Berlin, im Januar 2012
Stellungnahme Nr. 1/2012

abrufbar unter
www.anwaltverein.de

Stellungnahme des Deutschen Anwaltvereins

durch den Ausschuss Gefahrenabwehrrecht in Zusammenarbeit mit dem Ausschuss Strafrecht

zum

BMJ-Diskussionsentwurf für ein

„Gesetz zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet“

(Stand: 7.06.2011)

Mitglieder des Ausschusses Gefahrenabwehrrecht:

Rechtsanwältin Dr. Heide Sandkuhl, Potsdam (Vorsitzende)
Rechtsanwalt Wilhelm Achelpöhler, Münster
Rechtsanwalt Prof. Dr. Matthias Dombert, Potsdam
Rechtsanwalt Sönke Hilbrans, Berlin
Rechtsanwalt Dr. Stefan König, Berlin
Rechtsanwältin Dr. Regina Michalke, Frankfurt am Main (Berichterstatterin)
Rechtsanwältin Kerstin Oetjen, Freiburg

Zuständiger DAV-Geschäftsführer:

Rechtsanwalt Franz Peter Altemeier

Verteiler:

- Bundeskanzleramt
- Bundesministerium des Innern
- Bundesministerium der Justiz

- Bundesrat
- Deutscher Bundestag - Rechtsausschuss
- Deutscher Bundestag - Innenausschuss

- Arbeitsgruppen Inneres der im Deutschen Bundestag vertretenen Parteien
- Arbeitsgruppen Recht der im Deutschen Bundestag vertretenen Parteien

- Justizministerien der Länder
- Landesministerien und Senatsverwaltungen des Innern
- Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
- Landesdatenschutzbeauftragte
- Innenausschüsse der Landtage
- Rechtsausschüsse der Landtage

- Bundesrechtsanwaltskammer
- Deutscher Richterbund
- Bundesverband der Freien Berufe
- Gewerkschaft der Polizei (Bundesvorstand)
- Deutsche Polizeigewerkschaft im DBB
- Verd.di, Recht und Politik

- Vorstand und Landesverbände des DAV
- Vorsitzende der Gesetzgebungs- und Geschäftsführenden Ausschüsse des DAV
- Vorsitzende des FORUM Junge Anwaltschaft des DAV

- Frankfurter Allgemeine Zeitung
- Süddeutsche Zeitung
- Berliner Zeitung

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit derzeit ca. 68.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

Vorbemerkung:

Im Jahr 2006 verabschiedete die europäische Union die Richtlinie2006/24/EG, auf deren Grundlage die Mitgliedstaaten zu einer Speicherung von Telekommunikationsverkehrsdaten auf Vorrat verpflichtet wurden. Die Richtlinie ist in Deutschland durch das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ umgesetzt worden, das am 1. Januar 2008 (Telefoniedaten) bzw. am 1. Januar 2009 (Internetdaten) in Kraft getreten ist. Das Gesetz verpflichtete die Anbieter von öffentlich zugänglichen Telekommunikations- und Internetdiensten, Verkehrsdaten über einen Zeitraum von sechs Monaten auf Vorrat zu speichern und diese – im Bedarfsfall – Strafverfolgungsbehörden, Nachrichtendiensten oder mit Aufgaben der Gefahrenabwehr betrauten Behörden zur Verfügung zu stellen. Das Gesetz ist im Wege mehrerer Eilverfahren „angegriffen“ worden, zuletzt in Gänze erfolgreich mit der größten Verfassungsbeschwerde seit Bestehen des Bundesverfassungsgerichts mit nahezu 35.000 Klägern mit der Folge, dass das Bundesverfassungsgericht am 2. März 2010 das Gesetz für nichtig erklärte und außer Kraft setzte (1 BvR 256/08). Das Gericht wandte sich ausdrücklich an den Gesetzgeber, indem es mahnend daran erinnerte, „d*ass die Freiheitsvereinigung der Bürger nicht total erfasst und registriert werden darf“.* Dies gehöre *„zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss."*

Wegen der Tiefe des Grundrechtseingriffs und des Fehlens von Belegen für einen statistisch signifikanten Einfluss der Maßnahme auf die Begehung und Verfolgung von Straftaten muss die Richtlinie2006/24/EG nach Auffassung des DAV zugunsten gezielter, anlassbezogener und verhältnismäßiger Verfahren im Lichte der national und international gewährten Grund- und Freiheitsrechte grundlegend überarbeitet werden (vgl. bereits DAV-Stellungnahme Nr. 41/2007, abrufbar unter www.anwaltverein.de).

Das Bundesministerium der Justiz legte im Juni 2011 einen Diskussionsentwurf vor, nachdem es bereits im Januar 2011 ein sog. „Eckpunktepapier zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet“ vorstellte.

Während bei Telekommunikationsunternehmen ohnehin vorhandene Verkehrsdaten künftig nur noch anlassbezogen für kurze Zeit gesichert („eingefroren“) werden sollen (sog. „Quick-Freeze-Verfahren“), die gegebenenfalls in einer zweiten Stufe mit Zustimmung eines Richters den Ermittlern zur Verfügung gestellt werden können ("aufgetaut"), sehen die Pläne im Online-Sektor eine eng befristete Speicherung von Verkehrsdaten vor, um Strafverfolgungsbehörden Bestandsdatenauskünfte, d.h. die Zuordnung von IP-Adressen zu Personen bzw. Kundendaten bei einem konkreten Verdacht zu ermöglichen (sog. „Vorratsdatenspeicherung-Light“).

Der DAV fasst mit vorliegender Stellungnahme seine grundsätzlichen Bedenken zusammen (**Teil. I**), um im Anschluss auf die Detailregelungen einzugehen (**Teil. II**).

