Gerhard KUNNERT*

Der sicherheitspolizeiliche Griff nach Telekommunikationsdaten. Möglichkeiten – Grenzen – Kritik

Inhaltsübersicht

* Der Beitrag spiegelt ausschließlich die persönliche Meinung des Autors wider.

I. Einleitung

Das am 1. Jänner 2008 in Kraft getretene Bundesgesetz, mit dem das Sicherheitspolizeigesetz, das Grenzkontrollgesetz und das Polizeikooperationsgesetz geändert werden,[1] brachte unter anderem eine Neufassung bzw Ergänzung jener Bestimmungen des § 53 des Sicherheitspolizeigesetzes (SPG), welche die Auskunftsrechte der Sicherheitsbehörden gegenüber Betreibern öffentlicher Telekommunikationsdienste regel(te)n (bisher: § 53 Abs 3a; nunmehr zusätzlich: § 53 Abs 3b), mit sich. Derartige sicherheitspolizeiliche Anfragen durften sich bis 31. Dezember des Jahres 2007 im Wesentlichen nur auf Namen, Anschrift und Teilnehmernummer beziehen.[2] Nach der neuen Rechtslage reicht die Bandbreite zulässiger Anfragen für Zwecke der „Gefahrenabwehr“ weit darüber hinaus: Zusätzlich zu den genannten Daten darf nunmehr – vereinfacht gesagt – auch auf der Basis von bzw nach Internetprotokolladressen (IP-Adressen) sowie nach

1 BGBl I 2007/114.

2 Vgl § 53 Abs 3a Satz 1 SPG idF vor BGBl I 2007/114. Auf die Anfragevoraussetzungen nach § 53 Abs 3a Satz 2 wird an dieser Stelle der Einfachheit halber nicht näher eingegangen.

dem Standort sowie der internationalen Mobilteilnehmerkennung („International Mobile Subscriber Identity", kurz: „IMSI") von Mobiltelefonen gefragt werden.[3]

Die Reichweite der den Sicherheitsbehörden damit eingeräumten Befugnisse einerseits und die Veränderung der ursprünglichen Regierungsvorlage in zentralen Punkten mittels Abänderungsantrag[4] im Plenum des Nationalrates am 6. Dezember 2007 unter Umgehung des Innenausschusses andererseits haben nach Beschlussfassung kurz vor Mitternacht desselben Tages[5] zu massiver Kritik nicht nur der parlamentarischen Opposition, sondern auch einzelner Vertreter der Regierungsparteien,[6] Experten,[7] Interessenvertretungen,[8] Organisationen der Zivilgesellschaft[9] sowie zu entsprechend kritischer Medienberichterstattung[10] geführt.

„Die Grünen" initiierten in der Folge gar eine „parlamentarische Petition"[11] mit dem Ziel, die hier diskutierten SPG-Regelungen einer „ernsthaften" Befassung durch den Innenausschuss zuzuführen.[12] Darüber hinaus sollten „alle gesetzlichen und behördlichen Ermächtigungen zur Überwachung ohne ausreichende Abwägung der Verhältnismäßigkeit und ohne genügende Kontrolle durch Richter

3 Vgl § 53 Abs 3a Satz 1 Z 2 und 3 und Abs 3b SPG idgF.

4 Abänderungsantrag AA-89 (XXIII. GP) der Abgeordneten *Kößl*, *Parnigoni*, Kolleginnen und Kollegen zu der Regierungsvorlage (272 BlgNR): Bundesgesetz, mit dem das Sicherheitspolizeigesetz, das Grenzkontrollgesetz und das Polizeikooperationsgesetz geändert werden.

5 Vgl http://futurezone.orf.at/it/stories/241208/ (7.12.2007 – „SPG-Novelle passiert Nationalrat. Zugriff auf Standortdaten und IP-Adressen").

6 So etwa Nationalratspräsidentin *Prammer* (SPÖ), die sich (erfolglos) für eine ausführliche Diskussion im Innenausschuss und spätere Beschlussfassung des SPG ausgesprochen hatte (vgl heise online news 16.12.2007 „Neues österreichisches Sicherheitspolizeigesetz in der Kritik"; http://www.heise.de/newsticker/Neues-oesterreichisches-Sicherheitspolizeigesetz-in-der-Kritik--meldung/100667, abgerufen am 9.4.2008).

7 Bspw das geschäftsführende Mitglied der Datenschutzkommission (DSK), Dr. *Kotschy*, im Ö1-Mittagsjournal am 15.12.2007, welche ua feststellte, dass es eindeutig verabsäumt wurde, die im SPG vorgesehenen heiklen Eingriffe in Grund- und Freiheitsrechte wohlüberlegt durchzudiskutieren (vgl wieder heise online news 16.12.2007 [FN 6]).

