

etwa in Form eines endgültig lektorierten Dokuments. Unverständnis in der hinsichtlich des üblichen Ablaufs von Gesetzgebungsverfahren weitgehend uninformierten breiten Öffentlichkeit löste vor allem der Umstand aus, dass die zweite und die dritte Lesung zusammen in einem Durchgang erfolgte, der insgesamt kaum eine Minute dauerte.

Angesichts des ausgesprochen negativen öffentlichen Echos distanzierte sich selbst die *Bundesregierung* unverzüglich von dem Gesetzesbeschluss des *Bundestags* und erklärte, sie gehe davon aus, dass es in diesem Punkt bei der Beratung des BMG im *Bundesrat*, mit der allerdings nicht vor September 2012 zu rechnen ist, noch zu Änderungen kommen werde. Da es sich um ein zustimmungspflichtiges Gesetz handelt und gerade die großen Bundesländer parteiüber-

greifend signalisiert haben, dass sie die Gesetzesvorlage in dieser Form im *Bundesrat* nicht passieren lassen werden, ist mit einer erneuten Änderung in der Tat fest zu rechnen. Wahrscheinlich wird sie darauf hinauslaufen, dass die ursprünglich vorgesehene Opt-in-Regelung wiederhergestellt wird. Im Ergebnis hätte die zunächst scheinbar höchst erfolgreiche Lobbyarbeit der Werbe- und der Adresshandelsbranche damit das Gegenteil dessen erreicht, was sie beabsichtigt hatte.

■ Vgl. zur Fortentwicklung des Melderechts und zur Neuregelung *Petri*, ZD 2012, 403 – in diesem Heft. Vgl. auch die Diskussion im Beck-Blog sowie ZD-Aktuell 2012, 02934 und die Stellungnahme des *BfDI*, ZD-Aktuell 2012, 03025.

Dr. Eugen Ehmann
ist Regierungsvizepräsident von Mittelfranken in Ansbach.

vgl. Art. 141 Abs. 3 Bayerische Verfassung (BV). Das *Landesamt für Datenschutzaufsicht* als Aufsichtsbehörde nach § 38 BDSG lässt unter engen Voraussetzungen eine Überwachung zu. Denn § 6b Abs. 1 BDSG gestattet eine Überwachung öffentlich zugänglichen Raums, soweit dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für überwiegende schutzwürdige Interessen der Betroffenen vorliegen. Zwar wird im Regelfall bei frei zugänglichen Stellen das schutzwürdige Interesse der betroffenen Waldbesucher überwiegen, für entlegene Örtlichkeiten kann allerdings ausnahmsweise anderes gelten. Demgegenüber hat der *Bayerische Landesbeauftragte für den Datenschutz* das *Bayerische Staatsministerium für Ernährung, Landwirtschaft und Forsten* bereits darauf hingewiesen, dass eine Videoüberwachung durch die staatliche Forstverwaltung grundsätzlich nicht in Betracht kommt. Der Grund für die strengere Beurteilung: Art. 21a Abs. 1 BayDSG verlangt, dass die Videoüberwachung zum Schutz näher definierter hochwertiger Rechtsgüter erforderlich ist. Die Überwachung durch Wildkameras dient jedoch nicht dem Schutz derartiger Schutzgüter.

Dr. Thomas Petri
ist der Bayerische Landesbeauftragte für den Datenschutz und Mitglied des Wissenschaftsbeirats der ZD.

Thomas Petri „Schäferstündchen“ in Kärnten löst Datenschutzdebatte über Wildkameras aus

ZD-Aktuell 2012, 03038

Das Schäferstündchen eines Regionalpolitikers aus Kärnten hat in Österreich und Bayern eine Debatte über die datenschutzrechtliche Zulässigkeit von Wildkameras ausgelöst.

An und für sich werden solche Kameras vor allem eingesetzt, um den Wildbestand zu kontrollieren. Dabei werden jedoch immer wieder auch Menschen aufgenommen. So erwischte eine Wildkamera einen Kärntner Politiker beim Schäferstündchen. Seither wird in Österreich über die Melde- und Kennzeichnungspflicht von Wildkameras diskutiert (zu den Voraussetzungen einer Videoüberwachung in Österreich vgl. §§ 50a-50d öDSG 2009).

