Stellungnahme der Rechtsanwaltskammer Berlin

zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz für ein „Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“

BRAK-Nr. 227/2015

Verteiler:

- Bundesrechtsanwaltskammer
- Rechtsanwaltskammern im Bundesgebiet
- Vorstand des Deutschen Anwaltvereins
- Vereinigung Berliner Strafverteidiger e.V.
- Organisationsbüro der Strafverteidigervereinigungen
- Deutscher Richterbund - Landesverband Berlin e.V.
- Vereinigung Berliner Staatsanwälte e.V.
- Berliner Senatsverwaltung f. Justiz u. Verbraucherschutz
- Republikanischer Anwaltsverein

Berlin, 10.06.2015

Der Vorstand der Rechtsanwaltskammer Berlin nimmt auf der Grundlage der Diskussion in der Sitzung des Vorstands vom 10. Juni 2015 zu dem Referentenentwurf Stellung wie folgt:

Vorweg ist auf die Pressemeldung des Deutschen Instituts für Menschenrechte vom 27. Mai 2015 zu verweisen, in der es heißt:

„Die anlasslose Speicherung von Telekommunikationsverkehrsdaten ist ein besonders schwerer Eingriff in das Menschenrecht auf Privatsphäre. Selbst eine begrenzte Speicherdauer von nur vier Wochen ermöglicht im digitalen Zeitalter die Erstellung aussagekräftiger individueller Persönlichkeits- und Bewegungsprofile und die Aufdeckung gruppenbezogener Einflussstrukturen und Entscheidungsabläufe. Entsprechend hoch sind die Anforderungen, die das Bundesverfassungsgericht und der Europäische Gerichtshof an eine grundrechtskonforme Ausgestaltung des Instrumentes Vorratsdatenspeicherung stellen.“

Dem schließt sich die RAK-Berlin an. Der vorliegende Referentenentwurf wird den verfassungsrechtlich gebotenen Anforderungen nicht gerecht.

I. Eilbedürftigkeit

Am 15. März 2006 erließ das Europäische Parlament die Richtlinie 2006/24/EG zur Vorratsspeicherung von Daten, weshalb im Dezember 2007 vom Bundestag entsprechende gesetzliche Regelungen zur Vorratsdatenspeicherung beschlossen wurden. Das Bundesverfassungsgericht hat diese, insbesondere § 113a, b TKG und § 100g I 1 StPO mit seinem Urteil vom 2. März 2010 für nichtig erklärt. Über mehrere Jahre wurde daraufhin über die Einführung der Vorratsdatenspeicherung in der Politik heftig gestritten, bis der Gerichtshof der EU am 8. April 2014 die besagte Richtlinie für ungültig erklärt hat. Eine Verpflichtung zur Einführung einer Speicherpflicht besteht seither nicht mehr.

Im Hinblick auf die Historie und des Umstandes, dass über die Vorratsdatenspeicherung seit nunmehr 5 Jahren diskutiert wird, ist vollkommen unverständlich, dass von Seiten des BMJV der Referentenentwurf an die interessierten Verbände lediglich zur Kenntnisnahme übersandt wird, verbunden mit dem Hinweis, dass aufgrund „der großen Eilbedürftigkeit“ eine Kabinettsbefassung in Kürze erfolgen werde. Die Anhörung bzw. die Einholung einer Stellungnahme der interessierten Verbände ist offensichtlich nicht vorgesehen.

Angesichts der umfassenden Auswirkungen des Gesetzes auf alle Teile der Bevölkerung ist dieses Eilverfahren vollkommen inakzeptabel und muss in aller Schärfe beanstandet werden.

II. Erfüllungsaufwand

Indem die Telekommunikationsunternehmen verpflichtet werden, ihre Daten zu speichern, ist dies mit einem erheblichen zusätzlichen Aufwand verbunden, zumal die Telekommunikationsunternehmen gleichzeitig recht umfassend verpflichtet werden, die gespeicherten Daten zu sichern und die Datensicherheit und Datenqualität zu gewährleisten. Ferner entsteht ein zusätzlicher personeller und technischer Aufwand, indem die Telekommunikationsunternehmen die gespeicherten Daten bei Abfrage an die Strafverfolgungsbehörden kurzfristig und sicher übermitteln müssen. Es dürften ca. 1.000 Unternehmen betroffen sein. Der Referentenentwurf behauptet, dass der Aufwand derzeit nicht bezifferbar sei, da unklar sei, inwieweit die Investitionen zum Teil schon vorgenommen wurden und inwieweit die Verpflichteten gem. § 113a TKG Entschädigung verlangen könnten.

