSG zählt die Personengruppen auf, die „Beschäftigte“ iSd. § 32 BDSG sind. Diese ebenfalls neue Vorschrift stellt nun gesetzlich klar, dass das BDSG nicht nur für Arbeitnehmer, sondern auch z.B. für Bewerber und arbeitnehmerähnliche Personen gilt. Nach wie vor sind aber z.B. in einen Betrieb eingegliederte Selbständige oder Leiharbeitnehmer nicht vom Schutz umfasst.

Der **E-BDatG** greift die Beschäftigten-Definition des § 3 Abs. 11 BDSG auf.

3. Erlaubnistatbestände für Datenerhebungen/-nutzungen/-verwendungen

Eine Datenerhebung, -nutzung, -verarbeitung darf laut BDSG nur

- mit Einwilligung sowie
- auf Grundlage jedweder gesetzlicher Ermächtigung erfolgen.

Als gesetzliche Ermächtigungen kommen im Beschäftigungsverhältnis in erster Linie § 32 und § 28 Abs. 1 S. 1 Nr. 2 in Betracht. § 28 Abs. 1 BDSG enthält einen Erlaubnistatbestand nicht nur für Arbeitgeber, sondern allgemein für jede datenerhebende Stelle (zum Inhalt i.E. unten).

- Eine **Einwilligung** bedarf zwar grundsätzlich der Schriftform (§ 4a BDSG). Von Teilen der Literatur und auch vom Bundesdatenschutzbeauftragten wird aber in Frage gestellt, ob Einwilligungen überhaupt eine geeignete Ermächtigungsgrundlage für Datenerhebungen im Arbeitsverhältnis sein können. Wegen des sozialen Abhängigkeitsverhältnisses gegenüber dem Arbeitgeber werden Einwilligungen regelmäßig unfeilig abgegeben. § 4a BDSG sei daher zumindest entsprechend einschränkend auszulegen, so dass die Umstände der Einwilligungserteilung genau betrachtet werden sollten.

- Ob auch **Tarifverträge und Betriebsvereinbarungen** gesetzliche Ermächtigungen darstellen und ob sie dementsprechend das Schutzniveau des BDSG unterschreiten dürfen, ist umstritten; in der Gesetzesbegründung zum Datenschutzauditgesetz von Juli 2009 wird dies bejaht. Insbesondere Betriebsräte sehen sich daher in der Praxis teilweise gezwungen, den Arbeitnehmerdatenschutz als „Verhandlungsmasse“ einzusetzen.



Anette Kramme

Mitglied des Deutschen Bundestages

Laut § 4 Abs. 1 **E-BDatG** ist die Erhebung oder Verwendung von Beschäftigtendaten *für Zwecke des Beschäftigtenverhältnisses* nur zulässig, wenn das BDatG es erlaubt. Dies schließt implizit aus, dass die gesetzlich vorgesehenen Zulässigkeitsanforderungen durch eine Einwilligung des Beschäftigten oder durch einen Tarifvertrag oder eine Betriebsvereinbarung herabgesetzt werden dürfen. Klarstellend erklärt auch § 34 E-BDatG die Rechte des BDatG für unabdingbar und schließt einen Verzicht auf diese Rechte aus. Der E-BDatG sieht allerdings in *einzelnen* Vorschriften ausdrücklich vor, dass eine Einwilligung des Beschäftigten eine sonst unzulässige Datenerhebung oder -verwendung legitimieren kann.

§ 4 Abs. 1 E-BDatG erlaubt in S. 2 aber auch das Erheben und Verwenden von *Beschäftigtendaten*, wenn ein anderes Gesetz oder eine Rechtsverordnung es *für Zwecke des Beschäftigtenverhältnisses* erlaubt. Zulässig ist demnach etwa das Erheben von Beschäftigtendaten durch die Sozialversicherungsträger auf Grundlage eines der Sozialgesetzbücher.

Weiterhin werden Rechtsvorschriften und Gesetze, die das Erheben und Verwenden von Beschäftigtendaten *zu anderen Zwecken* erlauben oder anordnen, durch das BDatG nicht berührt (§ 4 Abs. 1 S. 3). Gegenüber anderen Gesetzen oder Rechtsvorschriften ist das BDatG somit nicht abschließend. Ausgeschlossen ist aber, dass Arbeitgeber Beschäftigtendaten *für Zwecke des Beschäftigungsverhältnisses* aufgrund eines nicht ausdrücklich für Zwecke des Beschäftigungsverhältnisses zugeschnittenen Erlaubnistatbestandes außerhalb der im BDatG oder in anderen Gesetzen/Rechtsverordnungen erheben oder verwenden.

Zudem sind (nur) soweit das BDatG keine Regelung trifft, die Vorschriften des BDSGs entsprechend anzuwenden (§ 4 Abs. 2). Ein Arbeitgeber darf demnach eine Datenerhebung oder -verwendung auch auf das BDSG stützen, jedoch nur, wenn der Sachverhalt nicht schon im BDatG geregelt ist.

Die Regelungen dieses Paragraphen des E-BDatG erschließen sich nicht auf Anhieb und könnten im Sinne größerer Transparenz weit klarer formuliert und die einzelnen Bestimmungen noch besser aufeinander abgestimmt werden.

4. Voraussetzungen der Erlaubnistatbestände

Kernnorm für den Arbeitnehmerdatenschutz ist § 32 BDSG, der speziell für Beschäftigungsverhältnisse die **zulässigen Zwecke** einer Datenerhebung, -verarbeitung oder -nutzung konkretisiert.

- Laut § 32 BDSG dürfen *bei der Begründung* des Beschäftigungsverhältnisses nur Daten erhoben werden, die *für eine Entscheidung hierüber* erforderlich sind.

