Mitteilung

der Regierung der Bundesrepublik Deutschland

an die Europäische Kommission

vom 15. August 2011

Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland nach Artikel 258 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV)

hier: Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG

- Verfahren Nr. 2011/2091 -

Bezug: Schreiben der Europäischen Kommission vom 17. Juni 2011 (SG-Greffe(2011)D9667

Anlagen: - 2 -

Die Bundesregierung beehrt sich, der Europäischen Kommission Folgendes mitzuteilen:

I. Vorab möchte die Bundesregierung gegenüber der Europäischen Kommission deutlich machen, dass seit dem 21. Januar 2011 weitere Gespräche auf Fachebene über die Entwicklungen in Deutschland geführt wurden. Sie erlaubt sich in diesem Zusammenhang den Hinweis auf Kontakte von Regierungsvertretern mit der Europäischen Kommission auf Arbeitsebene in der ersten Hälfte diesen Jahres, die schließlich zu einem Gespräch am 23. Juni 2011 geführt haben, für das sich die Bundesregierung nochmals bedanken möchte.

II. Nach Ansicht der Bundesregierung sind Bestimmungen der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung

von Daten (im Folgenden: Richtlinie 2006/24/EG) im deutschen Recht teilweise umgesetzt. Die Schlussfolgerung der Kommission im Bezugsschreiben, S. 2, dritter Absatz, dass es seit der Nichtigerklärung des Bundesverfassungsgerichts keine gültige deutsche Rechtsvorschrift zur Umsetzung der Richtlinie mehr gebe, trifft daher nicht zu.

1. **Zur innerstaatlichen Umsetzung der Richtlinie 2006/24/EG**

In seinem am 2. März 2010 verkündeten Urteil hat der Erste Senat des Bundesverfassungsgerichts die §§ 113a und 113b des Telekommunikationsgesetzes wegen Verstoßes gegen Artikel 10 Grundgesetz für nichtig erklärt. § 100g Absatz 1 Satz 1 der Strafprozessordnung wurde ebenfalls wegen Verstoßes gegen Artikel 10 Grundgesetz für nichtig erklärt, soweit danach Verkehrsdaten nach § 113a des Telekommunikationsgesetzes erhoben werden dürfen.

Das Bundesverfassungsgericht hat jedoch nicht alle Vorschriften des am 9. Januar 2008 an die Kommission übermittelten

> „Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007"

für nichtig erklärt. Überdies waren bestimmte Vorgaben der Richtlinie 2006/24/EG in wesentlichen Teilen bereits vor dem Inkrafttreten der Richtlinie Bestandteil des deutschen Rechts.

Nachfolgende Teile der Vorgaben der Richtlinie 2006/24/EG sind daher in Deutschland weiterhin umgesetzt:

a) In Deutschland weiterhin umgesetzt sind die Vorgaben von Artikel 5 Absatz 1 Buchstabe a Nummer 1 Ziffer ii und Artikel 5 Absatz 1 Buchstabe b Nummer 1 Ziffer ii der Richtlinie 2006/24/EG, nach der die Mitgliedstaaten sicher stellen, dass betreffend Telefonfestnetz und Mobilfunk die Namen und Anschriften der Teilnehmer oder registrierten Benutzer gespeichert werden. Ebenfalls weiterhin umgesetzt ist die Vorgabe von Artikel 5 Absatz 1 Buchstabe a Nummer 2 Ziffer iii der Richtlinie 2006/24/EG, soweit diese bestimmt, dass betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie der Name und die Anschrift des Teilnehmers beziehungsweise registrierten Benutzers gespeichert werden, dem eine Benutzerkennung oder Rufnummer zum Zeitpunkt der Nachricht zugewiesen war. Ebenso umgesetzt ist auch die Vorgabe von Artikel 5 Absatz 1 Buchstabe b Nummer 2 Ziffer ii der Richtlinie 2006/24/EG, soweit

diese bestimmt, dass betreffend Internet-E-Mail und Internet-Telefonie die Namen und Anschriften der Teilnehmer oder registrierten Benutzer gespeichert werden.

Diese Vorgaben der Richtlinie sind im innerstaatlichen Recht im geltenden § 111 des Telekommunikationsgesetzes (TKG) abgebildet, dessen Absatz 1 Satz 1 bis 3 lautet:

> „(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt und dabei Rufnummern oder andere Anschlusskennungen vergibt oder Telekommunikationsanschlüsse für von anderen vergebene Rufnummern oder andere Anschlusskennungen bereitstellt, hat für die Auskunftsverfahren nach den §§ 112 und 113
> 1. die Rufnummern und anderen Anschlusskennungen,
> 2. den Namen und die Anschrift des Anschlussinhabers,
> 3. bei natürlichen Personen deren Geburtsdatum,
> 4. bei Festnetzanschlüssen auch die Anschrift des Anschlusses,
> 5. in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkendgerät überlassen wird, die Gerätenummer dieses Gerätes sowie
> 6. das Datum des Vertragsbeginns
>
> vor der Freischaltung zu erheben und unverzüglich zu speichern, auch soweit diese Daten für betriebliche Zwecke nicht erforderlich sind; das Datum des Vertragsendes ist bei Bekanntwerden ebenfalls zu speichern. Satz 1 gilt auch, soweit die Daten nicht in Teilnehmerverzeichnisse (§ 104) eingetragen werden. Die Verpflichtung zur unverzüglichen Speicherung nach Satz 1 gilt hinsichtlich der Daten nach Satz 1 Nr. 1 und 2 entsprechend für denjenigen, der geschäftsmäßig einen öffentlich zugänglichen Dienst der elektronischen Post erbringt und dabei Daten nach Satz 1 Nr. 1 und 2 erhebt, wobei an die Stelle der Daten nach Satz 1 Nr. 1 die Kennungen der elektronischen Postfächer und an die Stelle des Anschlussinhabers nach Satz 1 Nr. 2 der Inhaber des elektronischen Postfachs tritt."

§ 111 Absatz 1 Satz 1 Halbsatz 1 TKG gibt die Speicherung von Namen und Anschrift der Teilnehmer vor, denn dort ist bestimmt, dass die Daten zu speichern sind, auch wenn diese Daten für betriebliche Zwecke nicht erforderlich sind.

§ 111 TKG wurde durch das Bundesverfassungsgericht nicht für nichtig erklärt. Allerdings umfasst diese Regelung die Speicherung von Bestandsdaten, das sind gemäß § 3 Nr. 3 TKG Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden. Die Speicherung der gem. Art. 5 zu speichernden Verkehrsdaten wurde vom Bundesverfassungsgericht für nichtig erklärt.

b) Ebenfalls weiterhin umgesetzt ist die Vorgabe von Artikel 4 der Richtlinie 2006/24/EG, die u. a. bestimmt, dass die Mitgliedstaaten Maßnahmen erlassen, um sicherzustellen, dass die gespeicherten Bestandsdaten nur in bestimmten Fällen und in Übereinstimmung mit dem innerstaatlichen Recht an die zuständigen nationalen Behörden weitergegeben werden.

Diese Vorgabe ist in § 113 TKG i. V. m. §§ 161, 163 Strafprozessordnung (StPO) umgesetzt; § 113 Absatz 1 Satz 1 TKG gibt vor:

> „(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, hat im Einzelfall den zuständigen Stellen auf deren Verlangen unverzüglich Auskünfte über die nach den §§ 95 und 111 erhobenen Daten zu erteilen, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes erforderlich ist."

Strafverfolgungsbehörden können die nach § 111 TKG gespeicherten Bestandsdaten gemäß § 113 TKG i. V. m. §§ 161, 163 StPO erheben. Die Vorgabe des § 113 TKG, dass ein Diensteanbieter Auskünfte über die nach § 111 TKG gespeicherten Bestandsdaten zu erteilen hat, soweit dies für die Verfolgung von Straftaten erforderlich ist, erfüllt auch teilweise die Zielsetzung von Artikel 1 Absatz 1 der Richtlinie 2006/24/EG. Danach ist sicherzustellen, dass neben Verkehrs- und Standortdaten, die derzeit nicht verpflichtend gespeichert werden, auch „alle damit im Zusammenhang stehenden Daten, die zur Feststellung des Teilnehmers oder registrierten Benutzers erforderlich sind" (Bestandsdaten) zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten zur Verfügung stehen, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden.

Die § 113 TKG und §§ 161, 163 StPO wurden durch das Bundesverfassungsgericht nicht für nichtig erklärt.

c) Ebenfalls weiterhin umgesetzt sind die Vorgaben des Artikels 9 und Teile der Vorgaben der Artikel 7 und 13 der Richtlinie 2006/24/EG.

Artikel 9 der Richtlinie 2006/24/EG bestimmt u. a., dass jeder Mitgliedstaat eine oder mehrere öffentliche Stellen benennt, die für die Kontrolle der Anwendung der zur Umsetzung von Artikel 7 der Richtlinie 2006/24/EG erlassenen Vorschriften bezüglich der Sicherheit der gespeicherten Daten in seinem Hoheitsgebiet zuständig ist/sind.

Diese Vorgabe der Richtlinie 2006/24/EG ist in § 115 i. V. m. § 109 TKG umgesetzt. § 115 Absatz 1 TKG lautet:

> „(1) Die Bundesnetzagentur kann Anordnungen und andere Maßnahmen treffen, um die Einhaltung der Vorschriften des Teils 7 und der auf Grund dieses Teils ergangenen Rechtsverordnungen sowie der jeweils anzuwendenden Technischen Richtlinien sicherzustellen. Der Verpflichtete muss auf Anforderung der Bundesnetzagentur die hierzu erforderlichen Auskünfte erteilen. Die Bundesnetzagentur ist zur Überprüfung

der Einhaltung der Verpflichtungen befugt, die Geschäfts- und Betriebsräume während der üblichen Betriebs- oder Geschäftszeiten zu betreten und zu besichtigen."