Der Referentenentwurf stellt dar, dass im Jahr 2007 der Branchenverband BITKOM erforderliche Investitionen in Höhe von **75 Mio. EUR** errechnete, hinzu kämen jährliche Betriebskosten in **zweistelliger Millionenhöhe**. Der Verband der Deutschen Internetwirtschaft e.V. (eco) hatte errechnet, dass die Internetwirtschaft Investitionen in Höhe von **300 Mio. EUR** in Technik zu investieren habe. Bei der Bundesnetzagentur wird mit einem Personalaufwand in Höhe von **2,9 Mio. EUR** gerechnet und für Sachmittel mit Kosten in Höhe von **150.000,00 EUR** im ersten Jahr. Diese geschätzten Kosten orientierten sich noch nicht an den inzwischen weit höheren Anforderungen an die Datensicherheit und Datenqualität, die also noch weit höhere Kosten verursachen werden.

Es ist davon auszugehen, dass der Aufwand zumindest von den größeren Telefonanbietern (die 98% des Marktes ausmachen) zu tragen sein wird. Lediglich die kleineren Unternehmen (2%) können sich ggf. auf die Härteregelung des § 113a TKG berufen. Selbst der Referentenentwurf geht davon aus, dass die betroffenen Unter-

nehmen die erhöhten Kosten einkalkulieren und an ihre Kunden weitergeben werden. Die Kosten der Speicherung wird also auf die Verbraucher durch höhere Telefongebühren umgelegt werden.

Die Aussage im Referentenentwurf, für die Bürgerinnen und Bürger entstehe kein Erfüllungsaufwand (siehe S. 31), ist also irreführend. Tatsächlich werden mittelbar die Bürgerinnen und Bürger die Kosten zu tragen haben, die dadurch entstehen, dass ihre Telekommunikationsdaten anlasslos gespeichert werden. Um es überspitzt zu formulieren: Die Bevölkerung zahlt, dass sie umfassend überwacht wird!

Bei den weiteren Kosten wird im Referentenentwurf behauptet, dass für die Kommunen und die Judikative kein nennenswerter Aufwand bzw. kein Erfüllungsaufwand entsteht. Auch hier sei eine transparente Darstellung angemahnt. Datenmassen, die erhoben werden, müssen ausgewertet werden, sonst sind sie sinnlos. Zu verschweigen, dass dies mit einem erhöhten technischen und personellen Aufwand einhergeht, ist irreführend.

III. Erforderlichkeit der Einführung einer Speicherpflicht

Der Referentenentwurf geht davon aus, dass die bestehenden Regelungen Daten zu erheben zu Lücken bei der Strafverfolgung und bei der Gefahrenabwehr führen. Diese Behauptung ist umstritten und bleibt ohne Beleg. Insbesondere der Vergleich des Zeitraumes, in dem in Deutschland die Vorratsdatenspeicherung erfolgte, nämlich Dezember 2007 bis März 2010 mit dem Zeitraum März 2010 bis heute wäre hier aussagekräftig, wird im Referentenentwurf jedoch nicht bemüht.

Auch wenn aussagekräftige Daten offenbar schwer zu erheben und auszuwerten sind, so sollten für den Beleg der These, die Lücken der Strafverfolgung seien durch eine Speicherpflicht zu schließen, aussagekräftige Forschungen erfolgen. Bisher beschränken sich die Verfechter einer Speicherpflicht auf plakative und nicht belegte Behauptungen. Auch der Referentenentwurf verhält sich bedauerlicherweise zu der Prüfung der Erforderlichkeit der Regelung nicht.

