Vorratsdatenspeicherung: Bestandsaufnahme und Ausblick

Von Rechtsanwalt **Felix Rettenmaier**, Frankfurt a.M., Rechtsreferendarin **Lisa Palm**, Mainz

I. Einleitung

Im Bereich des Cybercrime, d.h. im Bereich von Straftaten, bei denen der Computer als Tatmittel oder Tatgegenstand einer strafbaren Handlung eingesetzt wird, stellt die Beweissicherung eines der größten Probleme der Strafverfolgung dar. Delikte wie Computerbetrug, Softwarepiraterie und das Ausspähen von Daten (z.B. einer PIN), aber auch eine Vielzahl von Delikten aus anderen Bereichen des Strafrechts, sind häufig nur dann verfolgbar, wenn elektronische Daten, insbesondere Telekommunikationsverbindungsdaten (Telefon, Fax, E-Mail, SMS etc.), gesichert und zu Beweiszwecken verwendet werden können. Die Speicherung dieser Telekommunikationsverbindungsdaten, die sog. „Vorratsdatenspeicherung", sollte eine solche Sicherung ermöglichen. Für die rechtliche Betrachtung ist dabei zwischen Bestandsdaten nach § 3 Nr. 3 TKG, die als Daten eines Teilnehmers für die Begründung, Änderung oder Beendigung eines Vertragsverhältnisses erhoben werden – insbesondere Name, Kundenanschrift und Internetprotokolladresse (im Folgenden: „IP-Adresse") –, sowie den sensibleren Verkehrsdaten nach § 3 Nr. 30 TKG, die mit jedem Telekommunikationsvorgang erhoben, verarbeitet oder genutzt werden, zu unterscheiden.

II. Rechtliche Grundlagen

1. RL 2006/24/EG

Die Vorratsdatenspeicherung ist eine Reaktion der EU auf die Terroranschläge von New York, Madrid und London. Als Konsequenz regte die EU mit der Richtlinie RL 2006/24/EG an, alle Telekommunikationsverbindungsdaten der Europäer zu speichern, um diese den Ermittlungsbehörden zur Verfügung zu stellen.[1] Die Erhebung sollte anlassunabhängig (d.h. ohne Tatverdacht) erfolgen und die Daten sollten den Ermittlungsbehörden auf Abruf zur Verfügung stehen. Vorgesehen war eine möglichst flächendeckende präventive Speicherung aller für die Strafverfolgung oder Gefahrprävention nützlichen Daten. Infolgedessen verpflichtete die Richtlinie die Telekommunikationsanbieter, die von ihnen erfassten Daten mindestens sechs Monate und höchstens zwei Jahre zu speichern, um diese für die Verfolgung von schweren Straftaten bereitzustellen. Nach Maßgabe der Richtlinie oblag es den Mitgliedstaaten dafür Sorge zu tragen, dass die gespeicherten Daten insbesondere „unter vollständiger Achtung der Grundrechte" des jeweils Betroffenen an die zuständigen Behörden weitergegeben werden.

Vom ersten Entwurf der Richtlinie bis zu ihrer Verabschiedung im Parlament vergingen nur drei Monate. Die Richtlinie enthält keine näheren Regelungen zur Verwendung der Daten. Die Maßnahmen zum Datenschutz werden überwiegend den Mitgliedstaaten überlassen. Eine gerichtliche Überprüfung der Richtlinie am Maßstab der Charta der Grundrechte der Europäischen Union ist bislang nicht erfolgt.

[1] ABl. EU Nr. L 105 v. 13. 4.2006, S. 54.

2. §§ 113a, 113b TKG und § 100g Abs. 1 S. 1 StPO – eingeführt durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung v. 21.12.2007

Seit 2008 wurden in der Folge in Deutschland auf der Grundlage des Telekommunikationsgesetzes Verbindungsdaten aus der Telefon-, E-Mail- und Internetnutzung sowie Handy-Standortdaten für sechs Monate gespeichert. Diese Daten waren für die Strafverfolgungsbehörden sowohl zur Strafverfolgung (repressiv) als auch zu Zwecken der Gefahrenabwehr (präventiv) abrufbar.

