23850

In Kooperation mit:
bitkom e.V.
BvD e.V.
davit im DAV
eco e.V.
VPRT e.V.

ZD ZEITSCHRIFT FÜR DATENSCHUTZ

AUS DEM INHALT

www.zd-beck.de

Seiten 149–200
7. Jahrgang 3. April 2017
Verlag C.H.BECK München

4/2017

O850201704

Zeitschrift für Datenschutz – ZD
www.zd-beck.de

Anke Zimmer-Helfrich | Chefredakteurin
RAin Katharina Joachim | Redakteurin
Karin Löscher, M.A. | Redaktionsassistentin

ZD FOKUS

Axel Spies US Court of Appeals for Second Circuit: Zugriff auf Server in Irland mittels Search Warrant erneut abgelehnt

ZD-Aktuell 2017, 05469

Das *Richterplenum* des *Second Circuit* hat am 24.1.2017 den Antrag der *US-Regierung* mit knapper Mehrheit abgelehnt, eine Entscheidung des *Gerichts* zu überdenken und abzuändern. Im Kern geht es darum, ob US-Dienstleister wie *Microsoft* dazu gezwungen werden können, E-Mails eines bestimmten Kontos, die im Ausland auf einem Server gespeichert sind, auf Grund eines Search Warrant an die US-Strafverfolgungsbehörden herauszugeben (Case Nr. 14-2985). Der Fall hatte auch in Europa hohe Wellen geschlagen (vgl. Urteil der *Richterkammer* des *Berufungsgerichts* v. 14.7.2016, ZD 2016, 480 m. Anm. *Schröder/Spies*).

In einer knappen 4 zu 4-Entscheidung mit drei Berufungsrichtern, die sich aus verschiedenen Gründen nicht an der Entscheidung beteiligt haben („recused"), wies das *Plenum* des *Berufungsgerichts* (sog. „en banc" hearing) den Antrag auf Neuverhandlung der einstimmigen Entscheidung der *Richterkammer* v. 14.7.2016 ab. Das Berufungsurteil der *Richterkammer* erging gegen ein viel beachtetes Urteil des *Untergerichts (US District Court Southern District of New York)*. Die *Richterkammer* hatte einen Durchsuchungsbefehl (Search Warrant) des *FBI* zur Herausgabe von in Irland auf einem Server gespeicherten E-Mails nach dem Stored Communications Act (SCA) aufgehoben. Hiergegen hatte sich die *US-Regierung* an das *Richterplenum* desselben *Gerichts* gewandt. Der Gleichstand der Richterstimmen „en banc" führte zur Ablehnung des Antrags.

Während die *Richter* der *Kammer*, die am 14.7.2016 für die Zurückweisung der Berufung verantwortlich waren, keine weitere Argumentation für ihre Entscheidung veröffentlichten, fügten die übrigen *Richter* dem Tenor, der die Wiedereinsetzung des Search Warrant ablehnte, ihre schriftlichen Begründungen von insgesamt 55 Seiten bei, die die starken Meinungsverschiedenheiten zwischen den beteiligten *Richtern* offenlegen.

In der den Beschluss tragenden Begründung der Berufungsrichterin *Susan L. Carney*, die von Richter *Gerald Lynch* und Richter *Victor Bolden*, die schon Teil der *Richterkammer* der Entscheidung vom 14.7.2016 waren, mitgetragen wird, ist im Einzelnen ausgeführt, dass die ursprüngliche Kammerentscheidung „vollständig erklärt", warum die Aufhebung des Search Warrant durch das genannte Fallrecht des *US Supreme Court* zur Exterritorialität und den Text des SCA gerechtfertigt sei.

Die *Richter* erhöhen mit der Entscheidung den Druck auf den Gesetzgeber. In ihrer 14-seitigen Stellungnahme bringt Richterin *Carney* klar zum Ausdruck, dass der SCA, der 1986 verabschiedet wurde, dringend einer gesetzgeberischen Reform bedürfe: „In vielerlei Hinsicht ist der SCA von [der] Technologie überholt worden", schreibt die *Richterin*. Eine Überarbeitung durch den *US-Kongress* solle weiterhin die Privatsphäre der Betroffenen schützen, aber auch die Interessen der internationalen Wirtschaft mit den Anforderungen an die Strafverfolgung und den Verpflichtungen des Dienstleistungserbringers im globalen Kontext, in dem dieser Fall spielt, mit der „Privacy" zum Ausgleich bringen.

