dienfreiheit, der droht, wenn Informanten aus Furcht vor Enttarnung den Medien wichtige Hinweise vorenthalten. Im Gegenschluss hieße das, dass das Redaktionsgeheimnis nicht greife, wenn Interessen eines schützenswerten Dritten (namentlich des Informanten) nicht betroffen seien.

Vor der Beantwortung der Frage, ob dieser Schluss gültig ist, bedarf es einer Erklärung. Mit Vertraulichkeit des Verhältnisses zum Informanten ist nicht gemeint, dass der Informationsinhalt eine gewisse Qualität im Hinblick auf die sog. Sphärentheorie aufweisen müsse, dass etwa nur Informationen aus der Privat- und nicht der Öffentlichkeitssphäre dem Redaktionsgeheimnis unterliegen würden. Vielmehr geht es darum, dass ein Verhältnis zum Medium aufgebaut wird, in dem der Informant sein Anonymitätsbedürfnis ausdrücklich oder konkludent zum Ausdruck bringt oder sich ein solches aus den weiteren Umständen des Einzelfalls ergibt. Die Unterscheidung dieser beiden Anknüpfungspunkte ist wichtig, zumal sie in der aktuellen österreichischen Diskussion mitunter durcheinandergeraten. Ein Vertrauensverhältnis fehlt typischerweise, wenn mit versteckter Kamera gefilmt wird (vgl. *EGMR* BeckEuRS 1998, 230577 – Nordisk Film). Andersherum muss die öffentliche Wahrnehmbarkeit einer Information (etwa Fotos von illegalen Straßenrennen) die Annahme eines Vertrauensverhältnisses nicht zwangsläufig beseitigen (vgl. auch *EGMR*, MMR-Aktuell 2010, 308986 m.w.Nw. – Sanoma Uitgevers).

Zu klären ist nun, ob auch Informationen schützenswert sind, denen kein Vertrauensverhältnis zwischen Medium und Informant innewohnt. In Deutschland herrscht eine weite Begriffsvorstellung des Redaktionsgeheimnisses, die der polizeilichen Maßnahme eine besondere Verhältnismäßigkeitsprüfung nicht entzieht. Nach st. Rspr. des *BVerfG* schützt Art. 5 Abs. 1 Satz 2 GG nämlich auch die Vertraulichkeit der Redaktionsarbeit eines Medienunternehmens, etwa wenn es um Recherchemethoden oder andere Redaktionsinterna geht (vgl. nur *BVerfG* NJW 1984, 1741 – Wallraff I). Nach eingangs erwähnter *BVerfG*-Entscheidung fallen auch organisationsbezogene Informationen eines Medienunternehmens wie etwa Grundrisszeichnungen der Redaktionsräume unter das Redaktionsgeheimnis. Geschützt ist also nicht nur das konkrete Vertrauen des Informanten, sondern auch das abstrakte Vertrauen der Allgemeinheit in Funktionsfähigkeit und Staatsferne der Medien.

In Österreich zieht man dagegen den Begriff des Redaktionsgeheimnisses enger. Geschützt ist nur das Vertrauensverhältnis zwischen Medium und Informant. Vom Schutz ausgenommen sind daher nicht nur redaktionelle Abläufe, sondern auch das sog. selbst produzierte Material, also solches, das die Medien ohne besonderes Zutun eines Dritten erlangen, etwa Filmmaterial von öffentlichen Veranstaltungen. Doch auch in diesen Fällen kann Art. 10 EMRK hinreichend Rechnung getragen werden, da die öStPO eine Generalklausel enthält, die für jede Rechtsgutbeeinträchtigung eine Verhältnismäßigkeitsprüfung anordnet.

