Hintergrundpapier

zur Diskussion um ein neues Gesetz zur Vorratsdatenspeicherung

Berlin, 19.05.2015

I. Begriff

Unter dem Begriff Vorratsdatenspeicherung versteht man die gesetzlich angeordnete Pflicht für Telekommunikations-Dienstbetreiber, die Verbindungsdaten (oder Metadaten, im TKG heißen sie „Verkehrsdaten“) ihrer Nutzer für einen bestimmten Zeitraum zu speichern, damit Strafverfolgungsbehörden gegebenenfalls darauf zugreifen können. Dabei wird das gesamte Kommunikationsverhalten der Nutzer (in Bezug auf Telefon und Textnachrichten) aufgezeichnet, um gegebenenfalls im Nachhinein im Zuge von Ermittlungen darauf zugreifen zu können. Diese Datenspeicherung geschieht also anlasslos und ohne Verdacht auf eine Straftat.

II. Stand des Gesetzgebungsvorhabens

Basierend auf einer entsprechenden EU-Richtlinie aus dem Jahr 2006, hatte die Bundesregierung Ende des Jahres 2007 ein Gesetz verabschiedet, dass die Speicherung von Telekommunikationsdaten der Nutzer regelte. Mit Urteil vom 2. März 2010 hat das Bundesverfassungsgericht dieses Gesetz für verfassungswidrig erklärt.

Aufgrund des Bestands der EU-Richtlinie forderten u.a. die Strafverfolgungsbehörden in der Folge stetig eine sich an den vom Verfassungsgericht aufgestellten Maßstäben orientierende Umsetzung der Vorratsdatenspeicherung. Eine Einigung über eine gesetzliche Regelung scheiterte damals jedoch am Widerstand der damaligen FDP-Justizministerin Leutheusser-Schnarrenberger.

Nach der Bundestagswahl im September 2013 einigte sich die nunmehr aus SPD und CDU/CSU bestehende Regierungskoalition im Koalitionsvertrag auf eine Neuregelung der Datenspeicherung. Eine zeitnahe Umsetzung wurde allerdings wiederum durch den Justizminister – mittlerweile Heiko Maas (SPD) – verhindert, der die anstehende Entscheidung des EuGH über die zugrundeliegende Richtlinie abwarten wollte.

Am 8. April 2014 erklärte der Europäische Gerichtshof die EU-Richtlinie zur Vorratsdatenspeicherung für ungültig, da sie mit der Charta der Grundrechte der Europäischen Union unvereinbar sei.

In der Folge ließ die EU-Kommission verlauten, dass eine Initiative für eine neue europäische Richtlinie derzeit nicht geplant sei.

Am 15. April hat Bundesjustizminister Heiko Maas die mit Innenminister Thomas de Maizère abgestimmten Leitlinien für eine nationale gesetzliche Regelung vorgestellt. Ein entsprechender Referentenentwurf wurde am 18. Mai zur Kenntnisnahme an die betroffenen Verbände verschickt; er soll voraussichtlich am 27. Mai ins Kabinett eingebracht werden.

III. Rechtliche und technisch-organisatorische Vorgaben nach den Urteilen von EuGH und BVerfG

Es ist fraglich, ob nach den Urteilen von BVerfG und EuGH eine Regelung zur anlasslosen und verdachtsunabhängigen Vorratsdatenspeicherung von Verbindungsdaten technisch und rechtlich noch möglich ist. Jedoch hat das BVerfG eine Regelung ausdrücklich nicht von Vorneherein mit der Verfassung für unvereinbar gehalten.

Ausdrückliche Vorgaben des BVerfG und des EuGH

- In jedem Fall notwendig sind rechtliche Vorgaben zur Datensicherheit zum Schutz vor Datenmissbrauch (getrennte Speicherung, asymmetrische Verschlüsselung, Vier-Augen-Prinzip verbunden mit fortschrittlichen Verfahren zur Authentifizierung für den Zugang zu den Schlüsseln, revisionssichere Protokollierung von Zugriff und Löschung).
- Zudem müssen Form und Zeit von Speicherdauer und Löschungsverpflichtungen vorgegeben werden. Die Vorratsdaten müssen auf europäischem Gebiet gespeichert werden, sodass eine Kontrolle durch eine unabhängige Stelle gewährleistet werden kann.
- Es müssen zwingend Ausnahmen für Berufsgeheimnisträger (Seelsorger, Ärzte, Anwälte, Journalisten usw.) beachtet werden. Wie dies bei den Providern technisch-organisatorisch, wirtschaftlich und datenschutzkonform umgesetzt werden soll, ist aber fraglich.

