Die entscheidende Schlacht wird derzeit in Europa geschlagen

Interview mit dem Vorsitzenden der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) Peter Schaar*

Peter Schaar wurde 1954 in Berlin geboren. Nach dem Studium der Volkswirtschaftslehre in Berlin, Frankfurt und Hamburg war er von 1980 bis 1986 in der Hamburger Verwaltung tätig und seit 1994 als stellvertretender Hamburgischer Datenschutzbeauftragter. Nach einem kurzen Wechsel in die Privatwirtschaft war er von 2003 bis Ende 2013 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI). Seit September 2013 ist Peter Schaar der Vorsitzende der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID). Er ist Parteimitglied von Bündnis 90/Die Grünen.

Bonner Rechtsjournal (BRJ): *Herr Schaar, am 17. Dezember 2013 endete Ihre Amtszeit als Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI). Ihre Nachfolgerin im Amt ist Andrea Voßhoff (CDU). In einem Interview mit der Frankfurter Rundschau[1] wünschten Sie Ihrer Nachfolgerin eine „völlige Unabhängigkeit im Amt". Bei der EU-Kommission sind Beschwerden gegen die Bundesregierung anhängig. Dabei geht es um die mangelhafte Umsetzung von Art. 28 RL 95/46/EG und Art. 25 Rahmenbeschluss 2008/977/JI. Diese sollen die Unabhängigkeit nationaler Kontrollstellen wie dem BfDI sicherstellen. Wo sehen Sie Defizite bei der Umsetzung der EU-Richtlinien und welche konkreten Änderungen würden Sie für erforderlich halten?*

Schaar: Vor allem drei Punkte sind dringend änderungsbedürftig: Der erste ist die Frage der Rechtsaufsicht. Nach dem Bundesdatenschutzgesetz (BDSG) *kann* die Bundesregierung über den Bundesdatenschutzbeauftragten die Rechtsaufsicht ausüben, d.h. auch inhaltlich auf seine Arbeit Einfluss nehmen, etwa indem entsprechende Vorgaben gemacht werden. Diese Möglichkeit, die im Gesetz vorgesehen ist, von der aber – soweit ich weiß – noch niemals Gebrauch gemacht wurde, verstößt gegen das Gebot der Weisungsunabhängigkeit. Ein zweiter Punkt ist die Dienstaufsicht, die der Bundesinnenminister über den bzw. die Bundesbeauftragte ausübt. Auch das ist, wenn man der Rechtsprechung des *Europäischen Gerichtshofs* (EuGH) folgt, europarechtswidrig. Ein dritter Aspekt betrifft die Einbindung des Personalkörpers des Bundesbeauftragten in den Personalkörper des Bundesinnenministeriums. Zwar darf das Bundesinnenministerium niemanden entgegen der Meinung oder ohne die Zustimmung des Bundesdatenschutzbeauftragten in seinem Amt anstellen. Aber dies ist noch weit entfernt von einer eigenen Personalhoheit, sodass der bzw. die Bundesbeauftragte darauf angewiesen ist, aus der Vorauswahl des Bundesinnenministeriums eine Kandidatin oder einen Kandidaten zu berücksichtigen. Der bzw. die Bundesbeauftragte hat keine Möglichkeit, selbst aktiv nach Personal zu suchen und einzustellen. Die Änderung des BDSG in diesen Fragen ist dringend erforderlich, wegen der Entscheidung des *EuGH* gegen Deutschland in Sachen Unabhängigkeit der Datenschutzbehörden der Länder, aber auch vor dem Hintergrund der *EuGH*-Entscheidung bezüglich der Situation in Österreich. Hier wurde die personale Unabhängigkeit noch einmal betont, gerade im Hinblick auf die Anbindung an ein Ministerium. Lösungsmöglichkeiten sehe ich auf zwei Wegen: Einmal wäre es denkbar, den BfDI in ähnlicher Weise einer Obersten Bundesbehörde mit voller Unabhängigkeit auszugestalten, vergleichbar mit dem Bundesrechnungshof. Eine andere Möglichkeit könnte darin bestehen, den Bundesdatenschutzbeauftragten nicht mehr wie bisher an ein Ministerium zu binden, sondern an den Deutschen Bundestag. Aber auch hier kommt es natürlich darauf an, dass gegenüber dem Parlament und der Parlamentsverwaltung die Unabhängigkeit gewährleistet wird.