8 Seitens der österreichischen Richtervereinigung hieß es etwa, man sei zwar an effizienter Strafverfolgung interessiert, doch müsse man in so sensiblen Bereichen besonders vorsichtig agieren. „Und niemals heiligt der Zweck die Mittel." (vgl heise online news 16.12.2007 [FN 6]).

9 Kritisch Stellung nahmen ua Menschenrechtsorganisationen wie die „Reporter ohne Grenzen" (http://futurezone.orf.at/it/stories/242217/; 11.12.2007 - „Reporter ohne Grenzen: Kritik am SPG") oder die Österreichische Liga für Menschenrechte („Weitreichende Überwachungsmöglichkeiten ohne rechtsstaatliche Kontrolle. Da fehlt dann nicht mehr viel auf die Schreckensvision in George Orwells ‚1984'"; vgl heise online news 16.12.2007 [FN 6]).

10 Vgl bspw *Nowak,* Schöne Werkzeuge für Horngacher und Co. Das Polizeigesetz erlaubt Handy- und Netz-Ortung ohne richterliches o.k. […], Die Presse, 14.3.2008, 39; „Unkontrollierte Handy-Überwachung. Gesetzesnovelle erlaubt Polizei künftig Zugriff auf Standortdaten und IP-Adressen", der Standard, 7./8./9.12.2007, 9.

11 Vgl § 100 Abs 1 Z 1 Geschäftsordnungsgesetz 1975 BGBl 410 idgF (NRGOG).

12 Vgl http://futurezone.orf.at/it/stories/243503/ (17.12.2007 - „Initiative gegen Überwachungsstaat"); http://www.ocg.at/presse/2007/071217-petition.html.

zurückgenommen werden".[13] Die immerhin von mehr als 24.000 Bürgern unterstützte Petition[14] wurde von den Organisatoren am 27. Februar 2008 an die amtierende Präsidentin des Nationalrates übergeben[15] und am 5. März erstmals im Petitionsausschuss behandelt.[16] Mittlerweile wurden auch gegen die (behauptete) Verfassungswidrigkeit der neu eingeführten Ermächtigungen gerichtete Individualbeschwerden beim Verfassungsgerichtshof eingebracht.[17]

II. Kernpunkte der öffentlichen Diskussion

A. Die Argumente der Kritiker

Inhaltlich zielt(e) die auf breiter Basis (teils schon während der Begutachtungsphase) vorgetragene Kritik zusammenfassend einmal auf das große „Missbrauchspotential" ab, das in der den Sicherheitsbehörden eröffneten Möglichkeit liege, im Wege einer formlosen Anfrage direkt an Betreiber von Telekommunikationsdiensten künftig nicht nur sog „Stammdaten" (im Wesentlichen Namen, Wohnadresse, Telefonnummer, ggf E-Mailadresse)[18] von Nutzern, sondern auch sog „Verkehrsdaten" (dh insbesondere sog IP-Adressen und Standortdaten von Mobiltelefonen)[19] zu erhalten.[20] Es sei zu befürchten, dass letztere Auskunftsmöglichkeiten in der polizeilichen Praxis auch außerhalb konkreter Gefahrensituationen, wie dies nach der neuen Rechtslage formal vorgesehen sei,[21] in Anspruch genommen und damit die Kommunikation unbescholtener Bürger ausgespäht würde(n).[22] Das Fehlen jeglicher (auch einer nachträglichen) richterlichen Kontrolle im gegebenen Kontext bedeute „eine neue Qualität, die nicht in den

13 Vgl den Wortlaut der Petition „Gegen die Ausweitung der polizeilichen Überwachung auf Handys, Internet und ihre User. Parlamentarische Petition zur Behandlung des Sicherheitspolizeigesetzes im Innenausschuss des Nationalrats" (Dezember 2007), abgerufen (am 4.4.2008) über http://www.ueberwachungsstaat.at/ueberwachungsstaat/unterlagen/.

14 Vgl http://futurezone.orf.at/it/stories/259280/ (25.2.2008 – „SPG-Petition soll vor Innenausschuss").

15 Vgl http://futurezone.orf.at/it/stories/259818/ (27.2.2007 – „SPG soll vor den Verfassungsgerichtshof" bzw Zwischenüberschrift „Petition eingereicht").

16 Vgl näher zum Verfahren § 100 ff NRGOG.

17 http://futurezone.orf.at/it/stories/263387/ (13.3.2007 - „Erste Verfassungsklagen gegen SPG"); http://diepresse.com/home/techscience/hightech/369686/index.do (13.3.2008 - Telekom-Branche: „Polizei missbraucht Überwachung").

18 Für den genauen Umfang siehe § 92 Abs 3 Z 3 Telekommunikationsgesetz 2003 BGBl I 70 (TKG 2003).

19 Zum Begriff aus Sicht des TKG 2003 siehe § 92 Abs 3 Z 4, 4a und 6 leg cit.

20 In diesem Sinne etwa die Österreich-Präsidentin der Menschenrechtsorganisation „Reporter ohne Grenzen [RoG/RSF]", *Rubina Möhring* (vgl http://futurezone.orf.at/it/stories/242217; 11.12.2007 - „Reporter ohne Grenzen: Kritik am SPG").

