



BUNDESRECHTSANWALTSKAMMER

Stellungnahme
der Bundesrechtsanwaltskammer
zur
Evaluation der Vorratsdatenspeicherung

erarbeitet durch den
Ausschuss Datenschutzrecht
der Bundesrechtsanwaltskammer

Mitglieder:

- RA Klaus **Brisch**, LL.M., Vorsitzender
RA Prof. Dr. Armin **Herb**
RA Dr. Hans **Klees**
RA Stephan **Kopp**
RA Jörg Martin **Mathis**
RA Dr. Hendrik **Schöttle**
RA Dr. Ralph **Wagner**, LL.M., *Berichterstatter*
RAin Friederike **Lummel**, BRAK Berlin

Juli 2011

BRAK-Stellungnahme-Nr. 44/2011

Im Internet unter www.brak.de

Verteiler:

Europäische Kommission

Bundesministerium der Justiz

Bundesministerium des Inneren

Landesjustizminister/Justizsenatoren der Länder

Innenausschuss des Deutschen Bundestages (BT)

Rechtsausschuss des Deutschen Bundestages (BT)

Ausschuss für Wirtschaft und Technologie (BT)

Ausschuss für Arbeit und Soziales (BT)

Ausschuss für Verkehr, Bau und Stadtentwicklung (BT)

Ausschuss für Kultur und Medien (BT)

Bundesnotarkammer

Bundessteuerberaterkammer

Wirtschaftsprüferkammer

Deutscher Notarverein

Deutscher Anwaltverein

Deutscher Steuerberaterverband

Deutscher Richterbund

Bundesverband der Freien Berufe

Deutscher Industrie- und Handelskammertag

Redaktion der Neuen Juristischen Wochenschrift/NJW

Die Bundesrechtsanwaltskammer (BRAK) ist als Dachorganisation der 27 regionalen deutschen Rechtsanwaltskammern und der Rechtsanwaltskammer beim BGH die gesetzliche Vertretung der derzeit ca. 157.000 in Deutschland zugelassenen Rechtsanwältinnen und Rechtsanwälte. Sie tritt für die wirtschaftlichen und rechtlichen Belange der Anwaltschaft ein.

Die Kommission der Europäischen Union hat am 18.04.2011 ihren Evaluationsbericht zur Richtlinie über Vorratsdatenspeicherung (2006/24/EG) vorgelegt. Sie hat Stellungnahmen dazu erbeten, wie hinsichtlich der Vorratsdatenspeicherung weiter verfahren werden soll. Sie hat aus ihrer Sicht problematische Positionen und Fragen im Internet veröffentlicht (http://ec.europa.eu/home-affairs/policies/police/police_data_en.htm). Von den dazu bisher vorliegenden Stellungnahmen ist besonders jene des EU-Datenschutzbeauftragten (vom 31.05.2011) hervorzuheben.

Die BRAK legt folgende Kernaussagen von Seiten der Kommission der nachfolgenden Stellungnahme zugrunde:

Improving the current framework

In line with its recent evaluation report, the Commission believes that the EU should continue to support and regulate the storage of, access to and use of telecommunications data a tool for law enforcement, the protection of victims and the criminal justice systems. More harmonised rules in this area are needed to ensure that it remains effective but that industry has legal certainty in a smoothly functioning internal market, and that the high levels of respect for privacy and the protection of personal data are applied consistently throughout the EU.

In the coming weeks and months, the Commission will consult with judiciary, law enforcement authorities, data protection authorities, industry and civil society on the impact of options for reforming the current framework. There are three broad options for the future:

- **Better enforcement** of the current Directive, and particularly data protection requirements,
- Changing the **scope** of data covered by EU rules and the **purpose** for which they may be stored and used, and

- **Greater harmonisation and stronger regulation** in the interests of privacy, the internal market and the EU's internal security.

1 Evaluation

Die Kommission hat im Evaluationsbericht vom 18.04.2011 für die geltende Richtlinie zur Vorratsdatenspeicherung sehr ausführlich dargestellt, welcher Umsetzungsstand in den Mitgliedsstaaten erreicht ist und welche Erfahrungen sich in Anwendung der Richtlinien ergeben haben.

