REPUBLIK ÖSTERREICH
DATENSCHUTZRAT

A-1010 Wien, Ballhausplatz 1
Tel. ++43-1-531 15/2527
Fax: ++43-1-53109/2702
e-mail: dsrpost@bka.gv.at
DVR: 0000019

GZ BKA-817.265/0007-DSR/2007

Betrifft: Regierungsvorlage betreffend ein Bundesgesetz, mit dem das Sicherheitspolizeigesetz (SPG), das Grenzkontrollgesetz (Greko) und das Polizeikooperationsgesetz (PolKG) geändert werden
Stellungnahme des Datenschutzrates

Der Datenschutzrat hat in seiner 178. Sitzung am 6. November 2007 mehrheitlich beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

I. Zum Themenkomplex „Telekommunikationsüberwachung“

A. Zu § 53 Abs. 3a SPG (Art 1 Z 4 des Entwurfs idF der RV)

Die vom DSR in seiner Stellungnahme vom 21. September 2007 zu § 53 Abs. 3a SPG angeregte Sitzung der Expertengruppe mit Vertretern des BKA-VD, des BMI und des BMVIT, sowie der DSK und den Betreibern im Mobilfunkbereich, sowie Vertretern der AK und der WKO fand am 11. Oktober 2007 im BMI statt. In diesem Rahmen kam insbesondere die Problematik der Reichweite des geltenden § 53 Abs. 3a Satz 1 und 2 SPG zum Tragen. Der in Satz 1 enthaltene Passus „Teilnehmernummer eines Bestimmten Anschlusses“ erscheint im Lichte der gegenwärtigen Technik (Internet, E-Mail, Voice-over-IP-Telefonie) auslegungsbedürftig.
Aus den Äußerungen des BMI in der Sitzung des 11. Oktober 2007 geht im gegebenen Kontext hervor, dass das BMI eine weite Auslegung des
§ 53 Abs. 3a SPG dahingehend praktiziert, dass darunter auch E-Mail-Adresse und IP-Adresse subsumierbar seien.

Diese Praxis einer weiten Auslegung, dh über die (vom Gesetzgeber seinerzeit wohl anvisierte) traditionelle Sprachtelefonnummer hinaus, wirft jedoch Probleme auf. Zur Feststellung des Anschlussinhabers im Falle von E-Mail-Adresse und IP-Adresse muss über die Stammdaten hinaus auf sog. Verkehrsdaten zurückgegriffen werden.
Dies bedeutet jedenfalls einen Eingriff in das Fernmeldegeheimnis. Zu verweisen ist hier auch auf die rezente Entscheidung der Datenschutzkommission vom 3. 10. 2007, K121.279/0017-DSK/2007. In dieser wird explizit festgehalten, dass sich die DSK „der Auffassung, dass die Ermittlung jenes Anschlusses und seines Inhabers, der Ursprung einer Telekommunikation war (- oft auch als „Rufdatenrückerfassung" bezeichnet -), kein grundrechtsnaher Sachverhalt wäre, jedenfalls nicht anschließen kann. Ob Art. 10a StGG auch „äußere Gesprächsdaten", d.h. die „Verbindungs-„ oder „Verkehrsdaten" schützt, sei zwar strittig, doch sei festzuhalten, „dass die grundsätzliche Vertraulichkeit von Kommunikationen zwischen bestimmten Personen gegenüber Dritten sich anerkanntermaßen nicht nur auf den Inhalt, sondern auch auf die Verkehrsdaten erstreckt (vgl. Art. 5 der RL 58/2002 und das Kommunikationsgeheimnis nach § 93 TKG, das zwar nicht selbst in Verfassungsrang steht, aber jedenfalls als Ausfluss des Art. 8 EMRK und des Grundrechts auf Datenschutz im Telekommunikationsbereich zu sehen ist)." Die Ermittlung solcher Daten greife daher iSd § 28a Abs. 3 SPG in Rechte von Betroffenen ein und sei daher ohne besondere Befugnis der Sicherheitsbehörden nicht zulässig. […] Daraus folge, dass § 53 Abs. 1 SPG allein keine ausreichende Rechtsgrundlage für die Ermittlung von Verkehrsdaten darstellen kann, sondern hiefür der Umfang besonderer Eingriffsbefugnisse maßgeblich ist, die den Sicherheitsbehörden nach dem Sicherheitspolizeigesetz oder anderen Gesetzen eingeräumt sind. […] § 53 Abs. 3a SPG könne aber für die Übermittlung der (dynamischen) IP-Adresse, die unzweifelhaft ein Verkehrsdatum darstelle, etwa auf Basis eines ‚nickname', keine geeignete Grundlage bieten.
Verschärft wird die skizzierte Problematik nun einmal durch die (bereits im Erstentwurf vorgesehene) Ersetzung des Begriffs „Zeitpunkt" in Satz 2 des § 53 Abs. 3a SPG durch den Begriff „Zeitraum". Damit wird für den Fall der angestrebten Identifizierung des „bestimmten Anschlusses" durch die Bezeichnung mittels passiver Teilnehmernummer und eben „Zeitraum" manifest, dass nicht nur ein bestimmter Betroffener, sondern potentiell eine Vielzahl von Fernmeldeteilnehmern zum Gegenstand einer Rückrufdatenerfassung werden.