21 Vgl § 53 Abs 3a Satz 1 SPG idgF.

22 In diese Richtung etwa der Vizepräsident der österreichischen Richtervereinigung, *Herrnhofer*, zitiert nach heise online, news 16.12.2007, Neues österreichisches Sicherheitspolizeigesetz in der Kritik (http://www.heise.de/newsticker/Neues-oesterreichisches-Sicherheitspolizeigesetz-in-der-Kritik--/meldung/100667, abgerufen am 4.4.2008).

bisherigen Umgang mit den Grundrechten pass(t)e“.[23] Die bloße Information des sog Rechtsschutzbeauftragten per se reiche dagegen keineswegs aus.[24] Dieser sei kein Richter, könne die Eingriffe weder unterbinden noch Sanktionen verhängen.[25] Die Betroffenen selbst würden von einer Überwachung – wenn überhaupt – nur Kenntnis erlangen, wenn es in letzter Konsequenz zu einem gerichtlichen Strafverfahren gegen sie komme.[26]

Auf der verfassungsrechtlichen Ebene wurde/wird argumentiert, das Fehlen des Erfordernisses einer richterlichen Kontrolle der hier interessierenden polizeilichen Eingriffe stehe dem verfassungsgesetzlich für Eingriffe in das Fernmeldegeheimnis vorgesehenen Richtervorbehalt entgegen.[27]

Vor allem seitens der Auskunftspflichtigen (Betreiber) wurden weiters eine Reihe praktischer Umsetzungsprobleme geltend gemacht. Diese reichten von der behaupteten Unbestimmtheit zentraler Gesetzesbegriffe (Bsp: „konkrete Gefahrensituation“) über Unklarheiten über das „Prozedere“ für die Herausgabe der Daten (Bsp: Welche sicherheitsbehördliche Stellen dürfen anfragen?) bis hin zur Unsicherheit über das Verhältnis verschiedener, für die Beauskunftung von Telekommunikationsdaten relevanter Normenkreise (SPG, Telekommunikationsgesetz [TKG], Strafprozessordnung [StPO]).[28] Aus all diesen Gründen sei eine „Reparatur“ des SPG gefordert.[29]

Neben den vorhin angesprochenen praktischen Schwierigkeiten äußerten die Internetdienst(e)anbieter auch die Befürchtung, dass „durch die Überwachungs-Lawine im Internet“ eine vermehrte Unsicherheit bei den Bürgern entstehe und

---

23 So Richter Dr. *Schmidbauer* gegenüber dem ORF, zitiert nach http://futurezone.orf.at/it/stories/240514/ (5.12.2007 – „SPG erlaubt Zugriff auf Standortdaten“ bzw Zwischenüberschrift „Die Probleme“).

24 So etwa *A Min Tjoa*, Professor am Institut für Softwaretechnologie und Interaktive Systeme der TU Wien anlässlich der Vorstellung der „Initiative für den Schutz vor dem Überwachungsstaat“ (vgl http://futurezone.orf.at/it/stories/243503/; 17.12.2007 – „Initiative gegen Überwachungsstaat“).

25 So der Obmann der Bundessparte Information und Consulting der Wirtschaftskammer (WKÖ-BSIC) *Pollirer*, zitiert nach heise online, news 13.03.2008 - Österreich: Verfassungsbeschwerden gegen Sicherheitspolizeigesetz (http://www.heise.de/newsticker/Oesterreich-Verfassungsbeschwerden-gegen-Sicherheitspolizeigesetz--/meldung/105020/from/rss09, abgerufen am 7.4.2008).

26 So Abg z NR Dr. *Pilz*, zitiert nach heise online, news 17.12.2007, Österreich: Petition gegen den Überwachungsstaat gestartet (http://www.heise.de/newsticker/Oesterreich-Petition-gegen-den-Ueberwachungsstaat-gestartet--/meldung/100700, abgerufen am 9.4.2008).

27 Vgl in diesem Sinne etwa die Stellungnahme der Bundesarbeitskammer vom 1.10.2007 zum Ministerialentwurf (auf der Homepage des Parlaments abrufbar unter 18/SN-118/ME [XXIII. GP]) oder die Argumentation der Individualbeschwerdeführer beim Verfassungsgerichtshof (dazu wieder Quelle in FN 17).

28 Vgl in diesem Sinne die Kritik seitens der Spartenvertreter der Wirtschaftskammer Österreich (WKÖ) (http://futurezone.orf.at/it/stories/243929/ [19.12.2007 - SPG-Verabschiedung „indiskutabel“]) bzw der ISPA (Internet Service Providers Austria) etwa auf der gemeinsamen Pressekonferenz von ISPA und WKÖ-BSIC am 13.3.2008 zum Thema „Stoppt die Überwachungs-Lawine im Internet!“ (vgl OTS0169 5 CI 0735 ISP0001 II Do, 13.3.2008).