Zu den Vorschriften des Teils 7 des Telekommunikationsgesetz gehört die Vorschrift des § 109 TKG, dessen Absatz 1 die Diensteanbieter u. a. verpflichtet, angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze des Fernmeldegeheimnisses und personenbezogener Daten zu treffen. § 109 TKG Absatz 1 ist daher eine Umsetzung von Artikel 7 Buchstabe b der Richtlinie 2006/24/EG. Nach § 115 Absatz 2 Nummer 2 TKG kann die Bundesnetzagentur z. B. Zwangsgelder bis zu 100.000 Euro zur Durchsetzung der Verpflichtungen des § 109 TKG festsetzen. § 115 Absatz 2 Nummer 2 i. V. m. § 109 Absatz 1 TKG entspricht daher der Zielsetzung der Vorgabe des Artikels 13 Absatz 2 der Richtlinie 2006/24/EG, unzulässige Datenübermittlungen mit Sanktionen, einschließlich verwaltungsrechtlicher und strafrechtlicher Sanktionen zu belegen.

Die §§ 109, 115 TKG wurden durch das Bundesverfassungsgericht nicht für nichtig erklärt.

d) Ebenfalls weiterhin umgesetzt sind die Begriffsbestimmungen des Artikels 2 Absatz 1 und Absatz 2 Buchstabe a bis d der Richtlinie 2006/24/EG.

Zur Vermeidung von Wiederholungen wird hierzu auf die detaillierten Ausführungen in der Mitteilung der Regierung der Bundesrepublik Deutschland an die Kommission der Europäischen Gemeinschaften vom 25. März 2009 verwiesen (**Anlage**), die eine Umsetzungsliste beinhaltet, welche auf die innerstaatlichen Vorschriften der §§ 3, 111 TKG verweist, mit denen die Vorgaben des Artikels 2 Absatz 1 und Absatz 2 Buchstabe a bis d der Richtlinie 2006/24/EG umgesetzt sind.

Die §§ 3, 111 TKG wurden vom Bundesverfassungsgericht nicht für nichtig erklärt.

Nach alledem sind daher Teile der Vorgaben der Artikel 1, 2, 4, 5 bis 7, 9 und 13 der Richtlinie 2006/24/EG, die insbesondere die Speicherung von Namen und Anschrift der Teilnehmer oder registrierten Benutzer, die Weitergabe dieser Daten für Zwecke der Strafverfolgung, die Gewährleistung von Datenschutz und Datensicherheit und die Einrichtung einer Kontrollstelle betreffen, auch nach der Entscheidung des Bundesverfassungsgerichts durch geltende deutsche Rechtsvorschriften umgesetzt.

Auf Grund der geltenden Rechtsvorschriften der §§ 3, 109, 111, 113, 115 TKG und §§ 161, 163 StPO besteht nach Auffassung der Bundesregierung somit eine Teilumsetzung der Richtlinie 2006/24/EG in Deutschland.

Die in Bezug genommenen Regelungen finden sich im

> „Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 3 des Gesetzes vom 24. März 2011 (BGBl. I S. 506) geändert worden ist"

und in der

> „Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 2 des Gesetzes vom 22. Dezember 2010 (BGBl. I S. 2300) geändert worden ist",

die unter http://www.gesetze-im-internet.de/bundesrecht/tkg_2004/gesamt.pdf bzw. http://www.gesetze-im-internet.de/bundesrecht/stpo/gesamt.pdf im Volltext abgerufen werden können.

2. Berücksichtigung umfassender nationaler und europäischer Vorgaben

Die vorstehend aufgezeigten Regelungen, die eine teilweise Umsetzung der Richtlinie 2006/24/EG beinhalten, sind in dem Urteil des Bundesverfassungsgerichts vom 2. März 2010 nicht verworfen worden und gelten daher weiter. Nur soweit das Bundesverfassungsgericht die ursprünglich in Deutschland in vollem Umfang erfolgte Umsetzung der Richtlinie 2006/24/EG für nichtig erklärt hat, was insbesondere die §§ 113a (Speicherungspflichten für Daten), 113b (Verwendung der nach § 113a gespeicherten Daten) TKG betrifft, stellt sich die Frage, wie insoweit eine Neuumsetzung der Richtlinie in Deutschland erfolgen kann, insbesondere welche Rahmenbedingungen hierfür zu berücksichtigen sind.

Die Richtlinie 2006/24/EG selbst war Gegenstand einer Bewertung durch die Organe der Europäischen Union: Artikel 14 der Richtlinie 2006/24/EG gibt vor, dass die Kommission dem Europäischen Parlament und dem Rat spätestens am 15. September 2010 eine Bewertung der Anwendung dieser Richtlinie sowie ihrer Auswirkungen auf die Wirtschaftsbeteiligten und die Verbraucher vorlegt, um festzustellen, ob die Bestimmungen

dieser Richtlinie, insbesondere die Liste von Daten in Artikel 5 und die in Artikel 6 vorgesehenen Speicherungsfristen, gegebenenfalls geändert werden müssen.

Unter dem 18. April 2011 hat die Europäische Kommission ihren Bewertungsbericht vorgelegt und angekündigt, eine Folgenabschätzung durchzuführen und auf dieser Grundlage Änderungsvorschläge für die Richtlinie vorzulegen.