Die in der überarbeiteten Fassung vorgeschlagene Eingrenzung auf „einen möglichst genauen Zeitraum“ ist begrüßenswert.

Der Datenschutzrat regt an, auch im Bereich der Gefahrenabwehr eine – der richterlichen Genehmigung vergleichbare – Genehmigung durch eine Rechtsschutzinstanz (etwa den Rechtsschutzbeauftragten) vorzusehen. In dringenden Fällen - wie z.B. bei Gefahr in Verzug - wäre zumindest eine Ex-post-Überprüfung durch eine derartige Rechtsschutzeinrichtung anzustreben.

Seitens des Datenschutzrates wird angeregt, eine Expertengruppe mit Vertretern des BKA-VD, dem BMVIT, BMJ, BMI,der DSK, den Betreibern im Mobilfunkbereich sowie Vertretern der AK und der WKO einzurichten, welche sich mit den anstehenden juristischen und technischen Fragen im Zusammenhang mit der TKG - Novelle zur Umsetzung der Richtlinie über die Vorratsdatenspeicherung bzw. mit der Verzahnung zum SPG beschäftigen soll.
Der Datenschutzrat wird nach Anhörung der Expertengruppe eine abschließende Stellungnahme abgeben.

B. Zu § 53 Abs. 3b SPG (Art 1 Z 6 des Entwurfs idF der RV)

Die in der zuletzt zitierten Norm vorgesehene Ortungsmöglichkeit mittels eigener „technischer Mittel“ (gemeint: sog. IMSI-Catcher) des BMI geht noch einen Schritt weiter. IMSI-Catcher sind Geräte, mit denen die auf der Mobilfunk-Karte eines Mobiltelefons gespeicherte International Mobile Subscriber Identity (IMSI) ausgelesen und der Standort eines Mobiltelefons innerhalb einer Funkzelle eingegrenzt werden kann. Auch das Mithören von Handy-Telefonaten ist theoretisch möglich, aber rechtswidrig. Verwendet werden IMSI-Catcher insbesondere von Geheimdiensten (Das BMLV verfügt deshalb ebenfalls über ein derartiges Gerät). Warum die Ortung nicht mittels der schon jetzt möglichen „Peilung“ mittels Funkmasten durch die Mobilfunkbetreiber selbst eingreifen soll, bleibt unklar.
Insgesamt sprechen die einfachgesetzliche Praxis (§§ 149a ff StPO), aber auch die grundsätzliche hohe „Aussagekraft“ von Verkehrs- bzw. Verbindungsdaten bzw. deren Nahebezug zum Kernbereich der Privatsphäre sowie die Judikatur der DSK für

eine unabhängige bzw. am besten richterliche Kontrolle der hier diskutierten Eingriffe. Die aktuelle Fassung der RV trägt diesem Aspekt nur bedingt Rechung.
Vor dem skizzierten Hintergrund ist der Wunsch der Provider nach Rechtssicherheit und Schutz vor dem Risiko, etwa im Falle von Anfragen nach § 53 Abs. 3a bzw. 3b SPG eine Grundrechtsverletzung zu verursachen, verständlich. Eine automatische Exkulpierung kann es aber vor dem Hintergrund der Bestimmungen der §§ 7 ff DSG 2000 nicht geben. Aus deren System folgt, dass der Auftraggeber vor einer Übermittlung stets zumindest eine Plausibilitätsprüfung vorzunehmen hat. Die im Entwurf vorgesehene Anordnung „die Sicherheitsbehörde trifft die Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehrens“ ist iVm den Erläuterungen im gegebenen Kontext insofern irreführend. Die Behörde trifft in jedem Fall die rechtliche Verantwortung ihres Tuns in haftungsrechtlicher und (betreffend die Amtswalter) letztlich in diszipliar- und strafrechtlicher Sicht. Ein spezifischer datenschutzrechtlicher Mehrwert ergibt sich hingegen aus dem zitierten Vorschlag nicht.