Das Max-Planck-Institut jedenfalls, das im Juli 2011 im Auftrag des Bundesamtes für Justiz ein Gutachten zu möglichen Schutzlücken durch den Wegfall der Vorratsdatenspeicherung erstellte, kam zu dem Ergebnis, dass *„nichts darauf hindeutet, dass durch die Zugriffsmöglichkeit auf Vorratsdaten, die im Jahr 2008 sowie im Jahr 2009 zur Verfügung standen, eine Veränderung der Tendenz“* der Aufklärungsquote erreicht wurde (Gutachten des Max-Planck-Instituts zu möglichen Schutzlücken durch den Wegfall der Vorratsdatenspeicherung vom Juli 2011, dort S. 121) und eine Veränderung der Aufklärungsquote im Jahr 2009/2010 nicht ersichtlich sei (a.a.O. S. 219). Der Vergleich der Aufklärungsquoten mit Ländern, in denen die Vorratsdatenspeicherung praktiziert wird, widerlegt ebenfalls die These, dass Aufklärungslücken bestehen. Es lassen sich keine Hinweise ableiten, dass die Vorratsdatenspeicherung zu einer systematischen höheren Aufklärung führe (a.a.O., S. 219).

Ohne Beleg bleibt auch die immer wieder bemühte Behauptung, die Vorratsdatenspeicherung reduziere eine etwaige Bedrohung durch (islamistische) Terroristen. Es liegen keinerlei Hinweise vor, dass auf Vorrat gespeicherte Verkehrsdaten in den letzten Jahren zu einer Verhinderung eines Terroranschlages geführt hätten (vgl. a.a.O. S. 219). Auch der Verweis auf die Anschläge auf die Redaktion Charlie Hebdo geht fehl, da in Frankreich die Vorratsdatenspeicherung praktiziert wird.

Die Aufklärungsquote der Delikte schwerster Kriminalität, um die es bei der Vorratsdatenspeicherung nur gehen kann, liegt dauerhaft im sehr hohem Bereich (i.d.R. über 80% teilweise bei über 95%). Es ist insoweit davon auszugehen, dass keine Lücken bei der Strafverfolgung bestehen, die eine neue Regelung notwendig machen. Effektiver wäre mit den erheblichen finanziellen Mitteln, die die Speicherpflicht erfordert, die Ermittlungsorgane auszustatten.

Für die Bekämpfung schwerster Kriminalität stehen somit effektivere und deutlich mildere Mittel zur Verfügung als die Speicherung von Kommunikationsdaten der gesamten Bevölkerung. Ferner ist zu bezweifeln, dass die vorgesehene Speicherpflicht ein geeignetes Mittel ist, um angebliche Ermittlungslücken zu schließen.

IV. Die einzelnen gesetzlichen Regelungen

1. § 100g I StPO-E

Durch § 100g I StPO wird die Erhebung der von den Telefondienstanbietern gespeicherten Daten möglich, sobald die Straftat mittels Telekommunikation begangen wurde. Schon das BVerfG hat in seinem Beschluss vom 02.03.2010, (BVerfGE 125, 260-385, zitiert bei juris dort Rdnr. 279) darauf hingewiesen, dass angesichts der fortschreitenden Bedeutung der Telekommunikation im Lebensalltag auf diese Weise der Regelung der Ausnahmecharakter genommen wird und praktisch jede Straftat hiervon umfasst ist. Auch wenn durch § 113c TKG-E eine weitere Einschränkung erfolgt, nämlich die Verfolgung besonders schwerer Straftaten, ist die Norm in der gegebenen Form nicht verhältnismäßig.

