Anmerkungen

der Gesellschaft für Datenschutz und Datensicherung e.V. (GDD)

zur

Stellungnahme des Bundesrates zum Entwurf eines Gesetzes zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste

(Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz-ElGVG) - BR-Drs. 556/06 (Beschluss) vom 22.09.2006

Im Rahmen der Fortentwicklung der Medienordnung hat das Bundeskabinett am 14.06.2006 den Entwurf für ein Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz-ElGVG beschlossen (BR-Drs. 556/06 vom 11.08.2006). Hierzu hat der Bundesrat am 22.09.2006 Stellung genommen (BR-Drs. 556/06 vom 22.09.2006).

Aus Sicht der Gesellschaft für Datenschutz und Datensicherung e.V. (GDD) enthält die Stellungsnahme des Bundesrates zu Artikel 1 des Gesetzentwurfs (Telemediengesetz – TMG) an verschiedenen Stellen Ungenauigkeiten und zum Teil rechtlich unzutreffende Ausführungen, die im Rahmen der nachstehenden Anmerkungen – nicht zuletzt mit Blick auf die von der Bundesregierung beabsichtigte Gesamtnovellierung staatlicher Überwachungsbefugnisse – aufgezeigt werden sollen:

Zu § 14 Abs. 2 TMG (Punkt 4. der BR-Stellungnahme)

Nach der Formulierung im Regierungsentwurf *„darf“* der Diensteanbieter bestimmten Behörden bzw. Diensten im Einzelfall Auskunft über Bestandsdaten erteilen. Diese Formulierung ist entgegen der Stellungnahme des Bundesrates sachgerecht.

In der Begründung der Bundesregierung heißt es hierzu:

„Die Vorschrift besagt, dass Diensteanbieter aus der Aufgabenerfüllung im Bereich der Strafverfolgung sowie der genannten Behörden erwachsende Auskunftsansprüche nicht aus datenschutzrechtlichen Erwägungen zurückweisen können“.

Dies kann freilich nur gelten, wenn die entsprechenden Anordnungsvoraussetzungen auch tatsächlich vorliegen. Insofern weist die Regierungsbegründung zutreffend darauf hin, dass die Anordnung der zuständigen Stellen nach Maßgabe der hierfür geltenden Bestimmungen (Strafprozessordnung, Bundes- und Landesverfassungsschutzgesetze, Bundesnachrichtendienstgesetz, Gesetz über den militärischen Abschirmdienst) erfolgt. Liegen die Anord-

nungsvoraussetzungen aber offensichtlich nicht vor, so ist der Diensteanbeiter gerade nicht verpflichtet, die begehrten Daten zu übermitteln.

Soweit der Bundesrat die Parallelvorschrift des § 113 Abs. 1 Satz 1 TKG in Bezug nimmt, wonach der Diensteerbringer die betreffenden Daten im Einzelfall zu übermitteln *„hat“*, sollte im Rahmen der anstehenden TKG-Änderung eine Anpassung im Sinne des TMG-Regierungsentwurfs erfolgen.

Abermals zu § 14 Abs. 2 TMG (Punkt 5. der BR-Stellungnahme)

Nach der vom Bundesrat vorgeschlagenen Gesetzesformulierung soll der staatliche Auskunftsanspruch nicht nur zu Strafverfolgungszwecken sondern auch *„zur Gefahrenabwehr durch die Polizeibehörden der Länder“* bestehen. Zur Begründung führt der Bundesrat unter anderem Folgendes aus:

„Bestands- und Nutzungsdaten von Telemediendiensten werden auch zur Gefahrenabwehr, die auch die vorbeugende Bekämpfung von Straftaten umfasst, benötigt“.