In Hessen wurde ein Jäger an einer Lockfütterstelle heimlich abgebildet. Bekannt wurde dieser Vorfall, weil ein anderer Jäger, der die Kamera angebracht hatte, über den Aufgenommenen hergezogen sein soll (vgl. dazu *Dienstbühl*, NuR 2012, 395). Ein Antrag der *SPD-Fraktion* im *Bayerischen Landtag* soll nun zur Klärung der datenschutzrechtlichen Zulässigkeit von Wildkameras beitragen (vgl. BayLT-Drs. 16/12803). Auf Grund der unterschiedlichen Gesetzeslage werden die beiden zuständigen Datenschutzbehörden

in Bayern jeweils für ihren Kontrollbereich zu unterschiedlichen Bewertungen gelangen.

Übereinstimmend gehen die Datenschutzbehörden zunächst davon aus, dass der Wald im Freistaat Bayern einen öffentlich zugänglichen Raum darstellt,

Axel Spies USA: Privacy-Verhaltenskodex kommt nicht recht aus den Startlöchern

ZD-Aktuell 2012, 02918

Das *US-Department of Commerce* hat am 12.7.2012 ein Treffen mit Vertretern der *US-Wirtschaft* abgehalten, um über freiwillige Verhaltenskodizes für die Wirtschaft zu sprechen, die den Online-Datenschutz für Verbraucher verbessern sollen. Der Schwerpunkt liegt auf dem Bereich von Mobilfunkanwendungen (Apps etc.). Solche Kodizes sind in der vom Weißen Haus im Februar 2012 vorgestellten *Consumer Privacy Bill of Rights* (s. Spies, ZD-Aktuell 2012, 02788) vorgesehen und von der *US-Regierung* sehr erwünscht. Von der Industrie selbst ausgearbeitete Verhaltensrichtlinien sind unerlässlich, um dieses Dokument, das noch

nicht vom *US-Kongress* gebilligt ist, in die Praxis umzusetzen. Obgleich es Unternehmen freisteht, ob sie die von der Industrie entwickelten Verhaltenskodizes annehmen, müssen diejenigen Unternehmen, die dies tun, mit Maßnahmen und Sanktionen der *Federal Trade Commission (FTC)* rechnen, wenn sie ihre Versprechen nicht einhalten und die Regeln nicht intern vollständig umsetzen.

Der Schwerpunkt der gut besuchten Sitzung beim *US-Department of Commerce* war das Thema, wie dem Verbraucher mehr Transparenz zum Datenschutz bei mobilen Anwendungen gewährt werden kann. Federführend ist die *National Tele-*

communications und Information Administration (NTIA) – eine Behörde innerhalb des US-Department of Commerce. Ein großer Teil der ganztägigen Sitzung wurde damit verbracht, dass die Teilnehmer versuchten, sich auf ein Verfahren zu verständigen, mit dem man tatsächlich zu Verhaltensrichtlinien für die Industrie gelangt. Am Ende der Sitzung kündigte ein Beamter der NTIA an, dass die Behörde ein weiteres Treffen in Washington im August 2012 veranstaltet, um den Prozess voranzubringen. Die Regierungsvertreter betonten in diesem Zusammenhang mehrmals, dass die NTIA nur ein ehrlicher Makler sei und dass die eigentlichen Verhandlungen zwischen den Industrievertretern, Datenschützern und anderen Gruppen, die an dem Treffen als „Stakeholders“ teilnehmen, geführt werden müssten.

Zuerst bei den Apps ansetzen?

