Kurt Graulich

Vorratsdatenspeicherung – Neustart der Geisterfahrer

Wie man nach der NSA-Affäre noch behaupten kann, die lückenlose Erfassung und Speicherung aller digitalen Kommunikationsvorgänge stelle deren Vertraulichkeit nicht in Frage und die Daten seien bei den Providern sicher gelagert – dies bleibt das Geheimnis der Großen Koalition. Zugleich kann die NSA-Affäre aber helfen bei der Klärung der Frage, warum die Koalition dieses Vorhaben – gegen alle Kritik von den höchsten Gerichten – dennoch stur umsetzen will: Die kontinuierlich anfallenden Datenmassen sind der Rohstoff, auf den die Werkzeuge zur Standortkontrolle, zur Profilbildung und Netzwerkanalyse angewiesen sind. Ohne diese Daten wären Polizei wie Geheimdienste heute blind, beteuern die Befürworter des Instruments immer wieder. Kurt Graulich erinnert noch einmal an die Vorgeschichte der Vorratsdatenspeicherung und untersucht den vorliegenden Gesetzentwurf der Bundesregierung auf seine Schwachstellen.

Zur Überraschung des politischen Publikums hat der Bundesminister für Justiz und Verbraucherschutz, der sich bislang gegen eine nationale Regelung über die Vorratsdatenspeicherung ausgesprochen hatte, am 15. April 2015 zunächst „Leitlinien zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten“ veröffentlicht und genau einen Monat später den „Referentenentwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ nachgelegt. Der ursprüngliche Zeitfahrplan[1] sah eine sehr schnelle Umsetzung bis zur parlamentarischen Sommerpause 2015 Anfang Juli vor, wurde jedoch auf Herbst diesen Jahres verschoben. Dies macht einige Anmerkungen notwendig.

I. Funktion und rechtliche Einordnung von Metadaten der Telekommunikation

Die Telekommunikation ist in technisierten Gesellschaften zu einer der gebräuchlichsten Kommunikationsformen überhaupt geworden. Telefonate, Text-, Sprach- und Bildnachrichten – alles wird heutzutage per Telekommunikation übermittelt. Die E-

Mail ist nicht nur vor den Webseiten des *World Wide Web* der meistgenutzte Dienst des Internet, sie wird auch weitaus häufiger genutzt als der traditionelle Brief, d.h. die Print-Mail. Infolge der Digitalisierung entstehen beim Aussenden, Übermitteln und Empfangen von Fernmeldesignalen technische Daten, die – im Verhältnis zu den beförderten Inhalten – pauschal als Meta-Daten bezeichnet werden. Im Kern handelt es sich um die gesetzlich definierten Verkehrs- sowie die Standortdaten.

Nach § 3 Nr. 30 TKG sind „Verkehrsdaten" Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Zu diesem Zweck darf nach § 96 Abs. 1 Satz 1 TKG der Diensteanbieter folgende Verkehrsdaten erheben: (Nr. 1) die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen auch die Standortdaten, (Nr. 2) den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen, (Nr. 3) den vom Nutzer in Anspruch genommenen Telekommunikationsdienst, (Nr. 4) die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen und (Nr. 5) sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten. Außerdem sind sie vom Diensteanbieter nach Beendigung der Verbindung unverzüglich zu löschen.[2] Es handelt sich bei Verkehrsdaten im Ausgangspunkt also ausschließlich um Informationen für die Bedienung der Geschäftsbeziehung zwischen einem Telekommunikationsdienstleister und seinen Kunden ohne die Beteiligung staatlicher Stellen.

„Standortdaten" sind nach § 3 Nr. 19 TKG Daten, die in einem Telekommunikationsnetz oder von einem Telekommunikationsdienst erhoben oder verwendet werden und die den Standort des Endgeräts eines Endnutzers eines öffentlich zugänglichen Telekommunikationsdienstes angeben. Nach § 98 Abs. 1 Satz 1 TKG dürfen Standortdaten, die in Bezug auf die Nutzer von öffentlichen Telekommunikationsnetzen oder öffentlich zugänglichen Telekommunikationsdiensten verwendet werden, nur im zur Bereitstellung von Diensten erforderlichen Umfang und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der Teilnehmer dem Anbieter des Dienstes seine Einwilligung erteilt hat. Typische Anwendungsfälle sind die Nutzung sog. Zusatzdienste durch mobile Systeme, beispielsweise unter Verwendung von GPS. Sie fallen aber notwendigerweise an durch die Verbindung eines Endgerätes mit dem Sendemast eines TK-Dienstleisters, denn die Kommunikation ist dann der sog. Funkzelle der entsprechenden Sendeeinrichtung zuzuordnen, und jede Funkzelle hat eine Cell-ID. Auch insoweit dienen sie lediglich den Geschäftsbeziehungen zwischen TK-Dienstleister und Kunden ohne hoheitliche Einmischung. Eine Ausnahme macht insoweit lediglich das Notrufregiment nach § 108 TKG.

Für Sicherheitsbehörden sind Verkehrs- und Standortdaten von Interesse, weil sich insbesondere durch ihre Vielzahl aussagekräftige Strukturen und Verläufe von Kommunikationsbeziehungen – ganz unabhängig von den Inhalten – herausarbeiten sowie Bewegungsprofile etwa des Trägers eines Mobiltelefons erstellen lassen. Der Zugriff darauf zählt daher – repressiv – zu den Maßnahmen zur Überwachung des Fern-

meldeverkehrs im Strafverfahren[3] und – präventiv – zu den Maßnahmen der Gefahrenabwehr im Polizeirecht in bestimmten Fällen[4] und zu den Aufklärungsmaßnahmen im Nachrichtendienstrecht[5]. Gegenstand des Zugriffs sind die jeweils beim TK-Dienstleister noch vorhandenen Verkehrs- oder Standortdaten. Dies trifft grundsätzlich weder auf verfassungsrechtliche noch auf rechtspolitische Bedenken, denn für die Aufklärung von Straftaten sowie für die Abwehr von Gefahren oder die nachrichtendienstliche Aufklärung darf nach gesetzlicher Maßgabe auf die verschiedenartigsten Erkenntnismittel zurückgegriffen werden, wenn sie Spuren zu enthalten versprechen, auf Meta-Daten der Telekommunikation ebenso wie auf Tatwerkzeuge, Kontounterlagen, Büroabfälle oder den Hausmüll. Auf Bedenken trifft aber die gesetzliche Verpflichtung zur anlasslosen Speicherung der Verkehrsdaten.