BRJ: *Wären aus Ihrer Sicht zudem weitere Kompetenzen für den Bundesdatenschutzbeauftragten wünschenswert?*

Schaar: Sie sind aus meiner Sicht nicht nur wünschenswert, sondern geboten. Schon jetzt mangelt es dem BfDI, anders als etwa den Aufsichtsbehörden der Länder, an Durchsetzungsmöglichkeiten gegenüber nicht-öffentlichen Stellen, die seiner Datenschutzkontrolle unterliegen. Die Landesdatenschutzbehörden können nach dem BDSG bei Verstößen gegen

* Das Interview wurde am 28. Dezember 2013 geführt und aufgezeichnet von *Philipp Bender*. Vorbereitet wurde es von *Lorenz Posch* und *Philipp Bender*. Bildnachweise für die Aufnahmen von *Peter Schaar*: Bundesregierung/Kugler (Print), REGIERUNGonline/Kugler (Online).

1 Schaar fordert verbesserten Datenschutz, fr-online, http://www.fr-online.de/datenschutz/peter-schaar-schaar-fordert-verbesserten-datenschutz-,1472644,25620780.html, Abruf v. 30.12.2013.

datenschutzrechtliche Vorschriften Bußgelder verhängen und sie können im Falle nachhaltiger Verstöße unzulässige Verfahren untersagen, mit denen personenbezogene Daten verarbeitet werden. Diese beiden Befugnisse hat der Bundesbeauftragte nicht. Im Hinblick auf die Ermächtigung zur Bußgeldverhängung muss er an die Bundesnetzagentur herantreten, um dort Überzeugungsarbeit dafür zu leisten, dass ein entsprechender Bußgeldbescheid erlassen wird. Allerdings ist die Bundesnetzagentur keine unabhängige Stelle, sondern sie ist weisungsabhängig von den jeweils zuständigen Bundesministerien. Auch dies entspricht nicht den Vorgaben der EU-Datenschutzrichtlinie, wonach den Aufsichtsbehörden wirksame Mittel in die Hand zu geben sind.

BRJ: *Im Juni 2013 sagten Sie im ZDF, dass wenn sich die Meldungen rund um Prism und Tempora bestätigten, der deutsche Datenschutz „für die Katz" sei.[2] Ist das Datenschutzniveau in Deutschland tatsächlich niedrig, auch im Vergleich zu angelsächsischen und skandinavischen Staaten?*

Schaar: Dieser Satz ist Teil eines längeren Interviews, das sich rund um die dramatischen Enthüllungen von *Edward Snowden* rankte. Dass nun diese spontane Äußerung als eine vermeintliche Grundposition von mir interpretiert wird, darüber bin ich nicht wirklich glücklich. Es geht im Zusammenhang mit den *Snowden*-Enthüllungen ja nicht nur um das deutsche Datenschutzniveau, etwa im Vergleich zu dem Niveau in Skandinavien oder Frankreich. Vielmehr stellt sich in ganz Europa und international die Frage: Welche praktische Relevanz hat ein Datenschutzrecht, das lediglich territorial wirkt? Das betrifft sowohl den Geltungsbereich als auch die praktische Durchsetzbarkeit der rechtlichen Vorgaben. Inwieweit kann ein solches auf dem Territorialprinzip fußendes Recht angesichts globaler Datenströme und auch gegenüber global agierenden Unternehmen und außerhalb der eigenen Staatsgrenzen agierende öffentlichen Stellen durchgesetzt werden? Die auf *Edward Snowden* zurückgehenden Enthüllungen zeigen ja, wie weit die globale Überwachung bereits gängige Praxis ist. Ich denke, dass die Frage der internationalen Kodifizierung von Datenschutz deshalb an Bedeutung gewinnt und auch gewinnen muss.

