DeutscherAnwaltVerein

Stellungnahme

des Deutschen Anwaltvereins durch die Ausschüsse Gefahrenabwehrrecht, Informationsrecht und Strafrecht

zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz für ein Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (Stand: 15.05.2015)

Stellungnahme Nr.: 25/2015 Berlin, im Mai 2015

Mitglieder des Ausschusses Gefahrenabwehrrecht

- Rechtsanwältin Dr. Heide Sandkuhl, Potsdam (Vorsitzende und Berichterstatterin)
- Rechtsanwalt Wilhelm Achelpöhler, Münster
- Rechtsanwalt Prof. Dr. Björn Gercke, Köln (Berichterstatter)
- Rechtsanwältin Andrea Groß-Bölting, Wuppertal
- Rechtsanwalt Dr. Stefan König, Berlin
- Rechtsanwältin Dr. Regina Michalke, Frankfurt / Main (Berichterstatterin)
- Rechtsanwältin Kerstin Oetjen, Freiburg

Zuständig in der DAV-Geschäftsführung

- Rechtsanwalt Thomas Marx

Mitglieder des Ausschusses Informationsrecht

- Rechtsanwalt Dr. Helmut Redeker, Bonn (Vorsitzender)
- Rechtsanwältin Dr. Christiane Bierekoven, Nürnberg
- Rechtsanwältin Isabell Conrad, München
- Rechtsanwalt Dr. Malte Grützmacher, LL.M., Hamburg
- Rechtsanwalt Prof. Niko Härting, Berlin (Berichterstatter)
- Rechtsanwalt Peter Huppertz, LL.M., Düsseldorf
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München (Berichterstatter)
- Rechtsanwalt Prof. Dr. Holger Zuck, Stuttgart

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Zuständig in der DAV-Geschäftsführung

- Rechtsanwalt Thomas Marx

Mitglieder des Ausschusses Strafrecht

- RA Prof. Dr. Stefan König, Berlin (Vorsitzender und Berichterstatter)
- RA Dr. h.c. Rüdiger Deckers, Düsseldorf
- RAin Dr. Margarete Gräfin von Galen, Berlin
- RAin Dr. Gina Greeve, Frankfurt am Main
- RA Prof. Dr. Rainer Hamm, Frankfurt am Main
- RA Eberhard Kempf, Frankfurt am Main
- RA Dr. Ali B. Norouzi, Berlin
- RAin Gül Pinar, Hamburg
- RA Michael Rosenthal, Karlsruhe
- RA Martin Rubbert, Berlin
- RAin Dr. Heide Sandkuhl, Potsdam (Berichterstatterin)
- RA Dr. Rainer Spatscheck, München
- RA PD Dr. Gerson Trüg, Freiburg im Breisgau

Zuständig in der DAV-Geschäftsführung

- RAin Tanja Brexl, DAV-Berlin

Verteiler

Bundesministerium der Justiz und für Verbraucherschutz
Bundesministerium für Wirtschaft und Energie
Bundesministerium des Inneren

Ausschuss für Recht und Verbraucherschutz im Deutschen Bundestag
Ausschuss für Wirtschaft und Energie im Deutschen Bundestag
Ausschuss Digitale Agenda im Deutschen Bundestag
Innenausschuss im Deutschen Bundestag
Vorsitzende des Ausschusses für Recht und Verbraucherschutz im Deutschen Bundestag, Renate Künast
Vorsitzender des Innenausschusses im Deutschen Bundestag, Wolfgang Bosbach

Bundesgerichtshof
Bundesanwaltschaft

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Die Datenschutzbeauftragten der Bundesländer

Arbeitsgruppen Recht der Bundestagsfraktionen
Arbeitsgruppen Inneres der Bundestagsfraktionen
Justizministerien und Justizsenatoren der Länder
Landesministerien und Senatsverwaltungen des Inneren
Wirtschaftsministerien der Länder
Innenausschüsse der Landtage

Europäische Kommission - Vertretung in Deutschland
Bundesrechtsanwaltskammer
Bundesnotarkammer
Bundesverband der Freien Berufe
Deutscher Richterbund
Deutscher Notarverein e.V.
Deutscher Steuerberaterverband
Bundesverband der Deutschen Industrie (BDI)
GRUR
BITKOM
DGRI
Gewerkschaft der Polizei (Bundesvorstand)
Deutsche Polizeigewerkschaft im DBB
Ver.di, Recht und Politik
Deutscher Strafverteidiger e.V., Mirko Roßkamp
Regionale Strafverteidigervereinigungen
Organisationsbüro der Strafverteidigervereinigungen und – initiativen
Bund Deutscher Kriminalbeamter
Strafrechtsausschuss der BRAK
Vorsitzende des Strafrechtsausschusses des KAV, BAV

DAV-Vorstand und Geschäftsführung
Vorsitzende der DAV-Gesetzgebungsausschüsse

Vorsitzende der DAV-Landesverbände
Vorsitzende des FORUMs Junge Anwaltschaft
Gefahrenabwehrrechtsausschuss des Deutschen Anwaltvereins
Informationsrechtsausschuss des Deutschen Anwaltvereins
Strafrechtsausschuss des Deutschen Anwaltvereins
Geschäftsführender Ausschuss der Arbeitsgemeinschaft Strafrecht des Deutschen Anwaltvereins

Frankfurter Allgemeine Zeitung
Süddeutsche Zeitung GmbH
Berliner Verlag GmbH
Redaktion NJW
Juve-Verlag
Redaktion Anwaltsblatt
Juris
Redaktion MultiMedia und Recht (MMR)
Redaktion Zeitschrift für Datenschutz ZD
Redaktion heise online
Strafverteidiger-Forum (StraFo)
Neue Zeitschrift für Strafrecht, NStZ
Strafverteidiger

Prof. Dr. Jürgen Wolter, Universität Mannheim
Deutscher Juristentag (Präsident und Generalsekretär)
Prof. Dr. Schöch, LMU München

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit derzeit ca. 66.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

Zusammenfassung und Vorbemerkung

Nach Auffassung des DAV ist der Referentenentwurf weit davon entfernt, den mit einer Vorratsdatenspeicherung verbundenen schweren Eingriff in das Fernmeldegeheimnis zu rechtfertigen. Das Rechtfertigungsdefizit wiegt umso schwerer, als keine gesicherten empirischen Erkenntnisse darüber vorliegen, ob mit der flächendeckenden Vorratsdatenspeicherung das Ziel der Gefahrenabwehr und der Strafverfolgung überhaupt erreicht werden kann.

Der Schutz des anwaltlichen Berufsgeheimnisses erfordert einen gesteigerten Schutz jedweder beruflichen Kommunikation des Anwalts. Berufsgeheimnisträger sind durch die Vorratsdatenspeicherung besonders betroffen, ihre Arbeit ist auf Vertraulichkeit angelegt. Diesem besonderen Schutz wird der Referentenentwurf nicht gerecht.

