



REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR JUSTIZ

BMJ-L884.067/0001-II 3/2010

An das Bundesministerium für Verkehr,
Innovation und Technologie
Abt. III/PT2
Ghegastraße 1
1030 Wien

Email: jd@bmvit.gv.at

Adresse
1070 Wien, Museumstraße 7

e-mail
kzl.L@bmj.gv.at

Telefon Telefax
(01) 52152-0* (01) 52152 2753

Sachbearbeiter(in): Mag. Gertraud Eppich
*Durchwahl: 2157

Betrifft: Entwurf für ein Bundesgesetz, mit dem das
Telekommunikationsgesetz 2003 -TKG 2003
geändert wird.

Bezug: BMVIT 630.33/1-III/PT2/2009

Das Bundesministerium für Justiz beehrt sich, zu dem im Betreff genannten Entwurf wie folgt Stellung zu nehmen:

I. Vorbemerkung

Das Bundesministerium für Justiz anerkennt das Bemühen des Entwurfs, die europarechtlichen Vorgaben unter besonderer Berücksichtigung der betroffenen Grundrechte, hier insbesondere der Grundrechte auf den Schutz persönlicher Daten, auf Achtung des Privat- und Familienlebens (Art 8 EMRK) und des Schutzes des Fernmeldegeheimnisses (Art 10a StGG) umzusetzen. Gerade deshalb muss bedauert werden, dass die zwischen den betroffenen Ressorts geführten Gespräche nicht fortgesetzt bzw. einseitig unterbrochen wurden, sodass keine für die betroffenen Rechtsgebiete (vor allem SPG, StPO und Urheberrechtsgesetz) abgestimmte Lösung vorgestellt und der Begutachtung unterzogen werden kann.

Gleichzeitig hat man sich aber auch dadurch der Chance begeben, jüngste Entwicklungen im Bereich der Europäischen Kommission nachzuvollziehen, die im Wesentlichen davon geprägt sind, dass die bisherigen nationalen Umsetzungsakte nicht nur sehr unterschiedlich ausgefallen sind, sondern auch über das

europarechtlich Geforderte hinausgehen dürften (auf die Ergebnisse der im BMJ mit Vertretern der EK geführte Videokonferenz am 24.11.2009 wird hingewiesen).

Es ist aus Sicht des Bundesministeriums für Justiz unbestritten, dass in diesem grundrechtlich besonders sensiblen Bereich der (verdachtsunabhängigen) Speicherung von Kommunikationsdaten die Wesensgehaltsgarantie der angesprochen Grundrechte auch im Verhältnis zum Gebot der Unschuldsvermutung (Art. 6 Abs. 2 EMRK) eine entsprechend strikte Berücksichtigung des Gebote der Bestimmtheit, der Notwendigkeit (einer solchen Maßnahme in einer demokratischen Gesellschaft) und der Verhältnismäßigkeit erfordern. Der Versuch, einer maßhaltenden, grundrechtsverträglichen Umsetzung der Richtlinie 2006/24/EG über die Vorratsdatenspeicherung wird daher insoweit vorbehaltlos unterstützt.

Auf der anderen Seite darf jedoch die Umsetzung der erwähnten Richtlinie nicht zu einer Einschränkung der bisherigen Ermittlungsmaßnahmen führen. So lässt auch der EGMR keinen Zweifel daran, dass den Strafverfolgungsbehörden zur Prävention und zur Verfolgung von Straftaten moderne dem Stand der Technik angepasste Techniken zur Verfügung stehen müssen (siehe dazu Rz 105 f. des Urteils der Großen Kammer des EGMR vom 4. Dezember 2008 im Fall S. und Marper gegen Vereinigtes Königreich: *„The Court finds it to be beyond dispute that the fight against crime, and in particular against organised crime and terrorism, which is one of the challenges faced by today's European societies, depends to a great extent on the use of modern scientific techniques of investigation and identification....“*). Hier ist aus Sicht des Bundesministeriums für Justiz jedenfalls abzulehnen, dass die Auskunft über Stammdaten gegenüber der bisherigen (aus § 103 Abs. 4 TKG abzuleitenden) Verpflichtung zur Auskunftserteilung nur deshalb eingeschränkt bzw. zum Teil an die Voraussetzungen einer Auskunft über Daten einer Nachrichtenübermittlung im Sinne der §§ 134 Z 2 und 135 Abs. 2 StPO geknüpft werden soll, weil die Umschreibung des Begriffs der Vorratsdaten auch Stammdaten umfasst (siehe einerseits § 90 Abs. 7 und 8 iVm § 92 Abs. 3 Z 3 TKG und andererseits § 99 Abs. 5 iVm § 102a Abs. 2 Z 1, Abs. 3 Z 3 und Abs. 4 Z 2 TKG jeweils in der Fassung des Entwurfs).

