ISPA - Positionspapier

Vorratsdatenspeicherung

September 2005

Die ISPA, der Verband der österreichischen Internet Service Provider, bezieht zu den Plänen zur verpflichtenden generellen Vorratsspeicherung von Telekommunikationsdaten, die bei der Kommunikation im Internet anfallen (Data Retention) für einen Zeitraum von bis zu 48 Monaten, die derzeit im Rahmen der Europäischen Union diskutiert werden, folgende Position:

Die ISPA lehnt die zur Zeit vorliegenden Entwürfe des Rates und der Kommission zur Data Retention aus folgenden Gründen ab:

- Es konnte bis zum heutigen Tag nicht belegt werden, dass mit der Data Retention die angestrebten Ziele der Verhinderung bzw. Aufklärung von Terror überhaupt erreicht werden können.
- Der marginale Sicherheitsgewinn durch eine generelle Speicherpflicht, insbesondere in der vorgesehenen Dauer von bis zu 48 Monaten, würde in keinem Verhältnis zu den massiven Eingriffen in das Grundrecht auf Privat- und Familienleben, in das Fernmeldegeheimnis und das Grundrecht auf Datenschutz stehen.
- Die zur Speicherung vorgesehenen Datenarten haben für ISPs keinerlei wirtschaftlichen Wert und müssten unter hohem zusätzlichen finanziellen Aufwand zum ausschließlichen Zweck der Strafverfolgung gespeichert werden.

Zu den angesprochenen Punkten im Einzelnen:

1. Effizienz und Verhältnismäßigkeit

Im Gefolge der Terroranschläge März 2004 in Madrid und Juli 2005 in London wird vor allem von der derzeitigen britischen Ratspräsidentschaft die europaweite Speicherung von Telekommunikationsdaten auf Vorrat forciert. Die Data Retention wird von ihr als probates Mittel zur Verhinderung von Terror bzw. für die Aufklärung von terroristischen Akten dargestellt.

Bis zum heutigen Tag liegen keinerlei Studien oder eindeutige Belege über die Wirksamkeit der Vorratsdatenspeicherung vor. Vielmehr legen vorhandene Statistiken nahe, dass von den Ermittlungsbehörden in der Regel ohnehin meistens nur Stammdaten für Ermittlungszwecke benötigt werden.

Es ist keineswegs sicher, dass den Fahndern signifikant mehr Terroristen durch die Data Retention ins Netz gehen würden, da diesen eine ganze Reihe von Möglichkeiten zur Verfügung stehen, Kommunikationsvorgänge zu verschleiern (anonyme Accounts, Pre-Paid-Handies, öffentliche Internet-Terminals, ausweichen

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at
UID-Nr.: ATU 543 97 807 • IBAN=AT95 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

auf Provider außerhalb der EU etc). Betroffen von der Data Retention wären also in erster Linie gänzlich Unbeteiligte oder Straftäter, die nur eine geringe kriminelle Energie aufbringen. Darüber hinaus ist aufgrund der enormen Menge von Daten, die bei der Vorratsdatenspeicherung anfallen, ein effizientes Durchsuchen des Datenvorrats kaum möglich, sodass riesige „Datenfriedhöfe“ ohne signifikanten ermittlungstechnischen Wert entstünden.

Es muss auch darauf hingewiesen werden, dass derzeit in keinem europäischen Land eine verpflichtende umfassende Vorratsdatenspeicherung praktiziert wird: Entweder ist eine solche gesetzlich nicht vorgesehen oder eine gesetzliche Regelung existiert zwar, wird aber mangels entsprechender Durchführungsbestimmungen nicht angewendet. Selbst UK, der glühendste Verfechter der Data Retention, konnte innerstaatlich aufgrund von massivem Widerstand nur eine freiwillige Speicherung derjenigen Daten, die ohnehin beim Betreiber bzw. Provider vorhanden sind, einführen. Ein dringender Harmonisierungsbedarf, mit dem die Notwendigkeit einer europaweiten Data Retention begründet wird, besteht demnach nicht.

Nicht einmal in den USA, wo als Folge der Anschläge vom 11. September 2001 Bürgerrechte zum Teil empfindlich eingeschränkt wurden, gibt es eine gesetzliche Grundlage für eine Vorratsdatenspeicherung. Der US-Kongress hat entsprechende Gesetzesvorhaben mehrfach mit der Begründung abgelehnt, dass eine Vorratsdatenspeicherung zu weit in die Grundrechte eingreife. Statt dessen ist in den USA eine anlassbezogene Datenspeicherung (Data Preservation, data freeze) vorgesehen, die einen weitaus geringeren Eingriff in die Grundrechte der Bürger darstellt. Auch die Cybercrime Convention des Europarates sieht keine Data Retention, sondern Data Preservation vor.