Aus datenschutzrechtlicher Hinsicht werden mit dem vorgeschlagenen Entwurf in vielerlei Hinsicht die Vorgaben des EuGH nicht eingehalten. Dies betrifft unter anderem die Datensicherheit bei Speicherung der Daten und die Bezeichnung derjenigen Kommunikationsformen, die vom Gesetz erfasst sein sollen.

Neu im Vergleich zu den Leitlinien vom 15. April 2015 ist die geplante Einführung eines Straftatbestandes der Datenhehlerei. Damit unternimmt es die Bundesregierung – an verborgener Stelle eines Gesetzentwurfes, dessen Überschrift insinuiert, es gehe um Datenspeicherfristen – staatlichen Stellen die Früchte illegaler Datenerhebungen zu sichern. Dies wäre angesichts des bekannt gewordenen Verdachts systematischer Ausspähung von Bürgern, Unternehmen und Amtsträgern durch (ausländische) staatliche Stellen ein

fatales Signal. Zu dem vorgeblichen Zweck des neuen Straftatbestandes, das formelle Datengeheimnis vor einer Fortsetzung und Vertiefung seiner durch eine vorausgegangene Straftat erfolgten Verletzung zu schützen, steht dies in einem grotesken Widerspruch (dazu unter IV.).

Schließlich sollten auch die Erfahrungen in der Europäischen Union mit nationaler Gesetzgebung zur Vorratsdatenspeicherung berücksichtigt werden. In den Niederlanden, Bulgarien und der Slowakei wurden die Gesetze zur Speicherung von Vorratsdaten im Jahr 2015 für nichtig erklärt, in Österreich, Rumänien und Slowenien bereits im Jahr 2014. In mehreren Mitgliedstaaten der Europäischen Union sind derzeit verfassungsrechtliche Verfahren zur nationalen Gesetzgebung zur Speicherung von Vorratsdaten anhängig.

I.

Kein Anlass für eine anlasslose Vorratsdatenspeicherung

Während der Bundesminister der Justiz und für Verbraucherschutz seit seinem Amtsantritt im Kalenderjahr 2013 wiederholt und zu Recht (!) darauf hingewiesen hatte, dass „*eine anlasslose Vorratsdatenspeicherung gegen das Recht auf Privatheit und gegen den Datenschutz*“ verstößt[1], hat er nun eine Kehrtwende vollzogen. Nachdem das Ministerium sein Vorhaben zunächst in „Leitlinien zur Einführung einer Speicherfrist und Höchstspeicherfrist für Verkehrsdaten“ am 15. April 2015 vorgestellt hatte, legte es jetzt am15. Mai 2015 einen Referentenentwurf für ein Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vor. Weder in den Leitlinien noch im Referentenentwurf findet sich eine Begründung, weshalb jetzt eine Vorratsdatenspeicherung für erforderlich und angemessen erachtet wird. Der Referentenentwurf rekurriert lediglich auf Lücken bei der Strafverfolgung und bei der Gefahrenabwehr. Wenn – so argumentieren die Entwurfsverfasser – es nach geltender Rechtslage vom Zufall abhängt, ob Verkehrsdaten zum Zeitpunkt der

[1] DER SPIEGEL 13/2015, S. 34 f..

Anfrage noch vorhanden sind oder nicht, „kann (es) im Einzelfall dazu führen, dass strafrechtliche Ermittlungen ohne Erfolg bleiben, weil weitere Ermittlungsansätze nicht vorhanden sind."

1.

Inhalt des Referentenentwurfes

Der Referentenentwurf sieht im Wesentlichen folgendes vor:

- Speicherung von Verkehrsdaten, die bei der Telekommunikation anfallen,
- Speicherfrist: Standortdaten: vier Wochen, im Übrigen: zehn Wochen,
- Abruf der Daten:
  - zur Gefahrenabwehr durch Polizeibehörden, wenn tatsächliche Anhaltspunkte für bestimmte konkrete schwerste Gefahren vorliegen,
  - zu Strafverfolgungszwecken durch die Strafverfolgungsbehörden (umfassender Richtervorbehalt, keine Eilkompetenz der Staatsanwaltschaft, Straftatenkatalog),
- vor dem Abruf der Daten sind die Betroffenen grundsätzlich zu benachrichtigen,
- Telekommunikationsdiensteanbieter müssen die Daten gegen unbefugte Kenntnisnahme und Verwendung schützen; tun sie dies nicht, sollen sie mit „Sanktionen belegt" werden,
- bei unverhältnismäßiger Kostenlast Entschädigung der Telekommunikationsdiensteanbieter für die Umsetzung der Speicherverpflichtung,
- Löschung der Daten nach Ablauf der Höchstspeicherfrist,
- Androhung von Ordnungsgeld für den Fall, dass die Löschverpflichtung verletzt wird,
- Einführung eines Straftatbestandes der Datenhehlerei (§ 202d StGB-E)

2.

Verfassungsrechtlicher Rahmen

Mit Urteil vom 2. März 2010 hat das Bundesverfassungsgericht klargestellt, dass eine vorsorgliche anlasslose Speicherung der Telekommunikationsverkehrsdaten die **Ausnahme** bleiben müsse, da es sich um einen besonders schweren Eingriff mit einer Streubreite handele, wie sie die Rechtsordnung bisher nicht kenne und der geeignet sei, ein „diffus bedrohliches Gefühl des Beobachtetseins“ hervorzurufen[2]. Insoweit korrespondiert hiermit die Entscheidung des Europäischen Gerichtshofs vom 8. April 2014, nach der der Schutz des Grundrechts auf Achtung des Privatlebens verlangt, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkung auf das absolut Notwendige beschränken müssten[3]. Geht es aber mit der anlasslosen Vorratsdatenspeicherung um eine absolute Ausnahme vom geltenden Recht, die auf das absolut Notwendige beschränkt werden muss, bedeutet dies für den rechtspolitischen Handlungsrahmen Folgendes:

Bereits aus der Beachtung des rechtsstaatlich kaum zu überschätzenden Verhältnismäßigkeitsprinzips ergibt sich, dass den Gesetzgeber von vornherein eine Darlegungslast trifft. Darzulegen ist, dass die Vorratsdatenspeicherung „erforderlich“ und – wenn man die Erforderlichkeit unterstellt – zur Erreichung der sicherheitspolitischen Ziele „geeignet“ ist. Die damit einhergehende Darlegungslast bedeutet der Sache nach, dass der Gesetzgeber zur Rechtfertigung des beabsichtigten Eingriffs der Notwendigkeit unterfällt, darzutun, dass und inwieweit es überhaupt zur Gefahrenabwehr eines derartigen Eingriffs bedarf. Nichts anderes gilt im verfassungsrechtlichen Ergebnis, wenn man an den den Gesetzgeber überantworteten Gestaltungsspielraum verfahrensbezogene Anforderungen knüpft. Immerhin ist nach der Rechtsprechung des BVerfG davon auszugehen, dass Gesetze, die auf einer Prognose beruhen, stets aus sich

[2] *BVerfG* NJW 2010, 833.
[3] *EuGH* U. v. 08.04.2014, I-25; verbundene Rechtssachen C-293/12 und C-594/12.

selbst heraus eine spätere und überprüfbare Begründung zu den Annahmen über ihre voraussichtliche Wirkung erkennen lassen[4]. Diese Darlegungslast ist die Kehrseite des dem Gesetzgeber eingeräumten Entscheidungs- und Beurteilungsspielraums, denn nur hierdurch wird der Bürger in die Lage versetzt, die Gründe für den Eingriff in seine Grundrechte zu erfahren und erforderlichenfalls Rechtsschutz in Anspruch zu nehmen.

