

Sicherheit statt Rechtsstaat

Der Konflikt bei der Vorratsdatenspeicherung spitzt sich zu

Ohne mit der Wimper zu zucken nahm die versammelte Riege der großen Koalition das Ergebnis eines vom Wissenschaftlichen Dienst des Bundestages veröffentlichten Gutachtens entgegen.¹ In ihm wurden schwere Bedenken gegen die Anfang 2006 verabschiedete Richtlinie der Europäischen Gemeinschaft (EG) zur Vorratsdatenspeicherung² geäußert, nach der in Zukunft Telekommunikationsdaten zwischen sechs und 24 Monaten verdachtsunabhängig gespeichert werden sollen. Es handelt sich dabei um annähernd alle Verkehrs-, also Standort- und Kennungsdaten, die beim Telefonieren, Mailen, Simsen oder Surfen anfallen. Bereits nach den Madrider Zugenschlägen vom 11. März 2004 wurde ein Vorschlag für einen Rahmenbeschluss im Ministerrat der Europäischen Union (EU) eingebracht, der an eine im Jahr 2002 abgelehnte Vorlage Dänemarks anknüpfte. Da allerdings Streitigkeiten darüber bestanden, ob die Regelung im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen liegt, oder aber einem Gesetzgebungsverfahren mit Beteiligung des Parlaments unterfällt, blieb der Vorschlag zunächst auf Eis. Auslöser für die erneute Initiative war die Überführung eines Verdächtigen der Anschläge von London 2005 an Hand seiner Handy-Telefonate. Auf Druck des scheidenden EG-Ratspräsidenten Tony Blair wurde die Richtlinie daraufhin im zweiten Halbjahr 2005 durch die Kommission eingebracht und im schnellsten Gesetzgebungsverfahren der europäischen Geschichte beschlossen. Schon drei Monate später stimmte das EG-Parlament mit der Mehrheit der beiden großen europäischen Volksparteien dem Richtlinienvorschlag zu. Weitere drei Monate später folgte der Ministerrat. Daran konnte auch das von Beginn an eröffnete Dauerfeuer der Datenschutzbeauftragten und Bürgerrechtsorganisationen nichts mehr ändern. Sie sahen das Recht auf informationelle Selbstbestimmung und die Unschuldsvermutung in Gefahr und verwiesen darauf, dass die bereits in vielen europäischen Ländern praktizierte verdachtsabhängige Datenerfassung vollkommen ausreichend ist.

Ein skandalöses Gesetzgebungsverfahren

Europas SicherheitspolitikerInnen konnten die gesammelte Mannschaft der europäischen und nationalen Politik von ihrem unsinnigen Gesetzesvorschlag überzeugen. Die unbekannt und technisch komplexe Materie der Datenspeicherung sowie ein zeitlich künstlich verengtes parlamentarisches Verfahren spielte ihnen dabei kräftig zu. Mit dem Argument der dringenden Terrorismusbekämpfung wurde ein notwendiger Dialog – insbesondere mit fachlich versierten Nichtregierungsorganisationen – verhindert. Außer einer Handvoll Abgeordneten und MitarbeiterInnen in den zuständigen Gremien und Ausschüssen, hatte das Gros der Europaabgeordneten nur begrenzt Einblick in die Bestimmungen und deren Auswirkungen auf Daten- und Privatsphärenschutz. Der zuständige parlamentarische Berichterstatter Alexander Alvaro bezeichnete den Vorgang später als skandalös und nahm seinen Namen von der Parlamentsvorlage. Sein deutlich abgeschwächter wengleich auch von DatenschützerInnen kritisierte Vorschlag enthielt zumindest noch die Bestimmungen, dass die Daten ausschließlich in Sachen Terrorismus und organisierter Kriminalität verwendet dürfen, sowie dass die Speicherdauer abschließend auf zwölf Monate begrenzt wird. Doch nicht nur die Entscheidung im Parlament, sondern auch jene im Ministerrat entbehrt eines sauberen Verfahrens. So hatte sich der Bundestag noch im Februar 2005 neben den Parlamenten von England und den Niederlanden ausdrücklich gegen jegliche Datenspeicherung auf Vorrat ausgesprochen und der Bundesregierung im Rahmen der Ratsverhandlungen mitgegeben, sich gegen eine entsprechende Richtlinie auszusprechen.

