ALEXANDER DIX / DENNIS-KENJI KIPKER / PETER SCHAAR

Schnellschuss gegen die Grundrechte

Plädoyer für eine ausführliche öffentliche Debatte in Sachen Vorratsdatenspeicherung

Datenhehlerei
TK-Daten
Berufsgeheimnisträger
Whistleblowing
Verwertungsverbot

■ Angesichts der erheblichen Grundrechtsrelevanz der von der Bundesregierung beabsichtigten Wiedereinführung der Vorratsdatenspeicherung ist eine ausführliche parlamentarische und verfassungsrechtliche Prüfung des Vorhabens unerlässlich. Die vorgesehene anlasslose und flächendeckende Speicherung von TK- und Internetdaten ist gemessen an der Rechtsprechung des BVerfG und des EuGH unverhältnismäßig. Schließlich mangelt es an überzeugenden Nachweisen, dass die Vorratsdatenspeicherung schwerste terroristische Straftaten verhindert hätte oder signifikant zu ihrer Aufklärung beigetragen hätte. Auch die vorgesehene neue Strafvorschrift § 202d StGB zur „Datenhehlerei" ist äußerst problematisch. Sie würde nicht nur zur Kriminalisierung von Whistleblower-Plattformen, Bloggern oder Medien führen, die dem Ziel dienen, Informationen über rechtswidriges Verhalten von Amtsträgern oder Organisationen zu sammeln oder aufzudecken. I.E. wäre sogar eine Schwächung des journalistischen Quellenschutzes zu befürchten und mithin eine Beeinträchtigung von Art. 5 Abs. 1 GG. Zudem würde die vorgesehene generelle Privilegierung von Amtsträgern oder deren Beauftragten den durch § 44 BDSG gewährleisteten Schutz personenbezogener Daten aushöhlen und andere gesetzliche Verwertungsverbote unterlaufen.

■ In view of the substantial relevance in regards to the constitution of the intended re-introduction of data retention by the federal government, a comprehensive parliamentary and constitutional law review of the plan is indispensable. The planned indiscriminate and comprehensive data retention of telecommunication and Internet data is disproportionate compared to the adjudication by the German Federal Constitutional Court (BVerfG) and ECJ. Ultimately, there is a lack of convincing evidence that data retention has hindered severe terrorist crimes or had significantly aided in solving the same. The envisioned new penal provision Sec. 202d German Penal Code (StGB) regarding „receiving stolen data" is also quite problematic. It would not only lead to the criminalization of whistleblower platforms, bloggers and media, which serve the purpose of collecting or unveiling information on illegal behavior by officials or their organizations. Specifically, one must be apprehensive of a weakening of the journalistic protection of sources and thus an impairment of Art. 5 Subsec. 1 German Constitution (GG). Furthermore, die envisioned general privileging of officials or their authorized representatives could lead to an undermining of the protection of personal data as provided by Sec. 44 German Federal Data Protection Act (BDSG) and circumvent other statutory prohibitions for utilization.

I. Vorbemerkung

Das *Bundesministerium der Justiz und für Verbraucherschutz* (*BMJV*) hat den Referentenentwurf eines „Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten"[1] vorgelegt. Das Artikelgesetz enthält Änderungsbefehle verschiedener Rechtsvorschriften, mit denen die Vorratsdatenspeicherung von TK- und Internetdaten wieder eingeführt werden soll, die seit dem Urteil des *BVerfG* v. 2.3.2010[2] in Deutschland nicht mehr zulässig ist. Daneben sieht der Entwurf die Einführung eines Straftatbestands der „Datenhehlerei" vor, der allerdings in keinem erkennbaren inhaltlichen Zusammenhang mit der vorgesehenen Wiedereinführung der Vorratsdatenspeicherung steht.

Das Artikelgesetz soll nach Presseberichten[3] noch vor der parlamentarischen Sommerpause, die am 4.7.2015 beginnt, durch den *Bundestag* gebracht werden. Zwischen dem Versand des ersten Referentenentwurfs durch das zuständige Ministerium und einem möglichen Beschluss des *Deutschen Bundestags* würden mithin maximal sieben Wochen liegen, in denen die gebotene fundierte parlamentarische und außerparlamentarische Diskussion kaum möglich erscheint. Die mit dem Gesetzentwurf vorgesehene Wiedereinführung der Vorratsdatenspeicherung hätte erhebliche Auswirkungen auf die Grundrechte. Betroffen wären sämtliche Nutzer von TK-Diensten und des Internets, mithin nahezu die gesamte Bevölkerung. Aus diesem Grund muss ein solches Gesetzesvorhaben einer ausführlichen parlamentarischen und verfassungsrechtlichen Prüfung unterzogen werden, in der die Argumente, die für und gegen das Vorhaben sprechen, gründlich erörtert und abgewogen werden können. Die Verabschiedung eines derart eingriffsintensiven Gesetzespakets ohne ausführliche öffentliche Debatte quasi im Schnelldurchgang wäre unverantwortlich. Angesichts der Komplexität der Materie wäre zudem zu befürchten, dass rechtliche und handwerkliche Fehler auftreten, die sich bei einer gründlicheren Behandlung vermeiden ließen.

