Deutscher Bundestag
Enquete-Kommission
Internet und digitale Gesellschaft

Ausschussdrucksache
17(24)033

17(24)033

TOP 1c am 4.7.2011

PG Datenschutz

Ergänzender Vorschlag der Fraktion der SPD und der Sachverständigen Alvar Freude, Lothar Schröder und Dr. Wolfgang Schulz für das Kapitel 3. Handlungsempfehlungen zum Thema Vorratsdatenspeicherung:

Der grundrechtliche Schutz informationeller Selbstbestimmung wurde durch die Rechtsprechung des Bundesverfassungsgerichts in jüngerer Zeit schärfer konturiert, nicht zuletzt durch die Entscheidung zur Vorratsdatenspeicherung. Das Bundesverfassungsgericht hat am 02. März 2010[1] entschieden, dass die Vorratsdatenspeicherung in Deutschland in ihrer bisherigen Umsetzung verfassungswidrig sei, da das Gesetz zur anlasslosen Speicherung umfangreicher Daten sämtlicher Nutzer elektronischer Kommunikationsdienste keine konkreten Maßnahmen zur Datensicherheit vorsehe und hat zudem die Hürden für den Abruf dieser Daten als zu niedrig bewertet. Das Urteil verpflichtete deutsche Telekommunikationsanbieter zur sofortigen Löschung der bis dahin gesammelten Daten. Das Bundesverfassungsgericht hat jedoch auch festgestellt, dass die Vorratsdatenspeicherung unter schärferen Sicherheits- und Transparenzvorkehrungen sowie begrenzten Abrufmöglichkeiten für die Sicherheitsbehörden grundsätzlich zulässig sei.

Die Enquete-Kommission empfiehlt dem Deutschen Bundestag,

- eine grundsätzliche und offene Debatte über die Notwendigkeit und auch die Grenzen der Vorratsdatenspeicherung zu führen. Dabei ist auch zu klären, ob und wie eine Speicherung auf Vorrat grundrechtsschonend und verfassungskonform ausgestaltet werden könnte. Die Enquete-Kommission geht dabei davon aus, dass es eine Zustimmung des Deutschen Bundestages für die Vorratsdatenspeicherung nur geben kann, wenn es zu einer grundsätzlichen Überarbeitung der damaligen Vorgaben zur Umsetzung der der Vorratsdatenspeicherung und auch eine Überarbeitung der europäischen Rechtsgrundlage kommt.

- auch mögliche Alternativen zu einer anlasslosen Vorratsdatenspeicherung zu überprüfen.

- zu klären, ob bezüglich der Dauer einer Speicherung und des Datenumfangs eine Rückkehr zu der bis ca. 2006 geltenden Situation möglich ist: Internet-Access-Provider haben damals IP-Adressen ca. 80 Tage gespeichert, E-Mail-Verbindungsdaten hingegen nur wenige Tage zu technischen Analysezwecken,

- dass, sofern eine Datenspeicherung auf Vorrat erfolgen soll, die Art der zu speichernden Daten als auch die Speicherdauer nicht einzelnen Unternehmen überlassen werden darf, sondern gesetzlicher Regelungen bedürfen.

Die Enquete-Kommission fordert deshalb den Deutschen Bundestag auf:

1. die Bundesregierung aufzufordern, auf europäischer Ebene darauf hinzuwirken, dass die Richtlinie 2006/24/EG über die Vorratsspeicherung grundlegend überarbeitet und eine Verkürzung der Speicherfrist von deutlich unter 6 Monaten aufgenommen wird. Dabei sollten

[1] BVerfG, Urteil vom 2. März 2010 - 1 BvR 256/08 zur Vorratsdatenspeicherung.

insbesondere für sensible Daten wie beispielsweise Telefon-Verbindungsdaten, Mobilfunk-Ortsdaten und E-Mail-Verbindungsdaten maximal eine auf wenige Tage beschränkte Speicherdauer und hohe Zugriffshürden gelten. Bei den weniger sensiblen aber in der Praxis wichtigeren IP-Adressen sind längere Speicherfristen denkbar.

2. dass, sollte an der Vorratsdatenspeicherung festgehalten werden, verfassungskonforme gesetzliche Regelungen notwendig sind, die eine Speicherung von Daten und den Zugriff auf diese durch den Staat regelt und mit dem Urteil des Bundesverfassungsgerichts vereinbar ist.