- *Nach der Begründung* des Beschäftigungsverhältnisses dürfen nur Daten erhoben werden, die *für die Durchführung oder Beendigung* des Beschäftigungsverhältnisses erforderlich sind.



Anette Kramme

Mitglied des Deutschen Bundestages

- Darüberhinaus dürfen Daten eines Beschäftigten erhoben werden, wenn eine *Straftat aufgedeckt werden soll*, wobei zu dokumentierende tatsächliche Anhaltspunkte vorliegen und die – im Gesetz ausformulierten – Anforderungen einer Verhältnismäßigkeitsprüfung eingehalten werden müssen (Erforderlichkeit der Erhebung/Verarbeitung/Nutzung, Abwägung mit dem Interesse des Beschäftigten am Ausschluss der Erhebung/Verarbeitung/Nutzung, keine Unverhältnismäßigkeit der Maßnahme im Hinblick auf den Anlass).

§ 28 Abs. 1 S. 1 BDSG enthält mehrere Alternativen, von denen die Nr. 1 Erlaubnistatbestände für *rechtsgeschäftliche oder rechtsgeschäftsähnliche Schuldverhältnisse* enthält; diese ist aber im Beschäftigungsverhältnis nicht anwendbar, da § 32 BDSG hier die speziellere Norm ist. Insbesondere § 28 Abs. 1 S. Nr. 2 BDSG, der eine Datenerhebung *bei berechtigten Interessen* der datenerhebenden Stelle zulässt, kann jedoch als zusätzlicher Erlaubnistatbestand neben § 32 BDSG auch im Beschäftigungsverhältnis herangezogen werden.

Die Eingrenzung der zulässigen Zwecke einer Datenerhebung durch den Arbeitgeber, die mit dem neuen § 32 BDSG erfolgt ist, war überaus wünschenswert, auch wenn mit ihr nur die ständige Rechtsprechung aufgegriffen wurde. Insbesondere entsteht dadurch für beide Seiten Transparenz, in welchen Situationen eine Datenerhebung erlaubt ist und in welchen nicht. Dem läuft aber zuwider, dass § 28 Abs. 1 S. 1 Nr. 2 BDSG mit seiner sehr offenen Formulierung („berechtigten Interessen“ der datenerhebenden Stelle) nicht für das Arbeitsverhältnis ausgeschlossen wurde, wie es schlüssig gewesen wäre. So besteht nach wie vor die Unsicherheit, ob für eine konkrete Datenerhebung ein „berechtigtes Interesse“ anzuerkennen ist, was wiederum nur durch die Rechtsprechung konkretisiert werden kann.

Der **E-BDatG** normiert in §§ 6, 7 die zulässigen Zwecke einer Datenerhebung oder -verwendung *im Einstellungsverfahren* (dazu unten), und in §§ 8 ff. die zulässigen Zwecke einer Datenerhebung oder -verwendung *nach Begründung des Beschäftigungsverhältnisses*.

Danach dürfen *während* des Beschäftigungsverhältnisses Daten nur

- zur Erfüllung bestimmter gesetzlicher und vertraglicher Pflichten erhoben werden oder
- soweit sie für den Arbeitgeber erforderlich sind, *um bei der Durchführung des Beschäftigungsverhältnisses bestehende Rechte wahrzunehmen*.

Für den Fall, dass Zweck einer Datenerhebung die Aufdeckung einer Straftat ist, übernimmt E-BDatG die Anforderungen des § 32 BDSG, trifft aber strengere Regelungen für eine *Verwendung* von Daten, egal zu welchem Zweck. Hier setzt § 9 E-BDatG voraus, dass

- sie rechtmäßig erhoben wurden,
- die Verwendung für den Erhebungszweck oder einen anderen nach dem BDatG zulässigen Zweck erforderlich und
- die Verwendung nicht unverhältnismäßig ist.



Anette Kramme

Mitglied des Deutschen Bundestages

5. Datensparsamkeit

§ 3a BDSG normiert das Ziel möglichst weitgehender **Datenvermeidung** sowie das Ziel, erhobene Daten möglichst zu anonymisieren oder zu pseudonymisieren (Gebot der **Datensparsamkeit**). Die Vorschrift enthält aber nur nicht zwangsweise durchsetzbare Zielvorgaben.

Der **E-BDatG** übernimmt das Ziel der Datenvermeidung und ergänzt es um das Ziel, Persönlichkeitsrechtsverletzungen zu vermeiden (§ 5 Abs. 2). §§ 5, Abs. 1, 16 E-BDatG enthalten die Gebote, Beschäftigtendaten vertraulich zu behandeln und möglichst zu verschlüsseln. Einzelne Vorschriften des E-BDatGs enthalten spezielle Anonymisierungsverpflichtungen, so etwa bzgl. der äußeren Verbindungsdaten von Dritten, die bei Telefonaten und E-Mails anfallen.

Damit das Gebot der Datenvermeidung tatsächlich wirksam ist, wäre allerdings eine noch deutlichere Regelung wünschenswert, die bestimmt, dass Arbeitnehmerdaten immer pseudonymisiert/anonymisiert werden müssen, wenn der verfolgte Zweck dies zulässt, was insb. bei statistischen Auswertungen der Fall ist.