3. BVerfG, Urt. v. 2.3.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08

Das Bundesverfassungsgericht hat mit seinem Urteil[2] zur Vorratsdatenspeicherung die §§ 113a und 113b des TKG und auch § 100g Abs. 1 S. 1 StPO, soweit danach Verkehrsdaten i.S.d. § 96 Abs. 1 TKG, die nach § 113a TKG (Nummer, Kennung des Anschlusses, personenbezogene Berechtigungskennung, Beginn und Ende, Datum und Uhrzeit der Verbindung) erhoben wurden, wegen Verstoßes gegen Art. 10 Abs. 1 GG (Brief-, Post und Fernmeldegeheimnis) – entgegen einer zuvor ergangenen einstweiligen Anordnung – für nichtig erklärt.

Zur Begründung führte das BVerfG u.a. aus, dass durch die Datenspeicherung bei den Bürgern ein bedrohliches Gefühl des „Beobachtetseins" hervorgerufen werde. Das Gesetz stelle zudem nicht sicher, dass nur schwerwiegende Straftaten Anlass für eine Datenerhebung begründen dürfen. Ferner sei es unverhältnismäßig, Daten ohne Wissen des Betroffenen und ohne richterliche Anordnung abzurufen. Darüber hinaus werde der Verhältnismäßigkeitsgrundsatz verletzt.[3]

Aus Sicht des BVerfG ist der Ansatz der Vorratsdatenspeicherung jedoch nicht schlichtweg unvereinbar mit den Vorgaben des Grundgesetzes. Allerdings handle es sich um einen besonders schweren Eingriff mit einer Streubreite, wie ihn die Rechtsordnung bisher nicht kenne.[4] Das BVerfG hat die Vorschrift des § 100g StPO in seinem Urteil jedoch nicht vollumfänglich beanstandet.

Vielmehr hat es u.a. vorgegeben, dass eine Speicherung der Daten nicht direkt durch den Staat erfolgen dürfe. Die Speicherung für die Dauer von sechs Monaten müsse zudem die zeitliche Obergrenze darstellen[5] und die anlasslose Spei-

[2] BVerfG, Urt. v. 2.3.2010 – 1 BvR 256/08 u. a. = NJW 2010, 833 = EuZW 2010, 280; Auswertung im Lichte der „Solange-Rechtsprechung" von *Bäcker*, EuR 2011, 103; umfassende Bespr. bspw. bei *Schramm/Wegener*, MMR 2011, 9.

[3] BVerfG NJW 2010, 833 (848 f.).

[4] BVerfG NJW 2010, 833 (834).

[5] Dazu krit. *Forgó/Krügel*, K&R 2010, 217 (219): Das Gericht weicht damit den im Volkszählungsurteil manifestierten Grundsatz auf, dass der Einzelne gegen die unbegrenzte Erhebung seiner persönlichen Daten geschützt sei, indem es eine „vorsorgliche, anlasslose Datenspeicherung" als mit dem

cherung müsse – als erklärte Ausnahme – mit einem Begründungs- und Ausgestaltungsaufwand verbunden sein, da die Vorratsspeicherung von personenbezogenen Daten zu lediglich unbestimmten oder noch nicht bestimmbaren Zwecken[6] verboten sei. Insbesondere sollten die Daten nicht anlasslos, sondern ausschließlich zur Verfolgung schwerer Straftaten genutzt werden können. Im Rahmen der Strafverfolgung müsse demnach ein durch bestimmte Tatsachen begründeter Verdacht einer schweren Straftat vorliegen. Dabei sei es Aufgabe des Gesetzgebers, abschließend festzulegen, zur Verfolgung welcher Taten ein Datenabruf möglich sein soll.[7] Darüber hinaus sei in den fraglichen Gesetzen weder dem Datenschutz noch der Datensicherheit ausreichend Rechnung getragen worden.[8] Der Datenabruf dürfe nur bei einer hinreichend konkreten Gefahr für ein bedeutsames Rechtsgut erfolgen.[9] Eine Übermittlung und Nutzung der gespeicherten Daten sei zudem grundsätzlich unter einen Richtervorbehalt zu stellen.[10] Weniger strenge Anforderungen stellte das BVerfG an die (mittelbare) Verwendung vorsorglich gespeicherter Daten in Form von behördlichen Auskunftsansprüchen hinsichtlich bereits bekannter IP-Adressen, da hierdurch keine Persönlichkeits- und Bewegungsprofile verwirklicht werden könnten.[11]

Im Ergebnis stellte das BVerfG fest, dass die Bundesrepublik Deutschland über eine verfassungsrechtliche Identität[12] verfüge, nach der die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht vollständig erfasst und registriert werden darf. Die (teilweise) verfassungsrechtliche Unbedenklichkeit folgt somit aus dem Ausnahmecharakter der Regelung.[13]