Teil I: Stellungnahme zu dem Diskussionsentwurf (Summary)

Gemessen an den Möglichkeiten, die den Ermittlungsbehörden durch die neuen Eingriffsbefugnisse gegeben werden, sind die Sicherungen gegen Eingriff in das Persönlichkeitsrecht von (nicht zuletzt unbeteiligten) Bürgern in rechtsstaatlicher Hinsicht mangelhaft.

I. Das „Einfrieren“ von Verkehrsdaten für maximal 2 Monate nach **§ 100j StPO-E** ist eine Maßnahme, die – im Vergleich zur anlasslosen Vorratsdatenspeicherung des aufgehobenen § 113a TKG a.F. – zumindest anlassbezogen angeordnet bzw. durchgeführt wird. Allerdings sind die Voraussetzungen, auf Grund derer die Anordnung zum „Einfrieren“ der Verkehrsdaten ergehen kann, äußerst niedrig angesiedelt. Erforderlich ist allein, dass die Daten der Erforschung des (irgendeines?) Sachverhalts oder des Aufenthalts eines Beschuldigten dienen können. Dies sind konturenlose Voraussetzungen mit weitreichenden Interpretationsmöglichkeiten in der Hand allein des Anordnenden. Dass in § 100j StPO-E von einer Erforderlichkeit der Datensicherung für die „Erforschung des Sachverhalts“ und nicht von einer „Ermittlung des Sachverhalts“ gesprochen wird, zeigt z. B., dass das „Einfrieren“ auch weit im Vorfeld eines Anfangsverdachts stattfinden kann. Hierüber entscheiden die Polizei bzw. Staatsanwaltschaft autark. Ein Richtervorbehalt oder eine Überprüfung der Anordnung ist – jedenfalls ausdrücklich – nicht vorgesehen.

Die Quasi-Kompensation für diese niedrigere Eingriffsschwelle, dass nämlich eine Sicherungsanordnung dann unzulässig ist, wenn bei ihrem Erlass absehbar ist, dass die Voraussetzungen für eine spätere Erhebung oder Verwendung der Daten nach § 100g StPO „voraussichtlich“ nicht vorliegen werden, kann nicht als wirksames einschränkendes Korrektiv angesehen werden. Ob „voraussichtlich“ keine i. S. des § 100g StPO schwere Straftat vorliegt oder keine Tat, die mittels des Internet begangen wurde, wird in den

seltensten Fällen im frühen Stadium von Ermittlungen („Erforschung“) feststehen. Im Gegenteil dürfte regelmäßig nicht auszuschließen sein, dass das Internet in irgendeiner Weise in das zu „erforschende“ Geschehen hineinspielt, wenn TK-Daten im Fokus stehen. Von daher wird sich jedenfalls diejenige Alternative des § 100g StPO, wonach die Tat mittels des Internets begangen sein muss, „voraussichtlich“ meistens bejahen lassen. Gerade diese Anwendungsalternative des § 100g StPO wurde aber vom Bundesverfassungsgericht wegen ihrer (bedenklich) weiten Ausdehnung auf alle Straftaten als problematisch angesehen (BVerfG, Urteil vom 02.03.2010, 1 BvR 256/08, 586/08, Rn. 27).

Dem allen steht gegenüber, dass die Verkehrsdaten, die für maximal 2 Monate auf diese „einfache“ Weise „eingefroren“ werden können, weitreichende Erkenntnisse nicht nur im Hinblick auf das Bewegungsprofil (über Rufnummer, Kennung, Funkzellen- und Uhrzeitdaten) ermöglichen, sondern mittels der IP-Adressen, SMS etc. bei Internettelefondiensten sehr weitgehende Einblicke auch in die jeweilige Nutzung des Internet. Die IP-Adressen werden nicht von ungefähr als das „Gold der Internetwelt“ bezeichnet (Hoeren, JZ 2011, 995 ff./996). Mit ihnen lassen sich – nicht zuletzt in Verbindung mit anderen Daten (z. B. über die Nutzung von Google) – in vielfältiger Weise auch höchst personenbezogene Erkenntnisse (Bewegungsprofile, Internetnutzung etc.) gewinnen.

Die Sensibilität dieser Daten wird gegenwärtig noch dadurch verstärkt, dass die rechtliche Einordnung von IP-Adressen als Bestands- oder Verkehrsdaten immer noch umstritten ist. Dies ist mit weitreichenden Konsequenzen z. B. hinsichtlich der Verwertung dieser Daten im Strafprozess verbunden. Sind IP-Adressen z. B. Bestandsdaten (so BGH, Urt. vom 12.5.2010 – I ZR 121/08), dann wäre eine Verwertung nach § 100g StPO gar nicht zulässig. Auch die Frage der Anwendbarkeit des Bundesdatenschutzgesetzes wird uneinheitlich beantwortet (vgl. Karg MMR-Aktuell 2011, 345).

Hinzu kommt, dass die technischen Dimensionen des Internet und damit insbesondere deren Gefahren, noch weitgehend unbekannt sind. Fast täglich erreichen uns neue Hiobsbotschaften, welche gigantischen Datenmengen wie leicht öffentlich zugänglich sind bzw. mit wenigen „Hackerhandgriffen“ zugänglich gemacht werden können. Ausreichende Sicherungsmechanismen und -maßnahmen fehlen in rechtlicher, technischer und tatsächlicher Hinsicht. Bei alledem stehen wir auch nach Einschätzung von Fachleuten erst am Anfang einer Entwicklung, die noch nicht einmal annähernd abschätzbar wäre.

