C. Europarecht

Unsere Position

- Wir beantragen,dem Europäischen Gerichtshof die Frage vorzulegen, ob die Richtlinie 2006/24/EG gültig ist.
- Das BVerfG ist nach Artikel 267 AEUV (ex-Artikel 234 EGV) zur Vorlage verpflichtet. Denn wenn die Richtlinie 2006/24/EG ungültig ist, ist unsere Verfassungsbeschwerde gegen § 113a TKG insgesamt zulässig und begründet.
- Die Richtlinie 2006/24/EG ist ungültig.
  - Die Richtlinie ist mit den Gemeinschaftsgrundrechten aus Art. 7 (Privatleben), 8 (Datenschutz), 11 (Meinungsfreiheit), 15 (Berufsfreiheit), 17 (Eigentum) und 20 (Gleichheitssatz) der Grundrechte-Charta unvereinbar.
    - Sie verletzt das in Art. 52 GRCh verankerte Verhältnismäßigkeitsgebot
    - Der Verfassungsgerichtshof Rumäniens hat bereits einen Verstoß gegen die EMRK angenommen. Nach Art. 52 GRCh folgt daraus zugleich ein Verstoß gegen die Gemeinschaftsgrundrechte.
    - Der Europäische Gerichtshof für Menschenrechte (S. und Marper gg. das Vereinigte Königreich, Urteil vom 4.12.2008) hat schon in der Vorratsspeicherung von Fingerabdrücken eine Grundrechtsverletzung gesehen, weil eine solche „umfassende und wahllose Befugnis zur Speicherung [...] einen unverhältnismäßigen Eingriff“ begründe. Erst recht muss dies für die weit tiefer eingreifende Totalprotokollierung des Telekommunikations-, Bewegungs- und Internetnutzungsverhaltens gelten.
  - Die Richtlinie mangels Rechtsgrundlage ungültig.
    - Entgegen der Meinung des EuGH rechtfertigt Art. 114 AEUV (ex-Artikel 95 EGV) nicht den Erlass der Richtlinie. Das Fernmeldegeheimnis und die Strafverfolgung gehören nicht zu den „Rechts- und Verwaltungsvorschriften der Mitgliedstaaten, welche die Errichtung und das Funktionieren des Binnenmarkts zum Gegenstand haben“. Andernfalls könnte die EU weite Teile des Straf- und Strafprozessrechts mit der Begründung harmonisieren, Unterschiede begründeten Wettbewerbsverzerrungen.
    - Auch der EU-Vertrag rechtfertigt die Richtlinie nicht. Sie betrifft nicht die grenzüberschreitende Zusammenarbeit der Polizei.

Gegenargumente widerlegt

„Die Verfassungsbeschwerde gegen Umsetzungsrecht ist unzulässig. Anderweitiger Rechtsschutz ist durch Anrufung der Fachgerichte eröffnet, die ihrerseits den EuGH befassen können.“

- Eine Abweisung als unzulässig ist mit Art. 93 Abs. 1 Nr. 4a GG, § 93 Abs. 3 BVerfGG unvereinbar, wo eine unmittelbare Gesetzesverfassungsbeschwerde ausdrücklich vorgesehen ist, weil gegen Gesetze „ein Rechtsweg nicht offensteht“.
- Die Beschwerde ist „von allgemeiner Bedeutung“ und daher vor Erschöpfung des Rechtswegs zulässig (§ 90 Abs. 2 BVerfGG).
- Die Vorratsdatenspeicherung zieht „schwere und unabwendbare Nachteile“ (§ 90 Abs. 2 BVerfGG) für die Beschwerdeführer nach sich, weil sie sich bei vertraulichen Aktivitäten der Telekommunikation nicht mehr geschützt vor Nachteilen bedienen können. Falls sie auf die Fachgerichte verwiesen würden, müssten sie unzumutbar lange auf Abhilfe warten.
- Die lange Verfahrensdauer, die eingeschränkte Qualität und Autorität einer Vorlage durch ein Amts- oder Landgericht wäre mit dem Recht auf effektiven Rechtsschutz unvereinbar (Art. 19 Abs. 4 GG).
- Das italienische Verfassungsgericht hat die Zulässigkeit von Verfassungsbeschwerden gegen Umsetzungsgesetze inzwischen anerkannt und legt in solchen Fällen vor.

D.I.1. Gewicht der Datenspeicherung

Unsere Position

- Die Vorratsdatenspeicherung zieht nicht wiedergutzumachende Nachteile für die Betroffenen nach sich.
  - Bürger können Beratung, Informationen und Hilfsangebote am Telefon und im Internet (z.B. Telefonseelsorge, Eheberatung, Suchtberatung, AIDS-Beratung) nicht mehr ohne das Risiko eines Bekanntwerdens ihres Problems in Anspruch nehmen. Dies kann schwerste Folgen nach sich ziehen, bis hin zu schweren Straftaten (z.B. Kindesmissbrauch durch Pädophilen, der sich zu einer Behandlung hätte überzeugen lassen).
  - Die Arbeit regierungs- und staatskritischer Personen und Gruppierungen wird beeinträchtigt, wenn sie Ermittlungen aufgrund ihrer elektronischen Kontakte befürchten müssen. Der Beschwerdeführer zu 2 ist allein wegen Kontakten zu „linksradikalen Gruppen“ vom Verfassungsschutz beobachtet worden. Die Furcht vor staatlichen Ermittlungen kann etwa die Vorbereitung von Demonstrationen beeinträchtigen.
  - Die Informationsfreiheit im Internet ist nicht mehr gewährleistet, weil man zurzeit Nachteile durch den Aufruf „potenziell verdächtiger“ Seiten oder die Verwendung „potenziell verdächtiger“ Suchwörter befürchten muss. Bis 2008 ermittelte das Bundeskriminalamt gegen Personen, die „auffällig oft“ auf Internetseiten über die „militante gruppe“ zugriffen, obwohl dies aus vielerlei Gründen, etwa journalistischer Art, legitim sein kann. 2007 ist eine – ergebnislose – Wohnungsdurchsuchung bei Globalisierungskritikern damit begründet worden, der Betroffene habe eine „umfassende Internetrecherche“ zu einer Firma vorgenommen, die später Ziel eines Brandanschlags wurde.
  - *Journalisten verlieren Informanten und damit Informationen, mit deren Hilfe Missstände in Staat und Gesellschaft aufgedeckt werden können.*
  - *Strafverfolgungsbehörden und Aufsichtsbehörden entgehen wichtige Informationen über Rechtsverletzer, weil Voraussetzung einer Übermittlung solcher Insider-Informationen oft die absolute Anonymität des Informanten ist („Whistleblower“).*
  - Insgesamt führt die Vorratsdatenspeicherung teilweise dazu, dass sensible Kontakte und Kommunikationen auf umständlichere Kanäle verlegt werden müssen und dadurch erschwert werden oder sogar insgesamt enden. Dies fügt nicht nur den Betroffenen, sondern auch ihren Mitmenschen und der Gesellschaft gravierenden Schaden zu.