IV. Inhalt des Referentenentwurfs

- Im TKG soll eine Speicherpflicht für alle TK-Anbieter zur Speicherung von Verkehrsdaten eingeführt werden. Die Speicherdauer beträgt grundsätzlich 10 Wochen, für Standortdaten jedoch nur vier Wochen, nach Ablauf der Fristen sind die Unternehmen unverzüglich, spätestens jedoch binnen

einer Woche nach Ablauf der Frist, zur Löschung der Daten verpflichtet. Gespeichert werden die im TKG bezeichneten Verkehrsdaten, die bei der Telekommunikation anfallen (also insbesondere die Rufnummern der beteiligten Anschlüsse, Zeitpunkt und Dauer des Anrufs, bei Mobilfunk auch die Standortdaten, sowie IP-Adressen einschließlich Zeitpunkt und Dauer der Vergabe einer IP-Adresse).

- Die Unternehmen müssen „nach dem Stand der Technik höchstmöglichste Sicherheit der Daten“ gewährleisten. Die Daten dürfen nur in Deutschland gespeichert werden. Eine Regelung, die die Sicherheit der Daten bei Abruf durch die jeweiligen Behörden regelt, gibt es hingegen nicht.

- Eine Entschädigung für die Umsetzung der Vorratsdatenspeicherung wird grundsätzlich nicht gewährt. Ausnahmsweise kann „soweit dies zur Abwendung oder zum Ausgleich unbilliger Härte geboten erscheint“ für die Umsetzung der Speicherpflicht eine Erstattung gezahlt werden. Für den Abruf der Daten im Einzelfall ist eine Entschädigungsregelung geplant.

- Der Zugriff der Sicherheitsbehörden auf die Daten soll nur bei schwersten Straftaten im Rahmen eines abschließenden Straftatenkatalogs sowie bei tatsächlichen Anhaltspunkten für bestimmte konkrete schwerste Gefahren unter Beachtung eines Richtervorbehalts möglich sein. Betroffene sollen über den Abruf grundsätzlich informiert werden. Außerdem ist die Speicherung von Verkehrsdaten in Bezug auf zeugnisverweigerungsberechtigte Personen (gemäß §53 StPO) nicht zulässig; Zufallsfunde werden einem Verwertungsverbot unterstellt.

- Der Abruf von Verkehrsdaten gemäß §96 TKG soll weiterhin bei Straftaten von auch im Einzelfall erheblicher Bedeutung und Straftaten, die mittels Telekommunikation begangen wurden, möglich sein. Diese Maßnahme kann bei Gefahr im Verzug auch von der Staatsanwaltschaft angeordnet werden.

V. Bewertung/Probleme

Der Gesetzentwurf lässt viele technische und rechtliche Probleme offen, beziehungswiese wirft neue auf:

1. verfassungsrechtliche Probleme

Die Verfassungsmäßigkeit des Gesetzes ist weiterhin problematisch.
Fraglich ist immer noch, ob das Vorhaben **gegen Grundrechte verstößt**.
Die beteiligten Ministerien haben zwar in einigen Punkten den in den Urteilen von BVerfG und EuGH aufgestellten Maßstäben Rechnung getragen, es sind

etwa kürzere Speicherfristen geplant (s.o.). Jedoch müssten durch den in der Zwischenzeit vollzogenen technologischen Wandel de facto viel mehr Verkehrsdaten gespeichert werden, um die Informationen, die abrufbar sein sollen, zu generieren (s.u. IP-Adressen). Das könnte sogar einen noch intensiveren Eingriff in das Post- und Fernmeldegeheimnis (Art. 10 GG) und die informationelle Selbstbestimmung (Art. 2 I i.V. m. 1I GG) bedeuten. Außerdem bleibt es bei dem Grundproblem der **anlasslosen**, also vorsorglichen, verdachtsunabhängigen Speicherung, die alle Nutzer von Telekommunikation unter Generalverdacht stellt.