Dem Beschluss zur Vorratsdatenspeicherung von Telekommunikations-Verkehrsdaten[14] ist darüber hinaus zumindest zu entnehmen, dass der neu eingefügte § 110 Abs. 3 StPO[15], der die Sicherung und Durchsicht von Daten erlaubt, die sich auf externen Speichermedien befinden, auf die der Betroffene Zugriff hat, bei einer ordnungsgemäßen Verfahrensausgestaltung als verfassungskonform anzusehen ist.[16] Auch hier spielt das Kriterium der Anlassbezogenheit eine übergeordnete Rolle. Die Daten dürfen demnach gesichert werden; sind allerdings unmittelbar zu löschen, sobald sie für die Strafverfolgung nicht mehr erforderlich sind.[17]

III. Auswirkungen der Entscheidung des BVerfG

In der Praxis der Strafverteidigung stellt sich im Zusammenhang mit der bislang vorgenommenen Vorratsdatenspeicherung insbesondere das Problem, ob – und wenn ja, in welchem Umfang – diese Daten von den Ermittlungsbehörden zu Lasten des Betroffenen verwendet werden dürfen. Zur Beurteilung dieser Fragen ist zwischen einer Datenerhebung vor und nach der (abschließenden) Entscheidung des BVerfG zu unterscheiden.

1. Datenerhebungen vor der BVerfGE

Das BVerfG gab dem Eilantrag auf Außer-Kraft-Setzung der angegriffenen §§ 113a und 113b TKG im März 2008 mithilfe einer einstweiligen Verfügung teilweise statt.[18] Die Verwendung gespeicherter Daten wurde aufgrund drohender schwerwiegender und irreparabler Schäden auf schwere Straftaten im Sinne des § 100a Abs. 2 StPO begrenzt. Die Pflicht zur Datenspeicherung blieb bestehen.

Nach der späteren Nichtigkeitserklärung wurde die Verwertung von Datenerhebungen vor der Hauptsacheentscheidung des BVerfG bezweifelt. Ohne jegliche gesetzliche Ermächtigungsgrundlage gewonnene Beweismittel dürften in einem rechtsstaatlichen Verfahren nicht verwertbar sein. Dies müsse auch gelten, wenn die Rechtsgrundlage nachträglich entfalle. Dass das BVerfG eine zukünftige Regelung zur Beweiserhebung für verfassungsrechtlich zulässig halte, könne hieran nichts ändern. Die erhobenen Daten hätten unverzüglich nach der Feststellung der Nichtigkeit der Vorschriften gelöscht werden müssen.[19] Für alle Fälle, die nicht von der einstweiligen Anordnung des BVerfG umfasst waren, sollte in Ansehung der Schwere des Rechtsverstoßes von einem fernwirkenden Verwertungsverbot ausgegangen werden.[20]

Nach Auffassung des OLG München[21] und des BGH[22] sind die Daten – auch nach Feststellung der (teilweisen) Nichtigkeit der gesetzlichen Grundlagen der Vorratsdatenspeicherung – verwertbar. Die Erhebung sei nach der zum Zeitpunkt der Erhebung geltenden Rechtslage zulässig gewesen, da sie den Anforderungen entsprach, die das BVerfG in

Telekommunikationsgeheimnis prinzipiell vereinbar qualifiziert.

[6] BVerfG NJW 2010, 833 (841 in Rn. 231).

[7] Dazu eingehend *Schramm/Wegener*, MMR 2011, 9 (11).

[8] BVerfG NJW 2010, 833 (840 in Rn. 221-225).

[9] BVerfG NJW 2010, 833 (849).

[10] BVerfG NJW 2010, 833 (843 in Rn. 247).

[11] BVerfG NJW 2010, 833 (844 in Rn. 254 f.).

[12] BVerfG, Beschl. v. 28.10.2008 – 1 BvR 256/08, eine direkt gegen die Vorschrift gerichtete Verfassungsbeschwerde wurde mangels Rechtswegerschöpfung insoweit als unzulässig verworfen, BVerfG NVwZ 2009, 103.

[13] Näher dazu *Roßnagel*, NJW 2010, 1238 (1240).

[14] BVerfG, Beschl. v. 16.6.2009 – 2 BvR 902/06 = NJW 2009, 2431.