Die Meta-Daten der Telekommunikation sind gegenüber hoheitlichen Eingriffen allerdings verfassungsrechtlich hoch bewertet. Artikel 10 Abs. 1 Grundgesetz (GG) gewährleistet das Telekommunikationsgeheimnis, welches die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs vor einer Kenntnisnahme durch die öffentliche Gewalt schützt. Dieser Schutz erfasst nicht nur die Inhalte der Kommunikation. Geschützt ist vielmehr auch die Vertraulichkeit der näheren Umstände des Kommunikationsvorgangs, zu denen insbesondere gehört, ob, wann und wie oft zwischen welchen Personen oder Telekommunikationseinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist. Der Schutz durch Art. 10 Abs. 1 GG gilt nicht nur dem ersten Zugriff, mit dem die öffentliche Gewalt von Telekommunikationsvorgängen und -inhalten Kenntnis nimmt. Seine Schutzwirkung erstreckt sich auch auf die Informations- und Datenverarbeitungsprozesse, die sich an die Kenntnisnahme von geschützten Kommunikationsvorgängen anschließen, und auf den Gebrauch, der von den erlangten Kenntnissen gemacht wird. Ein Grundrechtseingriff ist jede Kenntnisnahme, Aufzeichnung und Verwertung von Kommunikationsdaten sowie jede Auswertung ihres Inhalts oder sonstige Verwendung durch die öffentliche Gewalt. In der Erfassung von Telekommunikationsdaten, ihrer Speicherung, ihrem Abgleich mit anderen Daten, ihrer Auswertung, ihrer Selektierung zur weiteren Verwendung oder ihrer Übermittlung an Dritte liegen damit je eigene Eingriffe in das Telekommunikationsgeheimnis. Folglich liegt in der Anordnung gegenüber Kommunikationsunternehmen, Telekommunikationsdaten zu erheben, zu speichern und an staatliche Stellen zu übermitteln, jeweils ein Eingriff in Art. 10 Abs. 1 GG.[6]

II. Vorratsdatenspeicherung

Zum Problem geworden ist der Zusammenhang zwischen Telekommunikationsfreiheit und sicherheitsrechtlichen Eingriffen in die Verkehrsdaten, seitdem es unternommen wurde, den potentiellen Eingriffsumfang durch gesetzliche Maßgaben erheblich auszuweiten. Zum wesentlichen Regelungsinstrument wurde die gesetzliche Auflage an die TK-Dienstleister, eine Mindestspeicherdauer für Verkehrs- und Standortdaten einzuhalten, die länger ist als dies für Abrechnungszwecke erforderlich

wäre; die kommerzielle Notwendigkeit der Speicherung hat sich durch die erhebliche Ausweitung von Flatrate-Angeboten zudem immer mehr vermindert.

Die gesetzliche Verpflichtung zur Speicherung von Verkehrsdaten greift massenhaft in das Grundrecht aus Art. 10 Abs. 1 GG ein. Sie wurde in der Absicht eingeführt, eine Datenmenge für eventuelle Sicherheitsmaßnahmen – anlasslos – zu bevorraten, weshalb sich für die gesamte Konstruktion das Sprachbild „Vorratsdatenspeicherung" eingebürgert hat. Der in der Vorratsdatenspeicherung liegende Rechtseingriff in Art. 10 Abs. 1 GG schafft zugleich die Voraussetzungen für potentiell weitere Eingriffe, nämlich den Abruf und die Verarbeitung der Daten durch verschiedene Sicherheitsbehörden. Im Gegensatz zu den unterschiedlichen strafprozessualen, polizei- und nachrichtendienstlichen Erhebungen von Verkehrsdaten erfolgt die Vorratsspeicherung ohne Anlass, also ohne dass ein Anfangsverdacht, eine wie auch immer geartete polizeiliche Gefahr oder tatsächliche Anhaltspunkte für ein nachrichtendienstliches Tätigwerden vorliegen. Es handelt sich also um ein typisches Produkt präventionsstaatlichen Denkens.

Ein solcher Vorgang ist beispiellos. In der reichhaltigen Geschichte deutscher Sicherheitsorganisationen im 20. Jahrhundert ist es bislang nie unternommen worden, tatsächlich vom gesamten Postverkehr Absender und Empfänger festzuhalten. Selbst während des Zweiten Weltkriegs beschränkte sich die Kontrolle der Feldpost auf Stichproben. Demgegenüber bedeutet die Vorratsdatenspeicherung die zeitlich befristete und staatlich veranlasste Bevorratung sämtlicher Telekommunikationsnummern und somit die Erfassung sämtlicher Absender und Empfänger im Bereich der Telekommunikation. Diese bilden sich zwar zunächst nur als technische Daten der die Kommunikation tragenden Geräte ab. Mit einem weiteren Schritt, nämlich der Bestandsdatenauskunft,[7] können die dahinter stehenden Inhaber der Anschlüsse aber deanonymisiert werden. Die Bestandsdatenauskunft greift dann wiederum in das Grundrecht auf informationelle Selbstbestimmung[8] ein.[9]

Der rechtspolitische Streit um die Vorratsdatenspeicherung weist wie in einem breit angelegten Drama Elemente von Verletzungen, Enttäuschungen, Listen, funktionellen Verlagerungen der Konflikte sowie Siegen und Niederlagen auf und wird von anscheinend unerschöpflichen Energien an Durchsetzungswillen gespeist. Die nachfolgende summarische Beschreibung der Streitstationen ist nützlich, um den aktuellen Ort der Auseinandersetzung zu verstehen.