II. Zu den einzelnen Bestimmungen

Zu Z 2, 14 und Z 16 des Entwurfs (§ 90 Abs. 7 und § 99 Abs. 1 und 5 Z 1 TKG 2003):

a) Einleitend ist zu bemerken, dass § 92 Abs. 2 TKG 2003 unverändert beibehalten werden soll, wonach die Bestimmungen der StPO von den Bestimmungen des 12. Abschnittes des TKG 2003 unberührt bleiben, ein Vorbehalt also, der etwa im Verhältnis zu § 87b Urheberrechtsgesetz oder den Bestimmungen des Sicherheitspolizeigesetzes nicht besteht. Schon aus diesem Grund (siehe auch die ausdrückliche Anordnung einer Mitwirkungsverpflichtung gemäß § 138 Abs. 2 StPO) lassen sich die Überlegungen des OGH in seinem Urteil vom 14.07.2009, 4 Ob 41/09x nicht unbesehen auf das Verhältnis zwischen TKG 2003 und StPO 1975 übertragen. Mag daher auch grundsätzlich begrüßt werden, dass nunmehr in § 90 Abs. 7 TKG 2003 in der Fassung des Entwurfs eine klare und gegenüber § 103 Abs. 4 TKG 2003 in der geltenden Fassung eindeutige Auskunftspflicht geschaffen wird, so führt doch der Halbsatz „..., soweit dies ohne Verarbeitung von Verkehrsdaten möglich ist“ dazu, dass – anders als nach geltendem Recht – eine Auskunft darüber, wem (d.h. welchem Anschluss) eine (bekannte!) dynamische IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war, nur mehr unter den Voraussetzungen des § 135 Abs. 2 StPO angeordnet werden kann. Das bedeutet, dass diese Auskunft bei Straftaten, die mit einer Freiheitsstrafe bis zu sechs Monaten bedroht sind, nicht mehr angeordnet werden kann. So bliebe den Strafverfolgungsbehörden etwa bei Verdacht eines Betrugs im Wege des Internets („e-bay- Betrug“) bis zu einem Betrag von Euro 2.999.- jeder sinnvoller Ermittlungsansatz verwehrt, womit das Strafrecht in diesem Bereich auch nahezu gänzlich seiner generalpräventiven Wirkung beraubt würde. Gleiches gilt für die Cyber-Crime- Tatbestände der §§ 118a, 119a, 126a Abs. 1, 126b Abs. 1 und 126c StGB, aber auch etwa bei fehlenden Einverständnis des Inhabers im Fall der pornographischen Darstellungen Minderjähriger gemäß § 207a Abs. 3 und 3a StGB.

Es erscheint wenig sinnvoll, hier in das System der abgestuften Strafdrohungen des StGB einzugreifen und den Gesetzgeber zu veranlassen, diese nur deshalb anzuheben, um Ermittlungslücken zu vermeiden.

An diesem Befund ändert auch die Bestimmung des vorgeschlagenen § 99 Abs. 5 Z 1 TKG 2003 wenig, weil die die Verarbeitung von Verkehrsdaten zu Auskunftszwecken nur dann zulässig wäre, wenn diese zur Auskunft über Daten einer Nachrichtenübermittlung (§ 134 StPO) an die zuständigen

Strafverfolgungsbehörden notwendig ist und eine gerichtliche Bewilligung zugrunde liegt (diese Hervorhebung der gerichtlichen Bewilligung ist schon aus der einleitend erwähnten Bestimmung des § 92 Abs. 2 TKG 2003 nicht erforderlich, weil sich diese Voraussetzung aus § 137 Abs. 1 StPO erschließt). Nach dem Wortlaut wird überdies die Verarbeitung erst bei Vorliegen der gerichtlichen Bewilligung zulässig, weshalb grundsätzlich eine Speicherung historischer Verkehrsdaten nicht zulässig wäre, es sei denn, dies wäre aus betrieblichen Gründen oder verrechnungstechnischen Gründen erlaubt. Die Erläuterungen dazu gehen davon aus, dass eine Auskunft über Verkehrsdaten (z.B. dynamische IP- Adresse, oder bestimmte Telefonie- Rufdaten bei Vorauszahlungsmodellen) im sogenannte niederschweligen Straftatenbereich, bei welchem eine Auskunft über Vorratsdaten nach § 102b TKG 2003 in der Fassung des Entwurfs nicht zulässig wäre, solange zulässig wäre, als diese Daten zu betrieblichen Zwecken gespeichert werden. In der Regel werden dynamische IP- Adressen aus diesem Grund jedoch bloß für 96 Stunden gespeichert. Im Regelfall wird diese Frist wohl durch den Zeitablauf zwischen Tatbegehung und Entdeckung der Tat bzw. der ersten Ermittlungsmaßnahmen seitens der Strafverfolgungsbehörden verstrichen und daher ein Auskunftersuchen erfolglos sein.