[15] Aufgehoben mit Wirkung v. 1.9.2004 durch Gesetz v. 24.8. 2004 (BGBl. I 2004, S. 2198); Abs. 3 eingef. mit Wirkung v. 1.1.2008 durch Gesetz v. 21.12.2007 (BGBl. I 2007, S. 3198), entsprechend der Forderung des Art. 19 Abs. 2 des Übereinkommens des Europarats über Computerkriminalität.

[16] Vgl. *Klein*, NJW 2009, 2996 (2999).

[17] *Nack*, in: Hannich (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung, 6. Aufl. 2008, § 110 Rn. 8.

[18] BVerfG, Beschl. v. 11.3.2008 – 1 BvR 256/08 = NVwZ 2008, 543.

[19] Anm. OLG München NJW-Spezial 2010, 601; Anm. BGH NJW-Spezial 2011, 216.

[20] *Volkmer*, NStZ 2010, 318 (320).

[21] OLG München MMR 2010, 793 = BeckRS 2010, 19914.

[22] BGHSt 56, 138 = NJW 2011, 1377; BGH NJW 2011, 1827; OLG München MMR 2010, 793 = BeckRS 2010, 19914.

seiner einstweiligen Verfügung aufgestellt hatte. Durch die Hauptsacheentscheidung sei die Rechtsgrundlage für die Maßnahme auch nicht rückwirkend entfallen. Die Verfassungsrichter hatten insoweit zwar angeordnet, dass im Rahmen laufender Auskunftsersuchen der Behörden erhobene Daten zu löschen seien. Hinsichtlich bereits übermittelter Daten seien jedoch auch für noch nicht rechtskräftig abgeschlossene Verfahren keine Restriktionen angeordnet worden. Ein rückwirkendes Beweisverwertungsverbot sei deshalb vom BVerfG nicht gewollt gewesen. Insoweit stellte der BGH fest, dass Telekommunikationsdaten, die vor dem 2.3. 2010 auf der Grundlage der einstweiligen Anordnung des BVerfG rechtmäßig gewonnen und an die ersuchenden Behörden übermittelt wurden, in einem Strafverfahren zu Beweiszwecken verwertet werden dürfen.

Zwar begründet eine anlasslose Speicherung aller Telekommunikationsdaten und folglich auch deren Verwertung einen schwerwiegenden Grundrechtseingriff.[23] Beweiserhebung und -verwertung greifen hier indes nicht in den absolut geschützten Kernbereich privater Lebensgestaltung ein. Der Eingriff in das Telekommunikationsgeheimnis kann durch die damit verfolgten Zwecke (Effektivierung der Strafverfolgung, der Gefahrenabwehr und der Erfüllung der Aufgaben der Nachrichtendienste) gerechtfertigt sein. Art. 10 Abs. 1 GG verbietet nicht jede vorsorgliche Erhebung und Speicherung von Daten überhaupt, sondern schützt vor einer unverhältnismäßigen Gestaltung solcher Datensammlungen und hierbei insbesondere vor einer entgrenzenden Zwecksetzung.[24]

Im vorliegenden Fall erfolgte die Datenerhebung und -verwertung in einem Ermittlungs- bzw. Strafverfahren und war auf den Verdacht einer Straftat nach § 244a StGB gestützt, die als schwer zu qualifizieren ist. Auch beschränkte sich der Eingriff auf Standortdaten eines benutzten Mobiltelefons und den Umstand, dass gewisse Telefonate geführt wurden, obwohl sogar eine Telekommunikationsüberwachung mit Aufzeichnung der Gesprächsinhalte auf der Grundlage von § 100a Abs. 2 Nr. 1 lit. j StPO zulässig gewesen wäre. Schließlich sei bei einer Gesamtabwägung auch zu berücksichtigen, dass eine Tataufklärung und ein Tatnachweis ohne die bereits erhobenen Daten – deren Erhebung zum Zeitpunkt ihrer Speicherung und Übermittlung von einer einstweiligen Anordnung des Bundesverfassungsgerichts als fortwirkende Legitimationsgrundlage gedeckt war – nicht oder zumindest nur wesentlich erschwert möglich gewesen wären. Die Nichtigkeitserklärung wirkt zwar ex tunc, dies betrifft indessen nicht die ebenfalls in Gesetzeskraft erwachsene einstweilige Anordnung. Ein Löschungsgebot wurde durch das BVerfG nicht statuiert.