Die BRAK erlaubt sich, auf folgende Gesichtspunkte hinzuweisen, die im Evaluationsbericht nicht vertieft behandelt werden, jedoch entscheidende Bedeutung für die Frage besitzen, ob Vorratsdatenspeicherung weiterhin erfolgen muss, soll oder darf:

- 2 Die Kommission hat im Evaluationsbericht dargelegt, dass polizeiliche Ermittlungen durch Rückgriff auf vorratsgespeicherte Daten unterstützt oder auch erheblich erleichtert oder auch überhaupt erst ermöglicht werden. Insoweit ist eindeutig festzuhalten, dass dieser Effekt der Vorratsdatenspeicherung vernünftigerweise von niemandem bestritten werden kann. Es liegt auf der Hand, dass jede Sachverhaltsklärung, insbesondere polizeiliche Ermittlungsarbeit, erleichtert wird, wenn möglichst große Datenmengen abrufbar sind. Durch systematische Vorratsdatenspeicherung und Bereitstellung dieser Daten an die Ermittlungsbehörden lässt sich ohne weiteres erwarten, dass Ermittlungen schneller, umfassender und mit höherer Aufklärungsquote geführt werden können.
- 3 Ebenso eindeutig ist mit der Vorratsdatenspeicherung ein enormer Eingriff in die Privatsphäre jedes Bürgers der Europäischen Union verbunden. Die komplette Belastung ist in den einzelnen Mitgliedsstaaten - wie im Evaluationsbericht der Kommission detailliert ausgeführt - sehr verschieden. Als von der Richtlinie geforderte Mindestbelastung lässt sich aber zusammenfassen:

Für jedes Telefonat (über Festnetz, Funknetz oder Internet), jede Internetnutzung und jede E-Mail werden für mindestens ein halbes Jahr Beginn und Ende, Absender und Empfänger sowie Aufenthaltsort gespeichert. Angesichts moderner Kommunikationsgewohnheiten bedeutet dies für EU-Bürger, dass für die jeweils (mindestens) letzten sechs Monate nicht nur ihre Kommunikation, sondern auch ihr räumlicher Aufenthalt fast lückenlos aufgezeichnet wird.

Dieser enorme Nachteil der Vorratsdatenspeicherung ist - wie ihr klarer Vorteil für polizeiliche Ermittlungen - eindeutig.

- 4 Für die Gesamtbeurteilung der Vorratsdatenspeicherung ist zwingend eine Abwägung erforderlich zwischen ihrem klaren Vorteil (Erleichterung polizeilicher Ermittlungen) und ihrem klaren Nachteil (Überwachung der Kommunikation und der Aufenthaltsorte sämtlicher Bürger für einen langen Zeitraum). Dies ist auch europarechtlich spätestens seit dem Urteil des EuGH vom 09.11.2010 in den Rechtssachen Schecke und Eifert (C-92/09 und C-93/09) geklärt. Das vom Europäischen Gerichtshof dort entwickelte Prüfschema („proportionality test“) für Eingriffe in den Datenschutz wurde unmittelbar vor Fertigstellung des Evaluationsberichtes auch in der Konferenz vom 03.12.2010 ausführlich diskutiert (Bericht der Kommission über die Konferenz zur Vorratsdatenspeicherung am 03.12.2010 in Brüssel, Kommissionsdokument home.a.3(2011)295871, Statement Prof. Dr. Adamski, Seite 8 et passim).
- 5 Bei Anlegung dieser Kriterien verbleiben erhebliche Zweifel an der Verhältnismäßigkeit (und damit europarechtlichen Zulässigkeit) der Vorratsdatenspeicherung:
- 6 Die Zweifel betreffen nicht die erste Stufe des Verhältnismäßigkeits-Tests, nämlich jene der Geeignetheit. Die ergriffene Maßnahme (Vorratsdatenspeicherung) ist - wie oben unter Tz. 2 dargestellt - sicher geeignet, polizeiliche Ermittlungen zu erleichtern. Dagegen lässt sich nicht das (teils verwendete) Argument anführen, gerade schwere und planmäßig begangene Verbrechen würden mit Vorbedacht unter Nutzung solcher Kommunikationsmittel begangen, die nicht der Vorratsdatenspeicherung unterfallen. Es mag sein, dass deshalb die vorratsgespeicherten Daten nicht für alle Ermittlungen hilfreich sind. Unzweifelhaft bleiben sie aber zweckdienlich bei vielen anderen Sachverhalten.
- 7 Erhebliche Bedenken bestehen demgegenüber bereits auf der zweiten Stufe der Verhältnismäßigkeits-Prüfung, jener der Erforderlichkeit. Wie der Evaluationsbericht der Kommission klar darstellt, wurden die Vorgaben der Richtlinie in zwei Mitgliedstaaten (Österreich und Schweden) überhaupt nicht umgesetzt. In weiteren drei Mitgliedsstaaten (Tschechien, Deutschland und Rumänien) wurden die zur Umsetzung erlassenen Vorschriften von den nationalen Gerichten wieder außer Kraft gesetzt. In zahlreichen weiteren Mit-