29 So etwa die Forderung von ISPA-Generalsekretär Dr. *Einzinger* am 19.3.2008 (http://futurezone.orf.at/it/stories/264913/; 20.3.2008 - „WKO Wien bietet SPG-Rechtsberatung“ bzw Zwischenüberschrift „Keine Statistik“).

die Internet-Nutzung insgesamt abnehme.[30]

In punkto Standortdaten zu Mobiltelefonen wurde – vom Fehlen der gerichtlichen Kontrolle einmal abgesehen – insbesondere ins Treffen geführt, dass im Falle einer sicherheitsbehördlichen Anfrage für Zwecke der Nothilfe nach dem Telekommunikationsgesetz 2003 (nachfolgend: TKG 2003) immerhin entsprechende nachträgliche Dokumentations- bzw Mitteilungspflichten gegenüber dem angefragten Betreiber eingreifen,[31] für eine auf das SPG gestützte Anfrage jedoch analoge Vorkehrungen fehlten.[32]

Speziell in Bezug auf die bereits eingangs erwähnte neue Verpflichtung zur Bekanntgabe der internationalen Mobilteilnehmerkennung (IMSI) wurde Unverständnis signalisiert. Die IMSI nütze den Sicherheitsbehörden nur, wenn diese sog „IMSI-Catcher"[33] einsetzten. Letztere seien jedoch nicht nur zur Ortung von Mobiltelefonen, sondern auch zum Abhören von Gesprächen geeignet. Deshalb müsse (auch der sicherheitspolizeiliche) der Einsatz von IMSI-Catchern unter Richtervorbehalt stehen. Zudem greife der IMSI-Catcher funktionsbedingt massiv in das Kommunikationsgeheimnis Unbeteiligter ein. Schließlich drohten durch den sicherheitspolizeilichen Einsatz von IMSI-Catchern Störungen und Ausfälle der Mobilfunknetze.[34] Im Übrigen seien IMSI-Catcher zur Ortung nur eingeschränkt geeignet bzw überflüssig;[35] die bisher praktizierte Suche nach Mobiltelefonen (Vermisster) über den Weg der Versendung eines (stillen) SMS und anschließender sog Kreuzpeilung mittels stationärer Mobilfunkmasten der Betreiber sei ausreichend und auch das gelindere Mittel.[36]

Eine gewisse Rolle in der öffentlichen Debatte spielte schließlich auch der (behauptete) Zusammenhang zwischen den erweiterten Auskunftsbefugnissen der Sicherheitsbehörden und den aktuell noch im Stadium der innerstaatlichen Umsetzung befindlichen EU-rechtlichen Vorgaben zur sog „Vorratsspeicherung" von Telekommunikationsdaten[37]. Um Erstere erfüllen zu können, würden die Betreiber öffentlich zugänglicher Kommunikationsdienste noch vor Inkrafttreten des entsprechenden Umsetzungsgesetzes, gewissermaßen „durch die Hinter-

30 So ISPA-Präsident Roland Türke in einer Pressekonferenz von WKÖ-BSIC und ISPA am 13.3.2008 zum Thema „Stoppt die Überwachungs-Lawine im Internet!", zitiert nach OTS0169 5 CI 0735 ISP0001 II Do, 13.3.2008.

31 Vgl im Einzelnen § 98 TKG 2003.

32 Vgl dazu die im Rahmen des Begutachtungsverfahrens abgegebene Stellungnahme der Wirtschaftskammer Österreich (WKÖ) v 27.9.2007, AZ Rp 1685/07/DrRo/SM, Seite 4 f.

33 Näheres zur Funktionsweise unten bei FN 185.

34 Vgl dazu die Stellungnahme der WKÖ v 27.9.2007, GZ Rp 1685/07/DrRo/SM, zum Entwurf eines Bundesgesetzes, mit dem das Sicherheitspolizeigesetz […] geändert wird, Seite 5 f.

35 So etwa Abg z NR Dr. Peter Pilz im Oktober 2007, zitiert nach heise online news 16.10.2007 - Grüne: Österreichs Innenminister will Handyüberwachung ohne Kontrolle (http://www.heise.de/newsticker/Gruene-Oesterreichs-Innenminister-will-Handyueberwachung-ohne-Kontrolle--/meldung/97425).

36 In diesem Sinne etwa die Argumentation von T-Mobile Austria GmbH in ihrer VfGH-Beschwerde betreffend § 53 Abs 3 a und 3b SPG vom 7.3.2008, 30 f.

