WIRTSCHAFTSKAMMER ÖSTERREICH

An das
Bundesministerium für Inneres
Bmi-III-1@bmi.gv.at

In Kopie
Begutachtungsverfahren@parlament.gv.at

Abteilung für Rechtspolitik
Wiedner Hauptstraße 63 | Postfach 195
1045 Wien
T +43 (0)5 90 900-DW | F +43 (0)5 90 900-243
E rp@wko.at
W http://wko.at

Ihr Zeichen, Ihre Nachricht vom	Unser Zeichen, Sachbearbeiter	Durchwahl	Datum
BMI-LR1340/0019-III/1/07; 4.9.2007	Rp 1685/07/DrRo/SM	4273	27.9.2007

Entwurf eines Bundesgesetzes, mit dem das Sicherheitspolizeigesetz, das Grenzkontrollgesetz und das Polizeikooperationsgesetz geändert werden; Stellungnahme

Sehr geehrte Damen und Herren!

Die Wirtschaftskammer Österreich teilt zu dem im Betreff genannten Entwurf Folgendes mit:

Allgemeines:

Die Beurteilung, ob der Datenschutz im konkreten Fall eine Schranke darstellt, wird über den Weg der in diversen Materiengesetzen verankerten Auskunftsbestimmungen mittlerweile sehr oft auf Private überwälzt. Dieser Umstand stellt für die betroffenen Auskunftspflichtigen eine nicht unproblematische Situation dar, müssen sie doch selbst entscheiden, ob das Auskunftsbegehren gerechtfertigt ist bzw. die notwendigen, tatbestandsmäßigen Voraussetzungen vorliegen. Trifft dies nicht zu, verstoßen sie bei Datenherausgabe gegen Datenschutzrechte und haben sie unter Umständen mit verwaltungsrechtlichen und/oder zivilrechtlichen Konsequenzen zu rechnen. Diese Entwicklung scheint bedenklich. Verschärft wird diese Situation der Auskunftspflichtigen dadurch, dass es bei bestimmten Fallkonstellationen zu "Überschneidungen" der Anwendungsbereiche diverser Auskunftsansprüche kommen kann (zB Auskunftsanspruch nach SPG oder ECG); derartige Überschneidungsmöglichkeiten sollten durch eindeutige und klare Bestimmungen in den jeweiligen Materiengesetzen möglichst ausgeschlossen werden.

Zu Art 1 Z 3 (§ 53 Abs 3a):

Grundsätzliche Erwägungen:

Grundsätzlich wird darauf hingewiesen, dass bereits die **bestehende Bestimmung in der Vergangenheit zum Teil zu Diskussionen des Fachverbandes Telekom/Rundfunk und der betroffenen Unternehmen mit den Sicherheitsbehörden bzw. betroffenen Bundesministerien** geführt hat, da der Wortlaut Auslegungsfragen aufwirft.

Insbesondere wurde dabei diskutiert, in welchen Fällen tatsächlich diese Bestimmung zur Anwendung kommen kann ("als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben benötigen") bzw. was unter den Bezeichnungen "unverzüglich" und "kostenlos" zu verstehen ist. Es ist schon derzeit im Einzelfall mitunter fraglich, in welchem Fall ein „Telekommunikationsdienst“ im Sinne dieser Bestimmung vorliegt und daher diese Bestimmung zur Anwendung kommt. Insbesondere ist in diesem Zusammenhang fraglich, ob bereits der derzeitige § 53 Abs 3a Internetprovider erfasst (und inwieweit auch dynamische IP-Adressen zu beauskunften wären).

Auch der gegenständliche Entwurf weist eine Reihe von Unklarheiten bzw. gravierenden Änderungen für die betroffenen Unternehmen auf und wird daher in der vorliegenden Form abgelehnt.