2. § 100g II StPO-E

Das BVerfG hat ausgeführt, dass der Rückgriff auf die Verbindungsdaten detaillierte Persönlichkeits- und Bewegungsprofile ermöglichen kann, weshalb die Erhebung dieser Daten grundsätzlich nicht geringer wiege, als eine inhaltsbezogene Telekommunikationsüberwachung (vgl. BVerfGE 125, 260-385, zitiert bei juris dort Rdnr. 227). Sie sei nur dann gerechtfertigt, wenn sie besonders hochrangigen Gemeinwohlinteressen diene. *„Eine Verwendung der Daten kommt deshalb nur für überragend wichtige Aufgaben des Rechtsgüterschutzes in Betracht, das heißt zur Ahndung von Straftaten, die überragend wichtige Rechtsgüter bedrohen oder zur Abwehr von Gefahren für solche Rechtsgüter.“* (siehe a.a.O Rdnr. 227)

Ferner legt das BVerfG fest, dass der Abruf der vorsorglich gespeicherten Daten *„nur zur Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr zugelassen werden darf*“ (siehe a.a.O. Rdnr. 232 unter Verweis auf BVerfGE 122, 120, 141 ff.)

Der Straftatenkatalog des § 100g II StPO-E entspricht diesen Vorgaben nicht. Auffällig sind beispielsweise

- Geldwäsche § 261 IV S.2 StGB bzw. Verschleierung unrechtmäßig erlangter Vermögenswerte im besonders schweren Fall, § 261 StGB
- das gewerbsmäßige Einschleusen von Ausländern gemäß § 96 II Aufenthaltsgesetz
- Verstöße gegen das Betäubungsmittelgesetz, beispielsweise
    - der gewerbsmäßige Handel mit Betäubungsmitteln,

    - o das illegale Verschreiben von Betäubungsmitteln,
    - o das Verschaffen der Gelegenheit zum unbefugten Erwerb oder Verbrauch von Betäubungsmitteln etc.
- der Verstoß gegen das Gesetz zur Überwachung des Verkehrs mit Grundstoffen, die für die unerlaubte Herstellung von Betäubungsmitteln missbraucht werden können (§ 19 Grundstoffüberwachungsgesetz GÜG)
- der besonders schwere Fall des Landfriedensbruchs §125a StGB,
- der räuberische Angriff auf Kraftfahrer, § 316a StGB

Bei allen Tatbeständen handelt es sich nicht um Straftaten gegen Leib, Leben oder Freiheit einer Person. Straftaten, deren Schutzgüter die öffentliche Ordnung, die Volksgesundheit oder Vermögenswerte sind, stellen keine schwerwiegenden Straftaten dar, die der Abwehr von Gefahren überragend wichtiger Rechtsgüter dienen. Nur schwerwiegende Straftaten rechtfertigen die anlasslose Speicherung, nicht etwa Straftaten, die lediglich von erheblicher Bedeutung sind (BVerfGE 125, 260-385, zitiert bei juris dort Rdnr. 279).

Zwar erwähnte das BVerfG auch Straftaten, bei denen die Telekommunikationsverkehrsdaten eine besondere Bedeutung haben. Der Referentenentwurf verweist insoweit darauf, dass bei bestimmten Straftaten „die gespeicherten Verkehrsdaten nach der kriminalistischen Erfahrung besonders wertvolle Dienste leisten konnten“ (vgl. S. 35 des RefE). Auch bezogen auf diese Straftaten muss es sich jedoch fraglos um schwerwiegende Straftaten handeln.

Anzumerken ist, dass auch gewisse Wertungswidersprüche nicht nachvollziehbar sind. Beispielsweise sind im Katalog Straftaten gegen die sexuelle Selbstbestimmung wie der schwere sexuelle Missbrauch von Kindern erfasst. Bei der Vergewaltigung sind jedoch nicht alle Alternativen des besonders schweren Falls (§177 II StGB) aufgenommen, sondern lediglich die Vergewaltigung, die von mehreren gemeinschaftlich begangen wurde. Gleiches gilt für den sexuellen Missbrauch Widerstandsunfähiger. Die besonders schwere Vergewaltigung ordnet in sämtlichen Fallkonstellationen, somit auch in den Fallkonstellationen, die im Katalog des Referentenentwurfs nicht erfasst werden, eine Freiheitsstrafe nicht unter zwei Jahren an, also eine weit höhere Strafandrohung als viele andere Delikte, die im Katalog erfasst sind, wie beispielsweise das Einschleusen von Ausländern, der besonders schwere Fall des Landfriedensbruchs oder der Geldwäsche.

