

Der Rechtsstaat als Überwachungsstaat – die Vorratsdatenspeicherung

Wenn wir uns heute mit anderen austauschen wollen, greifen wir regelmäßig auf Telefon, Handy, E-Mails oder das Internet zurück. Das geht einfach, schnell und unkompliziert. Dieser technische Fortschritt hat aber auch eine Kehrseite: Mit jedem Telefonat, jeder SMS oder jeder E-Mail erzeugen wir elektronische Datenspuren, die von den technischen Dienstleistern gespeichert werden. Je mehr wir auf elektronische Hilfsmittel zurückgreifen, umso mehr Kommunikationsdaten erzeugen wir. Aus diesen Verbindungs- bzw. Verkehrsdaten lässt sich rekonstruieren, wer, wann, von wo aus, mit wem, wie und wie lange gesprochen hat. Der rechtsstaatliche Umgang mit diesen Kommunikationsdaten ist eine Aufgabe des Datenschutzes. Wer Verbindungsdaten auswertet, kann damit Kommunikationsnetze identifizieren, Bewegungsprofile ermitteln und persönliche Interessen feststellen. Verkehrsdaten können, anders als das gesprochene Wort, bereits heute automatisiert durchsucht, analysiert, mit anderen Datenbeständen verknüpft und ausgewertet werden. Entsprechend hoch ist die Gefahr, dass Verbindungsdaten von anderen missbraucht werden. Wieweit damit einzelne Nutzer ausgeforscht werden können und welche Rückschlüsse auf ihre Kommunikationsinhalte möglich sind, hängt davon ab, wie intensiv und auf welche Art und Weise sie die elektronische Medien im Einzelnen nutzen. Allerdings wäre der Verzicht auf moderne Kommunikationsmittel nur eine negative Form der Freiheit und für viele Menschen keine Alternative.

Unter dem Grundgesetz sind deshalb nicht nur die Inhalte der Kommunikation – was wir sagen oder schreiben – sondern auch ihre äußeren Umstände geschützt. Insbesondere wegen der Möglichkeiten zur automatischen Auswertung der Verbindungsdaten verlangt das Bundesverfassungsgericht in seiner Rechtsprechung einen besonderen Schutz. Mit der automatisierten Verarbeitung steigt nämlich „nicht nur die Menge der anfallenden Verbindungsdaten, sondern auch deren Aussagegehalt. Sie lassen in zunehmendem Maße Rückschlüsse ... auf den jeweiligen Kommunikationsinhalt zu und vermitteln – je nach Art und Umfang der angefallenen Daten – Erkenntnisse, die an die Qualität eines Persönlichkeitsprofils heranreichen können.“¹ Deshalb ist die Speicherung der Verbindungsdaten bisher nur zulässig, sofern die Daten für Abrechnungszwecke erforderlich sind. Für alle Nutzer von Pauschaltarifen (Flatrates) müssen die Verbindungsdaten nach spätestens 7 Tagen gelöscht sein.

¹BVerfG, Urteil vom 02.03.2006, Az. 2 BvR 2099/04, <http://www.bverfg.de>, Abs. 91.

Das soll sich nach dem Willen der Bundesregierung ändern. Mit der von ihr geplanten Vorratsdatenspeicherung wird der Schutz der fernmündlichen Kommunikation auf den Kopf gestellt: An die Stelle von Vorschriften zur fristgerechten *Löschung* der Kommunikationsdaten bei den Providern tritt nun die *Pflicht zur Speicherung*. Alle Telekommunikationsunternehmen sollen verpflichtet werden, sämtliche Verkehrsdaten über Telefon-, Handy-, Internet- und E-Mailverbindungen von Jedermann sechs Monate lang zu speichern. Dabei beruft sich der deutsche Gesetzgeber auf seine Pflicht zur Umsetzung einer europäischen Richtlinie zur Vorratsdatenspeicherung (2006/24/EG), wohl wissend, dass diese Regelung mit dem deutschen Datenschutzrecht kollidiert und den bisherigen Entscheidungen des Bundesverfassungsgerichts zum Schutz des Fernmeldegeheimnisses zuwiderläuft.