Zahlen und Fakten

- Die mit Schriftsatz vom 11.02.2008 vorgetragene Umfrage des Arbeitskreis Vorratsdatenspeicherung ergab, dass die Vorratsdatenspeicherung die Nutzung von Telefon, Handy, E-Mail und Internet in weiten Teilen der Gesellschaft behindert:
  - Bürger, die keine E-Mails mehr versenden, Journalisten, die den Kontakt zu Informanten verlieren, Unternehmer, die Unterlagen wieder per Post verschicken müssen - die Vorratsdatenspeicherung führt in weiten Bereichen der Gesellschaft zurück in die Zeit, als es weder Telefon noch Internet gab.
  - Eine Bürgerin berichtet, ein Selbsthilfeforum von Missbrauchsopfern im Internet werde nicht mehr genutzt.
  - Ein Journalist berichtet, ein Informant aus einer Sicherheitsbehörde habe ihm bereits in der Neujahrsnacht mitgeteilt, er möchte "ab heute nie mehr unter dieser Nummer" angerufen werden. Auch SMS mit "Sitzungsergebnissen" erhalte der Journalist seit Jahresbeginn nicht mehr.
  - Ein Steuerberater teilt mit, seine Mandanten würden seit Jahresanfang telefonische Rückfragen bei ihm scheuen. Er befürchte, "dass sich die Mandanten mangels Beratung strafbar machen" könnten.
  - Ein Unternehmer aus Süddeutschland klagt, seine Kunden würden "sicherheitsrelevante Beschreibungen" nur noch persönlich übergeben wollen, was dem Unternehmen große Schwierigkeiten bereite. Seine Firma habe dadurch vor wenigen Tagen "einen Großkunden verloren", was den Verlust von 2-3 Arbeitsplätzen nach sich ziehen werde.
  - Drogenberater und Psychotherapeuten beklagen, dass Anrufe ausbleiben oder inhaltslos verlaufen.
  - Ein Rettungsassistent berichtet gar von einem Patienten, der nicht wollte, dass sein Zustand telefonisch an die Klinik durchgegeben wird, in die er eingeliefert werden sollte.

- Berichte über nachteilige Auswirkungen kamen auch von Anwälten, Forschern, betrieblichen Vertrauenspersonen, Ärzten, Seelsorgern und Geistlichen.

- Eine repräsentative Umfrage des Meinungsforschungsinstituts Forsa unter 1.002 Bundesbürgern am 27./28. Mai 2008 ergab:
  - Die Mehrheit der Befragten würde wegen der Vorratsdatenspeicherung davon absehen, per Telefon, E-Mail oder Handy Kontakt zu einer Eheberatungsstelle, einem Psychotherapeuten oder einer Drogenberatungsstelle aufzunehmen, wenn sie deren Rat benötigten (517 der Befragten). Hochgerechnet entspricht dies über 43 Mio. Deutschen.
  - Jede dreizehnte Person hat wegen der Verbindungsdatenspeicherung bereits mindestens einmal darauf verzichtet, Telefon, Handy oder E-Mail zu benutzen (79 der Befragten). Hochgerechnet entspricht dies 6,5 Mio. Deutschen.
  - Jede sechzehnte Person hat den Eindruck, dass andere Menschen seit Beginn der Vorratsdatenspeicherung seltener per Telefon, Handy oder E-Mail Kontakt mit ihr aufnehmen (62 der Befragten). Hochgerechnet entspricht dies 5 Mio. Deutschen.
  - Besonders stark ist die Veränderung des Kommunikationsverhaltens unter Menschen mit geringem Bildungsniveau (Haupt- oder Grundschulabschluss), die annehmbar besonders hohen Beratungsbedarf haben.

- 96% der deutschen Haushalte verfügen über mindestens einen Telefonanschluss. 71% der Haushalte verfügen über einen Internetzugang.

- Nach Angaben der Deutschen Telekom AG fallen jährlich 120 Mrd. Verbindungsdaten von Telefongesprächen bei ihr an, unter Einschluss von Fehlverbindungen 180 Mrd. Datensätze.

- Laut MIT entspricht der Informationsgehalt der von 95 Personen in neun Monaten erzeugten Verkehrsdaten dem Ergebnis einer 35-jährigen Beobachtung der Personengruppe. Im Vergleich zu den traditionellen Befugnissen ist der Zugriff auf Verkehrsdaten also 46mal eingriffsintensiver.

- Die Verkehrsdaten von 8% der Mitglieder einer Gruppe genügen, um die Beziehungen sämtlicher Mitglieder der Gruppe zueinander aufzudecken.