6. Kontrollrechte des Beschäftigten über die über ihn erhobenen und gespeicherten Daten

Bei erstmaliger Speicherung oder Übermittlung von Daten an Dritte hat ein Betroffener Anspruch auf **Benachrichtigung** (§ 33 BDSG), daneben hat er einen Anspruch auf **Auskunft** über die über ihn gespeicherten Daten, deren Herkunft, die Empfänger/Kategorien von Empfängern und den Zweck der Speicherung (§ 34 BDSG). Ein Anspruch eines Beschäftigten auf **Einsicht in die Personalakte** ergibt sich aus § 83 Abs. 1 S. 1 BetrVG. Die Verortung dieses Rechts im BetrVG ist systemwidrig, denn sie gilt – so die Meinung in Literatur und Rechtsprechung - auch in betriebsratslosen Betrieben.

§ 18 **E-BDatG** sieht vor, dass Beschäftigte schriftlich über die erstmalige Erhebung oder Speicherung ihrer Daten sowie über den Zweck benachrichtigt werden müssen, wenn sie nicht schon auf andere Weise Kenntnis davon haben. Bei Datenerhebungen durch technische Einrichtungen bestehen noch weitergehende Benachrichtigungspflichten, z.B. hinsichtlich Methoden und Verfahren. Bei Datenpannen besteht laut § 19 E-BDatG eine gesonderte Benachrichtigungspflicht. § 20 E-BDatG enthält einen Anspruch auf Einsicht in die Personalakte, § 21 E-BDatG enthält ein dem § 34 BDSG im Wesentlichen nachgebildetes allgemeines Auskunftsrecht.

7. Zulässige Datenerhebungen und -speicherungen im Rahmen von Bewerbungen

Für die Anbahnungsphase eines Beschäftigungsverhältnisses gelten die o.g. Grenzen des § 32 BDSG. Die Rechtsprechung und die Literatur haben insbesondere Fragen nach folgenden Themen für grundsätzlich unzulässig erklärt: zur Schwangerschaft, zu Erkrankungen von Verwandten, zur Gewerkschaftszugehörigkeit, zu einer (Schwer-)Behinderung, zum sexualmedizinischen Bereich, zur „rassischen“ oder ethnischen Herkunft sowie zu religiösen, philosophischen und politischen Überzeugungen. Gerade um das von der Rechtsprechung eröffnete „Recht zur Lüge“ bei unzulässigen Fragen als Bewerber in der Praxis wahrnehmen zu können, ist eine klare und



Anette Kramme

Mitglied des Deutschen Bundestages

eindeutige Rechtslage hinsichtlich aller unzulässigen Themen Voraussetzung. Daran fehlt es, solange die unzulässigen Fragethemen nicht konkret im Gesetz genannt sind.

§ 6 **E-BDatG** sieht vor, dass der Arbeitgeber einen Bewerber über die auszuübende Tätigkeit informieren muss, bevor er diesem Fragen stellen darf. Inhaltlich ist das Fragerecht auf die Erlangung von Kenntnissen beschränkt, die zur Eignungsfeststellung erforderlich sind. Grundsätzlich unzulässig ist das Einholen von Auskünften über die Abstammung, ethnische und sonstige Herkunft, Nationalität, Religion oder Weltanschauung, Behinderung, Alter, politische oder gewerkschaftliche Betätigung oder Einstellung, Geschlecht oder sexuelle Identität. Etwas anderes gilt, wenn eins der Merkmale eine wesentliche und entscheidende Anforderung für die Tätigkeit ist wegen ihrer Art oder der Bedingungen ihrer Ausübung. Besonderheiten gelten zudem für Beschäftigungen bei Religionsgemeinschaften.

Auch wenn die Rechtsprechung die Frage nach einer Schwangerschaft – allerdings mit Ausnahmen – für verboten erklärt hat, sollte sie in den Themenkatalog mit aufgenommen werden; wenn dieses Thema in einem ausdrücklich normierten Katalog fehlt, könnte dies sonst auf eine Absicht deuten, diese Frage für zulässig zu erklären.

§ 7 **E-BDatG** regelt zudem, dass Entscheidungen über die Begründung eines Beschäftigungsverhältnisses nicht ausschließlich auf eine automatisierte Verarbeitung gestützt werden dürfen und dass Bewerbungsunterlagen grundsätzlich 2 Monate nach Abschluss des Bewerbungsverfahrens zurückgegeben bzw. gelöscht werden müssen.

8. Auskunftseinholung bei Dritten (z.B. ehemaliger Arbeitgeber)

Es gilt der **Vorrang der Direkterhebung** (§ 4 Abs. 2 S. 1 BDSG): Daten müssen grundsätzlich beim Betroffenen selbst erhoben werden; eine Datenerhebung bei Dritten (z.B. ehemaligem Arbeitgeber) ist aber zulässig, wenn die Direkterhebung unverhältnismäßig aufwändig ist. Diese Ausnahme wird in der Literatur vielfach als Verletzung des Persönlichkeitsrechts angesehen, auch wenn überwiegend angenommen wird, dass zumindest die Frageverbote jedoch auch bei erlaubter Informationseinholung bei Dritten eine absolute Grenze grenzen.

Nach § 6 Abs. 4 **E-BDatG** dürfen Auskünfte über Beschäftigte nur mit Einwilligung des Beschäftigten bei Dritten eingeholt werden. Dem Beschäftigten muss auf Verlangen der Inhalt der Auskunft mitgeteilt werden.

9. Zulässigkeit ärztlicher Untersuchungen und psychologischer Tests

Ärztliche Untersuchungen (insbesondere bei Einstellungen) erfordern laut BAG immer eine Einwilligung des Betroffenen und sind nur dann und nur insoweit zulässig als die Erkenntnisse für die Beurteilung der Eignung für die Tätigkeit erforderlich sind. Zudem dürfen sie nur von einem Arzt vorgenommen werden, der dem Arbeitgeber nur Schlussfolgerungen („geeignet“ oder „nicht geeignet“), jedoch keine konkreten Informationen zu den Befunden mitteilen darf. Eine konkrete gesetzliche Regelung hierzu fehlt bislang jedoch, obwohl es sich um einen für die Praxis sehr relevanten Bereich handelt, der massive Gefahren von Persönlichkeitsverletzungen birgt.