2. Ermittlung der IP-Adresse nach bisherigem deutschem Datenschutzrecht

Das OLG Hamburg[25] stellte in einer anderen Entscheidung im Zusammenhang mit einer bereits erfolgten Urheberrechtsverletzung fest, dass das Ermitteln der IP-Adressen nach deutschem Datenschutzrecht nicht rechtswidrig sei. Es komme insofern kein Beweisverwertungsverbot in Betracht, zumal bei den ermittelten IP-Adressen ein Personenbezug mit normalen Mitteln ohne weitere Zusatzinformationen nicht hergestellt werden könne. Der Personenbezug werde erst durch die seitens der Staatsanwaltschaft nach § 161 Abs. 1 S. 1 und § 163 StPO angeforderte oder gemäß § 101 Abs. 9 UrhG gerichtlich angeordnete Auskunft des Providers ermöglicht.[26]

3. Diskussionsentwurf des Bundesministeriums der Justiz (Stand: 7.6.2011)

Das Bundesministerium der Justiz leitete aus dem Urteil des BVerfG zunächst die grundsätzliche Pflicht der Bundesregierung ab, sich für die Freiheitsrechte der Bürger auf europäischer Ebene einzusetzen.[27] Trotz der durch das BVerfG vorgegebenen Beschränkungen soll den wesentlichen Interessen der Strafverfolgung im Rahmen einer Abwägung von Sicherheitsbelangen und Grundrechten noch Rechnung getragen werden können. Vor diesem Hintergrund sollte sowohl die StPO als das TKG wie folgt geändert werden:

a) § 100j StPO-E

Der neue § 100j StPO (Sicherungsanordnung) sieht eine Anordnungsbefugnis für eine anlassbezogene Speicherungspflicht vor. Diese ist mit einem Erforderlichkeitsvorbehalt versehen und ist auf das notwendige Maß begrenzt. Die Sicherungsanordnung muss damit für die Erforschung des Sachverhalts – oder die Ermittlung des Aufenthaltsortes eines Beschuldigten – erforderlich sein. Von der Anordnung ist weiterhin gemäß § 100j Abs. 1 S. 2 StPO-E abzusehen, wenn die Voraussetzung des § 100g StPO (Straftaten von erheblicher Bedeutung) nicht vorliegen würden. Eine Begrenzung des Grundrechtseingriffs wird insbesondere dadurch erreicht, dass nur ein Rückgriff auf die bei den Telekommunikationsunternehmen ohnehin bereits vorhandenen gesicherten („eingefrorenen", sog. Quick-Freeze, in den USA üblich) und durch das Telekommunikationsunternehmen erhobenen Daten genommen werden kann. Die vorhandenen Daten werden also erst in dem Moment eingefroren, in dem die Verdachtslage den Anforderungen der Eingriffsnorm entspricht, sodass auf diese im Verfahren zurückgegriffen werden kann.

Die Speicherung der Daten erfolgt nach der Anordnung auf eine begrenzte Zeit. Mit Ablauf der Sicherungsfrist (höchstens ein Monat, § 100j Abs. 2 StPO-E) sind die erhobenen Daten unverzüglich zu löschen, § 100j Abs. 5 StPO-E, soweit keine Fortdauer der Maßnahme für maximal einen weiteren Monat angeordnet wird. In der Regel schließt sich an die Sicherungsanordnung eine Auskunftserteilung zur Verwendung der erhoben Daten im Ermittlungsverfahren nach § 100g StPO an. §100j StPO-E lässt es insoweit zunächst genügen, dass die – auch von der Polizei oder der Staatsan-

[23] BVerfG NJW 2010, 833 (838 f. in Rn. 212).
[24] BVerfG NJW 2010, 833 (838 in Rn. 206 f.).
[25] OLG Hamburg MMR 2011, 281 = GRUR-Prax 2010, 536.
[26] OLG Hamburg MMR 2011, 281 (282).
[27] Entwurf des „Gesetzes zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet", RDV 2011, 202.

waltschaft in eigener Kompetenz zu treffende – Anordnung für die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes eines Beschuldigten erforderlich ist. Den Strafverfolgungsbehörden werden die gespeicherten Daten schließlich durch Zugriff gemäß § 100g StPO unter Richtervorbehalt und dem Vorbehalt einer Straftat von erheblicher Bedeutung für einen begrenzten Zeitraum zur Verfügung gestellt.