gliedsstaaten erfolgte die Umsetzung der Richtlinie unvollständig. Die Jahre seit Inkrafttreten der Richtlinie (2006 bis 2011) können also geradezu als Probe dafür betrachtet werden, ob sich zwischen Staaten mit und ohne Vorratsdatenspeicherung erhebliche Unterschiede im Kriminalitätsaufkommen, in der Aufklärungsquote von Verbrechen (insbesondere auch schweren Verbrechen) zeigen. Solche Effekte sind eindeutig nicht zu beobachten.

Auch in der Konferenz vom 08.12.2010 wurde durch Teilnehmer aus dem Bereich der Polizei mehrfach bestätigt, dass Instrumente der e-privacy-Richtlinie (insbesondere Art. 15 Abs. 1) mit ähnlichen Ermittlungserfolgen eingesetzt werden und in der Praxis Verwendung finden.

Damit ist einerseits indiziert, dass mit Vorratsdatenspeicherung verbundene Vorteile nicht signifikant werden, andererseits ohne Vorratsdatenspeicherung keine signifikanten Nachteile bei der Verbrechensbekämpfung auftreten.

- 8 Die dritte Stufe der Verhältnismäßigkeits-Prüfung (nämlich jene der „Verhältnismäßigkeit im engeren Sinne“, „proportionality sensu strictu) ergibt für die Vorratsdatenspeicherung (jedenfalls in der Ausgestaltung durch die aktuelle Richtlinie) sehr eindeutig einen Verstoß gegen den Verhältnismäßigkeitsgrundsatz: Zugelassen werden Speicherzeiten bis zu zwei Jahren. Die im Evaluationsbericht der Kommission veröffentlichten empirischen Daten belegen, dass die Nachfragen zu weit über 80 % Daten der letzten zurückliegenden sechs Monate, zu ca. zwei Drittel Daten der zurückliegenden letzten drei Monate betreffen. Nachfragen zu Daten jenseits des Jahreszeitraums kommen fast nicht vor.

Damit ist belegt, dass die Datenspeicherung derzeit auch Zeiträume erfasst, in denen sie keinen praktischen nennenswerten Ermittlungsvorteil bringt, der die Speicherung rechtfertigen könnte.

- 9 Mit ähnlicher Argumentation hat auch das deutsche Bundesverfassungsgericht in seiner Entscheidung vom 02.03.2010 (1 BvR 256, 263 und 586/08) festgehalten, dass „eine Speicherdauer von sechs Monaten angesichts des Umfangs und der Aussagekraft der gespeicherten Daten sehr lang“ sei und „an der Obergrenze dessen, was unter Verhältnismäßigkeitserwägungen rechtfertigungsfähig ist“ liege (a.a.O., Textziff. 215 unter C IV 4 b bb).

- 10 Neben dem Verstoß hinsichtlich der übermäßig langen Speicherfrist enthält die Richtlinie in der aktuellen Fassung zahlreiche weitere – teils offensichtliche – Verstöße gegen den Verhältnismäßigkeitsgrundsatz, z. B.
- wegen fehlender ausreichender Vorgaben zur technischen Sicherung der gespeicherten Daten,
 - wegen Unbestimmtheit der Zwecke, für die die gespeicherten Daten abgerufen und verwendet werden dürfen,
 - wegen Unbestimmtheit der zum Abruf und zur Verwendung berechtigten Personen,
 - wegen fehlender Schutzbestimmungen für besonders gefährdete Kommunikationsbereiche, in denen Vorratsdatenspeicherung nicht stattfinden darf (insbesondere ärztliche, anwaltliche und seelsorgerische Kommunikation).

Geboten und im Evaluationsbericht der Kommission nicht enthalten ist also eine Prüfung der Vorratsdatenspeicherung nach den europarechtlichen Grundsätzen der Verhältnismäßigkeit staatlicher Eingriffe in die Unionsbürgerrechte.