Dass die „eingefrorenen“ Daten gemäß § 100j Abs. 5 StPO-E nach Ablauf der Sicherungsfrist von dem TK-Diensteanbieter „unverzüglich zu löschen“ sind, ist demgegenüber keine ausreichende Sicherheit. Es ist weder geregelt, wie entsprechende Zuwiderhandlungen des Dienstanbieters zu ahnden sind, noch wie die Ermittlungsbehörden die aus den Daten entnommenen Informationen zu behandeln haben, nachdem diese gelöscht wurden oder, nachdem sich herausgestellt hat, dass die Voraussetzung für eine

Speicherung der Daten nach § 100j StPO-E von vorneherein nicht vorlagen. Dass solche (oder ähnliche Fälle) einer Speicherfristüberschreitung ohne weiteres ein Verwertungsverbot nach sich zögen, hat die Rechtsprechung – jedenfalls bislang – nicht entschieden (vgl. hierzu BT-Drs. 17/1482, S. 2 und Meyer-Goßner, 54. Auflg., Rn. 30 zu § 100g StPO).

II. § 100k Abs. 1 StPO-E verpflichtet die Diensteanbieter zur Auskunftserteilung im Hinblick auf die Bestandsdaten nach § 95 TKG, d. h. den für die Begründung des Vertragsverhältnisses bei den TK-Diensteanbietern vorhandenen u. a. Adressdaten. Diese Auskunft darf nur zu den bei den Strafverfolgungsbehörden bereits bekannten IP-Adressen erfolgen. Nach dem Diskussionsentwurf dient diese Maßnahme (allein) der Bekämpfung der Kinderpornographie im Internet. Hiermit soll die personelle Zuordnung (Identifizierung) der über die Internetportale der entsprechenden Seiten bereits ermittelten IP-Adressen erfolgen.

Die Anordnungsvoraussetzung für die Strafverfolgungsbehörden (ohne Richtervorbehalt) sind – wie bei § 100j StPO-E – denkbar niedrig. Es reicht aus, dass die Daten für die Erforschung des (irgendeines?) Sachverhaltes und die Ermittlung des Aufenthaltsortes eines Beschuldigten benötigt werden. Bereits diese Anordnungsvoraussetzung ist problematisch, weil das BVerfG in seiner Entscheidung vom 02.03.2010 (Absatz Nr. 289) die Auskünfte über Bestandsdaten ausdrücklich (nur) bei Vorliegen eines hinreichenden Anfangsverdachts oder bei einer konkreten Gefahr i. S. der polizeilichen Generalklauseln für zulässig erklärt hat.

Obwohl die Auskunftsverpflichtung gemäß § 100k StPO-E allein mit der Bekämpfung von Kinderpornografie im Internet begründet wird, bezieht sie sich dennoch – mangels gesetzlicher Beschränkungen – bedenklich weit auf alle Tatbestände des StGB.

Um die Zuordnung zu ermöglichen, wurde die Auskunftspflicht des § 100k StPO-E durch die Verpflichtung der Diensteanbieter zu einer anlasslosen 7-tägigen Speicherpflicht von bestimmten Verkehrsdaten nach § **113a TKG-E** (darunter auch IP-Adressen) ergänzt. Erst mithilfe dieser Daten kann festgestellt werden, wer wann unter welcher IP-Adresse mit dem Internet verbunden war. Die Verpflichtung zur Speicherung bezieht sich auf einen Zeitraum von 7 Tagen.

Es handelt sich hierbei um eine - wenngleich kurze – anlasslose Speicherung von Daten „auf Vorrat“.

In einem hohen Maße problematisch ist selbst auf Basis der vergleichsweise kurzen Dauer des „Einfrierens“, dass über die Identifizierung von IP-Adressen weitreichende anderweitige Informationsquellen ausgeschöpft werden können. Dies gilt nicht nur im Hinblick auf die bevorstehende Umstellung auf das neue Internet-Adress-System „IPv6“ mit dann konstanten IP-Adressen. Ist eine IP-Adresse erst einmal identifiziert, ermöglichen andere (den staatlichen Stellen z. B. nach § 15 Abs. 5 S. 4 TMG zugängliche) Internet-Nutzungsdaten

weitreichende Einblicke in ein „Internetleben“ einer Person, bis hin zu Telekommunikationsinhalten.

Auch hier – wie bei § 110j StPO-E – bietet § 113a Abs. 5 TKG-E mit seiner Verpflichtung gegenüber den Diensteanbietern, die gespeicherten Daten unverzüglich nach Ablauf von 7 Tagen zu löschen, keine genügende Sicherheit. Es fehlen auch hier entsprechende gesetzliche Vorkehrungen, mit denen den Gefahren durch entsprechende Zuwiderhandlungen des Dienstanbieters oder auch einer weiteren Verwertung der einmal erhobenen Daten durch die Ermittlungsbehörden begegnet werden könnte.

In der vorliegenden Form sind die Vorschläge des Diskussionsentwurfs demnach abzulehnen.

Teil II. Stellungnahme im Einzelnen

Der Diskussionsentwurf sieht u.a. Änderungen der StPO sowie der TKG vor.

I. Der neue §§ 100j StPO-E

§ 100j existierte bislang nicht. Mit § 100j StPO-E soll die Sicherung (Speicherung bzw. „Einfrieren“) von Verkehrsdaten im weitesten Sinne geregelt werden (nicht deren Erhebung, die weiterhin für strafprozessuale Zwecke dem § 100g StPO vorbehalten ist). Mit § 100k StPO-E wird die Auskunft über Bestandsdaten bei bereits vorhandenen IP-Adressen ermöglicht.