Es ist festzuhalten, dass bereits derzeit und auch durch die geplante Änderung des § 53 Abs 3a SPG in gewissen denkbaren Fallkonstellationen die **Möglichkeit der "Umgehung" der Überwachungsmaßnahmen der Telekommunikation nach §§ 149a ff StPO** (mit Inkrafttreten des Strafprozessreformgesetzes: §§ 134 ff StPO-RG), welche unter Richtervorbehalt (Beurteilung der Erforderlichkeit und Verhältnismäßigkeit) stehen, eröffnet werden kann. Aufgrund des direkten Auskunftsrechtes der Sicherheitsbehörden ohne vorherige Einschaltung eines Richters (oder einer sonstigen Institution) kommt es im Verhältnis zu § 149a ff StPO auch zu einem Wertungswiderspruch (einerseits Richtervorbehalt, andererseits keiner).

Anmerkungen im Detail:

1. „Sonstige Kontaktinformationen“:

Es ist unklar, was unter dem Begriff ***"sonstige Kontaktinformation"*** eines bestimmten Anschlusses zu verstehen ist. Der nunmehr auch um die "sonstige Kontaktinformation" erweiterte Auskunftsanspruch könnte wohl auch E-Mail-Adressen, Domains, Netzwerkadressen, statische und dynamische IP-Adressen, individuelle Kennungen bei Selektivrufen im Funkbereich etc. umfassen. Aufgrund dieser weiten Interpretationsmöglichkeit scheint eine genauere Umschreibung in datenschutzrechtlicher Hinsicht notwendig.

(Anmerkung, insbesondere zu dynamischen IP-Adressen: Zwar wären gemäß den Erläuternden Bemerkungen (EB) zu § 92 Abs 3 lit d TKG 2003, wo - neben § 107 Abs 3 Z 1 leg. cit. - die "sonstige Kontaktinformation" als Teil der Stammdaten erwähnt wird, nach dem Willen des Gesetzgebers lediglich "individuelle dauerhafte Rufzeichen oder Kennungen", also lediglich statische, nicht jedoch dynamische IP-Adressen als sonstige Kontaktinformation anzusehen (und zu beauskunften), im Hinblick auf die OGH-Entscheidung vom 26.7.2005, 11 Os 57/05z u.a., ist diese Unterscheidung jedoch durch die Rechtsprechung zweifelhaft geworden (vgl aber DSK, K 213.000/0005-DSK/2006, wo dynamische IP-Adressen als „ausschließlich Verkehrsdaten“ angesehen werden; auch in der Literatur sind zur Richtigkeit der Einordnung von dynamischen IP-Adressen als Stammdaten durchaus kritische Stimmen vorhanden, vgl Schmidbauer, Die Metamorphose der Auskunftspflicht = http://www.internet4jurists.at/news/aktuell92.htm)

Die Möglichkeiten der Netzbetreiber, diese Kontaktinformation zu beauskunften oder anhand anderer Stammdaten zu beauskunften wird einerseits von den technisch-betrieblichen Gegebenheiten beim "Mitliefern" von Informationen bei deren Durchlaufen zweier oder mehrerer beteiligter Netze (lediglich Verbindungsnetzbetreiberfunktion) sowie andererseits von der durch die Verrechnungszwecke gemäß § 99 Abs 2 leg. cit. limitierte Speicherdauer von Verkehrsdaten

abhängen. Verbindungsnetzbetreiber können daher bei mangelndem Datenbestand auch keine Auskunft erteilen und sollte zumindest in den EB klargestellt werden, dass Anforderungen mangels Vorliegen der Daten nicht beantwortet werden müssen.

2. Ausdehnung des Zeitpunktes auf einen Zeitraum:

Die geplante Bestimmung geht insofern über die bestehende Regelung hinaus, als nunmehr nicht mehr von einem Zeitpunkt, sondern einem ***"Zeitraum"*** die Rede ist. Eine Begrenzung dieser Zeitspanne ist im Gesetz nicht vorgesehen. Die Erläuterungen sprechen lediglich von einem angemessenen Zeitraum ("sachgerechte und verhältnismäßige Zeitspanne"). Dieser unbestimmte Gesetzesbegriff scheint nicht unproblematisch.