Der Referentenentwurf ist weit davon entfernt, den mit einer Vorratsdatenspeicherung verbundenen schweren Eingriff in das Fernmeldegeheimnis zu rechtfertigen.

a.

Gefahrenabwehrrecht

Dass mit einer Vorratsdatenspeicherung Gefahren nicht abgewehrt werden können, zeigen die Pariser Attentate. Obwohl Frankreich die Vorratsdatenspeicherung längst eingeführt hatte, half sie nicht, den Anschlag zu verhindern.

b.

Strafverfolgung

Ob mit einer Speicherung der Telekommunikationsdaten von 80 Millionen Bundesbürgerinnen und Bundebürgern tatsächlich Kriminalität, insbesondere der internationale Terrorismus, wirksam bekämpft werden kann, steht überhaupt nicht fest. Im Gegenteil:

- Der wissenschaftliche Dienst des Deutschen Bundestages hat festgestellt, dass die Vorratsdatenspeicherung auf die Aufklärungsquoten in den EU-

[4] Zur Darlegung bereits in der Begründung des Gesetzes, siehe *BVerfG*E 79, 311 ff., 343.

Mitgliedsstaaten „*praktisch keine Auswirkungen*“ hat[5]. Nach einem Rechtsgutachten des wissenschaftlichen Dienstes des Deutschen Bundestages, das sich auf Zahlen des Bundeskriminalamtes beruft, steigt die Aufklärungsquote mit Vorratsdatenspeicherung nur marginal um 0,006 %[6].

- Geht man nach dem vom Bundesamt für Justiz in Auftrag gegebenen Gutachten der kriminologischen Abteilung des Max-Planck-Instituts für ausländisches und internationales Strafrecht „zu möglichen Schutzlücken durch den Wegfall der Vorratsdatenspeicherung“ von Juli 2011 aus, erfolgt der Zugriff auf Vorratsdaten der Telekommunikation lediglich „*in einer sehr kleinen Zahl von Verfahren*“[7]. Das Gutachten gelangt unter anderem zu folgenden Ergebnissen:

  > „*Gegenwärtig können die Auswirkungen des BVerfG-Urteils vom 2.3.2010 noch nicht mit belastbaren Zahlen quantifiziert werden. (…) Die Untersuchung von Schutzlücken bei Wegfall der Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten kann auch im Hinblick auf die Auswirkungen auf Aufklärungsquoten nur eingeschränkt erfolgen. Dieses bedingt durch das Fehlen von spezifischen empirischen Untersuchungen, die Nichterfassung von verfahrensbezogenen Daten zur Abfrage von Verkehrsdaten sowie Vorratsdaten oder IP-Adressen und die im Zusammenhang mit besonderen Deliktsphänomenen nur bruchstückhaft vorliegenden (und erfassten) Informationen zur Aufklärungsquote. Der Diskussion zu Nutzen und Konsequenzen der Vorratsdatenspeicherung kann entnommen werden, dass geeignete Daten, die zu einer quantitativen Überprüfung der Auswirkungen der Vorratsdatenspeicherung auf die Aufklärungsquote führen könnten, bislang nicht erfasst werden,* ***und im Übrigen auch nicht systematisch erfasst werden sollen****. Die Resultate der bis heute vorliegenden Antworten auf Anfragen zu dem Nutzen der Vorratsdatenspeicherung in Landtagen lassen ferner davon ausgehen, dass entsprechende statistische Erfassungen deshalb nicht vorgenommen worden sind und nicht vorgenommen werden,* ***weil sie als zu kostenträchtig angesehen werden***.“[8]

Mit anderen Worten heißt dies:

---

[5] Vgl. wissenschaftlicher Dienst des Deutschen Bundestages, Sachstandsbericht v. 18.03.2011, WD 7-3000-036/11.
[6] Vgl. wissenschaftlicher Dienst des Deutschen Bundestages, Rechtsgutachten v. 25.02.2011, WD 11-3000-18/11.
[7] Vgl. Gutachten Max-Planck-Institut (zweite erweiterte Fassung) Juli 2011, S. 120.
[8] Vgl. Gutachten Max-Planck-Institut (zweite erweiterte Fassung) Juli 2011, S. 218.

Obwohl keine gesicherten empirischen Erkenntnisse darüber vorliegen, ob mit der flächendeckenden Vorratsdatenspeicherung das Ziel der Gefahrenabwehr und der Strafverfolgung überhaupt erreicht werden kann, soll in das Grundrecht aus Art. 10 GG von 80 Millionen Bundesbürgerinnen und Bundesbürgern eingegriffen und die eine Demokratie ausmachende freie und offene Kommunikation gefährdet sowie das Risiko eines Datenmissbrauchs angelegt werden. Nochmal:

Nach der Rechtsprechung des Bundesverfassungsgerichts und des Europäischen Gerichtshofs muss die vorsorglich anlasslose Speicherung aller Telekommunikationsverkehrsdaten eine absolute Ausnahme bleiben, da sie – um es mit den Worten des Bundesverfassungsgerichts zu sagen – „*ein Gefühl des ständigen Überwachtwerdens hervorrufen kann; sie erlaubt in unvorhersehbarer Weise tiefe Einblicke in das Privatleben, ohne dass der Rückgriff auf die Daten für den Bürger unmittelbar spürbar oder ersichtlich ist. Der Einzelne weiß nicht, was welche staatliche Behörde über ihn weiß, weiß aber, dass die Behörden vieles, auch höchstpersönliches über ihn wissen können*“[9]. Wiegt ein Eingriff derart schwer, ist es die vornehmliche Pflicht des Gesetzgebers, den Bürgerinnen und Bürgern die sachlichen Gründe darzutun, die es aus seiner Sicht rechtfertigen sollen, Grundrechte des Einzelnen auszuhöhlen. Sieht der Gesetzgeber hiervon ab – etwa weil ihm die dafür erforderlichen statistischen Erfassungen zu kostenträchtig sind und/oder die damit einhergehende Transparenz nicht willkommen ist –, haben schwerwiegende Eingriffe in die Grundrechte der Bürgerinnen und Bürger zu unterbleiben. Sie sind unverhältnismäßig, zumal folgendes noch hinzukommt:

Für diejenigen, die sich der Datenüberwachung entziehen wollen, gibt es zahlreiche Möglichkeiten, eine Überwachung durch Vorratsdatenspeicherung zu umgehen – sei es durch gestohlene Prepaid- oder SIM-Karten oder durch Nutzung offener W-LAN-Netze oder öffentlicher Netzzugänge, bei denen die

[9] *BVerfG* NJW 2010, 833.