37 Richtlinie 2006/24/ EG des Europäischen Parlaments und des Rates vom 15. März 2006 ABl L 105, 54 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden.

türe“, zu einer Speicherung von Verkehrsdaten gezwungen.[38]

B. Die Argumente der Befürworter

Auf politischer Ebene wurde die Kritik an der fehlenden richterlichen Kontrolle des sicherheitsbehördlichen Zugriffs auf Standortdaten von Mobiltelefonen in erster Linie mit dem Notfallcharakter der neu geschaffenen Ermächtigung verteidigt. Bei „Gefahr in Verzug“ sei es „meistens nicht möglich, so rasch wie dies nötig“ sei, „eine richterliche Genehmigung einzuholen“. Als typisches Beispiel wurden „vermisste Bergsteiger“, die mittels Handypeilung gefunden werden müssen, zitiert. Dabei zähle „jede Minute“. Der richterliche Befehl im Bereich der StPO „bleibe natürlich weiterhin Voraussetzung für die Telekomüberwachung“.[39]

Falsch sei auch das Argument, die Ortung Vermisster sei anstatt mittels IMSI-Catcher auch mit einer „stillen SMS“ möglich. In Tälern oder Grenzgebieten sei dies meist nicht möglich, da die Sendemasten dort bis zu 35 km auseinander stünden. Hier könne nur ein IMSI-Catcher helfen. Ein Abhören ohne richterliche Genehmigung sei weiterhin nicht zulässig und eine Gesprächsbelauschung der Polizei mit den IMSI-Catcher wäre illegal und strafrechtlich zu verfolgen.[40]

Die ausdrückliche Normierung der sicherheitspolizeilichen „Ausforschung von IP-Adressen in Notfällen“ wurde ua damit begründet, dass diese nunmehr „nur auf eine explizite Rechtgrundlage gestellt worden“ sei. Schon bisher sei die Weitergabe von IP-Adressen in Notfällen „Praxis“ gewesen, da man IP-Adressen unter „Telefonanschlüsse“ subsumiert habe.[41]

Zur Frage der Vereinbarkeit des Zugriffs der Sicherheitsbehörden auf Standortdaten ohne richterliche Erlaubnis mit dem verfassungsrechtlich für Eingriffe ins Fernmeldegeheimnis verankerten Richtervorbehalt sei an dieser Stelle angemerkt, dass in den Erläuterungen sowohl zum Ministerialentwurf als auch zur späteren Regierungsvorlage im Wesentlichen argumentiert wurde, dass „nur Inhaltsdaten dem Fernmeldegeheimnis iSd Art 10a Staatsgrundgesetz (StGG) zuzurechnen sind“ und (nur) „ihre Erhebung unter Gesetzes- und Richtervorbehalt zu stellen ist“.[42]

Seitens des Bundeskriminalamtes wurde allgemein auf die Problematik verwiesen, dass die organisierte Kriminalität (OK) mit eigenen Regeln, nachrichtendienstlichen Methoden und „nahezu unbeschränkten Mitteln“ arbeite. Die Polizei sei hingegen an nationale und internationale Vorschriften gebunden.[43]

---

38 Vgl wieder http://futurezone.orf.at/it/stories/263387/ (13.3.2008 - Erste Verfassungsklagen gegen SPG bzw Zwischenüberschrift „Vorgriff auf Vorratsdatenspeicherung“).

39 So etwa der stv Direktor des ÖVP-Parlamentsklubs und Vorsitzende des Datenschutzrates (DSR), Dr. *Wögerbauer*, am 6.12.2007, zitiert nach OTS0191 5 II 0292 VPK0006 Do, 06. Dez 2007.

40 So der SPÖ-Konsumentenschutzsprecher und stv. Vorsitzender des Datenschutzrates, Mag. *Maier,* am 19.12.2007, zitert nach OTS0192 5 II 0534 SPK0011 CI Mi, 19. Dez 2007.

41 So der stv Direktor des SPÖ-Parlamentsklubs, Dr. *Pointner*, zitiert nach http://futurezone.orf.at/it/stories/243929/ (19.12.2007 - SPG-Verabschiedung „indiskutabel“).

42 Vgl die Erl „Zu Artikel 1“, „Zu Z 3 (§ 53 Abs 3a)“ des Ministerialentwurfes (118/ME XXII. GP, Seite 5) und Erl „Zu Art 1“, „Zu Z 5 und 6 (§ 53 Abs 3b und 3c)“ der RV 272 BlgNR 23. GP, 5.

