

Bundesministerium der Justiz
Referat R B 3 / K. Schwerin, S. Bockemühl
Mohrenstraße 37

D-10117 Berlin

Berlin, 19.01.2007
Unser Zeichen: BMJ_070119

Stellungnahme zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG („Vorratsdatenspeicherung“, Stand: 27. November 2006).

Über den BVDW:

Der BVDW vertritt als größte Interessenvertretung der deutschen Internet- und Multimediabranche die Interessen von ca. 1.500 Unternehmen aus dem Netzwerk der Digitalen Wirtschaft, davon rund 900 Direktmitgliedern im BVDW und fungiert als Bindeglied zwischen der Branche und den staatlichen Organen auf nationaler und internationaler Ebene.

Inhalt	Seite
Zusammenfassung	2
Einzelne Kritikpunkte	2
1. Grundsätzliches	2
2. rechtliche Aspekte	3
a) im Hinblick auf Deutsches Recht	3
b) im Hinblick auf Europäisches Recht	5
3. Definition und Speicherung der Daten	6
4. Dauer der Datenspeicherung	6
5. betroffener Personenkreis	7
6. Kosten und Umsetzung	7
7. Zugriff	8

Zusammenfassung

Der BVDW ist mit einer Reihe der vorgesehenen Regelungen im Referentenentwurf nicht einverstanden und äußert zudem grundsätzliche Bedenken gegen eine gesetzliche Normierung der Speicherung von Verbindungs- und Standortdaten. Dies begründet sich einerseits mit Zweifeln an der – schon formellen - Rechtmäßigkeit der EU-Richtlinie zur Vorratsdatenspeicherung, andererseits mit der wohl drohenden Unvereinbarkeit der angestrebten nationalen Regelungen mit bedeutenden verfassungsrechtlich garantierten Bürgerrechten.

Der vorgelegte Entwurf stellt unweigerlich alle Bürger unter einen – verfassungsrechtlich höchst bedenklichen – Generalverdacht, was einer Abkehr von der bisherigen Unschuldsvermutung gleich kommt.

Aus Sicht des BVDW wäre daher zunächst eine größere Differenzierung bei den zu speichernden Datentypen zwischen verschiedenen Datentypen nach ihrer datenschutzrechtlichen Sensibilität wünschenswert, um sicherzustellen, dass die unterschiedlich schweren Eingriffe in die Grundrechte der Betroffenen auch jeweils noch im Verhältnis zu dem mit der Datenspeicherung und –nutzung verfolgten Zweck stehen.

Ferner steht zu befürchten, dass aus den Daten der Vorratsspeicherung detaillierte Nutzerprofile der Betroffenen rekonstruiert werden können.

Der BVDW ist darüber hinaus der Auffassung, dass Geheimnisträger (Seelsorger, Anwälte oder Journalisten, Ärzte etc.) grundsätzlich von einer Überwachung ausgenommen werden müssen.

Der BVDW regt daher an, die aktuelle deutsche EU-Ratspräsidentschaft dazu zu nutzen, die umstrittene EU-Richtlinie zur Vorratsdatenspeicherung neu auf den Verhandlungstisch zu bringen und solange mit einer nationalen Umsetzung der in der aktuellen Richtlinie vorgesehenen Regelungen zu warten.

Einzelne Kritikpunkte

Der BVDW sieht insbesondere hinsichtlich der folgenden Punkte deutlichen Nachbesserungsbedarf am Referentenentwurf:

1. Grundsätzliches

Der Referentenentwurf sieht eine verdachtsunabhängige Speicherung von Telefon- und Internetdaten vor. Dies hat zur Folge, dass über die Erfassung weiter Teile des Kommunikations-, Bewegungs- und Internetnutzungsverhaltens der Bevölkerung ein bisher nicht da gewesener Eingriff in verfassungsmäßige Rechte gesetzlich legitimiert werden soll.

Der Entwurf geht mit seiner weitgehenden Erfassung aller Verkehrsdaten sehr weit und stößt deshalb aus Sicht des BVDW auf erhebliche verfassungsrechtliche Bedenken. Es fehlt eine Differenzierung zwischen weniger datenschutzsensiblen Daten (wie z.B. der schlichten Zuweisung dynamischer IP-Adressen zu einem Telefonanschluss im Rahmen des

Internet-Access) und sehr weit in den persönlichen Bereich hineinreichenden Daten wie etwa Informationen über Kommunikationspartner oder Standortdaten.