IP-Adresse nicht einer einzelnen Person zugeordnet werden kann. Auf der anderen Seite verfügen Strafverfolgungsbehörden über neue Ermittlungsansätze – etwa das Auslesen von Datenträgern, die der Kommunikation zwischen Mensch und Maschine dienen, beispielsweise SIM-Karten, die in einer Vielzahl von technischen Geräten vorzufinden sind (z. B. in Navigationsgeräten, Geräten zum Aufspielen von Programmen zur Fehlersuche oder für Updates in Kraftfahrzeugen). Werden Computer zu Zahlungszwecken eingesetzt, können über die so gespeicherten Daten retrograde Bewegungsbilder erstellt werden. Wissenschaftler untersuchen zudem, ob über den Akku-Status des Mobiltelefons dessen Standort ermittelt werden kann. Mit anderen Worten: Zur Erreichung des hier in Rede stehenden Zwecks kann es mildere Mittel als die Vorratsdatenspeicherung geben. Jedenfalls muss dies aufgeklärt werden, bevor von der Regel abgewichen und eine Ausnahme statuiert wird, mit der höchstpersönliche Daten von Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte[10], gespeichert und dadurch die Möglichkeit geschaffen wird, sehr genaue Schlüsse auf das Privatleben unbescholtener Bürgerinnen und Bürger, mithin auf Gewohnheiten des täglichen Lebens, Aufenthaltsorte, ausgeübte Tätigkeiten und soziale Beziehungen zu ziehen.

II.

Unzureichender Schutz der Berufsgeheimnisträger

Berufsgeheimnisträger sind durch die Vorratsdatenspeicherung besonders betroffen, ihre Arbeit ist auf Vertraulichkeit angelegt. Die „Vorratsdatenspeicherung“ schafft aber gerade das Gegenteil von Vertrauen: Kontrolle. Kontrolle der Datenströme, die die technischen Endgeräte mannigfaltig produzieren sowie Kontrolle der Personen – und damit auch der Berufsgeheimnisträger – die die Datenströme verursachen.

[10] Vgl. *EuGH* U. v. 08.04.2014, 1-25; verbundene Rechtssache C-293/12 und C-594/12.

Der Referentenentwurf wirft gerade in Bezug auf Berufsgeheimnisträger besondere Probleme auf:

Ein effektiver Schutz eines engen Kreises von auf besondere Vertraulichkeit angewiesenen Berufsgeheimnisträgern bereits auf Datenerhebungsebene wie bei anderen Überwachungsmaßnahmen ist bei der Vorratsdatenspeicherung schwierig, da sie eben schon begrifflich anlasslos ist und damit kraft Natur keine vorherige Befassung im Einzelfall ermöglicht. Für – die praktisch ganz überwiegend verwandten – dynamischen IP-Adressen soll dies schon in technischer Hinsicht gelten; Simitis und Spiecker haben deutliche Zweifel daran geäußert, ob dieses Argument wirklich hieb- und stichfest ist (Simitis/Spiecker, A Never-Ending Story, Beitrag vom 5.5.2015, http://www.verfassungsblog.de/a-never-ending-story-die-vorratsdatenspeicherung/).

Dem Schutz des Berufsgeheimnisses soll lediglich dadurch Rechnung getragen werden, dass die Verkehrsdaten von Berufsgeheimnisträgern nicht *abgerufen* werden dürfen, mithin einem Schutz erst auf Verwertungsebene. Dies steht nicht im Einklang mit dem Schutz von Berufsgeheimnisträgern, wie er in den § 97 StPO und § 160a StPO normiert ist, welche einen Schutz von Berufsgeheimnisträgern bereits auf der Erhebungsebene vorsehen. Ausweislich der Gesetzgebungsmaterialien gerade zu § 160a StPO ist ein solcher absoluter Schutz im Hinblick auf die Anwaltschaft geboten, um die Gewährleistung ausreichender Verteidigungsrechte, welchen von Verfassung wegen besondere Bedeutung zu kommt, zu garantieren. Die Verfasser des Referentenentwurfes ziehen mithin den falschen Schluss: Weil es technisch – angeblich – im Regelfall nicht anders geht, will es Berufsgeheimnisträger erst auf der Verwertungsebene schützen. Dabei kann letztlich nur durch den Verzicht auf die Vorratsdatenspeicherung effektiv gewährleistet werden, dass die Verteidigungsrechte nicht beeinträchtigt werden.

Alternativ muss der Schutz des Berufsgeheimnisses bereits bei einem Datenabgleich erfolgen, also auf Erhebungsebene. Hier sind Vorkehrungen zu treffen, die „Treffer" in geschützter Kommunikation vermeiden. Auf diese Weise lässt sich eine „Identifizierung" geschützter Kommunikation im Vorfeld eines Grundrechtseingriffs erreichen. Konkret bedeutet dies, dass bei der Programmierung des Datenabgleichs Negativmerkmale zu verwenden sind (Telefonnummern, Mailadressen, Suchbegriffe), die es in größtmöglichem Umfang ausschließen, dass anwaltliche Kommunikation in „Trefferlisten" aufscheint. Gegen ein derartiges „Identifizierungsgebot" lässt sich nicht einwenden, dass dies eine gezielte Suche nach geschützter Kommunikation bedingt und somit Grundrechtseingriffe fördert bzw. intensiviert. Die „Identifizierung" ist typischerweise möglich, ohne Kenntnis vom Inhalt der Kommunikation zu nehmen. Bei der Briefpost lässt sich die „Identifizierung" regelmäßig anhand der Absender- und Empfängerangaben vornehmen, die sich auf dem Briefumschlag befinden. Beim Abhören lässt sich die „Identifikation" zumeist anhand der beteiligten Rufnummern erreichen. Die „Identifizierung" erfordert somit keinen intensiven Grundrechtseingriffs und kann im „Vorfeld" eines Grundrechtseingriffs erfolgen.

Die Bedeutung von Beweiserhebungsverboten im Vorfeld bloßer Verwertungsverbote kann aber nicht hoch genug geschätzt werden: Was gespeichert ist, wird auch wahrgenommen, kann in den Akten erfasst werden und letztlich auch inhaltlich Eingang in Verfahren finden; auch wenn diese Informationen im Ergebnis nicht verwertet werden dürfen, erhöht allein dieser Umstand jenseits aller juristischen Dogmatik und ggf. unter Begründungsakrobatik die Gefahr, dass jene auf die ein oder andere Art ihren Eingang ins Verfahren finden. Genau vor diesem Hintergrund hat der Gesetzgeber in der jüngeren Gesetzgebung, insbesondere im Telekommunikationsneuregelungsgesetz vom 21.12.2007 (TKÜN-RegG, BGBl. I, 3198) etwa in § 100a Abs. 4 S. 1 StPO und § 160a Abs. 1 S. 1 StPO wie schon zuvor in § 100c Abs. 4 S. 1 StPO den Grundrechtsschutz durch ein Beweis*erhebungs*verbot sichergestellt.