Die folgenden schon am 1. Oktober geäußerten Bedenken bzw. Anregungen des Datenschutzrates wurden vom BMI bisher noch nicht berücksichtigt und werden daher nochmals eingebracht:

II. Zu Art 1 Z 8 des Entwurfs idF der RV (§ 53a Abs. 2 Z 4 SPG)

Zu Abs. 2 Z 4 des § 53a SPG ist festzuhalten, dass die hier genannte Kontakt- oder Begleitpersonen nicht automatisch selbst kriminelle Handlungen begeht. Auch hinsichtlich eines zunächst „Verdächtigen“ (Abs. 2 Z 1) kann sich auf Grund weiterer Ermittlungen herausstellen, dass er in weiterer Folge als nicht mehr verdächtig gilt Zeigt sich, dass ein zunächst Verdächtigter oder eine Kontakt- oder Begleitperson selbst nicht deliktisch handelt bzw. für den weiteren Verlauf von Ermittlungen nicht notwendigerweise im Visier der Behörden bleiben muss, sind Daten unverzüglich zu löschen. Dieser Ansatz kommt in der jetzigen Textierung nicht ausreichend zum Tragen. Es sollte daher eine Präzisierung bzw. einschränkendere Formulierung, die sich am Vorbild des Art. 6 Abs. 3 des oben zitierten Rechtsaktes für die von Europol geführten Analysedateien orientieren sollte, erfolgen.

III. Zu Art 1 Z 21 des Entwurfs idF der RV (§ 75 Abs. 1 SPG)

Im Zusammenhang mit der hier angestrebten „Rationalisierung“ im Bezug auf die Verwendung erkennungsdienstlicher Daten ist zu betonen, dass eine solche nicht zu einem Verlust von Transparenz für die Betroffenen führen darf. Werden also beispielsweise von einer Person nach dem Fremdenpolizeigesetz Fingerabdrücke abgenommen und diese sowohl nach Fremdenpolizeigesetz als auch später nach SPG weiterverarbeitet, wäre sicherzustellen, dass der betreffenden Person eine entsprechende Mitteilung über diese Doppelverwendung zugeht. Legistisch wäre dies durch einen entsprechenden Verweis auf § 65 Abs. 5 SPG zu lösen.

IV. Zu Art. 3 Z 1 (§ 7 Abs. 5 PolKG)

Der Entwurf sieht vor, dass künftig die Sicherheitsbehörden ermächtigt sein sollen, Amtshilfe durch das Verwenden von Daten, die von ausländischen Sicherheitsbehörden und Sicherheitsorganisationen in gemeinsam geführten Informationssammlungen verarbeitet werden, unmittelbar in Anspruch zu nehmen.

Der vorgeschlagene Abs. 5 des § 7 PolKG steht einmal in offenkundigem Widerspruch zu § 7 Abs. 1 PolKG. Zufolge Letzterer nehmen nachgeordnete Sicherheitsbehörden Amtshilfe im Wege des Bundesministers für Inneres in Anspruch. Davon abgesehen ist nicht ersichtlich, wie durch eine solche Norm sichergestellt werden soll, dass nicht etwa Exekutivorgane auf unüberprüfte bzw. unzuverlässige ausländische Informationen (etwa aus problematischen Drittstaaten ohne Überprüfungsmöglichkeit der Datenqualität) zurückgreifen. Den berechtigten Anliegen der Datenrichtigkeit, der Datenlöschung bzw. der Auskunft gegenüber Betroffenen kann durch eine solche rudimentäre Bestimmung ebenfalls nicht ausreichend Rechnung getragen werden.

Weiters wird zu dieser Bestimmung eine Überprüfung dahingehend angeregt, ob nicht in bestehenden völkerrechtlichen Verträgen Regelungen derart vorgesehen sind, dass Amtshilfe durch das Verwenden von Daten im Wege einer bestimmten Stelle bzw. Einrichtung in Anspruch zu nehmen ist. Bejahendenfalls würde die geplante Bestimmung in Widerspruch zu den völkerrechtlichen Verträgen stehen, da

eine entsprechende Regelung betreffend unmittelbare Datenverwendung durch die Sicherheitsbehörden selbst zwar – innerstaatlich - entgegenstehenden Bestimmungen in Staatsverträgen auf Gesetzesstufe zu derogieren vermag, gegenüber den Vertragsparteien hätte eine Änderung jedoch grundsätzlich in Form der Abänderung des völkerrechtlichen Vertrages zu erfolgen.

Anlage: Votum Separatum

8. November 2007
Für den Datenschutzrat
Der Vorsitzende:
WÖGERBAUER

Elektronisch gefertigt