

KONGRESSBERICHT

„Neue Technologien = neues Recht?“

Sind neue Technologien ohne modernes Recht chancenlos? – Am Beispiel Datenschutz eco MMR Kongress am 22. März 2011 in Berlin

Der mittlerweile fünfte Kongress des Verbandes der deutschen Internetwirtschaft und der Zeitschrift MultiMedia und Recht (MMR) aus dem Beck-Verlag fand erneut unter Schirmherrschaft der Bundesjustizministerin Sabine Leutheusser-Schnarrenberger statt. In der Vertretung des Landes Niedersachsen beim Bund fanden sich über 100 Gäste zu der Veranstaltung ein.

Nach einer kurzen Begrüßung durch **Anke Zimmer-Helfrich**, Chefredakteurin der MMR, und **Prof. Michael Rotert**, Vorstandsvorsitzender des Verbandes der deutschen Internetwirtschaft - eco, gab **Prof. Dr. Martin Selmayr**, Kabinettschef von Viviane Reding, Vizepräsidentin der Europäischen Kommission und EU-Kommissarin für Justiz, Grundrechte und Bürgerschaft, einen aktuellen Einblick in die Datenschutz-Reformvorhaben auf europäischer Ebene. Zu Beginn wies er darauf hin, dass der Datenschutz eine zunehmend große Bedeutung für Europa habe – dies werde bereits dadurch deutlich, dass seine Prinzipien im Vertrag von Lissabon sowie in der Charta der Grundrechte festgeschrieben seien. Ziel der Kommission sei es nun, starke und praxistaugliche Datenschutz-Regeln in Europa zu etablieren. Fünf Komponenten prägten dabei die Arbeit der zuständigen Kommissarin: Die Vereinfachung bestehender Prozesse, die Stärkung des Datenschutzes an sich, seine Durchsetzung in der Praxis, die Schaffung eines kohärenten Rechtsrahmens und die Stärkung des Binnenmarktes durch Vereinheitlichung der Wettbewerbsbedingungen. Die Vereinfachung sei nötig, da die geltenden Datenschutzregelungen der EU noch in Prä-Internet-Zeiten formuliert worden seien und zum Teil aufwändige Verfahren vorsähen, die heutigen Formen der Informationsverarbeitung nicht gerecht würden. Bei der Stärkung des Datenschutzes wies er darauf hin, dass EU-Kommissarin Reding als Luxemburgerin nicht unerheblich von der deutschen Datenschutz-Kultur und der hiesigen Bedeutung des Themas geprägt sei. Aus diesem Grund messe sie dem Gebot der Datensparsamkeit eine große Bedeutung bei und sehe die zunehmende "Datensammelwut" öffentlicher wie privater Stellen mit Skepsis. Dadurch, dass das Thema Datenschutz in der EU-Kommission im Justizressort liege und nicht im Bereich des Innern, komme die zuständige Kommissarin zudem nicht in direkte Interessenkonflikte zwischen polizeilichem "Datenhunger" und dem Bürgerrecht auf Kontrolle über die eigenen Daten. Auch die praktische Umsetzung des Datenschutzes stehe auf der Agenda: So werde aktuell die Bundesrepublik Deutschland genau beobachtet, da sie anders als vorgeschrieben und trotz eindeutigen Urteils des Europäischen Gerichtshofs noch keine völlig unabhängigen Datenschutzbehörden eingerichtet habe – was einigermaßen erstaunlich sei, da Deutschland sonst in Sachen unabhängiger Behörden für Europa ein Vorreiter sei (Beispiel Bundesbank, Bundeskartellamt). Bei weiterer Missachtung des Europäischen Rechts drohe Deutschland ein Bußgeldverfahren. Ein Vorteil der aktuell geplanten Reform sei die Vereinheitlichung des Rechtsrahmens: Die bisherigen Datenschutzbestimmungen hätten ausdrücklich keine Geltung in Fragen der der polizeilichen und justiziellen Zusammenarbeit in Strafsachen gehabt. Dies ändere sich mit der anstehenden Reform, die auf der Grundlage von Art. 16 des Vertrags über die Arbeitsweise der Union alle Politikbereiche der Union in das europäische Datenschutzrecht einbeziehen könne. Ziel der Reform sei es auch, Marktvorteile für Staaten zu beseitigen, die im Bereich Datenschutz weniger strenge Maßstäbe anlegen. Noch offen sei, ob die Reform auf dem Wege einer Verordnung oder einer Richtlinie umgesetzt würde. Eine Verordnung sei als direkt geltendes Recht das geeignetere Mittel zur raschen Vereinheitlichung der Marktbedingungen, wie es vor allem für den