1. Regelungsumfang

Absatz 1 beinhaltet die Anordnungsbefugnis zur Sicherung von TK-Verbindungsdaten. Damit wird derjenige, der öffentlich zugängliche Telekommunikationsdienste erbringt, verpflichtet, die bei der Nutzung des Dienstes bereits erzeugten, verarbeiteten und künftig anfallenden Verkehrsdaten – wie in den Absätzen 3 und 4 des § 100j StPO-E im Einzelnen bezeichnet – zu sichern. Sinn und Zweck der Datensicherung ist, es den Strafverfolgungsbehörden kurzfristig zu ermöglichen, die ggf. routinemäßige Löschung von später vielleicht einmal relevant werdenden Daten zu verhindern. Voraussetzung für das „Einfrieren“ der Daten ist (allein), dass diese für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich sind (§ 100j Abs. 1 StPO-E). Insoweit handelt es sich also – im Vergleich zu der vom BVerfG aufgehobenen *anlasslosen* Vorrats-Speicherung nach § 113a TKG) um eine *anlassbezogene* Sicherungsanordnung (Diskussionsentwurf S. 15).

In den **Absätzen 3 und 4** des 100j StPO-E ist geregelt, auf welche Daten bezüglich Telefonie und Internetzugang sich die Sicherungs-Anordnung beziehen kann (z. B. Rufnummer, Kennung, Datum, Uhrzeit, internationale Kennung für mobile Teilnehmer, Funkzellen, im Falle von Internet-Telefondiensten auch IP-Adressen, SMS etc.). Die Absätze 3 und 4 sind vom Wortlaut nahezu identisch mit den Absätzen 2 und 4 des vom BVerfG aufgehobenen § 113a TKG a.F. In diesem früheren (§ 113a TKG a.F.) Kontext war klar, dass die TK-Diensteanbieter die entsprechenden Daten nur speichern müssen, wenn sie von ihnen bei der Nutzung der bereit gestellten TK-Dienste ohnehin erzeugt oder verarbeitet werden (Arndt/Fetzer/Scherer, TKG-Kom., Rn. 14 zu § 113a). Dieses ist auch hier vorgesehen, wobei auch die während der Laufzeit der Anordnung anfallenden Verkehrsdaten gespeichert werden dürfen (Diskussionsentwurf S. 15, 23).

Nach **Absatz 2** ist die Anordnung auf höchstens einen Monat zu befristen. Soweit die Voraussetzungen der Anordnung fortbestehen, ist eine Verlängerung um einen weiteren Monat möglich.

Für die Sicherung der TK-Daten reicht eine Anordnung von Polizei oder Staatsanwaltschaft aus (**Absatz 5**). Gewissermaßen als „Kompensation“ für diese niedrigere Eingriffsschwelle (Anordnung ohne Gericht) ist in § 100j **Abs. 1 Satz 2** StPO-E vorgesehen, dass eine Sicherungsanordnung dann unzulässig ist, wenn bereits bei ihrem Erlass absehbar ist, dass die Voraussetzungen für eine spätere Erhebung oder Verwendung der Daten nach § 100g StPO „voraussichtlich“ nicht vorliegen werden. D.h., wenn nicht sicher feststeht, dass es sich um eine Straftat von erheblicher Bedeutung oder einer mittels TK begangenen handelt, ist die Sicherungsanordnung unzulässig (vgl. Diskussionsentwurf S. 23).

Nach § 100j Abs. 5 StPO-E sind die gespeicherten Daten von den TK-Diensteanbietern unverzüglich nach Ablauf der ein- bzw. zweimonatigen Frist zu löschen.

2. Bewertung

a) Die im Diskussionsentwurf jetzt vorgelegten Regelungen entsprechen im Wesentlichen dem von der Bundesjustizministerin im Januar 2011 vorgelegten „Eckpunktepapier zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften“.

b) Die maximal 2-monatige Datensicherung („Einfrieren“) durch den neuen § 100j StPO-E muss zunächst vor dem Hintergrund gesehen werden, dass nach den §§ 96 ff. TKG Verkehrs- und Standortdaten von Telekommunikationsverbindungen bis zu 6 Monaten gespeichert („erhoben und verwendet“) werden können, wenn diese Daten zu den im 2. Abschnitt des 7. Teils des TKG genannten Zwecken (Abrechung, Aufbau und Aufrechterhalten der TK-Verbindung auch von IP-Adressen etc.) benötigt werden (vgl. Arndt/Fetzer/Scherer, TKG-Kom., Rn. 6 zu § 96 zum Problem der Weite der dadurch ermöglichten Datenerhebung).

   In diesem Zusammenhang ist anzumerken, dass die im Regierungsentwurf zur Novelierung u. a. des § 97 Abs. 4 S.2 TKG ursprünglich geplante Änderung, die für Zwecke der gegenseitigen Abrechnung zwischen den einzelnen Diensteanbietern verwendeten Daten nach 3 Monaten zu löschen (BT-Drs. 17/5707, S. 30), nicht übernommen wurde (entsprechend der Beschlussempfehlung des Ausschusses für Wirtschaft und Technologie am 27.10.2011 im BT: 17/7521; endgültiger Gesetzesentwurf: BT-Drs. 685/11, S. 45). Das Gesetz befindet sich zurzeit im Vermittlungsausschuss. Es ist zu erwarten, dass es bei der derzeitigen Rechtslage verbleibt, wonach die Daten so lange verwendet werden dürfen, wie dies aus Abrechnungszwecken erforderlich ist. Auch hiermit hätte der Gesetzgeber eine Chance zur Regulierung der Datenspeicherung vertan.