Im Sinne der dem Datenschutz inhärenten Grundprinzipien, dass allfällige unbedingt erforderliche Eingriffe in das Grundrecht auf Datenschutz möglichst verhältnismäßig und schonend bzw. mit den gelindesten Mitteln verhältnismäßig und so wenig intensiv wie möglich zu erfolgen haben, sollte daher bereits im Gesetzestext ein exakter, allenfalls ein präziser und kurz umrissener Zeitraum festgelegt werden.

3. Bezugnahme auf „eine von diesem Anschluss geführte Kommunikation"

Es ist nicht klar erkennbar, ob mit der Verwendung des Begriffs „Kommunikation" anstelle des bisherigen Begriffs „Gespräch" im 2. Satz des § 53 Abs 3a eine Ausdehnung dieser Bestimmung auf Internetkommunikation bezweckt wird.

4. Ausdehnung der Rufdatenauswertung auf Basis der „aktiven" Teilnehmernummern:

Die Sicherheitsbehörde kann nach dem 2. Satz des § 53 Abs 3a nunmehr die „aktive oder passive" Teilnehmernummer bezeichnen. Dies ist ebenfalls eine Erweiterung der bisherigen Bestimmung, da bislang im Rahmen des SPG lediglich auf Basis der passiven Teilnehmernummer beauskunftet werden musste.

Zunächst muss dazu festgehalten werden, dass die Rufdatenrückerfassungen gemäß § 149a Abs 1 Z 1 lit b StPO ausdrücklich unter Richtervorbehalt steht. Die Regelung des § 53 Abs 3a SPG steht im eindeutigen Wertungswiderspruch zu den bereits gesetzlich geregelten Fällen der §§ 149a ff StPO. Dieser Wertungswiderspruch wird dadurch weiter problematisch, als Konstellationen denkbar sind, bei denen es bezüglich des Anwendungsbereiches der StPO und des SPG zu "Überschneidungen" kommen kann.

Rufdatenrückerfassungen unterliegen nach der StPO strengen Formvorgaben (Gerichtsbeschluss gemäß § 149b Abs 2 StPO), die neben der Gewährleistung der Entscheidung durch den Richter über die Erforderlichkeit und Verhältnismäßigkeit, auch zur Sicherstellung der Nachvollziehbarkeit einer Anforderung dienen.

Durch eine nicht klar definierte Anforderung durch die Sicherheitsbehörde gemäß § 53 Abs 3a SPG (in der geplanten Fassung) würden daher jene in der StPO vorgesehenen Kontrollmechanismen, die eine Überprüfung ermöglichen, im "Überschneidungsbereich" von StPO und SPG außer Kraft gesetzt werden können.

Die Vorlage eines entsprechenden richterlichen Beschlusses (bzw. sonstiger adäquater Kontrollmechanismen) ist jedoch aus Gründen der Rechtssicherheit für die Betreiber und generellen rechtsstaatlichen Erwägungen aus unserer Sicht erforderlich.

Grundsätzlich ist unseres Erachtens auch davon auszugehen, dass es durch die Erweiterung der Auskunftsrechte des § 53 Abs 3a SPG und dem mangelnden Richtervorbehalt und/oder sonstigen Kontrollmechanismen bei derartigen Überwachungsmaßnahmen zu einem wesentlichen Anstieg der Auskunftsanforderungen kommen würde.

Anhand der EB zu der Auskunft über Standortdaten zeigt sich, dass der Gesetzgeber möglicherweise von einem zu engen Begriff des Kommunikations-(Fernmelde-)geheimnis ausgeht: *„ Solange Standortdaten nicht auf dem Übertragungsweg abgefangen werden sollen, sondern durch Erhebung beim Diensteanbieter gewonnen werden, liegt kein Eingriff in das Fernmeldegeheimnis des Art. 10a StGG vor. Nur Inhaltsdaten sind dem Fernmeldegeheimnis iSd Art. 10a StGG zuzurechnen…“* (aus der Erläuterung).