Dieser Vorschlag ist nach Auffassung der GDD gleich in mehrerlei Hinsicht bedenklich:

1. Wie aus der Begründung des Regierungsentwurfs hervorgeht, sind etwaige Befugnisse zur Auskunftserteilung zum Zwecke der Gefahrenabwehr ggf. im Rahmen der jeweiligen spezialgesetzlichen Ermächtigungsnormen – normenklar – zu regeln. Insofern sei darauf hingewiesen, dass das Bundesverfassungsgericht gerade in zwei jüngeren Entscheidungen der Vertraulichkeit der Kommunikation bzw. dem Recht auf informationelle Selbstbestimmung den Vorrang vor präventiven Maßnahmen des Staates zur Gewährleistung der Inneren Sicherheit gegeben (vgl. BVerfG, NJW 2005, 2603 = MMR 2005, 674 sowie BVerfG, NJW 2006, 1939 = RDV 2006, 158) und dabei auf die besondere Intensität von technikbasierten, verdachtlosen Grundrechtseingriffen mit großer Streubreite hingewiesen hat.
2. Die Begründung des Bundesrates zur vorgeschlagenen Gefahrenabwehr bezieht sich überdies sowohl auf Bestands- als auch auf Nutzungsdaten. Insofern verkennt der Bundesrat zum einen, dass § 14 Abs. 2 TMG-E lediglich die Auskunft über Bestandsdaten betrifft. Der Umgang mit Nutzungsdaten soll in § 15 TMG geregelt werden.

   Zum anderen wird aufgrund dieses undifferenzierten Begründungsansatzes die unterschiedliche Eingriffsintensität von Zugriffen auf Bestandsdaten einerseits und Nutzungsdaten andererseits verkannt. Ein Zugriff auf Bestandsdaten ist – solange er nicht in Verbindung mit einem konkreten Telekommunikationsvorgang steht – weniger intensiv als der Zugriff auf Daten der Internetnutzung, die Aufschluss über das „Surf-Verhalten“ des Nutzers geben und deswegen strengeren Eingriffsvoraussetzungen bzw. im Regelfall einer richterlichen Anordnung unterliegen.
3. Der Bundesrat verkennt die Reichweite des Fernmeldegeheimnisses. Noch zutreffend ist die Feststellung, wonach die Erhebung von Bestands- und Nutzungsdaten einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt. Allerdings verkennt der Bundesrat, dass Nutzungsdaten im Herrschaftsbereich des Diensteanbieters durch das Recht auf informationelle Selbstbestimmung in seiner speziellen Ausprägung des Fernmeldegeheimnisses, das heißt nach Artikel 10 GG geschützt sind. Das Grundrecht aus Artikel 10 Abs. 1 GG gewährleistet die freie Entfaltung der Persönlichkeit durch einen privaten, vor der Öffentlichkeit verborgenen Austausch

von Kommunikation und schützt so zugleich die Würde des Menschen (vgl. BVerfGE 67, 157, 171). Um diesen Grundrechtsschutz effektiv zu gewährleisten, muss sich dieser auch nach Ende der Kommunikation dort fortsetzen, wo kommunikationsbezogene Informationen in irgendeiner Form gespeichert oder auf sonstige Weise verarbeitet werden (vgl. etwa die Anmerkung von Bär, MMR 2005, 523 f.). Danach unterliegen beispielsweise Daten, die in einem elektronischen Postfach oder einer Mailbox des jeweiligen TK-Betreibers gespeichert sind, unzweifelhaft weiterhin dem Schutzbereich von Artikel 10 GG.

Anders ist lediglich der Fall zu beurteilen, dass die Daten sich bereits im alleinigen Herrschaftsbereich eines Telekommunikationsteilnehmers, also zum Beispiel auf seinem PC oder der zu seinem Mobiltelefon gehörenden SIM-Karte befinden (vgl. BVerfG, NJW 2006, 976 = MMR 2006, 217 = RDV 2006, 116).