43 So der für Computer- und Netzwerkkriminalität zuständige Chefinspektor im Bundes-

Eine richterliche Genehmigung für den polizeilichen Zugriff auf Daten von Internet-Usern sei schon deshalb unmöglich, weil in der Regel gar kein strafbarer Tatbestand vorliege. Außerdem liege hier gar keine „Überwachung“ vor. Von einer solchen könne man nur in Bezug auf sog „Inhaltsdaten“ (gemeint: Gesprächsinhalte oder Inhalte von E-Mails)[44] sprechen und eine solche Überwachung gebe es nur auf Basis einer richterlichen Genehmigung. Ohne eine solche fordere die Polizei nur in Einzelfällen Stamm-, Standort-, oder Verkehrsdaten an. Ein Missbrauch dieser Befugnis sei strafrechtlich relevant.[45]

Zur Ortung Vermisster seien IMSI-Catcher keineswegs ungeeignet. Sie würden überdies nur bei „gegenwärtiger Gefahr für Leben oder Gesundheit“ eingesetzt; anschließend werde der im Innenministerium (in der Folge kurz: BMI) angesiedelte Rechtsschutzbeauftragte informiert.[46]

Mit Blick auf den behaupteten Konnex zwischen den neuen SPG-Bestimmungen und dem Thema „Vorratsdatenspeicherung“ wurde festgestellt, die davon betroffenen Daten würden bereits jetzt – illegaler Weise – von den Providern gespeichert.[47]

III. Zum Gang der Untersuchung

Die Komplexität der technischen Grundlagen der modernen Telekommunikationswirtschaft stellt selbst einschlägig interessierte bzw beruflich befasste Juristen vor gewisse Schwierigkeiten beim Nachvollzug von gewissen Argumentationen, mögen diese von Sicherheitsbehörden stammen oder von Verkehrskreisen, die sonst in irgendeiner Form von hier interessierenden staatlichen Überwachungsmaßnahmen betroffenen sind.

Dieser Umstand scheint sich nicht zuletzt in substantiellen Unterschieden niederzuschlagen, die bei der Auslegung zentraler Rechtsbegriffe in hier maßgeblichen einfachen Bundesgesetzen etwa durch ordentliche Gerichte einerseits und die Datenschutzkommission oder die Ministerialverwaltung andererseits zu Tage treten. Darüber hinaus besteht weder in der rechtswissenschaftlichen Literatur noch zwischen den Experten der einschlägig befassten Fachministerien Einigkeit über die genaue Reichweite des verfassungsrechtlichen Fernmeldegeheimnisses (Art 10a StGG). Eine Klärung dieser Frage etwa durch die Rechtsprechung des Verfassungsgerichtshofes steht noch aus. Damit in Zusammenhang steht schließlich die Frage, ob und inwieweit andere grundrechtliche Gewährleistungen neben dem Schutz des Fernmeldegeheimnisses im Einzelfall Relevanz erlangen und eingreifen können.

In diesem Lichte darf die Thematik der Überwachung moderner Telekommunikationsmittel bzw -wege ohne Übertreibung als Herausforderung für den Bürger und seine (parlamentarischen) politischen Vertreter bezeichnet werden. So

kriminalamt, *Ernst Österreicher*, zitiert nach heise online news 15.1.2008 - Ranghoher Polizist verteidigt österreichisches Sicherheitspolizeigesetz (http://www.heise.de/newsticker/Ranghoher-Polizist-verteidigt-oesterreichisches-Sicherheitspolizeigesetz-/-meldung/101778, abgerufen am 9.4.2008).

44 Vgl dazu auch die Legaldefinition in § 92 Abs 3 Z 5 iVm Z 7 TKG 2003.

45 Vgl wieder die Quelle in FN 43.

46 Vgl ebenda.

47 Vgl ebenda.

gesehen bedürfen manche im Zuge der öffentlichen Debatte getätigte Wortmeldungen einer besonders kritischen Aufnahme.

Ziel dieses Beitrages ist es einmal, die Reichweite der seit dem 1. Jänner 2008 bestehenden sicherheitsbehördlichen Eingriffsbefugnisse auf dem Felde der Telekommunikation möglichst genau herauszuarbeiten und den Unterschied zur früheren Rechtslage zu verdeutlichen. Zugleich soll unter Berücksichtigung der im Vorabschnitt skizzierten öffentlichen Diskussion exkursorisch die Erforderlichkeit und Eignung der Instrumente zur Erreichung der angestrebten Ziele hinterfragt werden.

Auf dieser Grundlage können sodann auch (vorläufige) Einschätzungen der Verhältnismäßigkeit der aus den Befugnissen im konkreten Einzelfall jeweils (potentiell) resultierenden Grundrechtseingriffe vorgenommen werden. Für die Beurteilung der Verfassungskonformität der den Sicherheitsbehörden (abstrakt) eingeräumten Auskunftsrechte bedarf es – wie oben angedeutet – schließlich auch der Auseinandersetzung mit dem Gehalt des verfassungsgesetzlichen Fernmeldegeheimnisses.