Nach Ansicht der Judikatur sowie eines Teiles der Lehre unterliegen sehr wohl auch Vermittlungsdaten dem Schutz des Fernmeldegeheimnisses nach Art 10a StGG.[1] Darüber hinaus vertrat der Gesetzgeber bereits in den EB zu § 93 TKG 2003 die Ansicht, dass die Standortdaten in aller Regel ein Spezialfall der Verkehrsdaten sind und für ein geringeres Schutzniveau ersterer keine sachliche Rechtfertigung besteht (128 der Beilagen XXII. GP, RV, Materialien, 18).[2]

5. Bekanntgabe von Standortdaten:

Mit der Wortfolge *„.. sind die Sicherheitsbehörden zur Abwehr dieser Gefahr darüber hinaus berechtigt, von den Betreibern im Mobilfunkbereich Auskunft über Standortdaten und die internationale Mobilteilnehmerkennung (IMSI) zu verlangen sowie technische Mittel zur Lokalisierung einer von einem gefährdeten Menschen mitgeführten Endeinrichtung zum Einsatz zu bringen....“* sind für die Mobilfunkbetreiber erhebliche Änderungen verbunden.

Die derzeitigen gesetzlichen Regelungen sehen Folgendes vor: Gemäß § 98 TKG 2003 sind Betreiber von Notrufdiensten berechtigt, Standortdaten im Notfall anzufordern.

Gemäß § 149a Abs 1 Z 1 lit a StPO ist die Feststellung des räumlichen Bereiches im Zuge der Aufklärung einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten straf-

---

1 Vgl. Schmölzer, Rückwirkende Überprüfung von Vermittlungsdaten im Fernmeldeverkehr - Anmerkungen zu OGH 6.12.1995, 13 Os 161/95, JBl 1997, 214; dies, Cyberstructure: Die "Fangschaltung", Juridikum 1997, 43, 46; Schmölzer/Mayer-Schönberger, Das Telekommunikationsgesetz 1997 - Ausgewählte rechtliche Probleme, ÖJZ 1998, 383; Reindl, Telefonüberwachung zweimal neu? JBl 2002, 71; OGH 06.12.1995, 13 Os 161/95, JBl 1997, 260; OGH 18.01.2001, 12 Os 152/00, JBl 2001, 531 (Burgstaller) = EvBl 1998/191; Wiebe, Auskunftsverpflichtung der Access Provider, MR 2005 H 4 Beilage, 1, 20; Einzinger/Schubert/Schwabl/Wessely/Zykan, Wer ist 217.204.27.214? MR 2005, 113, 5; Reindl in Fuchs-Ratz, Wiener Kommentar zur StPO, Vor §§ 149a-c Rz 9; Helmreich, Auskunftspflicht des Access-Providers bei Urheberrechtsverletzungen? ecolex 2005, 379, 2; OGH 26.7.2005, 11 Os 57/05z u.a., JBl 2006, 130, 6.)

2 Die im o.a. Zusammenhang mit dem neu zu schaffenden § 53 Abs 3a SPG zitierte Entscheidung des OGH vom 19.12.2005, 14 Os 102/05m, stellt auf Daten aus einem beim Rechtsmittelwerber im Zuge einer Hausdurchsuchung sichergestellten Organizer - also einem beschlagnahmten Beweismittel - ab. Für Betreiber und deren Mitarbeiter gilt - im Gegensatz zu einem an einer Kommunikation beteiligten Benutzer - hingegen das strenge Regime des § 108 Abs 1 Z 1 TKG 2003, wonach bereits das unbefugte Mitteilung machen allein über die Tatsache eines Telekommunikationsverkehrs mit gerichtlicher Freiheitsstrafe bis zu drei Monaten oder mit Geldstrafe bis zu 180 Tagessätzen pönalisiert ist.

baren Handlung sowohl für einen historischen, gegenwärtigen als auch zukünftigen Überwachungszeitraum zulässig. Die Bestimmungen der §§ 149a ff StPO stehen jedoch eindeutig unter Richtervorbehalt.

