A Never-Ending Story : Die Vorratsdatenspeicherung

verfassungsblog.de/a-never-ending-story-die-vorratsdatenspeicherung/

Indra Spiecker genannt Döhmann , Spiros Simitis Di 5 Mai 2015

Di 5 Mai 2015

2004 erschütterten Terroranschläge in London und Madrid die Welt. Die Reaktion der EU/EG im seinerzeit schnellsten Gesetzgebungsverfahren seit Bestehen: Verabschiedung der Vorratsdatenspeicherungsrichtlinie. 2009 sah der EuGH die Richtlinie trotzdem als Binnenmarktregelung an, mit der Harmonisierung auf dem Informationsmarkt herbeigeführt werden sollte. Äußerungen zum Inhalt – quasi als obiter dictum möglich gewesen – versagte er sich. 2010 beurteilte dann das BVerfG die bundesdeutsche Umsetzung, aber – ganz dem Verhältnis von EuGH und BVerfG entsprechend – nur den die europäischen Mindestvorgaben überschießenden Teil. Dieses Gesetz hatte national schon für reichlich Sprengstoff im Rechtsstaat gesorgt und u.a. den Rücktritt der beharrlich widersetzlichen Justizministerin bewirkt.

Fazit des BVerfG seinerzeit: Wichtige Präzisierungen fehlten, das Gesetz war nichtig. Indes: Es war wohl eher ein Pyrrhus-Sieg. Denn im Kern hatte das deutsche Verfassungsgericht es tatsächlich als möglich erachtet – und damit in nicht offen ausgesprochener Abweichung von der bisherigen Rechtsprechung -, eine anlasslose Speicherung durchzuführen, wenngleich nur unter bestimmten Bedingungen, die (noch) nicht eingehalten worden waren. 2014 entschloss sich der EuGH endlich, seinerseits auch inhaltlich Stellung zu beziehen. In seinem Urteil ging das europäische Gericht allerdings deutlich weiter als das deutsche: Die (reichlichen) Fehler des europäischen Gesetzgebers wurden aufgelistet, auch wenn wohl schon die breite Anlasslosigkeit der Speicherung ohne nennenswerte Beschränkung der Verwendung für den Todesstoß ausgereicht hatte.

Wer nun glaubte, damit sei endlich ein Schlussstrich gezogen unter eine Präventivmaßnahme, deren Geeignetheit höchst fraglich ist, wird nunmehr endgültig eines Besseren belehrt: Zum einen ist noch unklar, ob – auf der Basis des EuGH-Urteils zu Åkerberg Fransson – womöglich auch weiteren nationalen Alleingängen wegen Ausstrahlungswirkung der EU-Charta die Grundlage entzogen ist. Nach zunächst tapferem Widerstand hat sich jetzt aber das Justizministerium entschlossen, dem Drängen der Big-Data-Fraktion nachzugeben und erneut eine Vorratsdatenspeicherung in Deutschland mitzutragen. Diese soll deutlich maßvoller ausfallen: Statt mindestens sechs Monaten soll nunmehr vier (Standortdaten) bzw. zehn Wochen (alle übrigen Verkehrsdaten) gespeichert werden dürfen; der Abruf ist nur möglich bei „eng definierten Strafverfolgungszwecken“; Berufsgeheimnisträger müssen zwar damit leben, dass sie erfasst werden, der Abruf ihrer Daten ist aber untersagt.

Davon erfährt das Volk – der Souverän – aber nicht etwa durch Vorlage eines Gesetzesentwurfs. Nein, vielmehr werden seitens des Ministeriums (das übrigens erstaunlicherweise statt des bisher drängenden Innenministeriums als Urheber in Erscheinung tritt) in einem ersten Schritt „Leitlinien“ präsentiert, aus denen im Kern herausgelesen werden kann, was herausgelesen werden will. Insofern ist Kritik und Lob am Inhalt gleichermaßen unangebracht: Solange kein exakter Text vorliegt, ist eine saubere Einschätzung gar nicht möglich. Auffällig ist aber, dass gleich an mehreren Stellen eine Bürgerrechtsfreundlichkeit postuliert wird, die auch in der wenig aussagekräftigen Absichtserklärung wenig überzeugend gelingt, so dass man gespannt auf das Gesetz sein darf.