Aus den bereits zuvor erwähnten Gründen ist eine derartige Einschränkung bestehender Ermittlungsansätze abzulehnen.

b) Nach § 99 Abs. 1 TKG 2003 in der Fassung des Entwurfs sollen Verkehrsdaten außer in den in diesem Gesetz geregelten Fällen weder gespeichert noch verwendet werden dürfen. Nach den Erläuterungen soll dadurch bestehenden Auskunftsverpflichtungen nach anderen gesetzlichen Bestimmungen materiell derogiert werden. Das BMJ spricht sich nachdrücklich gegen diese Änderung aus. Vielmehr sollte der Entwurf bestehende gesetzliche Auskunftsverpflichtungen unberührt lassen und die in den Erläuterungen zitierte Judikatur zum Anlass dafür nehmen, diese Auskunftsverpflichtungen (wie insb. nach § 87b Abs. 3 UrhG und § 18 Abs. 4 ECG) durch die Anordnung abzusichern, dass – jedenfalls – Zugangsdaten auch zur Erfüllung anderer gesetzlicher Auskunftsverpflichtungen wie etwa nach § 87b Abs. 3 UrhG und § 18 Abs. 4 ECG für zumindest drei Monate zu speichern sind. Hier ist grundrechtlich zu betonen, dass sich die genannten Bestimmungen auf den Ausnahmetatbestand des Art. 8 Abs. 2 EMRK stützen, der auf den Schutz der Rechte anderer bezogen ist. Rechtsvergleichend sei in diesem Zusammenhang

erwähnt, dass auch § 96 Abs. 2 des deutschen Telekommunikationsgesetzes es erlaubt, gespeicherte Verkehrsdaten über das Ende der Verbindung hinaus zu verwenden, soweit sie u.a. *„für die durch andere gesetzliche Vorschriften begründeten Zwecke erforderlich sind“*.

Zum Auskunftsanspruch nach § 87b Abs. 2 und 3 UrhG kann die Notwendigkeit der Zulässigkeit der Verarbeitung von hierfür erforderlichen Verkehrs- bzw. Zugangsdaten und eine befristete Verpflichtung zur Speicherung auch aus dem Gemeinschaftsrecht selbst abgeleitet werden:

Art. 8 der Rechtsdurchsetzungs-RL 2004/48/EG enthält nämlich eine eindeutige gemeinschaftsrechtliche Verpflichtung zu einer gesetzlichen Auskunftspflicht. Auch der EuGH hat in seiner Entscheidung C-275/06 („Promusicae“) zum Spannungsverhältnis zwischen der Rechtsdurchsetzungs-RL und der Datenschutz-RL 2002/58/EG ausdrücklich festgehalten, dass die Mitgliedstaaten verpflichtet sind, sich bei der Umsetzung dieser beiden Richtlinien auf eine Auslegung derselben zu stützen, die es ihnen erlaubt, ein angemessenes Gleichgewicht zwischen den verschiedenen durch die Gemeinschaftsrechtsordnung geschützten Grundrechten sicherzustellen. Eine Rechtslage, die den Auskunftsanspruch für einen signifikanten Teil aller Fälle illegalen File-Sharings – nämlich jene, bei denen dynamische IP-Adressen verwendet werden – schlichtweg aushebelt, weil sie keine Verpflichtung zur Speicherung der relevanten Daten vorsieht, würde diesen gemeinschaftsrechtlichen Vorgaben keineswegs entsprechen. Dies kommt auch in der Entscheidung des OGH 4 Ob 41/09x zum Ausdruck, wenn dort angemerkt wird, dass derzeit eine ausdrückliche Regelung über die Speicherung und Verarbeitung von Verkehrsdaten fehlt. Ohne eine solche Auskunftsverpflichtung wäre aber auch dem mit Art. 3 der Richtlinie 2001/29/EG harmonisierten Recht der interaktiven öffentlichen Wiedergabe (das in § 18a UrhG als „Zurverfügungstellungsrecht“ umgesetzt wurde) für einen wichtigen Bereich die praktische Durchsetzbarkeit schlicht genommen. Darüber hinaus würde in Zukunft auch dem in § 18 Abs. 4 ECG geregelten Anspruch dritter Personen auf Auskunft gegen einen Dienstanbieter über Namen und Adressen von Nutzern ihres Dienstes die Grundlage entzogen. Auch hier geht es darum, dass ohne diese Auskunft einer in seinen Rechten verletzten Person die Verfolgung ihrer Rechte nicht möglich wäre. Wenn aber durch die Verwehrung dieser Auskünfte den in ihren Rechten verletzten Personen jegliche praktische

Möglichkeit genommen ist, ihre Rechte durchzusetzen, ist auch ihr Anspruch auf ein faires Verfahren nach Art. 6 MRK in Frage gestellt.