Die Erkenntnisse aus diesem Bericht sowie damit verbundene europarechtliche Fragen sind nach Auffassung der Bundesregierung ebenso wie das Urteil des Bundesverfassungsgerichts und die daraus zu ziehenden Konsequenzen für das nationale Recht in die abschließende Gesamtbewertung zum Inhalt und Umfang des gesetzgeberischen Handlungsbedarfs einzubeziehen, um abzuschätzen, welche Maßnahmen konkret zur Verwirklichung der Ziele der Richtlinie 2006/24/EG eingeleitet werden müssen.

Dabei gilt es, unter Berücksichtigung der verfassungsrechtlichen Vorgaben und der Anforderungen an den Datenschutz und die Datensicherheit eine Regelung zu treffen, die die Einschränkung grundrechtlich geschützter Interessen auf das zur Sicherung der Belange von Strafverfolgung erforderliche Maß begrenzt, gleichzeitig aber den wesentlichen Bedürfnissen der Strafverfolgungsbehörden angemessen Rechnung trägt.

a) Eine Speicherung bestimmter Telekommunikationsverkehrsdaten im Umfang der Vorgaben in der Richtlinie 2006/24/EG bedarf nach dem Urteil des Bundesverfassungsgerichts vom 2. März 2010 der gesetzlichen Gewährleistung eines besonders hohen Standards der Datensicherheit. Zur Begründung führt das Gericht aus (Absatz-Nummer 222):

> „Dieses gilt besonders, weil die Daten bei privaten Diensteanbietern gespeichert werden, die unter den Bedingungen von Wirtschaftlichkeit und Kostendruck handeln und dabei nur begrenzte Anreize zur Gewährleistung von Datensicherheit haben. Sie handeln grundsätzlich privatnützig und sind nicht durch spezifische Amtspflichten gebunden. Zugleich ist die Gefahr eines illegalen Zugriffs auf die Daten groß, denn angesichts ihrer vielseitigen Aussagekraft können diese für verschiedenste Akteure attraktiv sein. Geboten ist daher ein besonders hoher Sicherheitsstandard, der über das allgemein verfassungsrechtlich gebotene Maß für die Aufbewahrung von Daten der Telekommunikation hinausgeht. Solche Anforderungen der Datensicherheit gelten dabei sowohl für die Aufbewahrung der Daten als auch für deren Übermittlung; ebenso bedarf es effektiver Sicherungen zur Gewährleistung der Löschung der Daten."

Insgesamt soll ein Standard gewährleistet werden, der sich - etwa unter Rückgriff auf einfachgesetzliche Rechtsfiguren wie den Stand der Technik - an dem Entwicklungsstand der Fachdiskussion orientiert und neue Erkenntnisse und Einsichten fortlaufend aufnimmt. Die speicherpflichtigen Unternehmen müssen dabei ihre in regelmäßigen

Abständen zu erneuernden Sicherheitskonzepte am Entwicklungsstand der Fachdiskussion orientieren (Absatz-Nummer 224).

Zusammengefasst fordert das Gericht als mögliche Instrumente zur Gewährleistung eines besonders hohen Standards der Datensicherheit folgende Maßnahmen:

- getrennte Speicherung,
- eine anspruchsvolle Verschlüsselung,
- ein gesichertes Zugriffsregime unter Nutzung etwa des Vier-Augen-Prinzips sowie
- eine revisionssichere Protokollierung (Absatz-Nummer 224).

Die Sachverständigen haben darüber hinaus auf folgende Standards zur Datensicherheit hingewiesen:

- Speicherung auch auf physisch getrennten und vom Internet entkoppelten Rechnern,
- asymmetrische kryptografische Verschlüsselung unter getrennter Verwahrung der Schlüssel,
- Vier-Augen-Prinzip für den Zugriff auf die Daten mit fortschrittlichen Verfahren zur Authentifizierung für den Zugang zu den Schlüsseln,
- revisionssichere Protokollierung des Zugriffs und der Löschung,
- automatisierte Fehlerkorrektur- und Plausibilitätsverfahren,
- Schaffung von Informationspflichten bei Datenschutzverletzungen,
- Einführung einer verschuldensunabhängigen Haftung und
- Stärkung der Ausgleichsansprüche für immaterielle Schäden.