Schließlich ist darauf hinzuweisen, dass in dieser Angelegenheit kein Grund zu einer beschleunigten Beschlussfassung zu erkennen ist. So findet in Deutschland seit dem Urteil des *Ersten Senats des BVerfG* v. 2.3.2010 keine Speicherung von TK-Daten auf Vorrat statt. Seit dem Urteil des *EuGH* (*Große Kammer*) v. 8.4.2014[4], in welchem der *EuGH* die RL 2006/24/EG für unvereinbar mit Art. 7 und Art. 8 der Charta der Europäischen Grundrechte (GRCh) erklärte, ist auch keine rechtliche Verpflichtung für den deutschen Gesetzgeber mehr vorhanden, die Speicherung von Daten aus der Telekommunikation und dem Internet auf Vorrat gesetzlich anzuordnen.

Auch auf faktischer Ebene sind keine Gründe für eine Eilbedürftigkeit der Entscheidung des *Deutschen Bundestags* über den Gesetzentwurf ersichtlich. Die auf politischer Ebene für die eilige Verabschiedung einer gesetzlichen Verpflichtung zur Vorratsdatenspeicherung genannten Argumente überzeugen nicht: So ist behauptet worden, die Attentate von Paris im Januar 2015 belegten die Dringlichkeit. Dabei wird übersehen, dass in Frankreich seit 2006 sämtliche TK- und Internetdaten für einen Zeitraum von zwölf Monaten auf Vorrat gespeichert werden. Weder hat sich dadurch der terroristische Anschlag verhindern lassen, noch gibt es Belege dafür, dass die auf Vorrat gespeicherten Daten für die Aufklärung des terroristischen Verbrechens erforderlich waren. Auch die Behauptung, dass sich der rechtsterroristische Anschlag in Norwegen im November 2011 nur durch die wegen einer angeblichen Vorratsdatenspeicherung verfügbaren Daten schnell habe aufklären lassen, erweist sich bei näherem Hinsehen als nicht überzeugend, insbesondere weil in Norwegen bis heute keine gesetzliche Verpflichtung zur Speicherung von TK- und Internetdaten besteht. Insofern ist der schnelle Ermittlungserfolg der norwegischen Behörden eher ein Beleg für die These, dass sich selbst schwerste Straftaten ohne eine Verpflichtung zur anlasslosen und umfassenden Speicherung von personenbezogenen TK-Daten aufklären lassen.

II. Verfassungsrechtlicher Rahmen

Der aktuelle Gesetzentwurf muss im Lichte des deutschen Verfassungsrechts und der GRCh betrachtet werden.

Der *EuGH* hat in seinem U. v. 8.4.2014 festgestellt, dass die 2006 vom *Europäischen Parlament* gebilligte RL 2006/24/EG zur Vorratsspeicherung von Telekommunikationsverkehrsdaten eklatant gegen die GRCh verstößt, und zwar gleichermaßen gegen den in Art. 7 garantierten Schutz der Privatsphäre und den durch Art. 8 verbrieften Schutz personenbezogener Daten. Legitime Zwecke der Strafverfolgung, der Gefahrenabwehr und der Terrorismusbekämpfung rechtfertigen die mit einer anlasslosen, regional unbegrenzten, langfristigen und umfangreichen Speicherung personenbezogener Daten verbundenen Grundrechtseingriffe nicht. Dies gilt jedenfalls dann, wenn von einer solchen Maßnahme ganz überwiegend Unverdächtige betroffen sind.

In erster Linie hat der *EuGH* die RL von 2006 für unvereinbar mit der GRCh und mit sofortiger Wirkung für nichtig erklärt. Es sei zunächst daran erinnert, dass die RL zur Vorratsspeicherung unter dem Eindruck der Bombenanschläge von Madrid 2004 und London 2005 auf Vorschlag der *EU-Kommission* vom *Europäischen Parlament* und vom *Rat* mehrheitlich angenommen und am 15.3.2006 in Kraft gesetzt wurde.[5] Dabei wurde als zentrale Begründung vorgebracht, die anlasslose und flächendeckende Speicherung solcher Daten ermögliche die schnellere Festnahme von terroristischen Gewalttätern, auch wenn diese These zu keiner Zeit belegt werden konnte. Zuvor hatte der *Deutsche Bundestag* noch im Januar 2005 die vom *Bundesrat* vorgeschlagene Einführung einer Speicherung von TK-Verkehrsdaten auf Vorrat abgelehnt.[6]

Auch wenn der *EuGH* in der Begründung seines Urteils sich in mehrfacher Hinsicht an der Entscheidung des *BVerfG* v. 2.3.2010 zum deutschen TKG orientiert hat, geht er doch deutlich über diese Entscheidung ebenso wie über die Anträge des eigenen Generalanwalts *Cruz Villalón* v. 12.12.2013 hinaus. Wie das *BVerfG* betont der *EuGH* die Aussagekraft der auf Vorrat zu speichernden Metadaten. Denn aus diesen Daten können „sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert wurden, gezogen werden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren."[7] Die dadurch entstehende Gefahr der Profilbildung

1 Vgl. *BMJV*, Referentenentwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten v. 15.5.2015, abrufbar unter: http://www.eaid-berlin.de/wp-content/uploads/2015/05/2015-05-15-BMJV-RefE-Ho%CC%88chstspeicherfrist.pdf.