### III. Fazit

Obwohl der Begriff des Redaktionsgeheimnisses sowohl in der deutschen als auch in der österreichischen Rechtssprache geläufig ist, lassen sich Unterschiede deutlich erkennen, vor allem im Hinblick auf Begriffsverständnis und gesetzliche Ausgestaltung. Die eingangs erwähnten Entscheidungen des *BVerfG* und des *ÖOGH* führen die bisher eingeschlagene Judikaturlinie fort. Beide Gerichtshöfe entsprechen dabei den Vorgaben des *EGMR*, der im Hinblick auf staatliche Eingriffe in Art. 10 EMRK stets für erforderlich hält, dass diese einer besonderen Verhältnismäßigkeitsprüfung standhalten, bei der die Interessen im Einzelfall sorgfältig abzuwägen sind. Überdies sind politische Bestrebungen zur Stärkung des Schutzes journalistischer Quellen sowohl auf deutscher als auch auf österreichischer Seite zu konstatieren.

**Christopher Mersch**
ist wissenschaftlicher Mitarbeiter am Lehrstuhl von Prof. Walter Berka, Paris-Lodron-Universität Salzburg.

## Axel Spies Cloud Computing: Keine personenbezogenen Daten bei Verschlüsselung

MMR-Aktuell 2011, 313727

Im Beck-Blog gab es kürzlich zwischen den Teilnehmern eine hochinteressante Diskussion zum Thema, ob und wann die Vorschriften des deutschen BDSG, insbesondere dessen Normen zur Regelung der Übermittlung von personenbezogenen Daten ins Ausland, auf verschlüsselte Daten i.R.d. Cloud Computing anwendbar sind.

### 1. Problem

Cloud Computing führt zur Verlagerung von Dienstleistungen, Ressourcen und Serviceangeboten in das Internet. Jeder kann sie überall auf der Welt nutzen. Cloud-Strukturen werden dadurch immer relevanter für Unternehmen. Die Nutzung ausgelagerter Dienste wie Virtualisierung und „Software as a service" (SaaS)-Angebote werden bald unverzichtbar für Unternehmen sein. In vielen Fällen kennt der Auftraggeber nicht einmal den Ort, an dem die Speicherung stattfindet. Dementsprechend gibt es Bestrebungen der Anbieter, zu argumentieren, dass bei Nutzung entsprechender Verschlüsselungstechniken (Encryption) keine personenbezogenen Daten ins Ausland transportiert werden. Das BDSG schützt nur personenbezogene Daten. Personenbezogene Daten müssen sich i.S.d. § 3 Abs. 1 BDSG auf eine bestimmte oder eine bestimmbare natürliche Person beziehen. Für die Bestimmbarkeit kommt es auf die Kenntnisse, Mittel und Möglichkeiten der speichernden Stelle an. Die Frage ist, ob das BDSG beim Cloud Computing eingreift, wenn die speichernde Stelle gar nicht den Schlüssel zur Dekodierung hat, sondern nur der „Betroffene" (oder nach EU-Terminologie das „Data Subject").

### 2. Beobachtungen

Die meisten Kommentatoren waren der Ansicht, dass auch in diesen Fällen das BDSG anwendbar sei: Ein wichtiger Beleg hierfür sei, dass über kurz oder lang heute als nicht dekodierbar geltende Verschlüsselungen bei entsprechend fortschreitender technischer Entwicklung mit einfachsten Mitteln zu brechen sein könnten. Ein Beispiel hierfür sei die Verschlüsselung von DVDs. Wenn man also bei „Kenntnissen, Mitteln und Möglichkeiten" nur auf den heutigen techni-

schen Stand und nicht auf absehbar erfolgende technische Entwicklungen schaue, werde der Schutz des BDSG unterlaufen. Die Unsicherheit, wann das Dekodieren der Verschlüsselung mit „realistischen" Mitteln erfolgen kann, dürfe nicht auf Kosten des zu Schützenden gehen. Hinzu komme, dass die Sicherheit einer Verschlüsselung schwer zu beweisen sei. Man könne zwar Sicherheitsmetriken für Verschlüsselungstechniken entwerfen (z.B. die Häufigkeit mittels einer wissenschaftlichen Untersuchung) – diese würden aber regelmäßig eine hohe und kaum bezifferbare Unsicherheit behalten.