Ein weiterer, verfassungsrechtlich problematischer Punkt ist der **Schutz von Berufsgeheimnisträgern**.
Der EuGH hat in seinem Urteil klargestellt, dass die Verkehrsdaten dieser Personen nicht gespeichert werden dürfen.
Es gibt aber kein Verzeichnis von Berufsgeheimnisträgern, es dürfte im Einzelfall nicht einmal sicher sein, welche Personen unter diese Bezeichnung fallen (z.B.: wer ist eigentlich Journalist und wer nicht?).
Selbst wenn aber abschließend geklärt wäre, welche Personen hierunter zu fassen sind, wäre die Anlage einer Datenbank mit diesen Personen, die dann von der Speicherung ausgenommen werden könnten, technisch nicht möglich. Denn auch wenn ein Telekommunikationsanbieter tatsächlich wissen sollte, dass einer seiner Kunden bspw. Rechtsanwalt ist und bei ihm eingehende Anrufe deshalb nicht speichert, würden diese Anrufe trotzdem durch andere Anbieter aufgezeichnet, die die Daten ihrer Kunden (und damit der Anrufer) speichern.
Trotzdem soll die Speicherung der Daten von Berufsgeheimnisträgern unzulässig sein. Dennoch erlangte Erkenntnisse sollen nicht verwendet werden dürfen, werden also einem Verwertungsverbot unterstellt. Dieses Verwertungsverbot dürfte in der Praxis die Regel werden. Hier stellt sich die Frage, ob diese Konstruktion den verfassungsrechtlichen Anforderungen der Obergerichte entspricht.

Verfassungsmäßigkeit soll ferner auch durch **Transparenz** hervorgerufen werden; der Referentenentwurf sieht eine Benachrichtigungspflicht des Betroffenen vor Abruf seiner Daten vor. Eine heimliche Verwendung soll nach gerichtlicher Prüfung nur ausnahmsweise zulässig sein, dann soll es aber einer Benachrichtigung bedürfen, von der wiederum aber mit richterlicher Bestätigung abgesehen werden kann.
Faktisch wird eine Benachrichtigung aber nur im Ausnahmefall erfolgen. In der Praxis wird der Richter eine heimliche Verwendung (mit Recht) immer dann für erforderlich halten, wenn durch die Benachrichtigung des Betroffenen die polizeilichen Ermittlungen gefährdet würden. Das dürfte – gerade in Fällen, in

denen sonst keine Ermittlungsansätze vorhanden sind – so gut wie immer der Fall sei, da der Verdächtige sonst über den Kenntnisstand der Strafverfolger informiert würde. Ein Fall, in dem die vorherige Benachrichtigung des Betroffenen keine Gefährdung darstellt, ist nur dann vorstellbar, wenn der Betroffene ohnehin schon von Maßnahmen gegen sich weiß und andere Beweise schon vorliegen. Dann aber bedürfte es zu einer effektiven Strafverfolgung nicht der Vorratsdatenspeicherung.

Nach dem Entwurf unklar bleibt, ob nach Beendigung der Maßnahme eine Benachrichtigungspflicht der anderen Beteiligten (dem jeweiligen B-Ende der Kommunikation) gegenüber entsteht.

2. Aufwand, Kosten und möglicher Vertrauensverlust in der Bevölkerung stehen in keinem Verhältnis zum **Nutzen**.

a) Aufwand/Kosten
Durch die geplante Differenzierung der Speicherdauer (Speicherung der Standortdaten für vier Wochen, übrige Daten zehn Wochen) wird bei den verpflichteten Unternehmen ein noch größerer Aufwand entstehen als nach der ersten Regelung 2008. Es wird die Anschaffung komplett neuer Infrastruktur zur Speicherung notwendig sein; außerdem ist absehbar, dass die technische Sicherung enorm aufwendig ausfallen wird, da sie sich an den Vorgaben der Obergerichte orientieren muss (wie etwa getrennte Speicherung, asymmetrische Verschlüsselung etc., s.o.). Erschwerend kommt hinzu, dass wirtschaftliche Erwägungen in diesem Zusammenhang keine Rolle spielen dürfen.

Das bedeutet eine erhebliche Kostenlast für die betroffenen Unternehmen, eine Entschädigung ist nach dem Entwurf aber nur dann vorgesehen, „soweit dies zur Abwendung oder zum Ausgleich unbilliger Härte geboten erscheint“. Das soll nach der Begründung dann der Fall sein, wenn die Anbieter darlegen können, dass die Auswirkungen der Speicherpflicht für ihr Unternehmen erdrosselnde Wirkung haben könnten. Lediglich für die Kosten, die durch den Abruf der Daten entstehen, soll eine Entschädigungsregelung vorgesehen werden.
Anbieter elektronischer Kommunikation sehen sich ohnehin immer weitergehenden und umfassenden regulatorischen Verpflichtungen, etwa in der IT-Sicherheit, ausgesetzt und sind zusätzlich angehalten, durch eigene Investitionen die Grundlagen für die zukünftige digitale Infrastruktur zu sichern. Alle weiteren Verpflichtungen werden sich negativ auf die Investitionsmöglichkeiten der betroffenen Unternehmen auswirken. Es ist für diese Unternehmen natürlich weiterhin selbstverständlich, dass sie im Rahmen der gesetzlichen

