BUNDESRECHTSANWALTSKAMMER

Stellungnahme Nr. 35
Juni 2012

zum Diskussionsentwurf eines „Gesetzes zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet“ des Bundesministerium der Justiz vom 07.06.2011 (Vorratsdatenspeicherung)

Mitglieder des Strafrechtsausschusses

RA Prof. Dr. Dr. Alexander Ignor, Vorsitzender
RA Dr. Jan Bockemühl
RA Prof. Dr. Alfred Dierlamm
RA Thomas C. Knierim (Berichterstatter)
RA Dr. Daniel M. Krause
RA Prof. Dr. Holger Matt
RAin Anke Müller-Jacobsen
RA Prof. Dr. Tido Park
RA Prof. Dr. Reinhold Schlothauer
RA Dr. Jens Schmidt (Berichterstatter)
RAin Dr. Anne Wehnert
RAin Dr. Annette von Stetten
RA Frank Johnigk, Bundesrechtsanwaltskammer

Verteiler: Bundesministerium der Justiz
Rechtsausschuss des Deutschen Bundestages
Arbeitskreise Recht der Bundestagsfraktionen
Landesjustizminister/Justizsenatoren der Länder
Rechtsanwaltskammern
Bundesverband der Freien Berufe
Bundesnotarkammer
Bundessteuerberaterkammer
Deutscher Steuerberaterverband
Wirtschaftsprüferkammer
Institut der Wirtschaftsprüfer
Deutscher Anwaltverein
Deutscher Notarverein
Deutscher Richterbund
Deutscher Juristinnenbund
Bundesvorstand Neue Richtervereinigung
Redaktionen der NJW, Strafverteidiger, Neue Zeitschrift für Strafrecht, ZAP Verlag,

Bundesrechtsanwaltskammer
The German Federal Bar
Barreau Fédéral Allemand
www.brak.de

Büro Berlin – Hans Litten Haus
Littenstraße 9
10179 Berlin
Deutschland
Tel. +49.30.28 49 39 - 0
Fax +49.30.28 49 39 -11
Mail zentrale@brak.de

Büro Brüssel
Avenue des Nerviens 85/9
1040 Brüssel
Belgien
Tel. +32.2.743 86 46
Fax +32.2.743 86 56
Mail brak.bxl@brak.eu

Zeitschrift für höchstrichterliche Rechtsprechung im Strafrecht

Die Bundesrechtsanwaltskammer ist die Dachorganisation der anwaltlichen Selbstverwaltung. Sie vertritt die Interessen der 28 Rechtsanwaltskammern und damit der gesamten Anwaltschaft der Bundesrepublik Deutschland mit zurzeit rund 157.000 Rechtsanwältinnen und Rechtsanwälten gegenüber Behörden, Gerichten und Organisationen - auf nationaler, europäischer und internationaler Ebene.

Stellungnahme

1. A. Leitlinien

Der Strafrechtsausschuss der Bundesrechtsanwaltskammer hat

- vor dem Hintergrund andauernder politischer Diskussionen um die Gründe und Wirkungen der sog. Vorratsdatenspeicherung,
- in Anbetracht der verfassungsrechtlich gebotenen Anforderungen an eine innerstaatliche Umsetzung nach dem Urteil des Bundesverfassungsgerichts vom 2. März 2010 (1 BvR 256/08) über die Nichtigkeit der erst 2007 eingeführten Regelungen zur Vorratsdatenspeicherung,
- unter Berücksichtigung der verfassungs- und datenschutzrechtlichen Bedenken europäischer Staaten gegen die Eingriffe in bürgerliche Freiheitsgrundrechte durch eine einschränkungslose Umsetzung der EU-Richtlinie 2006/24/EG, sowie
- im Licht neuerer Erkenntnisse der Rechtstatsachenforschung über den Bedarf und den Umgang mit Vorratsdaten für Zwecke der Strafverfolgung

über den DiskE des BMJ vom 7. Juni 2011 beraten. Angesichts unterschiedlicher Modelle für eine gesetzliche Umsetzung der EU-Vorgaben erscheint es erforderlich, folgende Leitlinien voranzustellen:

1. Die Grundrechte auf Verwirklichung einer freien Telekommunikation, auf Gewährleistung der Vertraulichkeit und der Integrität informationstechnischer Systeme sowie auf freie Entfaltung der Persönlichkeit des einzelnen Bürgers und der Unternehmen gewährleisten den uneingeschränkten Zugang und die freie Nutzung aller gewerblich oder privat angebotenen Dienste für Bild-, Sprach- oder Datenkommunikation. Diese Grundrechte beanspruchen grundsätzlichen Vorrang vor staatlicher Steuerung und Überwachung.

2. Eine zu Strafverfolgungszwecken einzurichtende, gesetzlich verpflichtende langfristige **Bevorratung von Daten** über das Kommunikationsverhalten der Bürger und Unternehmen, insbesondere auch der Anwaltschaft, **ohne** einen begründeten **Anlass** mit der Möglichkeit unkontrollierter Rasterung durch Strafverfolgungs-, Gefahrenabwehrbehörden und Nachrichtendienste stigmatisiert. Sie ist ein **Fremdkörper in einer freiheitlichen Grundordnung**, dessen Einsatz auch nicht durch vermeintlich präventive oder repressive Informations- und Auswertungsbedürfnisse gerechtfertigt werden kann. Schon rechtstatsächlich gesehen setzt die Verwirklichung staatlicher Ordnungs-, Sicherheits- und Strafverfolgungsaufgaben keine langfristige, allgemeine Bevorratung von elektronischen Kommunikationsdaten voraus.

