

## Literaturüberblick

### **Mitarbeiterkontrolle**

Unter der Überschrift „Fernmeldegeheimnis und Datenschutz bei der Mitarbeiterkontrolle“ untersucht Prof. Dr. Dr. Manfred Löwisch in Der Betrieb (DB 51-52/09, Seite 2782) Anwendungsbereich und Eingriffsvoraussetzungen des Fernmeldegeheimnisses nach § 88 Telekommunikationsgesetz (TKG) sowie sein Verhältnis zum allgemeinen Datenschutzrecht. Seiner Meinung nach gilt auch bei zugelassener privater Nutzung das Fernmeldegeheimnis nicht. Seine Durchbrechung könne nicht durch Betriebsvereinbarungen gerechtfertigt werden (§ 88 Abs. 3 Satz 3 TKG). Der Beitrag geht insbesondere auch auf § 32 Bundesdatenschutzgesetz ein und widmet sich unter dem Oberbegriff „Verhältnismäßigkeitsprüfung“ auch Screening-Maßnahmen zur Aufdeckung von Interessenskonflikten. Abschließend schildert Löwisch die Mitwirkungs- und Mitbestimmungsrechte von Betriebsrat und Sprecherausschuss. ■ SF

### **Google, Facebook & Co als Bewerberdatenbank für Arbeitgeber?**

Dieser Fragestellung gehen Dr. Christian Rolf und Michael Röttinger in ihrem Aufsatz in der Zeitschrift Recht der Datenverarbeitung (RDV 6/09, Seite 263) nach. Ihr Ergebnis: „Die Online-recherche lässt sich zwar nicht auf § 32 BDSG stützen. Allerdings bietet § 28 Abs. 1 Satz 1 Nr. 3 BDSG, der durch § 32 BDSG nicht verdrängt wird, eine ausreichende Rechtsgrundlage, mit der der Arbeitgeber auf allgemein zugängliche Informationen zugreifen darf, die er über einen Bewerber findet. Unzulässig ist der Zugriff auf Daten, die ersicht-

lich das Persönlichkeitsrecht des Bewerbers verletzen und damit auch der Zugriff auf solche Daten, die der Bewerber in einem sozialen Netzwerk ausschließlich privaten Nutzern zur Verfügung stellt oder gestellt haben will. Im Übrigen sollte sich jeder Arbeitgeber darüber klar sein, dass im Internet gewonnene Erkenntnisse über einen Bewerber mitunter von begrenztem Wahrheitsgehalt sind. Als alleinige Entscheidungsgrundlage wird ein verständiger Personalleiter das Internet somit nicht nutzen.“

■ HK

### **Fragerecht zu Krankheitsdaten**

Stephanie Iraschko-Luscher und Pia Kiekenbeck gehen in der Neuen Zeitschrift für Arbeitsrecht (NZA 22/09, Seite 1239) der Frage nach, welche Krankheitsdaten der Arbeitgeber von seinen Mitarbeitern abfragen darf. Sie untersuchen das Fragerecht in den verschiedenen Phasen des Vertragsverhältnisses (Anbahnung, Durchführung und Beendigung). Fazit: „Viele Unternehmen wollen dazu übergehen, Standards für diese Fragen, gegebenenfalls in Zusammenarbeit mit der Arbeitnehmervertretung, zu entwickeln und zu etablieren. Dabei muss der Erforderlichkeitsgrundsatz im Mittelpunkt jeglicher Betrachtung stehen. Denn, was bei einem Dienstleistungsunternehmen an Gesundheitsfragen notwendig sein mag, kann in einem Handwerksunternehmen völlig irrelevant sein.“ ■ HK

### **Gleichbehandlungsgesetz**

„Das AGG nennt als verbotene Diskriminierungsmerkmale unter anderem die Rasse und die ethnische Herkunft. Beide Merkmale

werden im Gesetz aber nicht definiert, was zu Auslegungsproblemen führt. Im folgenden wird daher untersucht, ob die Anforderung eines Passfotos und die Suche nach dem `muttersprachlichen Mitarbeiter (m/w)` den Tatbestand einer verbotenen Diskriminierung erfüllt.“ Diese einleitende Erläuterung ist dem Beitrag von Prof. Dr. Joachim Gruber mit dem Titel „Zwei problematische Punkte des AGG: Die Anforderung eines Passfotos und die Suche nach dem `muttersprachlichen Mitarbeiter (m/w)`“ in der Neuen Zeitschrift für Arbeitsrecht (NZA 22/09, Seite 1247) vorangestellt. ■ HK

### **Telekommunikationsrecht**

„Die Entwicklung des Telekommunikationsrechts in den Jahren 2007 - 2009“ beschreiben Prof. Dr. Joachim Scherer und Caroline Heinickel in der Neuen Zeitschrift für Verwaltungsrecht (NVwZ 22/29, Seite 1405). In Kapitel VIII des Beitrages werden auch Entwicklungen des Fernmeldegeheimnisses, Datenschutzes und der öffentlichen Sicherheit dargestellt. ■ HK

### **Personaldatenverarbeitung in verteilten Systemen**

Zunehmend werden Personaldaten nicht mehr nur im eigenen Unternehmen verarbeitet, sondern an weltweit tätige Unternehmen verschickt beziehungsweise wird Unternehmen Zugang zu den Daten ermöglicht. In dem Beitrag „Datenverarbeitung außerhalb der eigenen vier Wände“ in der Zeitschrift Computer und Arbeit (CuA 12/09, Seite 20) schildert Thomas Michler, wie der Schutz von Mitarbeiterdaten bei weltweit verteilten Systemen

sichergestellt werden kann und wie die Belegschaftsvertretung die Datenverarbeitung auch außerhalb des eigenen Unternehmens im Sinne der Beschäftigten mitbestimmen kann. ■ HK