- In einem Versuch des US-amerikanischen Forschungszentrums MIT wurden Telekommunikations-Verbindungsdaten und auf 10m genaue Standortdaten von 100 Versuchspersonen erhoben. Mithilfe dieser Daten gelang es mit einer 90%igen Genauigkeit, die Arbeitskollegen, Bekannten und Freunde einer jeden Person zu identifizieren. Ferner waren umfangreiche Vorhersagen möglich. Anhand der Bewegungsdaten einer Person während eines Monats konnte mit einer 95%igen Genauigkeit vorhergesagt werden, wann sich die Person am Arbeitsplatz, zu Hause oder an einem anderen Ort aufhalten würde. Weiter konnte mit einer 90%igen Genauigkeit vorhergesagt werden, ob sich zwei Personen innerhalb der nächsten Stunde begegnen würden. Anhand der Aktivitäten einer Person während der ersten 12 Stunden eines Tages konnten die Aktivitäten während der verbleibenden 12 Stunden mit etwa 80% Genauigkeit vorhergesagt werden.

Gegenargumente widerlegt

„Durch strikte Begrenzung der Zugriffsrechte und hohe Datensicherheitsanforderungen lässt sich das Vertrauen der Bürger und damit eine unbefangene Telekommunikation wieder herstellen."

- Falsch. Ungeachtet striktester Vorkehrungen beeinträchtigt das mit der Vorratsdatenspeicherung notwendig verbundene Risiko von Nachteilen infolge eines Bekanntwerdens vertraulicher Kontakte, Aktivitäten und Interessen die Fernmeldefreiheit unzumutbar.

- Im Bereich der legalen Datennutzung begründen Verkehrsdaten ein hohes Risiko von Falschverdächtigungen. Immer wieder lenken sie den Verdacht auf Unschuldige. So wurde 2007 die Wohnung eines deutschen Professors durchsucht und seine Computer beschlagnahmt, weil er Kinderpornografie über das Internet verbreitet haben soll. Tatsächlich hatte sein Internet-Zugangsanbieter der Polizei eine falsche Auskunft erteilt. Häufig sind auch Fälle, in denen Anschlüsse von Dritten genutzt werden und der Inhaber zu Unrecht in Verdacht gerät.

- Auch außerhalb des Bereichs der legalen Datennutzung begründet die Vorratsdatenspeicherung unzumutbare Risiken.
  - Die mit der Vorratsdatenspeicherung verbundenen Risiken übersteigen das allgemeine Datensicherheitsrisiko, weil die Vorratsdatenspeicherung eine so große Menge an so sensiblen Informationen bei so vielen Unternehmen anfallen lässt. Dementsprechend ist die Gefahr eines unerwünschten Bekanntwerdens von Vorratsdaten besonders groß.

- Es besteht das Risiko illegaler Zugriffe durch das speichernde Unternehmen. So wertete die Deutsche Telekom AG über einen Zeitraum von insgesamt anderthalb Jahren missbräuchlich 250.000 Telefonverbindungsdaten von Journalisten sowie von Arbeitnehmer-Aufsichtsräten, Managern und Betriebsräten des Unternehmens aus. Anhand von Handy-Standortdaten wurden auch die Bewegungen der Betroffenen nachverfolgt.
- Europaweit erfolgten in den letzten Jahren wiederholt versehentliche und absichtliche Weitergaben und Missbräuche von Informationen über unsere Telekommunikation, so in Italien, Griechenland, Lettland, Bulgarien, der Slowakei und in Ungarn.
- Es besteht das Risiko illegaler Zugriffe durch Alleingänge einzelner Mitarbeiter eines der speichernden Unternehmen.
    - Im Jahr 2006 verkaufte ein Mitarbeiter von T-Mobile die Daten der 17 Mio. Prepaid- und Postpaid-Kunden des Mobilfunkunternehmens, darunter eine erstaunliche Anzahl geheimer Nummern und Privatadressen von bekannten Politikern, Ministern, Ex-Bundespräsidenten, Wirtschaftsführern, Milliardären und Glaubensvertretern, für die die Verbreitung ihrer Kontaktdaten in kriminellen Kreisen eine Bedrohung ihrer Sicherheit darstellt (etwa Charlotte Knobloch, Präsidentin des Zentralrats der Juden).
    - Im Jahr 2009 veranlassten zwei rheinland-pfälzische CDU-Politiker Polizistinnen zu illegalen Datenabrufen aus dem Polizeicomputer. Ähnliche Kontakte zu TK-Unternehmen sind nicht auszuschließen. Zugriffe werden zurzeit nicht einmal protokolliert; selbst dann aber wäre keine effektive Überprüfung der vielen Protokolle möglich.
    - Es besteht das Risiko einer versehentlichen Bekanntgabe der Daten (Datenpanne). So waren im Januar 2009 bei der Deutschen Telekom Vertragsdaten für jedermann über das Internet abrufbar. In der letzten Zeit sind immer wieder Datenpannen verschiedenster Wirtschaftsunternehmen bekannt geworden.
    - Es besteht das Risiko illegaler Zugriffe Dritter (Hacker).
    - Es besteht das Risiko illegaler staatlicher Datenzugriffe. Oft wird die Rechtswidrigkeit erst nachträglich oder nie festgestellt, denn der Betroffene kann Rechtsmittel erst einlegen, wenn die Informationen bereits bekannt geworden sind.
    - Es besteht das Risiko von Missbrauch durch einzelne Staatsbeamte, besonders, wo kein Richtervorbehalt existiert (Identifizierung von Internetnutzern).
- Letztlich sind nur nicht gespeicherte Daten sichere Daten. Deswegen lässt sich nur durch strikte Datensparsamkeit und die Aufhebung der Vorratsdatenspeicherung selbst eine spurenlose und furchlose Telekommunikation wieder herstellen.

„Etwaige Beeinträchtigungen der unbefangenen Telekommunikation sind dem Staat nicht zuzurechnen, weil sie auf politischen Kampagnen oder unbegründeten Ängsten beruhen.“

- Falsch. Sowohl die Bürgerinitiativen wie auch die Ängste der Bürger sind begründet, wie die o.g. Beispiele zeigen.