Noch in der letzten Legislaturperiode, weit nach dem 11. September 2001, war sich die große Mehrheit des Bundestages einig, dass eine europäische Vorgabe für die Mindestspeicherfristen von Verkehrsdaten abzulehnen sei. Die Parlamentarier betonten im Februar 2005, dass derartige Vereinbarungen nur im Bereich der sogenannten „Dritten Säule“ der EU, als Rahmenbeschluss und damit einstimmig beschlossen werden könnten. Der Europäischen Gemeinschaft dagegen fehle die Kompetenz, über Strafrechtsachen zu entscheiden. Ein solcher Rahmenbeschluss kam aber nicht zustande, vor allem bei den Mindestspeicherfristen wurde man sich nicht einig. Vielmehr stimmte das Europäische Parlament am 14. Dezember 2005 einem von den Justizministern vorgelegten Kompromisstext für eine Richtlinie zu, der sich auf Artikel 95 EG-Vertrag, d.h. auf die „Erste Säule“ stützte. Dies begegnete sofort massiven Bedenken, weil Artikel 95 des EG-Vertrages der Regulierung des Binnenmarktes dient. Die Richtlinie dagegen verfolgt primär das Anliegen einer effektiven Strafverfolgung.

Irland hat deswegen eine Nichtigkeitsklage vor dem Europäischen Gerichtshof erhoben. Über diese Klage wurde bisher noch nicht entschieden. Nach der Entscheidung des Europäischen Gerichtshofes über die Fluggastdaten wird allgemein erwartet, dass auch die Vorratsdatenrichtlinie aufgehoben wird, weil die EG mit der Richtlinie ihre Kompetenzen überschritten habe. Die mittlerweile regierende große Koalition beschloss gleichwohl, mit einer deutschen Regelung der Richtlinie zu folgen, ohne eine Entscheidung des Europäischen Gerichtshofes abzuwarten.

Das jetzt im Bundestag vorliegende Gesetz ist darüber hinaus auch grundsätzlich umstritten. So hat der Wissenschaftliche Dienst des Bundestags am 3. 8. 2006 ein Rechtsgutachten zur „Zulässigkeit der Vorratsdatenspeicherung nach europäischem und deutschem Recht“

vorgelegt, in dem es heißt: „Es bestehen Bedenken, ob die Richtlinie in der beschlossenen Form mit dem Europarecht vereinbar ist. Dies betrifft zum einen die Wahl der Rechtsgrundlage, zum anderen die Vereinbarkeit mit den im Gemeinschaftsrecht anerkannten Grundrechten.“ Auch im Hinblick auf die deutschen Grundrechte sei „zweifelhaft, dass dem Gesetzgeber aufgrund der europarechtlichen Vorgaben eine verfassungsgemäße Umsetzung gelingen“ könne.

Die Zweifel daran, ob es gerechtfertigt ist, dass der Staat die Daten von allen Telekommunikationsbenutzern auf Vorrat speichern darf, beziehen sich auf zwei grundsätzliche Einwände: Kann sich der Rechtsstaat wie ein Überwachungsstaat organisieren, indem er die Verfügbarkeit aller anfallenden Kommunikationsdaten für eine spätere, noch nicht absehbare Verwendung anordnet, ohne sich damit selbst aufzuheben? Zum anderen müssen wir uns heute fragen, ob ein Grundrechtseingriff dieser Intensität überhaupt zu rechtfertigen ist, bzw. wenn man ihn rechtfertigt, ob dies nicht der Suspendierung des grundrechtlich geschützten Fernmeldegeheimnisses gleichkommt.