kommerziellen Bereich sinnvoll sei. Im Bereich der Strafverfolgung hätten allerdings die Mitgliedsstaaten teilweise unterschiedliche Bedürfnisse und Ansprüche, so dass ein gewisser Gestaltungsspielraum durchaus angemessen sein könne. Eine Richtlinie, die lediglich die Mindeststandards festschreibt, sei deshalb ebenfalls in Diskussion. Denkbar sei auch, Teile der Reform per Verordnung, andere per Richtlinie durchzuführen. Mit einem ersten Entwurf des Reformpakets rechnete Prof. Selmayr im Laufe des Sommer des Jahres 2011, wobei allerdings von einer weiten Definition des Begriffs "Sommer" ausgegangen werden könne.

Sabine Leutheusser-Schnarrenberger, Bundesministerin der Justiz, stellte die Pläne zum Aufbau der Stiftung Datenschutz vor und bezog Stellung zum weiteren Vorgehen hinsichtlich Vorratsdatenspeicherung und Zugangerschwerungsgesetz. Die Stiftung sei für verschiedene Aspekte des Themas Datenschutz die geeignetste Organisationsform, um die gesteckten Ziele zu erreichen. Sie könne beispielsweise mit Aufklärungsarbeit bei älteren und jüngeren Bürgern das Bewusstsein für Datenschutzbelange in der digitalen Kommunikation wecken. Ein weiteres Tätigkeitsfeld könne die Durchführung von Datenschutz-Audits und Vergabe entsprechender Zertifikate für Unternehmen und andere Institutionen sein. So ließen sich eine bessere Informationslage für Verbraucher und zugleich ein Wettbewerbsvorteil für datenschutzbewusste Unternehmen schaffen. Als Stiftungskapital seien zehn Millionen Euro im Haushalt des Innenministeriums vorgesehen. Aktuell würde die Satzung der Stiftung erarbeitet. Wann sie ihre operative Tätigkeit aufnimmt, ließe sich zum jetzigen Zeitpunkt noch nicht verlässlich prognostizieren. Im zweiten Abschnitt ihrer Ausführungen stellte die Ministerin ihre Position zu aktuellen Datenschutzfragen dar: Sie zweifelte an der technischen Umsetzbarkeit eines „digitalen Radiergummis“, der im Netz preisgegebene Informationen nach Ablauf einer voreingestellten Frist selbständig löscht.

Zur Vorratsdatenspeicherung äußerte sie, ein gemeinsames Konzept der Regierungskoalition gebe es zurzeit nicht. Der erste, noch von der großen Koalition verabschiedete Versuch einer Umsetzung der EU-Richtlinie wurde vom Bundesverfassungsgericht für nichtig erklärt. Da auf europäischer Ebene ohnehin eine Revision der Richtlinie vorbereitet würde, sei es nicht sinnvoll, zum jetzigen Zeitpunkt den absehbar bald veralteten Stand umzusetzen. Die Notwendigkeit der Maßnahme sei im Übrigen immer nur behauptet, aber nie bewiesen worden. Um dennoch Beweismittel zur Bekämpfung schwerer Straftaten zu sichern, habe das Justizministerium die Quick-Freeze-Lösung vorgeschlagen, bei der im Fall eines konkreten Verdachtes die Nutzerdaten für die spätere Auswertung festgehalten würden. Dieses Verfahren sei grundrechtsverträglich, da es nicht die gesamte Bevölkerung unter Generalverdacht stelle. Ein Kompromiss hingegen, bei dem zwar die Speicherzeit verkürzt würde, dennoch aber die Telekommunikationsdaten aller Einwohner festgehalten würden, sei nicht akzeptabel. Zum Zugangerschwerungsgesetz äußerte die Ministerin, dass der aktuelle Zustand der Nichtanwendung aus ihrer Sicht keine Missachtung des Parlaments darstelle, da das Gesetz selbst in § 1 einen entsprechenden Spielraum schaffe. Da die Erfolgsquote des BKA bei der Löschung kinderpornographischer Inhalte deutlich steige und die Hotlines des INHOPE-Netzwerks bereits jetzt sehr gute Erfolge erzielten, sehe sie auch keinen Bedarf für das Gesetz. In diesem Kontext dankte sie der eco-Internetbeschwerdestelle und dem INHOPE-Netzwerk für das Engagement bei der mittlerweile hocheffizienten Bekämpfung der illegalen Inhalte. Unabhängig vom jetzigen Schwebezustand setze sie sich für eine Aufhebung des Gesetzes vor Ablauf der Gültigkeitsdauer Ende 2012 ein.