Dieser engen Auslegung wurde entgegengehalten, dass man zwischen der Verschlüsselung zum Schutz von bestehenden personenbezogenen Daten und der Verschlüsselung, die gar nicht erst personenbezogene Daten entstehen lässt, unterscheiden sollte. Wenn auf Grund der Verschlüsselung gar keine personenbezogenen Daten entstehen, sei es nicht leicht, die Anwendung des BDSG zu begründen. Außerdem stelle das BDSG auf die Sicht des Speichernden ab und weniger auf die Sicht des Betroffenen. Sicherheit sei praxisgerecht nie absolut zu betrachten, meinte ein anderer Kommentator, sondern immer nur im Verhältnis zu einer Referenzlösung. Wäre für einzelne Geschäftsprozesse nicht eine „ausreichende" Sicherheit bestimmbar, sondern müssten sie pauschal „abgesichert" werden, wären sie wirtschaftlich nicht durchführbar. Die Antwort auf die aufgeworfene Frage hänge von den konkreten technischen Rahmenbedingungen ab: Cloud Computing biete eine Vielzahl von Ansatzpunkten für Kryptografie. Standard für die Datenübermittlung sei die Transportverschlüsselung zwischen dem Dienstleister und dem Kunden. Dies sei eine Selbstverständlichkeit im Interesse des Kunden, in der Regel bilde aber deren Implementierung die größte Schwachstelle eines Cloud Computing-Angebots.

Um auszuschließen, dass die Daten zwischen Daten- und Transportverschlüsselung unverschlüsselt abgegriffen werden (oder der Schlüssel aus dem RAM extrahiert wird), müssten die Systeme physisch eine gewisse „Tamper Resistance" (Maßnahmen gegen ein Aufbrechen der Verschlüsselung) aufweisen, die dem Kunden einen unerlaubten Zugriff erkennbar oder jedenfalls nachweisbar mache. Wirkungsvolle Lösungen hierfür, so der Kommentator, seien im Cloud Computing nicht verbreitet, aber verfügbar und z.B. im Bereich der TKÜ zwischen Abhörschnittstellen und Ausleitungskomponenten (den sog. „Sina-Boxen") anzutreffen. Alternativ könnte bereits der Kunde die Daten verschlüsseln und in dieser Form auf das Anbietersystem übertragen. Für Online-Backups sei dies ein alltäglicher Vorgang. Ungleich komplizierter sei die Prozessverschlüsselung, wenn Daten z.B. in einer Virtualisierung verarbeitet werden sollen.

Ein weiterer Kommentator wies darauf hin, dass man bei der rechtlichen Würdigung unterscheiden müsse, ob der Zugang zur Festplatte oder zum einzelnen Datensatz verschlüsselt sei. Angenommen, es handele sich um eine verschlüsselte Festplatte, dann würden die Daten beim Hochfahren immer entschlüsselt – und der Zugriff auf eine Datenbank erfolgt auch nicht unbedingt verschlüsselt. Anders gesprochen, verschlüsselt sei dann für den Server nur der Zugriff auf die Festplatte selbst. Wenn aber auf das System zugegriffen wird oder es Sicherheitslücken aufweist, so seien die Daten eben genauso lesbar wie auf einem unverschlüsselten System. Ein Cloud-System, das Daten nicht entschlüsselt, wäre gar nicht funktionsfähig.

Auf der rechtlichen Ebene wurde weiterhin argumentiert, dass die Verschlüsselung der Daten diese Daten an sich nicht verändere. Bei der Verschlüsselung handele es sich wohl eher um eine technisch-organisatorische Maßnahme, die sicherstellen soll, dass die Daten Unbefugten nicht zugänglich sind. An der datenschutzrechtlichen Qualifikation der Daten dürfte dies nichts ändern. Die grundsätzliche datenschutzrechtliche Einordnung des Cloud Computing spiele sich – sofern personenbezogene Daten vorliegen – dann eher in dem Bereich der wirksamen Einwilligung des Betroffenen ab sowie bei der Beantwortung der Frage, ob ein Datenverkehr mit Drittstaaten vorliege und wie dieser ggf. regelungstechnisch in den Griff zu bekommen ist. Dem wurde entgegengehalten, dass die „Einwilligungslösung" dann zu Schwierigkeiten führe, wenn der Anbieter keinen „Generalschlüssel" zu den Daten habe. In diesem Zustand würden keine personenbezogenen Daten ins Ausland übertragen, weil keiner im Ausland diese Daten entschlüsseln könne. Die Daten könne nur der Betroffene einsehen, der allein über den Schlüssel verfüge. Eine Einwilligung in die Übermittlung sei dann nicht erforderlich, weil gar keine personenbezogenen Daten übertragen würden.