2 BVerfGE 125, 260 = MMR 2010, 356.

3 Vgl. etwa Zeit Online v. 16.5.2015, Vorratsdatenspeicherung soll vor Sommerpause Gesetz werden, abrufbar unter: http://www.zeit.de/digital/datenschutz/2015-05/gesetzentwurf-vorratsdatenspeicherung.

4 Verb. Rs. C-293/12 (Digital Rights Ireland) und C-594/12 (Seitlinger), ZD 2014, 296 m. Anm. *Petri*; vgl. auch *Boehm/Cole*, Data Retention after the Judgement of the Court of the European Union, 2014 und *Dix/Schaar*, Der EuGH zur Vorratsdatenspeicherung: Wegweisend für den gesamten Datenschutz, Jahrbuch Informationsfreiheit und Informationsrecht 2014, S. 17 m.w.Nw.

5 Zur Vorgeschichte der RL näher *Leutheusser-Schnarrenberger*, DuD 2014, 589 f.

6 Beschluss und Bericht des *Rechtsausschusses* v. 26.1.2005, BT-Drs. 15/4748, Plenarprotokoll 15/154 der 154. Sitzung v. 27.1.2005, 14418 B.

7 *EuGH* (o. Fußn. 4), Rdnr. 27.

ist keineswegs nur theoretischer Natur.[8] Nahezu wörtlich übernimmt der *EuGH* das Argument des *BVerfG*, dass die Vorratsdatenspeicherung geeignet sei, „das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Beobachtung ist."[9] Dies erinnert zugleich an den vom *U.S. Supreme Court* schon früh beschriebenen, von Grundrechtseingriffen ausgehenden „chilling effect"[10]. Folgerichtig sieht der *EuGH* auch – wie zuvor bereits das *BVerfG* – einen engen Zusammenhang zwischen der vorgeschriebenen Erhebung personenbezogener Daten und der Freiheit der Meinungsäußerung, die durch Art. 11 GRCh geschützt ist.[11] Im Kern betrachtet der *EuGH* die unionsrechtliche Pflicht zur anlasslosen Vorratsdatenspeicherung als einen Verstoß gegen die Grundrechte auf Achtung des Privatlebens (Art. 7 GRCh) und auf Schutz der personenbezogenen Daten (Art. 8 GRCh). Dabei betont er zu Recht den engen Zusammenhang zwischen dem Recht auf Privatheit und dem Recht auf Datenschutz, in die durch die Vorratsdatenspeicherung gleichzeitig eingegriffen wird, ohne dass die i.Ü. bestehenden dogmatischen Unterschiede[12] zwischen diesen Grundrechten vernachlässigt werden sollen. Sie spielen aber in den Augen des *EuGH* bei der Vorratsdatenspeicherung keine praktische Rolle.

Wie das *BVerfG* hält auch der *EuGH* durch die Pflicht zur Vorratsdatenspeicherung den Wesensgehalt der Grundrechte auf Privatheit und Datenschutz nicht für verletzt.[13] Allerdings scheint der *EuGH* eine solche Verletzung – anders als das *BVerfG* – auch nicht bei Überschreitung einer bestimmten Höchstspeicherfrist ins Auge zu fassen.[14] Das steht in gewissem Widerspruch zu den zuvor gemachten Feststellungen zur weitreichenden Aussagekraft der Metadaten, die im Einzelfall sogar aussagekräftiger sein können als belanglose Inhaltsdaten. So können mittels Metadaten Bewegungsprofile erstellt oder schutzwürdige Kommunikationsbeziehungen zwischen Betroffenen und Berufsgeheimnisträgern wie Ärzten und Rechtsanwälten bekannt werden. Auf der anderen Seite bringen belanglose Gespräche zwischen Terroristen z.B. über das Wetter meist keinen zusätzlichen Erkenntnisgewinn.

Entscheidend ist aber, dass der *EuGH* letztlich die in der RL von 2006 vorgeschriebene Vorratsdatenspeicherung trotz ihrer prinzipiellen Geeignetheit für die Bekämpfung schwerer Straftaten als einen unverhältnismäßigen Eingriff in die Grundrechte ansieht und deshalb für nichtig erklärt hat.[15] Im Kern hält der *EuGH* in Anlehnung an die Rechtsprechung des *EGMR* die in der RL geregelte Vorratsdatenspeicherung nicht für „zwingend notwendig in einer demokratischen Gesellschaft."[16]

In mehreren Punkten macht der *EuGH* deutlich, weshalb die in der RL von 2006 vorgeschriebene Vorratsspeicherung im engeren Sinne unverhältnismäßig ist: Es müssen zum einen Daten aller Personen und aller von ihnen genutzten Kommunikationsmittel gespeichert werden und dies unabhängig davon, in welchem Zusammenhang diese Personen zu einer schweren Straftat stehen. Schon dieser „Eingriff in die Grundrechte fast der gesamten europäischen Bevölkerung"[17] geht über das absolut Notwendige hinaus. Die undifferenzierte und über das Erforderliche hinausschießende Speicherpflicht zeigt sich auch bei den fehlenden Begrenzungen in geografischer und zeitlicher Hinsicht.[18] Es werden pauschale Speicherfristen vorgegeben, die wiederum keine Unterscheidung hinsichtlich einer bestimmten Gefährdung der öffentlichen Sicherheit oder bestimmter Datenkategorien ermöglichen.