Es steht zu befürchten, dass aus den Daten der Vorratsspeicherung detaillierte Nutzerprofile der Betroffenen rekonstruiert werden können, was es unbedingt zu verhindern gilt.

Sofern man dennoch – nicht zuletzt aufgrund der Verpflichtung der Bundesrepublik zur Umsetzung der EU-Richtlinie zur Vorratsdatenspeicherung – die Verabschiedung der vorgelegten Regelungen bezweckt, kann dies nur unter sehr engen Voraussetzungen erfolgen.

So muss sicher gestellt sein, dass jeglicher Zugriff auf die gespeicherten Daten nur nach richterlicher Anordnung und unter Abwägung der Rechts- und Strafverfolgungsinteressen gegenüber den Interessen der von der Auskunft Betroffenen erfolgen darf, der Zweck der Datenerhebung klar definiert und der Betroffene umfassend informiert wird, um dadurch sein Rechtsschutzinteresse zu gewährleisten.

Die in dem Referentenentwurf vorgesehenen Regelung, wonach die Strafverfolgungsbehörden auch bei "mittels Telekommunikation begangener Straftaten" in den erhobenen Daten „schürfen“ dürfen, ist grundsätzlich berechtigt, da eine Nichtverwendung von IP-Access-Logfiles zur Verfolgung von Internet-Straftaten das Internet faktisch zum rechtsfreien Raum werden lassen würde. Auch hier muss allerdings stärker nach der Schwere der Tat und dem jeweiligen Grundrechtseingriff differenziert werden, um zu gewährleisten, dass richterlich angeordnete Zugriffe der Strafverfolgungsbehörden nur nach einer ausgewogenen Interessensabwägung zwischen den Grundrechtspositionen der Bürger und den staatlichen Schutzinteressen erfolgen.

2. rechtliche Würdigung

a) im Hinblick auf Deutsches Recht

Der BVDW sieht in dem vorgelegten Referentenentwurf einen Verstoß gegen das in Artikel 10 des Grundgesetzes verankerte Fernmeldegeheimnis sowie gegen das Grundrecht auf informationelle Selbstbestimmung. Damit verletzt der Gesetzgeber grundlegende allgemeine rechtsstaatliche Prinzipien.

Dies stellt eine Abkehr von der bisherigen Unschuldsvermutung dar und führt dazu, dass der Bürger zur Duldung der verdachtsunabhängigen Speicherung seiner Daten und darauf basierenden polizeilichen Maßnahmen verpflichtet wird.

Die Durchführung der Maßnahmen erfolgt zudem zunächst ohne Wissen des Betroffenen. Dass eine nachträgliche Mitteilungsverpflichtung für die

Behörden sowie ein Rechtsmittel gewährt werden, vermag den vorliegenden Eingriff in Grundrechte nicht zu schmälern.

Dabei erscheint dieser immense Eingriff in die Grundrechte der Bundesbürger vordergründig nicht gerechtfertigt. Aus dem Bericht "Mindestspeicherungsfristen für Telekommunikationsverbindungsdaten" des Bundeskriminalamts vom November 2005 geht eindeutig hervor, dass in den vergangenen Jahren 381 Straftaten wegen fehlender Telekommunikationsdaten nicht aufgeklärt werden konnten. Diese Straftaten bewegten sich vor allem in den Bereichen Internetbetrug, Austausch von Kinderpornografie und Diebstahl.

Beachtet man dabei, dass jährlich 6,4 Millionen Straftaten begangen werden, von denen 2,8 Millionen - also knapp 44% - nicht aufgeklärt werden können, so beträgt der Anteil der wegen fehlender Telekommunikationsdaten nicht aufklärbaren Straftaten gerade einmal weniger als 0,001 Prozent des Gesamtaufkommens.

Die tatsächliche Zahl der Straftaten – allen voran Urheberrechtsverletzungen - die im Internet begangen werden und wegen fehlender Telekommunikationsdaten unverfolgt bleiben, mag durchaus höher sein und zudem stetig steigen. Jeden Nutzer von Telefon-, Mobil- und Internetdiensten dafür allerdings unter Generalverdacht zu stellen, erscheint übertrieben.