Unbestritten greifen gesetzliche Speicherungspflichten für Telekommunikationsverkehrsdaten in die Grundrechte sowohl der Nutzer als auch der Anbieter von Telekommunikationsdiensten ein. Konkret sind hiervon das Fernmeldegeheimnis nach Artikel 10 Abs. 1 des Grundgesetzes (GG) und die Freiheit der Berufsausübung nach Artikel 12 Abs. 1 GG betroffen. Die Abfrage der gespeicherten Daten kann zudem auch die Pressefreiheit nach Artikel 5 Abs. 1 Satz 2 GG berühren. Diese Grundrechte sind für ein freiheitliches demokratisches Gemeinwesen konstitutiv. Die mit der Vorratsdatenspeicherung verbundenen Grundrechtseingriffe sind umso weniger gerechtfertigt, als von ihnen zahlreiche Personen betroffen sein werden, denen kein konkreter Tatvorwurf gemacht werden kann und die mit ihrem eigenen Verhalten keinen Anlass für eine Überwachung ihres Kommunikationsverhaltens gegeben haben.

Die Speicherung der Verkehrsdaten soll die „Ermittlung, Feststellung und Verfolgung von schweren Straftaten“ erleichtern, heißt es in Artikel 1 Absatz 1 der im März 2006 in Kraft getretenen Richtlinie zur Vorratsdatenspeicherung. Doch nicht jeder, der zum Telefon oder Handy greift bzw. den Computer nutzt, kann allein deshalb als potentieller Straftäter behandelt werden. In einer freiheitlichen Demokratie darf die Spurensicherung nur im Verdachtsfall bzw. beim Vorliegen einer konkreten Gefährdung erfolgen. Mit der anlass- und verdachtslosen Speicherung sämtlicher Verbindungsdaten würde praktisch allen Benutzern elektronischer Telekommunikationsmittel unterstellt, sie könnten demnächst zum Objekt staatlicher Strafverfolgung werden. Dieser generelle Verdacht schränkt nicht nur das Recht

auf vertrauliche Kommunikation ein, sondern setzt auch grundlegende Prinzipien des Datenschutzes außer Kraft, etwa die Sparsamkeit und Zweckgebundenheit von staatlich angeordneter Datenspeicherung. Eine verdachtslose „vorbeugende Verbrechensbekämpfung“ bzw. eine „Strafverfolgungsvorsorge“ ist kein legitimer Zweck.

Selbst wenn man die anlass- und verdachtslose Speicherung sämtlicher Verbindungsdaten rechtfertigen könnte, sind die jetzt im deutschen Umsetzungsgesetz vorgesehenen Regelungen unverhältnismäßig. Die europäische Richtlinie wollte die Kommunikationsdaten „nur“ für die Strafverfolgung, genauer gesagt für die Verfolgung *schwerer* Straftaten (Art. 1 Abs. 1 RL 2006/24/EG) zugänglich machen. Der Gesetzentwurf der Bundesregierung sieht bereits eine wesentlich breitere Nutzung der Kommunikationsdaten vor: Die Strafverfolgungsbehörden sollen auf die Verbindungsdaten auch zur Verfolgung von Straftaten des mittleren Kriminalitätsbereichs sowie einfachsten Delikten (sofern sie mittels Telekommunikationsdiensten begangen wurden) zugreifen können. Außerdem ist vorgesehen, dass auch die Nachrichtendienste zum Zwecke der „Gefahrenabwehr“ oder im Rahmen ihrer „Vorfeldermittlungen“ darauf zugreifen dürfen. Nach der Ratifizierung der Cybercrime-Konvention des Europarates kommen eine Vielzahl ausländischer Staaten hinzu, die auf deutsche Telekommunikationsdaten zugreifen können. Damit geht die Vorratsdatenspeicherung in Deutschland bereits jetzt weit über ihren ursprünglichen Anlass, den Kampf gegen den Terrorismus und die Aufklärung schwerer Straftaten, hinaus.

Prof. Dr. Rosemarie Will

lehrt Öffentliches Recht an der Humboldt-Universität zu Berlin und ist Bundesvorsitzende der Bürgerrechtsorganisation Humanistische Union