Data Retention stellt einen unverhältnismäßigen Eingriff in fundamentale Freiheitsrechte, namentlich in das Recht auf Privat- und Familienleben (Art 8 EMRK), das Fernmeldegeheimnis (Art 10a StGG) sowie das Grundrecht auf Datenschutz (§ 1 DSG 2000), dar. Insbesondere der datenschutzrechtliche Grundsatz der Zweckbindung ist durch eine nicht anlassbezogene Datenspeicherung verletzt. Die Aufweichung des Fernmeldegeheimnisses könnte dazu führen, dass Kunden das Vertrauen in Telekommunikationsdienste verlieren und dadurch eine nachhaltige Beeinträchtigung der Entwicklung der Informationsgesellschaft zu befürchten ist, was ganz offensichtlich den Zielsetzungen der EU widerspricht.

2. Zu speichernde Datenarten

Sowohl der Entwurf eines Rahmenbeschlusses des Rats zur Vorratsdatenspeicherung als auch der Richtlinienentwurf der Kommission sind im Bezug auf die zu speichernden Datenarten nicht ausreichend klar formuliert, um genau zu wissen, welche Details von Internet-Kommunikation aufgezeichnet werden müssten. Jedenfalls erwähnen die Entwürfe auch E-Mail, was angesichts der Tatsache, dass der weltweite E-Mail-Verkehr zum überwiegenden Teil aus SPAM (oft mit gefälschten E-Mail-Adressen) besteht, eine höchst zweifelhafte und kaum zielführende Maßnahme wäre. Darüber hinaus ist die Speicherung von Datenarten vorgesehen, die nicht den Verkehrsdaten (also Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at
UID-Nr.: ATU 543 97 807 • IBAN=AT95 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

Fakturierung dieses Vorgangs verarbeitet werden), sondern den Inhaltsdaten (also dem Inhalt der Kommunikation an sich) zuzuordnen sind. Eine Erhebung und Speicherung solcher Daten ohne konkreten Tatverdacht verletzt jedenfalls das Recht auf Privat- und Familienleben (Art 8 MRK), wie auch der Europäische Gerichtshof für Menschenrechte (EGMR; Fall Malone ua.) mehrfach festgestellt hat.

Darüber hinaus sollen Betreiber bzw. ISPs zur Speicherung von Daten verpflichtet werden, welche sie für ihre eigene Tätigkeit gar nicht benötigen. Das heißt, dass sie ihre Systemtechnik und Abläufe unter immensem finanziellen Aufwand umstellen müssten, um Daten zu generieren, die ausschließlich der Strafverfolgung dienen.

Überhaupt stellt die Data Retention eine vollständige Umkehrung des derzeitigen telekommunikationsrechtlichen Datenschutzregimes dar: In Österreich ist nach der geltenden, auf Art 5 und 6 der Datenschutzrichtlinie für die elektronische Kommunikation beruhenden Rechtslage die Speicherung von Inhaltsdaten nur zulässig, soweit dies zur Erbringung der Dienstes technisch notwendig ist. Die Speicherung von Verkehrsdaten darf nur erfolgen, soweit dies zu Abrechnungszwecken erforderlich ist. Andernfalls sind die Daten umgehend zu löschen oder zu anonymisieren.

3. Dauer der Speicherung

In der Praxis werden von Strafverfolgungsbehörden 85% der Daten innerhalb von 3 Monaten und 95% der Daten innerhalb von 6 Monaten nach ihrer Entstehung angefordert. Vor diesem Hintergrund sind darüber hinaus gehende Speicherdauern von bis zu 48 (!) Monaten unverhältnismäßig und daher abzulehnen.

4. Zugriff auf die gespeicherten Daten, Missbrauchspotential

Auch wenn die Notwendigkeit der Vorratsdatenspeicherung meist mit der Bekämpfung des Terrorismus begründet wird, sehen die Entwürfe des Rates und der Kommission keine Beschränkung des Datenzugriffs auf die Aufklärung terroristischer Akte oder allenfalls besonders schwerer Delikte im Allgemeinen vor. Vielmehr ist der Zugriff grundsätzlich für die Verfolgung jedweder strafbarer Handlung (inklusive Privatanklagedelikte) vorgesehen.

Nach den vorliegenden Entwürfen bleibt es den Mitgliedsstaaten überlassen, welche Behörde auf die Daten zugreifen darf. Nicht vorgesehen ist daher, dass ein Richter über die Zulässigkeit eines Zugriffs auf die gespeicherten Daten entscheiden muss. Dies widerspricht klar dem Richtervorbehalt, den Art 10a StGG für Eingriffe in das Fernmeldegeheimnis vorsieht.