1 Deutscher Bundestag, WD 3 – 282/06.

2 Richtlinie 2006/24/EG vom 15.3.2006, ABl L 105/54.

All diese Entscheidungen hatten Union und SPD voll und ganz mitgetragen. Mit den Stimmen eben dieser nunmehr als große Koalition auftretenden Parteien wurde dann Anfang 2006 eine Zustimmung des Bundestags zum ausgearbeiteten Richtlinienentwurf durchgebracht. Man fühlte sich zur Umsetzung gezwungen, obwohl selbst einschlägige Stimmen aus den eigenen Reihen darin einen „inakzeptablen Anschlag auf die Bürgerrechte“³ sahen. Dabei wäre die Richtlinie wohl nie so gekommen, wenn sich die Regierungsunterhändler an den ursprünglichen Auftrag des Bundestags und somit an Art. 23 des Grundgesetzes (GG) und das Gesetz zur Zusammenarbeit von Bundesregierung und Bundestag in Angelegenheiten der Europäischen Union⁴ gehalten hätten. Und anstatt die eigene Unzulänglichkeit einzugestehen, wird „Brüssel“ für die Richtlinie verantwortlich gemacht, die die Bundesregierung unter Missachtung des Bundestagsvotums ausgehandelt hat. Das Machtlosigkeitsargument als Bankrott-erklärung der rechtstaatlichen Demokratie – ein Blankoschein für sinnlose Sicherheitsträumereien auf Kosten der Grundrechte.

Das Ende der freien Kommunikation

So erscheint die Richtlinie zur Verbesserung der Sicherheit noch nicht mal geeignet. Rund 450 Millionen Menschen leben in Europa und die meisten von ihnen telefonieren, simsen, mailen und surfen. Alle Spuren dieser Aktivitäten, sprich Zeit, Dauer und Anfangsstandort sowie die Kennungsdaten, wie Gerätenummer, Simkartenummer oder IP-Adresse, sollen laut der Richtlinie auf Vorrat gespeichert werden. Nach Zahlen von BITKOM, die unwidersprochen geblieben sind, würden allein für Deutschland pro Tag(!) 639.000 CDs voll geschrieben.⁵ Immer wieder wurde von ExpertInnen ausgeführt, dass es nahezu unmöglich ist, eine solche Menge an gesammelten Verbindungsdaten sinnvoll und sicher zu verwerten. Die bezweckte Wirkung wäre damit gleich null. Doch der Richtlinie, die sich auch im Europarecht an einem angemessenen Verhältnis zwischen Mittel und Zweck messen lassen muss,⁶ fehlt es nicht bloß an der Eignung. Durch die generelle Speicherung aller Verbindungsdaten wird künftig Jede und Jeder potentiell verdächtig. Der Grundsatz der Unschuldsvermutung aus Art. 6 II der Europäischen Menschenrechtskonvention (EMRK) tritt gänzlich außer Kraft. Sogar die Konstruktion von Persönlichkeitsprofilen anhand der Standortdaten und Nutzungszeiten wird ermöglicht, wobei die Gefahr des Missbrauchs vollkommen unbeachtet bleibt. So sollen künftig Staatsanwaltschaft, Polizei, Gerichte, Zoll und Geheimdienste gleichermaßen Zugriff auf die Daten haben. Und selbst andere Staaten wie etwa die USA können über Rechtshilfeabkommen ohne Richteranordnung Verbindungsdaten einsehen. Zudem lässt die EU den Mitgliedstaaten genügend Hintertüren bei der Definition des Verwendungstatbestands „schwerer Straftaten“, um auch bei minder schweren Straftaten in den anzulegenden Datenbergen schürfen zu können. Die Zweckbindung erscheint absolut untauglich, eine schleichende Zweckentfremdung hin zu leichteren Straftaten zu verhindern. Nicht nur die Äußerung des US-Justizministers Alberto Gonzales, die durch die Vorratsdatenspeicherung erlangten Daten natürlich auch zur Bekämpfung leichterer Kriminalitätsformen zu verwenden,⁷ deutet darauf hin: Noch vor der Verabschiedung der Vorratsdatenspeicherung auf EG-Ebene hatte Bundesjustizministerin Brigitte Zypries vorgeschlagen, man könne die so gewonnenen Daten auch zur Verfolgung von Stalking-Praktiken einsetzen.⁸ Ebenso ist es den Mitgliedsländern überlassen, ob es eine Kostenerstattung für die von den Behörden zur Datenspeicherung verpflichteten Telekommunikationsunternehmen geben wird. So wären zu Gunsten des staatlichen Sicherheitsbedürfnisses kleine und mittelständische Unternehmen langfristig in ihrer Existenz bedroht. Was als präventive Terrorismusbekämpfung beschlossen wurde, ist offensichtlich