Schon diese für das Urteil tragenden Gesichtspunkte lassen künftig eine anlasslose Vorratsspeicherung in Europa nicht mehr zu. Schließlich bemängelt der *EuGH*, dass die RL keine präzisen Vorgaben für technisch-organisatorische Sicherungsmaßnahmen und für eine Speicherung der zu bevorratenden Daten im Unionsgebiet vorsah.[19] Letzteres ist eine Konsequenz aus dem NSA-Skandal, denn seit den von *Edward Snowden* initiierten Veröffentlichungen ist klar, dass die Sicherung von Datenbeständen vor dem unkontrollierten Zugriff von Nachrichtendiensten, so schwierig sie in jedem Fall bleibt, außerhalb der EU offenbar aussichtslos ist.

Die abschließende Bemerkung des *EuGH*, aus der „Gesamtheit" der genannten Erwägungen ergebe sich die Grundrechtswidrigkeit der Vorratsdatenrichtlinie, könnte zu dem Fehlschluss verleiten, die Grundrechtskonformität einer künftigen europäischen Regelung könne schon durch Behebung eines der genannten Mängel erreicht werden.[20] I.E. müssen die vom *EuGH* formulierten Anforderungen vielmehr kumulativ verstanden werden.[21]

Dass jeder erneute Versuch, eine anlasslose Vorratsspeicherung europaweit vorzuschreiben, scheitern muss, kann an einer bestimmten Gruppe von Betroffenen deutlich gemacht werden. Sowohl das *BVerfG* als auch der *EuGH* haben betont, dass eine grundrechtskonforme Vorratsspeicherung von Verkehrsdaten der Telekommunikation die Träger von Berufsgeheimnissen ausschließen müsste.[22] Telefonkontakte mit Ärzten, Psychotherapeuten und Rechtsanwälten dürfen auch zur Abwendung schwerer Straftaten nicht flächendeckend erfasst werden. Das aber würde bedeuten, dass in allen EU-Mitgliedstaaten zentrale Filterdateien mit den Kontaktdaten aller Berufsgeheimnisträger eingerichtet werden müssten, die technisch die Speicherung derartiger Anrufe oder Anrufversuche bei den TK-Anbietern unterbinden müssten. Jedenfalls genügt eine Regelung, die – wie der vom *BMJV* vorgelegte Referentenentwurf – (aus praktischen Gründen) die flächendeckende Speicherung von Daten von Berufsgeheimnisträgern vorsieht und den Schutz lediglich im Hinblick auf den behördlichen Zugriff und die Nutzung der Daten einschränkt, diesen Anforderungen nicht.

Schließlich ist darauf hinzuweisen, dass die Regierungen der EU-Mitgliedstaaten bis heute nicht den Beweis für die Erforderlichkeit der Vorratsdaten geführt haben. Insbesondere fehlen unabhängige wissenschaftliche Untersuchungen darüber, wie sich die seit 2006 eingeführten gesetzlichen Regelungen zur Vorratsdatenspeicherung auf die Bekämpfung schwerer Straftaten ausgewirkt haben. Angesichts der Tatsache, dass es in Deutschland – anders als in nahezu allen anderen Mitgliedstaaten – zwischen 2010 und 2014 keine obligatorische Datenspeicherung auf Vorrat gab, wäre es ohne weiteres möglich, im Rahmen rechtsvergleichender Studien Aussagen über die Wirksamkeit der Maßnahmen zu treffen. Wenn seitens der Regierungen entsprechende Studien nicht in Auftrag gegeben worden sind, kann dies als Indiz dafür gewertet werden, dass selbst die Befürworter der Vorratsdatenspeicherung Zweifel an deren nachweisbarer Notwendigkeit haben.

---

8 Anders offenbar *Kühling*, NVwZ, 2014, 683.
9 *EuGH* (o. Fußn. 4), Rdnr. 37.
10 Vgl. Wieman v. Updegraff, 344 U.S. 183 (1952).
11 *EuGH* (o. Fußn. 4), Rdnr. 28.
12 Vgl. dazu *Kokott/Sobotta*, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law 2013, S. 222.
13 *EuGH* (o. Fußn. 4), Rdnr. 39 f.; *BVerfG* (o. Fußn. 2).
14 Darauf weist *Petri*, ZD 2014, 300 hin.
15 Vgl. *Roßnagel*, MMR 2014, 375; anders offenbar *Simitis*, NJW 2014, 2160.
16 St. Rspr. des *EGMR* seit dem U. v. 6.9.1978 (5029/71 – Klass u.a. gegen Deutschland), vgl. auch das U. v. 26.3.1987 (9248/81 – Leander gegen Schweden), wo der *Gerichtshof* von einem „zwingenden gesellschaftlichen Erfordernis" (pressing social need, Rdnr. 58) spricht, ohne das Grundrechtseingriffe nicht zulässig sind. Mit dieser Orientierung an der Rspr. des *EGMR* unterscheidet sich der *EuGH* in seiner Begründung ebenfalls deutlich vom *BVerfG*.
17 *EuGH* (o. Fußn. 4), Rdnr. 56.
18 *EuGH* (o. Fußn. 4), Rdnr. 59, 63.
19 *EuGH* (o. Fußn. 4), Rdnr. 67 f.
20 Vgl. *Kühling*, NJW 2014, 683.
21 So auch *Kühling*, NJW 2014, 683.
22 *BVerfG* (o. Fußn. 2), Rdnr. 237; *EuGH* (o. Fußn. 4), Rdnr. 58.