In der Europäischen Union gab es im Anschluss an die terroristischen Anschläge von Madrid (11.03.2004) und London (07.07.2005) insbesondere seitens der Regierungen von Frankreich, Schweden, Irland und Großbritannien Anstrengungen zur europaweiten Einführung einer Vorratsdatenspeicherung. Allerdings blieb die Frage der formellen unionsrechtlichen Umsetzung – nämlich Rahmenbeschluss des Rats oder Richtlinie durch das EU-Parlament – umstritten.

Der 15. Deutsche Bundestag – es war noch die Zeit der Rot/Grünen Koalition unter Gerhard Schröder – lehnte in einem am 17. Februar 2005 fraktionsübergreifend gefassten Beschluss die geplante Mindestspeicherfrist und damit eine Speicherung von Verkehrsdaten auf Vorrat ausdrücklich ab. Er forderte die Bundesregierung auf, diesen Beschluss auch auf EU-Ebene mit zu tragen. Davon unbeeindruckt agierten deut-

sche Regierungsvertreter und EU-Parlamentarier im Zusammenwirken mit den Vertretern anderer Mitgliedsländer gegenläufig.

Nach einem mehrmonatigen Streit über den richtigen Verfahrensweg stimmte am 14. Dezember 2005 das Europaparlament mit 378 zu 197 Stimmen für die Richtlinie zur unionsweiten Einführung der Vorratsdatenspeicherung. Am 21. Februar 2006 stimmte der Europäische Rat – ohne weitere Aussprache – durch die Innen- und Justizminister ebenfalls mehrheitlich für die Richtlinie; lediglich die Vertreter Irlands und der Slowakei stimmten dagegen. Die Frist für die Umsetzung der Richtlinie über die Vorratsdatenspeicherung[10] lief gemäß Artikel 15 Absatz 1 der Richtlinie am 15. September 2007 ab, durfte allerdings für die Dienste Internetzugang, Internet-Telefonie und E-Mail bis längstens zum 15. März 2009 aufgeschoben werden. Hierzu war eine besondere Erklärung der Mitgliedsstaaten notwendig. Eine solche Erklärung haben 16 der 25 Mitgliedsstaaten abgegeben, darunter Deutschland und Österreich.

Fast auf den Tag genau ein Jahr nach seinem ersten Beschluss– der Bundestag war neu gewählt worden, nunmehr regierte das erste Kabinett von Angela Merkel – gab der 16. Deutsche Bundestag am 16. Februar 2006 seine frühere Position auf und forderte die Bundesregierung auf, den sog. Kompromissvorschlag für eine EG-Richtlinie zur Vorratsdatenspeicherung im Rat der Europäischen Union zu unterstützen. Der Beschluss wurde mit den Stimmen der Großen Koalition gegen die Stimmen von FDP, Linkspartei und Bündnis 90/Die Grünen gefasst.

Die Bundesregierung legte daraufhin – unter Federführung des Wirtschaftsministeriums – den Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung vor,[11] der im Wesentlichen die eigentliche Vorratsspeicherung in §§ 113a und 113b TKG enthielt, darüber hinaus aber auch strafprozessuale Eingriffsbefugnisse in der StPO. Aus ihm wurde das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007[12], das am 1. Januar 2008 in Kraft getreten ist. Die deutschen Bundesländer folgten mit jeweils eigenen Regelungen.

Mit Urteil vom 10. Februar 2009 wies der Europäische Gerichtshof die Nichtigkeitsklage Irlands gemäß Art. 230 EGV ab,[13] die sich darauf gestützt hatte, dass vorherrschender Zweck der Richtlinie die Erleichterung der Verfolgung von Straftaten sei und deshalb als Rechtsgrundlagen nur die Einstimmigkeit voraussetzenden Regelungen des EU-Vertrages alte Fassung über die polizeiliche und justizielle Zusammenarbeit, insbesondere Art. 30, Art. 31 Abs. 1 Buchstabe c und Art. 34 Abs. 2 Buchstabe b EUV a.F. in Betracht kämen.[14] Dabei stellte der Gerichtshof ausdrücklich klar, dass die Entscheidung nicht eine etwaige Verletzung von Gemeinschaftsgrundrechten zum Gegenstand habe.[15]

Das Bundesverfassungsgericht erklärte auf mehrere Verfassungsbeschwerden hin u.a. die §§ 113a und 113b TKG für nichtig.[16] Das gesetzgeberische Vorhaben einer Vorratsdatenspeicherung in Deutschland sah es jedoch prinzipiell als verfassungskonform an. Nach den Erwägungen des Gerichts müsse eine solche Datenspeicherung lediglich nach dem Grundsatz der Verhältnismäßigkeit ausgestaltet werden, um dem besonderen Gewicht des damit verbundenen Grundrechtseingriffs angemessen Rechnung zu tragen. Erforderlich seien hinreichend anspruchsvolle und normenklare Re-

gelungen hinsichtlich der Datensicherheit, der Datenverwendung, der Transparenz und des Rechtsschutzes.

Mit dem Urteil geriet die Bundesrepublik Deutschland in Umsetzungsverzug gegenüber der Europäischen Richtlinie. Dennoch starteten Bundesregierung und Große Koalition zunächst keine gesetzliche Initiative. CDU und CSU traten politisch eher für eine Umsetzung der Richtlinie ein. Die SPD beförderte die Position mit etwas weniger Nachdruck, zielte aus Verhältnismäßigkeitsgründen auf kürzere Speicherfristen und stützte sich etwas mehr auf den Umsetzungsdruck der EU-Richtlinie. Der Koalitionsvertrag von CDU, CSU und SPD für die 18. Legislaturperiode enthält dementsprechend die Formulierung:

> *„Wir werden die EU-Richtlinie über den Abruf und die Nutzung von Telekommunikationsverbindungsdaten umsetzen. Dadurch vermeiden wir die Verhängung von Zwangsgeldern durch den EuGH. Dabei soll ein Zugriff auf die gespeicherten Daten nur bei schweren Straftaten und nach Genehmigung durch einen Richter sowie zur Abwehr akuter Gefahren für Leib und Leben erfolgen. Die Speicherung der deutschen Telekommunikationsverbindungsdaten, die abgerufen und genutzt werden sollen, haben die Telekommunikationsunternehmen auf Servern in Deutschland vorzunehmen. Auf EU-Ebene werden wir auf eine Verkürzung der Speicherfrist auf drei Monate hinwirken".*

Der Bezug auf die EU-Richtlinie ging indes dadurch verloren, dass der EuGH auf Vorlagen des Irischen High Court`s und des Österreichischen Verfassungsgerichtshofs mit Urteil vom 08. April 2014[17] diese Richtlinie für ungültig erklärte. Der Gerichtshof sah in der Verpflichtung zur Vorratsspeicherung von Verkehrsdaten und der Gestattung des Zugangs der zuständigen nationalen Behörden zu ihnen einen besonders schwerwiegenden Eingriff in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, erklärte die EU-Richtlinie (und nicht allein nationale Umsetzungsgesetze) für grundrechtswidrig und ging in seinem – allerdings auf unionsrechtliche Grundrechtserwägungen gestützten – Verdikt weiter als zuvor das BVerfG, das noch eine wenn auch stark eingeschränkte gesetzliche Realisierungsmöglichkeit offen gehalten hatte. Mit dem EuGH-Urteil entfiel der Umsetzungszwang durch nationales Recht; für diesen Fall enthielt der Koalitionsvertrag zur 18. Wahlperiode keine explizite Aussage.

Dessen ungeachtet hielten CDU/CSU an ihrer Forderung nach Wiedereinführung der nationalrechtlichen Vorratsdatenspeicherung fest. Der SPD-Bundesvorsitzende und Bundeswirtschaftsminister Sigmar Gabriel griff Mitte März 2015 – im Nachgang zu Attentaten in Paris und Dänemark – dieses Drängen auf und im April bzw. Mail 2015 legte der – politisch zuvor anders argumentierende – Bundesjustizminister Heiko Maas die bereits erwähnten Leitlinien bzw. den Referentenentwurf vor. Bemerkenswert ist, dass die Federführung für das Projekt nicht in dem von Gabriel geleiteten Wirtschaftsministerium liegt, sondern in dem von Maas geleiteten Justizressort, obwohl der Regelungsschwerpunkt weiterhin im Telekommunikationsrecht liegt und

nicht in klassischen Justizmaterien. Damit wird möglicherweise die politische Reputationslast umverteilt.

III. Anmerkungen zum „Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“

In seinem Buch „Warum Strafe sein muss“ hat Winfried Hassemer Nutzen und Risiko des Präventionsstaates durchdacht. Darin findet sich folgende Beobachtung: Nicht mehr die Angemessenheit, die Gerechtigkeit von Sanktionen beschäftige unsere Phantasie und steuere unser Handeln, sondern die Aussicht, unser Leben auch mit Hilfe des Strafrechts sicherer zu machen und die Risiken krimineller Übergriff verlässlicher zu beherrschen. Unser Kontrollbedürfnis entwickele sich gleichsinnig mit den rasanten Fortschritten der modernen Informationstechnologie und den Möglichkeiten, in Bereiche einzudringen, die einem informationellen Zugriff bisher einfach faktisch verschlossen gewesen seien. In diesem Klima gedeihe ein „Grundrecht auf Sicherheit“ – ein Geisterfahrer, der so tue als bewege er sich in derselben Richtung wie die anderen Grundrechte, die Abwehrrechte gegen Eingriffe des Leviathan in die bürgerliche Freiheit sind. Genau das Gegenteil sei aber der Fall.[18]

1. Systematische Einordnung des Referentenentwurfs des BMJuV vom 15. Mai 2015 eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

Wer Sicherheitsbehörden nach deutschem Recht Verkehrsdaten zur Verfügung stellen will, muss auf zwei legislativen Ebenen ansetzen, so wie es das Bundesverfassungsgericht deutlicher als in seiner Entscheidung über die Vorratsdatenspeicherung im Jahr 2010 zu Art. 10 Abs. 1 GG zwei Jahre später (2012) in derjenigen zur Bestandsdatenauskunft zum informationellen Selbstbestimmungsrecht[19] erklärt und bildhaft als Doppeltüren-Modell beschrieben hat.[20] Das Telekommunikationsrecht trifft in diesem Zusammenhang typischerweise die gesetzliche Ebene von Erhebung, Speicherung und Verwendung von Daten, insbesondere auch ihre Übermittlung, während die Ebene von Befugnissen zur Abfrage in den Sicherheitsgesetzen zum Strafprozess, Polizei- und Nachrichtendienstrecht ausgefüllt wird. Der am 15. Mai 2015 vorgelegte Referentenentwurf, der das Wort „Vorratsdatenspeicherung“ peinlich vermeidet,[21] ist insofern nur die Hälfte des gesamten Regelungszusammenhangs, weil die Befugnisnormen für die Abfrage der Verkehrsdaten längst in § 100g StPO, § 20 m BKAG, § 8a Abs. 2 Nr. 4 BVerfSchG sowie den einschlägigen Normen des Landesrechts vorhanden sind. Wer die Wirkungsmacht des Referentenentwurfs vollständig begreifen will, muss sich diese Regelungen immer hinzudenken.

Dies vorausgeschickt wird klar, weshalb der Referentenentwurf überwiegend das TKG betrifft mit – z.T. nur noch ergänzenden – Regelungen zur Speicherung (§ 113b

TKG-E) und der Verwendung (§ 113c TKG-E) von Verkehrsdaten. Weitere Regelungen über Begriffliches und den Umgang mit Verkehrsdaten sind in §§ 96 und 97 TKG und über Standortdaten in § 98 TKG bereits enthalten. An bundesrechtlichen Befugnisnormen für die Abfrage von Verkehrsdaten wird lediglich § 100g StPO für eine Neuregelung vorgesehen und zur Besänftigung die Regelung des § 101a TKG-E über Gerichtliche Entscheidung, Datenkennzeichnung und -auswertung, Benachrichtigungspflichten bei der Erhebung von Verkehrsdaten angekündigt; der Rest ist ohne besonderes Gewicht.