3 Zitat MdB Jörg Tauss, medienpolitischer Sprecher der SPD-Fraktion, im Bundestag am 16.2.2006.

4 BGBl I 1993, 311, 12. März 1993.

5 <http://www.heise.de/newsticker/meldung/66965>

6 BVerfG 2 BvR 2236/04 vom 18.7.2005.

7 BVerfG 1 BvR 518/02 vom 4.4.2006.

8 BVerfGE 65, 1 vom 19.10.1983.

nichts anderes als die Bekämpfung der unbeobachteten Kommunikation. Mit den Worten von Thilo Weichert, Landesdatenschutzbeauftragter in Schleswig-Holstein: „Wenn über Monate hinweg minutiös nachvollzogen werden kann, wer wo im Internet gesurft hat, wer wann mit wem per Telefon, Handy oder E-Mail kommuniziert hat, dann wird die Schwelle von der freiheitlichen Informationsgesellschaft zum digitalen Überwachungsstaat überschritten“.⁹

Verfassungskonforme Auslegung nicht möglich

Das Ergebnis des bereits benannten Bundestagsgutachtens kommt nicht überraschend. Das Bundesverfassungsgericht hat dem Gesetzgeber in der Entscheidung zum EU-Haftbefehl auferlegt, dass er alle Spielräume des Gemeinschaftsrechts grundrechtsschonend ausschöpfen muss.¹⁰ Ob dem Bundesgesetzgeber eine grundrechtskonforme Ausgestaltung gelingen wird, ist äußerst fragwürdig. Sollte das Bundesverfassungsgericht seine bisherige Rechtsprechung, die es zuletzt in der Rasterfahndungsentscheidung bekräftigt hat,¹¹ beibehalten, so muss es jedes deutsche Umsetzungsgesetz zur Vorratsdatenspeicherung als verfassungswidrig bezeichnen. Seit dem Volkszählungsurteil¹² gilt ein striktes Verbot der Sammlung personenbezogener Daten auf Vorrat außerhalb statistischer Zwecke. Bei der Lektüre des Rasterfahndungsurteils entsteht nahezu der Eindruck, als sei er gerade auch im Hinblick auf die Vorratsdatenspeicherung formuliert worden. In einem umfassenden Gutachten stellt die Humanistische Union fest, dass das Vorhaben gegen Art. 10 GG und insbesondere Art. 8 EMRK verstößt. Gemeinsam mit anderen BündnispartnerInnen strengt sie nun bereits im Vorfeld des Gesetzgebungsprozesses Verfassungsbeschwerden an, die nach den benannten Gutachten und Urteilen gute Aussichten auf Erfolg haben. Nach der Entscheidung des Bundesverfassungsgericht zum Großen Lauschangriff vom März 2004 ist der Kernbereich privater Lebensführung absolut geschützt, was der systematischen Erfassung von Verkehrsdaten widerspricht. Besonders bei RechtsanwältInnen, ÄrztInnen, Geistlichen und JournalistInnen beschneidet die Vorratsdatenspeicherung viele verfassungsrechtlich geschützte Bereiche. Wie soll gerade ohne inhaltliche Analyse der Kommunikation festgestellt werden, ob gerade ein InformantInnen-, PatientInnen- oder MandantInnenverhältnis besteht? Damit steuert die Politik unabänderlich auf einen Konflikt zwischen Europarecht und deutschem Verfassungsrecht zu. Stets hat das Bundesverfassungsgericht betont, dass es für sich die Aufgabe des Grundrechtsschutz proklamiert, solange auf europäischer Ebene nicht ein im wesentlichen vergleichbarer gewährleistet ist.¹³ Doch selbst wenn die Richter aus Karlsruhe sich um die Konsequenz dieser Aussage drücken sollten, so könnte die Vorratsdatenspeicherung in Form der EU-Richtlinie in Luxemburg vorm Europäischen Gerichtshof gekippt werden. Bereits jetzt klagen dort Irland und die Slowakei auf Grund der aus ihrer Sicht falschen Kompetenzgrundlage. Sie bezweifeln, dass die Vorratsdatenspeicherung in die Kompetenzen des supranationalen EG-Rechts fallen und sehen lediglich eine Regelung über die intergouvernementale polizeiliche und justizielle Zusammenarbeit als rechtmäßig an.

