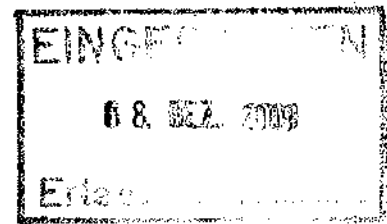




# Bundesverfassungsgericht

Erster Senat  
- Geschäftsstelle -



Bundesverfassungsgericht • Postfach 1771 • 76006 Karlsruhe

Herrn Rechtsanwalt  
Meinhard Starostik  
Schillstraße 9  
10785 Berlin

**Aktenzeichen**

**Bearbeiter**

**☎ (0721)**

**Datum**

1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08  
(bei Antwort bitte angeben)

9101-403

07.12.2009

**Verfassungsbeschwerden Vorratsdatenspeicherung**  
**Dortiges Aktenzeichen: 82/06**

Sehr geehrter Herr Rechtsanwalt,

in den vorbezeichneten Verfassungsbeschwerdeverfahren wird Ihnen anliegend das Schreiben des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vom 24. November 2009 zur Kenntnisnahme übersandt.

Mit freundlichen Grüßen

Auf Anordnung



(Andrick)  
Regierungshauptsekretärin



Der Bundesbeauftragte  
für den Datenschutz und  
die Informationsfreiheit

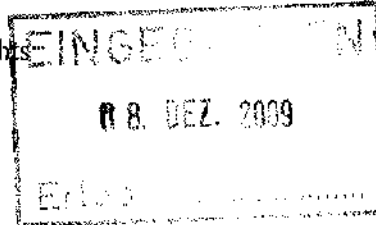
- 4. Dez. 2009 *3f*

**Peter Schaar**

Bundesbeauftragter für den Datenschutz  
und die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,  
Postfach 20 01 12, 53131 Bonn

Präsidenten des  
Bundesverfassungsgerichts  
Postfach 1771  
76006 Karlsruhe



HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn  
VERBINDUNGSBÜRO Friedrichstraße 50, 10117 Berlin

TELEFON (0228) 997799-100

TELEFAX (0228) 997799-550

E-MAIL [Ref8@bfdi.bund.de](mailto:Ref8@bfdi.bund.de)

INTERNET [www.bfdi.bund.de](http://www.bfdi.bund.de)

DATUM Bonn, 24.11.2009

BETREFF **Verfassungsbeschwerden gegen die Regelung zur Vorratsdatenspeicherung im Gesetz zur  
Neuregelung der Telekommunikationsüberwachung und anderer verdeckter  
Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21.12.2007**  
HIER Ergänzung meiner Stellungnahme vom 10.06.2009  
BEZUG 1. Ihr Schreiben vom 21.04.2009  
2. Mein Schreiben vom 10.06.2009

Sehr geehrter Herr Präsident,

in meiner Stellungnahme vom 10.06.2009 konnte ich zu einzelnen Fragen mangels eigener Erkenntnisse und Erfahrungen teilweise keine Angaben machen. Inzwischen liegen solche Erkenntnisse vor, die ich im Wesentlichen im Rahmen eines Evaluierungsprojekts der Artikel 29-Gruppe der Datenschutzbehörden der EU-Mitgliedstaaten, die die europaweite Umsetzung der Richtlinie zur Vorratsdatenspeicherung (2006/24/EG) untersucht, gewonnen habe. Hierzu habe ich die praktische Durchführung der Vorratsdatenspeicherung bei einigen deutschen Anbietern vor Ort geprüft. Im Folgenden möchte ich die bis jetzt gewonnenen wichtigsten Ergebnisse mitteilen.

### *1. Informationen zum Evaluierungsprojekt der Artikel-29-Gruppe*

Das wichtigste Ziel der Studie besteht in einer Analyse, ob und wie Datenschutzerfordernisse in Bezug auf die Art gespeicherter Daten, Sicherheitsmaßnahmen, der Prävention von



Missbrauch sowie Verpflichtungen aus Speicherfristen in der Telekommunikationsbranche in den Mitgliedstaaten erfüllt werden. Zu diesem Zweck habe ich sechs Unternehmen, die einen repräsentativen Querschnitt des nationalen Markts der Telekommunikationsanbieter darstellen, ausgewählt und einen Fragebogen zur Beantwortung übersandt. Im Nachgang haben meine Mitarbeiter dann vier der Unternehmen besucht, um sich vor Ort offen gebliebene Punkte erläutern zu lassen und die Umsetzung der Vorratsdatenspeicherung in der Praxis zu begutachten.