Dem wurde von einem anderen Kommentator entgegengehalten, dass rechtliche Lösungen, bei denen nun auch die verantwortliche Stelle keinen Schlüssel zu den Daten hätte, die Anwendungsmöglichkeiten zu sehr begrenzen würden. Eine Datenspeicherung durch Cloud Computing sei gerade dann erforderlich, wenn andere als der Betroffene Zugriff auf die Daten nehmen sollen. Zudem seien in den denkbaren Geschäftsbeziehungen zwischen dem Cloud Computing-Nutzer und dessen Kunden, dem Betroffenen, heute keine Schlüsselverwaltung üblich, bei der der Betroffene einen tatsächlich nur ihm bekannten Schlüssel verwendet, der nicht anderweitig von der verantwortlichen Stelle ersetzt werden könnte. Wenn sich die speichernde Stelle ihres Kunden für die Entschlüsselung bedienen könne, lägen personenbezogene Daten vor.

## 3. Fazit

Ein Patentrezept, wie mit der Verschlüsselung i.R.d. Cloud Computing umzugehen ist, gibt es noch nicht, wie die Diskussion gezeigt hat. Die geschilderte Blog-Diskussion hat allerdings einige wichtige Gesichtspunkte zur Klärung der Frage genannt, wer mit welchem Schlüssel auf die Daten zugreifen kann. Eine neue Cloud Computing-Studie des *Fraunhofer-Instituts* (Vorabversion v. 29.11.10) beschäftigt sich ebenfalls mit dem Thema: Dort heißt es auf S. 116: „Strenge Anforderungen sind an die Kommunikation einerseits zwischen Cloud-Kunde und -Anbieter, andererseits zwischen verschiedenen Rechenzentren in der Cloud gestellt: Ein derartiger Datenaustausch ist grundsätzlich zu verschlüsseln. Das *BSI* unterscheidet hierbei nicht zwischen dem Austausch personenbezogener bzw. aus anderen Gründen sensibler und sonstiger Daten; für letztere ist die Notwendigkeit einer Verschlüsselung nicht unmittelbar einsichtig."

Dieser Ansatz scheint auf eine Art Beweislastumkehr hinauszulaufen: Das BDSG ist grundsätzlich bei der Übermittlung von verschlüsselten Daten anwendbar, es sei denn der Anbieter weist nach,

- dass die Daten sicher verschlüsselt sind (s. dazu die vorgeschlagene Checkliste des Instituts auf derselben Seite) und
- dass nur der Betroffene seine Daten mit dem Schlüssel einsehen kann.

Dieser Beweis dürfte in der Praxis allerdings schwer zu führen sein.

■ Vgl. auch MMR-Aktuell 2010, 312178; *Heidrich/Wegener*, MMR 2010, 803; *Gaycken/Karger*, MMR 2011, 3; MMR-Aktuell 2010, 312179.