3. Der rechtlich schwerwiegende Eingriff in die Grundrechte aller Bürger, d.h. sowohl der aktiven als auch der passiven Teilnehmer an der Telekommunikation, bedarf daher einer eindeutigen gesetzlichen Grundlage, die den konkreten Speicherungs- und Abrufzweck benennt, eine nachprüfbare Definition der für solche Zwecke zu bevorratenden Daten enthält, die normenklare Abgrenzung der unterschiedlichen Datenbestände, besondere Sicherungs- und Schutzmechanismen gegen unbefugten Abruf oder missbräuchliche Verwendung umfasst sowie eine effektive, nicht ausschließlich behördeninterne Kontrolle der Verarbeitung, Speicherung und Löschung solcher Vorratsdaten sicherstellt. Werden Strafverfolgungszwecke außerhalb der bereits bestehenden Regelungen des Strafverfahrensrechts verfolgt, ist der Gesetzgeber gehalten, die den Einzelnen schützenden Vorgaben des Strafverfahrensrechts in der jeweils zu schaffenden Rechtsgrundlage eigenständig aufzunehmen.

4. Mit Blick auf den europaweiten Wettbewerb der Telekommunikationsanbieter sind die Speicherung, Übertragung und Löschung solcher Vorratsdaten durch möglichst einheitliche Grundsätze, Mittel und Verfahren zur Gewährleistung von Marktgerechtigkeit, zur effektiven Kontrolle der Telekommunikationsdienstleister sowie zur Begrenzung des Missbrauchs derartiger Datenbestände in der Europäischen Union einzurichten. Soweit ausländische Anbieter solcher Dienstleistungen unterschiedlichen Datenschutzvorgaben in ihren jeweiligen Sitzländern unterworfen sind, sind ein hohes einheitliches Datenschutzniveau, geeignete Sicherungskonzepte und vorbeugende Sperren sowie eine strenge, effektive Aufsicht über die Datenspeicherungs- und –verwendungspraxis solcher Unternehmen vorzusehen.

5. Eine im Einzelfall anlassbezogene langfristige Speicherung von Telekommunikationsdaten zu Zwecken der Strafverfolgung bedarf einer stets aktuellen, individuellen Rechtfertigung eines solchen Eingriffs aufgrund einer dokumentierten, nachträglich überprüfbaren fallbezogenen Abwägung von erheblichen Rechtsgütern sowie der zeitpunktbezogenen Feststellung von Erforderlichkeit, Geeignetheit und Verhältnismäßigkeit des Eingriffs in einem Verfahren, das rechtsstaatlichen Garantien unterworfen ist.

6. Ein Richtervorbehalt entspr. §§ 100b Abs. 1, 100g Abs. 2, 105 StPO ist dann vorzusehen, wenn personenbezogene Daten über die Durchführung der Telekommunikation (Verbindungsdaten) aus dem Verfügungsbereich von Telekommunikationsanbietern zu Zwecken der Strafverfolgung abgerufen und verarbeitet werden sollen.

7. Die Eingriffsvoraussetzungen in einen etwaigen, umfassend angelegten Vorratsdatenbestand für Zwecke der Gefahrenabwehr und der Nachrichtendienste sind noch restriktiver auszugestalten. Nur ausgesuchte Rechtsgüter wie bspw. der Schutz von Leib und Leben sowie überragende Rechtsgüter der Allgemeinheit dürfen hier in der Güterabwägung eingesetzt werden, zudem sind höhere Verdachtsschwellen, enge Verwendungsgrenzen, kurze Speicherfristen und zuverlässige Löschungsroutinen vorzusehen.

8. In allen Fällen sind sowohl die Anforderungen an Speicherung, Übertragung, Verwendung und zuverlässige wie auch zeitnahe Bearbeitung und Löschung abgerufener Daten gesetzlich so präzise zu beschreiben, dass eine unabhängige gerichtliche Nachkontrolle den Eingriff nachvollziehen und ihn nach verfassungsrechtlichen Grundsätzen auf Rechtmäßigkeit und Verhältnismäßigkeit beurteilen kann.

9. Die gelegentlich einer solchen Kommunikation erzeugten technischen Daten einschließlich der Geräte- und Standortdaten dürfen ohne Zustimmung der Kommunikationsteilnehmer grundsätzlich ebenso wenig unter einem Regulierungs- oder Beobachtungsregime staatlicher Behörden stehen, wie bspw. andere Daten über die Fortbewegung von Fahrzeugen oder Personen im öffentlichen Straßenverkehr, wie Bankkonto- oder Kreditkartendaten oder Personaldaten in Unternehmen. Der von derartigen Grundrechtseingriffen Betroffene muss möglichst rechtzeitig vorher, spätestens aber dann, wenn eine unmittelbare Gefährdung übergeordneter wichtiger Rechtsgüter nicht mehr besteht, von den heimlichen Maßnahmen nach Art und Umfang unterrichtet werden. Ihm muss umfassend die Gelegenheit gegeben werden, die Gründe des Abrufs sowie die Verwendung der Vorratsdaten zu erfahren. Die muss gerichtlich überprüfbar sein (vgl. dazu § 101 StPO).
10. Eine unzulässige Speicherung, ein unerlaubter Zugriff auf den Vorratsdatenbestand, der anlasslose Abruf von Vorratsdaten oder die unerlaubte Weiterverwendung abgerufener Vorratsdaten sind als Eingriffe in die Telekommunikation zu verbieten und mit wirksamen strafrechtlichen Sanktionen zu belegen.