11 Hauptfragen der Kommission

- 12 In relation to what types of crime should it be possible to access and use stored telecommunications data?
- a) Wesentlich ist zunächst, dass die Vorratsdatenspeicherung in Folge gemeinschaftsrechtlicher Anordnung (kraft EU-Richtlinie) nur der Bekämpfung solcher Verbrechen dienen kann, die in sämtlichen EU-Mitgliedsstaaten als Straftaten klassifiziert sind. Vermieden werden muss die Situation, dass die Ermittlung, Verfolgung und Ahndung von Straftaten im Mitgliedsstaat A mit Hilfe von Vorratsdaten aus dem Mitgliedsstaat B durchgeführt wird, in dem die in A kriminalisierten Handlungen nicht unter Strafe stehen.
 - b) Es ist zwingend erforderlich, einen abschließenden Katalog besonders schwerer Straftaten zu erstellen, für deren Verfolgung auf gespeicherte Vorratsdaten zurückgegriffen werden kann. Dieser Katalog könnte sich z. B. an jenen – in verschiedenen Mitgliedsstaaten existierenden – De-

liktsgruppen orientieren, für die (ihrerseits strafbewehrte) Anzeigepflichten existieren (vgl. z. B. § 138 deutsches StGB).

- c) Nicht gerechtfertigt – wenn auch unstrittig naheliegend – wäre die Nutzung der vorratsgespeicherten Daten für die Verfolgung von (auch weniger schweren) Straftaten im Telekommunikations- und Internetbereich. Diese Deliktsgruppen weisen durch ihre Begehungsart, nicht durch ihre Schwere, eine besondere Nähe zur Vorratsdatenspeicherung auf. Es ist jedoch allein die Schwere des Delikts (nicht dessen Begehungsart), die (wie oben ausführlich dargestellt) eine Vorratsdatenspeicherung rechtfertigen kann.

13 What precise categories of data should be retained in the light of evolutions in technology and criminal behaviour?

- a) Die Vorratsdatenspeicherung muss in jedem Fall auf die Speicherung von Verkehrsdaten beschränkt bleiben und darf keinerlei Inhaltsdaten einschließen. Es gilt der Grundsatz, dass Kommunikationsinhalte nur im Rahmen konkreter und laufender Ermittlungen (nicht präventiv) staatlich gespeichert werden dürfen. Die anlasslose und auf Vorrat erfolgende Speicherung von Kommunikationsinhalten wäre mit der Menschenwürde unvereinbar.
- b) Darüber hinaus gilt, dass auch die in der aktuellen Richtlinie vorgesehenen Datenkategorien kritisch daraufhin durchgemustert werden müssen, ob die Speicherung des einzelnen Kriteriums überhaupt den angestrebten Zweck (Verfolgung und Aufklärung von Straftaten) erfüllen kann. So scheinen – auch in den wenigen konkret veröffentlichten Beispielen – allein die Teilnehmer einer Kommunikation, deren Aufenthaltsorte sowie die Tatsache des Kommunikationsvorgangs entscheidend zu sein. Es bestehen Zweifel, ob Anfangs- und Endzeitpunkt des Kommunikationsvorgangs gespeichert werden müssen, nicht stattdessen z. B. zur Zuordnung die Speicherung des Anfangszeitpunkts genügt.
- c) Erweiterungen der Datenkategorien sind nicht allein unter dem Gesichtspunkt der (stets gegebenen und natürlich darstellbaren, vgl. oben Tz. 2) Nützlichkeit für Ermittlungszwecke erlaubt. Im Einzelfall muss geprüft werden, wie groß entstehende Ermittlungsvorteile einerseits und der Eingriff in die Privatsphäre des Bürgers andererseits sind.

14 For how long should these categories of data be stored?

Speicherung über einen längeren Zeitraum als sechs Monate scheint – auch nach der im Evaluationsbericht der Kommission wiedergegebenen empirischen Erfassung – nicht gerechtfertigt.

15 How can the EU ensure that data is stored and used only where it is strictly necessary to do so for the protection of the public against the harm of crime and terrorism?

a) Der Kreis zugriffsberechtigter Personen ist eng zu limitieren (dazu unten).

b) Gegen missbräuchlichen Zugriff und missbräuchliche Verwendung der vorratsgespeicherten Daten müssen in sämtlichen Mitgliedsstaaten wirksame – auch strafrechtliche – Sanktionen bestehen.

c) Für die effektive Prävention, wie auch für eine effiziente Überwachung des korrekten Einsatzes vorratsgespeicherter Daten muss eine Zugriffsprotokollierung erfolgen. Sie sollte gemeinschaftsrechtlich einheitlich geregelt werden.