Eine Erhebung bzw. Auswertung dieser Daten für Zwecke der Strafverfolgung ist auch ohne § 100j StPO-E jederzeit über § 100g StPO möglich unter der Voraussetzung, dass der Verdacht einer schweren Straftat oder einer Straftat mittels Telekommunikation begründet ist. Außerdem besteht die Möglichkeit eines „Manuellen Auskunftsverfahrens“ nach § 113 TKG, mit dem u. a. Strafverfolgungsbehörden, Verfassungsschutz und MAD Auskünfte über die nach § 95 TKG (Bestandsdaten) und § 111 TKG (Kundendaten für Auskunftsersuchen der Sicherheitsbehörden) erhobenen und gespeicherten Daten einholen dürfen.

§ 100j StPO-E verfolgt demzufolge offenkundig den Regelungszweck, das „Einfrieren“ von Daten schneller (ohne Richtervorbehalt) und einfacher (Voraussetzung: Ermittlung des Sachverhalts oder Aufenthaltsort des Beschuldigten) bewirken zu können und damit nicht zuletzt einer Löschung von nicht mehr benötigten Verkehrsdaten durch die TK-Diensteanbieter nach den §§ 96 ff. TKG vorzubeugen. Weiter als die Diensteanbieter unter den Voraussetzungen der §§ 96 ff. TKG speichern dürfen, reichen auch die Sicherungsmöglichkeiten nach § 100j StPO-E nicht.

c) Bereits der Informationsrechtsausschuss des DAV hat in seiner Stellungnahme zu § 100j StPO-E auf den Widerspruch in den Anordnungsvoraussetzungen hingewiesen, der darin liegt, dass auf der einen Seite durch die Polizei oder Staatsanwaltschaft die Sicherung der Daten angeordnet werden kann, wenn dies zur Erforschung des Sachverhalts oder der Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist (§ 110j Abs. 1 StPO-E), auf der anderen Seite aber die Zulässigkeit der Sicherungsanordnung auch davon abhängig gemacht wird, dass „voraussichtlich“ die Voraussetzungen für eine Erhebung der Daten (nach § 100g StPO, also: schwere Straftat oder eine solche mittels TK) vorliegen.

Im Interesse der Eindeutigkeit der Vorschrift sollte deshalb klargestellt werden, dass die Sicherung der Daten nach § 100j StPO-E, die zur Sachverhaltsaufklärung oder der Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist, nur in den Fällen erfolgen darf, in denen ein Tatverdacht i. S. des § 100g StPO besteht.

d) Dass mit der engen systematischen Anbindung des § 100j StPO-E an die Voraussetzungen des § 100g StPO eine enge Verknüpfung zwischen den Sicherungsvoraussetzungen und den Erhebungsvoraussetzungen hergestellt wird, ist des Weiteren auch aus folgenden Gründen nicht unproblematisch:

Die als „Kompensation“ für die niedrige Eingriffsschwelle bei der Datensicherung (Anordnung ohne Richtervorbehalt) gedachte Anbindung an die engeren Voraussetzungen des § 100g StPO könnte in der Praxis den Eindruck vermitteln,

dass in den Fällen, in denen – auf niedriger Anordnungsstufe – die Datensicherung zulässig ist, „automatisch“ bereits die Frage der Zulässigkeit auch der Erhebung und Verwendung der Daten „geklärt“ sei; denn die Sicherung ist nur dann erlaubt, wenn die Voraussetzungen des § 100g StPO zu bejahen sind.

Auf der anderen Seite dürfte ein Bejahen der Zulässigkeitsvoraussetzungen des § 100g StPO für die Datensicherung nach § 100j StPO-E in der Praxis nicht wirklich ein Problem sein. Da man vor der Erhebung der Daten nie weiß, welche Erkenntnisse man gewinnen wird, wird sich vor einer Sicherung auch nie sicher ausschließen lassen, dass die Voraussetzungen des § 100g StPO „voraussichtlich“ nicht gegeben sind. Auch bei einem vagen Anfangsverdacht auf eine (nur) leichte Straftat wird man regelmäßig argumentieren können, dass die TK-Daten „voraussichtlich“ Beweise liefern werden, die im Hinblick auf eine schwere Straftat (z. B. bandenmäßige Begehung) oder eine mittels TK verübte dienlich sein könnten. Damit wird es praktisch in keinem Fall zu einer unzulässigen Anordnung kommen. Dies gilt umso mehr, als keine Rechtsmittel- oder Beschwerdemöglichkeiten isoliert gegen die Sicherung nach § 100j StPO-E existieren und damit Polizei oder Staatsanwaltschaft über die Zulässigkeit ihrer Anordnung immer selbst befinden werden.

Diese sich wechselseitig beeinflussenden Zulässigkeitsvoraussetzungen können in der Praxis (leicht) dazu führen, dass die niedrigeren Eingriffsanforderungen der – isoliert betrachtet wenig eingriffsintensiven – Datensicherung incidenter die strikteren Voraussetzungen des § 100g StPO „aufweichen“. Eine bereits erfolgte Sicherungsanordnung suggeriert, dass auch bereits die Voraussetzungen des § 100g StPO geprüft und bejaht wurden. Ein Übriges wird die „Macht des Faktischen“ bewirken: Wenn die Daten schon einmal gesichert sind, muss man sie doch wohl auch auswerten dürfen.

e) Eine solche schleichende „Verwässerung“ der Anforderungsvoraussetzungen kann sich § 100g StPO nicht leisten. Zwar ist in dem Diskussionsentwurf davon die Rede, dass das BVerfG § 100g StPO – abgesehen von der Bezugnahme auf die Vorschrift über die Vorratsdatenspeicherung nach § 113a TKG a.F. – in seinem Urteil nicht beanstandet habe (Diskussionsentwurf S. 22). Dies trifft so aber nicht zu. Das BVerfG hat sich vielmehr bemerkenswert kritisch zur Weite des § 100g StPO geäußert. Es heißt hierzu im Urteil des BVerfG (Rn. 279):