Diese Leitlinien werden im DiskE, der ein anlassbezogenes sog. „Quick-Freeze-Verfahren“ konsequent in die Normenhierarchie der Strafprozessordnung einbettet, in weiten Teilen verwirklicht. Zwar hat sich das BVerfG im Urteil vom 2. März 2010 (1 BvR 256/08) nicht mit einem solchen Verfahren auseinandergesetzt, da es noch nicht Gegenstand der Gesetzgebung zur Telekommunikationsüberwachung gewesen ist. Allerdings ist durch die klare Begrenzung auf eine konkrete, anlassbezogene und nachweisbare strafrechtliche Verfolgungssituation im Sinne des § 152 Abs. 2 StPO eine begrüßenswerte Einbettung der Strafverfolgungszwecke in die Normumgebung des Strafverfahrensrechts vorgesehen, was einer angemessenen Gewichtung von Freiheitsrechten einerseits und staatlichen Verfolgungsinteressen andererseits entspricht. Damit wird der Entscheidung des BVerfG durch eine alternative Lösung Rechnung getragen. Eine von dem DiskE abweichende Absenkung der Eingriffs- und Schutzvoraussetzungen ist ebenso wie ein Verzicht auf vorbeugende Sperren und nachfolgende Kontrollen dagegen strikt abzulehnen. Auch sind im weiteren Gesetzgebungsverfahren höhere Abrufschwellen für anlassabhängige Abrufe von Kommunikationsdaten einzuführen.

B. Rechtsstaatliche Gewährleistungen

I. Vorratsdatenspeicherung im Sinne des DiskE

1. Die folgende Stellungnahme behandelt „Vorratsdaten“ als die längerfristig gespeicherten Bestandsdaten (§ 95 TKG) und darauf bezogene Verkehrsdaten (§ 96 TKG) der Bild-, Ton- und Daten-Kommunikation. Die vergleichbar bei dem Verbindungsauf- und -abbau entstehenden, langfristig zu speichernden Daten der Internet- und sonstigen Datenübermittlungssysteme werden ebenfalls zu dem Begriff der „Vorratsdaten“ gezählt. Davon zu unterscheiden sind Inhaltsdaten, die die Inhalte der Kommunikation selbst betreffen. Standortdaten werden bei der Einbuchung eines Gerätes an eine Funkstation erzeugt. Alle diese Daten werden vom Schutzbereich der Grundrechte auf Verwirklichung einer freien Telekommunikation, auf Gewährleistung der Vertraulichkeit und der Integrität informationstechnischer Systeme sowie auf freie Entfaltung der Persönlichkeit des

einzelnen Bürgers und der Unternehmen erfasst. Der DiskE selbst sieht eine „Vorratsdatenspeicherung“ im Sinne des Urteils des BVerfG nur für eine kurzfristige Speicherung der IP-Adressen gem. § 113a TKG n.F. vor,

2. Europarechtlich wird die Zulässigkeit einer anlasslosen Vorratsdatenspeicherung zu Strafverfolgungszwecken durch die EU-Richtlinie 2006/24/EG vorausgesetzt, aber nicht als solche bestätigt. Im Evaluierungsbericht der EU-Kommission vom 18. April 2011 (Komm 2011/225) sowie im Bericht des Europäischen Datenschutzbeauftragten vom 31. Mai 2011 wird erhebliche Kritik an einzelstaatlichen Umsetzungen der Richtlinie geäußert. Das Bundesverfassungsgericht hat im Urteil vom 2. März 20101 keine generelle verfassungsrechtliche Unzulässigkeit der anlasslosen Vorratsdatenspeicherung angenommen, da es eine anders gestaltete Umsetzung der EU-Richtlinie für möglich erachtete.

3. Gegen die Zulässigkeit einer europaweit auf dem Gebiet der Strafverfolgung und der Telekommunikation vorgegebenen Datenspeicherung sprechen die von den EU-Ländern Rumänien und Tschechien – aufgrund eigener verfassungsgerichtlicher Entscheidungen – sowie Schweden aufgrund parlamentarischer Beschlüsse erhobenen verfassungsrechtlichen Bedenken über die Eingriffe in die Grundfreiheiten ihrer Bürger. In diesen Ländern ist die EU-Richtlinie nicht umgesetzt. In Irland hat der irische High Court eine Klage gegen das entsprechende nationale Umsetzungsgesetz am 27. Januar 2012 dem Europäischen Gerichtshof zur Entscheidung vorgelegt, weil das Umsetzungsgesetz seiner Auffassung nach gegen die Europäische Grundrechtecharta und die Europäische Menschenrechtskonvention verstößt.[2]

4. Nicht gegen die Zulässigkeit als solcher, aber gegen eine uferlose Praxis sprechen nach Auffassung der EU-Kommission in einer im Internet veröffentlichten Bewertung vom 15. Dezember 2011[3] Gründe der Marktgerechtigkeit, der unterschiedlichen Datenschutzhöhen der Länder und der gänzlich unterschiedlichen Anwendungspraxis im Bereich der Strafverfolgung und der Gefahrenabwehr.[4] Dies wird von Veröffentlichungen des Arbeitskreises Vorratsdatenspeicherung[5] aufgegriffen, der schon gegen das TKÜ-Gesetz vom 21.12.2006 die Verfassungsbeschwerde mit rd. 35.000 Beschwerdeführern im Jahr 2007 initiiert hatte.6 Die ungeprüfte Umsetzung der EU-Richtlinie führt infolge der massenhaften, regelmäßig sinnlosen Abrufe und der Speicherung von Funkzellendaten ohne eine gerichtliche Kontrollmöglichkeit7 zu einer die Freiheiten der Bürger nachhaltig infrage stellenden staatlichen Beobachtungs- und Überwachungswelt.

---

[1] BVerfG, Urt. v. 02.03.2010, 1 BvR 256/08 u.a., NJW 2010, 833, Leitsatz 1 und Abschn. C.