Für die Einhaltung solcher besonders hoher Sicherheitsstandards sind eine für die Öffentlichkeit transparente Kontrolle unter Einbeziehung des unabhängigen Datenschutzbeauftragten sowie ein ausgeglichenes Sanktionensystem verfassungsrechtlich geboten, das auch Verstößen gegen die Datensicherheit ein angemessenes Gewicht beimisst (Absatz-Nummer 225).

b) Auch für die Verwendungsregelung hat das Bundesverfassungsgericht hohe Anforderungen aufgestellt und insoweit für die Strafverfolgung vorgegeben (Absatz-Nummer 228):

„Für die Strafverfolgung folgt hieraus, dass ein Abruf der Daten zumindest den durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraussetzt. Welche Straftatbestände hiervon umfasst sein sollen, hat der Gesetzgeber abschließend mit der Verpflichtung

zur Datenspeicherung festzulegen. Ihm kommt hierbei ein Beurteilungsspielraum zu. Er kann dabei entweder auf bestehende Kataloge zurückgreifen oder einen eigenen Katalog schaffen, etwa um Straftaten, für die die Telekommunikationsverkehrsdaten besondere Bedeutung haben, zu erfassen. Die Qualifizierung einer Straftat als schwer muss aber in der Strafnorm - insbesondere etwa durch deren Strafrahmen - einen objektivierten Ausdruck finden (vgl. BVerfGE 109, 279 <343 ff., insbesondere 347 f.>). Eine Generalklausel oder lediglich die Verweisung auf Straftaten von erheblicher Bedeutung reichen hingegen nicht aus."

c) Nach Übermittlung an die abrufenden Behörden muss nach den Vorgaben des Bundesverfassungsgerichts die Begrenzung der Datenverwendung auf bestimmte Zwecke, deren Änderung nur auf gesetzlicher Grundlage zulässig ist, sichergestellt werden. Zu gewährleisten ist dabei eine unverzügliche Auswertung der übermittelten Daten und deren Löschung, sofern sie für die Erhebungszwecke unerheblich sind. Wenn die Daten für die festgelegten Zwecke nicht mehr benötigt werden, sind sie zu löschen, worüber ein Protokoll zu fertigen ist (Absatz-Nummern 235 f.). Verfassungsrechtlich geboten ist zudem, als Ausfluss des Verhältnismäßigkeitsgrundsatzes zumindest für einen engen Kreis von auf besondere Vertraulichkeit angewiesenen Telekommunikationsverbindungen (z.B. Anrufe bei Seelsorgetelefonen) ein grundsätzliches Übermittlungsverbot vorzusehen (Absatz-Nummer 238).

d) Darüber hinaus hat das Bundesverfassungsgericht auch Vorgaben zur Gewährleistung der Transparenz und des effektiven Rechtsschutzes aufgestellt (Absatz-Nummern 239 ff.). Die Verwendung der Daten hat grundsätzlich offen - also durch Benachrichtigung des Betroffenen vor Abfrage und Übermittlung - zu erfolgen, eine Verwendung ohne Wissen des Betroffenen kommt nur in Betracht, wenn ansonsten der Untersuchungszweck vereitelt würde. In diesem Fall ist der Betroffene grundsätzlich nachträglich zu benachrichtigen, wenn auch diese Benachrichtigung unterbleibt, bedarf die Nichtbenachrichtigung einer richterlichen Entscheidung.

Um einen effektiven Rechtsschutz zu gewährleisten, unterfallen die Abfrage und Übermittlung von Telekommunikationsverkehrsdaten grundsätzlich dem Vorbehalt richterlicher Anordnung, da Richter aufgrund ihrer persönlichen und sachlichen Unabhängigkeit und ihrer ausschließlichen Bindung an das Gesetz die Rechte der Betroffenen im Einzelfall am besten und sichersten wahren können (Absatz-Nummer 248). Eine Ausnahme zu diesem Richtervorbehalt gilt nur für die Kontrolle von Eingriffen in die Telekommunikationsfreiheit durch die Nachrichtendienste. An die Stelle einer vorbeugenden richterlichen Kontrolle kann die Kontrolle durch ein von der Volksvertretung bestelltes Organ oder Hilfsorgan treten (Absatz-Nummer 248).

Nach dem Bundesverfassungsgericht gehört zu einer wirksamen Kontrolle auch, dass die Behörden keinen Direktzugriff auf die gespeicherten Daten haben. Dadurch, dass die Daten von den Telekommunikationsunternehmen als speicherungsverpflichtete Dritte herausgefiltert und übermittelt werden, „wird die Verwendung der Daten auf das Zusammenwirken verschiedener Akteure verwiesen und damit in sich gegenseitig kontrollierende Entscheidungsstrukturen eingebunden" (Absatz-Nummer 250).

e) Die unter den Buchstaben a) bis d) dargestellten Vorgaben des Bundesverfassungsgerichts zur Datensicherheit, zur Verwendungsregelung, zur Zweckbegrenzung, zur Transparenz und zur Gewährleistung eines effektiven Rechtsschutzes beziehen sich auf die Fälle, in denen ein unmittelbarer Zugriff auf die gespeicherten Verkehrsdaten erfolgt, also z.B. bei der Erhebung von Telefonverbindungsdaten oder der Funkzellenabfrage. Wird nur mittelbar auf die gespeicherten Daten zurückgegriffen, greifen in Bezug auf die Datenerhebung vergleichsweise geringere Anforderungen. Dies gilt namentlich für Bestandsdatenauskünfte zu Inhabern bestimmter dynamischer Internetprotokoll-Adressen, für deren Ermittlung nur unternehmensintern auf vorsorglich gespeicherte Telekommunikationsverkehrsdaten zurückgegriffen werden muss. Zur Begründung für diese Abstufung führt das Gericht aus (Absatz-Nummern 256 f.):