**Dr. Axel Spies**
ist Rechtsanwalt in der Kanzlei Bingham McCutchen, Washington DC, und Mitherausgeber der MMR.

## Axel Schneider BVerwG: Rundfunkgebührenpflicht für internetfähige PC

MMR-Aktuell 2011, 313725

Mit gleichlautenden Urteilsgründen hat das *BVerwG* am 27.10.2010 (MMR-Aktuell 2010, 310117) die Revision zweier Rechtsanwälte und eines Studenten zurückgewiesen, die sich gegen die sog. „PC-Gebühr" gewandt hatten. Damit beseitigt das *Gericht* eine bundesweite Rechtsunsicherheit, die durch zahlreiche Zeitungsartikel, Internetforen, Fachpublikationen und divergierende Urteile der Verwaltungsgerichte befeuert wurde.
Vielleicht wird sich aber noch das *BVerfG* mit dem Problemkreis beschäftigen. Eine frühere Verfassungsbeschwerde war noch mit der Begründung abgelehnt worden, zunächst seien der Begriff des neuartigen Rundfunkempfangsgeräts sowie die technischen Voraussetzungen des Bereithaltens zum Empfang von den Fachgerichten zu klären (*BVerfG*, B. v. 30.1.2008 – 1 BvR 829/06).
Diesen Tatbestandsmerkmalen des RGebStV hat das *BVerwG* nun hinreichende Konturen verliehen, auch wenn Aussagen zur konkreten Hard- und Softwareausstattung fehlen. Das ist nicht nur wegen der unüberschaubaren Gerätevielfalt verständlich, sondern auch deshalb, weil konkrete Ausstattungs- und Konfigurationsmerkmale sich im Massenverfahren kaum verifizieren ließen. An der Gebührenerhebung für neuartige Rundfunkempfangsgeräte können die Rundfunkanstalten nach Ansicht der Richter aber nur dann festhalten, wenn sich diese auch tatsächlich durchsetzen lässt. Im Kern stellt das *BVerwG* fest, dass die Rundfunkgebührenpflicht an den bloßen Besitz eines internetfähigen PC anknüpft, ohne dass es auf dessen tatsächliche Nutzung zum Rundfunkempfang oder einen subjektiven Nutzungswillen ankäme.
Auf die verfassungsrechtlichen Grundlagen der Gebührenfinanzierung geht das *Gericht* nicht näher ein, sondern verweist lediglich auf die ständige Rechtsprechung des *BVerfG*. Allerdings hätte die öffentliche Diskussion, ob der Funktionsauftrag des öffentlich-rechtlichen Rundfunks sich auf das Internet erstreckt und z.B. die „Tagesschau-App" von der verfassungsrechtlichen Entwicklungsgarantie gedeckt ist, eine vertiefte Auseinandersetzung gerechtfertigt. Auch die Darstellung der zunehmenden Medienkonvergenz, die Entwicklung der Medienmärkte und Veränderungen in der Mediennutzung hätten die Urteilsgründe sinnvoll ergänzen können. Möglicherweise wird das nächste Rundfunkurteil des *BVerfG* diese Aspekte vertiefen.

■ Das Urteil wird in Heft 4/2011 zusammen mit einer ausführlichen Anmerkung des Autors erscheinen.

**Axel Schneider**
ist Referent in der Juristischen Direktion des Bayerischen Rundfunks und hat den beklagten Bayerischen Rundfunk im Verfahren BVerwG 6 C 21.09 vertreten.

**MMR** *MultiMedia und Recht*

**Redaktion:** Anke Zimmer-Helfrich, Chefredakteurin (verantwortlich für den Textteil); RAin Ruth Schrödl, Redakteurin; Marianne Gerstmeyr, Redaktionsassistentin, Wilhelmstr. 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München, Telefon: 089/ 381 89-427, Telefax: 089/ 38189-695, E-Mail: mmr@beck.de

**Manuskripte:** Manuskripte sind an die Redaktion zu senden. Der Verlag haftet nicht für Manuskripte, die unverlangt eingereicht werden. Sie können nur zurückgegeben werden, wenn Rückporto beigefügt ist. Die Annahme zur Veröffentlichung muss schriftlich erfolgen. Mit der Annahme zur Veröffentlichung überträgt der Autor dem Verlag das ausschließliche Verlagsrecht für die Zeit bis zum Ablauf des Urheberrechts. Eingeschlossen sind insbesondere auch die Befugnis zur Einspeicherung in eine Datenbank sowie das Recht der weiteren Vervielfältigung zu gewerblichen Zwecken im Wege eines fotomechanischen oder eines anderen Verfahrens. Dem Autor verbleibt die Befugnis, nach Ablauf eines Jahres anderen Verlagen eine einfache Abdruckgenehmigung zu erteilen; ein Honorar hieraus steht dem Autor zu.