D.I.3.a. Datenabruf zur Strafverfolgung

Unsere Position

- Eine Nutzung von Vorratsdaten zur Strafverfolgung muss dem Staat schon deswegen insgesamt untersagt werden, weil die Vorratsdatenspeicherung selbst verfassungswidrig ist.
    - Die Richtlinie 2006/24/EG steht nicht entgegen. Sie regelt laut EuGH nicht, ob und unter welchen Voraussetzungen Datenzugriffe zugelassen werden.
- Die Vorratsdatenspeicherung ist aus empirischer Sicht bei der Strafverfolgung problemlos verzichtbar. Eine angemessene und wirksame Strafverfolgung ist auch ohne Vorratsdatenspeicherung möglich.
    - Dies belegt die Situation in Deutschland vor Einführung der Vorratsdatenspeicherung (bis 2007)
    - Dies belegt die Situation in Staaten ohne Vorratsdatenspeicherung noch heute (z.B. Österreich)
- Insbesondere genügt die Möglichkeit von Speicher- und Aufbewahrungsanordnungen im Verdachtsfall.
- Die Vorratsdatenspeicherung erhöht die Aufklärungsrate oder senkt die Kriminalitätsrate nicht in einem statistisch signifikanten Maß.
- Umgekehrt gefährdet die Vorratsdatenspeicherung Menschenleben, indem sie Straftätern, Kranken und Hilfsbedürftigen die Möglichkeit nimmt, sich anonym und ohne Furcht vor Nachteilen helfen zu lassen. So hat ein Schüler, der einen Amoklauf an seiner Schule plante, vor Beginn der Vorratsdatenspeicherung noch ohne Furcht vor Verhaftung die Telefonseelsorge anrufen können und konnte überzeugt werden, sein Vorhaben aufzugeben.
- Dass es der Vorratsspeicherung in der Telekommunikation nicht bedarf, zeigt sich daran, dass auch mündliche und schriftliche Kontakte sowie unsere Bewegungen noch nie nachvollziehbar gewesen sind und trotzdem entsprechende Straftaten ausreichend verfolgt werden können.

Zahlen und Fakten

- Die durchschnittliche Aufklärungsquote unter den polizeilich registrierten Straftaten beträgt 55%. Mittels Telekommunikation begangene Straftaten müssen ebensowenig immer aufklärbar sein wie andere Straftaten, zumal es sich – wenn es bei einem einmaligen Kontakt bleibt – typischerweise um leichte Vergehen handelt.
- Das Max-Planck-Institut für ausländisches und internationales Strafrecht hat festgestellt, dass schon die nach bisherigem Recht verfügbaren Kommunikationsdaten eine effektive Strafverfolgung sicher stellen: Bei nur 4% der Zielanschlüsse konnten die begehrten Verkehrsdaten nicht erlangt werden. Selbst wenn man mit Rheinland-Pfalz davon ausginge, dass die Zahl das 2,5-fache betrage, weil gelöschte Verkehrsdaten zum Teil schon nicht abgefragt würden, so wären Abfragen doch zu 90% erfolgreich. Das reicht vollauf, um die Aufklärungsquote von 55% zu sichern.
- 70% der vom Max-Planck-Institut untersuchten, abgeschlossenen Verfahren mit Zugriffen auf Verkehrsdaten wurden trotz vorhandener Verkehrsdaten eingestellt.
- Unter Berücksichtigung aller Umstände ergibt sich, dass die Verfolgung von Straftaten zu bestenfalls 0,006% durch eine Vorratsspeicherung von Verkehrsdaten effektiviert werden kann (näher Schriftsatz vom 17.03.2008).
- Das Bundeskriminalamt nennt in einer Studie 381 Ermittlungsverfahren, in denen den Behörden Verbindungsdaten fehlten – gemessen an den 6 Mio. pro Jahr begangenen Straftaten ein verschwindend geringer Bruchteil von nicht einmal 0,01%.

Gegenargumente widerlegt

„Wegen der zunehmenden Verbreitung von Flatrates werden immer weniger Abrechnungsdaten gespeichert."

- Diese Entwicklung wird durch andere Entwicklungen mehr als ausgeglichen:
    - Im Informationszeitalter spielt sich ein immer größerer Teil unseres Lebens an Telefon, Handy und im Internet ab. Unter dem Strich werden heute daher so viele Abrechnungsdaten gespeichert wie noch nie.
    - Auch die staatlichen Zugriffsmöglichkeiten sind beständig ausgeweitet worden. Unter dem Strich eignet sich der Staat Verkehrsdaten heute so häufig an wie noch nie (2008 in über 8.000 Ermittlungsverfahren).
    - Es ist daher falsch, dass die Ermittlungsmöglichkeiten heute geringer wären als früher; das Gegenteil ist der Fall. Bis 1990 fielen überhaupt keine Telekommunikations-Verbindungsdaten an.

- Außerdem hat die Verbreitung von Flatrates in der Praxis keinerlei messbare Auswirkung auf die Aufklärungsquote gehabt. So hat die Zahl der Internet-Flatrates schon vor Einführung der Internet-Vorratsdatenspeicherung 2009 rasant zugenommen; gleichwohl belegen die Statistiken des Bundeskriminalamts keinen merklichen Rückgang der weit überdurchschnittlichen Aufklärungsquote bei Internetkriminalität.

„Schwerste Straftaten (z.B. Stalking, Betrug, Bombendrohungen) können ohne Vorratsdatenspeicherung nicht aufgeklärt werden."