„Von Bedeutung ist hierfür zum einen, dass die Behörden selbst keine Kenntnis der vorsorglich zu speichernden Daten erhalten. Die Behörden rufen im Rahmen solcher Auskunftsansprüche nicht die vorsorglich anlasslos gespeicherten Daten selbst ab, sondern erhalten lediglich personenbezogene Auskünfte über den Inhaber eines bestimmten Anschlusses, der von den Diensteanbietern unter Rückgriff auf diese Daten ermittelt wurde. Dabei bleibt die Aussagekraft dieser Daten eng begrenzt: Die Verwendung der vorsorglich gespeicherten Daten führt allein zu der Auskunft, welcher Anschlussinhaber unter einer bereits bekannten, etwa anderweitig ermittelten IP-Adresse im Internet angemeldet war. Eine solche Auskunft hat ihrer formalen Struktur nach eine gewisse Ähnlichkeit mit der Abfrage des Inhabers einer Telefonnummer. Ihr Erkenntniswert bleibt punktuell. Systematische Ausforschungen über einen längeren Zeitraum oder die Erstellung von Persönlichkeits- und Bewegungsprofilen lassen sich allein auf Grundlage solcher Auskünfte nicht verwirklichen.

Maßgeblich ist zum anderen, dass für solche Auskünfte nur ein von vornherein feststehender kleiner Ausschnitt der Daten verwendet wird, deren Speicherung für sich genommen unter deutlich geringeren Voraussetzungen angeordnet werden könnte. Eine Speicherung allein der für solche Auskünfte erforderlichen Internetzugangsdaten zur Identifizierung dynamischer IP-Adressen hätte ein erheblich weniger belastendes Gewicht als die nahezu vollständige Speicherung der Daten sämtlicher Telekommunikationsverbindungen. Aus dem Zusammenwirken dieser Gesichtspunkte ergibt sich, dass die für die Verwendung von vorsorglich gespeicherten Telekommunikationsverkehrsdaten ansonsten maßgeblichen Anforderungen für solche Auskünfte nicht gleichermaßen gelten."

3. Diskussionsentwurf des BMJ zur nationalen Umsetzung der Richtlinie 2006/24/EU

a) Das BMJ hat am 7. Juni 2011 einen Diskussionsentwurf für ein Gesetz zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet an die Ressorts versandt. Dieser sieht im Wesentlichen Folgendes vor

- § 100j StPO-E: eine anlassbezogene Speicherungspflicht für zukünftig anfallende und eine Aufbewahrungspflicht für noch nicht gelöschte Verkehrsdaten (Quick Freeze),
- § 100k StPO-E: eine Regelung zur Beauskunftung von Bestandsdaten auch unter Nutzung von Verkehrsdaten (dynamische IP-Adressen) sowie eine Statistikpflicht,
- § 113a TKG-E:eine anlassunabhängige siebentägige Speicherung von Internetprotokoll-Adressen, Zeitangaben und Anschlusskennungen,
- §§ 113b-f TKG-E: eine Verwendungsregelung, Maßnahmen zur Sicherung der nach § 113a TKG-E erhobenen Daten und Protokollierung sowie
- § 23 JVEG-E: eine Gebührenregelung für Auskunftsersuchen

Mit dem neuen § 100j StPO-E soll eine Anordnungsbefugnis für eine anlassbezogene Speicherungspflicht für zukünftig anfallende und eine Aufbewahrungspflicht für noch nicht gelöschte Verkehrsdaten geschaffen werden, soweit dies zur Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes eines Beschuldigten erforderlich ist. Es würden dadurch die bei den Telekommunikationsunternehmen noch nicht gelöschte bzw. zukünftig anfallenden Verkehrsdaten gesichert („eingefroren") und den Strafverfolgungsbehörden unter Richtervorbehalt für eine begrenzte Zeit zur Verfügung stehen.

Der Diskussionsentwurf sieht in § 113a TKG-E eine siebentägige Speicherung von Internetprotokoll-Adressen, Zeitangaben und Anschlusskennungen vor, auf die die Strafverfolgungsbehörden keinen direkten Zugriff haben, sondern die nur mittelbar für eine Bestandsdatenauskunft verwendet werden, . In Umsetzung der Zielsetzung der Vorgaben von Artikel 5 Absatz 1 Buchstabe a Nummer 2, Buchstabe c Nummer 2 und Buchstabe e Nummer 3 der Richtlinie 2006/24/EG werden in § 113a TKG-E Einzelheiten zu den von den Anbietern von Internetzugangsdiensten zu speichernden Datenkategorien geregelt. Die Verfügbarkeit der zu speichernden Daten ist für Ermittlungszwecke notwendig, um nachvollziehen zu können, welchem Anschluss zu einem bestimmten Zeitpunkt eine bestimmte, den Strafverfolgungsbehörden bekannt gewordene Internetprotokoll-Adresse zugewiesen war, die für einen bestimmten Kommunikationsvorgang im Internet genutzt wurde. Diese befristete Speicherung soll zu dem Zweck erfolgen, auf Grundlage des neuen § 100k StPO-E Bestandsdatenauskünfte insbesondere zur Bekämpfung von Kinderpornografie im Internet zu den den

Strafverfolgungsbehörden bereits bekannten Internetprotokoll-Adressen zu ermöglichen.