[2] http://www.thejournal.ie/ecj-asked-to-rule-on-mandatory-retention-of-phone-and-internet-data-339434-Jan2012/?utm_source=shortlink, zuletzt abgerufen am 29.01.2012

[3] Veröffentlicht auf der Homepage der Bürgerinitiative Quintessenz, https://www.unwatched.org/EDRigram_10.1_Kommission_bestaetigt_Widerrechtlichkeit_der_Vorratsdatenspeicherung?pk_campaign=twun&pk_kwd=20120126; zuletzt abgerufen am 29.01.2012

[4] Quintessenz: Veröffentlichung vom 04.01.2012, abrufbar unter http://quintessenz.org/doqs/000100011699/2011_12_15,Eu_Commission_data_retention_reform.pdf, zuletzt abgerufen am 29.01.2012

[5] AK Vorratsdatenspeicherung, Pressmitteilung vom 09.01.2012, http://www.vorratsdatenspeicherung.de, zuletzt abgerufen am 29.01.2012

[6] Veröffentlicht auf http://de.wikipedia.org/wiki/Vorratsdatenspeicherung, zuletzt abgerufen am 29.01.2012

[7] i.e. Standortdaten für Mobilfunkgeräte, bspw, in Berlin am 19.01.2012 und in Dresden am 19.02.2011, http://www.berliner-zeitung.de/berlin/funkzellenabfragen-berliner-polizei-checkt-tausende-handy-daten,10809148,11477408.html; zuletzt abgerufen am 29.01.2012

5. Eine anlasslose langfristige Vorratsdatenspeicherung stellt nach den Erkenntnissen der Rechtstatsachenforschung in Deutschland keine zwingende Notwendigkeit zur Wahrung eines funktionierenden Rechtsstaates dar. Das Gutachten des Max-Planck-Institutes Freiburg zu „Schutzlücken durch Wegfall der Vorratsdatenspeicherung?“, 2. Auflage, Juli 2011, (im Folgenden: MPI-Gutachten) belegt, dass der Wunsch nach einer langfristigen Vorratsdatenspeicherung unreflektiert anhand von Einzelfällen vorgetragen wird, dagegen der damit verbundene tiefgehende Eingriff in die private Lebensgestaltung eher bagatellisiert wird. Das trifft auch auf die Diskussionen um die Speicherfristen zu. Weder für eine lange sechs- oder zwölfmonatige Speicherfrist konnten tragfähige sachliche Gründe gefunden werden, noch wird das „Quick-Freeze-Verfahren“ als einzige Lösungsmöglichkeit bewertet.

6. Durch den Rückgriff auf die rechts- und verfahrenssichernden Garantien und Begrenzungen des Strafverfahrensrechts bedient sich der DiskE eines grundsätzlich anderen, aber mindestens ebenso wirksamen, rechtsstaatlichen Sicherungskonzeptes zum Schutz der bürgerlichen Grundfreiheiten, wie dies in dem Urteil des BVerfG vom 2. März 2010 für die anlasslose Vorratsdatenspeicherung allein für eine Neuregelung im TKG vorgegeben wird. Wird der vom DiskE genutzte Boden des strafprozessualen Sicherungskonzepts verlassen, werden nach der Entscheidung des BVerfG für die anlasslose Vorratsdatenspeicherung gesetzliche Regelungen vorgesehen und deren Umsetzung verwaltungsrechtlich überwacht werden müssen, die dem geltenden Strafverfahrensrecht entsprechen. Das sind namentlich:

   - „anspruchsvolle und normenklare Regelungen hinsichtlich der Datensicherheit, der Datenverwendung, der Transparenz und des Rechtschutzes“ insbes. in den §§ 113a ff. TKG-E;[8]
   - Zuständigkeiten für eine Abrufregelung sowie die Ausgestaltung von Transparenz- und Rechtschutzanforderungen in den jeweiligen Verfahrensordnungen;
   - eine Datenreglement, das „einen besonders hohen Sicherheitsstandard normenklar und verbindlich vorgibt“;[9]
   - bestimmte Voraussetzungen und eine Verhältnismäßigkeitsprüfung, die für den Abruf und die unmittelbare Nutzung der Daten, die den „überragend wichtigen Aufgaben des Rechtsgüterschutzes dienen“. Im Bereich der Strafverfolgung setzt dies einen durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraus. Für die Gefahrenabwehr und die Erfüllung der Aufgaben der Nachrichtendienste dürfen sie nur bei Vorliegen tatsächlicher Anhaltspunkte für eine konkrete Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für eine gemeine Gefahr zugelassen werden“;[10]
   - auch bei der nur mittelbaren Nutzung von Standortdaten oder Bestandsdaten zu IP-Adressen für Auskünfte an Behörden der Strafverfolgung, Gefahrenabwehr und nachrichtendienstlicher Aufgaben eine gesetzliche Schwelle von schwerer gewichtigen Rechtsverletzungen vorgesehen ist;
   - für das Verfahren der Verarbeitung, Speicherung und Löschung der Vorratsdaten geeignete Rechtschutzmechanismen und Kontrollen vorgesehen sind sowie der

[8] BVerfG, Urt. v. 02.03.2010, Leitsatz 2
[9] BVerfG, Urt. v. 02.03.2010, Leitsatz 4
[10] BVerfG, Urt. v. 02.03.2010, Leitsatz 5

Missbrauch und der unerlaubte Datenzugriff durch effektive Sanktionen abgesichert sind.[11]

7. Andere Regelungen der §§ 100a ff StPO, die durch das TKÜ-Gesetz vom 21.12.2007 eingeführt worden sind, sind nach dem Beschluss des BVerfG vom 12. Oktober 2011 (2 BvR 236/08) mit dem Grundgesetz vereinbar.