Anette Kramme

Mitglied des Deutschen Bundestages

Psychologische Tests (z.B. Intelligenztests, gezielte Provokationen zum Austesten der Stressresistenz, Persönlichkeitstests mittels Fragebogen) dürfen laut Literatur und Rechtsprechung nur von Psychologen durchgeführt werden; auch hier darf der Arbeitgeber nur über die Eignung, nicht aber über Einzeldaten aus der Untersuchung informiert werden. Auch hier fehlt es bislang an einer Regelung, obwohl auch in diesem Bereich ein großer praktischer Bedarf an schützenden Klarstellungen besteht.

§ 6 Abs. 5, 6 **E-BDatG** normiert einheitliche Regelungen sowohl für ärztliche Untersuchungen als auch für psychologische Tests. Der Arbeitgeber darf den Vertragsschluss von einer gesundheitlichen oder sonstigen Untersuchung oder Prüfung abhängig machen, wenn

- sie erforderlich ist, um festzustellen, ob der Beschäftigte zum Zeitpunkt der Arbeitsaufnahme für die Tätigkeit geeignet ist,
- sie nach den Regeln der Fachkunde erfolgt und
- der Beschäftigte über Art und Umfang der Untersuchung/Prüfung aufgeklärt wurde und ihr zugestimmt hat.

Eine weitere Einwilligung des Beschäftigten ist erforderlich, wenn die Ergebnisse, die dem Beschäftigten zwingend mitzuteilen sind, auch dem Arbeitgeber mitgeteilt werden sollen.

Die Durchführung einer gesundheitlichen oder sonstigen Untersuchung oder Prüfung *nach Begründung des Beschäftigungsverhältnisses* darf der Arbeitgeber laut E-BDatG nur verlangen, wenn sie

- in einer Rechtsvorschrift angeordnet oder
- zur Eignungsüberprüfung erforderlich ist.

Auskünfte über medizinische Diagnosen oder über Befunde medizinischer Untersuchungen darf er vom Beschäftigten nicht verlangen, es sei denn, der Arbeitgeber ist zur Kostenerstattung der Untersuchung oder Behandlung verpflichtet und die Diagnose ist für die Abrechnung von Bedeutung.

Die Formulierung im Entwurf ist nicht ganz deutlich bei der Frage, ob die Weitergabe von Ergebnissen der Untersuchung oder Prüfung mit einer Einwilligung des Beschäftigten nur bzgl. dessen Geeignetheit oder Ungeeignetheit zulässig sein soll oder ob auch die Weitergabe einzelner Diagnosen und Details mit einer Einwilligung erlaubt sein soll. Es sollte daher klargestellt werden, dass die Mitteilung von Ergebnisdetails an den Arbeitgeber soweit sie über die Eignungsinformation hinausgehen auch mit Einwilligung des Bewerbers unzulässig sind. Nur so können qualitative (z.B. auf dem Gesundheitszustand beruhende) Abstufungen von Bewerbern wirksam vermieden werden, die mehr Informationen enthalten als nur Auskünfte über die Erfüllung von Mindestanforderungen für die Tätigkeit und die zu Persönlichkeitsverletzungen führen würden.



Anette Kramme

Mitglied des Deutschen Bundestages

10. Zulässigkeit von graphologischen Gutachten

Das Einholen graphologischer Gutachten ist laut BAG und Literatur nur mit Einwilligung zulässig, und nur insoweit als es für das konkrete Beschäftigungsverhältnis erforderlich ist. Die Aussagefähigkeit dieser Methode ist jedoch nicht wissenschaftlich gesichert.

Graphologische Untersuchungen sind laut **E-BDatG** ausnahmslos unzulässig.

11. Zulässigkeit von genetischen Untersuchungen

Eine Auswertung von DNA, die insbesondere über die Prädisposition für Krankheiten Auskunft gibt, betrifft das Persönlichkeitsrecht in gravierender Weise. Genetische Untersuchungen *vor Begründung eines Beschäftigungsverhältnisses* sind laut §§ 19, 20 Gendiagnostikgesetz, die im April 2009 verabschiedet wurden und im Februar 2010 in Kraft treten werden, ausnahmslos verboten. *Während eines Beschäftigungsverhältnisses* sind sie nur erlaubt, wenn wegen der speziellen Tätigkeit eine Gefahr für den Beschäftigten droht, der durch eine genetische Untersuchung vorgebeugt werden kann.

Für die Zulässigkeit genetischer Untersuchungen verweist **E-BDatG** auf die Regelungen des Gendiagnostikgesetzes.

12. Zulässigkeit von Videoüberwachung von Betriebsgelände und Beschäftigten

Regelungen, die konkret die Zulässigkeit der verschiedenen Möglichkeiten zur Überwachung von Beschäftigten regeln, gibt es nicht. Die Rechtslage ist überaus undurchsichtig. Zur Zulässigkeit von Videoüberwachungen hat das BAG bisher nur vereinzelt Entscheidungen getroffen, die sich zudem ganz überwiegend auf die heimliche Videoüberwachung beziehen. Es gelten verschiedene Regelungen für vier Konstellationen:

Die **offene Videoüberwachung** ist in **nicht-öffentlichen Räumen** (d.h. Räumen ohne Publikumsverkehr) im Rahmen des § 32 BDSG oder § 28 BDSG zulässig. Konkret ist unklar, welche Grenzen das Verhältnismäßigkeitsprinzip setzt. Die Literatur etwa sieht z.B. eine allgemeine Zugangskontrolle in nicht-öffentlichen Gebäuden wie etwa Bürogebäuden mittels Video als unzulässig an, wenn sie ebenso effektiv durch den Einsatz von Chipkarten oder Pfortnern erfolgen kann. Rechtlich undeutlich ist auch, wann ein Raum als „nicht-öffentlich“ einzustufen ist. Die Rechtsprechung hat z.B. sogar den Arbeitsplatz einer Kassiererin hinter der Kasse, auf den gezielt eine Videokamera gerichtet ist, als nicht-öffentlichen Raum eingeordnet. Unklar ist auch, welche Grenzen z.B. für eine Überwachung von Toiletten, Duschen oder Pausenräumen gelten.