Peter Schaar, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, näherte sich der Frage, ob neue Technologien ein neues Recht notwendig machten, aus historischer Perspektive. Er beleuchtete die Entwicklung der Informationsverarbeitung ab der Mitte des 18. Jahrhunderts und wies darauf hin, dass die

Rechtswissenschaft bereits im ausgehenden 19. Jahrhundert ein „right to be left alone“ postulierte. In Deutschland wurde dieses Recht ab Beginn der 1970er Jahre gesetzlich verankert. Mit der technischen Entwicklung der vergangenen zwei Jahrzehnte gewann die Frage des Datenschutzes dann eine bisher nicht geahnte Bedeutung, da Datenverarbeitung mittlerweile allgegenwärtig und unsichtbar geschehe – in immer mehr Alltagsgeräten seien Prozessoren integriert, die als Abfallprodukt auswertbare, zumindest indirekt personenbezogene Daten erzeugten. Beispiele seien Smart Grids oder Lokalisierungsdienste. Damit erwachsen neue Gefahren für die Persönlichkeitsrechte: Zum einen entstehe ein umfassender Datenschatten, der alles Handeln nachvollziehbar mache; zum anderen falle Material an, das zur Erstellung umfassender Persönlichkeitsprofile genutzt werden könne; abschließend sei eine Manipulation der Daten möglich, deren Konsequenzen nicht absehbar seien. Die Gesetzgebung müsse darauf reagieren, beispielsweise mit dem Rote-Linie-Gesetz. Zur Frage der Vereinbarkeit von Datenschutz und Cloud Computing äußerte er die Auffassung, dass Bundesdatenschutzgesetz und EU-Datenschutz-Richtlinie 95/46/EG hohe rechtliche, formale und technische Anforderungen stellten. Er sprach sich für die Übernahme des angelsächsischen Grundsatzes der Accountability aus, wonach für die datenschutzkonforme Verwendung der Daten jenes Unternehmen verantwortlich sei, das es an Dienstleister weitergebe. Ein bisher ungelöstes Problem für den Datenschutz seien Informationen, die sich aus Veröffentlichungen in sozialen Netzwerken über unbeteiligte Dritte generieren ließen.

Aus Werte der Rechtswissenschaft beleuchtete **Prof. Dr. Jürgen Taeger** von der Universität Oldenburg das Thema. Anhand der Haftungsregelungen im Preußischen Eisenbahngesetz zeigte er mit einem fast zweihundert Jahre alten Beispiel, dass neue Technologien selbstverständlich die Gesetzgebung beeinflussen – die Frage sei somit nicht das Ob, sondern das Wie. Neue Herausforderungen für den Gesetzgeber ergeben sich dabei laufend, wie beispielsweise die Regelungen für immaterielle Wirtschaftsgüter wie Software. Ergänzend zur Regulierung können Selbstverpflichtungen der Wirtschaft rechtliche Probleme lösen, wie beispielsweise Googles Verpflichtung zur Street View-Verpixelung auf Anfrage und in der Folge der Geodaten-Kodex vom 1. März 2011. Solche Selbstverpflichtungen seien nach Meinung der EU-Kommissarin auch ein geeignetes Mittel, um Datenschutz zu gewährleisten. Wo dies nicht greife, gebe es die Möglichkeit staatlicher Regulierung. Dabei müsse man sich bewusst sein, dass diese nicht immer zwingend aus einem objektiven Bedarf abgeleitet sei, sondern immer auch das aktuelle Kräfteverhältnis in der gesellschaftlichen Diskussion abbilde – ein aktuelles Beispiel dafür sei die Debatte um die Vorratsdatenspeicherung. Die Probleme der staatlichen Regulierung von Datenschutzfragen zeigten sich unter anderem darin, dass das Bundesdatenschutzgesetz nicht mehr eindeutig als allgemeines Datenschutzgesetz angesehen werden könne – zu viele bereichsspezifische Sonderlösungen seien mittlerweile in diesem Gesetz verankert, etwa im Bereich Scoring oder Beschäftigtendatenschutz. Zudem zeige das Gesetz handwerkliche Schwächen durch ungenaue Begriffsverwendungen, die in einigen Fällen die Anwendung in der Praxis erheblich erschweren.