Der Referentenentwurf verweist in seiner Begründung selbst auf mehrere Entscheidungen des Bundesverfassungsgerichts, nach denen "eine Straftat von erheblicher Bedeutung, ein konkreter Tatverdacht und eine hinreichend sichere Tatsachenbasis" unbedingte Voraussetzung einer Erfassung von Verbindungsdaten des Betroffenen ist.

Der Schutz des Kernbereichs der verfassungsmäßigen Rechte der Bürger darf sich nach Auffassung des BVDW nicht nur allein auf die Wohnung des Betroffenen erstrecken, sondern muss vielmehr auf den gesamten Bereich seiner unmittelbaren Privatsphäre und damit auch auf seine persönliche und intime Kommunikation ausgedehnt werden, um eine unverhältnismäßige Verletzung seiner Grundrechte auszuschließen.

Es ist Telekommunikationsanbietern nach geltendem Recht aktuell nur erlaubt, die zur Abrechnung ihrer Dienste erforderlichen Verbindungsdaten speichern. Die Erhebung und Speicherung von Volumendaten ist nach den Vorschriften des geltenden Telekommunikationsgesetzes unzulässig, da diese zur Abrechnung der Dienste nicht erforderlich sind. Zulässigerweise gespeichert werden dürfen aktuell folglich nur für eine Abrechnung des Dienstes erforderliche Daten, nicht etwa aber Positionsdaten von Mobilfunkgeräten oder Verbindungsdaten von Mobil- und Internetdiensten wie etwa der Email-Kommunikation.

Wie aus einer neueren Entscheidung des Landgerichts Darmstadt hervorgeht, beträgt die Speicherfrist für Daten über Beginn und Ende der Verbindung – zum Zwecke der Rechnungsstellung – aktuell maximal acht Wochen.

Zudem hat das Bundesverfassungsgericht zweifelsfrei festgestellt, dass ein systematisches Ansammeln sensibler Daten eines Betroffenen ohne konkreten (Tat)Verdacht verfassungswidrig ist und sich damit ausdrücklich gegen eine pauschale Überwachung Marke „gläserner Bürger“ ausgesprochen.

Eine Umsetzung der im Referentenentwurf vorgesehenen Regelungen, ohne dass den unterschiedlichen Eingriffstiefen bei den verschiedenen zu speichernden Datentypen Rechnung getragen wird, droht aus Sicht des BVDW nicht nur der Rechtsprechung des Bundesverfassungsgerichts zu widersprechen, sondern würde zudem dazu führen, dass verfassungsrechtliche und durch höchstrichterliche Rechtsprechung festgelegte unabdingbare Grundsätze durch den Gesetzgeber verletzt werden.

b) im Hinblick auf europäisches Recht

Zunächst ist zu begrüßen, dass über die EU-Richtlinie endlich seit langem auf internationaler Ebene beschlossene Regelungen des Cybercrime-Übereinkommens umgesetzt werden sollen – ein Schritt in die richtige Richtung, wenngleich unausgewogen und rechtlich zweifelhaft.

So ist aktuell auf Betreiben Irlands ein Verfahren vor dem EuGH anhängig, welches die (formelle und materielle) Rechtmäßigkeit der Richtlinie überprüfen soll. Denn ursprünglich waren die nunmehr über die EU-Richtlinie in nationales Recht umzusetzenden Regelungen als Entwurf zu einem Rahmenbeschluss vorgelegt worden. Als jedoch deutlich wurde, dass die für eine Verabschiedung erforderliche Einstimmigkeit nicht erreicht werden würde, wurde auf einen Richtlinienentwurf umgeschwenkt, für dessen Annahme schon die qualifizierte Mehrheit im gemeinsamen Entscheidungsverfahren mit dem EU-Parlament ausreichend ist.

Ein Richtlinienentwurf aber dient allein der Angleichung von Rechts- und Verwaltungsvorschriften zur Funktionsverbesserung des europäischen Binnenmarktes, so dass Bedenken an der Rechtmäßigkeit des gewählten Verfahrens mehr als angebracht sind. So ist auch eine Entscheidung des EuGH dahingehend zu erwarten, dass das gewählte Verfahren nicht rechtmäßig und die betroffene Richtlinie damit hinfällig ist.