BRJ: *Meinen Sie rückblickend, dass die deutsche Politik in diesem Bereich zu wenig getan hat in letzter Zeit?*

Schaar: Nicht nur, aber auch die deutsche Politik. Die Überwachung ist ein globales Phänomen. Festzustellen ist auch, dass die in den USA geführte Diskussion sich fast ausschließlich um den Schutz der eigenen Staatsbürger dreht, während der Schutz der restlichen Welt kaum thematisiert wird. Und bei uns ist das leider nicht viel anders! Auch wir haben diese Differenzierung nach der Staatsangehörigkeit bzw. nach dem Aufenthalt von Personen, etwa was die Tätigkeit der deutschen Nachrichtendienste betrifft. Der Bundesnachrichtendienst (BND) unterliegt bei der Überwachung von Inländern strikten Regeln und auch die sogenannte strategische Fernmeldekontrolle ist rechtlich normiert, obwohl ich hier durchaus Bedarf für Nachbesserungen sehe. Die eigentliche Auslandsüberwachung hingegen, die ja auch in großem Umfang erfolgt, unterliegt dagegen praktisch keinen gesetzlichen Beschränkungen. Mir ist wichtig, dass wir hier zu internationalen Standards finden. Schon heute wird in der völkerrechtlichen Diskussion zu Recht der Anspruch formuliert, den Schutz der Privatsphäre als internationales Menschenrecht anzusehen. Aber wenn wir uns die Rechtssysteme rund um den Globus anschauen, stellen wir fest, dass dieses Anliegen nirgendwo wirklich angekommen ist, dass hier nach wie vor in territorialen und nationalen Kategorien gedacht und gehandelt wird.

BRJ: *Stichwort Völkerrecht: Immerhin wurde am 18. Dezember 2013 durch die UN-Generalversammlung eine von Deutschland und Brasilien initiierte Resolution angenommen, die sich gegen die Überwachung wendet. Diese hat keinerlei Bindungswirkung für die Staaten und wurde insbesondere durch das Bestreben der USA zuvor deutlich entschärft. Auf EU-Ebene wird die neue Datenschutzverordnung nach Berichten gerade auch durch deutsche Spitzenbeamte des Bundesinnenministeriums „verwässert und verzögert"[3]. Sind wirkungsvolle multilaterale und verbindliche Abkommen zum Datenschutz unter solchen Umständen momentan überhaupt vorstellbar?*

Schaar: Ich sehe es als positiven Schritt, dass die UN-Vollversammlung diese Resolution einstimmig beschlossen hat. Natürlich hätte ich es für besser gehalten, wenn die ursprüngliche Version, die deutlicher den internationalen Charakter dieser Menschenrechtsverbürgungen betont hatte, angenommen worden wäre. Gleichwohl ist der Beschluss ein beachtenswertes Signal! Aber es darf nicht übersehen werden, dass hiermit kein neues verbindliches Völkerrecht geschaffen worden ist. Ich halte völkerrechtliche Regeln zum Datenschutz für notwendig, anknüpfend an die Menschenrechtscharta und an Art. 17 des internationalen Zivilrechtspaktes, die den Schutz des Privatlebens garantieren. Die recht allgemein gehaltenen Bekenntnisse müssen ausgefüllt und konkretisiert werden: Wir brauchen verbindliche Regeln im Völkerrecht, was erlaubt ist und was nicht und welche verfahrensrechtlichen Sicherungen zur Anwendung kommen müssen. Bei der Diskussion auf EU-Ebene geht es um etwas anderes: Ich halte es für dringend erforderlich, dass wir einen europäischen

[2] Zdf.de, http://www.zdf.de/ZDFmediathek#/beitrag/video/1930454/Schaar-fordert-neue-Datenschutzregeln, Abruf v. 02.01.2014.

[3] EU-Ministerrat: Deutsche Beamte bremsen Europas Datenschutz aus, Spiegel online http://www.spiegel.de/netzwelt/netzpolitik/deutsche-beamte-bremsen-europas-datenschutz-aus-a-936704.html, Abruf v. 02.01.2014.