Stephan Wrona, Director Legal & Regulatory und Data Protection Officer der Unitymedia Group, nahm den Blickpunkt der betrieblichen Alltagspraxis ein und wies mehrere Punkte auf, in denen rechtliche Anpassungen nötig seien, um neuen Techniken eine Chance zur Durchsetzung am Markt zu geben. Zunächst legte er dar, dass Cloud Computing aus rechtlicher Sicht eine Sonderform des IT-Outsourcing darstellt. Damit sei das outsourcende Unternehmen die für die Datenverarbeitung verantwortliche Stelle und an die Regelungen des Bundesdatenschutzgesetzes gebunden. Nach § 9 BDSG müsse es sich vor der Übermittlung von Daten an Auftragnehmer von dessen ordnungsgemäßer Einhaltung der Datenschutzrichtlinien überzeugen, unter anderem durch einen persönlichen Besuch der Rechenzentren, in denen die Daten verarbeitet werden. Im

Rahmen der Regelungen zur Auftragsdatenverarbeitung sei es zwar möglich, eine praktikable Lösung für dieses Problem zu finden, wenn die Daten nur innerhalb von EU und EWR gespeichert würden. Ein echtes Cloud Computing, bei dem die Daten in aller Welt gespeichert werden können, sei allerdings nicht möglich – Cloud Computing sei mit dem Bundesdatenschutzgesetz daher definitiv nicht vereinbar. Um die enormen Möglichkeiten dieser neuen Technologie zu nutzen, bedürfe es daher internationaler Standards, die den Unternehmen Rechtssicherheit bieten. Bezüglich der Quick-Freeze-Debatte wies er darauf hin, dass beim „Quick-Freeze“ eine höhere Gefahr falscher Auskünfte bestehe, weil während einer bestehenden Verbindung IP-Adressen wechseln könnten.

Die abschließende Podiumsdiskussion moderierte die IT-Journalistin **Monika Ermert**. In der Runde erörterten **Stephan Wrona** von Unitymedia, **Dr. Max Stadler**, parlamentarischer Staatssekretär bei der Bundesministerin der Justiz, **Dr. Alexander Dix**, Berliner Beauftragter für Datenschutz und Informationsfreiheit, **Dr. Astrid Auer-Reinsdorff**, Fachanwältin für Informationstechnologierecht und Vorstand DeutscherAnwaltVerein sowie **Oliver J. Süme**, stellvertretender Vorstandsvorsitzender des eco-Verbandes, Fragen zur geplanten Stiftung Datenschutz und zur Vorratsdatenspeicherung. Debattiert wurde zunächst, welchen Auftrag die Stiftung Datenschutz bei der Bewertung und Zertifizierung von Unternehmen erfüllen sollte. Herr Wrona eröffnete die Runde mit dem Statement, dass Unitymedia ein solches Zertifikat als Nachweis des sorgsamem Umgangs mit Kundendaten anstreben würde. Dr. Auer-Reinsdorff stellte in Frage, ob die Stiftungsaufträge der Zertifizierung und der vergleichenden Bewertung von Unternehmen miteinander vereinbar wären – denkbar sei die schwierige Konstellation, dass ein Unternehmen zwar zertifiziert sei, im Vergleichsranking aber schlechter abschneide als ein nicht zertifizierter Wettbewerber. Hierdurch entstehe entweder ein Glaubwürdigkeitsproblem oder ein Interessenkonflikt bei der Ranking-Erstellung. Zudem stellte sie in Frage, ob es neben den Datenschutzbehörden des Bundes und der Länder einer weiteren Institution bedürfe. Dr. Stadler vertrat hingegen die Ansicht, dass die Aufgaben klar abgegrenzt seien und die Stiftung für verschiedene Aufgaben besser geeignet sei als die etablierten Behörden. Ob das Zertifikat der Stiftung neben den bereits bestehenden Möglichkeiten von Landesbehörden oder privaten Anbietern vom Markt angenommen werde, müsse sich weisen. Dr. Dix hielt die Stiftung ebenfalls für einen vielversprechenden Ansatz, mahnte allerdings an, dass Datenschutz auch eine Aufgabe der Länder sei. Entsprechend solle auch die Stiftung keine reine Bundesstiftung sein, sondern von Bund und Ländern getragen werden. Herr Süme vertrat die Position, dass die Aufklärung zu Datenschutzfragen eine sehr wichtige Aufgabe der Stiftung sei. Für weitere Tätigkeiten wie die Zertifizierungen wünschte er sich ein tragfähiges, weithin akzeptiertes Gesamtkonzept statt kleinteiliger Insellösungen.