Daher regt auch der BVDW explizit an, die aktuelle deutsche EU-Ratspräsidentschaft dazu zu nutzen, um die umstrittene EU-Richtlinie zur

Vorratsdatenspeicherung neu auf den Verhandlungstisch zu bringen und solange mit einer nationalen Umsetzung der in der aktuellen Richtlinie vorgesehenen Regelungen zu warten.

3. Definition und Speicherung der Daten

Aus dem Referentenentwurf geht nicht eindeutig hervor, wo die Daten vorgehalten werden müssen, also auf bestehenden oder aber auf neu zu schaffenden, gesonderten Speichersystemen. Die letzte Alternative wäre für die Anbieter mit zusätzlichem Investitionsaufwand verbunden und wird daher abgelehnt. Hier ist eine Klarstellung im Interesse der Wirtschaft dringend erforderlich.

Aufgrund des Umstands, dass dem Diensteanbieter nicht immer alle der im Referentenentwurf definierten Daten bekannt sind, ist ferner eine Klarstellung im Hinblick auf die Formulierung „erzeugte oder verarbeitete Verkehrsdaten“ dahingehend erforderlich, dass die gesetzlich definierten Daten nur dann beim Anbieter zu speichern sind, wenn Sie von diesem auch erhoben werden, dass also eine absolute Speicherpflicht beim Anbieter nicht besteht.

4. Dauer der Datenspeicherung

Im Referentenentwurf ist eine Speicherungsfrist von 6 Monaten vorgesehen, die gespeicherten Daten sind dann binnen eines Monats nach Ablauf der Speicherfrist zu löschen. Dies ist grundsätzlich zu begrüßen, da der Entwurf damit nicht nur den Forderungen des Deutschen Bundestages nachkommt, sondern gleichzeitig auch nur die im Rahmen der EU-Richtlinie vorgegebene Mindestspeicherfrist festschreibt, während die EU-Richtlinie die Speicherung von Verbindungs- und Standortdaten durchaus für einen Zeitraum von bis zu 24 Monaten zulässt.

Dennoch aber gewährt diese – im Hinblick auf die bisher zulässige – verlängerte Speicherfrist einen unverhältnismäßig langen Zugriffszeitraum, der in keinem Verhältnis zu den dadurch verletzten Grundrechten des Betroffenen steht, zumindest jedoch zu undifferenziert ausfällt. Zudem werden zusätzliche Daten gespeichert, ohne dass dies durch das Vorhandensein eines konkreten (Tat)Verdachts begründet wäre.

5. betroffener Personenkreis

Der Gesetzesentwurf sieht eine Geltung der entsprechenden Regelungen für alle Kommunikationsteilnehmer vor und trifft damit keine – durchaus notwendige und wünschenswerte – Auswahl von fahndungsrelevanten Gruppen.

Der BVDW ist der Auffassung, dass Geheimnisträger (Seelsorger, Anwälte oder Journalisten, Ärzte etc.) grundsätzlich von einer Überwachung ausgenommen werden müssen und lehnt insoweit eine lediglich vorgesehene und nochmals in sich differenzierte deutliche Begrenzung der Überwachungsmaßnahmen für bestimmte Personengruppen entschieden ab.

Zwar sieht der Referentenentwurf in seiner vorgelegten Fassung vor, dass das Abhören bestimmter Berufsgruppen dann ausgeschlossen sein soll, wenn diese als Zeugen oder Nachrichtenübermittler betroffen sein könnten. So sollen etwa Seelsorger, Strafverteidiger und Abgeordnete mit einem umfassenden Verwertungsverbot ganz besonders geschützt werden. Für Ärzte, Rechtsanwälte, Journalisten sowie weitere Geheimnisträger hingegen sei eine Überwachung nach "sorgfältiger Entscheidung im Einzelfall" jedoch zulässig.