Dagegen wird teilweise vertreten, dass nicht nur ein „Quick-Freeze"-Verfahren einen verhältnismäßigen Eingriff in das Recht auf informationelle Selbstbestimmung und des Fernmeldegeheimnisses der Nutzer darstellt, sondern das Interesse an einer effektiven Terrorismusbekämpfung und sonstiger Kriminalität darüber hinausgehende Maßnahmen rechtfertigt.[28] Für die Wiedereinführung der bis zum Urteil des BVerfG bestehenden Rechtslage sollen vor allem zwei Gründe der Gefahrenabwehr sprechen: dass die moderne Telekommunikation zum einen eine ungeahnte Möglichkeit einer widerstandsfreien Bündelung von Wissen, Handlungsbereitschaft und krimineller Energie über Zeit und Raum hinweg verschafft und zum anderen, dass eine Speicherung von Spuren die Entstehung eines teilweise „rechtsfreien Raums" verhindert.[29]

b) § 100k StPO-E

Gemäß § 100k StPO-E (Auskunftspflicht) soll im Internetzugangsbereich eine eng befristete Speicherung von Verkehrsdaten zu dem Zweck erfolgen, Bestandsdatenauskünfte insbesondere zur Bekämpfung der Kinderpornografie zu den Strafverfolgungsbehörden bereits bekannten IP-Adressen zu ermöglichen, ohne die Verkehrsdaten selbst an die Strafverfolgungsbehörden herauszugeben. Anhand dieser Daten wird nicht ersichtlich, wer wen wann angerufen oder wem eine E-Mail geschrieben hat oder an welchem Standort sich der Nutzer wann befand, sondern nur zu welcher Zeit der Betroffene welcher IP-Adresse als Verantwortlicher zuzuordnen ist.

Für die nach Maßgabe des § 111 TKG erhobenen Bestandsdaten des Telekommunikationsunternehmens besteht eine Speicherungspflicht auch, soweit die Daten nicht für betriebliche Zwecke erforderlich sind, § 111 Abs. 1 S. 1 TKG. Strafverfolgungsbehörden dürfen die Herausgabe dieser Bestandsdaten bislang nach der Ermittlungsgeneralklausel (§§ 161 Abs. 1 S. 1, 163 StPO i.V.m. § 113 Abs. 1 TKG) unter der Voraussetzung verlangen, dass die Erhebung der Bestandsdaten für die Verfolgung einer verfahrensgegenständlichen Straftat erforderlich ist. Einer gerichtlichen oder staatsanwaltschaftlichen Anordnung bedurfte es dabei nicht.

Beachtenswert ist, dass das BVerfG diese Regelung zur Erhebung von Bestandsdaten grundsätzlich nicht beanstandet. Es hat jedoch angemerkt, dass auf der Ebene der Eingriffsschwelle sicherzustellen ist, dass eine Auskunft nur auf Grund eines „hinreichenden Anfangsverdachts oder einer konkreten Gefahr auf einzelfallbezogener Tatsachenbasis" erfolgen darf. Auch hier erfolgt für die Auskunftserteilung kein Zugriff der Strafverfolgungsbehörden auf die Verkehrsdaten.

c) § 113a TKG-E

§ 113a TKG (Datenspeicherung) sieht eine zeitlich eng befristete Speicherung von bei der Nutzung von Internetzugangsdiensten anfallenden Daten vor, ohne dass ein Zugriff der Strafverfolgungsbehörden auf Verkehrsdaten zulässig ist. Datensicherheit und Datenqualität der anlasslos gespeicherten Daten müssen nach Maßgabe des BVerfG verbessert werden. Die Speicherungsdauer wurde daraufhin auf sieben Tage beschränkt, für deren Ingangsetzung das Ende der Internetnutzung, d.h. der Entzug der zugewiesenen IP-Adresse, maßgeblich ist. Der Inhalt der Kommunikation darf hingegen nicht gespeichert werden.

Bis heute ist es aufgrund der von tiefen Meinungsverschiedenheiten geprägten Diskussion noch zu keiner Neuregelung gekommen.