Mit mehr Sicherheit andere Fehler ausbügeln

Dennoch will die Regierung an einem Gesetzesentwurf im Sinne der Richtlinie arbeiten. Die vorgebrachten Zweifel an der Unvereinbarkeit mit dem Grundgesetz wischt sie hinweg. Dabei vergisst sie offenbar, dass es sich beim Recht auf informationelle Selbstbestimmung um ein Verfassungsgut handelt, das nicht mal eben so zur Disposition steht. Auf die Spitze treibt es der parlamentarische Staatssekretär im Innenministerium Peter Altmaier (CDU), der eine öffentliche Debatte darüber fordert, „was an Datenschutz noch nötig ist“ und nun im Namen der Terrorismusbekämpfung auch noch auf

9 BVerfG, 2 BvL 1/97 vom 7.6.2000.

10

11

12

13

die Daten der Autobahnmautsysteme von TollCollect zugreifen will. Angesichts der verfassungsrechtlichen Konsequenzen einer verdachtsunabhängigen Vorratsdatenspeicherung fordert der Bundesdatenschutzbeauftragte Peter Schaar ein Moratorium für den Gesetzgebungsprozess und die Bundesregierung auf, sich angesichts der Entscheidung des Europäischen Gerichtshofes über die Nichtigkeit einer Weitergabe von Fluggastdaten an die USA für einen europaweiten Verzicht auf die Vorratsdatenspeicherung einzusetzen. Auch sein ehemaliger Berliner Kollege Hansjürgen Garstka vermutet hinter den immer wieder auftauchenden Forderungen der SicherheitspolitikerInnen vor allem ein Vollzugsdefizit. So dürfe der Bundesnachrichtendienst etwa bereits jetzt Auslandsgespräche auf Stichworte hin untersuchen, was bei den Anrufen der erfolglosen Kofferbomben-Attentäter in den Libanon schon im Vorfeld hätte greifen können. Und selbst die Attentäter von Madrid 2004 wären auch ohne Vorratsdatenspeicherung durch das Einfrieren und Auswerten der nach dem Anschlag vorhandenen Daten identifizierbar gewesen. Die mit der Vorratsdatenspeicherung verfolgte Terrorismusbekämpfung ist nämlich bereits nach geltendem Recht effektiv und grundrechtskonform möglich: Auf richterliche Anordnung können die Behörden alle Daten hinreichend verdächtiger Personen speichern lassen, ohne dabei jedeN NutzerIn elektronischer Kommunikation präventiv einem Verdacht zu unterwerfen. Die Regelung ist abseits aller weiteren Bedenken also vor allem nicht erforderlich.

Der Datensammlungswahn ist der hilflose Versuch der SicherheitspolitikerInnen, die letztlich ihnen angelasteten Versäumnisse der Kollegen aus dem Außen-, Sozial- und Entwicklungsressort mit Brachialmethoden auszubaden. Die fehlende Erkenntnis, dass Terror nicht Ursache, sondern ein unbeherrschbares Symptom einer Krankheit der Weltgemeinschaft ist, entwickelt sich langsam aber sicher zur größten Gefahr für Freiheit, Demokratie und Rechtsstaat. Die unkontrollierte Anhäufung von Daten Unverdächtiger darf kein Prinzip werden. Um das Verfassungsgut der informationellen Selbstbestimmung auch in Zukunft angesichts immer neuer technologischen Errungenschaften in der realen und virtuellen Welt zu sichern, bedarf es endlich eines modernisierten Datenschutzes, das eine zügellose Sicherheitspolitik verhindert, sowie einer umfassenden Sensibilisierung der Menschen beim Umgang mit eigenen Daten. Bis dahin muss die Umsetzung der Vorratsdatenspeicherung auf Eis gelegt und die deutsche EG-Ratspräsidentschaft zu einer Rücknahme der Richtlinie genutzt werden.

Jan Albrecht studiert Jura an der HU Berlin. Er ist Bundessprecher der Grünen Jugend.

Weiterführende Literatur:

Patrick Breyer: Vorratsdatenspeicherung – Die totale Protokollierung der Telekommunikation kommt. In: Datenschutz Nachrichten 1/2006, S. 17-20.

Alexander Alvaro: Die Richtlinie zur Vorratsdatenspeicherung. In: Datenschutz Nachrichten 2/2006, S. 52-55.

www.voratsdatenspeicherung.de