

Herausgeber:

Prof. Dr. Thomas Hoeren, Direktor des Instituts für Informations-, Telekommunikations- und Medienrecht (ITM), Universität Münster – Prof. Dr. Jochen Schneider, Rechtsanwalt, Kanzlei SSW Schneider Schiffer Weihermüller, München – Prof. Dr. Martin Selmayr, Kabinettschef von EU-Justizkommissarin Viviane Reding, Brüssel/Direktor des Centrums für Europarecht, Universität Passau – Dr. Axel Spies, Rechtsanwalt, Bingham McCutchen, Washington, D.C. – Tim Wybitul, Rechtsanwalt, FA für Arbeitsrecht, Head of Compliance & Investigations Hogan Lovells, Frankfurt/M./Lehrbeauftragter an der D.U.W., Berlin

Wissenschaftsbeirat:

Isabell Conrad, Rechtsanwältin, Kanzlei SSW Schneider Schiffer Weihermüller, München – Dr. Oliver Draf, LL.M., Leiter Datenschutz der Allianz Deutschland AG, München – Dr. Stefan Hanloser, Rechtsanwalt, München – Dr. Helmut Hoffmann, Richter am OLG Stuttgart a.D. – Prof. Dr. Gerrit Hornung, LL.M., Inhaber des Lehrstuhls für Öffentliches Recht, Informationstechnologierecht und Rechtsinformatik, Universität Passau – Prof. Dr. Jacob Jousen, Lehrstuhlinhaber für Bürgerliches Recht, Deutsches und Europäisches Arbeitsrecht und Sozialrecht, Ruhr-Universität Bochum – Thomas Kranig, Präsident des Bayerischen Landesamtes für Datenschutzaufsicht, Ansbach – Dr. Thomas Petri, Der Bayerische Landesbeauftragte für den Datenschutz, München – Priv.-Doz. Dr. Andreas Popp, M.A., Privatdozent für Strafrecht, Strafprozessrecht, Kriminologie und Rechtsphilosophie, Universität Passau – Prof. Dr. Alexander Roßnagel, Universitätsprofessor für Öffentliches Recht, Universität Kassel/Leiter der Projektgruppe verfasungsverträgliche Technikgestaltung (provet) – Dr. Christian Schröder, Rechtsanwalt und Leiter des Fachbereichs IP/IT der BDO Legal Rechtsanwalts-gesellschaft mbH, Düsseldorf – Dr. Jyn Schultze-Melling, LL.M., Rechtsanwalt, Konzerndatenschutzbeauftragter der Allianz Gruppe, München – Prof. Paul M. Schwartz, Professor der Rechtswissenschaft an der University of California – Berkeley Law School/Direktor des Berkeley Center for Law & Technology, USA – Thorsten Sörup, Rechtsanwalt, Kanzlei Schiedermaier, Frankfurt/M. – Prof. Dr. Jürgen Taeger, Lehrstuhlinhaber für Bürgerliches Recht, Handels- und Wirtschaftsrecht sowie Rechtsinformatik, Universität Oldenburg/Vorsitzender der Deutschen Stiftung für Recht und Informatik (DSRI) – Florian Thoma, Rechtsanwalt in Neubuern, stv. Leiter des AK Datenschutz des BITKOM e.V./Member of the Board of Directors, International Association of Privacy Professionals (IAPP) – Prof. Dr. Marie-Theres Tinnefeld, Professorin für Datenschutz und Wirtschaftsrecht, Hochschule München

Christian Schröder / Axel Spies USA: Vorlage von E-Mails an US-Behörden, die auf Servern in Irland gespeichert sind – Neue Gefahren für US-Clouds?