> *„Schon § 100g Abs. 1 Satz 1 Nr. 1 StPO stellt nicht sicher, dass allgemein und auch im Einzelfall nur schwerwiegende Straftaten Anlass für eine Erhebung der entsprechenden Daten sein dürfen, sondern lässt – unabhängig von einem abschließenden Katalog – generell Straftaten von erheblicher Bedeutung genügen. Erst recht bleibt § 100g Abs.1 Satz 1 Nr. 2, Satz 2 StPO*

hinter den verfassungsrechtlichen Maßgaben zurück, indem er unabhängig von deren Schwere jede mittels Telekommunikation begangene Straftat nach Maßgabe einer allgemeinen Abwägung im Rahmen einer Verhältnismäßigkeitsprüfung als möglichen Auslöser einer Datenabfrage ausreichen lässt. Mit dieser Regelung werden die nach § 113a TKG gespeicherten Daten praktisch in Bezug auf alle Straftatbestände nutzbar. Ihre Verwendung verliert damit angesichts der fortschreitenden Bedeutung der Telekommunikation im Lebensalltag ihren Ausnahmecharakter. Der Gesetzgeber beschränkt sich hier nicht mehr auf die Verwendung der Daten für die Verfolgung schwerer Straftaten, sondern geht hierüber – und damit auch über die europarechtlich vorgegebene Zielsetzung der Datenspeicherung, die sich auch ihrerseits allein auf die Verfolgung von schweren Straftaten ohne Einschluss der Gefahrenprävention beschränkt – weit hinaus."
(Unterstreichung nur hier)

Deshalb hat das BVerfG nicht zuletzt im Hinblick auf die richterliche Anordnung der Erhebung von Verkehrsdaten i. S. der §§ 100g Abs.2 i. V .m. 100b Abs. 2 StPO eine gesetzliche Regelung angemahnt, die eine „substantiierte Begründung" gewährleistet (BVerfG, a.a.O., Rn. 284, vgl. auch Rn. 281 zu den nicht genügenden Anforderungen an die Ausgestaltung der Benachrichtigungspflicht in § 100g StPO; nunmehr in § 100g Abs. 2 S. 1 StPO etwas modifizierter).

f) Besondere Beachtung verdient das „Einfrieren" der Verkehrsdaten mittels § 100j StPO-E auch unter dem Aspekt, dass von der Sicherung auch IP-Adressen erfasst werden können (§ 100j Abs. 3 Ziff. 5 StPO-E; vgl. auch Arndt/Fetzer/Scherer, TKG-Kom., Rn. 30 zu § 113a unter Hinweis auf den insoweit identischen Regelungsumfang des aufgehobenen § 113a Abs. 4 TKG,).

Hierbei taucht allerdings folgendes Problem auf: § 100g StPO erlaubt die Erhebung von Verkehrsdaten gemäß § 96 Abs. 1 TKG. IP-Adressen werden nach der (strafrechtlichen) Rechtsprechung aber grundsätzlich als Bestandsdaten angesehen (LG Würzburg NStZ-RR 2006, 46 f.; LG Stuttgart, NJW 2005, 614 ff.; a. A. Arndt/Fetzer/-Scherer, TKG-Kom., Rn. 3 (Fn. 3) zu § 95 unter Hinweis darauf, dass die dynamische IP-Adresse nicht zur Vertragsabwicklung mit dem Diensteanbieter erforderlich ist). Danach liefe die Verwertung von aufgrund des § 100j StPO-E „eingefrorenen" IP-Adressen über § 100g StPO aber ins Leere. Von § 100g StPO werden nur Verkehrsdaten erfasst.

Demgegenüber geht der Diskussionsentwurf aber davon aus, dass IP-Adressen Verkehrsdaten sind (s. unten S. 15). Auch der Informationsrechtsausschuss des DAV

weist daraufhin, dass die Definitionsgrenzen bei IP-Adressen fließend sind und z. B. nach § 101 Abs. 9 UrhG die IP-Adressen als Verkehrsdaten angesehen werden (Kuper ITRB 2009, 13 f.).

Diese Defizite in der rechtlichen Kategorisierung wiegen schon deshalb schwer, weil es sich bei IP-Adressen um besonders sensible Daten handelt. Mittels der IP-Adressen und der Anschlusskennung kann im Prinzip jede Bewegung im Internet auf Webseiten oder anderen Internet-Diensten einem konkreten Anschlussinhaber zugeordnet werden. Daraus kann zusammen mit anderen Verkehrsdaten ohne weiteres ein nahezu komplettes Persönlichkeitsprofil und Bewegungsbild erstellt werden (Arndt/Fetzer/Scherer, TKG, Rn. 30 zu § 113a; BVerfG, a.a.O., Rn. 259).Auch die nach § 100j StPO-E nur in einem Zeitraum von zwei Monaten gesicherten Daten können somit bei ihrer Erhebung und Verknüpfung mit anderen Daten grundsätzlich einen schwerwiegenden Eingriff in die Persönlichkeitsrechte bewirken. Dies gilt umso mehr, als mit der für Ende 2011 geplanten Umstellung auf das neue Internet-Adress-System „IPv6“ mit dann nicht mehr „dynamischen“, sondern konstanten IP-Adressen durch die einmalige Identifizierung einer IP-Adresse auf Monate hinweg dem Staat Einblick in alle Internet-Aktivitäten einer Person ermöglicht werden.

g) Schließlich ist unklar, wie der 2-Monatszeitpunkt, auf den sich maximal die Sicherung beziehen kann, zu berechnen ist. Gelten die maximal 2 Monate für einen Monat in der Vergangenheit und einen in der Zukunft? Oder ist durch 2 Monate in der Vergangenheit die Sicherung für die Zukunft „verbraucht“?

h) Dass nach § 100j Abs. 5 StPO-E die gespeicherten Daten von den TK-Diensteanbietern unverzüglich nach Ablauf der ein- bzw. zweimonatigen Frist zu löschen sind, bietet keine ausreichende Sicherheit gegen Zuwiderhandlungen der Diensteanbieter oder der weiteren Verwendung der Erkenntnisse der Daten durch die Ermittlungsbehörden, selbst wenn sich im Nachhinein herausstellt, dass die Anordnung von vorneherein unzulässig war.