II. Art und Umfang von anlasslosen Vorratsdatenspeicherungen

1. Das BVerfG hat im Urteil vom 2. März 2010 verlangt, die Regelungen in den künftigen §§ 113a-f TKG so auszugestalten, dass die im TKG an sich bereits geregelte Erfassung und Speicherung von sog. Bestandsdaten einschließlich der IP-Daten[12] (§ 95 TKG) und der Verkehrsdaten (§ 96 TKG) für Telekommunikationsnutzungen den Anforderungen an Grundrechtseingriffe entspricht, wie sie in ständiger Rechtsprechung des BVerfG für die Regelungen der Strafprozessordnung judiziert werden.

   Die Verfolgung gesetzlicher Zwecke der Strafverfolgung, Gefahrenabwehr und der Nachrichtendienste erfordert nach dem Urteil, dass der vorzuhaltende Datenbestand nach Art und Umfang sachlich und zeitlich begrenzt, datentechnisch höchsten Schutzvorkehrungen unterstellt und ein möglicher Abruf von hohen Eingriffsschwellen abhängig gemacht wird. Damit soll der Tatsache Rechnung getragen werden, dass der Vorratsdatenbestand eine Vielzahl von Daten über jeden Nutzer einer Kommunikationsverbindung enthalten kann und schon die Anlage eines solchen Datenbestandes ein Grundrechtseingriff darstellt.

2. Diesen Vorgaben kommt der DiskE nach, soweit dort eine „Vorratsdatenspeicherung“ geregelt ist, nämlich als verpflichtende anlasslose Speicherung von mobilen IP-Adressen auf die Dauer von sieben Tagen. Die detaillierten Regelungen in den §§ 113a-f TKG-E sehen eine anlasslose Speicherung der mobilen IP-Adresse vor, definiert Art und Umfang der zu speichernden Kommunikationsdaten sowie die Adressaten. Die Ausnahme für Kleinstunternehmen ist gerechtfertigt, da eine Speicherpflicht, die über Abrechnungszwecke (§ 96 TKG) hinausgeht, erhebliche Investitionen abverlangt.

3. Indem der DiskE nur teilweise die Vorgaben der EU-Richtlinie über die Vorratsdatenspeicherung umsetzt, folgt der Entwurf der Rechtsprechung des BVerfG zur zwingend notwendigen Abwägung von staatlichen Zwecken mit bürgerlichen Freiheitsrechten. Dabei sind sowohl die Verortung der Regelungsmaterie in der Strafprozessordnung als auch die nur auf mobile IP-Adressen bezogenen Regelungen in den §§ 113a ff TKG-E zu nennen. Zum einen ergibt sich nach den Erkenntnissen der Rechtstatsachenforschung kein überwiegendes staatliches Bedürfnis für eine längerfristige anlasslose Vorratsdatenspeicherung. Zu berücksichtigen ist weiter, dass durch die technische Weiterentwicklung der Mobilfunk- und Internettechnik alle dort eingesetzten Anwendungen sukzessive auf das Internet-Protokoll in der Version „IPv6" umgestellt werden, durch das jedem stationären oder mobilen Endgerät eine eigene, lebenslange IP-Adresse zugewiesen werden soll. Auch dessen technische Spezifikation wird in Zukunft es nicht erlauben, eine eindeutige Zuordnung zu nur einem bestimmten Anschlussinhaber oder einem bestimmten Nutzer vorzunehmen, da eine – wie bei dem bisherigen Protokoll

---

[11] BVerfG, Urt. v. 02.03.2010, Rn. 252, 266, 267

[12] IP = Internet-Protocol, in dem die jeweilige Anschlusskennung eines stationären oder mobilen Endgerätes bei Beginn der Telekommunikationsvorgangs aufgezeichnet wird

praktizierte – gleichzeitige mehrfache Vergabe der gleichen IP-Adresse möglich ist. Auch in Zukunft wird daher eine unklare Datenlage bestehen, die entgegen den Intentionen der Befürworter der Vorratsdatenspeicherung eine Identifikation eines Verdächtigen anhand von Verbindungs- und Gerätedaten nicht rechtssicher ermöglicht und daher eine etwaig beabsichtigte strafprozessuale Beweisführung schwächt. Zugleich bestehen angesichts der Grundfreiheiten erhebliche Bedenken dagegen, allein die technische Datenlage als Anknüpfungspunkt für eine allgemeine „Gefahrenlage“ oder einen „Generalverdacht“ ausreichen zu lassen.

4. Durch das Regelungskonzept des DiskE wird sichergestellt, dass die sog. IP-Bestandsdaten, durch die ein mobiles Datenkommunikationsgerät (bspw. iPhone, iPad, sms- oder mms-Dienste usw.) mit wechselnden Anschlusskennungen erfasst werden kann, gespeichert werden. Da diese anlasslose Speicherung engsten zeitlichen Grenzen unterliegt, erscheinen die Regelungen auch in Anbetracht des damit verbundenen Grundrechtseingriffs verhältnismäßig. Zudem werden durch konkrete Datenschutzvorkehrungen in den §§ 113c, 113e, 113f TKG-E höchste Sicherheitsstandards und eine Aufnahme in das allgemeine Sicherheitskonzept des Diensteanbieters vorgeschrieben. Die Bundesnetzagentur hat nach § 121 Abs. 1 S. 2 TKG-E außerdem die Befugnis, die Sicherheitskonzepte zu prüfen und eine jeweilige Aktualisierung einzufordern. Im Übrigen soll den Betreibern und Nutzern von technischen Einrichtungen gemeinsam aufgegeben werden, die Anforderungen an die Betriebssicherheit sicherzustellen.[13] Das Interesse an der Einhaltung der Vorgaben wird schließlich durch eine Aufnahme eines etwaigen Verstoßes in den Bußgeldtatbestand des § 149 TKG unterstrichen.