- Falsch. Es stehen mildere Mittel zur Verfügung (Fangschaltung im Verdachtsfall).
- Es ist nicht gesagt, ob Vorratsdaten die Überführung des Täters ermöglicht hätten. 70% der Verfahren werden ausweislich der Studie des Max-Planck-Instituts trotz vorhandener Verkehrsdaten eingestellt.
- Insgesamt gesehen hat die Vorratsdatenspeicherung keinen statistisch signifikanten Einfluss auf die Aufklärungsrate.
- Die Situation in Deutschland vor Einführung der Vorratsdatenspeicherung wie auch in Staaten, die bis heute keine Vorratsdatenspeicherung kennen, zeigt, dass die Vorratsdatenspeicherung problemlos verzichtbar ist.
- Die durchschnittliche Aufklärungsrate liegt bei 55%, in anderen Rechtsstaaten teils erheblich darunter. Es ist normal, dass viele Straftaten nicht aufklärbar sind. Es gibt keinen Grund, warum gerade mittels Telekommunikation begangene Straftaten total aufklärbar sein müssten, zumal es sich ganz regelmäßig um minderschwere Vergehen handelt.
- Der Zugriff auf Daten über die Telekommunikation von Bürgern in der Vergangenheit ist ebensowenig „unverzichtbar" wie Aufzeichnungen über das sonstige Kommunikations-, Bewegungs- und Informationsverhalten der Bürger.
- Das Interesse an einer strafrechtlichen Verfolgung einzelner Täter muss hinter die Telekommunikationsfreiheit der unzähligen rechtmäßig handelnden Nutzer zurücktreten.

„Ohne Vorratsdatenspeicherung ist die Sicherheit der Bevölkerung bedroht."

- Falsch. Umgekehrt gefährdet die Vorratsdatenspeicherung Menschenleben, indem sie Straftätern, Kranken und Hilfsbedürftigen die Möglichkeit nimmt, sich anonym und ohne Furcht vor Nachteilen helfen zu lassen. Schon zahlenmäßig wiegt diese jeden TK-Nutzer treffende Gefährdung schwerer als die von vereinzelten Straftätern schon immer ausgehenden Gefahren.

D.I.3.b. Datenabruf zur Gefahrenabwehr

Unsere Position

- Eine präventive Nutzung von Vorratsdaten muss dem Staat schon deswegen versagt bleiben, weil die Vorratsdatenspeicherung selbst verfassungswidrig ist.
    - Die Richtlinie 2006/24/EG steht nicht entgegen. Sie regelt laut EuGH nicht, ob und unter welchen Voraussetzungen Datenzugriffe zugelassen werden.
    - Besonders Nachrichtendienste dürfen keinen Zugriff erhalten:
        - Sie operieren in Abwesenheit jeder Gefahr.
        - Sie handeln im Geheimen, benötigen keine richterlichen Anordnungen und sind zur nachträglichen Benachrichtigung der Betroffenen nicht verpflichtet, weswegen eine effektive Kontrolle ihres Handelns nicht zu gewährleisten ist. Dies zeigen schon die Skandale um illegale Überwachungsmaßnahmen des Bundesnachrichtendienstes.
        - Die Beschwerdegegner haben in ihren Stellungnahmen nicht einen konkreten Fall aufzuzeigen vermocht, in dem ein Nachrichtendienst über vorhandene Abrechnungsdaten hinaus weitere Verkehrsdaten benötigt hätte.
- Die Vorratsdatenspeicherung ist aus empirischer Sicht problemlos verzichtbar. Eine angemessene und wirksame Gefahrenabwehr ist auch ohne Vorratsdatenspeicherung möglich.
    - Dies belegt die Situation in Deutschland vor Einführung der Vorratsdatenspeicherung (bis 2007)
    - Dies belegt die Situation in Staaten ohne Vorratsdatenspeicherung (z.B. Österreich)
- Insbesondere genügt die Möglichkeit von Speicheranordnungen und Ortungen im Verdachtsfall.
- Die Vorratsdatenspeicherung erhöht die Zahl abgewehrter Gefahren nicht in einem statistisch signifikanten Maß.
- Umgekehrt gefährdet die Vorratsdatenspeicherung Menschenleben, indem sie Straftätern, Kranken und Hilfsbedürftigen die Möglichkeit nimmt, sich anonym und ohne Furcht vor Nachteilen helfen zu lassen. So hat ein Schüler, der einen Amoklauf an seiner Schule plante, vor Beginn der Vorratsdatenspeicherung noch ohne Furcht vor Verhaftung die Telefonseelsorge anrufen können und konnte überzeugt werden, sein Vorhaben aufzugeben.
- Dass es der Vorratsspeicherung in der Telekommunikation nicht bedarf, zeigt sich daran, dass auch mündliche und schriftliche Kontakte sowie unsere Bewegungen noch nie nachvollziehbar gewesen sind und trotzdem entsprechende Gefahren ausreichend abgewehrt werden können.