IV. Der Zugriff auf Kommunikationsdaten nach dem SPG im Überblick

Wie bereits mehrfach angeklungen konnten die Sicherheitsbehörden bei Anfragen an „Betreiber von öffentlichen Telekommunikationsdiensten“ bis zum 31. Dezember 2007 im Grunde nur mit ihnen bekannten Telefonnummern oder Namens- bzw Adressdaten von Inhabern von Telefonanschlüssen operieren (§ 53 Abs 3a SPG idF vor BGBl I 2007/114). Zu diesen – hier als erste „Hauptgruppe“ bezeichneten – Auskunftsvarianten, die für Zwecke dieser Untersuchung nachstehend in „Anfragetypen“ untergliedert werden (hier: Anfragetypen 1-3), sind mit dem Inkrafttreten der jüngsten „SPG-Novelle“ eine Mehrzahl weiterer zulässiger Informationsmöglichkeiten auf unterschiedlicher technischer Grundlage hinzugetreten. Gleichzeitig haben sich aber auch die Voraussetzungen für die bereits vor der Novelle bestehenden Anfragemöglichkeiten geändert (dazu gleich unten in Abschn B.1.a.1 und B.1.c).

Gänzlich neu ist die ausdrückliche Ermächtigung der Sicherheitsbehörden, auf Basis von noch zu diskutierenden sog „Nachrichten“ nach IP-Adresse(n) und Zeitpunkt(en), zu denen diese verwendet wurd(e)n sowie – auf Basis ebensolcher Daten – nach Name(n) und Anschrift de/s/r Nutzer(s) zu fragen (§ 53 Abs 3a Z 2 und 3 SPG; „Zweite Hauptgruppe“ - Anfragetypen 4 und 5). Da es hier nicht um Anfragen an Anbieter „klassischer“ Sprachtelefondienste, sondern an sog Internetdienst(e)anbieter („Internet Service Provider“) geht, die (insbesondere) dem E-Commerce-Gesetz (ECG)[48] unterliegen, wurde der Kreis der zur Auskunft Verpflichteten folgerichtig von „Betreibern öffentlicher Telekommunikationsdienste“[49] auf „sonstige Diensteanbieter“ iSd § 3 Z 2 ECG erweitert. Erfasst sind damit bspw Anbieter von Internetzugängen („Access-Provider“).

Als „dritte Hauptgruppe“ werden hier schließlich die ebenfalls erstmals im SPG verankerten Auskunftsrechte bezüglich Standortdaten bzw internationale

48 BGBl I 2001/152.

49 Vgl § 53 Abs 3a Satz 1 iVm § 3 Z 1, 3, 9 und 21, § 92 Abs 3 Z 1 TKG 2003.

Mobilteilnehmerkennung (IMSI) von durch die Telefonnummer bestimmten Mobiltelefonen behandelt (§ 53 Abs 3b SPG; Anfragetypen 6 und 7). Adressaten sind hier im Wesentlichen die Betreiber von Mobilfunknetzen.

V. Die Anfragemöglichkeiten der Sicherheitsbehörden im Detail

A. Erste Hauptgruppe: Anfragen auf Basis von Telefonnummer(n), Name(n) und/oder Anschrift(en) oder auf Basis „passiver" Telefonnummer(n) iVm Anrufzeitraum (§ 53 Abs 3a Z 1 SPG)

1. Anfragetyp 1: Frage nach Name(n) und Anschrift(en) auf Basis der Telefonnummer(n)

a) Zum Kreis der Verpflichteten

Nach § 53 Abs 3a Z 1 SPG sind die Sicherheitsbehörden berechtigt, von Betreibern öffentlicher Telekommunikationsdienste und sonstigen Diensteanbietern (gemeint iSd § 3 Z 2 ECG) Auskunft zu verlangen über „Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses […]".

Wie bereits im Vorabschnitt erwähnt, ist die Erweiterung des Kreises der zur Auskunft nach § 53 Abs 3a SPG Verpflichteten auf „sonstige Diensteanbieter" in erster Linie als Ausfluss der Ausweitung der zu beauskunftenden bzw den zulässigen Gegenstand einer Anfrage bildenden Daten auf IP-Adressen zu begreifen (zu den Hintergründen der Ausweitung Näheres unter B.1 nach FN 168). Da sich – wie noch näher dargelegt werden wird - die Z 1 des § 53 Abs 3a SPG primär auf die dem TKG 2003 unterfallende Sprachtelefonie bezieht, kommen als Auskunftsverpflichtete bezüglich des Anfragetyps 1 in der Praxis freilich in aller erster Linie die Betreiber öffentlicher Telefondienste[50], dh Festnetz- oder Mobilfunkanbieter, in Betracht. Allerdings treten in jüngerer Zeit neben den Telefonnetzbetreibern heute auch Anbieter von über das Internet abgewickelter Sprachtelefonie auf (sog „Voice over IP [VoIP]-Dienste").[51] Je nach Umfang ihres Angebotes sind solche Anbieter entweder als „Dienst in der Informationsgesellschaft" iSd § 3 Z 2 ECG (etwa im Fall einer auf Internet-Nutzer beschränkte Vermittlung ohne Weiterschaltungsfunktion zu Anschlüssen des öffentlichen Telefonnetzes [engl: „Public Switched Telephone Network" - PSTN]; sog „Internet Only Voice Service") oder aber auch als „öffentlicher Telefondienst" iSd § 3 Z 16 TKG 2003 (Internet Voice Service mit Gateway-Funktionalität ins PSTN; „PSTN-Interconnected VoIP") einzustufen.[52] In beiden Fällen greift künftig die Auskunftspflicht des § 53 Abs 3a Satz 1 Z 1 SPG ein.