Vorgaben an der Aufklärung von Straftaten mitwirken, der Gesetzgeber sollte jedoch den Rahmen des wirtschaftlich Zumutbaren nicht überschreiten.

Besonders für kleine oder mittlere Betriebe dürfte die Auferlegung der Kosten der Vorratsdatenspeicherung eine enorme Belastung darstellen. Der Nachweis einer „erdrosselnden" Wirkung wird aber im Einzelnen nur sehr schwer und mit großem Aufwand zu führen sein. Dies umso mehr, als auch nach der Begründung des Gesetzentwurfs nicht klar wird, wann eine solche Wirkung angenommen werden kann.
Das scheint unverhältnismäßig, wenn man bedenkt, dass die Vorratsdatenspeicherung ausschließlich für staatliche Zwecke, namentlich die Strafverfolgung, eingeführt werden soll. Die Strafverfolgung ist eine originär staatliche Aufgabe. Die Kosten hierfür sollen aber vollständig auf die Unternehmen abgewälzt werden.

Bezüglich der finanziellen Belastungen stellt sich außerdem die Frage, wie verlässlich neue Investitionen durch die Unternehmen getätigt werden können. Nach Verabschiedung des §113a TKG a.F. haben deutsche Telekommunikationsanbieter mehrstellige Millionenbeträge für die Umsetzung der gesetzlichen Anforderungen aufgewendet. Nur zwei Jahre später wurde das Gesetz für verfassungswidrig erklärt, die Kosten für die Anbieter stellten sich als sinnlos heraus.
Bei Verabschiedung eines neuen Gesetzes ist sicher, dass dieses wiederum vor das Bundesverfassungsgericht (eventuell auch vor den EuGH) gebracht werden wird. Erst dann wird sich herausstellen, ob es Bestand hat. Also wird sich auch erst dann erweisen, ob erneute finanzielle Aufwendungen seitens der Anbieter überhaupt notwendig sind. Bei dieser klaren Ausgangslage ist es kaum zu rechtfertigen, die Anbieter zu verpflichten, große Summen vor einer gerichtlichen Klärung zu investieren.

b) Drohender Vertrauensverlust

Vertrauen in das Internet ist Grundlage für dessen gesellschaftlichen und wirtschaftlichen Erfolg: Bei der stets notwendigen und stets schwierigen Abwägung zwischen Freiheit und öffentlicher Sicherheit muss die neue Bedeutung des Internet und der elektronischen Kommunikation für demokratische Entfaltung und Teilhabe des Bürgers nicht nur stärker berücksichtigt, sondern in den Mittelpunkt der Erwägungen gestellt werden, damit sich die Prinzipien unserer freiheitlich demokratischen Grundordnung angesichts des Bedeutungswandels elektronischer Kommunikation nicht auflösen. Smartphones und mobiles Internet sind heute allgegenwärtig. Die neuen Geräte kommunizieren ständig mit einer immer größer werdenden Anzahl an Funkzellen, die detaillierte Be-

wegungsprofile ermöglichen. Es muss daher insbesondere bedacht werden, dass sowohl das BVerfG als auch der EUGH in ihren Urteilen zur Rechtmäßigkeit der Vorratsdatenspeicherung zum gleichen Schluss kamen: Die anlasslose und verdachtsunabhängige Speicherung der Verkehrsdaten im Rahmen elektronischer Kommunikation erzeugt beim Bürger das ständige und diffuse Gefühl des Überwachtseins. Zudem mahnte das BVerfG bereits im Jahre 2010, dass der Gesetzgeber, angesichts zunehmender, anlassloser Datensammlungen (z.B. bei Bank- und Fluggastdaten, aktuell die PNR-Debatte) eine (Überwachungs-)-Gesamtschau vornehmen müsse, um die Auswirkungen auf die Freiheitsausübung des Bürgers und seinen eigenen Spielraum beurteilen zu können. Gerade die Enthüllungen um die Abhörpraktiken von Geheimdiensten zeigen deutlich, dass das Vertrauen in die Nutzung elektronischer Kommunikation eine entscheidende Rolle für die Art und Weise seiner Nutzung darstellt und die Grundvorrausetzung für die zivilgesellschaftlichen sowie wirtschaftlichen Errungenschaften, die in den letzten Jahren mit dem Internet verbunden wurden, darstellt. Wenn der Gesetzgeber diese Grundlagen erhalten möchte, muss er dies bei seiner Bewertung dringend berücksichtigen.