Die zusätzlich vorgeschlagenen Änderungen im Telekommunikationsgesetz dienen im Wesentlichen der Sicherstellung der Vorgaben des Bundesverfassungsgerichts zur Gewährleistung der Datensicherheit und Datenqualität. So regeln die §§ 113a bis 113f TKG-E die Einzelheiten zu den Speicherungspflichten, zur Verwendung und Gewährleistung der Sicherheit der Daten sowie zur Protokollierung der Zugriffe auf die Daten. Zudem werden Einzelheiten für den von der Bundesnetzagentur zu erstellenden Anforderungskatalog der technischen Vorkehrungen und sonstigen Schutzmaßnahmen und für das von den verpflichteten Unternehmen zu erstellende Sicherheitskonzept geregelt.

Der Diskussionsentwurf dient nicht nur der bereits unter Buchstabe e) dargestellten Umsetzung der Zielsetzung der Vorgaben von Artikel 5 Absatz 1 Buchstabe a Nummer 2, Buchstabe c Nummer 2 und Buchstabe e Nummer 3 der Richtlinie 2006/24/EG, sondern darüber hinaus mit den §§ 113a Absatz 3 und 4 TKG-E und dem § 100k Absatz 4 StPO-E der Zielsetzung der Vorgaben aus Artikel 5 Absatz 2, Artikel 8 und 10 der Richtlinie 2006/24/EG:

- Entsprechend Artikel 5 Absatz 2 der Richtlinie 2006/24/EG sieht § 113a Absatz 3 TKG-E ein Verbot der Speicherung des Inhalts der Kommunikation und der Daten über aufgerufene Internetseiten auf Grund der Vorschrift des § 113a TKG-E vor.

- Artikel 8 der Richtlinie 2006/24/EG verpflichtet die Mitgliedstaaten dazu, die Daten so zu speichern, dass diese und alle sonstigen damit zusammenhängenden erforderlichen Informationen unverzüglich an die zuständigen Behörden weitergeleitet werden können. Dieser Vorgabe entspricht § 113a Absatz 4 TKG-E:

  > „(4)Die Speicherung der Daten hat so zu erfolgen, dass Auskunftsersuchen der berechtigten Stellen unverzüglich beantwortet werden können."

- Schließlich dient § 100k Absatz 4 StPO-E auch der Umsetzung eines Teils des Artikels 10 der Richtlinie 2006/24/EG, wonach der Kommission jährlich eine Statistik über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder eines öf-

fentlichen Kommunikationsnetzes erzeugt oder verarbeitet werden, zu übermitteln ist.

Im Vordergrund dieses Entwurfs steht neben der dargestellten Umsetzung bestimmter Vorgaben der Richtlinie 2006/24/EG ein quick-freeze-Verfahren (data preservation), also eine Regelung über die Sicherung zukünftig anfallender und vorhandener Verkehrsdaten bei den Telekommunikationsunternehmen ähnlich den Vorgaben in den Artikeln 16 und 17 des Übereinkommens des Europarats über Computerkriminalität vom 23. November 2001.

b) Die Geeignetheit dieses Verfahrens als Alternative zur anlasslosen Speicherung von Verkehrsdaten ist Gegenstand der Erörterungen auch auf der Ebene der Europäischen Union. Während die Kommission in ihrem Evaluierungsbericht zur Umsetzung der Richtlinie 2006/24/EG vom 15. März 2006 über die Vorratsspeicherung von Daten nicht davon ausgeht, dass das quick-freeze-Verfahren die Vorratsdatenspeicherung adäquat ersetzen könne[1], fordert der Europäische Datenschutzbeauftragte in seiner Stellungnahme zu dem Kommissionsbericht, dass im Rahmen der Folgenabschätzung auch weniger einschneidende Alternativen geprüft werden müssten[2], und zwar auch deshalb, weil die Notwendigkeit für eine Vorratsdatenspeicherung, wie in der Richtlinie vorgeben, nicht ausreichend nachgewiesen worden sei. Ferner hat die Kommission im Rahmen des 8. Treffens der Sachverständigengruppe „Vorratsspeicherung von elektronischen Daten zum Zwecke der Verhütung, Ermittlung, Feststellung und Verfolgung von schweren Straftaten“ (SV-Gruppe) am 17. Mai 2011 in Brüssel mitgeteilt, dass sie beabsichtige, die SV-Gruppe auch bei der Durchführung der von ihr in Aussicht genommenen Folgenabschätzung zu Rate zu ziehen und hierfür Untergruppen einzurichten, von denen sich eine mit der Untersuchung des quick-freeze-Verfahrens befassen sollte. Am 1. Juni 2011 wurde seitens der Kommission mitgeteilt, dass anstelle der Unterarbeitsgruppe nach Möglichkeit eine externe Studie zu dem Thema data preservation eingeholt werden soll.