ZD-Aktuell 2014, 03194

Ein neues Urteil des *US District Court Southern District of New York* (ZD 2014, 346 m. Anm. Spies/Schröder – in diesem Heft) sorgt gegenwärtig für einige Aufregung insbesondere in der Cloud Computing-Szene. Im Kern geht es darum, ob *Microsoft (MS)* als Internet Service Provider (ISP) E-Mails auf Grund einer Subpoena (Durchsuchungs- und Beschlagnahmebeschluss), die von einem US-Richter auf Antrag einer US-Behörde erlassen wurde, herausgeben muss, auch wenn diese für einen Kunden auf einem *MS*-Server in Dublin gespeichert sind. Ein Ermittlungsrichter des Gerichts, *Richter Francis*, hat diese Verpflichtung bejaht.

Richter Francis meint, dass ISP bei einem US-Beschlagnahmebeschluss die Herausgabe von E-Mails und anderen digitalen Informationen selbst dann nicht verweigern dürfen, wenn sich die Informationen auf Servern des Unternehmens außerhalb der USA befinden: „Der Aufstieg eines elektronischen Mediums, das alle geografischen Grenzen überschreitet, muss durch Gesetze geregelt werden, die vor keiner territorialen Souveränität haltmachen“, heißt es in der Urteilsbegründung. *MS* will die Entscheidung des *US-District Court* anfechten. *MS* ist der Ansicht, dass sich Durchsuchungsbeschlüsse eines US-Gerichts genauso wie im Offline-Bereich nicht auf Gebiete außerhalb des Territoriums der USA erstrecken können. Der gerichtliche Instanzenweg werde daher weiter beschritten. *MS* befände sich dabei insgesamt „auf einem langen Rechtsweg“, hieß es bei *MS*.

Ist die Schengen-Cloud tatsächlich eine „Datenfestung“?

Würde sich die Auffassung eines Einzelrichters eines US-District Court in New York verfestigen, würden grundsätzlich selbst dann keine bei US-Unternehmen gespeicherten Daten vor dem Zugriff von US-Behörden sicher sein, wenn sie auf Servern außerhalb der USA gespeichert sind. Damit würde die Strategie verschiedener US-Dienstleister, insbesondere EU-Datenschutzsorgen durch Verlagerung ihrer Server ins Ausland zu begegnen,

durchkreuzt. Die Auswirkungen einer solchen Rechtseinschätzung insbesondere auf die Cloud Computing-Industrie wären daher erheblich.

Die Zeitung „Die Welt“ (welt.de) interpretiert das (nicht rechtskräftige) Urteil so, dass der *Richter* damit „unfreiwillige Schützenhilfe für die Idee einer europäischen Datenfestung“ geleistet hat. Diese Einschätzung bezieht sich auf die Idee einer „Schengen-Cloud“ oder „Schland-Cloud“, die in Europa mit Unterstützung der Politik vorgebracht wird. Eine solche spontan getroffene Einschätzung ist jedoch durchaus fragwürdig. Bis heute ist unklar, was genau mit einer „Schengen-Cloud“, die schon von der Konzeption einige EU-Mitgliedstaaten ausschließen würde, überhaupt gemeint ist. Selbst wenn eine „Datenfestung“ innerhalb der Schengen-Länder technisch möglich ist, dürfte sie einer Mobilität der Nutzung von Daten nicht nur weltweit, sondern selbst innerhalb von Europa entgegenstehen.

Hinzu kommt, dass die europäischen Cloud-Anbieter zum großen Teil auch in den USA einen Geschäftssitz oder eine Niederlassung haben und insofern ebenfalls von US-Behörden aufgefordert werden könnten, Daten aus der EU für Zwecke der US-Behörden vorzulegen. Die vom *Richter* zitierte US-Vorschrift des ECPA (18 U.S.C. § 2703(b)(1)(B)(ii)) unterscheidet nicht zwischen inländischen und ausländischen Anbietern: „A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable.“ Sofern Rechtszuständigkeit (Jurisdiction) nach US-Recht besteht, könnte auch einem EU-Cloud-Anbieter eine Subpoena zugestellt werden – egal wo die Daten tatsächlich gespeichert werden. Ein Zugriff auf Daten des Anbieters i. R. d. internationalen Rechtshilfe ist ebenfalls denkbar. Was das im Einzelnen für die europäischen Cloud-Anbieter nach dem ECPA heißt, ist unklar. *Voigt* (MMR 2014, 158 ff.) hat letzters dazu ausgeführt: „Sogar die Anwesenheit von Mitarbeitern in den USA, z. B. bei einer Dienstreise, kann die Anwendbarkeit des