### Unternehmensverkäufe

„Datenschutz bei Unternehmenstransaktionen – Ein Überblick über Rechtslage und Diskussionsstand sowie Auswirkungen der BDSG-Novelle II“ ist der Beitrag von Dr. Robert Selk in der Zeitschrift *Recht der Datenverarbeitung* (RDV 2/09, Seite 254) überschrieben. Er gibt einen Überblick über den Diskussionsstand der letzten zehn Jahre in der Literatur, wichtige Urteile und die Auffassung der Datenschutzbehörden und beschreibt die möglichen Änderungen durch die Novellierung. ■ HK

### Tätigkeitsberichte

Dr. Kai von Lewinsk und Hajo Köppen plädieren unter der Überschrift „Tätigkeitsberichte der Datenschutzbehörden – Neuer Zugang zu sprudelnden Quellen“ in der Zeitschrift *Recht der Datenverarbeitung* (RDV 2/09, Seite 267) für eine systematische Erschließung des in den Datenschutzberichten gesammelten Erfahrungswissens für die wissenschaftliche Forschung und praxisbezogene Anwendung. Als neues Mittel zur Erreichung dieser Zielsetzung wird das digitale Archiv mit allen bisher erschienenen Tätigkeitsberichten in dem neuen Internetportal [zaftda.de](http://zaftda.de) vorgestellt. Im Anhang zu dem Beitrag findet sich eine Tabelle mit den Fundstellennachweisen (Landtagsdrucksachen) aller seit 1971 (1. Tätigkeitsbericht in Hessen) erschienenen Datenschutzberichte. ■ HK

### Parteien vernachlässigen Datenschutz

In der Zeitschrift *FifF-Kommunikation* (FifF-Kom 4/2009, Seite 18) des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung stellen Nils Lepperhoff und Björn Petersdorf die Ergebnisse ihrer Studie „Parteien und Datenschutz – Datenschutzpraxis deutscher Parteien und parteinaher Organisationen“ vor. Analysiert wurden unter anderem die Verfahren bei Online-Spenden oder das Vorhandensein eines datenschutzrechtlich vorgeschriebenen Verfahrensverzeichnis. Die Studie kommt zu dem Ergebnis, dass keine der im Deutschen Bundestag vertretenen Parteien beim Thema Datenschutz uneingeschränkt gesetzeskonform handelt. ■ HK

### „Hackerparagraph“

Bei der Schaffung des neuen § 202c Strafgesetzbuch (StGB) wurde intensiv diskutiert, ob der objektive Tatbestand der Strafvorschrift auch solche Computerprogramme umfasst, die sowohl für Straftaten wie auch zur Überprüfung der IT-Sicherheit eingesetzt werden können (sogenannte Dual-Use-Tools). Das Bundesverfassungsgericht (BVerfG) hat mit Beschluss vom 12. Mai 2009 geklärt, dass Dual-Use-Tools keine tauglichen Tatobjekte des § 202c StGB darstellen. In der Zeitschrift *Datenschutz und Datensicherheit* (DuD 12/09, Seite 742) beschreibt Heidi Schuster in dem Artikel „Der Hackerparagraph – ein kurzes Intermezzo?“ die Entstehungsgeschichte und die Tatbestände der Norm und die Position des BVerfG. ■ HK

### Data Loss Prevention

„An die Kette – Werkzeuge gegen Datenklau“ – unter diesem Titel liefert Max Ziegler, Berater bei

der *cirosec GmbH*, in der Zeitschrift *c't* (Heft 3/10, Seite 138) einen gut verständlichen Einstieg in das Thema *Data Loss Prevention* (DLP). Lobenswert ist insbesondere, dass er eine möglichst frühzeitige Einbindung des Betriebsrates und die Berücksichtigung der Datenschutzregelungen bei der Planung von DLP-Systemen empfiehlt, da diese Systeme auch zur Überwachung und Analyse des Mitarbeiterverhaltens benutzt werden können. ■ SF

### Netzneutralität und Deep Packet Inspection (DPI)

Axel Spies und Frederic Ufer geben in der Zeitschrift *Multimedia und Recht* (MMR 1/10, Seite 13) einen kurzen Einblick in die Themen und die auch für Deutschland relevante Rechtsentwicklung in den Vereinigten Staaten. Die Technik lässt es heute zu, dass die Datenströme in Netzwerken in Echtzeit kontrolliert werden. Diese Echtzeitkontrolle ermöglicht Ausschluss von bestimmten Inhalten und Wahrnehmung des Abrufs bestimmter Inhalte. Weitere Beispiele des Eingriffs: Ausschluss von Anwendungen wie Bittorrent-Dienste, Beschleunigen von Datenströmen nach Entscheidung des Netzbetreibers und eigenmächtiger Ausschluss von unerwünschten Website-Inhalten. So lässt sich beispielsweise durch den Provider gezielt bestimmte Werbung an den User senden. Das Besondere liegt darin, dass die Kontrolle von den Providern und nicht beispielsweise von dem zivilrechtlichen Vertragspartner betrieben wird. Da hier an der Quelle, nämlich direkt am Datenstrom, eingegriffen wird, hat sich eine erhebliche Diskussion über das offene und freie Internet ergeben. Die Entwicklung sollte auch der Datenschutzbeauftragte im Auge behalten. ■ PK