Die den Daten- und Verbraucherschutz vertretenden Teilnehmer betonten, dass es zu wenig sei, sich nur auf mobile Anwendungen, wie den praktisch wichtigen Datenschutz für Apps, zu fixieren; dieses Problem sei nur im Kontext der anderen Grundsätze in der vorgeschlagenen Privacy Bill of Rights zu lösen. Zu diesen Vertretern gehört z.B. die einflussreiche American Civil Liberties Union. Unterstützung fand dieser Ansatz von dem Vertreter der Association for Competitive Technology, die einige App-Entwickler vertritt. Andere Vertreter der Industrie äußerten Widerstand gegen die Erweiterung des Verfahrens über das ursprüngliche Thema hinaus, da die Diskussion ohne die Fokussierung auf Apps, zu denen die NTIA bereits schriftlich um Kommentare gebeten hatte, ziellos und zwecklos sei. Die Diskussion benötige einen konkreten Ausgangspunkt, hieß es. NTIA-Direktor Larry Strickling ließ in seiner Eröffnungsrede offen, welchen Ansatz seine Behörde bevorzugt. NetChoice, eine Gruppe, die Online-Unternehmen wie eBay, Facebook und Yahoo repräsentiert, ließ sich in der Sache so ein, dass die Informationen, die eine App über die Nutzer speichert, wie deren Standort, „erheblichen Wert“ hat und es dem Nutzer ermöglicht, Entscheidungen zu treffen. Für die NTIA steht einiges auf dem Spiel, da die Sicherstellung des Datenschutzes mittels Verhaltenskodizes, wie eingangs bemerkt, einer der Schwerpunkte der Consumer

Privacy Bill of Rights ist. Deswegen wird die Behörde den Prozess mit einiger Energie weiter verfolgen.

EPIC und Consumer Watchdog: Konkrete Vorschläge bei der FCC eingereicht

Die Privacy-Diskussion geht gleichzeitig auf der Ebene der Federal Communications Commission (FCC) weiter, auch wenn derzeit wegen des andauernden Wahlkampfes in den USA keine konkreten Gesetzesbeschlüsse zur Privacy auf der Ebene des US-Kongresses zu erwarten sind. Mittlerweile hat die international bekannte Datenschutzorganisation EPIC und die Verbraucherschützer von Consumer Watchdog am 13.7.2012 gemeinsame Kommentare bei der FCC im Verfahren „Privacy and Security of Information Stored on Mobile Communications Devices“ (CC Docket No. 96–115; DA 12–818) eingereicht. Das Verfahren greift Überlegungen der FCC aus dem Jahre 2007 wieder auf. Ein Schwerpunkt der von den beiden Organisationen eingereichten Kommentare ist es, dass die Anbieter von Mobilfunkdiensten die Einwilligung der Endnutzer vor der Nutzung ihrer personenbezogenen Daten für bestimmte Zwecke einholen sollen, und zwar im Wege des Opt-in – im Gegensatz zum in den USA gebräuchlichen Opt-out-System. Die Autoren der Kommentare berufen sich u.a. auf einen Bericht der

FTC vom vergangenen März, wonach allen US-Unternehmen empfohlen wird, die ausdrückliche Zustimmung der Verbraucher einzuholen, bevor sie personenbezogene Daten der Nutzer an Dritte außerhalb des jeweiligen Konzernverbands übermitteln. Die beiden Organisationen empfehlen auch den Gebrauch einer „Do Not Track“-Liste für Verbraucher und eine stärkere Zweckbindung der gesammelten Daten. Für sensitive Daten sollte wie in Europa eine ausdrückliche Zustimmung vorgesehen werden. Der Zugang der Verbraucher zu den über sie gespeicherten Daten soll ebenfalls ausgebaut werden.

Die Mobilfunkbetreiber AT&T Inc., Sprint Nextel Corp. und Verizon Communications Inc. sowie die Vertreter der Werbeindustrie wie Ad Biz haben sich erwartungsgemäß in dem genannten FCC-Verfahren gegen neue Datenschutzregelungen für Mobilfunkanwendungen ausgesprochen. Deren Vertreter sind der Ansicht, dass bessere Transparenz und Verbraucherschutz bei der Privacy zwar erstrebenswert seien, aber die von der FCC vorgegebenen Regeln wettbewerbshemmend seien und den „enormen Wert des mobilen Marketing“ vermindern würden. Ein geeignetes Forum für Industriestandards sei die Digital Advertisement Alliance (DAA), nicht die FCC. Die CTIA, welche die Mobilfunkbetreiber vertritt, stellt in ihrer Eingabe die Kompetenz der