3. § 100g IV StPO-E

Gem. § 100g IV StPO-E besteht ein Erhebungsverbot bzgl. der Zeugnisverweigerungsberechtigten gem. § 53 I 1 Nr. 1-5 StPO. Die Verbindungsdaten werden also gespeichert, dürfen aber nicht erhoben werden.

Die Anschlüsse von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen dürfen gem. § 113b VI TKG gar nicht erst gespeichert werden. Begründet wird dies damit, dass diese Personen einer besonderen Verschwiegenheitsverpflichtung unterliegen.

Unstrittig ermöglicht die Auswertung der gespeicherten Daten die Erstellung eines lückenlosen Bewegungsprofils. Dies birgt Gefahren in sich, die an anderer Stelle kompetent dargelegt wurden. Jeder Bürgerin und jedem Bürger muss es möglich sein, ohne dass dies erfasst wird, Kontakt zu einem Rechtsanwalt oder einer Rechts-

anwältin aufzunehmen. Allein das Bewusstsein der Speicherung dieser Kontaktaufnahme könnte dazu führen, dass Rechtsratsuchende die Kontaktaufnahme unterlassen.

Um dies zu verhindern reicht das im Referentenentwurf vorgesehene Erhebungsverbot nicht aus. Einerseits schützt es die Verbraucher nicht vor einem diffusen Gefühl der Überwachung durch Speicherung. Ferner schützt die Regelung nicht vor der bestehenden erheblichen Missbrauchsgefahr entweder durch die Ausspähung dieser Daten durch interessierte Stellen oder vor der rechtswidrigen Erhebung und Verwertung der Daten. Effektiv kann dem nur begegnet werden, indem der Missbrauch gar nicht erst ermöglicht wird. Insofern muss bereits die Speicherung der Verbindungsdaten mit Rechtsanwältinnen und Rechtsanwälten untersagt werden, nicht erst die Erhebung.

Dass dies technisch möglich ist, ergibt sich aus § 99 TKG und dem Speicherverbot der Anschlüsse sozialer Einrichtungen gem. § 113b VI TKG. Die unterschiedliche Behandlung der Geheimnisträger ist nicht zu rechtfertigen. Rechtsanwältinnen und Rechtsanwälte unterliegen ebenfalls der besonderen Verschwiegenheitsverpflichtung. Die Kommunikation gehört entsprechend den Vorgaben des BVerfG zu dem engen Kreis von auf besondere Vertraulichkeit angewiesenen Telekommunikationsverbindungen. Der Zugang zum Recht, der bereits durch die Speicherung beeinflusst werden könnte, ist ein überragendes Rechtsgut und besonders schutzwürdig.

Dies rechtfertigt den vom Referentenentwurf behaupteten höheren Aufwand, der dadurch entsteht, dass die Berufsgeheimnisträger gem. § 53 StPO in einer ständig zu aktualisierenden Liste geführt werden müssten. Im Übrigen gilt dies ebenso für die sozialen Einrichtungen und die dort beschäftigten Personen. Das behauptete Missbrauchsrisiko (S. 36 RefE) verträgt sich nicht mit dem Umstand, dass Rechtsanwälte und Rechtsanwältinnen Organe der Rechtspflege sind und muss scharf zurückgewiesen werden. Die Schlechterstellung von Rechtsanwälten gegenüber Sozialarbeitern u.ä. ist schlicht unvertretbar.

4. § 101a und b StPO-E

Die in § 101a und b StPO-E aufgenommenen Regelungen des sehr konkret ausgestalteten Richtervorbehalts und der Transparenz sowie Benachrichtigungspflichten entsprechen den Vorgaben des BVerfG und gehen weiter, als die Regelungen der Telefonüberwachung. Dies ist grundsätzlich zu begrüßen, auch wenn die bekannten Zweifel bestehen, ob der Richtervorbehalt angesichts der hoffnungslosen Überarbeitung und extrem hohen Fallzahlen der Ermittlungsrichter den Anforderungen einer Überwachung des Einsatzes der Erhebung genügen.