5. Die Schwere eines heimlichen Eingriffs in die Grundrechte erfordert nach der Rechtsprechung des BVerfG dann einen Richtervorbehalt, wenn ein dem Grundrechtsträger zuzuordnender Gegenstand (hier Verkehrsdaten) zu Zwecken der Strafverfolgung abgerufen und genutzt werden sollen (vgl. die verfassungskonformen Regelungen in den §§ 100g Abs. 2, 100b Abs. 1 StPO, dazu III.). Eines Richtervorbehaltes bedarf es nur dann nicht, wenn eine offene, dem Betroffen transparente Anordnung einer anlassabhängigen Speicherung sowie eines Abrufs von Vorratsdaten bei dem Telekommunikationsunternehmen ergeht. Dem Betroffenen müssten dann Art, Umfang und Gründe schriftlich bekannt gegeben werden, so dass ihm rechtzeitig vorher rechtliches Gehör gewährt ist und er ggfls. auf eine Klärung eigenständig hinwirken kann. Da auch die in § 101 StPO vorgegebene Mitteilungspflicht der Strafverfolgungsbehörden in der Praxis selten angewendet wird, kann nur der Richtervorbehalt selbst eine Gewähr für eine objektive Beurteilung der Rechtmäßigkeit und Verhältnismäßigkeit des heimlichen Eingriffs darstellen.

6. Um den Grundrechten angemessene Geltung zu verschaffen, sollte die Strafbarkeit anlassloser Speicher- und Abrufanordnungen im Kontext des § 206 StGB gesondert vorgesehen werden. Ohne eine solche Regelung könnte der Tatbestand des § 206 Abs. 1 StGB ins Leere laufen, wenn die Speicherung oder der Abruf von Daten nicht aus den vom BVerfG zugelassenen Gründen oder unter Verletzung der dafür vorgesehenen Eingriffsschwellen erfolgt.

---

[13] § 108 Abs. 2, 3 TKG n.F. in der am 27.10.2011 vom Bundestag beschlossenen Fassung, BTag-Drs. 17/7521; der Bundesrat hat allerdings in der Sitzung vom 25.11.2011 den Entwurf abgelehnt und den Vermittlungsausschuss angerufen (BRat-Drs.685/1/11); http://www.zdnet.de/news/41558279/bundesrat-erhebt-einspruch-gegen-tkg-novelle.htm, zuletzt abgerufen am 29.01.2012.

7. Eine Entschädigung der Telekommunikationsdienstleister für die fortwirkenden Speicherpflichten ist im DiskE nicht neu geregelt (vgl. § 113 Abs. 2 TKG). Lediglich eine neue Entschädigung für Abrufe in Höhe von 40,00 EUR wird nunmehr nach Anlage 3 Nr. 202 zu § 23 Abs. 1 JVEG-E vorgesehen.

III. Anlassabhängige Speicherung

1. Gem. § 113a Abs. 1 TKG-E sollen lediglich IP-Bestandsdaten auf eine Wochenfrist ohne Anlass gespeichert werden. Eine darüber hinausgehende anlassabhängige Speicherung von Vorratsdaten auf einen Zeitraum von einem, höchstens aber zwei Monaten ist nur gem. § 100j Abs. 1, 2 StPO-E vorgesehen, weil der damit verbundene Eingriff nur abhängig von einem konkreten, fallbezogenen Bedürfnis und einer Rechtsgüterabwägung erfolgen darf. Nach dem Urteil des BVerfG vom 2. März 2010 ist es konsequent, schon für die Speicherung erhöhte Voraussetzungen vorzusehen. Der damit verfolgte anlassabhängige Eingriff in die Grundrechte hat besonders Gewicht und muss daher von der Rechtsordnung anders behandelt werden, als eine „normale“, Informationsbeschaffung dieser in ihrem Aufgabenkreis handelnden Strafverfolgungsbehörden. Die nach § 100j StPO-E vorgesehene Regelung entspricht damit grundsätzlich den verfassungsrechtlichen Vorgaben.

2. Festzuhalten ist zunächst, dass durch die im DiskE vorgesehene StPO-Neuregelung die anlassabhängig von einem Justizorgan angeordnete Speicherung von Verbindungsdaten als Vorstufe für einen späteren Abruf eindeutig dem Strafverfolgungszweck zugeordnet ist und keine andere „Verwendungsoption“ für derartige Datenbestände eröffnet wird. Dies ist gegenüber einer allgemein im TKG verorteten gesetzlichen Speicherpflicht vorzugswürdig. Die auf einen Monat befristete schriftliche Speicherungsanordnung gewährleistet zudem - ebenso wie die lediglich einmonatige Verlängerungsoption – eine zeitlich überschaubare, verhältnismäßige Prüfung der Notwendigkeit eines Datenabrufs. Dieser ist weiterhin nur gem. den verbleibenden Regelungen des § 100g StPO zulässig. Für eine Verwendung von Daten in einem strafrechtlichen Ermittlungsverfahren ist daher grundsätzlich eine richterliche Anordnung erforderlich, die den durch „bestimmte Tatsachen“ begründeten Verdacht einer Straftat von erheblicher Bedeutung aus dem Katalog des § 100a Abs. 2 StPO oder eine vergleichbare schwere Straftat voraussetzt. Eine andere Abruf- oder Verwendungsmöglichkeit wird schon nicht eröffnet, so dass die Anforderungen des BVerfG-Urteils vom 2. März 2010 erfüllt sind.