Nach den Enthüllungen des amerikanischen Whistleblowers Edward Snowden hat das Vertrauen der Bevölkerung in die abstrakte Sicherheit von Daten bereits merklich gelitten. Einer Umfrage aus dem Mai 2014 zufolge[1] misstrauten 71% der Befragten den staatlichen Stellen im Umgang mit persönlichen Daten. Im Jahr 2011 waren es nur 40%. Dazu kommt aktuell noch die sogenannte BND-Affäre, die für die Steigerung des Vertrauens in den Staat in datenschutzrechtlichen Fragen ebenfalls nicht förderlich sein dürfte.
Zudem werden derzeit im Rahmen der Reform des Verfassungsschutzgesetzes ohnehin Regelungen diskutiert, die eine massive Ausweitung der Überwachungsmöglichkeiten auch im Inland zur Folge haben dürften.
Deshalb sollte es vorderstes Ziel der Bundesregierung sein, zu versuchen, das verlorene Vertrauen zurückzugewinnen. Mit einem übereilten Gesetz zur hochumstrittenen Vorratsdatenspeicherung dürfte sie aber das Gegenteil erreichen.

c) Nutzen

Der Nutzen der geplanten Regelung wird gering ausfallen. Zwar ist nachvollziehbar, dass sich die Strafverfolgungsbehörden angesichts der wachsenden Bedeutung des Internet und der damit einhergehenden Entwicklung neuer, netzspezifischer Deliktstypen wirksame Instrumente wünschen, die bei der Aufklärung helfen und ihnen das Gefühl geben, den technischen Anschluss nicht zu verlieren.

[1] Quelle: BITKOM

Jedoch ist das Mittel der Vorratsdatenspeicherung als wirksame und effiziente Strafverfolgungsmaßnahme nicht geeignet, positive Effekte konnten bislang nicht nachgewiesen werden.

Zum einen ist in dem Referentenentwurf vorgesehen, einen Zugriff der Behörden auf die gespeicherten Daten nach §113 b nur dann zu erlauben, wenn der Verdacht einer schweren Straftat besteht und diese auch im Einzelfall schwer wiegt. Katalogmäßig aufgezählt sind hier Delikte wie etwa Hochverrat, Landesfriedensbruch, Mord, Totschlag oder Menschenhandel. Bei diesen Taten handelt es sich aber gerade nicht um solche, bei denen die Auswertung von Verbindungsdaten typischerweise den einzig möglichen Ermittlungsansatz darstellt. Vielmehr dürften diese Daten oft nur ein Indiz unter mehreren sein.

Aber auch bei mittels des Internet oder mit Telekommunikation begangener Straftaten ist es ein Trugschluss, zu glauben, diese seien ohne ein Gesetz zur Vorratsdatenspeicherung nicht aufklärbar. Vielmehr fehlt es in der Praxis oft nur an rechtzeitigen Anfragen der Strafverfolgungsbehörden. Telekommunikationsanbieter speichern bereits jetzt viele Verbindungsdaten sieben Tage, die meisten Daten könnten also auch heute schon abgerufen werden. Dass dies nicht erfolgt, liegt vor allem an der technischen und personellen Ausstattung der betroffenen Behörden.
Des Weiteren sind auch bei Straftaten über das Internet vielmals weitere Ermittlungsansätze vorhanden: Bei einem Betrug etwa muss das Opfer das Geld irgendwohin überweisen, beim sog. Enkeltrick begegnen sich Täter und Opfer (wie auch bei einem „normalen“ Diebstahl oder Raub).