2. Die beabsichtigte Änderung des TKG

Nach eigenem Bekunden strebt der Referentenentwurf eine Regelung zur zeitlich befristeten Speicherung von Verkehrsdaten zur Strafverfolgungsvorsorge und zur Gefahrenabwehr an. Dies soll dadurch geschehen, dass zwar eine Pflicht der Telekommunikationsanbieter vorgesehen wird, im Einzelnen bezeichnete Verkehrsdaten für eine beschränkte Zeit zu speichern, die Erhebung der Daten durch staatliche Stellen aber nur unter sehr engen Voraussetzungen ermöglicht wird. Die Eingriffsintensität werde durch ein deutlich reduziertes Datenvolumen (keine verpflichtende Speicherung von E-Mail-Daten) und eine deutlich kürzere Speicherfrist (vier bzw. zehn Wochen) im Vergleich zur vorhergehenden Regelung verringert.[22] Irreführend ist der Wirkungsrahmen des Entwurfs beschrieben, weil die Regelungen über den Abruf der Daten zu Zwecken der Strafverfolgung und Gefahrenabwehr sowie für nachrichtendienstliche Belange bereits weitgehend vorhanden sind.

Notwendig ist aber ein sorgfältiger Blick auf einige der neuen telekommunikationsrechtlichen Regelungen in den §§ 113a ff. TKG-E. In § 113b TKG-E wird die Speicherung von genau bezeichneten Verkehrsdaten angeordnet. Dabei wird hinsichtlich der Speicherdauer differenziert. Während die Verbindungsdaten für zehn Wochen zu speichern sind, ist die Frist bei den besonders sensiblen Standortdaten auf vier Wochen beschränkt.[23] Die Vorschrift des § 113b TKG-E dient als Kernregelung der Umsetzung der Vorgaben der Entscheidungen des Bundesverfassungsgerichts und des Gerichtshofes der Europäischen Union, indem sie die Adressaten sowie die Grundvoraussetzungen der Speicherungspflichten bestimmt, die zu speichernden Datenkategorien sowie die Speicherungsfrist festlegt und Vorgaben macht, wie die Speicherung der Daten und deren Löschung zu erfolgen haben.[24]

a) Pflichtige Dienstleister

Bei staatlichen Eingriffen in die Telekommunikation entsteht ein rechtliches Dreiecksverhältnis, denn der Sicherheitsbehörde steht nicht einfach der mit der Maßnahme Adressierte gegenüber, sondern zusätzlich der jeweilige Dienstleister als technischer Organisator, der auch die zu bevorratenden Daten speichern muss. Dementsprechend nennt § 113a Abs. 1 Satz 1 TKG als Pflichtigen der Vorratsdatenspeicherung den „Erbringer öffentlich zugänglicher Telekommunikationsdienste“. Das TKG selbst definiert den Begriff in § 3 Nr. 17a in zirkulärer Weise – „öffentlich zugängliche Telekommunikationsdienste“ seien der Öffentlichkeit zur Verfügung stehende Telekommuni-

kationsdienste. Der Branchenverband BITKOM hat in einer ersten Stellungnahme erheblichen Präzisierungsbedarf zur Bestimmung des Adressatenkreises angemahnt.[25]

Der neue Entwurf zur Vorratsdatenspeicherung sieht in § 113b Abs. 3 TKG-E vor, dass „gewerbsmäßige Anbieter" von Internetzugangsdiensten nicht nur die IP-Adressen protokollieren, die sie ihren Kunden zugeteilt haben, sondern nun auch eine „zugewiesene Benutzerkennung" erfassen. Diese Formulierung ist undeutlich und verlangt möglicherweise eine Speicherung der Port-Nummern, die die Nutzer jeweils für den Abruf von Internet-Daten verwenden. Grund für die beabsichtigte Regelung dürfte sein, dass bisher Strafverfolger nicht alle Nutzer allein anhand der von Netzbetreibern gespeicherten IP-Adressen identifizieren können. Dies hängt mit der Knappheit der Internet-Protokolladressen der Protokollversion IPv4 zusammen, weshalb Provider die Adressen mehrfach vergeben. Wollen nun aber Ermittler herausfinden, wer für einen inkriminierenden Download verantwortlich war, hätten sie nach dem bisherigen Verständnis der Vorratsdatenspeicherung bei IPv4-Verkehr lediglich die öffentliche IPv4-Adresse eines Netzbetreiber-Routers und müssten dann noch anderweitig ermitteln, über welchen der dahinter liegenden Kundenanschlüsse die fragliche Datei geladen wurde. Hier käme nun die „zugewiesene Benutzerkennung" zum Tragen: Ein Anschluss ist nur dann eindeutig zu identifizieren, wenn neben der IP-Adresse des Netzbetreiber-Routers auch die Port-Nummer bekannt ist, die dieser Router für bestimmte Dienste einem Anschluss zugewiesen hat. In diesem Zusammenhang wird eine erhebliche Ausweitung der gespeicherten Datenmenge befürchtet.[26]

b) Speicherfrist für Verkehrsdaten

Nach § 113b Abs. 1 i.V.m. Abs. 2 TKG-E sind Verkehrsdaten für zehn Wochen im Inland zu speichern. Abweichend von § 113a TKG a. F. sind die Daten ausschließlich im Inland zu speichern; eine Erfüllung der Speicherpflicht durch die Speicherung in einem anderen Mitgliedstaat der Europäischen Union ist nicht mehr vorgesehen. Die Beschränkung der Speicherung der Vorratsdaten auf das Inland ist eine Beschränkung der Dienstleistungsfreiheit im Sinne von Artikel 56 AEUV. Eine solche lässt sich rechtfertigen, wenn sie notwendig ist, um zwingenden Gründen des Allgemeininteresses gerecht zu werden, und wenn sie zudem verhältnismäßig ist. Diese Voraussetzungen liegen nach Ansicht des Referentenentwurfs vor. Eine Beschränkung auf das Inland sei notwendig, um die grundrechtlichen Erfordernisse des Datenschutzes und der Datensicherheit zu gewährleisten, die gespeicherten Vorratsdaten wirksam vor Missbrauch sowie vor jedem unberechtigten Zugang und jeder unberechtigten Nutzung zu schützen und das durch eine unabhängige Stelle zeitnah und effizient überwachen zu können.[27]