Rechtsrahmen für den Datenschutz bekommen, der strikter und moderner ist als die Richtlinie von 1995. Ich habe es begrüßt, dass die Kommission vor zwei Jahren einen Vorschlag hierzu vorgelegt hat. Dieser ist zwar in verschiedenen Punkten änderungsbedürftig. Dennoch bin ich der Auffassung, dass wir damit nicht allzu lange warten sollten. Im Internetzeitalter kann eine Verzögerung von ein, zwei Jahren bedeuten, dass eine an und für sich gute Regelung nicht mehr greifen kann, weil sich die technischen Bedingungen rasant verändert haben. Wenn sich der Rat hier am „Kleingedruckten" festbeißt, könnte dies die Folge haben, dass die ganze Reform scheitert. Die wesentlichen Forderungen und Ziele sind entscheidend. In der unterschiedlichen Umsetzung der Richtlinie von 1995 in nationales Recht sehe ich eine Hauptursache für das Durchsetzungsdefizit des Datenschutzrechts, das wir heute in Europa beklagen. Zudem brauchen wir kraftvolle Datenschutzbehörden, die die rechtlichen Vorgaben durchsetzen. Auch hierfür sehen die Reformvorschläge richtige Ansätze vor, etwa die Möglichkeit, Bußgelder zu verhängen, die nicht nur die Portokassen großer Unternehmen belasten. *Last but not least* muss gewährleistet sein, dass Unternehmen aus Drittstaaten, die ihre Dienste in Europa anbieten und hier Daten erheben, sich nicht mehr dem EU-Datenschutzrecht entziehen können. Ich erinnere an den Fall *Google*: Das Unternehmen ist nach wie vor der Auffassung, das europäische Recht sei für es nicht verbindlich. Ein Unternehmen, das in riesigen Umfang Daten sammelt, die viele Europäerinnen und Europäer betreffen, darf sich nicht auf das Recht des Staates Kalifornien zurückziehen. Im Zuge der von *Snowden* angestoßenen Diskussion ist deutlich geworden, wie behutsam der Zugriff staatlicher Stellen aus Drittstaaten auf Daten ist, die durch das europäische Datenschutzrecht geschützt sind. Hier gibt es Vorschläge, einen zusätzlichen Artikel in die Verordnung aufzunehmen, der für mehr Transparenz sorgt und derartige Zugriffe an die Genehmigung der europäischen Datenschutzbehörden bindet. Das Europäische Parlament hat hierzu einen neuen Artikel 43a der Datenschutz-Grundverordnung vorgeschlagen. Die Bundesregierung hat im Rat einen vergleichbaren Vorschlag eingebracht. Natürlich würde eine solche Vorgabe Grenzüberschreitungen durch Nachrichtendienste nicht ausschließen, denn diese halten sich im Ausland ja bekanntermaßen nicht durchgängig an die dort geltenden Gesetze. Trotzdem würde der neue Artikel in der Datenschutz-Grundverordnung die europäische Rechtsposition stärken. Wenn wir dies im internationalen Kontext betrachten, wird Europa gegenüber den USA und Asien insoweit wieder auf Augenhöhe gebracht.

BRJ: *Warum hängt die EU-Datenschutzverordnung im Ministerrat? Bremst hier Deutschland das Ganze in Zusammenarbeit mit Großbritannien aus, wobei letztere vor allem in Richtung Nordamerika schielen? Andere europäische Staaten wie etwa Frankreich und Polen wollten in diesen Fragen sehr viel selbstbewusster und forscher voranschreiten.*

Schaar: Ich hätte mir gewünscht, dass Deutschland, Frankreich und Polen – also die Staaten, die nicht nur geographisch den Kern Mitteleuropas bilden – sich ganz besonders für diesen Schritt nach vorne eingesetzt hätten. Leider hat Deutschland hier aber geschwächelt, aus welchen Gründen auch immer. Ich möchte jetzt nicht spekulieren, inwieweit etwa personale Gründe mitursächlich waren. Wir hatten einen Minister [*Hans-Peter Friedrich* (CSU), Anm. d. Red.], dem dieses Anliegen etwas ferner lag, als vielleicht seinem Vorgänger und Nachfolger, der das Amt jetzt wieder übernommen hat [*Thomas de Maizière* (CDU), Anm. d. Red.], sodass ich jetzt bessere Chancen sehe, diesen Knoten zu durchschlagen. Die Voraussetzung ist jedoch, dass die neue Bundesregierung wirklich das Bremspedal lockert und die Datenschutzreform voran bringt.