Gerade das Urteil des EuGH zur Richtlinie über die Vorratsdatenspeicherung zeigt überdies auf, dass den Berufsgeheimnisträgern besonderer Schutz zu kommen muss. Der EuGH geht nämlich davon aus, dass eine europarechtskonforme Richtlinie Berufsgeheimnisträger von der Vorratsdatenspeicherung ausnimmt und letztere für Berufsgeheimnisträger gar nicht gelten soll. Insbesondere wenn man diese Äußerung in den Kontext der sehr hohen datenschutzrechtlichen Anforderungen durch den EuGH (wie auch durch das BVerfG) setzt, genügt die „neue“ Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten gerade nicht den Vorgaben der Rechtsprechung. Denn wenn man die Daten dem EuGH zufolge gar nicht erst speichern soll, bedeutet dies begrifflich notwendig, sie gar nicht erst zu erheben. Ein Schutz auf Verwertungsebene dürfte daher jedenfalls nach der Rechtsprechung des EuGH unzureichend sein.

Hinzu kommt, dass ein Abrufverbot immer nur auf der Seite des Berufsgeheimnisträgers greift: Ein Abruf der Einzelverbindungsdaten der Anwaltskanzlei lässt sich gesetzlich verbieten.

Ins Leere geht dagegen ein Abrufverbot, wenn der Abruf beim Mandanten erfolgt. Durch einen solchen Abruf beim Mandanten/Normalbürger können staatliche Stellen trotz eines Abrufverbots ohne weiteres herausfinden, wann, wie oft und wie lange der Bürger mit seinem Anwalt (und mit seinem Arzt, Seelsorger, Steuerberater und Journalisten) telefoniert hat.

III.

Datenschutzrechtliche Probleme

1. IP-Adressen

Mit Urteil vom 8. April 2014 hat die Große Kammer des Europäischen Gerichtshofs die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rats vom 15. März 2006 über die Vorratsspeicherung von Daten für ungültig erklärt. Maßgeblich hat sich das Gericht dabei auf die Unvereinbarkeit der Richtlinie mit Art. 7, 8, 52 Abs. 1 EU-Grundrechtecharta (GRCh) gestützt. Weiter gehend als das Bundesverfassungsgericht hat der EuGH der anlasslosen Speicherung von Daten eine Absage erteilt.

Das Urteil des EuGH ist in zweifacher Hinsicht von Bedeutung für das Thema Vorratsdatenspeicherung. Zum einen klärt es erstmals das Verhältnis der Art. 7 und 8 der GRCh zueinander. Nach Auffassung des EuGH wurde durch die Richtlinie gleichrangig in beide Grundrechte auf Datenschutz und Privatsphäre in schwerwiegender Weise eingegriffen. Zum anderen verbindet es die Rechtsordnung der EU und des Europarates dadurch, dass es eine parallele Auslegung der Rechte auf Datenschutz und Privatsphäre in Europa vornimmt und in diesem Zusammenhang (erstmals) im Hinblick auf die Vorratsdatenspeicherung mehrfach auf Entscheidung des EGMR zu Datenschutz und Datensammlungen Bezug nimmt.[11]

Der Klageweg gegen bestehende mitgliedstaatliche Vorratsdatenspeicherungsgesetze ist somit in verschiedenen Konstellationen eröffnet. Als Anrufungsgrund der nationalen Verfassungsgerichte kommt Art. 15 der ePrivacy-RL in Betracht, der bestimmt, dass die nationalen Vorratsdatenspeichergesetze dem EU-Recht unterliegen und damit auch im Hinblick auf die Art. 7, 8 und 52 (1) der Charta überprüfbar sind. Die Auslegung der GRCh durch den EuGH wird durch die vorliegende Entscheidung auch zum Maßstab generell für die Rechtmäßigkeit des nationalen Rechts im Hinblick auf jedwede staatlichen

[11] Urteil EuGH Rn. 47, 54 und 55.

Überwachungssysteme. Klagen von Privatpersonen gegen ihre Provider oder den Staat wären möglich. Auch der Provider könnte ein Interesse an der Abschaffung der ihm auferlegten Speicherpflicht haben. Als Individualbeschwerde wäre der Weg zum EGMR nach Straßburg möglich.[12]

Auch der Bundesgerichtshof sieht Klärungsbedarf in europarechtlicher Hinsicht: Der BGH hat dem EuGH unter dem 28. Oktober 2014 die Frage vorgelegt, ob die – nicht zuletzt für die Vorratsdatenspeicherung elementar bedeutsame – Speicherung der IP-Adressen durch Telekommunikationsdiensteanbieter über den jeweiligen Nutzungsvorgang hinaus mit der EG-Datenschutz-Richtlinie zu vereinbaren ist. In der Konsequenz bedeutet dies, dass der EuGH nunmehr auch über die grundsätzliche Frage zu entscheiden haben wird, ob es sich bei der IP-Adresse um ein vom Datenschutzrecht geschütztes personenbezogenes Datum handelte. Das aber wiederum hat Auswirkungen auf die Zulässigkeit der Vorratsdatenspeicherung, insbesondere bezüglich der IP-Adressen. Jedenfalls hat der EuGH in seiner Entscheidung vom 8. April 2014 die IP-Adressen zu den schützenswerten Daten gezählt.

Hinzukommt folgende Problematik:

Im Kontext der Vorratsdatenspeicherung dürften IP-Adressen allerdings immer personenbezogene Daten sein: Denn die Pflicht zur Speicherung dieser Daten trifft den Provider, also denjenigen, der die Internetverbindung für den User herstellt, mit diesem also in einem entsprechenden Vertragsverhältnis steht und dem damit zwingend dessen Identität bekannt ist. Stellt man auf den Provider als verantwortliche Stelle nach § 3 Abs. 7 BDSG ab, handelt es sich also stets um personenbezogene Daten, die er – im Falle einer anlasslosen Erhebung und Speicherung – zwecklos erhebt und speichert.

[12] Das Straßburger Gericht hat sich mit Fragen der Überwachung bereits mehrfach befasst: S and Marper v. United Kingdom [GC], nos 30562/04 und 30566/04, ECHR 2008-V; Liberty and Others v. United Kingdom, no 58243/00, s. LIBE-lang, Fn. 41.