Vor diesem Hintergrund bestehen schwerwiegende verfassungs- und europarechtliche Bedenken gegen den Gesetzentwurf und es wird angeregt, auf die Wiedereinführung der Vorratsdatenspeicherung zu verzichten.

Die vorgeschlagene neue Strafvorschrift § 202d StGB (Datenhehlerei) steht in keinem erkennbaren Zusammenhang mit den sonstigen durch das Gesetzesvorhaben verfolgten Zwecken. Sie würde einerseits zur Kriminalisierung von Whistleblower-Plattformen, Bloggern oder Medien führen, die dem Ziel dienen, Informationen über rechtswidriges Verhalten von Amtsträgern oder Organisationen zu sammeln oder aufzudecken. I.E. wäre sogar eine Schwächung des journalistischen Quellenschutzes zu befürchten und mithin eine Beeinträchtigung von Art. 5 Abs. 1 GG. Würde es den im Entwurf formulierten Straftatbestand schon heute geben, würde eine Vielzahl der in diesen Tagen erfolgenden Berichte und Blogs über illegale Aktivitäten von Geheimdiensten strafrechtlich verfolgt. Zudem würde die vorgesehene generelle Privilegierung von Amtsträgern oder deren Beauftragten, mit denen Daten „der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden sollen", den durch § 44 BDSG gewährleisteten Schutz personenbezogener Daten aushöhlen und andere gesetzliche Verwertungsverbote unterlaufen.

Die im Gesetzentwurf vorgesehene neue Strafvorschrift zur „Datenhehlerei" ist aus diesen Gründen abzulehnen. Unabhängig davon sollte allerdings gründlich geprüft werden, wie ein besserer strafrechtlicher Schutz personenbezogener Daten gewährleistet werden kann.[23] Unbeschadet dieser grundsätzlichen Kritik soll im Folgenden – ohne Anspruch auf Vollständigkeit – auf einige Detailfragen eingegangen werden.

III. Stellungnahme zu einzelnen Vorschriften

1. § 100g Abs. 1 Satz 1 Nr. 1 StPO-E

Gemäß dieser Ermächtigungsgrundlage dürfen Verkehrsdaten i.S.d. § 96 Abs. 1 TKG erhoben werden, soweit der Verdacht besteht, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung begangen hat, worunter insbesondere Straftaten i.S.d. Katalogs des § 100a Abs. 2 StPO fallen. Da der Schwerpunkt der Vorschrift auf der „Straftat von auch im Einzelfall erheblicher Bedeutung" liegt, ist die Bezugnahme auf den Katalog des § 100a Abs. 2 StPO nicht abschließend. Eine Verkehrsdatenabfrage ist damit auch dann gesetzlich zulässig, wenn kein Fall von § 100a Abs. 2 StPO vorliegt. Insbesondere in den Fällen der Funkzellenabfrage gem. § 100g Abs. 3 StPO-E, die zu ihrer Durchführung im Wesentlichen auf die Voraussetzungen des § 100g Abs. 1 Satz 1 Nr. 1 StPO-E verweist, ist solch eine allgemein gehaltene Ermächtigungsgrundlage verfassungsrechtlich problematisch, denn die Funkzellenabfrage ist in besonderem Maße geeignet, einen umfassenden Einblick in die engere Persönlichkeitssphäre eines Betroffenen zu ermöglichen. Die Eingriffsintensität und die Ausdehnung des Betroffenenkreises der Funkzellenabfrage wird ferner dadurch erhöht, dass gem. § 101a Abs. 1 Satz 3 StPO-E die räumlich und zeitlich eng begrenzte und hinreichend bestimmte Aufzeichnung der Telekommunikation anstelle der genaueren Vorgaben des § 100b Abs. 2 Satz 2 Nr. 2 StPO genügt.