Die Speicherdauer von zehn Wochen überzeugt weder dem Grund noch der Dauer nach. Die Verkehrsdaten der Telekommunikation eines gesamten Landes mit 80 Millionen Einwohnern werden anlasslos für zehn Wochen gespeichert, und zwar fortwährend. Diese gesetzliche Anordnung ist bereits dem Grunde nach unverhältnismäßig, und sie wird es nicht dadurch weniger, dass die Vorgängerregelung in § 113a TKG a.F. eine Speicherdauer von 6 Monaten vorsah. Keine der durchgeführten Untersuchungen zur Notwendigkeit der Vorratsdatenspeicherung hat einen messbaren Sinn für die Strafverfolgung oder Gefahrenabwehr erbracht. Die vielfach bemühten Beispiele

terroristischer Anschläge in Norwegen, London, Madrid oder Paris sind weder durch die Vorratsdatenspeicherung verhindert noch aufgeklärt worden. Ihre nachträgliche Aufarbeitung war Frucht traditioneller Polizeiarbeit. Die zeitnahe Erhebung von Verkehrsdaten gelingt auch ohne staatliche Bevorratung, weil die Daten noch für Tage und Wochen aus betriebswirtschaftlichen Gründen in den Systemen der TK-Dienstleister verbleiben. Die Speicherpflicht im Inland erhöht die Wirksamkeit des nationalen Gesetzesregimes.[28]

§ 113b Abs. 2 Satz 1 TKG-E regelt die einzelnen Speicherpflichten für Erbringer öffentlich zugänglicher Telefondienste und umfasst Ausprägungen wie Festnetz, Mobilfunk und Internettelefonie. Satz 2 stellt klar, dass diese Speicherpflichten bei der Übermittlung von Kurznachrichten (SMS), Multimedianachrichten (MMS) und ähnlichen Nachrichten (zum Beispiel EMS) entsprechend gelten, wobei sich die zu speichernden Zeitangaben mangels bestehender Verbindung auf die Versendung und den Empfang der Nachricht beziehen. Satz 3 erstreckt die Speicherpflicht auf unbeantwortete (das heißt nicht entgegengenommene) oder wegen eines Eingriffs des Netzwerkmanagements erfolglose Anrufe, soweit der Telefonieerbringer die entsprechenden Verkehrsdaten für die in § 96 Absatz 1 Satz 2 genannten Zwecke speichert oder protokolliert. Mit dieser, dem § 113a Absatz 5 TKG a. F. entsprechenden Regelung, werden beispielsweise Fälle erfasst, in denen ein Teilnehmer von seinem Diensteanbieter per Kurznachricht darüber informiert wird, dass ein für seinen Anschluss bestimmter Anruf nicht entgegengenommen wurde, weil etwa der Anschluss belegt war oder sich das Mobiltelefon zur Zeit des Anrufs außerhalb des Versorgungsbereichs einer Funkzelle befand.[29] Die Regelung bemüht sich um Detailgenauigkeit, überzeugt deshalb aber auch nicht hinsichtlich der Verhältnismäßigkeitsanforderung.

c) Speicherfrist für Standortdaten

Standortdaten sollen nach § 113b Abs. 1 i.V.m. Abs. 4 TKG-E für vier Wochen gespeichert werden dürfen. Nach der Begründung im Referentenentwurf entspricht dies dem Gebot einer möglichst grundrechtsschonenden Regelung. Diese Speicherdauer sei ausreichend, um in der weitaus überwiegenden Anzahl von Ersuchen eine Verfügbarkeit der maßgeblichen Daten sicherzustellen.[30] Zur Erläuterung des dahinter stehenden technischen Sachverhalts wird ausgeführt, bei der Nutzung von öffentlich zugänglichen Internetzugangsdiensten durch Mobilfunk werde die Bezeichnung der Funkzelle gespeichert, die bei Beginn der Internetverbindung genutzt wird. Absatz 4 Satz 3 bestimmt zudem, dass auch die Daten vorzuhalten sind, aus denen sich die geographische Lage und die Hauptstrahlrichtung der die jeweilige Funkzelle versorgenden Funkantennen ergeben. Diese § 113a Absatz 7 TKG a. F. aufgreifende Regelung betrifft Angaben zur Netzplanung der Mobilfunknetzbetreiber, regelt also nicht die Speicherung von Verkehrsdaten.[31] Die Speicherung von Standortdaten übersteigt das Programm der ursprünglichen Vorratsdatenspeicherung, die sich auf die eigentlichen Verkehrsdaten beschränkte. Die Auswertung von Standortdaten lässt die Erstellung von Bewegungsprofilen zu und enthält wichtige Momente der vom Bundesverfassungsgericht inkriminierten Totalüberwachung.[32] Das Bewegungsprofil ist aber nicht Ergebnis einer Observation, sondern einer Form von staatlich instrumentalisierter

„Selbstüberwachung“ mit Hilfe des eigenen Mobilfunkgerätes. Dies widerspricht dem allgemeinen rechtsstaatlichen Grundsatz, dass niemand sich selbst belasten muss.

d) Verwendung für Gefahrenabwehr nach Landespolizeirecht
Unverständlich und offensichtlich unverhältnismäßig ist die vorgesehene Regelung in § 113c Abs. 1 Nr. 2 TKG-E. Danach sollen die nach § 113b TKG-E gespeicherten Verkehrs- und Standortdaten an eine Gefahrenabwehrbehörde der Länder übermittelt werden dürfen, soweit diese die in § 113b genannten Daten gesetzlich erheben bzw. nutzen dürfen und sofern es zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes notwendig ist. Es ist kaum vorstellbar, welche konkrete Gefahr aufgrund wochenlang gespeicherter Verkehrsdaten wirksam bekämpft werden soll. Soweit es um solche Daten geht, die aktuell entstanden sind, sind bereits bereichsspezifische Regelungen im TKG vorhanden, etwa die Notrufregelung nach § 108 TKG.