   Bei der konkreten Fassung der Regelungen sollten folgende Anforderungen mit aufgenommen werden:
   a. Der Abruf und die Nutzung der Verbindungsdaten darf nur bei Verdacht auf schwerste Straftaten erfolgen. Das sind insbesondere Straftaten gegen das Leben, die körperliche Unversehrtheit und die sexuelle Selbstbestimmung.
   b. Als milderes und weniger eingriffsintensives Mittel kann eine Beauskunftung von IP-Adressen geregelt werden. Dabei sollte ein Abruf innerhalb einer kurzen Frist von wenigen Tagen ab Speicherung zudem zum Zwecke der Verfolgung von Straftaten erfolgen können. Nach Ablauf dieser Frist darf der Datenabruf bis zur Löschung der Daten nur noch zur Verfolgung schwerster Straftaten erfolgen.
   c. Für Berufsgeheimnisträger soll ein absolutes Verwertungsverbot gelten.
   d. Der Abruf aller Verbindungsdaten soll unter Richtervorbehalt stehen.
   e. Es ist eine Unterrichtungspflicht für die von einem Datenabruf Betroffenen aufzunehmen. Dies gebietet das Rechtsstaatsverständnis und entspricht im Übrigen den verfassungsrechtlichen Vorgaben.
   f. Die Bestimmungen zum technischen Datenschutz müssen entsprechend den verfassungsgerichtlichen Vorgaben deutlich ausgebaut werden. Dazu gehören namentlich eine getrennte Speicherung, die sichere Verschlüsselung von Daten, das Vier-Augen-Prinzip verbunden mit fortschrittlichen Verfahren zur Authentifizierung für den Zugang zu den Schlüsseln und eine revisionssichere Protokollierung von Zugriff und Löschung.
   g. Eine effektive Kontrolle muss gewährleistet werden, Verstöße müssen wirksam sanktioniert werden.
   h. Eine Nutzung der Daten darf ausschließlich für strafrechtliche, nicht für zivilrechtliche Auskünfte erfolgen.

Eine unterschiedliche Behandlung von IP-Adressen und anderen sensiblen Daten ist bereits im genannten Urteil des Bundesverfassungsgerichts zur Vorratsdatenspeicherung angelegt, ergibt sich aber auch aus der Eingriffstiefe und Sensibilität der Daten. Mit Telefon- und E-Mail-Verbindungsdaten lassen sich umfangreiche Nutzungs- sowie Kommunikationsprofile und mit Mobilfunkdaten zusätzliche Bewegungsprofile erstellen. Die mit dem Grimme Online Award ausgezeichnete[2] Visualisierung von Zeit Online der aufgrund der ehemaligen gesetzlichen Vorgaben gespeicherten Vorratsdaten von Malte Spitz zeigt eindrucksvoll, was eine allgegenwärtige Beobachtung bedeutet.[3]

[2] zur Begründung der Jury siehe http://www.grimme-institut.de/html/index.php?id=1345 (abgerufen am 30. Juni 2011)
[3] vgl. http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten und http://blog.zeit.de/open-data/2011/02/24/vorratsdaten-unter-der-lupe/ (abgerufen am 30. Juni 2011)

Eine viel geringere Eingriffstiefe hat jedoch die Speicherung der Zuordnung von IP-Adressen zu Anschlussinhabern bei Internetverbindungen. Anders als vielfach behauptet ist damit keine komplette Überwachung des Surfverhaltens der Nutzer möglich. Im Gegensatz zur Durchführung einer gezielten Telekommunikationsüberwachung kann damit nicht festgestellt werden, welche Webseiten ein Internetnutzer aufgerufen hat. Es ist ausschließlich möglich, im Nachhinein nach einer konkreten Straftat bei Kenntnis der IP-Adresse den Anschlussinhaber herauszufinden. Die Sorge einer Totalüberwachung der Bevölkerung ist daher im Gegensatz zur Speicherung von Handy- und E-Mail-Daten unbegründet.

Bei mit Hilfe des Internets begangenen Straftaten ist die IP-Adresse oftmals die einzige verwertbare Spur. Daher ist der Wunsch der Ermittlungsbehörden nachvollziehbar, dieses Ermittlungsinstrument nutzen zu können. Dennoch sollten die Transparenzpflichten erhöht und die Speicherfristen auf ein Maß verkürzt werden, das auch vor der Vorratsdatenspeicherung jahrelang üblich war.

Eine große Angst in der Bevölkerung ist, dass die Speicherung von IP-Adressen weiter zu Massenabmahnungen bei der Nutzung von P2P-Tauschbörsen führt. Allerdings sind diese Abmahnungen auch ohne Speicherung der IP-Adressen durch Echtzeitabfragen oder entsprechende Speicheranforderungen („Quick Freeze“) möglich.

Da mit der skizzierten Regelung sowohl den berechtigten Interessen der Strafverfolgung als auch der Privatsphäre der Bürger Rechnung getragen wird als auch eine grundrechtsschonende Lösung vorliegt, empfiehlt die Enquête-Kommission dem Deutschen Bundestag auf europäischer Ebene eine entsprechende Initiative zu empfehlen und in Deutschland auf den Weg zu bringen.