2. § 100g Abs. 1 Satz 1 Nr. 2 StPO-E

Gemäß dieser Regelung dürfen Verkehrsdaten i.S.d. § 96 Abs. 1 TKG erhoben werden, gestützt auf den Verdacht, dass jemand eine Straftat mittels Telekommunikation begangen hat. Dabei ist zwingende Voraussetzung, dass die Datenerhebung zur Erforschung des Sachverhalts erforderlich ist und die Erhebung in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Hinzu tritt die Ausschlussklausel, dass die Datenerhebung nur dann zulässig ist, wenn die Sachverhaltserforschung auf andere Weise aussichtslos wäre. Zwar handelt es sich bei den meisten Verkehrsdaten i.S.d. § 96 Abs. 1 TKG um solche Informationen über den Betroffenen, welche der Diensteanbieter ohnehin zur Wahrnehmung eigener Zwecke wie z.B. der Entgeltermittlung oder zum Aufbau weiterer Verbindungen sammelt. Gleichwohl kommt diesen Daten ein nicht unerheblicher Informationsgehalt zu, der nicht nur die Ermittlung des individuellen TK-Endgerätenutzers ermöglicht, sondern darüber hinaus ganz i.S.d. Social Engineering umfangreiche Rückschlüsse auf die sozialen Beziehungen des Betroffenen zulässt. Aus diesem Grunde sind an die Erhebung auch von Verkehrsdaten nach § 96 Abs. 1 TKG höhere Anforderungen zu stellen, als es der Entwurf aus dem *BMJV* zurzeit vorgibt. Das bloße Vorliegen eines Verdachts, dass jemand auch nur als Teilnehmer eine irgendwie geartete Straftat mittels Telekommunikation begangen hat, kann demgegenüber nicht ausreichend sein. Auch die in Absatz 1 Satz 1 und Satz 2 bestimmte Angemessenheitsklausel und die Ausschlussklausel allein sind nicht ausreichend, um einen Grundrechtseingriff allein für diesen Fall zu rechtfertigen, d.h. den Kreis durch diese Maßnahme potenziell Betroffener so weit einzuengen, dass von einer noch verhältnismäßigen wie auch hinreichend bestimmten Regelung gesprochen werden kann.

3. § 100g Abs. 2 StPO-E

Unabhängig davon, ob man in sämtlichen der aufgeführten Straftatbestände in § 100g Abs. 2 StPO-E tatsächlich derart schwerwiegende Straftaten sieht, welche die Erhebung der in § 113b TKG-E benannten Verkehrsdaten rechtfertigen, so ist zumindest der Straftatenkatalog in Absatz 2 deutlich bestimmt und abschließender Natur. Hierdurch werden entsprechend den bundesverfassungsgerichtlichen Vorgaben hinreichend hohe Hürden geschaffen, um auf die gespeicherten Vorratsdaten i.R.v. sicherheitsbehördlichen Ermittlungen zuzugreifen.

4. § 100g Abs. 4 StPO-E

Es wird bestimmt, dass die Erhebung von Verkehrsdaten, die sich gegen Berufsgeheimnisträger i.S.d. § 53 Abs. 1 StPO richtet, unzulässig ist, soweit hierdurch voraussichtlich Erkenntnisse erlangt würden, über die das Zeugnis verweigert werden dürfte. Dennoch erlangte Kenntnisse dürfen nicht verwendet werden. Diese Regelungen zum Schutz der Berufsgeheimnisträger sind in ihrer derzeitigen Fassung unzureichend und unter verfassungsrechtlichen Gesichtspunkten höchst problematisch, soweit sie sich lediglich auf ein Beweiserhebungs- und ein Beweisverwertungsverbot beschränken. Darüber hinaus verstoßen sie gegen die Vorgaben, welche der *EuGH* in seinem Urteil zur Ungültigkeit der Vorratsdatenspeicherungsrichtlinie festgelegt hat. Es wird darüber hinaus in keinster Weise gesetzlich bestimmt, durch welche verfahrensrechtlichen Vorkehrungen der Schutz von zeugnisverweigerungsberechtigten Personen im Konkreten gewährleistet werden soll. Im Falle des § 100g Abs. 4 StPO-E besteht in jedem Falle dringender Überarbeitungsbedarf, um das Zeugnisverweigerungsrecht nach § 53 StPO vor einer Entwertung durch die Vorratsdatenspeicherung zu schützen.

5. § 101a Abs. 2 StPO-E

Gemäß dieser Vorschrift kann die Anordnung einer Erhebung von Verkehrsdaten verlängert werden. Hier sollte, um die Verhältnismäßigkeit zu wahren, zumindest eine Obergrenze für die Anzahl von Maßnahmenverlängerungen eingesetzt werden, um die Bildung solcher Persönlichkeitsprofile zu vermeiden, die sich über die Dauer mehrerer Jahre erstrecken.

23 Vgl. hierzu auch unter IV.

6. § 101a Abs. 3 StPO-E

Positiv hervorzuheben ist die Kennzeichnungsverpflichtung gem. § 101a Abs. 3 StPO-E, denn hierdurch kann die Zweckbindung eines einmal erhobenen Datums deutlich besser gewahrt werden, als wenn dieses ohne entsprechende Hintergrundinformation verarbeitet würde. Auch nach Übermittlung an eine andere Stelle ist die Kennzeichnung durch diese aufrechtzuerhalten. Die Verpflichtung zur Kennzeichnung findet sich ebenso in § 113c Abs. 3 TKG-E wieder.

7. § 101b StPO-E

Die hier benannte Regelung zur statistischen Erfassung der Erhebung von Verkehrsdaten ist in ihrer jetzigen Form unzureichend. Sinnvoll wäre es, eine solche Dokumentationsvorschrift um die Nachweispflicht dahingehend zu ergänzen, in welchen Fällen die Durchführung der Ermittlungsmaßnahme tatsächlich kausal zu einem entscheidenden Ermittlungserfolg geführt hat. An einen derartigen Effektivitätsnachweis der Vorratsdatenspeicherung anknüpfend ist es denkbar, die Geltung der Gesetzesnovellen zunächst zu limitieren, um nur bei positiver statistischer Erfassung von Ermittlungserfolgen eine Fortgeltung zu bestimmen.