---

[1] Punkt 3.3. des Bewertungsberichts der Kommission zur Richtlinie über die Vorratsdatenspeicherung vom 18. April 2011 (KOM 2011 (225) endgültig).

[2] RN 76 der “Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)” vom 31. Mai 2011.

Sowohl die Kommission als auch der Europäische Datenschutzbeauftragte kommen ferner übereinstimmend zu dem Ergebnis, dass die Richtlinie 2006/24/EG mit dem Ziel der Harmonisierung überarbeitet werden muss.

So ist aus den in dem Evaluierungsbericht aufgeführten Berichten der Mitgliedstaaten ersichtlich, dass diese insbesondere die Vorgaben zum Zweck der Vorratsdatenspeicherung[3], zum Datenschutz und zur Datensicherheit[4], zum Zugang zu den Daten[5], zu den Speicherungsfristen[6] sowie zu dem Inhalt der Statistik[7] teilweise erheblich unterschiedlich umgesetzt haben. In den Schlussfolgerungen und Empfehlungen kommt der Evaluierungsbericht daher zu dem Ergebnis[8]:

„Die Kommission wird sicherstellen, dass jeder künftige Vorschlag zur Vorratsdatenspeicherung dem Grundsatz der Verhältnismäßigkeit Rechnung trägt, dem Ziel der Bekämpfung von schwerer Kriminalität und Terrorismus entspricht und nicht über das dazu Erforderliche hinausgeht. Sie wird respektieren, dass sich Einschränkungen in Bezug auf den Schutz personenbezogener Daten auf das Notwendige beschränken müssen. Sie wird sorgfältig prüfen, wie sich eine strengere Regulierung der Speicherung und Verwendung von Verkehrsdaten sowie des Zugangs zu ihnen auf die Wirksamkeit und Effizienz des Strafjustizsystems und der Strafverfolgung, die Privatsphäre und die Kosten der öffentlichen Verwaltung und der Betreiber auswirkt."

Der Europäische Datenschutzbeauftragte führt aus, dass die Vorratsdatenspeicherung weniger in die Privatsphäre eingreifend hätte geregelt werden können[9]. Zudem lasse die Richtlinie zu viel Spielraum für die Mitgliedstaaten, um zu entscheiden, für welche Zwecke die Daten verwendet werden können, und wem und unter welchen Bedingungen Zugang zu ihnen gewährt werden kann[10].

Diese von der Kommission und dem Europäischen Datenschutzbeauftragten angeführten Argumente und Schlussfolgerungen für eine Änderung der Richtlinie 2006/24/EG mit dem Ziel der Harmonisierung sollten nicht nur wie von der Kommission angekündigt in der anstehenden Folgenabschätzung berücksichtigt werden.

Sie sollen und werden auch bei dem initiierten Gesetzgebungsvorhaben in Deutschland im Vorgriff auf eine künftige Neuregelung der Richtlinie 2006/24/EG in die Ge-

---

[3] Punkt 4.1. des Bewertungsberichts.
[4] Punkt 4.6. des Bewertungsberichts.
[5] Punkt 4.3. des Bewertungsberichts.
[6] Punkt 4.5. des Bewertungsberichts.
[7] Punkt 4.7. des Bewertungsberichts.
[8] Punkt 8.6. des Bewertunsgberichts.
[9] RN 36 und 85 der „Opinion".
[10] RN 35 der „Opinion".

samtbewertung zum Inhalt und Umfang des gesetzgeberischen Handlungsbedarfs einfließen.

c) Mit dem Diskussionsentwurf des BMJ prüft und diskutiert die Bundesregierung grundrechtsschonende Möglichkeiten zur Umsetzung von Vorgaben der Richtlinie 2006/24/EG. Die Frage nach der Umsetzung weiterer Vorgaben der Richtlinie ist Gegenstand der im Juni 2011 eingeleiteten und noch nicht abgeschlossenen Ressortabstimmung.

4. Zum weiteren Verfahren

Die Bundesregierung hat im Gespräch mit der Europäischen Kommission am 21. Januar 2011 die Eckpunkte des Ansatzes des Bundesministeriums der Justiz zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet skizziert.

Zwischenzeitlich sind die Vorbereitungen zur Gestaltung eines künftigen Verfahrens zur Sicherung vorhandener Daten weiter fortgeschritten. Der auf der Grundlage dieser Eckpunkte durch das Bundesministerium der Justiz erstellte Diskussionsentwurf eines Gesetzes wurde im Juni 2011 den betroffenen Bundesministerien zur Abstimmung übermittelt. Am 7. Juli 2011 hat dazu eine erste Besprechung stattgefunden.

Die Bundesregierung wird die Europäische Kommission unaufgefordert über die weiteren Verfahrensschritte informieren.

Die Bundesregierung steht der Kommission zur vertiefenden Erörterung insbesondere in Bezug auf die geplanten datenschutzrechtlichen Vorkehrungen gerne zur Verfügung und bietet ein weiteres Gespräch ausdrücklich an.