Das fängt damit an, dass Emails von der VDS ausgenommen sein sollen. Erleichterung! Tatsächlich aber waren Emails ohnehin nie erfasst, denn die VDS ist gerade keine Inhalts-, sondern eine Verbindungsüberwachung. Schwerer aber wiegt die Behauptung, eine vollständige Nicht-Überwachung der Berufsgeheimnisträger, etwa durch eine entsprechende Auflistung, die dann von den speichernden TK-Unternehmen zu beachten ist, sei nicht möglich. Es verwundert doch nicht wenig, dass zum Schutz der Bürger eine Technik nicht funktionieren soll, die zu ihrer Verfolgung als effektiv hochgehalten wurde. Denn war nicht das Konzept der Sperrung kinderpornographischer Seiten genau darauf gestützt, über eine Liste den Zugriff auf bestimmte IP-Adressen zu verhindern? Nun hatten in der Tat die Kritiker seinerzeit darauf verwiesen, dass diese Liste nie aktuell gehalten werden könne, weil ein Kinderpornographie-Händler dem BKA wohl kaum seine Verbindungsdaten mitteilen werde. Von einer Rechtsanwaltskanzlei, einem Kloster, einer Seelsorgeeinrichtung kann man das aber durchaus

erwarten – und deren Neigung, immer wieder neue IP-Adressen zu generieren, dürfte nachvollziehbar gering sein. Warum zudem in der Erstellung einer Liste regelmäßig ein (schwerwiegenderer) Eingriff in die Rechte dieser Berufsgeheimnisträger sein soll, erschließt sich auch bei längerem Nachdenken nicht. Big Data darf durchaus auch einmal zugunsten des Bürgers wirken, und staatlicher Aufwand auch dem freiheitlichen Schutz gelten. Zudem bietet das Abrufverbot nur ein höchst eingeschränkt wirksames Schutzinstrument. Denn um dieses wirksam zu gestalten, muss der Staat just die Verbindung von Verbindungsdaten und Berufsgeheimnisträger auflösen. Dann kann es aber auch gleich auf der ersten Stufe erfolgen.

Auch die sonstigen Sicherungen sind im Idealfall kritisch zu betrachten. Dass ein „strenger Richtervorbehalt“ noch schützt, ist schon lange und längst nicht nur für den Datenschutz mehr als zweifelhaft, selbst wenn man parallel zur Wohnraumüberwachung Eilkompetenzen der Staatsanwaltschaft ausnimmt – angesichts der Speicherfristen allerdings wohl kaum ein echtes Problem für den Zugriff. Die über netzpolitik.org bekannt gewordene Nebenabrede über den Abruf von Bestandsdaten ohne Richtervorbehalt macht das noch einmal deutlich. Und auch die Transparenz dürfte gerade angesichts der aufgelisteten Straftaten, die einen Abruf ermöglichen sollen (die übrigens typische Internet-Straftaten ausnehmen), wenig ausgeprägt sein. Dass Informationseingriffe eben nicht mehr aus der Welt zu schaffen sind und daher jegliche nachträgliche Benachrichtigung faktisch den Rechtsschutz aushebelt, ist eine Binsenweisheit. Und die Vorstellungen zur IT-Sicherheit sind so vage, dass man sich fragen darf, ob sie dem IT-Sicherheitsgesetz wohl genügen werden?

Gut gemeint ist noch lange nicht gut gemacht, und die Salami-Taktik des Ministeriums, erst einmal eine grobe Richtschnur in den Raum zu stellen, um dann noch in concreto nachbessern zu können, zeigt, wie unsicher man sich dort eigentlich ist. Und dies durchaus zu Recht. Man würde sich wünschen, dass das Bauchgrimmen des Justiz- und Verbraucherschutzministeriums, das sich bisher in bemerkenswerter Weise zugunsten von Privatheit und Datenschutz hervorgetan hat, wieder auf diese Tugenden besinnt und endgültig an der „Vorratsdatenspeicherung“ nicht weiterschreibt. Totale Sicherheit gibt es nicht, und bei allem gerechtfertigten Selbstschutzbedürfnis eines wehrhaften Rechtsstaats sollte weiterhin gelten: Das Recht braucht dem Unrecht nicht zu weichen. Das gilt auch für den Datenschutz, um den Terror zu bekämpfen. Wem das zu abstrakt ist: Wohin der Versuch führt, Privatheit und Selbstbestimmung zum natürlichen Verbündeten des Verbrechers zu erklären, konnte man in Deutschland schon einmal beobachten: Vor dem Mauerfall.

SUGGESTED CITATION Spiecker genannt Döhmann, Indra; Simitis, Spiros: *A Never-Ending Story : Die Vorratsdatenspeicherung, VerfBlog,* 2015/5/05, http://verfassungsblog.de/a-never-ending-story-die-vorratsdatenspeicherung/.