**Urheber- und Verlagsrechte:** Alle in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Dies gilt auch für die veröffentlichten Gerichtsentscheidungen und ihre Leitsätze, denn diese sind geschützt, soweit sie vom Einsender oder von der Redaktion erarbeitet oder redigiert worden sind. Der Rechtsschutz gilt auch gegenüber Datenbanken und ähnlichen Einrichtungen. Kein Teil dieser Zeitschrift darf außerhalb der engen Grenzen des Urheberrechtsgesetzes ohne schriftliche Genehmigung des Verlages in irgendeiner Form – durch Fotokopie, Mikrofilm oder andere Verfahren – reproduziert oder in eine von Maschinen, insbesondere von Datenverarbeitungsanlagen verwendbare Sprache übertragen werden.

**Anzeigenabteilung:** Verlag C.H. Beck, Anzeigenabteilung, Wilhelmstraße 9, 80801 München; Postanschrift: Postfach 40 03 40, 80703 München, Telefon: Susanne Raff 089/3 81 89-601, Julie von Steuben 089/3 81 89-608, Bertram Götz 089/3 81 89-610, Telefax: 089/3 81 89-782.
Disposition: Herstellung Anzeigen, technische Daten, Telefon: 089/3 81 89-598, Telefax: 089/3 81 89-589, anzeigen@beck.de. Verantwortlich für den Anzeigenteil: Fritz Lebherz

**Verlag:** Verlag C.H. Beck oHG, Wilhelmstraße 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München, Tel.: 089/381 89-0, Telefax: 089/38 18 93 98, Postbank: München Nr. 62 29-802, BLZ 70010080.

**Erscheinungsweise:** Monatlich.

**Bezugspreise 2011:** Jährlich € 348,– (darin enthalten € 22,77 MwSt.). Vorzugspreis für Studenten und Rechtsreferendare € 172,– (darin enthalten € 11,25 MwSt.). Vorzugspreis für Mitglieder der davit € 272,– (darin enthalten € 17,79 MwSt.). Vorzugspreis für Studenten, die auch JuS-Bezieher sind: € 60,– (darin enthalten € 3,93 MwSt.). Einzelheft: € 33,– (darin enthalten € 2,16 MwSt.); Versandkosten: jeweils zuzüglich. Die Rechnungsstellung erfolgt zu Beginn eines Bezugszeitraumes. Nicht eingegangene Exemplare können nur innerhalb von 6 Wochen nach dem Erscheinungstermin reklamiert werden.
Jahrestitelei und -register sind nur noch mit dem jeweiligen Heft lieferbar.

**Bestellungen** über jede Buchhandlung und beim Verlag. Vertriebskooperation in der Schweiz: Helbing & Lichtenhahn Verlag AG (CH) & Co.KG, Elisabethenstraße 8, CH-4051 Basel, Tel.: +41 (0)61 228 90 70, Fax: +41 (0)61 228 90 71, E-Mail: zeitschriften@helbing.ch.

**Abo-Service:** Tel.: 089/3 81 89-750, Fax: 089/3 81 89-358, E-Mail: bestellung@beck.de

**Abbestellungen** müssen 6 Wochen vor Jahresschluss erfolgen.

**Adressenänderungen:** Teilen Sie uns rechtzeitig Ihre Adressenänderungen mit. Dabei geben Sie bitte neben dem Titel der Zeitschrift die neue und die alte Adresse an.
Hinweis gemäß § 4 Abs. 3 der Postdienst-Datenschutzverordnung: Bei Anschriftsänderungen des Beziehers kann die Deutsche Post AG dem Verlag die neue Anschrift auch dann mitteilen, wenn kein Nachsendeantrag gestellt ist. Hiergegen kann der Bezieher innerhalb von 14 Tagen nach Erscheinen des Heftes beim Verlag widersprechen.

**Satz:** FotoSatz Pfeifer GmbH, 82166 Gräfelfing.

**Druck:** Druckerei C.H. Beck (Adresse wie Verlag).

ISSN 1434-596X