US-Rechts eröffnen“ (ebd., S. 160). Wie dem auch sei – auf jeden Fall kommt das Urteil für die US-Anbieter zur Unzeit. Ob die von EU-Cloud-Anbietern getätigte Aussage „die Daten sind sicher“ (vor der NSA) stichhaltig ist, hängt insofern vom konkreten USA-Bezug ab. Deshalb ist es angebracht, beim Cloud Computing die Aussage „Datenfestung Europa“ mit einem Fragezeichen zu versehen. Ein Rückzug Deutschlands in eine „Datenfestung“ liegt auch nicht im Interesse der eigenen Wirtschaft, die auf einen schnellen Datenaustausch (nicht nur zwischen den Schengen-Staaten) angewiesen ist.

Vielmehr ist das Urteil des Ermittlungsrichters *Francis* erkennbar von dem Bestreben geprägt, dass das einschlägige US-Recht im Lichte der seit Jahren bestehenden Rechtsprechung so auszulegen ist, dass sich der US-Justizgewalt unterliegende Unternehmen der Herausgabe von Daten nicht dadurch entziehen können, dass sie Datensätze außerhalb der USA speichern. Der *Richter* nahm ausdrücklich Bezug auf Überlegungen von *Google*, sich durch Offshore-Server dem Zugriff von jeglichen staatlichen Behörden zu entziehen. Der *Richter* hat insofern genau erkannt, dass das Territorialprinzip bei der Datenverarbeitung (Speicherung, Übermittlung usw.) im Zeitalter des Cloud Computing, wo Daten in Sekundenschnelle ihren Speicherort wechseln, ein Anachronismus ist. Bislang beruhen die meisten Datenschutzgesetze jedoch auf diesem Prinzip (ausf. dazu *Spies* AICGS Report (April 2014), German/U. S. Data Transfers Crucial for Both Economies, Difficult to Regain Trust). Auch die EU-Datenschutzreform scheint davon auszugehen.

Datentransfer in Zeiten des Cloud Computing

Das System der nationalen Datensouveränität (Data Sovereignty), das darauf basiert, dass sich jedes Land um den Schutz „seiner“ Daten“ kümmert (auch wenn diese das Land verlassen), wird den Anforderungen einer globalisierten Wirtschaft in Zeiten des Cloud Computing nicht mehr gerecht. An Diskussionen, wie internationale Datentransfers aus Deutschland in Zusammenarbeit mit den USA rechtlich in den Griff zu bekommen sind, mangelt es nicht (*Spies*, a. a. O.). Offen ist vorliegend ja auch die Frage, wie

sich das irische Datenschutzrecht zu dem Herausgabeverlangen verhält. Hierzu hat sich *Richter Francis* nicht geäußert. An dieser Stelle dürfte es noch einigen argumentativen Spielraum für *MS* geben. Möglicherweise wird sich auch die *EU-Kommission* mit der Kommissarin *Reding* in das Gerichtsverfahren als Beigeladene zu Gunsten von *MS* einschalten. Weitere transatlantische Konflikte sind vorprogrammiert. Der dem Weißen Haus zugeordnete US-Handelsbeauftragte (USTR) hat sich, wie im Beck-Blog v. 17.4.2014 berichtet, bereits sehr kritisch öffentlich zu den Plänen einer „Schengen-Cloud“ geäußert (vgl. welt.de). Die Pläne könnten gegen das Welthandelsabkommen WTO verstoßen. Es ist zu vermuten, dass die Diskussion über die Datenübermittlung in die USA weitergeht – ein „Großer Wurf“ zur Lösung ist nicht wahrscheinlich.

Dr. Christian Schröder

ist Rechtsanwalt und Leiter des Fachbereichs IP/IT der BDO Legal Rechtsanwaltsgesellschaft mbH in Düsseldorf sowie im Wissenschaftsbeirat der ZD.