Für die Zulässigkeit einer **heimlichen** Überwachung in nicht-öffentlichen Räumen kommen die gleichen Erlaubnistatbestände wie bei einer offenen Überwachung in Frage, wobei aber im Rahmen der Verhältnismäßigkeitsprüfung ein ungleich strengerer Maßstab anzulegen ist. Laut BAG und BVerfG ist sie nur zulässig etwa bei einer Notwehrsituation oder einer notwehrähnlichen Lage des Arbeitgebers.



Anette Kramme

Mitglied des Deutschen Bundestages

Für Videoüberwachung **in öffentlichen Räumen**, die gleichzeitig Arbeitsplätze von Mitarbeiter sind (Museum, Schalterraum, Verkaufsraum,...) gilt die Spezialnorm § 6b BDSG. Danach gelten (in der Privatwirtschaft) für die **offene** Videoüberwachung in öffentlichen Räumen die gleichen Grundsätze wie bei der offenen Videoüberwachung im nicht-öffentlichen Raum, allerdings mit der Abweichung, dass auch eine Überwachung zu einem nur *präventiven* Zweck erlaubt ist, nämlich zur Wahrnehmung des Hausrechts.

Für **heimliche** Videoüberwachungen im öffentlichen Raum enthält § 6b BDSG ein ausdrückliches Verbot. Umstritten ist in Literatur und Rechtsprechung, ob dennoch auch hier die heimliche Videoüberwachung zulässig ist, wenn z.B. eine notwehrähnliche Situation vorliegt.

§ 11 **E-BDatG** trifft statt der Unterscheidung öffentlicher/nicht-öffentlicher Raum die Unterscheidung zwischen einer Überwachung des Betriebs und einer Überwachung von Beschäftigten. Er regelt, dass eine **offene** Videoüberwachung **des Betriebs** zulässig ist, wenn sie

- zur Zutrittskontrolle,
- zur Wahrnehmung des Hausrechts,
- zum Schutz des Eigentums gegenüber Dritten,
- zur Sicherung von Anlagen oder
- zur Abwehr von Gefahren für die Sicherheit des Betriebs erforderlich ist.

Dabei anfallende Beschäftigtendaten dürfen nicht zu anderen Zwecken verwendet werden. Mangels Erlaubnistatbestands ist eine **heimliche** Videoüberwachung des Betriebs demnach ausnahmslos unzulässig.

Eine **offene oder heimliche** Videoüberwachung **von Beschäftigten** ist (nur) zulässig bei tatsächlichen Anhaltspunkten für den Verdacht einer Straftat und wenn die Videoüberwachung verhältnismäßig ist.

13. Zulässigkeit der Überwachung von Telefon-, E-Mail- und Internetnutzung

Für das Speichern und Mithören von **Telefongesprächen** gilt neben dem BDSG auch Art. 10 Abs. 1 GG, der das Fernmeldegeheimnis schützt, sowie das Telekommunikationsgesetz (TKG). Die personenbezogenen Daten des Angerufenen fallen ebenfalls unter den Schutz. Auch für die Überwachung von Telefongesprächen fehlen konkrete gesetzliche Regelungen. Die von der Rechtsprechung vorgegebene Unterscheidung zwischen drei verschiedenen Arten von Telefondaten mit unterschiedlicher Eingriffsintensität verkompliziert die Rechtslage zusätzlich.

- Das heimliche Abhören oder Aufzeichnen von **Gesprächsinhalten** ist laut BVerfG und BAG nur zulässig bei einer notwehrähnlichen Situation des Arbeitgebers. Ein Mithören nach vorheriger Mitteilung ist dagegen unter den Voraussetzungen des § 32 BDSG bzw. § 28 BDSG grundsätzlich zulässig.
- Die Rechtslage bzgl. der **Erfassung von Zielnummern** ist umstritten. Laut BAG kommt es darauf an, ob der Beschäftigte auch Privatgespräche führen darf oder nicht. Hat der



Anette Kramme

Mitglied des Deutschen Bundestages

Arbeitgeber – was ihm freisteht - Privatgespräche untersagt, ist die Zielnummern Erfassung jedenfalls zwecks Kostenkontrolle zulässig. Sind Privatgespräche erlaubt, ist sie nur dann zulässig, wenn der Beschäftigte die Möglichkeit hat, ein Privatgespräch durch Vorwahl einer bestimmten Ziffer zu kennzeichnen. Das BAG hat aber der Rechtstellung des Angerufenen keine Beachtung geschenkt, weshalb die Literatur teilweise weitreichendere Einschränkungen (nur verkürzte Zielnummer) annimmt.

- Die Überwachung der **äußeren Verbindungsdaten (d.h. Datum, Uhrzeit, Dauer oder angefallene Entgelte ohne Zielnummern)** ist bei dienstlichen Gesprächen grundsätzlich zulässig.