D.I.4. Nutzung der Daten zur Auskunftserteilung nach § 113 Abs. 1 TKG

Unsere Position

- Die §§ 113b, 113 TKG ermöglichen es einer Vielzahl von Sicherheitsbehörden, ohne Eingriffsschwelle (schon zur Abwehr von Bagatellgefahren oder Verfolgung von Ordnungswidrigkeiten) und ohne richterliche Kontrolle, das Fernmeldegeheimnis durch „Bestandsdatenanfragen“ der folgenden Art zu durchbrechen:
  - Welcher Kunde Ihres Unternehmens hat am 01.01.2009 um 12:01 an der Internetverbindung mit der IP-Adresse 101.101.101.101 teilgenommen (über die auf ein AIDS-Beratungsportal zugegriffen wurde)?
  - Welche Kunden Ihres Unternehmens haben am 01.01.2009 zwischen 9.00 Uhr und 14.00 Uhr in den Funkzellen mobil telefoniert, welche den Schloßbezirk 3 in Karlsruhe abdecken?
  - Mit welchen Kunden Ihres Unternehmens sind in den letzten sechs Monaten über den Anschluss 072191010 Verbindungen hergestellt worden?
- Mit solche Anfragen zwingt der Staat Kommunikationsmittler, durch eine Rasterung von Verkehrsdaten die Identität der Teilnehmer an bestimmten Kommunikationsvorgängen zu ermitteln und dem Staat offen zu legen.
- Es ist offensichtlich, dass solche Anfragen der Ausforschung des Fernmeldeverkehrs dienen. Das Fernmeldegeheimnis schützt nämlich nach st. Rspr. des BVerfG die Information, „zwischen welchen Personen oder Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat“
- Die Information, wer kommuniziert hat, ist auch nicht weniger schutzwürdig wie die Information, wie lange man kommuniziert hat oder worüber. Sie ist integraler Bestandteil des Fernmeldevorgangs.
- Deswegen müssen solche Anfragen denselben gesetzlichen Anforderungen unterworfen werden wie die sonstige Ausforschung der Telekommunikation.
- Österreich hat dies bereits erkannt und will die Bestandsdatenabfrage entsprechend regeln (näher Schriftsatz vom 11.12.2009).
- Der deutsche Gesetzgeber hat den Eingriff in das Fernmeldegeheimnis verkannt. Deswegen ist § 113 TKG verfassungswidrig.
- Viele Anbieter von Internet-Portalen protokollieren zurzeit dem deutschen Telemediengesetz zuwider anhand der Internet-Kennung (IP-Adresse), wer welche Texte gelesen oder geschrieben, wer welche Videos betrachtet oder welche Suchwörter eingegeben hat. Die Zuordnung von Internetkennungen muss nach § 113a TKG sechs Monate lang gespeichert werden.
- Wer seine Zeitung statt gedruckt im Internet liest oder Informationen statt in der Bibliothek im Internet recherchiert, muss gegenwärtig – unter den lächerlich geringen Voraussetzungen des § 113 TKG – sechs Monate lang damit rechnen, in einen falschen Verdacht oder unter Beobachtung zu geraten.
- Was speziell die Vorratsdatenspeicherung angeht, muss die Nutzung von Vorratsdaten dem Staat schon deswegen generell versagt bleiben, weil die Vorratsdatenspeicherung selbst verfassungswidrig ist.

Zahlen und Fakten

- § 113 Abs. 1 TKG lautet: „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. Auskünfte über Daten, mittels derer der Zugriff auf Endgeräte oder in diesen oder im Netz eingesetzte Speichereinrichtungen geschützt wird, insbesondere PIN oder PUK, hat der nach Satz 1 Verpflichtete auf Grund eines Auskunftsersuchens nach § 161 Abs. 1 Satz 1, § 163 Abs. 1 der Strafprozessordnung, der Datenerhebungsvorschriften der Polizeigesetze des Bundes oder der Länder zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung, § 8 Abs. 1 des Bundesverfassungsschutzgesetzes, der entsprechenden Bestimmungen der Landesverfassungsschutzgesetze, § 2 Abs. 1 des BND-Gesetzes oder § 4 Abs. 1 des MAD-Gesetzes zu erteilen; an andere öffentliche oder nicht öffentliche Stellen dürfen diese Daten nicht übermittelt werden. Ein Zugriff auf Daten, die dem Fernmeldegeheimnis unterliegen, ist nur

unter den Voraussetzungen der hierfür einschlägigen gesetzlichen Vorschriften zulässig. Über die Auskunftserteilung hat der Verpflichtete gegenüber seinen Kundinnen und Kunden sowie Dritten gegenüber Stillschweigen zu wahren."

- § 113 TKG stellt wegen seiner unzureichenden Voraussetzungen den Schwerpunkt der Nutzung von Vorratsdaten dar. Der Deutsche Telekom-Konzern hat schon 2006 94.417 Auskünfte nach § 113 TKG erteilt und rechnete für 2007 mit über 210.000 Auskünften. Nach § 100g StPO erfolgten im Jahr 2008 hingegen nur knapp 14.000 Anfragen (Beschlüsse).
- Über § 113 TKG wird im Internetbereich massenhaft Kleinkriminalität verfolgt. Bei der Deutschen Telekom AG erfolgten die Anfragen
  - wegen Betrug und Computerbetrug zu 54,44%
  - wegen Beleidigungen zu 6,19%
  - wegen Ausspähens von Daten zu 6,18%
  - wegen Urheberrechtsdelikten zu 3,94%
  - wegen der Verbreitung pornographischer Schriften zu 3,15%
  - wegen sexuellen Missbrauchs zu 1,31%
- Laut polizeilicher Kriminalstatistik setzten sich die 2008 im Internet begangenen und registrierten Straftaten wie folgt zusammen:
  - zu 76,7% Betrug, vor allem Warenbetrug und Warenkreditbetrug (Aufklärungsquote 82%)
  - zu 5,9% Urheberrechtsdelikte (Aufklärungsquote 62%)
  - zu 6,2% die Verbreitung pornografischer Schriften (Aufklärungsquote 64%)
- Die Aufklärungsquote betrug 2008 – also vor Inkrafttreten der Vorratsdatenspeicherung für Internet-Zugangsanbieter – knapp 80% und überstieg die durchschnittliche Aufklärungsquote von 54,8% in allen Bereichen.
- Das Bundeskriminalamt ermittelte mit § 113 TKG seit 2004 insgesamt 417 Personen, die „auffällig oft" auf Internetseiten über die „militante gruppe" zugriffen. Die Personen stellten sich hauptsächlich als Pressemitglieder und Behörden heraus. Ermittlungen gegen die übrigen Personen verliefen im Sande.
- 2007 ist eine – ergebnislose – Wohnungsdurchsuchung bei Globalisierungskritikern damit begründet worden, der Betroffene habe eine „umfassende Internetrecherche" zu einer Firma vorgenommen, die später Ziel eines Brandanschlags wurde.

Gegenargumente widerlegt

„Ohne die Speicherung von IP-Adressen ist die Aufklärung schwerster Straftaten im Internet/die Durchsetzung des Urheberrechts im Internet von vornherein unmöglich."

Falsch. Auch ohne Vorratsdatenspeicherung ist eine angemessen wirksame Verfolgung von Internetdelikten möglich.