Dies widerspricht nicht nur den oben dargestellten verfassungsrechtlichen Vorgaben, insbesondere dem Verhältnismäßigkeitsgrundsatz, sondern auch dem das Datenschutzrecht beherrschenden Zweckbindungsgrundsatz. Dieser wird auch in der Entscheidung des EuGH zur Vorratsdatenspeicherung in Rn. 59 ausdrücklich aufgegriffen. Dort heißt es:

> *„Zum anderen soll die Richtlinie zwar zur Bekämpfung schwerer Kriminalität beitragen, verlangt aber keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit; insbesondere beschränkt sie die Vorratsspeicherung weder auf die Daten eines bestimmten Zeitraums und/oder eines bestimmten geografischen Gebiets und/oder eines bestimmten Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten.“*

Der EuGH fordert also einen spezifischen Zusammenhang zwischen den erhobenen Daten und der Zweckverfolgung zur Bekämpfung schwerer Kriminalität, insbesondere eine Beschränkung der Daten auf die *„Daten eines bestimmten Zeitraums und/oder eines bestimmten geografischen Gebiets und/oder eines bestimmten Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte.“*

Eine solche Beschränkung, die aber Grundvoraussetzung für einen rechtmäßigen und verhältnismäßigen Grundrechtseingriff ist, sehen weder die Leitlinien noch der Referentenentwurf vor. Hier bestehen also erhebliche (schwer behebbare) Mängel.

Ferner ist folgendes zu beachten:

IP-Adressen sind dem Anschlussinhaber zugeordnet. Derjenige User, der über den Anschluss das Internet verwendet, muss aber nicht notwendigerweise der Anschlussinhaber sein. Bei den wohl in Deutschland

am häufigsten anzufindenden privaten DSL-Anschlüssen ist Anschlussinhaber vielmehr oft eine andere Person (etwa ein Elternteil, der Hauptmieter, etc.), Nutzer also andere und zum Teil viele weitere Personen, etwa bei offenen WLAN-Zugängen, Internetcafes, etc.

Eine Zuordnung zu bestimmten Nutzerrechnern (etwa eines Hotelgasts, der über das Hotel-WLAN das Internet verwendet) erfolgt dabei allenfalls intern.

Erfasst werden in solchen Fällen also regelmäßig die Daten der „falschen“ Personen, nämlich nicht derjenigen, die kommunizieren, sondern der, die „nur“ die Technik dazu zur Verfügung stellen. Es erscheint zunächst zweifelhaft, ob diese „falschen“ Daten polizeilich überhaupt sinnvoll verwendet werden können.

Darüber hinaus widerspricht auch dies den Anforderungen des EuGH, wonach ein Bezug zu Personen gefordert wird, die Anlass zur Strafverfolgung geben, siehe Rn. 58:

> „*Die Richtlinie 2006/24 betrifft nämlich zum einen in umfassender Weise alle Personen, die elektronische Kommunikationsdienste nutzen, ohne dass sich jedoch die Personen, deren Daten auf Vorrat gespeichert werden, auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte. Sie gilt also auch für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte.“*

Zu beachten ist ferner, dass man im Zeitpunkt der Erhebung und Speicherung einer IP-Adresse dieser nicht ansieht, zu welchen Zwecken der betroffene Internet-User die Internetverbindung hergestellt hat: Dies kann etwa zum „Surfen“ sein, für die Internettelefonie, aber auch zum Versand von Emails oder zur Nutzung von Messenger-Diensten.

§ 113b-E sieht in Absatz 5 folgendes vor:

„Der Inhalt der Kommunikation, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post dürfen auf Grund dieser Vorschrift nicht gespeichert werden.“

Zu Daten der elektronischen Post gehört aber auch und gerade die IP-Adresse des Absenders (und Empfängers). Diese findet sich auch in aller Regel in einer versandten Email selbst (im sog. Header).

Wenn aber bei Aufbau und auch Nutzung einer Internetverbindung nicht klar ist, wozu diese verwendet wird, zugleich keine Daten, die die Nutzung elektronischer Post betreffen dürfen, verwendet werden sollen, heißt das, dass überhaupt keine Daten auf Vorrat erfasst werden dürfen, denn es könnte sich um Daten der Nutzung von elektronischer Post handeln.

2. Ins Leere laufende Ausnahme der elektronischen Post

Die vorgenannte Ausnahme im Referentenentwurf, Daten der Dienste der elektronischen Post auszunehmen, liefe zudem faktisch ins Leere und würde den Eingriff nicht weniger intensiv oder gar verhältnismäßig machen:

Zwar sollen die Daten der Dienste von elektronischer Post nicht erfasst werden, sehr wohl aber alle andere Formen der Kommunikation, also auch – und dies sogar ausdrücklich, siehe Anlage 1 der Leitlinie, dort bei den Telefondiensten am Ende – SMS, MMS und „ähnliche Nachrichten“.

Damit ist unklar, ob die aktuellen Kommunikationsformen wie die Nutzung von Messengers auf Mobilgeräten, Skype, Chats, Foren, IRC, etc. erfasst sind oder nicht.

Die Herausnahme (zumindest) der Email-Kommunikation minimiert zwar für sich genommen die Eingriffsintensität, ist bei weitem aber nicht ausreichend, wenn in Form von „ähnlichen Nachrichten“ vergleichbare Kommunikation doch beinhaltet sein soll. Dies gilt besonders deshalb, weil zumindest im Bereich der Privatkommunikation Messengerdienste E-Mails zunehmend ersetzen und funktional Dienste der elektronischen Post darstellen (dazu ausführlich: Stellungnahme 55/13 des DAV durch den Ausschuss

Informationsrecht zur Anwendung des TKG auf neue Kommunikationsplattformen (bspw. Whats App) v. 13.12.2013).

Ähnliches gilt für die vorgesehene Ausnahme hinsichtlich des Speicherns von Internetseiten, die aufgerufen werden: Denn der Aufruf selbst soll zwar nicht gespeichert werden, kann aber – sofern anderweitig erfasst – über die http-Anfrage zugeordnet werden. Ohne die Vorratsdatenspeicherung wäre genau dies nicht möglich.

3. Metadaten – aussagekräftiger als Inhaltsdaten

Der offenbar verfolgten Argumentationslinie, dass über die Ausnahme der Nichtspeicherung von Inhaltsdaten die Eingriffsintensität reduziert werde, ist falsch.

Denn diese Argumentation übersieht, dass Verkehrsdaten und vor allem deren Kombination oftmals aufschlussreicher als die Inhalte selbst sind, da Verkehrsdaten einerseits – anders als Inhaltsdaten – von Anfang an als strukturierte Daten (also in einem bestimmten und definierten Format vorliegend) sehr viel leichter automatisiert auswertbar sind und andererseits über die Kombination der Verkehrsdaten sehr einfach Strukturen und Zusammenhänge erfasst werden können und sich durch einfache Algorithmen eine um ein Vielfaches effektivere Auswertung und damit auch Verwertungsmöglichkeit ergibt.

Mit den schon heute vorhandenen Methoden des Data Mining und der im Rahmen der technischen Disziplin der „Business Intelligence“ entwickelten Methoden zum Entdecken von Mustern in Datenbeständen ist es ein Leichtes, aus den Verkehrsdaten und deren Kombination zukünftiges Verhalten vorauszuberechnen (sog. „predictive analytics“).[13]

Die Erhebung „nur“ von Verkehrsdaten stellt also kein „weniger“ als die Erhebung von Inhaltsdaten dar, sondern einen genauso intensiven, wenn nicht sogar noch intensiveren Grundrechtseingriff.