Bzgl. der **Kontrolle von E-Mails und Internet** sind zahlreiche Einzelfragen umstritten; auch hier geht es immer auch um geschützte Daten des Kommunikationspartners. Eine konkrete gesetzliche Regelung fehlt. Teilweise wird vertreten, dass die Kommunikation per Mail eher dem gesprochenen Wort gleichzustellen ist, weshalb die gleichen, eher strengen Grundsätze wie bei Telefonaten gelten sollen, teilweise werden Mails als dem Briefverkehr ähnlich angesehen, für den weit weniger Beschränkungen gelten.

§ 14 Abs. 1 **E-BDatG** trifft für Telefon, E-Mail und Internet zunächst die einheitliche Regelung, dass diese auch privat genutzt werden dürfen, wenn nicht Arbeitgeber und Beschäftigte etwas anderes vereinbart haben (in Betriebsvereinbarung oder Arbeitsvertrag). Je nachdem gelten dann – wie bisher – unterschiedlich intensive Datenschutzstandards.

Abs. 2 regelt für den Fall, dass die Kommunikationsdienste **nur dienstlich** genutzt werden dürfen, dass **äußere Verbindungsdaten** (von E-Mails, Telefonaten, Internetnutzung) erhoben werden dürfen (einschließlich Zielnummern/-adressen), wenn sie

- für eine stichprobenartige oder anlassbezogene Leistungs- oder Verhaltenskontrolle,
- zur Gewährleistung der Datensicherheit,
- für den ordnungsgemäßen Betrieb der Dienste oder
- zur Abrechnung erforderlich sind. Die Daten der Kommunikationspartner dürfen nur anonymisiert verwendet werden.

Das gleiche gilt grundsätzlich, wenn die **private Nutzung** erlaubt ist, mit der Abweichung, dass eine Erhebung und Verwendung äußerer Verbindungsdaten *zur Leistungs- und Verhaltenskontrolle* in dem Fall ausgeschlossen ist.

Sinnvoll wäre, einheitlich eine Überwachung der äußeren Verbindungsdaten zum Zweck der Leistungs- und Verhaltenskontrolle auch dann auszuschließen, wenn die private Nutzung nicht erlaubt ist; dies würde zugleich dem Arbeitgeber den eigentlich gesetzgeberisch unerwünschten Anreiz nehmen, zwecks größerer Überwachungsmöglichkeiten die private Nutzung von Telefon und Internet auszuschließen. Eine einheitliche Regelung würde zudem die Transparenz der Regelung erhöhen.



Anette Kramme

Mitglied des Deutschen Bundestages

Bzgl. der Kontrolle von Telefon- und E-Mail-**Inhalten** durch den Arbeitgeber gelten im E-BDatG unterschiedliche Regelungen für Telefon einerseits und E-Mail und Internet andererseits.

Für den Fall, dass das **Telefon nur dienstlich** genutzt werden darf, darf der Arbeitgeber Inhalte **offen** erheben und verwenden, wenn sowohl die Beschäftigten als auch die Kommunikationspartner eingewilligt haben. Ohne Einwilligung ist demnach auch bei nur dienstlicher Nutzung eine Telefonüberwachung unzulässig.

Abs. 4 bestimmt ausdrücklich, dass die Kenntnisnahme von Inhalten von Telefongesprächen oder E-Mails ausnahmslos unzulässig ist, wenn diese **auch privat** genutzt werden dürfen.

Für den Fall, dass **E-Mail und Internet nur dienstlich** verwendet werden dürfen, darf der Arbeitgeber Inhalte erheben und verwenden, wenn dies

- für eine stichprobenartige oder anlassbezogene Leistungs- oder Verhaltenskontrolle,
- für die Aufdeckung einer Straftat oder
- für die Datensicherheit erforderlich ist.

Mangels Erlaubnistatbestands ist bei **auch privater** Nutzung eine Überwachung von E-Mail- und Internetnutzung unzulässig.

Auch hier wäre eine Regelung vorzuziehen, die einen unerwünschten Anreiz für den Arbeitgeber vermeidet, die private Nutzung zwecks größerer Überwachungsmöglichkeiten auszuschließen. Denkbar wäre etwa, Arbeitgeber zu verpflichten, (ggf. getrennt von nur für die Dienstnutzung vorgesehenen Telefonen und Computern) für Arbeitnehmer Möglichkeiten zur Verfügung zu stellen, diese Dienste auch privat zu nutzen oder unterschiedliche Einwahln bzw. Passwort-Anmeldungen für private und dienstliche Nutzung der Geräte einzusetzen. Dem Arbeitgeber blieben die erweiterten Überwachungsmöglichkeiten für dienstlich genutzte Geräte bzw. der dienstlichen Nutzung der Geräte dann in jedem Fall erhalten. Zudem sollte überlegt werden, ob auch, wenn eine Einwilligung der Beschäftigten vorliegt, zeitliche Höchstgrenzen für die Überwachung der Inhalte von Telefonaten gesetzt werden, wie es auch die Rechtsprechung für erforderlich hält.

14. Zulässigkeit des Einsatzes von Ortungssystemen

Eine Überwachung von Beschäftigten mittels GPS oder RFID, mit denen Bewegungsprofile erstellt werden können, wird in der Literatur als unzulässig angesehen; sie komme einer „elektronischen Fußfessel“ gleich. Laut Rechtsprechung können aner kennenswerte Motive des Arbeitgebers für eine solche Überwachung bestehen. Eine konkrete gesetzliche Regelung fehlt.

§ 12 **E-BDatG** regelt, dass Ortungssysteme zur **offenen** Überwachung von Beschäftigten eingesetzt werden dürfen, wenn es



Anette Kramme

Mitglied des Deutschen Bundestages

- zur Sicherheit der Beschäftigten oder
- zur Koordinierung eines wechselnden Einsatzes an verschiedenen Orten erforderlich ist.