IV. Aktuelle Entwicklungen

1. Bericht der EU-Kommission über die Bewertung der Richtlinie

Im April 2011 legte die EU-Kommission einen Bericht über die Bewertung der Vorratsdatenspeicherungsrichtlinie (2006/24/EG) vor.[30] Dort wurde Bilanz über die Anwendung der Richtlinie gezogen – nicht ohne erneut die Bedeutung der Telekommunikationsdatenspeicherung als wichtiges Instrument zum Schutz vor schweren Straftaten zu betonen. Dabei wurde nicht übersehen, dass damit eine beträchtliche Einschränkung des Rechts auf Privatsphäre einhergeht.[31] Die Datensicherheit stelle ein hohes Risiko dar. Deshalb entschloss sich die EU-Kommission auch zu einer umfassenden Revision des EU-Datenschutzrechts.[32] In diesem Zusammenhang erwägt die EU-Kommission die Aufnahme des vom BVerfG geschaffenen Grundrechts der Vertraulichkeit und Integrität informationstechnischer Systeme, dessen Schutzbereich bei Massendatenbezug eröffnet ist, in das Gesamtkonzept des Datenschutzes der Europäischen Union.[33]

[28] Auf der Innenministerkonferenz vom 21.-22.6.2011 zeigte sich eine gewisse Tendenz zu Gunsten der Vorratsdatenspeicherung und die ebenfalls umstrittene Verlängerung der Anti-Terror-Gesetze; die Verlängerung wurde nachfolgend vom Bundestag im Wege einer Kompromisslösung beschlossen (vgl. im Einzelnen Presseinformation des BMI v. 29.6.2011, zu Schutzlücken: http://www.bmi.bund.de/SharedDocs/FAQs/DE/Themen/Sicherheit/SicherheitAllgemein/7.html?nn=2075656 (9.6.2012).

[29] So *Möstl*, ZRP 2011, 225 (227 ff.) mit eigenem Regelungsvorschlag mit kumulativem „Quick-Freeze"-Verfahren und Mindestspeicherung.

[30] ABl. EU Nr. L 105 v. 13. 4.2006, S. 54, eingehend *Gola/Klug*, NJW 2011, 2484.

[31] Zum Bericht *Möstl*, ZRP 2011, 225 (227).

[32] Mitteilung KOM 2010, 609; eingehend *Gola/Klug*, NJW 2011, 2484 (2490).

[33] Mitteilung KOM 2010, 609, S. 6.

2. Vertragsverletzungsverfahren

Die EU-Kommission hat die Bundesregierung bereits Mitte Juni 2011 gemäß Art. 258 AEUV zu einer Stellungnahme im Rahmen eines Vertragsverletzungsverfahren aufgefordert, da die Frist für die Umsetzung der Richtlinie 2006/24/EG bereits im April 2011 ablief. Die Bundesrepublik Deutschland weigert sich jedoch weiterhin, anlasslos Daten über sechs Monate zu speichern. Mit diesem Verhalten, so die EU-Kommission, behindere der Gesetzgeber die deutschen Ermittlungsbehörden bei der Aufklärung schwerer Verbrechen. Aus deutscher Sicht bleibt der Konflikt mit der Charta der Grundrechte und den Datenschutzrechten bestehen. Zudem wird teilweise bezweifelt, dass die Richtlinie 2006/24/EG den Anforderungen des europäischen Primärrechts genügt. Fraglich ist die binnenmarktrechtliche Kompetenz nach dem jetzigen Art. 114 AEUV sowie die Vereinbarkeit mit den europäischen Grundrechten.[34] Die Zweifel bezüglich der Vereinbarkeit mit der Grundrechtecharta der europäischen Union werden im Übrigen von der Justizministerin geteilt.[35]

Auch wenn diese Zweifel berechtigt sind, ändert dies jedoch nichts an der Umsetzungspflicht der Bundesrepublik, da sich Mitgliedstaaten nicht auf die Rechtswidrigkeit der umzusetzenden Richtlinie berufen können.[36] Seitens der EU wurde mit Rücksicht auf die bestehende Problematik bereits versichert, dass keine rückwirkenden Strafzahlungen verhängt werden. Ausschließlich ein Zwangsgeld könne erhoben werden. Nach der Entscheidung über das Vertragsverletzungsverfahren könnte Deutschland somit ohne weiteres zügig ein Gesetz entsprechend den europäischen Vorgaben verabschieden und der Schaden bliebe verhältnismäßig gering.