---

[13] Siehe mit einem guten Überblick, http://en.wikipedia.org/wiki/Predictive_analytics).

4. Standortdaten

Bei Blick auf die Standortdaten kann auch der Argumentation dazu nicht gefolgt werden, wonach nur einzelne Standortdaten abgerufen werden dürfen. Denn nach dem Referentenentwurf soll § 113b-Ein Absatz 4 folgende Regelung enthalten:

> *„Bezeichnung der Funkzelle, die durch den anrufenden und angerufenen Anschluss bei Beginn der Verbindung genutzt werden."*

Was aber ist mit „Verbindung" gemeint? Da es aus dem Kontext der Leitlinien heraus ausdrücklich auch um Verbindungen in das Internet geht, kann dies also heißen, dass bei jeder Verbindungsaufnahme eines mobilen Geräts der Standort erfasst und gespeichert wird, was alle paar Sekunden der Fall sein kann. Insofern würden sehr exakte Bewegungsprofile im Rahmen der Vorratsdatenspeicherung erstellt.

Aber selbst wenn man nur den Beginn eines Telefongesprächs erfassen würde (mit der Schwierigkeit, ein solches überhaupt von einer Internetverbindung abgrenzen zu können), ergäbe sich bei einer Speicherdauer von 4 Wochen ein sehr umfassendes Bewegungsprofil.

Die Regelung, die auf die erste Aktivierung von Diensten abstellt, ebenso die Bezeichnung der Funkzelle, wenn Dienste im Voraus bezahlt werden, ist zudem unklar. Wie soll festgestellt werden, was eine „erste" Aktivierung ist? Dazu müsste auch dieses Datum erhoben und gespeichert werden, was aktuell aber gemäß der Liste in Anlage 1 nicht vorgesehen ist.

Auch aus diesen genannten Gründen ist eine Erhebung und Speicherung schon nicht verhältnismäßig.

5. Datenspeicherung nur in der EU

Der Kritik des EuGH an der EU-Richtlinie, wonach nicht festgelegt war, dass die Daten innerhalb der EU gespeichert werden müssen, um eine unabhängige Kontrolle zu garantieren, ist vollständig zu folgen.

Diese Vorgabe greifen Leitlinien und Referentenentwurf zwar auf und betonen diesen Umstand. Es ist jedoch zu bezweifeln, dass dies viel nützt. Denn die Tendenz der US-Gerichte scheint dahin zu gehen, US-Anbieter (in einem konkreten Fall: Microsoft) zu verurteilen, auch Auskunft gegenüber den US-Behörden für in der EU gespeicherte Daten erteilen zu müssen (Urteil vom 5. April 2014, United States District Court des Southern District of New York).

Zumindest für Provider, die – auch – US-Bezug haben, dürfte ähnliches zu erwarten sein. Die vom EuGH und den europäischen Datenschutzregelungen ganz essenziell geforderte unabhängige Kontrolle wäre damit nicht nur unterlaufen, sondern ausgehebelt.

Dies ist zwar ein generelles Problem, das aber die Vorratsdatenspeicherung noch deutlich verstärken würde: Denn Daten, die nicht gespeichert sind, kann auch ein US-Provider einer US-Behörde nicht herausgeben.

6. Datensicherheit

Eine weitere Kritik des EuGH war, dass kein spezieller Schutz aus technischer und organisatorischer Sicht für die gespeicherten Daten in der EU-RL vorgesehen war.

Auch diesen Gedanken greifen die Richtlinien auf und sehen vor, dass „*die nach dem Stand der Technik höchstmögliche Sicherheit der Daten“* zu gewährleisten ist.

Was soll dieser Stand aber sein?

Die Speicherung von Daten in einem Hochsicherheitsrechenzentrum in einem Bergwerk mit 365/24/7 Bewachung durch schwer bewaffnetes Wachpersonal? Der Serverraum in einem normalen Rechenzentrum?

Der Referentenentwurf und die Leitlinien nennen zwar einige grundsätzlich erforderliche Maßnahmen, bleiben aber viel zu vage.

Der Ansatz der Leitlinien, auch den physikalischen Schutz der Daten vorzuschreiben, ist zwar richtig, die insofern genannten Punkte zur Datensicherheit sind aber schon heute für ganz „normale“ Daten Standard.

Dem Umstand, die über die Erhebung der Verkehrsdaten von 80 Millionen Deutschen über 10 Wochen (und über 4 Wochen bei Standortdaten) anfallende beispielslose Datenmasse in besonderer Weise zu schützen, werden diese Maßnahmen keineswegs gerecht.

Zu einer Minimierung des schon *durch die Erhebung* (!) erfolgenden Grundrechtseingriffs können Maßnahmen, die die *spätere Speicherung* betreffen, ohnehin nicht beitragen.

Selbst bei der Speicherung verringern sie die Eingriffsintensität nicht: Denn sie dienen dem Schutz vor Missbrauch, der selbstverständlich wichtig ist. Der unzulässige Grundrechtseingriff liegt aber nicht (erst) im Missbrauch, sondern schon im rechtmäßigen Zugriff.

Eine gute technische Absicherung minimiert diesen Eingriff nicht und kann ihn auch nie legitimieren.

Aus demselben Grund ist zwar begrüßenswert, bei Verstößen gegen die Vorgaben zur Datensicherheit Sanktionen zu verhängen. Dann aber wäre es aber einerseits dem verfassungsrechtlichen Bestimmtheitsgebot nach nötig, die Datensicherheitsmaßnahmen sehr konkret vorzugeben, die aktuelle Auflistung von nur generischen Vorgaben reicht nicht aus.

Andererseits kann aber auch hier eine *spätere* Sanktion bei Nichtbeachtung von Vorgaben nie einen *zuvor* erfolgenden Grundrechtsverstoß legitimieren.

Auffallend ist ferner, dass auch bei einer längeren Speicherung als die festgelegte Speicherfrist die TK-Anbieter zwar sanktioniert werden sollen, allerdings keine Regelung insoweit besteht, dass nach dem Überschreiten der Höchstfrist länger vorgehaltene Daten nicht mehr abgerufen werden dürfen und – wenn doch – ein Beweiserhebungs- und Beweisverwertungsverbot bestehen muss.

Verstoßen die TK-Anbieter damit gegen die geplante Regelung, geschieht das damit sogar regelmäßig im Sinne der Strafverfolgungsbehörden.

Alles in allem kann aus datenschutzrechtlicher Sicht der Referentenentwurf nicht überzeugen, ganz im Gegenteil: Er hält in vielerlei Hinsicht die Vorgaben des EuGH nicht ein.

IV.

Einführung eines Tatbestandes der „Datenhehlerei“ (§ 202d-E)

Die mit dem Entwurf vorgeschlagene Einführung eines Tatbestandes der „Datenhehlerei“ (§ 202d-E) geht auf einen Bundesratsentwurf zurück (BT-Drs. 17/14362 vom 10.07.2013), der jedoch nie zur Abstimmung gelangte. Der jetzige Vorschlag weist in der tatbestandlichen Ausgestaltung erhebliche Abweichungen auf.