5. § 113d TKG-E

Nach § 113d TKG-E hat der Telefondienstleister sicherzustellen, dass die gespeicherten Daten gegen unbefugte Kenntnisnahme und Verwendung geschützt werden. Die umfangreichen Vorgaben zur Gewährleistung der Datensicherheit sind zu begrüßen. Ob sie umsetzbar und ausreichend sind, sollen qualifiziertere Stellen beurteilen. Ferner stellt sich die Frage nach einer effektiven Kontrolle der Umsetzung der Vorgaben.

V. Einführung der neuen Straftat § 202 d StPO-E, Datenhehlerei

Die Regelung unterliegt eklatanten Wertungswidersprüchen. Der Ankauf illegal erlangter Daten ist nicht strafbar, wenn man sich durch den Ankauf nicht bereichern will. Die staatliche Ausspähung illegal erlangter Daten fällt somit nicht unter § 202d StGB-E.

Die rechtliche Interessenwahrnehmung, die Medien inklusive beispielsweise der Internetforen und Blogger und teilweise auch die Politik sind jedoch in bestimmten Fallkonstellationen darauf angewiesen, durch Informanten Daten also Informationen zu erlangen, die unter Umständen auch durch eine rechtswidrige Vortat, beispielsweise dem Geheimnisverrat erlangt wurden. Das klassische Whistleblowertum wird also zum strafbewehrten Unrecht.

Durch den Abs. III wird zwar abgesichert, dass Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen, von der Strafbarkeit ausgeschlossen sind. Hierunter fällt laut dem Referentenentwurf auch die journalistische Tätigkeit in Vorbereitung einer konkreten Veröffentlichung. Dennoch obliegt der Strafverfolgungsbehörde die Beurteilung ob es sich beim Verschaffen der Daten um eine rechtmäßige berufliche Pflicht handelt und ob die konkrete Aufgabenerfüllung der einzige Grund der Verwendung der Daten gewesen ist. Die Vorgaben sind unbestimmt und weit.

Aus diesem Grund ist durch § 202d III S. 2 StGB-E der Datenankauf von Amtsträgern ausdrücklich ausgenommen, die die Daten für Straf-, Ordnungswidrigkeiten- und Besteuerungsverfahren verwenden möchten. So wird sichergestellt wird, dass der Ankauf beispielsweise von CDs illegal erlangter Bankdaten durch die Länder nicht unter den Tatbestand der Datenhehlerei fällt. Hierin liegt eine unzulässige Bevorzugung der Handlungen der Steuerfahndung, die allein den finanziellen Interessen des Landes und Bundes dient.

Darüber hinaus wird aus dem Referentenentwurf (dort S. 26) deutlich, dass die Handlungen der Datenhehlerei bereits gem. § 44 i.V.m. 43 II Nr. 1 und 3 BDSG mit einer Freiheitsstrafe von bis zu 2 Jahren bestraft wird. Die Norm werde laut Referentenentwurf lediglich dem Unrechtsgehalt nicht gerecht, was nicht nachvollziehbar ist. Die Erforderlichkeit einer neuen gesetzlichen Regelung ist somit zu bezweifeln.

Ferner führt die Erweiterung des Ausschlusses der unzulässigen Ermittlungsmethoden gegenüber Rechtsanwältinnen und Rechtsanwälten (§ 160a StPO) durch den Tatbestand der Datenhehlerei (nun in § 160a IV S. 1 StPO-E) zu einer erheblichen Einschränkung der beruflichen Tätigkeit, da im Rahmen der Vertretung der rechtlichen Interessen des Mandanten es unter Umständen möglich sein muss, von anderen rechtswidrig (beispielsweise durch Geheimnisverrat) erlangte Daten zur Verteidigung zu verwenden. Es besteht die Gefahr des Missbrauchs, indem durch interessierte Kreise der Verdacht der Beteiligung an einer derartigen Datenhehlerei konstruiert wird, um die Durchsuchung einer Rechtsanwaltskanzlei zu veranlassen. Die Möglichkeit des absolut vertraulichen und vertrauensvollen Umgangs mit seinem Rechtsanwalt ohne die Gefahr der Ausspähung dieser vertrauensvollen Kommunikation ist von höchstem Rang. Sie darf in keiner Weise gefährdet werden.