Rezensionen · Tagungsberichte · Termine · Rezensionen · Tagungsberichte

NEU AUF DER HOMEPAGE

www.zd-beck.de

Rezensionen

- **Tim Wybitul** Klaus Moosmayer, Compliance. Praxisleitfaden für Unternehmen, München (C.H. Beck) 2. Aufl. 2012, ISBN 978-3-406-62821-4, € 34,90
- **Dr. Christoph Schnabel** Hermann Krallmann/Alfred Zapp (Hrsg.), Bausteine einer vernetzten Verwaltung. Prozessorientierung – Open Government – Cloud Computing – Cybersecurity, Berlin (Erich Schmidt) 2012, ISBN 978-3-503-13878-4, € 49,95
- **Dr. Sebastian Kraska** Johanna Schmidt-Bens, Cloud Computing Technologien und Datenschutz, Edewecht (oIWIR) 2012, ISBN 978-3-939704-71-3, € 24,80

Termine + Termine + Termine + Termine + Termine + Termine + Termine

FCC zur Regelung der Privacy bei Mobilfunkanwendungen in Frage.

Kurz zum Hintergrund: Einer der Gründe, warum die FCC das Verfahren zur Privacy bei Mobilfunkanwendungen im Jahre 2007 eingestellt hatte, war, dass die Behörde damals den Schwerpunkt auf das Löschen von Kundendaten bei „instandgesetzten“ (refurbished) Mobiltelefonen gelegt hatte, die dann wieder verkauft oder auf andere Kunden verteilt wurden. Die Mobilfunkbetreiber hatten damals argumentiert, dass sie diesen Prozess nicht kontrollieren könnten. Die FCC folgte diesem Argument damals. In dem jetzt wieder aufgenommenen Verfahren stehen andere, weitaus brisantere Themen im Fokus, wie die rechtliche Zulässigkeit von Software, die auf Smartphone-Apps installiert wird und Daten von Kunden auf den Telefonen zur Übermittlung ohne Wissen oder Zustimmung des Kunden

sammelt (Carrier-IQ-Kontroverse). Die FCC argumentiert in dem noch laufenden Verfahren, dass Carrier, die ihre Kunden nicht über solche Software oder ihre Datenpraktiken informieren, gegen Sec. 222 des Communications Act von 1934 verstoßen, wonach alle Kundendaten zu schützen sind, die „einem Carrier allein auf Grund der Netzbetreiber-Kunden-Beziehung zur Verfügung gestellt werden.“ Die *Federal Trade Commission (FTC)* hat unabhängig von der FCC vor kurzem eigene Workshops zum Thema „Privacy im Mobilfunksektor“ abgehalten und hat mehr als ein Dutzend Maßnahmen zur Durchsetzung der Datensicherheit im Bereich der mobilen Anwendungen gegen Unternehmen eingeleitet.

Dr. Axel Spies
ist Rechtsanwalt bei Bingham McCutchen in Washington DC und Mitherausgeber der Zeitschrift ZD.

Der gegen die ablehnende Entscheidung des LAVES erhobene Klage des SWR hat das VG Oldenburg stattgegeben. In der mündlichen Urteilsbegründung führte es aus, dass das Auskunftsbegehren wegen der Stellung des Klägers als Vertreter der Presse neben dem ursprünglich geltend gemachten Anspruch aus dem VIG auch nach dem Niedersächsischen PresseG zu beurteilen sei. Ein solcher presserechtlicher Auskunftsanspruch bestehe im vorliegenden Verfahren. Bei sorgfältiger Abwägung der entgegenstehenden Interessen sei hier dem öffentlichen Interesse an einer möglichen Berichterstattung über die lebensmittelrechtlichen Beurteilungen der Vorrang gegenüber dem privaten Interesse der betroffenen Lebensmittelhersteller an der Vermeidung einer negativen Berichterstattung einzuräumen. Zwar sei in diesem Zusammenhang zu berücksichtigen, dass die Beurteilungen der genommenen Proben aus den vom LAVES genannten Gründen unter Umständen nicht auf ein Fehlverhalten der Hersteller zurückzuführen seien. Der SWR sei aber zur ordnungsgemäßen journalistischen Verwendung und Verarbeitung der erteilten Auskünfte verpflichtet und müsse diesen Umstand i.R.d. ihm obliegenden Verpflichtung zu einer differenzierten und ausgewogenen Berichterstattung berücksichtigen.