BRJ: *Für Datenschützer ist die „GroKo", die Große Koalition, insgesamt gesehen wohl keine Wunschkoalition. Wie steht es aus Ihrer Sicht um die nahe Zukunft des deutschen Datenschutzes, auch unter dem Aspekt „Vorratsdatenspeicherung"?*

Schaar: Sowohl bei der Datenschutzreform als auch bei der Vorratsdatenspeicherung werden die entscheidenden Schlachten derzeit in Europa geschlagen. Wenn die Datenschutz-Grundverordnung scheitert, dann haben wir auch in Deutschland ein ganz großes Problem. Dann müssen nämlich sämtliche Arbeiten zur Reform des deutschen Datenschutzrechts mit voller Kraft wieder aufgenommen werden. Dies wäre die einzige Alternative, die man noch hätte, wenn die EU-Datenschutzreform misslingt. Ich halte dieses Szenario jedoch für einen „Plan B" und wünsche mir, dass der „Plan A", nämlich ein gutes Datenschutzniveau in Europa, realisiert werden kann. Der zweite Punkt – Sie haben es angesprochen – ist die Vorratsdatenspeicherung. Hier sehen wir auf europäischer Ebene inzwischen Bewegung: Der Generalanwalt am *EuGH* hat kürzlich ein Plädoyer[4] abgegeben, welchem zu entnehmen ist, dass die Vorratsdatenspeicherungs-Richtlinie von 2006[5] europarechtswidrig ist, dass sie insbesondere die europäischen Grundrechte verletzt, die nach dem Vertrag von Lissabon anwendbares Recht in fast allen EU-Mitgliedstaaten sind. Bei die Umsetzung der Richtlinie kann man diese Argumente nicht ignorieren. Die Bundesregierung wäre gut beraten, die Entscheidung des *EuGH* in dieser Sache abzuwarten. Insofern teile ich die Position des neuen Bundesjustizministers *Maas*. Darüber hinaus habe ich aber von meiner grundsätzlichen Kritik an der Vorratsdatenspeicherung nichts zurückzunehmen, egal ob sie jetzt oder später eingeführt wird. Gerade die NSA-Affäre belegt, dass dieses überbordende

[4] Abruf unter http://curia.europa.eu/jcms/upload/docs/application/pdf/2013-12/cp130157en.pdf, Abruf v. 02.01.2014.
[5] RL 2006/24/EG.

Datensammeln nicht unsere Freiheit sichert, sondern beeinträchtigt. Die Vorratsdatenspeicherung wäre ein weiterer Schritt in Richtung einer anlasslosen, vorsorglichen massenhaften Anhäufung personenbezogener Daten.

BRJ: *Sie sagten 2008 in einem Interview, eine Sicherheitspolitik, die sich darauf konzentriere, immer mehr Daten anzuhäufen, sei selbst ein Sicherheitsrisiko.[6] Ist die deutsche Politik bereits an diesem Punkt angelangt? Gerade im Zusammenhang mit dem Vorschlag der Koalition, bei Massengentests gemäß § 81h StPO auch sogenannte „Beinahe-Treffer" zu verwerten?*