V. Stellungnahme

1. Aus Sicht der Strafverteidigung ist zunächst darauf hinzuweisen, dass den Verkehrsdaten eine erhebliche Aussagekraft im Hinblick auf ihren Verursacher zukommt. Auf die grundgesetzlich in besonderem Maße zu schützende Intimsphäre des Betroffenen lassen sich – auch mit den in Rede stehenden legislativen Änderungen – hinreichende inhaltliche Rückschlüsse ziehen. Adressaten, Daten, Uhrzeit und Ort von Telefongesprächen erlauben insbesondere nach längerer Beobachtung und in ihrer Kombination detaillierte Aussagen zu gesellschaftlichen oder politischen Zugehörigkeiten, persönlichen Vorlieben, Neigungen und Schwächen. Hierüber lassen sich aussagekräftige Persönlichkeits- und Bewegungsprofile erstellen. Soweit der Richter am Bundesverfassungsgericht *Schluckebier* in seinem Sondervotum darauf verweist, dass die Vorratsdatenspeicherung Ausfluss der staatlichen Schutzpflicht gegenüber den Bürgern sei, geeignete Maßnahmen zu ergreifen, um die Rechtsgutsverletzung zu verhindern oder sie aufzuklären, überzeugt dies nicht in Gänze. Vielmehr muss es die Aufgabe des Gesetzgebers sein, diesen – unbestreitbar bestehenden – Schutzpflichten nachzukommen, ohne dass die Grundrechte des Einzelnen mehr als zwingend notwendig tangiert werden. Die von *Schluckebier* insoweit vertretene Auffassung, dass die Speicherung der zu erhebenden Daten durch „nichtstaatliche" Stellen den Einschüchterungseffekt beim Bürger entfallen lasse,[37] kann nach diesseitiger Auffassung nicht gefolgt werden. Zum einen erfolgt die Erhebung und Speicherung der Daten im Auftrag des Staates, zum anderen haben die in der Vergangenheit in gehäuftem Maße auftretenden „Datenpannen" und „Datenskandale" gezeigt, dass die Sicherheit von Daten keinesfalls selbstverständlich ist. Folgt man zudem der polizeilichen Kriminalstatistik des Bundeskriminalamtes hat die sechsmonatige Protokollierung aller Internetverbindungen im Jahr 2009 weder von der Begehung von Straftaten abgeschreckt, noch den Anteil der aufgeklärten Straftaten erhöht. Die präventiven und repressiven Ziele der Vorratsdatenspeicherung wurden daher – zumindest bis jetzt – verfehlt. Ein ausgewogenes – grundrechtsschonendes – Verhältnis von Zweck und Mittel scheint insoweit fraglich. Geht man überdies davon aus, dass sich der überwiegende Teil von Straftaten auch ohne die Sicherung und Auswertung von Telekommunikations*verkehrsdaten* aufklären lässt,[38] besteht für eine weitergehende Regelung keine Notwendigkeit.

2. Zusammenfassend lässt sich festhalten, dass die Vorratsdatenspeicherung – ungeachtet in welcher Form – als grundrechtsrelevante Maßnahme einen sensiblen Umgang erfordert. Dem Datenschutz und der Datensicherheit muss daher in einer dem betroffenen Grundrecht angemessenen Weise Rechnung getragen werden. Angesichts der Ergebnisse der polizeilichen Kriminalstatistik wird man außerdem den Mehrwert einer solchen Ermittlungshandlung ständig beobachten und daraufhin die Gewichtung von Eingriffsgut und Schutzgut dauerhaft neu hinterfragen müssen. Ergibt sich dabei, dass die staatliche Schutzpflicht durch eine Datenerhebung und Speicherung als grundrechtsrelevante Maßnahme nicht verbessert werden kann, ist eine Rechtfertigung zur Durchführung der Maßnahmen ausgeschlossen. Es sind daher – über das Grundsatzurteil des Bundesverfassungsgerichts hinaus – konkrete praktische Vorgaben des Parlaments für die Ermittler zu fordern. Diese müssen konkret, nachvollziehbar, ergebnisorientiert und von geringstmöglicher Grundrechtsrelevanz sein. Anderenfalls schadet die „Vorratsdatenspeicherung" dem Rechtsstaat.

[34] Vgl. *Gitter/Schnabel*, MMR 2007, 411 (412 ff.); *Westphal*, EuR 2006, 706 (711 ff.).

[35] http://www.bmj.de/SharedDocs/Interviews/DE/Printmedien/20120611_NJW_VDS_auf_dem_Pruefstand.html (7.9.2012); hierzu s. auch *Derksen*, WD 11-3000-18/11.

[36] EuGH MMR 2010, 783; *Möstl*, ZRP 2011, 225 (227).

[37] *Schluckebier*, NJW 2010, 852.

[38] Vgl. Verband der deutschen Internetwirtschaft Eco, http://www.golem.de/1010/78537.html (6.6.2012).