Auskünfte über Standortdaten werden somit derzeit bei Verdacht der Erfüllung bzw. bei Vorliegen eines Straftatbestandes gemäß Gerichtsbeschluss und im Falle eines Notfalles gemäß § 98 TKG 2003 seitens der Netzbetreiber auf Verlangen unverzüglich erteilt.

Unter anderem wird durch die den Betreibern des Notrufdienstes gesetzlich auferlegten Dokumentationspflichten (§ 98 TKG) sowie den in §§ 149a ff StPO normierten Richtervorbehalt das Kommunikationsgeheimnis iSd § 93 TKG 2003 gewahrt.

Durch die geplante Änderung des § 53 Abs 3a SPG ist jedoch der Schutz des Richtervorbehaltes sowie auch der des § 98 TKG 2003 nicht mehr gegeben, da diese keine ausreichende Dokumentationspflichten, und somit die Überprüfbarkeit der Voraussetzungen für eine Standortdaten-Anforderung, vorsehen, was unseres Erachtens im Widerspruch zu § 93 TKG 2003 steht.

Aus unserer Sicht wäre aus oben angeführten und datenschutzrechtlichen Gründen die Aufnahme der Schriftlichkeit sowie entsprechender Formvorschriften bei Anforderungen nach § 53 Abs 3a SPG, welche insbesondere den Anfragegrund und die Anspruchsgrundlage zu enthalten haben, in die geplante Änderung notwendig.

Weiters müsste der anfordernden Behörde, in Angleichung an § 98 TKG bzw. die ErläutRV zu § 98 TKG, die Verantwortung für die rechtliche Zulässigkeit der Anfrage übertragen werden - vgl. dazu ErläutRV zu § 98 TKG: „ *Wenn der Betreiber einem glaubhaften Übermittlungsersuchen entspricht, ist er im Falle eines missbräuchlichen Ersuchens von der Verantwortung befreit. Diese trifft die Notruforganisation*“.

6. Bekanntgabe der internationalen Mobilteilnehmerkennungen (IMSI):

Wortfolge „*.. sind die Sicherheitsbehörden zur Abwehr dieser Gefahr darüber hinaus berechtigt, von den Betreibern im Mobilfunkbereich Auskunft über Standortdaten und die internationale Mobilteilnehmerkennung (IMSI) zu verlangen sowie technische Mittel zur Lokalisierung einer von einem gefährdeten Menschen mitgeführten Endeinrichtung zum Einsatz zu bringen....*“.

Gegen die geplante gesetzliche Auskunftserteilung von IMSI-Nummern im Rahmen des § 53 Abs 3a SPG bestehen aus unserer Sicht folgende Bedenken:

Unter der Definition „*technische Mittel zur Lokalisierung einer von einem gefährdeten Menschen mitgeführten Endeinrichtung*“ sind u.a. die so genannten IMSI-Catcher zu verstehen.

Durch die Bekanntgabe von IMSI-Nummern nach § 53 Abs 3a SPG (in der geplanten Fassung) wird den Sicherheitsbehörden der Einsatz von IMSI-Catchern ermöglicht und dieser auch zugleich legitimiert (Einsatz von technischen Mitteln zur Lokalisierung).

Da durch den Einsatz eines IMSI-Catchers die Überwachung der Telekommunikation wie nach §§ 149a ff StPO, insbesondere Lokalisierung des Standortes sowie auch das Mithören von

Gesprächen („man-in-the-middle Angriffe"), ermöglicht wird, muss dieser Einsatz jedenfalls unter Richtervorbehalt stehen.[3]

Wird ein IMSI-Catcher in Betrieb genommen, so buchen sich alle in einem gewissen Umkreis befindlichen Endgeräte bei diesem ein, da durch diesen ein Mobilfunknetzwerk simuliert wird.

Somit werden Daten von unbeteiligten Dritten miterfasst und gegen das Kommunikationsgeheimnis nach § 93 TKG 2003 in einem erheblichen Ausmaß verstoßen.