Schaar: Zum einen geht es dabei um das massenhafte Sammeln und Speichern von Daten. Der zweite Aspekt ist die umfassende Verknüpfung und Verwertung. Im Hinblick auf das Anhäufen von sehr vielen Daten hat sich weltweit bei den Sicherheitsbehörden die Philosophie durchgesetzt: Je mehr Daten man sammelt, desto sicherer sind wir. Da heute immer mehr Daten digital entstehen, sind deren Anhäufung und Auswertung einfacher geworden. Sicherheitsbehörden in aller Welt folgen der Devise, je mehr desto besser. Das hat erhebliche Auswirkungen auf den Datenschutz. Gleich zwei wichtige Datenschutzgrundsätze werden verletzt: Der Erforderlichkeitsgrundsatz, d. h. die Begrenzung der Datenverarbeitung auf das zur Aufgabenerfüllung erforderliche Maß, und der Zweckbindungsgrundsatz, nach dem Daten nur für die Zwecke verwendet werden dürfen, für die sie erhoben worden sind. Diese Grundsätze sind durch das Recht auf informationelle Selbstbestimmung verfassungsrechtlich verbürgt. Die anlasslose Datensammlung ist ein Problem, nicht nur in Deutschland, sondern in ganz Europa. Nicht nur bei der Vorratsdatensammlung hat die EU einen Rahmen gesetzt, der weder mit dem Erforderlichkeitsgrundsatz noch mit der gebotenen Zweckbindung vereinbar ist. Zudem hat die Europäische Kommission weitere Vorhaben vorgeschlagen, die ebenfalls diesen Grundsätzen zuwiderlaufen. Denken Sie etwa an die Pläne zu einer Sammlung von Daten über Flugpassagiere, die nach Auffassung der Kommission nun auch in Europa auf Vorrat gespeichert werden sollen. Auch das von der Kommission vorgesehene Register aller Menschen, die - mit oder ohne Visum - die EU-Außengrenzen überschreiten, wäre eine derartige massenhafte Datensammlung. Den Vorhaben ist gemeinsam, dass vielfältige personenbezogene Informationen gespeichert werden sollen, ohne dass die betroffenen Personen Anlass dazu geben. Ganz überwiegend würden Daten von Menschen gespeichert von denen keine Gefahren ausgehen und die auch keiner strafbaren Handlung verdächtig sind. Hier müssen wir deutlich zurückfahren! Das *Bundesverfassungsgericht* hat in seiner Entscheidung zur Vorratsdatenspeicherung[7] dem deutschen Gesetzgeber und der Bundesregierung mit auf den Weg gegeben, die Vermeidung von anlassloser Vorratsdatenspeicherung und die Begrenzung derselben auch auf europäischer und internationaler Ebene zu vertreten. Diese Forderung des *Bundesverfassungsgerichts* darf nicht ignoriert werden. Die von der neuen Koalition angestrebte Verwertbarkeit von Beinahe-Treffern aus Massengentests, wäre die Legalisierung einer Datennutzung, die der *BGH* als rechtswidrig beurteilt hat.[8] Das Problem der Beinahe-Treffer ist ein doppeltes: Einmal finden sogenannte Massengentests nur auf freiwilliger Basis statt, weil sie Personen betreffen, bei denen kein Anfangsverdacht besteht. Durch die Verwertung von Beinahe-Treffern können aber Dritte, die gar nicht in den Eingriff eingewilligt haben, belastet werden. Sogar durch solche Personen, denen im Falle eines Ermittlungsverfahrens oder einer Anklageerhebung ein Aussageverweigerungsrecht zukäme. Insofern wäre von der Ausweitung der Verwertungsregeln nicht nur das Recht auf informationelle Selbstbestimmung betroffen, sondern z.B. auch das Recht auf Schutz von Ehe und Familie aus Art. 6 GG. Hier sollte man sehr genau hinschauen.

BRJ: *Nun werden IP-Adressen bislang nicht generell als personenbezogene Daten gewertet.*

Schaar: Das ist in dieser Pauschalität nicht korrekt! Das *Bundesverfassungsgericht* hat an verschiedenen Stellen darauf hingewiesen, dass es keinen Zweifel an dem regelmäßigen Personenbezug hat. Aber es hat in Abrede gestellt, dass IP-Adressen genauso schutzwürdig sind wie Verkehrsdaten der Telekommunikation.

BRJ: *Kann dieser Standpunkt auch Geltung beanspruchen im Fall der „Abmahnwelle" des Porno-Streamings Redtube?*

Schaar: Gerade hier sieht man doch, dass es sich um Daten handelt, die personalisiert werden, indem die Provider eine Identifikation eines einzelnen Nutzers oder eines Anschlussinhabers anhand der IP-Adresse vornehmen. Die Vorstellung, IP-Adressen seien regelmäßig nicht personenbezogen, hat noch nie gestimmt. Das Problem sehe ich weniger in der Frage, ob bei den IP-Adressen ein Personenbezug vorliegt oder nicht. Vielmehr halte ich es für problematisch, dass im Zuge dieser Abmahnaktion die Provider massenweise Daten herausgeben mussten. Ich frage mich, wie der vermeintliche Rechteinhaber bei einem *Streaming*-Dienst an die IP-Adressen der Nutzer gekommen ist, und ob die Datensammlung rechtmäßig war. Bei einem *peer-to-peer*-Netzwerk hat man immer noch den Umstand des Hochladens. In einem solchen Kontext kann die Gegenseite gegebenenfalls auch die IP-Adresse des Nutzers erfahren, weil