II. Der neue § 100k StPO-E i. V. m. § 113a TKG-E und § 113b TKG-E

1. Regelungsumfang

a) § 100k **Abs. 1** StPO-E verpflichtet die Diensteanbieter zur Auskunftserteilung im Hinblick auf die in § 113 TKG („Manuelles Auskunftsverfahren“) in Bezug genommenen Daten. Dies – von § 113 TKG in Bezug genommenen Daten – sind zum einen die Bestandsdaten nach **§ 95 TKG**, bei denen es sich nach der Definition in § 3 Nr. 3 TGK um Daten eines Teilnehmers handelt, „*die für die*

Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden“.

Die daneben in § 113 TKG genannten Daten sind die „Daten für Auskunftsersuchen der Sicherheitsbehörden“ nach **§ 111 TKG**, u. a. Rufnummern und andere Anschlusskennungen, Namen und Anschrift des Anschlussinhabers, Anschrift des Teilnehmers, Gerätenummer bei Mobile.

Für diese Bestandsdaten besteht bereits nach der geltenden Gesetzeslage eine Speicherungspflicht, auch soweit sie für betriebliche Zwecke der TK-Diensteanbieter nicht erforderlich sind (§ 111 Abs. 1 Satz 1 TKG). Strafverfolgungsbehörden dürfen die Herausgabe dieser Bestandsdaten nach der Ermittlungsgeneralklausel (§ 161 Abs. 1 Satz 2, § 163 StPO i. V. m. § 113 Abs. 1 TKG) verlangen, wenn diese für die Verfolgung einer verfahrensgegenständlichen Straftat erforderlich sind. Einer gerichtlichen oder staatsanwaltschaftlichen Anordnung bedarf es nicht.

Die Verpflichtung der Diensteanbieter zur Auskunft nach **§ 100k Abs. 1 StPO-E** setzt voraus, dass die in § 113 TKG in Bezug genommenen Bestandsdaten für die Erforschung des Sachverhaltes und die Ermittlung des Aufenthaltsortes eines Beschuldigten erforderlich sind. Auch hier sind also die Anordnungsvoraussetzungen niedrig. Es gibt keinen Richtervorbehalt und alle Straftaten können Anlass für eine solche Auskunft an die Strafverfolgungsbehörden sein. Der Diskussionsentwurf vertritt die Auffassung (S. 25), dass das BVerfG in seiner Entscheidung vom 02.03.2010 (Rn. 289) klargestellt habe, dass derartige Auskünfte nach § 113 TKG bei Vorliegen eines hinreichenden Anfangsverdachts oder bei einer konkreten Gefahr i. S. der polizeilichen Generalklauseln zulässig sind.

§ 100k **Abs. 2** StPO-E sieht vor, dass die Auskunft über die Bestandsdaten nach § 113 TKG auch zu den bei den Strafverfolgungsbehörden bereits bekannten IP-Adressen erfolgen kann. Hiervon verspricht man sich Erkenntnisse bei der Bekämpfung von Kinderpornographie im Internet, nicht zuletzt mittels einer dadurch ermöglichten Ermittlung des Aufenthaltsortes von Verdächtigen (Diskussionsentwurf S. 1, 29).

b) Mit den den Strafverfolgungsbehörden bereits bekannten IP-Adressen und den reinen Bestandsdaten wäre allerdings noch keine personenbezogene Zuordnung möglich. Zu einer personenbezogenen Identifizierung gehört noch das Wissen darüber, welcher durch die Bestandsdaten namhaft zu machenden Person der Netzanbieter die betreffende (bekannte) IP-Adresse zugeordnet hat. Deshalb haben die Verfasser des Diskussionsentwurfs die Auskunftspflicht des § 100k StPO-E durch die Verpflichtung der Diensteanbieter zu einer 7-tägigen Speicherpflicht von bestimmten

Verkehrsdaten nach § **113a TKG-E** angereichert (Diskussionsentwurf S. 27). Mittels dieser – auf „Vorrat“ 7 Tage lang gespeicherten – Verkehrsdaten kann dann nämlich festgestellt werden, wer wann unter welcher IP-Adresse mit dem Internet verbunden war. Und es wird damit verhindert, dass der Diensteanbieter diese von ihm – z. B. zu Abrechnungszwecken – erhobenen Daten kurzfristig löscht.

Nach § **113 a Abs. 2** TKG-E sind folgende Verkehrsdaten für 7 Tage zu speichern:

- die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse (IP-Adresse),
- eine eindeutige Kennung des Anschlusses, über den die Internet-Nutzung erfolgt,
- Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone von Beginn und Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse.

Die Verpflichtung zur Speicherung besteht nur, soweit die Daten bei der Erbringung des Diensteanbieters tatsächlich erzeugt oder verarbeitet werden (Diskussionsentwurf S. 28).