■ Vgl. auch VGH Kassel ZD 2012, 285 und ZD-Aktuell 2012, 30319.

VG Oldenburg: Auskunftspflicht des Niedersächsischen Landesamts bejaht

ZD-Aktuell 2012, 03020

Das VG Oldenburg hat (U. v. 26.6. 2012 – 7 A 1405/11; ZD wird die Entscheidung demnächst veröffentlichen) einer Klage des *Südwestrundfunks (SWR)* auf Gewährung von Auskünften in lebensmittelrechtlichen Fragen stattgegeben.

Im Mai 2008 beantragte der SWR beim *Niedersächsischem Landesamt für Verbraucherschutz und Lebensmittelsicherheit (LAVES)* unter Berufung auf das Verbraucherinformationsgesetz (VIG) die Mitteilung der Namen der Hersteller, deren Fleischprodukte bei einzelnen Proben in den Jahren 2006 und 2007 vom LAVES als gesundheitsschädlich, nicht zum Verzehr geeignet oder gesundheitsgefährdend beurteilt wurden. Daneben begehrte er die Nennung der Produktbezeichnungen sowie des jeweiligen Grundes für die Beurteilung.

Im Vorfeld seiner Entscheidungen über diesen Antrag hörte das LAVES fast 300 Hersteller an. Den Auskunftsanspruch lehnte es danach teilweise – soweit nämlich die schutzwürdigen privaten Interessen der Hersteller entgegenstünden – ab. Z.T. seien die Proben nicht bei den Herstellern selbst, sondern im Einzelhandel genommen worden. Es sei möglich, dass der Verderb der Ware durch die Unterbre-

chung der Kühlkette außerhalb des Einflussbereichs des Herstellers eingetreten sei. Diesen Herstellern drohten durch die zu erwartende Berichterstattung erhebliche Umsatzeinbußen, ohne dass sie verantwortlich für den Warenverderb seien.

Markus Schröder OLG Karlsruhe: Datenschutzvorschriften sind Marktverhaltensregelungen

ZD-Aktuell 2012, 30110

Das OLG Karlsruhe hat mit U. v. 9.5.2012 - 6 U 38/11 (ZD 2012, 432) entschieden, dass es sich bei den §§ 4, 28 BDSG um Marktverhaltensregelungen i.S.v. § 4 Nr. 11 UWG handelt. Damit hat das OLG Karlsruhe in dieser umstrittenen Frage entgegen einer aktuellen Entscheidung des OLG München (ZD 2012, 330 m. Amn. Schröder), welches einen Marktbezug eben dieser Normen ablehnt hat, entschieden.

I. Der Kontext

Die Entscheidung hat die hoch umstrittene Frage zum Gegenstand, ob Normen des Datenschutzrechts Marktverhaltensregelungen i.S.v. § 4 Nr. 11 UWG sind.

Die Rechtsprechung ist in dieser Frage seit jeher uneinig. So haben das KG, das OLG Frankfurt/M., das OLG Hamburg, das OLG Düsseldorf und eben das OLG München entschieden, dass ein Marktbezug datenschutzrechtlicher Normen nicht gegeben sei (zum Streitstand vgl. Schröder, ZD 2012, 193). Regelmäßig wird dabei darauf abgestellt, dass sich der Schutz der informationellen Selbstbestimmung und der Schutz des Wettbewerbs gegenseitig ausschließen. Demgegenüber haben das OLG Köln, das OLG Stuttgart und das OLG Naumburg einen Marktbezug angenommen. Demnach könne eine datenschutzrechtliche Norm auch eine Marktverhaltensvorschrift sein,