---

6 Datenspeicherung ist ein Sicherheitsrisiko, tagesschau.de, http://www.tagesschau.de/wirtschaft/schaarinterview2.html, Abruf v. 02.01.2014.
7 BVerfGE 125, 260.
8 *BGH*, Urteil v. 20.12.2012, 3 StR 117/12.

er gleichzeitig Empfänger und Sender ist. Wie aber bei einem *Streaming*-Dienst, bei dem der Anbieter diesen Dienst betreibt und der Nutzer in einem exklusiven Verhältnis zu diesem steht und keine eigenen Daten hochlädt, ein Dritter Kenntnis von den IP-Adressen der Nutzer erlangt, ist mir ein Rätsel. Daneben sind auch urheberrechtliche Fragen strittig.

BRJ: *Ist das BDSG, gerade was diese Drittbezüge auch zwischen Privatpersonen angeht, nicht strikt genug?*

Schaar: Wir haben im BDSG die sogenannte „Haushaltsausnahme", die in diesem Fall aber nicht einschlägig ist: Die Anwaltskanzlei und der Rechteinhaber fallen unter den Anwendungsbereich des BDSG. Eine andere Frage ist viel interessanter: Wie weit dürfen Unternehmen und andere Private im Rahmen eigener Ermittlungen gehen? Wie kommt jemand, der eine Rechtsverletzung behauptet, an die entsprechenden Daten, um gegebenenfalls den Beweis führen zu können? Hierbei muss er sich nach seinen Rechts- oder Anspruchsgrundlagen für ein solches Vorgehen fragen lassen.

BRJ: *Neben dem Bereich des Datenschutzes waren Sie auch für die Informationsfreiheit zuständig. Welche Schritte wünschen Sie sich von der neuen Bundesregierung auf diesem Gebiet? Auch im Hinblick auf das Gutachten des Instituts für Gesetzesfolgenabschätzung und Evaluation vom September 2012? Kann insofern das „Hamburger Modell" auch für den Bund als Vorbild dienen?*

Schaar: Der Evaluationsbericht, der im Auftrag des Bundestages in der vergangenen Legislaturperiode vorgelegt wurde, ist noch nicht gründlich diskutiert, geschweige denn umgesetzt worden. Er wirft eine Vielzahl sehr berechtigter Fragen auf. Einmal im Hinblick auf die große Anzahl von Ausnahmetatbeständen, die das Informationsfreiheitsgesetz (IFG) des Bundes enthält. Hier wünsche ich mir eine starke Reduktion. Zudem halte ich die Ausgestaltung mancher dieser Ausnahmeregelungen für zu strikt. Das gilt gerade im Hinblick auf die Betriebs- und Geschäftsgeheimnisse, die einen absoluten Ausnahmetatbestand darstellen und keinerlei Abwägung mit anderen Rechtsgütern zulassen, speziell nicht mit dem Informationsinteresse der Öffentlichkeit. Das öffentliche Interesse an Transparenz sollte m.E. hierbei sehr viel mehr Beachtung finden. In anderen Staaten gibt es den sogenannten *public-interest-test*, der bei dem Vorhandensein wesentlicher öffentlicher Interessen Anwendung findet. Zu denken ist beispielsweise an die Möglichkeit der öffentlichen Diskussion und Kontrolle bei Ausschreibungsverfahren öffentlicher Stellen: Hier kann die öffentliche Nachvollziehbarkeit ein höheres Gewicht haben als der ausnahmslose Schutz sämtlicher Betriebs- und Geschäftsgeheimnisse. In dem von Ihnen angesprochenen Hamburger Transparenzgesetz ist das Element der aktiven Datenbereitstellung, d.h. Veröffentlichung ohne vorliegende Anfrage, ein Thema, das stärker gewichtet werden muss. Für eine derartige aktive Informationsbereitstellung gibt es bisher nur ganz rudimentäre Ansätze im IFG des Bundes. Hier kann der Bundesgesetzgeber durchaus von einigen Landesgesetzgebern lernen. Nicht nur das Hamburger Transparenzgesetz, sondern auch die Informationsfreiheitsgesetze Bremens und Berlins sind transparenzfreundlicher als das Bundes-IFG.

BRJ: *Herr Schaar, wir bedanken uns bei Ihnen für dieses Gespräch.*