3. Die beabsichtigten Änderungen im Strafrecht und Strafprozessrecht

Eine mehr als zwei Textseiten lange Regelung in § 100g StPO (Erhebung von Verkehrsdaten) kann als wahres Verweisungsmonster bezeichnet werden, das damit die Grenze zur Unverständlichkeit überschreitet. Eine der zentralen Eingriffsbefugnisse für den Zugriff auf die vorrätig gespeicherten Verkehrs- und Standortdaten verschleiert sich durch Bezugnahmen auf zahllose andere Gesetze und Rechtsvorschriften. Hinzu kommt, dass die Reichweite der Vorschrift nicht zu überschauen ist. Die pauschale Befugnis zur Erhebung von Verkehrsdaten betrifft potentiell nicht nur die nach §§ 113a ff. TKG-E auf Vorrat gespeicherten, sondern auch andere wie z.B. aus Gründen der IT-Sicherheit gespeicherte Daten.[33]

Auf eine andere Weise verschleiernd wirkt der nach § 101a StPO-E vorgesehene Richtervorbehalt bei der Abfrage von Vorratsdaten. Der Richtervorbehalt gilt nur im Strafverfahren für Abfragen nach § 100g StPO-E, nicht aber für sonstige polizeiliche Abfragen (nach dem Gefahrenabwehrrecht) oder geheimdienstliche Auskunftsverlangen. Die rechtlich Betroffenen werden sich umso mehr durch dutzende von Einzelgesetzen arbeiten müssen, um zu festzustellen, ob der Richtervorbehalt auch wirklich von den Gesetzgebern in Bund und Ländern eingehalten wird.

4. Verhältnismäßigkeit des Gesetzesentwurfs insgesamt

Der vorgelegte Referentenentwurf für eine Vorratsdatenspeicherung erscheint wie der verfassungspolitische Versuch eines Rückspiels nach zwei vernichtenden Niederlagen in einem nationalen und einem europäischen Hinspiel. Die taktische Aufstellung für dieses Spiel folgt einem einfachen Muster: Man wiederholt das Meiste (aber etwas kleiner) und psalmodiert dabei fortwährend die Spielkritik in Gestalt der Entscheidungen des Bundesverfassungsgerichts und des Europäischen Gerichtshofs. Am Erfolg dieser Vorgehensweise bestehen Zweifel. Sie erinnert ein wenig an den Geldscheinfäl-

scher in DM-Zeiten, der auf die Druckplatte die ihm selbst geltende Strafdrohung gravieren musste: „Wer Geld in der Absicht nachmacht …“.

Zur Verhältnismäßigkeit eines Gesetzes, das in Grundrechte eingreift, gehört seine Erforderlichkeit. Nach fünf Jahren ohne Vorratsdatenspeicherung muss der Gesetzgeber dartun, welche Schutzlücken nach der Aufhebungsentscheidung durch das Bundesverfassungsgericht im Jahr 2010 überhaupt entstanden sind.[34] Außer einer Bezugnahme auf das aus der Rechtsprechung des Bundesverfassungsgerichts abgeleitete „verfassungsrechtliche Gebot einer effektiven Strafverfolgung“[35] finden sich im Referentenentwurf dazu keine Angaben.

Der in einer anlasslosen Speicherung von Telekommunikationsverkehrsdaten liegende Eingriff ist nach dem Bundesverfassungsgericht nur dann verhältnismäßig i.e.S., wenn er besonderen Anforderungen an die Datensicherheit, an den Umfang der Datenverwendung, an die Transparenz und an den Rechtsschutz genügt.[36] Die katastrophalen Erkenntnisse über die Ausspähung von Datenbeständen durch ausländische Nachrichtendienste sowie nichtstaatliche Hacker begründen Zweifel, ob die nunmehr durch Gesetz unternommene Anlegung einer riesigen Menge von Telekommunikationsdaten überhaupt wirksam vor unbefugten Zugriffen geschützt werden können.

Zweifel bestehen aber auch an der Eignung der miniaturisierten Vorratsspeicherung zur Zweckerreichung: Mit einer Speicherdauer von vier Wochen für Standortdaten und 10 Wochen für Verkehrsdaten werden Höchstfristen bestimmt, welche die aus betrieblichen Gründen beobachtbaren Speicherzeiten bei den TK-Dienstleistern nicht wesentlich, wenn überhaupt übersteigen. Allerdings beruhen die betriebsbedingten Speicherzeiten auf Grundlage der Freiwilligkeit im Rechtsverhältnis zwischen Kunden und Unternehmen. Der gesetzliche Eingriff versteinert diese Rechtsbeziehung, und darin liegt ein rechtfertigungsbedürftiger Vorgang, sonst ist die Maßnahme unverhältnismäßig. Die rechtfertigende Begründung bleibt der Entwurf schuldig und wartet stattdessen mit fatalistische Hingabe, ob am Ende der allfälligen Verfassungsbeschwerde „Karlsruhe“ das Gesetz wohl passieren lassen wird oder nicht. Eine Politik ist einem freiheitlichen Rechtsstaat nicht angemessen, die ihre Macht dazu nutzt, das Datennetz solange enger zu schneidern, bis es in die Substanz einschneidet.