Zur Frage der Vorratsdatenspeicherung erinnerte Dr. Stadler daran, dass es vor den Anschlägen von Madrid 2004 einen einstimmigen Bundestagsbeschluss gegeben habe, keine Vorratsdatenspeicherung einzuführen. Seine Partei setze weiterhin auf das bewährte Prinzip, keine Eingriffe in die Privatsphäre ohne Anlass oder Verdacht zuzulassen. Deutschland sei im Übrigen nicht das einzige EU-Land, das sich der anlasslosen Komplettüberwachung verweigere. Er vertraue auch nicht darauf, dass die Nutzungsbeschränkung auf schwere Straftaten in der Praxis bestehen bleibe – ähnliche Beschlüsse habe es auch beim Mautsystem Toll Collect gegeben, später sei doch davon abgewichen worden. Ähnlich beim Zugangerschwerungsgesetz: Dort habe es nicht einmal einen Tag gedauert, bis nach der Verabschiedung die Ausweitung auf weitere Straftatbestände gefordert worden sei. Zum Glück habe man jedoch mit dem EU-Parlament einen starken Partner im Hinblick auf die Durchsetzung von Datenschutzansprüchen. Herr Süme wünschte sich eine Debatte auf höherer Ebene: Statt zu diskutieren, ob Quick Freeze oder Vorratsdatenspeicherung die bessere Lösung

sei, solle man zunächst überprüfen, ob überhaupt Nutzerdaten aufgezeichnet werden müssten. Dies sei nicht belastbar belegt, nur acht Mitgliedstaaten der EU hätten ihre Erfahrungen überhaupt zur Evaluierung mitgeteilt. Vor diesem Hintergrund sei es unzumutbar, der Industrie wieder Investitionen im dreistelligen Millionen- oder sogar im Milliardenbereich zuzumuten. In anderen EU-Ländern, beispielsweise Österreich oder Finnland, trage der Staat die Investitions- und Betriebskosten ganz oder teilweise. Dies sei auch in Deutschland nicht vom Verfassungsgericht ausgeschlossen worden. Herr Wrona berichtete aus der Unternehmenspraxis, dass die Anzahl der Auskunftersuchen von der Gesetzeslage zur Vorratsdatenspeicherung nicht beeinflusst würde. Er zweifelte zudem an der technischen Umsetzbarkeit einer Vorratsdatenspeicherung, die den strengen Vorgaben des Bundesverfassungsgerichts genügt. So sei beispielsweise die geforderte asymmetrische Verschlüsselung der Daten bei solch gewaltigen Datenmengen technisch noch völlig ungeklärt. Aber selbst ohne diese Hürde kämen gewaltige Kosten auf die Unternehmen zu. Dr. Auer-Reinsdorff merkte an, dass die Datenschutzfragen nicht nur mit nationaler Gesetzgebung, sondern auf internationaler Ebene gelöst werden müssten – beispielsweise übermittle jeder iPhone-Nutzer große Datenmengen an Apple, die ermittlungrelevant sein könnten. Auch für diese Fälle bedürfe es einer Regelung zur Nutzung und zur Durchsetzung der Nutzungsansprüche. Dr. Dix machte darauf aufmerksam, dass sich das Problem nicht nur auf Internetnutzungsdaten beziehe – auch Reise- oder Zahlungsinformationen seien lange in den Blickpunkt der Ermittlungsbehörden gerückt. Neben dem Anspruch, möglichst viele Daten zu speichern, sei es ein Problem, dass die Hemmschwelle zur Nutzung immer weiter sinke: Die Vorratsdatenspeicherung, einst zur Terrorismusbekämpfung eingeführt, solle nun schon zur Aufklärung einfacher Betrugsdelikte genutzt werden.

Im Anschluss an die Diskussion nutzten viele Kongressteilnehmer die Gelegenheit, die Impulse des Vortragsprogramms beim gemeinsamen Networking zu vertiefen.