3. Indessen hatte das BVerfG darauf verwiesen, dass für die anlassunabhängige Speicherung besonders hohe datenschutzrechtliche Sicherheitsstandards zu erfüllen sind, die vor einem unberechtigten Zugriff oder Missbrauch des Datenbestandes bei privaten Diensteanbietern schützen müssen.14 Dies gilt aber auch für die anlassbezogene Speicherung. Die derzeitigen Schutzvorkehrungen des TKG für die anlasslose Speicherung müssen mithin auch dann erfüllt sein, wenn eine Speicherung aus besonderem Anlass angeordnet wird. In dem derzeitigen Vorschlag des DiskE besteht eine Inkongruenz zwischen den Speicheranforderungen nach § 113a TGK-E und den Anforderungen nach § 100j StPO-E, da eine entsprechende Anwendung der geplanten §§ 113c, 113e, 113f TKG-E für die anlassbezogene Speicherung nicht unmittelbar vorgesehen ist. Lediglich in § 113b Abs. 1 S. 2 TKG-E wird eine der Systematik entsprechende Anwendung für den Fall vorgesehen, dass eine Auskunft für eine Strafverfolgungsbehörde erteilt werden soll und dabei nach

[14] BVerfG, Urt. v. 02.03.2010, Entscheidungsgründe C.V.1. Tz. 221, 222

einer mobilen IP-Adressen gesucht wird. Gleiche Schutzvorkehrungen sind im TKG vorzusehen, wenn eine anlassabhängige Speicherung zu Zwecken der Gefahrenabwehr oder der Nachrichtendienste angeordnet werden sollte.

4. Die zentrale Eingriffsnorm für die anlassabhängige Speicherung soll nach dem DiskE § 100j Abs. 1 S. 1 StPO-E werden. Der Anordnungszweck soll bereits durch die allgemeine Ermittlungsklausel des § 152 Abs. 2 StPO und die Befugnis zur Aufenthaltsermittlung („zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes“) erreicht werden können. Damit wäre schon die Einleitung eines Ermittlungsverfahrens auf geringster Verdachtsschwelle eine Rechtfertigung für einen bedeutsamen Eingriff in das Grundrecht. Dem DiskE ist allerdings zuzugeben, dass durch die Einschränkung des § 100j Abs. 1 S. 2 StPO-E eine anlassabhängige Speicheranordnung in einem solchen Fall unzulässig wäre oder würde.

   Gleichwohl muss den vom BVerfG hervorgehobenen Ängsten und Unsicherheiten in der Bevölkerung über die Eingriffsbefugnisse staatlicher Behörden in die betroffenen Grundrechte schon durch eine klare Begrenzung der Speicheranordnungsbefugnis begegnet werden. Die Bewertung, wann es zu einer geeigneten Aufgriffsschwelle kommt oder wann eine Unzulässigkeit der weiteren Datenspeicherung vorliegen kann, wird durch die jetzige Fassung zu sehr in das Belieben der anordnenden Stelle gestellt. Daher ist einer ausdrücklichen Prüfungspflicht der Voraussetzungen des § 100g Abs. 1 StPO der Vorzug vor der vorgeschlagenen Regelung zu geben.

5. Dagegen ist die Wertung des DiskE richtig, dass eine Speicherung von Daten schon bei dem gewerblichen Diensteanbieter unzulässig ist oder wird, wenn ein späterer Abruf nicht in Betracht kommt (§ 100j Abs. 1 S. 2 StPO-E). Durch die Regelung wird erreicht, dass bei Unzulässigkeit eines Abrufs auch die vorausgehende Speicherungsanordnung unzulässig ist oder wird. Dadurch werden Vorgaben des § 100g StPO in die Eingriffsnorm des § 100j StPO-E integriert. Hier fehlt es aber an Bestimmungen darüber, dass dem von der Anordnung betroffenen Diensteanbieter die (nachträglich erkannte) Unzulässigkeit unverzüglich mitzuteilen ist und die Löschung des Datenbestandes zu veranlassen ist.

6. Für anlasslose oder auch anlassabhängige Speicherungsanordnungen der Gefahrenabwehrbehörden oder der Nachrichtendienste enthält der DiskE infolge der Verortung der Abrufbefugnisse allein in der StPO keine weiterführenden Regelungen. Das entspricht auch den Vorgaben des BVerfG.

IV. Anlassabhänger Abruf

1. Das BVerfG hat dem anlassabhängigen Abruf wie auch der Verarbeitung und Weiterübertragung von Vorratsdaten enge Grenzen auferlegt und besonders den Rechtsgüterschutz in den Mittelpunkt gestellt.[15] Daher steht bei der Ausgestaltung eines zukünftigen Gesetzes im Vordergrund, dass Beschränkungen der Grundrechte durch einen anlassabhängigen Abruf von Vorratsdaten nur dann hinzunehmen sind, wenn sie zur effektiven Verfolgung von schwerwiegenden Straftaten oder zum Schutz bedeutender Rechtsgüter wie Leib, Leben, persönliche Freiheit etc. erforderlich erscheint. Nicht nur der Abruf, auch das weitere Schicksal des Datenbestandes in dem – dann unmittelbaren - Zugriff der Strafverfolgungsbehörden muss begrenzt sein, weil nur dadurch der Grundrechtsschutz effektiv ausgestaltet ist. Das BVerfG betont: „Nach der Rechtsprechung

[15] BVerfG, Urt. v. 02.03.2010, Entscheidungsgründe C.V.2. Tz. 226 ff.

des Bundesverfassungsgerichts müssen die Voraussetzungen für die Datenverwendung und deren Umfang in den betreffenden Rechtsgrundlagen umso enger begrenzt werden, je schwerer der in der Speicherung liegende Eingriff wiegt. Anlass, Zweck und Umfang des jeweiligen Eingriffs sowie die entsprechenden Eingriffsschwellen sind dabei durch den Gesetzgeber bereichsspezifisch, präzise und normenklar zu regeln[16]“. Daher hat das BVerfG die Datenverwendung dem Eingriff in die Inhalte der Telekommunikation gleichgestellt.[17] Diese hohen Anforderungen reflektiert der DiskE, indem kein anlassloser Vorratsdatenbestand angelegt wird und der Abruf von anlassabhängig gespeicherten Daten gem. § 100j StPO-E nur nach § 100g StPO erfolgen darf.