- Im Bereich andauernder Straftaten (z.B. Urheberrechtsdelikte) genügt ein Anruf bei dem Anbieter, um noch während der bestehenden Verbindung die Identität des Anschlussinhabers gezielt zu sichern. Dieses Quick-Freeze-Verfahren ist in der Cybercrime-Konvention des Europarats vorgesehen und in Deutschland vertragswidrig noch nicht umgesetzt. Ein Urteil des Landgerichts Hamburg zeigt, dass gerade Urheberrechtsdelikte in diesem Verfahren wirksam verfolgt werden können.
- Im Bereich von Wiederholungstaten (z.B. Stalking) genügt eine verdachtsbezogene Fangschaltung. Auf diese Weise konnte beispielsweise ein Erpresser in einem Internet-Café festgenommen werden.
- Viele Fälle können trotz verfügbarer Daten nicht aufgeklärt werden, z.B. wegen der vielen Verschleierungsmöglichkeiten. Viele Verfahren werden trotz verfügbarer Daten eingestellt.
- In den verbleibenden, sehr wenigen Fällen (weniger als 0,01% aller Straftaten) ist es normal, dass im Internet – wie sonst auch – viele Straftaten nicht aufgeklärt werden können. Die Aufklärungsquote liegt im Schnitt bei 55%; 45% der angezeigten Straftaten können auch außerhalb des Internet nicht aufgeklärt werden. Es gibt keine Gründe, die es rechtfertigen könnten, gerade das besonders grundrechtswichtige Internet zu einem Raum der Überwachbarkeit und Nachverfolgbarkeit auszugestalten.
- Deutschland vor Einführung der Vorratsdatenspeicherung und ausländische Staaten ohne Vorratsdatenspeicherung (z.B. Österreich) belegen, dass auch ohne Vorratsdatenspeicherung eine angemessen wirksame Verfolgung von Internetdelikten möglich ist. Unternehmen, die nicht auf Vorrat speichern (z.B. Hansenet), und ausländische Anonymisierungsdienste ermöglichen schon heute eine spurenlose Internetnutzung, ohne dass dies zu untragbaren Folgen geführt hätte.
- Empirisch betrachtet führt die Vorratsdatenspeicherung auch im Internet nicht zu einer höheren Aufklärungsquote oder gar geringeren Kriminalitätsrate als wo nicht auf Vorrat gespeichert wird.

- Was Urheberrechtsdelikte angeht, kann der Gesetzgeber außerdem eine pauschale Abgeltung privater Vervielfältigungen in Betracht ziehen. Es ist nicht erforderlich und verhältnismäßig, wegen weniger Rechtsverletzer alle Internetnutzer erfassen zu lassen.
- Das Interesse an einer zivil- oder strafrechtlichen Verfolgung einzelner Täter muss hinter die Telekommunikationsfreiheit der unzähligen rechtmäßig handelnden Nutzer zurücktreten.

„Durch die Zunahme von Flatrates und eine veränderte Speicherpraxis der Internet-Zugangsanbieter stehen immer weniger Daten zur Verfolgung von Straftätern/'Musik-Piraten' zur Verfügung.“

- Diese Entwicklung hat nichts mit Flatrates zu tun. Internet-Zugangsanbieter durften die zugewiesene IP-Adresse noch nie zu Abrechnungszwecken speichern, weil sie abrechnungsirrelevant ist (§ 96 TKG).
- Die Abnahme betrieblich gespeicherter Daten wird zudem durch andere Entwicklungen mehr als ausgeglichen:
  - Im Informationszeitalter wickeln immer mehr Menschen einen immer größeren Teil ihrer Aktivitäten im Internet ab. Unter dem Strich werden heute daher so viele Daten betrieblich gespeichert wie noch nie.
  - Auch die staatlichen Zugriffsmöglichkeiten sind beständig ausgeweitet worden. Unter dem Strich werden Internetnutzer heute so häufig identifiziert wie noch nie.
  - Es ist daher falsch, dass die Ermittlungsmöglichkeiten heute geringer wären als früher; das Gegenteil ist der Fall.
  - Was Urheberrechtsverletzungen angeht, ist die Benutzung eines Tonbandgeräts, CD-Brenners oder Fotokopiergeräts viel weniger nachvollziehbar als die Internetnutzung – selbst ohne Vorratsdatenspeicherung.
- Außerdem hat die Verbreitung von Flatrates in der Praxis keinerlei messbare Auswirkung auf die Aufklärungsquote gehabt. So hat die Zahl der Internet-Flatrates schon vor Einführung der Internet-Vorratsdatenspeicherung 2009 rasant zugenommen; gleichwohl belegen die Statistiken des Bundeskriminalamts keinen merklichen Rückgang der (überdurchschnittlichen) Aufklärungsquote bei Internetkriminalität.

D.I.5. Transparenz, Rechtsschutz, Sanktionen

Unsere Position

- Wirksam wäre die Beteiligung eines unabhängigen Repräsentanten des Betroffenen, also eines „Bürgeranwalts“, schon vor dem staatlichen Zugriff. Nur ein Bürgeranwalt könnte gegebenenfalls noch vor Durchführung der Maßnahme Rechtsmittel einlegen und dadurch Grundrechtsverletzungen verhindern. Im Ausland bestehen solche Institutionen teilweise bereits.
- Nachschau: Der Richter sollte darüber informiert werden, zu welchem Ergebnis seine Anordnung geführt hat. Nur durch solche Rückmeldungen kann er die Erfolgsaussichten und damit die Verhältnismäßigkeit etwaiger künftiger Anordnungen beurteilen.
- Benachrichtigung: Die Benachrichtigungspflicht des § 101 StPO hat der Gesetzgeber so ausgehöhlt, dass sie in der Praxis fast durchgehend keine Wirkung mehr entfaltet; dies ist zu ändern (näher Schriftsatz vom 09.06.2009). Daneben ist eine Pflicht zur Benachrichtigung der Betroffenen auch von Auskünften über ihre Bestandsdaten zu fordern (§§ 112, 113 TKG, 101a UrhG).
- Verwertungsverbot: Zu fordern ist eine Pflicht zur sofortigen Vernichtung sowie ein Verwertungsverbot für Informationen, die durch rechtswidrige verdeckte Ermittlungsmaßnahmen erlangt worden sind.
- Entschädigungsanspruch: Zu fordern ist ein Anspruch der von rechtswidrigen Ermittlungsmaßnahmen Betroffenen auf angemessene Entschädigung. Für die Verletzung immaterieller Rechte ist wiederum eine angemessene Pauschale als Entschädigung vorzusehen. Nur durch solche Anreize kann eine gerichtliche Befassung mit dem Zugriff auf Telekommunikationsdaten erreicht werden.
- Verbandsklagerecht: Bürgerrechtsverbände sollten das Recht erhalten, gegen grundrechtsverletzende Praktiken von Behörden als Verband zu klagen. Der Individualrechtsschutz läuft oft aus finanziellen und fachlichen Gründen leer.
- Erfolgskontrolle: Zur rechtsstaatlichen Einhegung des Zugriffs auf Telekommunikationsdaten ist es geboten, fortlaufend die Wirksamkeit der staatlichen Zugriffspraxis auszuwerten und die Ergebnisse zu veröffentlichen, zumal vor dem Hintergrund der explodierenden Zugriffszahlen der letzten Jahre.