Weiters ist zu bedenken, dass der Einsatz von Überwachungsmaßnahmen auch aus Gründen der Beurteilung der Erforderlichkeit und Verhältnismäßigkeit der Überwachungsmaßnahme im Anwendungsbereich der StPO unter Richtervorbehalt steht und durch die geplante Regelung diese Beurteilung im Anwendungsbereich des SPG an die anfordernde Sicherheitsbehörde übertragen werden würde. Ein Kontrollmechanismus besteht nicht. Auch hier zeigt sich ein Wertungswiderspruch.

Überdies führt der Einsatz von IMSI-Catchern zu enormen Störungen und Ausfällen des Mobilfunknetzes, deren Folgen unter anderem wie folgt aussehen können:

- je nach Anwendung und verwendeter Sendeleistung (Einsatzzweck) kann es zu einem großflächigen Ausfall des Netzes kommen.
- Es können keine Gespräche, inklusive Notrufe, durch die miterfassten Teilnehmer geführt werden.
- Es können keine Lokalisierungen gemäß § 149a Abs 1 Z1 lit a StPO und § 98 TKG 2003 durchgeführt werden.

7. Kostenersatz:

Positiv ist anzumerken, dass nach dem vorliegenden Gesetzesentwurf nun der **Wegfall der kostenlosen Auskunftsverpflichtung** gegeben ist und eine gesetzliche Regelung des Kostenersatzes für die Auskunftserteilungen gemäß § 53 Abs 3a SPG eingeführt werden soll.

Festgehalten werden muss in diesem Zusammenhang jedoch die Tatsache, dass durch die derzeitige Fassung der Überwachungskostenverordnung (ÜKVO) lediglich die Beauskunftung/ Ermittlung von Standortdaten (gemäß § 7 Z 4 ÜKVO) und **nicht auch die Beauskunftung/ Ermittlung von IMSI-Nummern oder Stammdaten** in Rechnung gestellt werden können.

Demzufolge müsste § 8 Z 3 ÜKVO („Ermittlung von Rufnummern auf Basis von IMEI- oder IMSI-Nummern") angepasst werden sowie eine Regelung über den Kostenersatz für die Erhebung von Stammdaten getroffen werden.

Offen ist auch, wer für die Abwicklung der Rechnungslegung des Netzbetreibers zuständig ist. Es müsste daher der konkrete Rechnungslegungsverlauf, insbesondere Rechnungszustellung an eine zentrale Sicherheitsbehörde oder das zuständige Bundesministerium, festgelegt werden. Dies würde zumindest eine nachträgliche Überprüfung durch die zentrale Behörde (Anforderung und referenzierende Kostennote) in Teilbereichen ermöglichen. Eine direkte Rechnungslegung an

---

3 Vgl. dazu den Erlass des BMJ-L430.001/0002-II - Einführung von Formblättern für die Überwachung der Telekommunikation „TÜ-Beschluss-IMSI-Catcher- Gericht".

anfordernde Dienststellen würde in keinem Verhältnis zu den dafür anfallenden Aufwendungen bei den betroffenen Unternehmen stehen.

Da die Sicherheitsbehörden auch ohne richterlichen Beschluss Standortdaten und IMSI bekommen sollen, ist davon auszugehen, dass sich derartige Anfragen enorm vermehren werden. Damit hätten die Betreiber auch einen entsprechenden Mehraufwand zu bewältigen. **Wir weisen diesbezüglich daher insbesondere auf die noch nicht geklärte Frage der Kostenersatzpflicht für die Einrichtung von Telefonüberwachungsanlagen hin.** Hier soll einerseits ein Mehraufwand für die Betreiber generiert werden, ohne dass die grundsätzliche Kostenersatzpflicht geklärt ist. Eine Lösung der Frage des Investitionskostenersatzes muss daher dringend gefunden werden.

Die Stellungnahme wird auch dem Präsidium des Nationalrats übermittelt.

Mit freundlichen Grüßen

Dr. Christoph Leitl
Präsident

Dr. Reinhold Mitterlehner
Generalsekretär-Stv.