Eine Verwendung der anfallenden Daten zu anderen Zwecken ist unzulässig.

15. Zulässigkeit der Erhebung, Speicherung und Verwendung biometrischer Daten

Für **Biometrische Daten** (Fingerabdruck, Iris, Stimme, Unterschrift, Zahnabdruck, Körpergröße, ...) gelten die allgemeinen Regelungen der §§ 32, 28 BDSG. Rechtsprechung hierzu liegt nicht vor; eine konkrete gesetzliche Regelung fehlt.

Laut § 13 **E-BDatG** darf der Arbeitgeber biometrische Daten (nur) erheben und verwenden, wenn sie zu Autorisierungs- und Authentifikationszwecken erforderlich sind.

16. Zulässigkeit der Überwachung durch Privatdetektive

Die Beschränkungen der §§ 32, 28 BDSG gelten auch für den Einsatz von Privatdetektiven. Eine konkrete gesetzliche Regelung fehlt. Die Rechtsprechung hat einen Detektiveinsatz zur Überprüfung eines konkreten Tatverdachts bzgl. eines Beschäftigten für zulässig gehalten. Da Detektive (anders als technische Einrichtungen) sich ggf. auch gezielt in das Vertrauen einzelner Beschäftigter einschleichen können, besteht hier erhebliches Missbrauchspotential.

E-BDatG regelt den Detektiveinsatz in Abs. 4 des § 25, der auch weitere Regelungen zur Datenerhebung und -verwendung durch Dritte im Auftrag des Arbeitgebers trifft. Danach ist ein *Verdacht für eine schwerwiegende Vertragsverletzung, die eine außerordentliche Kündigung rechtfertigen würde*, oder eine *Straftat* Voraussetzung, zudem darf der Detektiveinsatz nicht unverhältnismäßig sein.

17. Whistleblowing

„**Whistleblowing**“ meint zum einen eine vertragliche Pflicht des Beschäftigten, das Unternehmen über rechtliche Verstöße im Betrieb zu informieren, zum anderen die Möglichkeit des Beschäftigten, bei Missständen im Betrieb gegen den Arbeitgeber Anzeige zu erstatten oder an die Presse zu gehen ohne Sanktionen befürchten zu müssen. Die Zulässigkeitsgrenzen eines **Whistleblowing-Systems** im Sinne einer Meldepflicht des Beschäftigten bzw. einer an ihn gerichteten Meldeaufforderung sind umstritten. Eine Gruppe von 25 Datenschutzbeauftragten der EU-Mitgliedstaaten hat Empfehlungen zum Datenschutz bei diesen Systemen herausgegeben, deren rechtliche Relevanz noch ungeklärt ist. Eine Gefahr liegt darin, in Betrieben eine „Kultur der Bespitzelung und Verleumdung“ zu etablieren.

Regelungen zum **arbeitsrechtlichen Schutz von Whistleblowern**, wenn Informationen an Stellen außerhalb des Unternehmens weitergegeben werden, sollen den Beschäftigten vor einer Kündigung und anderen Maßregelungen schützen. Solche Maßnahmen des Arbeitgebers sind nur zulässig, wenn der Beschäftigte seine vertragliche Verschwiegenheitspflicht verletzt, deren genaue Reichweite jedoch ungeklärt ist. Hier besteht die Gefahr, dass sich Beschäftigte aus Angst vor arbeitsrechtlichen Konsequenzen zum Schweigen etwa über gemeingefährliche Praktiken des



Anette Kramme

Mitglied des Deutschen Bundestages

Arbeitgebers veranlasst. Eine vorgeschlagene konkrete Regelung in einem neuen § 612a BGB scheiterte Anfang 2009 am Widerstand der CDU/CSU.

§ 31 Abs. 2 **E-BDatG** bestimmt, dass Beschäftigte sich an die Aufsichtsbehörde, d.h. den Landesdatenschutzbeauftragten wenden dürfen, wenn sie auf Grund konkreter Anhaltspunkte der Auffassung sind, dass Verstöße gegen das BDatG oder andere datenschützende Rechtsvorschriften begangen wurden und der Arbeitgeber einer darauf gerichteten Beschwerde nicht abhilft. Unmittelbar an die Aufsichtsbehörde wenden können Beschäftigte sich jedoch, wenn ein Beauftragter für den Beschäftigtendatenschutz nicht bestellt ist.

Das BDatG sollte darüber hinaus datenschützende Anforderungen an Whistleblowing-Systeme normieren (wie z.B., dass Rechtsverstöße nicht anonym gemeldet werden dürfen).

18. Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten

Ein Datenschutzbeauftragter muss gem. § 4 f BDSG in privatwirtschaftlichen Betrieben bestellt werden, in denen

- mehr als neun Personen ständig personenbezogene Daten automatisiert erheben/verarbeiten/nutzen oder
- mehr als 20 Personen ständig personenbezogene Daten auf nicht automatisiertem Wege verarbeiten.

Laut der Neufassung des § 4f Abs. 3 BDSG von Juli 2009 ist eine ordentliche Kündigung des Datenschutzbeauftragten während seiner Amtsführung sowie bis ein Jahr nach seiner Abberufung unzulässig. Rechtlich unklar ist, ob der Betriebsrat ein Mitbestimmungsrecht gem. § 99 BetrVG (bzw. § 95 Abs. 3) hat.