D.II. Art. 12 Abs. 1 GG

Unsere Position

- Die nach § 113a TKG zur Vorratsdatenspeicherung Verpflichteten müssen für die damit verbundenen Anschaffungs-, Investitions-, Speicher-, Vorhalte- und Personalkosten alleine aufkommen.
- Die Beschwerde führenden und schriftsätzlich näher beschriebenen Anbieter von Anonymisierungs- und Telekommunikationsdiensten haben die Vorratsdatenspeicherung bis heute nicht umgesetzt – unter Inkaufnahme der damit verbundenen, hohen Risiken. Bliebe ihre Verfassungsbeschwerde ohne Erfolg, könnte ihr Dienst jedenfalls in Deutschland nicht fortbestehen. Dies würde nicht nur die Anbieter und ihre Angestellten treffen, sondern auch für die Kunden zu einer weiteren Marktkonzentration, weniger Wettbewerb und höheren Preisen führen.
- Die entschädigungslose Speicherpflicht verletzt das Gleichbehandlungsgebot des Art. 3 GG. Es existiert kein Grund, der nach Art und Gewicht die Belastung der beteiligten Unternehmen oder mittelbar ihrer Kunden mit den Kosten einer Kommunikationsdatenspeicherung zu staatlichen Zwecken rechtfertigen könnte. Die Abwehr von Gefahren und die Ahndung von Straftaten ist eine Aufgabe der Allgemeinheit, deren Lasten nur die Allgemeinheit treffen dürfen und die deshalb im Wesentlichen nur aus Steuermitteln finanziert werden darf.
- Besonders kleine Unternehmen sind ohne hinreichenden Grund stärker belastet als größere Wettbewerber. Eine Umsetzung der Vorratsdatenspeicherung erfordert Fixkosten, die Kleinunternehmen überproportional viel stärker belasten als große Firmen.
- Bei kleinen Unternehmen liegt auch ein unzumutbarer Eingriff in die Berufsfreiheit (Art. 12 GG) vor, weil sie die hohen Fixkosten einer Vorratsdatenspeicherung nicht aufbringen können und andererseits praktisch niemals Auskunftsersuchen an sie gerichtet werden.
- Die Verfassungsgerichte Österreichs und Frankreichs haben bereits entschieden, dass eine Entschädigung von Telekommunikationsunternehmen für die Erfüllung staatlicher Aufgaben geboten ist, ebenso das VG Berlin. Österreich will Kleinunternehmen überhaupt von der Verpflichtung zur Vorratsdatenspeicherung befreien.
- Die Richtlinie 2006/24/EG steht einer Entschädigung nicht entgegen. Umgekehrt spricht ihr Zweck, Wettbewerbsverzerrungen zu vermeiden, gerade für eine Entschädigung, wie sie auch ausländische Staaten verbreitet gewähren.
- Für Anonymisierungsdienste kommt § 113a TKG einem Berufsverbot nahe und verletzt Art. 12 GG.
  - Ein Anonymisierungsdienst ist definitionsgemäß ein Dienst, der eine Rückverfolgung der Internetnutzung verhindern soll. Wird hinter den vorratsspeichernden Internet-Zugangsanbieter bloß ein weiterer vorratsspeichernder Anonymisierungsdienst geschaltet, so wird der Dienst überflüssig und sein Geschäftsmodell obsolet.
  - Wie wichtig die Möglichkeit anonymer Kommunikation in vielen Lebenssituationen ist, ist schriftsätzlich – auch im Parallelverfahren – umfassend ausgeführt worden.
  - Die Richtlinie 2006/24/EG sieht keine Speicherpflichten für Anonymisierungsdienste vor, sondern setzt das Fortbestehen echter Anonymisierungsdienste voraus.
  - Mir ist kein anderes Land in Europa bekannt, das Anonymisierungsdiensten Speicherpflichten auferlegt hätte.
  - Diese Pflichten sind auch nicht zielführend, weil sich Dutzende oder Hunderte von Nutzern eines solchen Dienstes gleichzeitig eine IP-Adresse teilen und § 113a TKG daher keine Rückverfolgbarkeit gewährleistet.

Gegenargumente widerlegt

„Die Beschwerdeführer haben eine unzumutbare Kostenbelastung nicht ausreichend dargelegt."

- Wir haben zu den drohenden wirtschaftlichen Auswirkungen sehr wohl vorgetragen.
- Außerdem hat es das OVG Berlin-Brandenburg mit Beschluss vom 02.12.2009 im Fall eines Webhosting-Unternehmens aus Bremen für glaubhaft gehalten, die Kosten einer Umsetzung der Vorratsdatenspeicherung würden das Unternehmen „zur sofortigen Geschäftsaufgabe zwingen" bzw. der Betrieb müsse „mangels Liquidität eingestellt werden". Die Situation des Beschwerde führenden Anonymisierungsdienstes ist nicht anders.