Der Schwerpunkt der Entscheidung des *Gremiums* lag jedoch auf der Frage, wie das Gesetz derzeit ausgelegt werden muss – in Anbetracht der Tatsache, dass keine Indizien dafür vorliegen, dass der *Kongress* beabsichtigte, dass der SCA elektronische Daten, die von einem Dienstleister im Ausland gespeichert wurden, abdecken soll (vgl. *Schröder/Spies*, ZD 2016, 482). Die Forderung der *Regierung*, dass der Dienstleister die Daten eines Kunden auf seinen Servern in Irland abrufen soll, könne die Datenschutzbestimmungen des Staats an dem Ort, an dem die Daten gespeichert sind, nicht aushebeln, meint Richterin *Carney*.

Eine Sprecherin des *US-Justizministeriums* sagte als Reaktion, dass die Behörde die knapp ergangene Entscheidung und die abweichenden Meinungen umfassend prüfen werde, bevor weitere rechtliche Schritte unternommen werden. Denkbar sei eine Revision zum *US Supreme Court*, eine Weiterverfolgung der Angelegenheit in anderen Gerichtsbezirken und/oder eine Gesetzesinitiative zur Reform des SCA. Ein Reformgesetz ist angesichts der hiesigen Mehrheitsverhältnisse durchaus möglich, sodass dann Unternehmen, die der US-Gerichtsbarkeit

unterliegen, alle Daten, die im Ausland auf von den USA aus zugänglichen Servern belegen sind, bei einem entsprechenden gültigen Search Warrant im konkreten Fall vorlegen müssten.

■ Vgl. auch ZD-Aktuell 2014, 04309; *Schröder/Spies*, ZD-Aktuell 2014, 04315 und *Bezirksgericht Southern District of New York* ZD 2014, 346 m. Anm. *Schröder/Spies*; ferner *Spies*, ZD-Aktuell 2015, 04588.

Dr. Axel Spies
ist Rechtsanwalt in der Kanzlei Morgan Lewis & Bockius in Washington DC und Mitherausgeber der ZD.

Wolfgang Kuntz
LAG Berlin-Brandenburg: Kündigung wegen Datenschutzverstößen möglich

ZD-Aktuell 2017, 05464

Mitarbeitern eines Bürgeramts droht die fristlose Kündigung, wenn sie unbefugt personenbezogene Daten abrufen und weitergeben. Das gilt auch dann, wenn dies allein aus persönlicher Neugierde geschieht und Informationen nur wenige Personen betreffen.

In dem verhandelten Fall vor dem *LAG Berlin-Brandenburg* (ZD 2017, 193 – in diesem Heft) hatte die Mitarbeiterin eines Bürgeramts hunderte Male Melderegisterdatensätze von ihr bekannten Personen abgerufen. Darunter waren z.B. die Tochter ihres Freunds sowie ein Bekannter und dessen Ex-Frau. Dem Bekannten soll sie außerdem einmal die Daten seiner Ex-Frau weitergegeben haben, um ihn im Rahmen eines Unterhaltsstreits zu unterstützen. Das ist zwischen den Parteien allerdings umstritten. Als der massenhafte Abruf von Meldedaten aufgedeckt wurde, kündigte ihr der Arbeitgeber. Die mit Meldedaten beschäftigten Arbeitnehmer seien einem besonderen Geheimnisschutz verpflichtet. Die Kl. war wegen des Abrufs der Daten auch strafrechtlich verurteilt worden. Das Verhalten sei so schwerwiegend, dass eine fristlose Kündigung gerechtfertigt sei.

■ Vgl. auch *LAG Berlin-Brandenburg* ZD-Aktuell 2016, 05008; *Wybitul*, ZD 2015, 453 und *Brink*, ZD 2015, 295.

Wolfgang Kuntz
ist Rechtsanwalt und Fachanwalt für IT-Recht in Saarbrücken.

Paul C. Johannes Bundestag: Gesetz zum Abbau der Schriftform im Verwaltungsrecht des Bundes beschlossen

ZD-Aktuell 2017, 05489

Am 26.1.2017 beschloss der *Bundestag* das Gesetz zum Abbau verzichtbarer Anordnungen der Schriftform im Verwaltungsrecht des Bundes (BT-Drs. 18/10183). Das Artikelgesetz soll in 181 unterschiedlichen Gesetzen und Verordnungen 476 Rechtsvorschriften ändern, um Schriftformerfordernisse ganz zu streichen oder um die Möglichkeit der Nutzung einfacher elektronischer Verfahren, wie der einfachen E-Mail, zu ergänzen. Das Artikelgesetz bedarf der Zustimmung durch den *Bundesrat*.