Nach § **113a Abs. 3** TKG-E dürfen der Inhalt der Kommunikation und Daten über aufgerufene Internetseiten nicht gespeichert werden.

c) **§ 113b TKG-E** regelt, dass die nach § 113a TKG-E gespeicherten Verkehrsdaten (z. B. IP-Adressen) nicht generell für Auskünfte über Bestandsdaten nach § 113 TKG verwendet werden dürfen, sondern nur für Auskünfte über vorher den Strafverfolgungsbehörden bereits bekannte Internetprotokoll-Adressen (Diskussionsentwurf S. 29 f.). Diese enge Zweckbegrenzung für die Auskunft soll auch dann gelten, wenn die Daten nach § 100j StPO-E gesichert wurden.

Schließlich dürfen die nach § 113a TKG-E gespeicherten Daten nicht an die Strafverfolgungsbehörden herausgegeben werden (§ 113b Abs. 2 TKG-E und Diskussionsentwurf S. 30).

d) Nach § 100k Abs. 5 StPO-E sind die gespeicherten Daten von den TK-Diensteanbietern unverzüglich nach Ablauf der einwöchigen Frist zu löschen

2. Bewertung

a) Der Diskussionsentwurf geht auch bei § 100k StPO-E i. V. m. den §§ 113a und 113b TKG-E davon aus, dass es sich bei den IP-Adressen um Verkehrsdaten handelt – entgegen der bisher in der strafrechtlichen Rechtsprechung und Literatur vertretenen

Auffassung, nach der selbst die dynamischen IP-Adressen als Bestandsdaten i. S. des § 95 TKG angesehen werden (oben S. 13).

b) Soweit der Diskussionsentwurf die Auffassung vertritt (S. 25), dass das BVerfG in seiner Entscheidung vom 02.03.2010 (Rn. 289) klargestellt habe, dass Auskünfte über Bestandsdaten bei Vorliegen eines hinreichenden Anfangsverdachts oder bei einer konkreten Gefahr i. S. der polizeilichen Generalklauseln zulässig sind, ist bei § 100k Abs. 1 StPO-E nicht erkennbar, dass diesen Voraussetzungen entsprochen wurde. In § 100k StPO-E wird als Voraussetzung der Auskunftsverpflichtung lediglich genannt, dass die in § 113 TKG in Bezug genommenen Daten für die Erforschung des Sachverhaltes (welches?) und die Ermittlung des Aufenthaltsortes eines Beschuldigten erforderlich sein müssen. Diese Anforderungen sind niedriger als die, die das BVerfG angesprochen hat.

c) Bei der Speicherung von Verkehrsdaten handelt es sich um eine anlasslose Vorratsdatenspeicherung, die als solche vom BVerfG als verfassungswidrig angesehen wurde, wenn auch nur für 7 Tage.

d) In einem hohen Maße problematisch ist – auch auf Basis einer vergleichsweise kurzen Dauer des „Einfrierens“ –, dass über die Identifizierung von IP-Adressen weitreichende anderweitige Informationsquellen ausgeschöpft werden können. Dies nicht nur im Hinblick auf die bevorstehende Umstellung auf das neue Internet-Adress-System „IPv6“ mit dann konstanten IP-Adressen.

Der AK Vorrat verweist in seiner Stellungnahme vom Juni 2011 daraufhin, dass die Identifizierung der IP-Adresse in Verbindung mit Internet-Nutzungsdaten, die staatliche Stellen ohne richterliche Anordnung von den Internetanbietern nach § 15 Abs. 5 S. 4 TMG anfordern können, mit einer identifizierten IP-Adresse sogar der Inhalt der Telekommunikation einer Person nachzuvollziehen ist:

„Ist ein Pseudonym (Benutzerkonto) über die IP-Adresse des Nutzers erst einmal identifiziert, ermöglichen Nutzungsdaten des Anbieters oft die Rückverfolgung jedes Klicks und jeder Eingabe des Inhabers über Tage, Wochen und Monate hinweg. Daneben wird in die meisten E-Mails die IP-Adresse des Absenders aufgenommen, ohne dass man einfach eine Unterdrückung dieser ‚Rufnummernübermittlung’ wählen könnte. Durch eine IP-Vorratsdatenspeicherung werden Meinungsäußerungen per E-Mail ohne Furcht vor Nachteilen unmöglich. Schließlich ermöglichen es IP-Adressen gerade beim mobilen Internetzugang, Bewegungsprofile zu erstellen, weil aus der jeweiligen IP-Adresse der ungefähre Standort des Nutzers ermittelt werden kann.“ (AK-Vorrat, S. 2).

Insofern ist nicht von der Hand zu weisen, wenn der AK Vorrat auch in einer nur kurzzeitigen, anlasslosen Speicherung von Internet-Verbindungsdaten den vom BVerfG bezeichneten „*Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt*“, sieht, der geeignet ist, „*ein diffus bedrohliches Gefühl des Beobachtetseins*“ hervorzurufen, „*das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann*“ (AK Vorrat, S. 2 unter Hinweis auf die Entscheidung des BVerfG vom 02.03.2010).

Sind die IP-Adressen dann auch noch konstant, wird dem Staat auf Monate hinweg Einblick in alle Internet-Aktivitäten einer Person ermöglicht.

Dass nach § 113a Abs. 5 StPO-E die gespeicherten Daten von den TK-Diensteanbietern unverzüglich nach Ablauf der einwöchigen Frist zu löschen sind, bietet keine ausreichende Sicherheit gegen Zuwiderhandlungen der Diensteanbieter oder der weiteren Verwendung der Erkenntnisse der Daten durch die Ermittlungsbehörden, selbst wenn sich im Nachhinein herausstellt, dass die Anordnung von vorneherein unzulässig war.