16 Which authorities should be authorised to access and analyse these data?

a) Wegen der Sensibilität des Bestandes an vorratsgespeicherten Daten sollte für den Zugriff ein Richter-Vorbehalt gelten (wie bisher in vielen Mitgliedsstaaten bereits eingeführt). Dies findet seine Rechtfertigung in der Vergleichbarkeit des Datenzugriffs mit anderen, die Persönlichkeitsrechte der Betroffenen ähnlich einschränkenden Maßnahmen (Wohnungsdurchsuchung).

b) Nach Abschluss der Prüfungen sollten nur die relevanten Datensätze und das Prüfergebnis (nicht die vollständig eingesehenen Daten) bei den Ermittlungsakten verbleiben.

17 How should the risks of breaches of privacy and data protection be managed and minimised throughout the process of storage by providers, handover and use by authorities?

Die Vorratsdatenspeicherung sollte in verschlüsselter Form erfolgen, die Verschlüsselung nur durch Provider und Behörden gemeinsam aufgehoben werden können.

18 How could the EU ensure independent supervision of requests for access and of the overall storage and use regimes applied in all Member States?

Die Aufsicht kann – wie bisher - den nationalen Datenschutz-Aufsichtsbehörden übertragen sein.

19 How can particularly confidential communications data be protected?

Vorratsdatenspeicherung darf nicht die berufliche Kommunikation der traditionell zur Berufsverschwiegenheit verpflichteten Personen betreffen (insbesondere Ärzte, Anwälte, Seelsorger; vgl. z. B. § 53 StPO Deutschland). Wegen der teilweise fehlenden Identifizierungsmöglichkeiten entsprechender Kommunikationsdaten und zur Absicherung der Beachtung des Speicherverbotes muss insoweit auch ein nachgelagertes Verwertungsverbot (bei vorsätzlich oder fahrlässig erfolgter Speicherung / Auswertung) geregelt werden.

20 How can the EU ensure that service providers are consistently reimbursed and that the impact on consumers is minimised?

a) Die extreme voneinander abweichenden Angaben der Diensteanbieter zu den mit der Vorratsdatenspeicherung verbundenen Kosten zeigen, dass es nicht oder nur mit erheblichem Aufwand möglich sein wird, angemessene Beträge festzustellen. Hinzutritt, dass – z. B. auch nach Einschätzung des deutschen Bundesverfassungsgerichts in seiner Entscheidung vom 02.03.2010 (dort Textziff. 301 und 302) - eine übermäßige finanzielle Belastung der speicherpflichtigen Unternehmen nicht eintritt. Weiter ist zu bedenken, dass die in Sondersituation – z. B. für kleine Unternehmen – möglicherweise relativ höheren Lasten durch Einschaltung externer (wiederum bündelnd wirkender) Dienstleister reduziert werden kann. Eine Kostenerstattung an die Provider ist daher nicht gerechtfertigt.

b) Die auf solchem Weg stattfindende Marktbelastung (weil Weitergabe über die Dienstleistungspreise letztlich an alle Nutzer der Kommunikationsdienste) scheint auch angemessener, als eine Belastungsumwälzung auf die Gemeinschaft der Steuerzahler (bei der das Nutzungsverhalten gegenüber den betroffenen Kommunikationsmitteln unberücksichtigt bleibt).

21 What metrics and reporting procedures would enable assessment and comparison of how Member States apply the EU framework? How can the EU ensure that citizens and data protection authorities are able to report abuses or seek information on how data is being used?

Gesonderte Berichtsvorschriften und Informationsmittel scheinen nicht notwendig. Sowohl auf nationaler Ebene (bei Zuständigkeit der Datenschutz-Aufsichtsbehörden, außerdem durch parlamentarische Anfragen etc.) als auch auf EU-Ebene (parlamentarischer Aktivitäten) bestehen bereits ausreichende Kontrollmechanismen.

- 22 What would be the impact for security, criminal justice systems, the work of law enforcement, service providers and consumers of greater regulation at EU level in this area?

Die Folgen einer stärkeren Regulierung auf EU-Ebene sind nicht sicher absehbar. Zu den Vorteilen gehören könnte eine einheitliche EU-weite Anwendung bestehender Vorschriften. Allerdings zeigt die Erfahrung, dass auch bei Regelungen im Verordnungsweg die mitgliedstaatliche Anwendungspraxis teils deutlich differiert.

Nachteilig auswirken könnte sich die schwierigere Integration entsprechender Normen in den mitgliedstaatlichen Rechts-Kontext (Aufbau der Strafverfolgungsbehörden, Ablauf des Strafverfahrens, Zuständigkeitsregelungen).