## *2. Umsetzung bei den Telekommunikationsunternehmen*

Die Telekommunikationsunternehmen verwenden verschiedene Ansätze zur Umsetzung der Vorratsdatenspeicherung. Teilweise wurden neue Systeme in Eigenregie entwickelt, teilweise wurden Lösungen bei externen Anbietern eingekauft. Dabei ist festzustellen, dass bei den kleineren der besuchten Anbieter das System noch nicht abschließend fertig gestellt ist. So wird bei einem Anbieter die Auskunftserteilung bezüglich der E-Mailnutzung nicht über eine hierfür entwickelte Benutzeroberfläche abgewickelt, sondern über einen – verhältnismäßig umständlichen – direkten Konsolen-Zugriff auf die Logfiles.

Die Vorratsdaten werden – bis auf eine Ausnahme – bei allen Anbietern auf von den übrigen Daten getrennten Systemen gespeichert. In einem Fall werden die Vorratsdaten bezüglich der Telefonie in einer gemeinsamen Datenbank mit den betrieblich genutzten Daten gehalten. Die Vorratsdaten werden bei den meisten Anbietern unverschlüsselt gespeichert.

Die Nutzungs- und Zugangsberechtigungskonzepte zu den Vorratsdaten werden bei allen Anbietern so umgesetzt, dass grundsätzlich nur ein eingeschränkter Mitarbeiterkreis nach Passworteingabe Zugriff auf die Vorratsdaten hat. Darüber hinaus wird der Zugang zu den Datenbanken bei der Mehrzahl der Anbieter auf eine limitierte Anzahl von IP-Adressen beschränkt, um den Kreis der Rechner zu beschränken, von denen aus der Zugriff möglich ist.

Die Arbeitsplätze der Mitarbeiter, die mit der Bearbeitung der Vorratsdaten beauftragt sind, befinden sich in der Regel in einem separierten Bereich, um eine (zufällige) Kenntnisnahme der Daten durch nicht für die Arbeit mit Vorratsdaten ermächtigte Mitarbeiter zu unterbinden. Lediglich bei einem Anbieter sind die mit der Beantwortung von Auskünften beauftragten Mitarbeiter zusammen mit Kollegen anderer Bereiche in einem Großraumbüro untergebracht.



Bei den von den Anbietern verwendeten Rechenzentren ist der physische Schutz der Server, auf denen die Vorratsdaten gespeichert werden, durchweg gewährleistet. Der Zugang zu den Rechenzentren ist nur mit Schlüsseln bzw. Zugangskarten möglich, die nach einem entsprechenden Berechtigungskonzept ausgegeben oder frei geschaltet werden. Das Berechtigungskonzept ist zudem in den meisten Fällen so differenziert, dass ein Zugang nur zu einzelnen Bereichen des Rechenzentrums möglich ist. Neben den Zugangsbeschränkungen existiert außerdem überall ein das komplette Rechenzentrum abdeckendes Videoüberwachungssystem.

Die Protokollierung der Zugriffe auf die Datenbanken (sowohl auf Anwender- als auch auf Administratorebene) ist bei den Anbietern unterschiedlich umgesetzt. Selten ist sie bereits detailliert und fälschungssicher implementiert, in der Regel erfolgt nur eine partielle Protokollierung oder sie ist gar nicht vorgesehen. Die Anbieter begründen den Verzicht auf die Protokollierung damit, dass noch verbindliche Regelungen fehlen, wie sie für die neue Fassung der TKÜV und der Technischen Richtlinie zur TKÜV angekündigt wurden.

Zusammenfassend kann festgestellt werden, dass bei der Umsetzung der Vorratsdatenspeicherung in technisch-organisatorischer Hinsicht grundsätzlich ein positiver Ansatz erkennbar ist. Gleichzeitig darf nicht verschwiegen werden, dass eine flächendeckende Einhaltung von Mindeststandards bei allen Unternehmen bislang noch nicht realisiert ist. Das Vorliegen eines solchen ist allerdings zwingend zu fordern, da es sich bei den Vorratsdaten um sensible Informationen handelt, die ein hohes technisch-organisatorisches Schutzniveau unumgänglich machen. Insofern möchte ich an dieser Stelle noch einmal explizit auf die Forderungen in meiner Stellungnahme vom 10.06.2009 verweisen, in der ich neben der strikten physischen Trennung betrieblich genutzter Daten von den Vorratsdaten sowie deren verschlüsselter Speicherung vor allem auch eine umfassende und revisionssichere Protokollierung gefordert habe.