Diese Differenzierung ist abzulehnen, da zunächst nicht trennscharf festgelegt wird, nach welchen Kriterien eine Entscheidung im Einzelfall vorzunehmen ist. Bis dafür über die Rechtsprechung entsprechende allgemeingültige Kriterien bereitgestellt werden, obliegt es dem jeweils für die Anordnung des Datenzugriffs zuständigen Richter, eine Entscheidung nach eigenem Ermessen zu treffen. Dies führt zwangsläufig zu uneinheitlichen und damit abzulehnenden Individualentscheidungen, zu Rechtsunsicherheit und einer nicht hinnehmbaren Grauzone gerade für die Geheimnisträger, die dadurch in Ihrer Berufsausübung unangemessen scharf beeinträchtigt werden.

6. Kosten und Umsetzung

Durch die Speicherung der Verbindungs- und Standortdaten bei den Unternehmen der Branche wird eine grundsätzlich hoheitliche Aufgabe von enormem Ausmaß auf die Wirtschaft abgewälzt, wodurch den dazu verpflichteten Unternehmen erhebliche zusätzliche Kosten entstehen. Diese fallen insbesondere bei der Bereitstellung von entsprechender Hardware und Infrastruktur an. Zusätzlich aber entstehen durch die Einrichtung entsprechender Datenbanken erhebliche personelle Kosten, die durch die Telekommunikationsunternehmen zunächst vorfinanziert werden müssen.

Im Referentenentwurf ist jedoch eine angemessene Entschädigung der Unternehmen für die anfallenden und laufenden Kosten nicht vorgesehen. Zudem ist äußerst fraglich, ob die für einen späteren Zeitpunkt vorgesehene

Entschädigungsregelung die den Unternehmen entstandenen Kosten vollumfänglich decken wird.

Denn selbst wenn das BMJ die Vorschriften des Justizvergütungs- und -entschädigungsgesetzes (JVEG) auf eine Entschädigungsregelung für die durch die Vorratsspeicherung anfallenden Kosten hin überarbeitet, so ist derzeit nicht absehbar, ob die dann festgeschriebene Regelung die tatsächlich entstandenen Kosten abdecken oder lediglich eine Aufwandsentschädigung darstellen wird, die dem Investitionsaufwand und laufenden Kostenvolumen bei den Unternehmen nicht gerecht wird. Die Vorschriften des JVEG lassen sich darüber hinaus aufgrund ihres Anwendungsbereichs nicht ohne weiteres auf die Kostenerstattung für die Vorratsdatenspeicherung übertragen.

Eine mögliche Entlastung der Unternehmen dadurch, dass die statistischen Erhebungen dann durch die Strafverfolgungsbehörden zu erfolgen hat, wird vom BVDW nicht gesehen, da die Unternehmen dennoch in technische Einrichtungen investieren und (zusätzliches) Personal für die erforderlichen Tätigkeiten bereitstellen müssen.

Dies stellt eine unangemessene Belastung für die Internetwirtschaft dar und wird nach Auffassung des BVDW dazu führen, dass der wirtschaftliche Aufschwung einer sich wieder erholenden Branche unnötig gebremst oder gar gestoppt wird. Zudem ist nicht zu erwarten, dass die zur Speicherung der vorgesehenen Daten erforderliche Technik und Infrastruktur zum im Entwurf avisierten Umsetzungstermin bereit stehen werden.

7. Zugriff

Der BVDW begrüßt die Regelung eines Richtervorbehalts im Referentenentwurf, nach der der Zugriff auf die auf Vorrat gespeicherte Daten nur aufgrund richterlicher Anordnung erfolgen darf.

Auch hier muss allerdings stärker nach der Schwere der Tat und dem jeweiligen Grundrechtseingriff differenziert werden, um zu Gewährleisten, dass richterlich angeordnete Zugriffe der Strafverfolgungsbehörden nur nach einer ausgewogenen Interessensabwägung zwischen den Grundrechtspositionen der Bürger und den staatlichen Schutzinteressen erfolgen. Zudem dürfen die dadurch gewonnenen Erkenntnisse nur zu dem Zweck der Verfolgung – nicht aber auch zur präventiven Bekämpfung bzw. Verhinderung von Straftaten verwandt werden.

Darüber hinaus ist der Betroffene über Zweck, Art und Umfang der hoheitlichen Maßnahmen umfassend zu benachrichtigen, um dessen Rechtsschutzinteresse zu wahren.