Zu Z 4 des Entwurfs (§ 92 Abs. 3 Z 3 TKG 2003):

Obwohl in § 90 Abs. 6 und 7 auf § 92 Abs. 3 Z 3 lit. a bis e verwiesen wird, werden auf Grund eines offensichtlichen Redaktionsversehens im Entwurf des § 92 Abs. 3 Z 3 lediglich lit. a. bis c angeführt.

Zu Z 11 des Entwurfs (§ 94 Abs. 1 und 2 TKG 2003):

Das Bundesministerium für Justiz muss an dieser Stelle ausdrücklich darauf verweisen, dass in den Budgetansätzen des Ressorts keine Vorsorge für eine Ausweitung des Investitionskostenersatzes für die Einrichtung der erforderlichen Vorkehrungen zur Speicherung von Vorratsdaten getroffen wurde. Abgesehen von der gemeinschaftsrechtlichen Vorgabe, keine unzulässigen Beihilfen vorzusehen (nach Mitteilung der EK hätten derzeit bloß zwei Mitgliedstaaten eine Kostenersatzpflicht hinsichtlich der Investitionen vorgesehen) muss das Bundesministerium für Justiz darauf hinweisen, dass keine Mittel für solche Zwecke zur Verfügung stehen, wobei es sich außerstande sieht, eine nur annähernde Kostenschätzung vorzunehmen. Nähere Anhaltspunkte lässt das Vorblatt vollkommen vermissen.

Zu Z 18 des Entwurfs (§ 102a Abs. 1 und § 102b Z 1 TKG 2003):

Aus gutem Grund überlasst die RL Richtlinie 2006/24/EG über die Vorratsdatenspeicherung die Definition des Begriffs der schweren Straftaten dem nationalen Gesetzgeber, um nicht ohne Grund in das System der Rechtfertigung schwerer Grundrechtseingriffe einzugreifen. Grundsätzlich knüpft der österreichische Gesetzgeber die Zulässigkeit schwerer Grundrechtseingriffe an den Verdacht einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten Straftat. Ein solcher Verdacht rechtfertigt etwa auch die Übergabe einer Person auf Grund eines europäischen Haftbefehls. Auch die Bestimmungen der §§ 134 ff. StPO über die Auskunft über Daten einer Nachrichtenübermittlung sowie Überwachung von Nachrichten gehen von dieser Eingriffsschwelle aus und berücksichtigen damit auch das System der abgestuften und verhältnismäßigen Strafdrohungen des StGB. Diese Regelungen bedürfen aus Sicht des Bundesministeriums für Justiz keiner ausdrücklichen Anpassung an die Regelungen der Vorratsdatenspeicherung, weil eine Auskunft ohnedies nur aufgrund einer konkreten Verdachtslage im Einzelfall auf

Grund einer gerichtlichen Bewilligung anzuordnen ist. Ein Abgehen vom bisherigen Regime in der StPO erscheint schon deshalb fragwürdig, weil kaum einzusehen wäre, dass auf historische Daten einer Kommunikation von Personen im Vergleich zur Überwachung des Inhalts von Nachrichten oder dem Entzug der persönlichen Freiheit nur unter erschwerten Bedingungen zurückgegriffen werden könnte.

Das Bundesministerium für Justiz verschließt sich jedoch nicht einer Diskussion über notwendige Anpassungen in der StPO und anderen in seinen Zuständigkeit fallender Materiengesetze, will nur vorweg jedenfalls sichergestellt wissen, dass gegenüber bestehenden Ermittlungsmöglichkeiten bzw. Möglichkeiten der außerstrafrechtlichen Rechtsdurchsetzung keine Einschränkungen vorgenommen werden.

Eine Ausfertigung dieser Stellungnahme wurde dem Präsidium des Nationalrates im Wege elektronischer Post an die Adresse: begutachtungsverfahren@parlament.gv.at übermittelt.

12. Jänner 2010
Für die Bundesministerin:
Mag. Christian Pilnacek

Elektronisch gefertigt