8. § 113b Abs. 1 TKG-E

Die Festlegung, allgemeine Verkehrsdaten für zehn Wochen und Standortdaten für vier Wochen zu speichern, ist mehr oder weniger willkürlich. Nicht klar wird, warum noch kürzere Speicherfristen nicht auch geeignet wären, um den Maßnahmenerfolg zu begründen.

9. § 113b Abs. 2 Satz 2 Nr. 2 TKG-E

Die Erbringer öffentlich zugänglicher Telefondienste sollen gemäß der Neuregelung ebenso dazu verpflichtet sein, unbeantwortete oder wegen eines Eingriffs des Netzwerkmanagements erfolglose Anrufe zu speichern. Eine solche Ermächtigungsgrundlage geht in ihrem Umfang sogar noch über die für verfassungswidrig erklärte Regelung von 2006 hinaus und ist deshalb abzulehnen.

10. § 113b Abs. 5 und Abs. 8 TKG-E

Zu begrüßen ist die Klarstellung in § 113b Abs. 5 TKG-E, dass Inhalts- und E-Maildaten nicht i.R.e. Vorratsdatenspeicherung zu Ermittlungszwecken verarbeitet werden dürfen, ebenso die unbedingte und technisch irreversible Löschungsverpflichtung des Diensteanbieters nach § 113b Abs. 8 TKG-E. In diesem Zusammenhang ist jedoch anzumerken, dass bloße gesetzliche Vorgaben ohne die Festlegung entsprechender Kontrollpflichten ihre rechtsverbindliche Wirkung nicht in vollem, tatsächlichem Maß entfalten können.

11. § 113c Abs. 1 Nr. 3 TKG-E

Diese neue Vorschrift sieht eine generelle Übermittlungsbefugnis der nach § 113b TKG-E gespeicherten Verkehrsdaten an die Verfassungsschutzbehörden, den *Militärischen Abschirmdienst* (*MAD*) und den *Bundesnachrichtendienst* (*BND*) vor, soweit die Daten „durch den Erbringer öffentlich zugänglicher Telekommunikationsdienste für eine Auskunft nach § 113 Absatz 1 Satz 3 verwendet werden". Diese Vorschrift ist inhaltlich nahezu unbestimmt, indem sie durch die Verweisungsregelung ein weites Anwendungsfeld für die Nutzung von Verkehrsdaten auch zu solchen Zwecken ermöglicht, die nicht nur der Abwehr oder Verfolgung schwerwiegender Straftaten dienen. Mithin fehlen jegliche Qualifikation im Hinblick auf die abzuwehrenden Gefahren sowie jede sonstige tatbestandsmäßige Einschränkung. Eine solche Regelung dürfte deshalb verfassungswidrig sein.

12. § 113d und § 113f TKG-E

Es mag sicherlich begrüßt werden, dass die Verpflichtung zur Wahrung der Informations- und Datensicherheit nunmehr auch ausdrücklich im Gesetz Benennung findet, da die zu Ermittlungszwecken gespeicherten Vorratsdaten von Millionen von Bundesbürgern nicht unerheblichen Manipulationsrisiken unterliegen. Gerade wenn sich der Staat der digitalen Datenverarbeitung bedient, um zu Zwecken der öffentlichen Sicherheit Maßnahmen zu ergreifen, muss er im Sinne seiner Gewährleistungsverantwortung für die informationstechnische Sicherheit der von ihm genutzten Datenverarbeitungssysteme besonders hohe Vorgaben bestimmen. Dennoch fehlen auch hier wieder konkrete Regelungen dahingehend, wie die abstrakten gesetzlichen Vorgaben in der Praxis effektiv auf ihre Umsetzung bei den Dienstebetreibern hin überprüft werden können. Auch hier gilt wieder: Bloße gesetzliche Vorgaben ohne die Festlegung entsprechend umfassender Kontrollpflichten können ihre Wirkung nicht in vollem Maß entfalten. Die Prüfpflicht durch die *Bundesnetzagentur* (*BNetzA*) nach § 113f Abs. 2 TKG-E für den Anforderungskatalog kann dabei keine richtige Kontrolle für jeden Einzelfall ersetzen. Sporadische IT-Sicherheitsüberprüfungen nach § 113f Abs. 3 Satz 2 TKG-E i.V.m. § 109 Abs. 7 TKG sind ebenfalls nicht ausreichend.

Darüber hinaus endet die Datensicherheit nicht beim TK-Diensteanbieter, sondern es müssen ebenso strenge Anforderungen für die Behörden gelten, welche die Daten nutzen. Hier fehlt es noch an speziellen, auf die Vorratsdatenspeicherung zugeschnittenen Festlegungen. Der Staatstrojaner-Skandal 2011 hat gezeigt, dass zahlreiche Behörden noch nicht in der Lage sind, in sicherer Weise mit den technischen Herausforderungen neuartiger Ermittlungsinstrumente umzugehen.