Schließlich ist auch die Folgerung des Bundesrates, wonach der Nutzer eines Teledienstes und der Diensteanbieter zueinander in einem Verhältnis von Kommunikationspartnern stehen sollen, unzutreffend. Insofern stellt auch die vorzitierte Entscheidung des Bundesverfassungsgerichts darauf ab, dass die Kommunizierenden sich auf die technischen Besonderheiten eines Kommunikationsmediums einlassen und sich dem eingeschalteten „Kommunikationsmittler“ anvertrauen. Inhalt und Umstände der Nachrichtenübermittlung seien dadurch dem erleichterten Zugriff Dritter ausgesetzt. Vor diesem Hintergrund hat das Gericht folgende Feststellung getroffen:

„Art. 10 Absatz 1 GG soll einen Ausgleich für die technisch bedingte Einbuße an Privatheit schaffen und will den Gefahren begegnen, die sich aus dem Übermittlungsvorgang einschließlich der Einschaltung eines Dritten ergeben (vgl. BVerfGE 85, 386 <396>; 106, 28 <36>; 107, 299 <313>).“

Die Ausführungen des Gerichts verdeutlichen, dass auch ein Internetnutzer nicht mit sondern über seinen Zugangsprovider kommuniziert, der insofern lediglich die technische Infrastruktur zur Verfügung stellt.

Zwar erfolgt beim Zugriff auf die Daten die Grundrechtsbeeinträchtigung nur vermittelt durch den privatrechtlich organisierten Telemediendiensteanbieter. Handelt der Diensteanbieter allerdings auf Grund einer verbindlichen hoheitlichen Anordnung, so ist sein diesbezügliches Verhalten der öffentlichen Gewalt zuzurechnen (vgl. BVerfG, NJW 2003, 1787, 1793).

Fazit

Die Stellungnahme des Bundesrates überzeugt insbesondere hinsichtlich seiner undifferenzierten Ausführungen zur vorbeugenden Bekämpfung von Straftaten und zur Reichweite des Fernmeldegeheimnisses nicht.

Folgte der Gesetzgeber der Begründung des Bundesrates zur rechtlichen Einordnung der Internetnutzung, würde ein folgenschwerer Schritt in die falsche Richtung unternommen, der insbesondere der von der Bundesregierung angestrebten Neukonzeption eines harmonischen Gesamtsystems der staatlichen Überwachungsbefugnisse in kontraproduktiver Weise vorgreifen würde. Aufgefordert ist die Bundesregierung vielmehr dazu,

das Fernmeldegeheimnis im Rahmen dieser Neukonzeption durch einen umfassenden Richtervorbehalt verfahrensrechtlich abzusichern.

In Sinne eines effektiven Grundrechtsschutzes wird seitens der GDD angeregt, gesetzlich klarzustellen, dass bei der Verwendung dynamischer IP-Adressen auch Bestandsdaten, die im Zusammenhang mit einem konkreten Kommunikationsvorgang stehen, vom Fernmeldegeheimnis umfasst sind (ebenso Beck`scher TKG-Komm/Bock, 3. Aufl., § 113 Rdnr. 24 m. w. N.) . Immerhin wird gerade aus der Kombination dieser Daten ersichtlich, wer zu welchem Zeitpunkt über welchen Zugangsanbieter welche Internetseiten aufgerufen hat.

Mit Blick auf die von der Bundesregierung geplante Umsetzung der Richtlinie über die Vorratsspeicherung von Daten der elektronischen Kommunikation (2006/24/EG) sei abschließend aus dem Vortrag der Bundesjustizministerin anlässlich des 66. Deutschen Juristentages am 19.09.2006 in Stuttgart noch Folgendes zitiert:

„Aber der Staat darf nicht ins Blaue hinein unbescholtene Bürger überwachen, um herauszufinden, ob jemand überhaupt verdächtig sein könnte. Dies wäre der Weg in einen Präventionsstaat, in dem Freiheitsrechte nur noch als Risiko für die Sicherheit gelten und letztlich jedermann als potenzieller Täter verdächtig ist.“

Bonn, den 09. Oktober 2006