Die Gesetzesinitiative ist im Kontext langjähriger Bemühungen zur Modernisierung der Verwaltungskommunikation zu sehen. In der Digitalen Agenda 2014-2017 der *Bundesregierung*, die dem Regierungsprogramm „Digitale Verwaltung 2020" zu Grunde liegt, wird die Überprüfung verwaltungsrechtlicher Formerfordernisse als eine Maßnahme genannt. Bereits 2013 trat das Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften in Kraft, welches das EGovG beinhaltet. Nach Art. 30 Abs. 2 EGovG hat die *Bundesregierung* die Pflicht, u.a. darüber zu berichten, in welchen verwaltungsrechtlichen Vorschriften des Bundes die Anordnung der Schriftform verzichtbar ist. Darauf folgte ein breit angelegtes Normenscreening (Bericht der *Bundesregierung* zur Verzichtbarkeit der Anordnungen der Schriftform und des persönlichen Erscheinens im Verwaltungsrecht des Bundes, BT-Drs. 18/9177). Dessen Empfehlungen sollen nun z.T. mit diesem Gesetz umgesetzt werden. So wurden Schriftformerfordernisse identifiziert, die mit dem Artikelgesetz entweder ersatzlos gestrichen werden (56 Rechtsvorschriften) oder die durch elektronische Verfahren ersetzt werden sollen (bei 420 Rechtsvorschriften wird die Formulierung „schriftlich oder elektronisch" ergänzt).

Bei der überwiegenden Zahl der zu streichenden oder zu ergänzenden Schriftformerfordernisse handelt es sich eher um Fälle mit begrenzter Relevanz für Bürger und Unternehmen. Es sind solche, die geschätzte Fallzahlen von weniger als 1.000 pro Jahr aufweisen (vgl. Stellungnahme des *Nationalen Normenkontrollrats*, NKR-Nr. 3703 v. 21.7.2016, S. 3). So darf z.B. die Erlaubnis zum Führen zusätzlicher Bezeichnungen zum Schutz gegen Wellenschlag, wie etwa eines roten Lichts bei Nacht, an Fahrzeugen auf der Donau gem. § 3.48 Nr. 2 lit. b der Anlage A zur Donauschifffahrtspolizeiverordnung durch die zuständige Behörde nun, man möchte ausrufen „endlich!", auch elektronisch erfolgen.

Zu beachten ist, dass mit dem Zusatz „oder elektronisch" in den geänderten Rechtsvorschriften nicht die elektronische Form gemeint ist, wie sie in § 126a BGB definiert ist. Gemeint sind auch nicht Ersatzmöglichkeiten der Schriftform nach § 3a Abs. 2 VwVfG (qualifizierte elektronische Signatur, De-Mail mit Absenderbestätigung, elektronisches Formular mit nPA-Identifizierung oder anerkanntes Bürgerportal). Diese Möglichkeiten bestehen ohnehin schon. „Elektronisch" soll, zur Vereinfachung der Verwaltungskommunikation, bedeuten, dass die Behörde grds. auch einfachere Kommunikationsmethoden, wie z.B. einfache E-Mail oder Messenger, verwenden kann. Die Gesetzesbegründung stellt klar, dass der Einsatz solcher einfachen elektronischen Kommunikationsmethoden zum einen von der tatsächlichen Zugangseröffnung auf Seiten des Empfängers abhängig ist (BT-Drs. 18/10183, S. 66). Zum anderen läge deren Einsatz im Ermessen der Behörden (a.a.O., S. 69). Es wird darauf hingewiesen, dass die jeweiligen Verwaltungen zu gewährleisten haben, dass auf personenbezogene Daten bei der elektronischen Übertragung, beim Transport oder bei ihrer Speicherung nicht unbefugt zugegriffen werden kann. Dies könne insbesondere durch Verschlüsselungsverfahren sichergestellt werden, die dem Stand der Technik entsprechen. Der Einsatz bestimmter elektronischer Verfahren wird nicht näher festgelegt. Dies soll eine größtmögliche Verfahrensflexibilität erlauben, da die jeweilige Behörde nach ihrem Ermessen und ohne gesetzliche Verpflichtung zur Nutzung eines bestimmten elektronischen Verfahrens beurteilen könne, welche Kommunikationsform und Sicherungsmethode sie für den jeweiligen Verfahrensschritt für ausreichend oder erforderlich hält. Inwiefern z.B. die einfache E-Mail als Kommunikationsweg tatsächlich ausreicht, muss jede Verwaltung verfahrensabhängig selbst