### *3. Kritische Punkte / Auffälligkeiten*

Nach meinem Eindruck ist den Anbietern offensichtlich nicht immer klar, welche Daten zu speichern sind. Der Gesetzeswortlaut des § 113a TKG ist an einigen Stellen zu unklar gehalten oder wird aufgrund der faktischen technischen Voraussetzungen von den Anbietern nicht einheitlich umgesetzt. Im Zweifelsfall werden mehr Daten gespeichert als es der Gesetzeswortlaut vorsieht.



So fordert § 113a Absatz 4 Nr. 2 TKG die Speicherung der Kennung des Anschlusses, über die der Internetzugang erfolgt. In der Praxis ist vielen Anbietern diese Kennung gar nicht bekannt. Ein Internetzugangsanbieter, der auf einen von einem Netzbetreiber gemieteten IP-Adressenblock zurückgreift, hat grundsätzlich keinerlei Kenntnis über die Kennung des Anschlusses seines Kunden. Er teilt ihm lediglich eine Benutzerkennung und ein Passwort zu. Diese Zugangsdaten werden bei der Verbindungsherstellung vom Netzanbieter abgeglichen und nach Bestätigung wird eine IP-Adresse für den Internetzugang zugeteilt. Eine Mitteilung der Kennung des Anschlusses des Nutzers seitens des Netzbetreibers erfolgt hierbei allerdings nicht. Der Internetzugangsanbieter könnte somit nur die Benutzerkennung speichern, was er in der Regel auch tut. Für diese besteht allerdings nach dem Wortlaut des § 113a Absatz 4 TKG keine Speicherverpflichtung. An dieser Stelle werden somit überobligatorisch Daten gespeichert.

Vergleichbare Unsicherheiten im Hinblick auf den Umfang der Speicherverpflichtung existieren auch beim Roaming im Mobilfunk und bei der Speicherung von internen IP-Adressen an öffentlich zugänglichen W-LAN-Hotspots.

Darüber hinaus habe ich festgestellt, dass selbst in Bereichen, in denen das Gesetz eindeutig ist, Daten über das vorgeschriebene Maß hinaus gespeichert werden. Hierbei handelt es sich beispielsweise um technische Informationen über genutzte Leitungen oder Vermittlungsstellen, die zwar – z.B. für eine potentielle Störungsbeseitigung – für den Anbieter eine essentielle Information darstellen können. Eine Befugnis oder Verpflichtung zu deren Nutzung im Rahmen der Vorratsdatenspeicherung vermag ich aber nicht zu erkennen.

Neben diesen rein technikorientierten Informationen werden von Anbietern auch Daten mit unmittelbarem Personenbezug außerhalb der gesetzlichen Verpflichtung vorgehalten. So wird bei der Internetnutzung regelmäßig auch das jeweils anfallende Datenvolumen gespeichert, woraus sich Rückschlüsse auf das Nutzungsverhalten ziehen lassen.

Ein extremer Fall der über den gesetzlich vorgegebenen Rahmen hinausgehenden Speicherung zeigt sich bei der mobilen Internetnutzung. Hier scheint es den Mobilfunkanbietern nicht bewusst zu sein, dass sich die Speichervorgaben für Anbieter von Internetzugangsdiensten – unabhängig ob sie kabelgebunden oder mobil angeboten werden – nach § 113a Absatz 4 TKG richtet. Zusätzlich zur (zulässigen Speicherung) der IP-Adresse und des Zeitstempels werden hier unzulässigerweise noch Daten nach § 113a Absatz 2 Nr. 4



TKG gespeichert, wie beispielsweise die Rufnummer, IMSI oder IMEI. Besonders kritisch erscheint mir die Speicherung der Funkzelle, da dies zur Folge haben kann, dass bei einer ausgedehnten mobilen Internetnutzung viele Datensätze mit Geodaten erzeugt werden. Dies geschieht vor allem bei vielen der zunehmend verwendeten Smartphones, die mit einer Datenflatrate genutzt werden und aufgrund von verschiedenen internetbasierten Diensten (wie beispielsweise E-Mail) immer online sind. Teilweise wird – anders als im stationären Internetzugangsbereich – beim mobilen Internetzugang nicht einmal eine Zwangstrennung der Verbindung nach 24 Stunden vorgenommen. Folglich kann es passieren, dass ein Mobiltelefon eine Internetverbindung auf längere Dauer aufrechterhält und die dabei entstehenden Standortdaten lückenlos erfasst werden. Da es äußerst schwierig ist, einen entsprechenden Datensatz in der Vorratsdatenspeicherung abzubilden, ist ein Anbieter dazu übergegangen, alle 15-30 Minuten eine Art Zwischendatensatz zu speichern, der jeweils auch die aktuelle Funkzelle beinhaltet, in der sich der Nutzer zu dieser Zeit aufgehalten hatte. Im Ergebnis ist es somit möglich, anhand der Vorratsdaten die Bewegungen eines Nutzers im letzten halben Jahr präzise nachzuverfolgen.