13. § 113e TKG-E

Grundsätzlich ist die Einführung einer Protokollierung zu Zwecken der Datenschutzkontrolle zu begrüßen, die Speicherfrist nach Absatz 3 sollte aber zur Behördenkontrolle sowie zur Gewährleistung eines effektiven Rechtsschutzes auf drei Jahre ausgedehnt werden.

IV. Neuer Straftatbestand „Datenhehlerei", § 202d StGB-E

Ausweislich der Gesetzesbegründung soll der neue Straftatbestand „den strafrechtlichen Schutz von Informationssystemen und der in ihnen gespeicherten Daten vor Angriffen und Ausspähungen" verbessern.[24] Danach soll sich strafbar machen, wer Daten, „die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen."

Die neue Strafvorschrift soll für sämtliche Daten gelten, nicht nur für solche mit Personenbezug. Letztere sind in aller Regel ohnehin schon durch § 44 BDSG strafrechtlich geschützt. Um deren Schutz zu verbessern, würden entsprechende Ergänzungen der BDSG-Vorschrift ausreichen. Die neue Regelung kann sogar zu einer Schwächung des Datenschutzes beitragen, denn nicht strafbar soll gem. § 202d Abs. 3 StGB-E die Beschaffung und Weitergabe von Daten sein „für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Nicht strafbar sollen insbesondere solche Handlungen von Amtsträgern oder deren Beauftragten sein, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungs-

24 Entwurf des *BMJV* (o. Fußn. 1), S. 2.

widrigkeitenverfahren zugeführt werden sollen." Eine entsprechende Ausnahmeregelung fehlt im § 44 BDSG. Sie würde zudem potenzielle Täter geradezu motivieren, illegal und insbesondere unter Bruch datenschutzrechtlicher Vorschriften an Informationen zu kommen, die für deutsche Behörden von Interesse wären, die sie aber mangels Befugnis oder faktischer Möglichkeit nicht selbst erheben können. Statt einer Bekämpfung der illegalen Datenweitergabe wäre die Vorschrift insofern geradezu eine Einladung zum Datendiebstahl und zur Weitergabe der erlangten Daten an Behörden. Zudem stellt sich die Frage, in welchem Verhältnis die neue Vorschrift zu anderen gesetzlichen Regelungen steht, welche die Befugnisse staatlicher Stellen beschreiben oder die Nutzungsbeschränkungen und Verwertungsverbote vorsehen. Angesichts der allgemein gehaltenen Formulierung von § 202d Abs. 3 ist zu befürchten, dass Behörden in Fällen, in denen ihnen eine direkte Datenbeschaffung nicht gesetzlich erlaubt ist, sich zukünftig verstärkt inoffizieller Zuträger bedienen.

Im Hinblick auf die Informationsfreiheit und die Transparenz staatlichen Handelns könnte die neue Strafvorschrift zusätzliche negative Folgen haben. So würde sich grundsätzlich jedermann strafbar machen, der sich durch Insider gewonnene Erkenntnisse über illegale Aktivitäten von Firmen, Behörden oder sonstigen Organisationen verschafft, diese öffentlich macht oder an Dritte weitergibt. Sowohl die Betreiber entsprechender Plattformen (etwa Wikileaks) als auch Blogger und ggf. auch Journalisten würden sich strafbar machen, wenn sie entsprechende Informationen weitergeben, die nicht aus internen IT-Systemen stammen. Der in der Gesetzesbegründung[25] enthaltene Hinweis auf eine angebliche Privilegierung von Journalisten aus der Kommentarliteratur überzeugt nicht. Zum einen müssten zukünftig auch Journalisten damit grundsätzlich mit strafrechtlicher Verfolgung rechnen, wenn sie Informationen verwenden, die angeblich aus illegalen Quellen stammen, selbst wenn sie sich auf berufliche Pflichten berufen. Zum anderen verweist die Begründung zutreffend darauf, dass allenfalls solche Handlungen von Journalisten geschützt wären, die in Vorbereitung einer konkreten Veröffentlichung erfolgen. Die Weitergabe von Ergebnissen journalistischer Recherchen, die ggf. weit im Vorfeld einer Veröffentlichung erfolgt, wäre demnach generell strafbar. Journalistisch tätige Amateure und Blogger wären keinesfalls privilegiert.

25 Entwurf des *BMJV* (o. Fußn. 1), S. 54.

Dr. Alexander Dix, LL.M.
ist seit Juni 2005 Berliner Beauftragter für Datenschutz und Informationsfreiheit.

Dennis-Kenji Kipker
ist wissenschaftlicher Assistent am Institut für Informations-, Gesundheits- und Medizinrecht (IGMR) an der Universität Bremen sowie Mitglied der Europäischen Akademie für die Informationsfreiheit und den Datenschutz (EAID).

Peter Schaar
ist Vorsitzender der Europäischen Akademie für die Informationsfreiheit und den Datenschutz (EAID) und ehem. Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI).

Der Beitrag entspricht im Wesentlichen der Stellungnahme, welche die Europäische Akademie für Informationsfreiheit und Datenschutz (EAID) am 25.5.2015 zum Referentenentwurf des BMJV eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten v. 15.5.2015 abgegeben hat, vgl. http://www.eaid-berlin.de/?p=646.