Die Notwendigkeit einer neuen Regelung wird 2013 wie heute mit dem Bestehen einer Strafbarkeitslücke begründet. Gegen die Existenz einer solchen Strafbarkeitslücke spricht, dass die Zahl der in der polizeilichen Kriminalstatistik registrierten Verfahren wegen eines Verstoßes gegen §§ 44, 43 BDSG extrem gering und auf diesem geringen Niveau zusätzlich seit Jahren rückläufig ist (erfasst werden „Straftaten gegen das Bundesdatenschutzgesetz“. 2010 wurden 748 Fälle registriert, 2011 noch 571 Fälle und 2012 nur noch 479 Fälle). Es wird also von der bisher bestehenden Strafnorm kaum Gebrauch gemacht. Soweit der Entwurf sich auf statistische Erhebungen stützt, handelt es sich nur um Daten über das

Begehungsaufkommen der *Vortaten (*§§ 202a und b StGB*).* Hier ist tatsächlich ein starker Anstieg zu verzeichnen. Dies mag Veranlassung dafür geben, diese Tatbestände zu ergänzen und die Strafdrohungen zu erhöhen. Für die Notwendigkeit der Pönalisierung von „Datenhehlerei“ lässt sich daraus wenig ableiten.

§ 202 Abs. 3 StGB-E sieht vor, dass *Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher und beruflicher Pflichten dienen* nicht von dem Tatbestand erfasst werden. Dazu gehörten *insbesondere solche Handlungen von Amtsträgern oder deren Beauftragten, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden sollen.*

Damit unternimmt es die Bundesregierung – an verborgener Stelle eines Gesetzentwurfes, dessen Überschrift insinuiert, es gehe um Datenspeicherfristen – staatlichen Stellen die Früchte illegaler Datenerhebungen zu sichern. Dies wäre angesichts des bekannt gewordenen Verdachts systematischer Ausspähung von Bürgern, Unternehmen und Amtsträgern durch (ausländische) staatliche Stellen ein fatales Signal. Zu dem vorgeblichen Zweck des neuen Straftatbestandes, das formelle Datengeheimnis vor einer Fortsetzung und Vertiefung seiner durch eine vorausgegangene Straftat erfolgten Verletzung zu schützen, steht dies in einem grotesken Widerspruch.

Die Entwurfsbegründung gibt vor, mit der Regelung, wonach Handlungen von der Strafbarkeit ausgenommen sind, die „ausschließlich der Erfüllung rechtmäßiger dienstlicher und *beruflicher* Pflichten dienen“ sollten nicht nur Amtsträger, sondern u. a. auch Journalisten vor Strafverfolgung geschützt werden (vgl. S. 54 d. Entwurfsbegründung). Ob von dieser sprachlichen Wendung aber auch tatsächlich ein Schutz für Angehörige dieser

Berufsgruppe ausgeht, darf bezweifelt werden. Auch bei der wortgleichen Regelung des § 184b Abs.5 StGB (Ausnahmen von der Strafbarkeit des Besitzes kinderpornographischer Materialen) ist es umstritten, ob Journalisten tatsächlich aus dem Anwendungsbereich ausgenommen sind. Es stellt sich schon die Frage, was „berufliche *Pflichten*“ eines Journalisten seien sollen. Besonders problematisch erscheint aber, dass nach der Entwurfsbegründung nur die journalistische Tätigkeiten *in Vorbereitung einer konkreten Veröffentlichung* von der Strafbarkeit ausgenommen sein soll. Dies dürfte mit den im Medienbetrieb üblichen Arbeitsweisen nicht in Einklang zu bringen sein. Ein Journalist, der Daten zugespielt bekommt, kann naturgemäß erst nach der Sichtung des Datenbestandes beurteilen, ob daraus eine Veröffentlichung werden kann bzw. soll. Strafbar hätte er sich dann aber womöglich schon gemacht. Hier ist eine Klarstellung unbedingt notwendig um die Arbeit kritischer Medien zu schützen.

V.

Kosten

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 2.3.2010 die derzeitige Regelung, dass nur die Abrufkosten und nicht die Investitionskosten den Telekommunikationsunternehmen erstattet werden, nicht beanstandet.[14] Hierdurch steht allerdings zu befürchten, dass die Auswahl der Sicherheitstechnologie anhand der jeweiligen Kosten bestimmt wird. Aufgrund der hohen sicherheitstechnischen Anforderungen ist mit deutlich höheren Investitions- und Betriebskosten zu rechnen, als dies die in den Jahren 2008 bis 2010 bestehende Datenspeicherungspflicht ausgelöst habe.[15]

Im Einzelnen:

- Anspruchsvolleres Verschlüsselungsverfahren bedeutet für viele Anbieter die Anschaffung neuer Software

[14] BVerfG v. 2.3.2010 – 1 BvR 256/08, 263/08/, 586/08 (Rn. 302).
[15] *Moser-Knierim*, Vorratsdatenspeicherung: Zwischen Überwachungsstaat und Terrorabwehr, S. 351.

- Gesonderte „Speichereinrichtungen“, d.h. neue Hardware bzw. Speichermedien in exorbitantem Umfang
- „revisionssichere Protokollierung“, d.h. mehr Personalaufwand und ggf. neue Software zur Protokollierung
- „Vier-Augen-Prinzip“, d.h. ein deutlich erhöhter (besonders kostenintensiver) Personalaufwand.

Hierdurch werden erhebliche – einmalige wie auch dauerhaft wiederkehrende – Kosten entstehen.

Der Referentenentwurf sieht eine Entschädigung für die „Umsetzung der Speicherpflichten“, also der Investitionskosten vor, allerdings nur, wenn diese „erdrosselnde Wirkung“ haben; näher konkretisiert wird dies nicht. Unabhängig hiervon trägt letztlich der Bürger diese Kosten: Entweder als Nutzer des jeweiligen Providers, der die Kosten auf seine Kunden umlegen wird (so auch der Entwurfsverfasser, S. 31 d. Entwurfsbegründung), oder schlicht als Steuerzahler, sollte der Staat tatsächlich „einspringen“.

VI.

Erfahrungen in der Europäischen Union

Schließlich – und abschließend – sollten auch die Erfahrungen in der Europäischen Union mit nationaler Gesetzgebung zur Vorratsdatenspeicherung berücksichtigt werden. In den Niederlanden, Bulgarien und der Slowakei wurden die Gesetze zur Speicherung von Vorratsdaten im Jahr 2015 für nichtig erklärt, in Österreich, Rumänien und Slowenien bereits im Jahr 2014. In mehreren Mitgliedstaaten der Europäischen Union sind derzeit verfassungsrechtliche Verfahren zur nationalen Gesetzgebung zur Speicherung von Vorratsdaten anhängig.