Des Weiteren habe ich bei einem Anbieter festgestellt, dass bei der E-Mailspeicherung entgegen § 113a Absatz 3 Nr. 2 TKG bei den empfangenen E-Mails eines Nutzers nicht nur der Absender und Empfänger der Nachricht, sondern zusätzlich auch alle weiteren E-Mail-Adressen der Nutzer gespeichert werden, die neben dem Empfänger die Nachricht in Kopie („cc“) erhalten haben. Die Speicherung von diesen „cc-Empfängern“ ist aber gemäß § 113a Absatz 3 Nr. 1 TKG nur bei den E-Mails zulässig, die der Nutzer von seinem Account aus abschickt. Als Begründung für diese „Zuvielspeicherung“ führt der Anbieter an, er habe (noch) kein spezielles System für die Vorratsdatenspeicherung von E-Mails implementiert und greife lediglich auf die ohnehin vorliegenden E-Mail-Logdaten zurück, in denen mehr Daten gespeichert werden als in § 113a Absatz 3 TKG vorgesehen. Dieses Vorgehen wird damit begründet, dass bisher noch kein Bedarfsträger bei dem betreffenden Unternehmen E-Mail-Daten abgefragt hat. Aus diesem Grund will dieser Anbieter zunächst die Entscheidung des BVerfG über die Rechtmäßigkeit der Vorratsdatenspeicherung abwarten, bevor er weitere kostenintensive Investitionen durchführt, die sich gegebenenfalls als überflüssig herausstellen könnten und nicht ersetzt würden.

Der Umstand, dass die Bedarfsträger bisher nur in sehr wenigen Fällen die Herausgabe von E-Mail-Daten verlangt haben, wird bei fast allen Anbietern offensichtlich. Bei einigen Unternehmen war bis zu meiner Prüfung vor Ort nicht eine einzige entsprechende Anfrage eingegangen. Der Großteil der Anfragen bezieht sich auf die Zuordnung von IP-Adressen.



SEITE 6 VON 6

Den Anfragen liegen dabei häufig Delikte zu Grunde, die keine Katalogstraftaten i.S.d. § 100a StPO sind. Dies bestätigt meine bereits im Rahmen meiner Stellungnahme vom 22.10.2008 geäußerte Befürchtung, dass vorliegend über den Umweg der Vorratsdatenspeicherung Informationen beschafft werden, die ansonsten mangels anderweitiger Speicherung gar nicht oder nur für eine kurze Zeit zugänglich sind. Der Grundsatz, dass die auf Vorrat gespeicherten Daten nur für die Aufklärung von schweren Delikten verwendet werden sollen, wird hierdurch klar unterlaufen.

Ferner habe ich bei mehreren Anbietern festgestellt, dass die auf Vorrat gespeicherten Daten nicht innerhalb der gesetzlich vorgeschriebenen Frist effektiv und endgültig gelöscht werden. Diese Fristüberschreitung bezieht sich zwar nicht auf die für die Beauskunftung an Sicherheitsbehörden vorgehaltenen Dateien, sondern auf für Zwecke der Datensicherung angelegte Backupdateien. Ich halte die zu lange Speicherung jedoch für bedenklich, da die Originaldatenbestände problemlos aus den Backupdateien wiederhergestellt werden können.

Ebenso musste ich feststellen, dass die Auskunftsschreiben an die Bedarfsträger, inklusive der darin enthaltenen Verkehrsdaten, teilweise bis zu einem Jahr archiviert werden. Bei einem Unternehmen war sogar beabsichtigt, die Auskünfte als Handelsbriefe über 10 Jahre zu archivieren. Hier zeigt sich, dass es bislang an einer Regelung, wie mit den Auskunftsschreiben zu verfahren ist, fehlt.

Als problematisch erscheint auch die Abfragepraxis mancher Bedarfsträger. So haben mir sämtliche Anbieter mitgeteilt, dass es recht häufig vorkomme, dass Beschlüsse nicht den formellen Anforderungen an die Nennung der Rechtsgrundlagen (insbesondere der einschlägigen Katalogstraftat) genügen. Wenn die Anbieter in derartigen Fällen entsprechenden Auskunftersuchen nicht nachkämen, würde ihnen oft die Beschlagnahme von Servern oder die Vernehmung der leitenden Angestellten als Zeugen angedroht, um auf diesem Wege eine Auskunft zu erzwingen.

Mit freundlichen Grüßen

Schaar