Gem. § 28 **E-BDatG** muss jeder Betrieb mit mindestens 5,25 Beschäftigten einen *Beauftragten für den Beschäftigtendatenschutz* bestellen, dessen Funktion und Rechte mit leichten Abweichungen denen des betrieblichen Datenschutzbeauftragten entsprechen. In Betrieben, in denen nach dem BDSG ein betrieblicher Datenschutzbeauftragter bestellt werden muss, kann dieser zugleich die Funktion des Beschäftigtendatenschutzbeauftragten wahrnehmen. Ausdrücklich geregelt ist, dass der Beauftragte für den Beschäftigtendatenschutz einen Anspruch auf Freistellung von der Arbeit hat. Dem Betriebsrat ist zudem ein Mitbestimmungsrecht bei der Bestellung und Abberufung eingeräumt.

19. Schadensersatzansprüche der Beschäftigten

Bei Verstößen gegen Datenschutzbestimmungen sieht § 7 BDSG einen verschuldensabhängigen Schadenersatzanspruch vor und regelt eine Beweislastumkehr für den Zusammenhang zwischen einer unzulässigen Datenerhebung und einem eingetretenen Schaden. Ein Anspruch auf Entschädigung für *immateriellen* Schaden kann laut BGH nur bei schweren Eingriffen in das allgemeine Persönlichkeitsrecht direkt auf Art. 1 und 2 GG gestützt werden.



Anette Kramme

Mitglied des Deutschen Bundestages

§ 23 Abs. 2 **E-BDatG** sieht einen Anspruch auf Ersatz in Geld auch für Schäden vor, die nicht Vermögensschäden sind. Bei unverschuldeten Pflichtverletzungen des Arbeitgebers gilt eine Höchstgrenze von 250.000 €.

20. Unterlassungsansprüche der Beschäftigten/des Betriebsrats

Die Literatur erkennt bei Verletzung von Datenschutzrechten einen *Anspruch auf Unterlassung der Datenerhebung-, verarbeitung, -nutzung* des einzelnen Arbeitnehmers sowie ein Zurückbehaltungsrecht hinsichtlich der Daten an. Bei Verstoß gegen ein Mitbestimmungsrecht besteht laut BAG auch ein Unterlassungsanspruch des Betriebsrats gem. § 1004 BGB.

In § 23 Abs. 1 normiert **E-BDatG** einen Unterlassungsanspruch von Beschäftigten für den Fall, dass ein Arbeitgeber voraussichtlich Beschäftigtendaten entgegen den Vorschriften des BDatG verwenden wird.

21. Ansprüche der Beschäftigten auf Löschung, Berichtigung und Sperrung von Daten

Nach § 35 BDSG hat ein Beschäftigter Anspruch auf **Löschung** von Daten, wenn

- sie auf unzulässige Weise erhoben wurden oder
- die Speicherung im Hinblick auf den mit der Datenerhebung verfolgten Zweck nicht mehr erforderlich ist.

Zudem besteht ein Anspruch auf **Berichtigung** erhobener Informationen, wenn diese inhaltlich falsch gespeichert sind, und auf **Sperrung**, wenn die Richtigkeit der gespeicherten Daten bestritten wird und sich nicht nachprüfen lässt.

§ 22 **E-BDatG** statuiert ebenfalls eine Pflicht des Arbeitgebers, unrichtige Beschäftigtendaten zu berichtigen. Sie müssen gelöscht werden,

- wenn sie für den Erhebungszweck nicht mehr erforderlich sind oder
- die Speicherung unzulässig war. Daten sind zu sperren, wenn die Richtigkeit bestritten wird und sich nicht nachprüfen lässt oder wenn eine gesetzlich geforderte Löschung unverhältnismäßig aufwändig wäre.

22. Ordnungswidrigkeits-/ Straftatbestände

Verstöße gegen das BDSG können gem. §§ 43, 44 BDSG als Ordnungswidrigkeit mit einem **Bußgeld** von bis zu 300.000 € bzw. von bis zu 30.000 € (bei Verstößen gegen bestimmte formale Anforderungen) geahndet werden. (Die Höchstgrenzen waren bis Juli 2009 noch etwas niedriger). Die Grenzen können im Einzelfall auch überschritten werden. Bei Bereicherungs- oder Schädigungsabsicht kann ein Verstoß als **Straftat** mit einer Freiheitsstrafe von bis zu 2 Jahren oder mit Geldstrafe bestraft werden.

§§ 35, 36 **E-BDatG** stellen Ordnungswidrigkeitstatbestände auf, die sich auf Verstöße gegen die Bestimmungen des BDatG beziehen und mit einem Bußgeld von 300.000 € bzw. 50.000 €



Anette Kramme

Mitglied des Deutschen Bundestages

geahndet werden. Bestimmte Verstöße werden bei Bereicherungs- oder Schädigungsabsicht als Straftat geahndet.

23. Zulässigkeit der prozessualen Verwertung unzulässig erhobener Daten

Die Rechtsprechung nimmt zudem bei Verletzung des allgemeinen Persönlichkeitsrechts oder von Vorschriften des BDSG ein **Beweisverwendungsverbot** der gewonnenen Informationen z.B. in einem Kündigungsschutzprozess an. Die Reichweite ist jedoch umstritten. Umstritten ist auch, ob eine unterlassene Betriebsratsbeteiligung ein Beweisverwendungsverbot der gewonnenen Informationen nach sich zieht.

§ 22 Abs.1 **E-BDatG** verbietet dem Arbeitgeber, Beschäftigtendaten, die durch eine unzulässige Erhebung gewonnen wurden, zu verwenden.

Eine klarstellende Regelung, dass auch eine unterlassene Betriebsratsbeteiligung ein Beweisverwendungsverbot nach sich zieht, könnte sinnvollerweise ergänzt werden.