Dr. Axel Spies

ist Rechtsanwalt in der Kanzlei Bingham McCutchen in Washington DC und Mitherausgeber der ZD.

AG München: Video-Türspion unzulässig ZD-Aktuell 2014, 04056

Das *AG München* hat (U. v. 4.12.2013 – 413 C 26749/13; ZD wird die Entscheidung demnächst veröffentlichen) festgestellt, dass die Überwachung eines Hausflurs mit einem Video-Türspion unzulässig ist. Dies gilt auch dann, wenn die Kamera aus Angst vor den Nachbarn eingesetzt wird.

Eine Mieterin brachte an der Eingangstür ihrer Etagenwohnung einen elektrischen Video-Türspion an, da sie Angst vor ihren Etagennachbarn hatte. Der Türspion übertrug tagsüber im Live-Modus das Geschehen im Hausflur im Bereich unmittelbar vor der Wohnungstür auf einen in der Wohnung befindlichen Bildschirm, fertigte aber keine Aufnahmen. In der Nacht war das Gerät auf „Automatikmodus“ geschaltet. Bei Aktivierung des Bewegungsmelders wurde die Videokamera ausgelöst und das Geschehen im Flur/Treppenhaus im Bereich vor der Tür der

Beklagten aufgezeichnet und gespeichert. Diese Aufnahmen konnten dann auf dem Bildschirm in der Wohnung oder einem PC angesehen werden. Die beklagte Mieterin sichtete morgens die Aufnahmen der vorangegangenen Nacht und löschte diese, sofern nichts Verdächtiges festgestellt wurde. Die Vermieterin forderte die Mieterin auf, die Kamera zu entfernen, da die Überwachung des Hauseingangs einen erheblichen Eingriff in das Persönlichkeitsrecht der Mitmieter und Besucher darstelle.

Das *AG München* gab der Vermieterin Recht. Das allgemeine Persönlichkeitsrecht gem. Art. 2 Abs. 1 GG gebe dem Einzelnen einen Anspruch auf Achtung der individuellen Persönlichkeit auch gegenüber einer Privatperson. Es umfasse auch die Freiheit vor unerwünschter Kontrolle oder Überwachung durch Dritte, insbesondere in der Privat- und Intimsphäre im häuslichen und privaten Bereich. Hier sei die Privatsphäre der Mieter und Besucher verletzt worden, da die Videoüberwachung und Aufzeichnung in der Nacht im häuslichen Bereich stattgefunden habe. Eine Überwachung des Hausflurs, der Hauseingangstür oder anderer gemeinschaftsbezogener Flächen sei grundsätzlich unzulässig, da diese Bereiche allgemein zugänglich seien und nicht dem alleinigen Hoheitsbereich der beklagten Mieterin unterständen oder ihrem alleinigen Hausrecht unterfielen. Da die beklagte Mieterin im Erdgeschoss des Anwesens wohne, müssten die übrigen Mieter bzw. deren Besucher an ihrer Wohnungseingangstür vorbei, um zu ihren Wohnungen zu gelangen. Somit würden sie, unabhängig von ihrem Verhalten, nachts gefilmt und die Aufnahmen würden gespeichert. Die Beklagte entscheide allein, ob die Aufnahmen gelöscht werden oder nicht. Dies stelle eine massive Verletzung des allgemeinen Persönlichkeitsrechts dar.

Das *Gericht* stellte weiter fest, dass dieser Eingriff auch nicht wegen der Streitigkeiten mit den Nachbarn gerechtfertigt war, da die Überwachung nicht zur Abwehr unmittelbar bevorstehender Angriffe auf die Person der Mieterin notwendig war. Die Fertigung und Speicherung von Aufnahmen sei völlig unabhängig von dem Verhalten der gefilmten Person erfolgt.

■ Vgl. auch *BGH* ZD 2013, 447; *BGH* ZD 2012, 176 und *LG München I* ZD 2012, 528.