2. Ein Datenabruf für Zwecke der Strafverfolgung muss daher einen durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraussetzen. Auch wenn das BVerfG dem Gesetzgeber dazu einen eigenen Gestaltungs- und Beurteilungsspielraum eingeräumt hat, reichen doch die Generalklausel des § 100g Abs. 1 StPO in der geltenden Fassung oder „lediglich die Verweisung auf Straftaten von erheblicher Bedeutung“ nicht aus.[18] Diese Vorschrift ist zukünftig enger zu fassen, weil das BVerfG mit Reflex auf § 161 Abs. 2 StPO auch eine weitere Verwendung der Daten von der konkreten Feststellung abhängig macht, dass Straftaten auch im Einzelfall schwer wiegen müssen19 und eine Verwendung der Daten dann noch verhältnismäßig sein muss. Hier ist eine Harmonisierung des § 100g Abs. 1 StPO mit dem Urteil des BVerfG erforderlich.

3. Über Regelungen zum Datenabruf für Zwecke der Gefahrenabwehr oder der Nachrichtendienste, die noch höheren Anforderungen an die zu beachtende Eingriffsschwelle unterliegen, enthält der DiskE keine Regelungen. Dies ist mit den Vorgaben des BVerfG vereinbar, solange und soweit kein abruffähiger Datenbestand vorgesehen wird.

4. Ebenfalls ungeregelt sind die besonderen Anforderungen an die Datenverwendung nach dem Abruf. Das BVerfG hat betont, dass für die Verwendung der Daten „gesetzlich zu gewährleisten (ist), dass die Daten nach Übermittlung unverzüglich ausgewertet werden und, sofern sie für die Erhebungszwecke unerheblich sind, gelöscht werden. Im Übrigen ist vorzusehen, dass die Daten vernichtet werden, sobald sie für die festgelegten Zwecke nicht mehr erforderlich sind, und dass hierüber ein Protokoll gefertigt wird.“[20]

   Schließlich ist die Weitergabe der Daten und Informationen an weitere Stellen ist möglichst von der abgebenden Stelle zu protokollieren, dabei ist nach den gesetzlichen Schranken zu fragen, und eine Übertragung nur ermöglicht werden, wenn „sie zur Wahrnehmung von Aufgaben erfolgt, deretwegen ein Zugriff auf diese Daten auch unmittelbar zulässig wäre.“[21]

---

[16] BVerfGE 100, 313 <359 f.>; 110, 33 <53>; 113, 29 <51>; 113, 348 <375>; 115, 166 <191>; 115, 320 <365>; 118, 168 <186 f.>

[17] BVerfG, Urt. v. 02.03.2010, Entscheidungsgründe C.V.2 Tz.227, danach muss die Verwendung „besonders hohen Gemeinwohlbelangen dienen“.

[18] BVerfG, Urteil vom 02.03.2010, Entscheidungsgründe C.V.2.b Tz. 230

[19] BVerfGE 121, 1 <26>; 107, 299 <322>; 109, 279 <346>

[20] BVerfG, Urteil vom 02.03.2010, Entscheidungsgründe C.V.2.d Tz. 235

[21] BVerfG, Urteil vom 02.03.2010, Entscheidungsgründe C.V.2.d Tz. 236

V. Auskunft über Bestandsdaten

1. Die Ermittlungsbehörden sollen nach dem DiskE in Zukunft Auskunft über Bestandsdaten für Strafverfolgungszwecke nur noch gem. § 100k StPO-E in Verbindung mit § 113 Abs. 1 TKG erlangen. Damit würde die allgemeine Ermittlungsgeneralklausel für solche bei dem Diensteanbieter verpflichtend vorgehaltenen Daten modifiziert und eine engere Zugriffsregelung eingeführt. Zwar verbleibt es bei der einfachen Verdachtsschwelle einer Straftat, indessen müssen sich die Anordnungen auf einen konkreten Sachverhalt beziehen, es darf nur wegen der Aufenthaltsermittlung eines Beschuldigten abgefragt werden und es soll eine Benachrichtigungspflicht des Betroffenen eingeführt werden. Diese Regelung ist zu begrüßen.

2. Die anstelle des § 101 StPO normierte neue Benachrichtigungspflicht nach Abs. 2 S. 2-4 des § 100k StPO-E soll für diese Fälle des Datenabrufs eine für den Telekommunikationsteilnehmer beschränkte Transparenz ermöglichen. Angesichts der vorgesehenen weiten Möglichkeiten der rein zweckbezogenen Zurückstellung (S. 3) oder des Absehens von Mitteilungen (S. 4) wird allerdings keine sehr praktische Relevanz der Norm erwartet. Hohe Begründungserfordernisse für einen Verzicht auf die Maßnahmen sind nicht vorgesehen. Dennoch kann der Norm ein Disziplinierungseffekt zukommen, da im Zweifel eine geeignete Rechenschaft und Nachprüfung verfahrensimmanent durch den erkennenden Richter zu erfolgen hat.

- - -