Zum anderen ist das Mittel der Vorratsdatenspeicherung **nicht mehr zeitgemäß**.
Die Datenspeicherung soll nach dem Entwurf alle Dienste betreffen, die im Telekommunikationsgesetz geregelt sind. **Andere Dienste** – die unter das Telemediengesetz fallen – sind demnach **nicht betroffen**. Auch würden die Regelungen nur für deutsche Unternehmen gelten, da natürlich nur diese unter das deutsche TKG fallen.
Das heißt: Die Verbindungsdaten von Gesprächen über „klassische“ Telekommunikationsdienste werden gespeichert, die Daten der Nutzung anderer Dienste, etwa über Skype, hingegen nicht. Oder: Die Verbindungsdaten einer SMS werden gespeichert, die einer WhatsApp-Nachricht nicht. Das ist insofern bemerkenswert, als internetbasierte, alternative Chat-Dienste immer beliebter werden: Verschickten die Deutschen im Jahr 2012 noch fast 60 Milliarden SMS, waren es im Jahr 2014 nur noch 22,5 Milliarden. Es ist auch zu erwarten, dass diese Entwicklung ebenso rasant weitergehen wird, wenn man bedenkt, dass Dienste über das Internet häufig kostenfrei (bzw. in der Inter-

netflat eines Smartphones enthalten) sind. Unklar ist weiter, wie die Bundesregierung auf die technischen Neuerungen der letzten Jahre sowie auf kommende Entwicklungen reagieren wird.
Die Vorratsdatenspeicherung ist eine Idee des Jahres 2006.

d) Ausmaß der Datenspeicherung
Die Dimension der Datenspeicherung wäre heute durch die veränderten technischen Gegebenheiten auch eine ganz andere als noch vor knapp zehn Jahren.
Dies liegt vor allem an der **Zuordnung von IP-Adressen**: Konnten diese zu Zeiten des ersten Gesetzes zur Vorratsdatenspeicherung noch einem einzigen Anschluss zugeordnet werden, werden sie mittlerweile mehrfach und nur temporär vergeben. Grund hierfür ist eine wachsende IPv4-Adressen-Knappheit, da es immer mehr Anschlüsse gibt. Das führt dazu, dass die IP-Adresse alleine nicht mehr ausreicht, um einen bestimmten Anschluss zu identifizieren, hierzu werden vielmehr weitere Daten benötigt. Dazu müsste durch die Anbieter zunächst eine neue, riesige Datenbank aufgebaut werden. Neben der IP-Adresse gespeichert werden müsste der sogenannte Port, der den genutzten Dienst feststellt; darüber hinaus müsste der Provider etwa die exakten Nutzungszeiten aufzeichnen. Damit besteht die Gefahr, dass das gesamte Nutzerverhalten gespeichert werden muss, um den gesetzlichen Vorgaben entsprechen zu können; also eine lückenlose Aufzeichnung des Verhaltens aller Nutzer im Netz entsteht. Dies stellt einen weitaus tieferen Eingriff in die Grundrechte der User dar, als es bei der alten Regelung der Fall war. Denn so kann – auch bei kürzeren Speicherfristen – ein vollständiges Nutzerprofil des Einzelnen erstellt werden.

Die Wirkung der Vorratsdatenspeicherung wird überschätzt. Ihre Effektivität ist nicht belegt. Eine einseitige Speicherung der vom TKG umfassten Dienste ist aus den oben beschriebenen Gründen nutzlos, eine flächendeckende Speicherung aller Dienste, inklusive derer des TMG, dürfte aber nur wenig effektiver sein. Insbesondere werden sich Personen, die wirklich schwerwiegende Verbrechen beabsichtigen, Wege suchen, die Speicherung zu umgehen.
Wird die Vorratsdatenspeicherung aber wie geplant eingeführt, besteht die Gefahr, dass sie als Einfallstor für die Speicherung auch aller weiteren Dienste verwendet wird. Dann entsteht aber die Situation, dass das Nutzungsverhalten aller User flächendeckend anlasslos gespeichert wird, eine vollständige Überwachung ist dann zumindest technisch Realität. Dieses Szenario geht aber noch viel weiter als die vom Bundesverfassungsgericht bereits für verfassungswidrig erklärte Norm des §113a TKG a.F. und steht in keinem Verhältnis zu einem möglichen Nutzen für die Bevölkerung.

Zusammenfassung eco Position:

Eine vorsorgliche, verdachtsunabhängige Speicherung auf Vorrat im Zeitalter allgegenwärtiger elektronischer Kommunikation ist weder zeit- noch verfassungsgemäß. Die mit der Speicherung verbundenen Eingriffe in die Grundrechte der Bürger und Unternehmen stehen in keinem Verhältnis zum behaupteten, aber nicht belegten Effektivitätsgewinn bei der Strafverfolgung und dem einhergehenden Vertrauensverlust in die Nutzung des Internet.