5. Zeitpunkt des Inkrafttretens des beabsichtigten Gesetzes und Verfassungsbeschwerden

Als Kuriosum des Gesetzgebungsverfahrens darf im Übrigen gelten, dass es in übertriebener Eile durch sämtliche Gesetzesinstanzen gebracht werden,[37] aber erst 18 Monate später in Kraft treten soll. Denn § 150 Abs. 13 TKG-E bestimmt zum Inkrafttreten der Vorratsdatenspeicherung:

> *„(13) Die Speicherverpflichtung und die damit verbundenen Verpflichtungen nach den §§ 113b bis 113e und 113g sind spätestens ab dem … [einsetzen: Datum des ersten Tages des 19. auf die Verkündung dieses Gesetzes folgenden Kalendermonats] zu erfüllen. Die Bundesnetzagentur veröffentlicht den nach § 113f Absatz 1 zu erstellenden Anforde-*

rungskatalog spätestens am … [einsetzen: Datum des ersten Tages des 13. auf die Verkündung dieses Gesetzes folgenden Kalendermonats."

Die Frist zur Einlegung der Verfassungsbeschwerde gegen ein Gesetz beträgt gem. § 93 Abs. 3 BVerfGG ein Jahr seit dem Inkrafttreten. Gegen das Gesetz muss nach seiner parlamentarischen Verabschiedung also nicht nur mit sofortiger Wirkung, sondern auch vorbeugend geklagt werden, denn die Belastung durch §§ 113b ff. TKG-E treten ja nach dieser Konzeption erst ein, nachdem die Frist zum Einreichen der Verfassungsbeschwerde bereits verstrichen ist.[38]

DR. KURT GRAULICH Jahrgang 1949, studierte Rechtswissenschaften in Frankfurt am Main und war anschließend als Staatsanwalt in Darmstadt, als Richter am Verwaltungsgericht Frankfurt am Main und zeitweilig am Verwaltungsgerichtshof Kassel tätig. Er promovierte 1983 an der Universität Frankfurt und wurde im Dezember 1991 als Leitender Ministerialrat an das Hessische Ministerium der Justiz versetzt. 1999 wurde er zum Richter am Bundesverwaltungsgericht ernannt, wo er bis zu seiner Pensionierung (Anfang 2015) dem 6. Senat angehörte. Er war dort mit Fragen der Wehrpflicht, des Polizei- und Ordnungsrechts, dem Recht der Nachrichtendienste sowie mit Presse- und Rundfunkrecht befasst. Graulich weist zahlreiche Veröffentlichungen zum Sicherheitsrecht des Bundes und zum Telekommunikationsrecht vor und lehrt an der Humboldt Universität zu Berlin. Im Juli 2015 wurde er von der Bundesregierung zur Sachverständigen Vertrauensperson in der NSA-Affäre ernannt.

Anmerkungen:

1 Der ursprüngliche Zeitplan sah vor:
27. Mai: Beschluss der Bundesregierung
09. Juni: Beschluss und Einbringung der Fraktionen
11. oder 12. Juni: Erste Lesung im Bundestag
17. Juni: Beratung und Anhörung der zuständigen Ausschüsse, wahrscheinlich nur Rechtsausschuss
02. oder 03. Juli: Zweite und Dritte Lesung im Bundestag.
2 Vgl. § 96 Abs. 1 Satz 3 TKG.
3 Vgl. § 100g StPO.
4 Z.B. § 20m BKAG, § 23g ZfdG.
5 Z.B. § 8a Abs. 2 Satz 1 Nr. 4 BVerfSchG, § 2a BNDG, § 4a MADG.
6 BVerfG, Urteil vom 02. März 2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 –, BVerfGE 125, 260-385, Rn. 190.
7 Vgl. §§ 112 und 113 TKG.

8 Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG.
9 Vgl. im Einzelnen BVerfG, Beschluss vom 24. Januar 2012 – 1 BvR 1299/05 –, BVerfGE 130, 151-212, Rn. 124.
10 Richtlinie 2006/24/EG.
11 Vgl. BT-Drs 16/5846.
12 BGBl I S. 3198.
13 Vgl. EuGH, Urteil vom 10. Februar 2009 – Rs. C-301/06.
14 Vgl. Klage vom 6. Juli 2006 - Rs. C-301/06 -, ABl C 237 vom 30. September 2006, S. 5.
15 Vgl. EuGH, Urteil vom 10. Februar 2009 - Rs. C-301/06 -, Rn. 57.
16 BVerfG, Urteil vom 02. März 2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 –, BVerfGE 125, 260-385.
17 Urteil in den verbundenen Rechtssachen C-293/12 und C-594/12 Digital Rights Ireland und Seitlinger u.a.
18 Hassemer, Warum Strafe sein muss, S. 74 ff.
19 Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG.
20 BVerfG, Beschluss vom 24. Januar 2012 – 1 BvR 1299/05 –, BVerfGE 130, 151-212, Rn. 123.
21 Vgl. dazu Kremer, Vorratsdatenspeicherung: Gefährliche Eile, am 20.05.2015 in www.netzpiloten.de.
22 S. Referentenentwurf, S. 2.
23 A.a.O., S. 29.
24 A.a.O., S. 41.
25 Stellungnahme vom 22.05.2015.
26 Krempl in heise online. 24.05.2015.
27 S. Referentenentwurf, S. 41.
28 A.a.O., S. 41 ff.
29 A.a.O., S. 42.
30 A.a.O., S. 41.
31 A.a.O., S. 43.
32 BVerfG, Urteil vom 12. April 2005 – 2 BvR 581/01 –, BVerfGE 112, 304-321.
33 Vgl. § 100 TKG-E nach IT-SicherheitsG-E in BT-Drs. 18/4096, S. 35 sowie den Beitrag von Hügel in diesem Heft.
34 Vgl. Peter Schaar, Verfassungs- und europarechtliche Bedenken gegen Gesetzesentwurf zur Vorratsdatenspeicherung am 24.05.2015 in TELEPOLIS, http://www.heise.de/tp/.
35 Der Referentenentwurf, S. 1 verweist auf BVerfGE 129, 208 (260) m.w.N.
36 BVerfG, Urteil vom 02. März 2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 –, BVerfGE 125, 260-385, Rn. 221.
37 Kremer, a.a.O. (Anm. 21).
38 Vgl. Starostik, Der Referentenentwurf zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten gemessen an der Rechtsprechung des BVerfG und des EuGH, S. 11 – abrufbar unter http://www.starostik.de.