Auch gemessen an den vorgeblichen Zielen der Data Retention ist eine derartig breite Zugriffskompetenz unverhältnismäßig und aus datenschutzrechtlicher wie grundrechtlicher Sicht massiven Einschränkungen zu unterwerfen.

Die Speicherung von Daten wirft immer auch die Frage der Datensicherheit auf. Die Speicherung einer derart großen Menge zum Teil höchst sensibler Daten im Rahmen der Data Retention birgt ein immenses Missbrauchspotential und widerspricht dem datenschutzrechtlichen Grundsatz der Datenvermeidung.

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at
UID-Nr.: ATU 543 97 807 • IBAN=AT95 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

5. Kosten

Wie schon dargestellt, müssten von den Betreibern bzw. ISPs Datenarten generiert werden, die weder aus Unternehmens- noch aus Kundensicht von Interesse sind und ausschließlich der Strafverfolgung dienen. Diese ist eine staatliche Aufgabe. Es ist daher nicht einzusehen, dass die Unternehmen die gänzlich unverhältnismäßigen Kosten der Anpassung der Systemtechnik und der Abläufe, der Zurverfügungstellung von Speicherplatz sowie die laufenden Kosten tragen müssen und gegenüber ausländischen Unternehmen, die der Speicherpflicht nicht unterliegen, einen Wettbewerbsnachteil erleiden.

Die Kosten einer Vorratsdatenspeicherung müssten den Betreibern bzw. ISPs daher zur Gänze ersetzt werden.

Aus volkswirtschaftlicher Sicht muss jedenfalls klar festgehalten werden, dass es am Ende immer der Bürger ist, der – ohne allerdings dafür einen signifikanten Sicherheitsgewinn zu genießen - die Kosten der Data Retention tragen muss: entweder über höhere Kosten von Telekommunikationsleistungen oder über die vom Staat eingehobenen Steuern.

6. Zusammenfassung

Die Vorratsdatenspeicherung in der vorgesehenen Form ist gemessen an ihren vorgeblichen Zielen weder zweck- noch verhältnismäßig. Viel geeigneter und aus grundrechtlicher Sicht weniger bedenklich wäre eine anlassbezogene Datenspeicherung (Data Preservation), wie sie etwa in den USA vorgesehen ist.

Im Rahmen der Entwürfe des Rates und der Kommission zur Data Retention ist weder der Umfang noch die Dauer der Speicherung befriedigend geregelt, sodass technische, datenschutz- und verfassungsrechtliche Bedenken dagegen bestehen. Aus Sicht der ISPA sollten, falls – trotz der geäußerten Bedenken – die Vorratsdatenspeicherung eingeführt werden sollte, ausschließlich Zugangsdaten (das sind diejenigen Verkehrsdaten, die beim Zugang eines Nutzers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind) für einen Zeitraum von maximal drei Monaten gespeichert werden müssen.

Die vorgesehene Kostenersatzregelung greift nicht weit genug. Den Betreibern bzw. ISPs müssten sämtliche Investitions- und laufenden Kosten ersetzt werden, da sie mit der Vorhaltung von Daten einen Beitrag zur Strafverfolgung, also einer ausschließlich staatlichen Aufgabe, leisten.

Die vorliegenden Entwürfe des Rates und der Kommission sind nach Meinung der ISPA sowohl aus rechtlicher als auch aus ökonomischer Sicht nicht zu rechtfertigen. Daher fordert die ISPA die österreichische Bundesregierung auf, eine Verabschiedung der vorgeschlagenen Rechtsakte mit allen zu Gebote stehenden Mitteln zu verhindern.

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at
UID-Nr.: ATU 543 97 807 • IBAN=AT95 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

Die ISPA spricht sich weiters klar dafür aus, dass eine Regelung zur Vorratsdatenspeicherung nur in Rahmen der „ersten Säule“ der EU diskutiert werden soll, da es sich um eine Materie handelt, die den Datenschutz und somit den Binnenmarkt betrifft (Art 95 des EG-Vertrages). Derartige Maßnahmen erfordern gemäß Art 251 des EG-Vertrages eine breite demokratische Legitimation, die nur im Rahmen des Mitbestimmungsverfahrens unter Mitwirkung des Europäischen Parlaments erzielt werden kann.

Aufgrund der massiven Eingriffe in Grundrechte und der zu befürchtenden Auswirkungen auf die Entwicklung der Informationsgesellschaft durch eine mögliche Data Retention sollte eine breite Diskussion unter Einbeziehung aller Betroffenen über Notwendigkeit und Umfang der Vorratsdatenspeicherung stattfinden, anstatt „Anlassgesetzgebung“ zu betreiben, die nicht nur die bürgerlichen Freiheiten bedroht, sondern auch die Entwicklung des europäischen Binnenmarktes beeinträchtigt.

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at
UID-Nr.: ATU 543 97 807 • IBAN=AT95 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977