---

50 Zum Begriff siehe § 3 Z 1 iVm Z 16 TKG 2003.

51 Siehe etwa den Anbieter Skype (http://www.skype.com/intl/de/). Näheres zur technischen Funktionsweise unten vor und nach FN 124.

52 Vgl in diesem Sinne *RTR – Rundfunk & Telekom Regulierungs-GmbH,* Vorläufige regulatorische Einstufung von öffentlich angebotenen Voice Over IP Diensten in

b) Zulässige Anfragezwecke

• *Vergleich zur bisherigen Rechtslage*

Sehr wohl geändert haben sich mit Jahresbeginn 2008 allerdings die Zwecke, für welche Anfragen auf Basis einer Telefonnummer gestellt werden dürfen. Nach der „alten" Fassung des § 53 Abs 3a SPG waren die Sicherheitsbehörden dazu berechtigt, wenn sie die Auskunft „als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz (dh dem SPG) übertragenen Aufgaben benötig(t)en".[53] Die den Sicherheitsbehörden durch das SPG übertragenen Aufgaben bestehen im Kern in der sog „Sicherheitspolizei". Letztere definiert § 3 SPG als die „Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit, ausgenommen die örtliche Sicherheitspolizei (Art 10 Abs 1 Z 7 B-VG)," und die „erste allgemeine Hilfeleistungspflicht".[54]

Als der zentrale Begriff des ersten Teiles dieser Liste ist die „öffentliche Sicherheit" anzusehen. Die Aufrechterhaltung Letzterer umfasst nach § 20 SPG wiederum „die Gefahrenabwehr, den vorbeugenden Schutz von Rechtsgütern, die Fahndung, die kriminalpolizeiliche Beratung und die Streitschlichtung". Zu beachten ist, dass den Sicherheitsbehörden gem § 21 Abs 1 SPG nicht nur die Abwehr „allgemeiner Gefahren" in Form „gefährlicher Angriffe"[55] oder „krimineller Verbindungen"[56] oder in engem zeitlichen Zusammenhang mit der angestrebten Verwirklichung einer gerichtlich strafbaren Handlung stehenden „Vorbereitungshandlungen"[57] obliegt. Vielmehr sind die Sicherheitsbehörden gem § 21 Abs 3 SPG auch zur „Beobachtung von Gruppierungen" ermächtigt, „wenn im Hinblick auf deren bestehende Strukturen und auf zu gewärtigende Entwicklungen in deren Umfeld damit zu rechnen ist, dass es zu mit schwerer Gefahr für die öffentliche Sicherheit verbundener Kriminalität, insbesondere zu weltanschaulich oder religiös motivierter Gewalt, kommt". Das SPG selbst spricht hier von der sog „erweiterten Gefahrenerforschung".[58] Diese bei ihrer Einführung höchst umstrittene Aufgabe besteht insofern nicht in der „Gefahrenabwehr", sondern ist dem Gebiet der sog Prävention zuzuordnen. Grundlage für ein Tätigwerden ist hier nicht eine konkrete Gefahr für bestimmte Rechtsgüter, sondern im Grunde die bloße Hypothese, dass es irgendwann zu einer solchen kommt bzw kommen könnte. Wenn überhaupt, kann insofern höchstens nur von einer „abstrakten Gefahr", die von einer Gruppe ausgeht, gesprochen werden. Ein strafrechtlich relevantes Verhalten Einzelner liegt bei einer solchen Sachlage typischerweise nicht vor.

Zur letzten in § 3 SPG genannten sicherheitspolizeilichen Aufgabe, nämlich der „ersten allgemeinen Hilfeleistungspflicht", ist auszuführen, dass diese nach § 19 Abs 1 iVm Abs 2 SPG darin besteht, im Falle, dass Leben, Gesundheit,

---

Österreich (Juli 2004) 2 f sowie *dies,* Richtlinien für Anbieter von VoIP Diensten. Version 1.0 (Oktober 2005) 3 ff (7); Näheres bei *Gschweitl/Langmantel/Reichinger,* Voice over IP - Rechtliche Einordnung eines neuen Konzeptes, MR 2005, 503.

53 Vgl § 53 Abs 3a Satz 1 SPG idF vor BGBl I 2007/114.

54 Vgl als Überblick *Demmelbauer/Hauer,* Sicherheitsrecht (2002) Rz 115 ff.

55 Vgl § 16 Abs 1 Z 1 SPG.

56 Vgl § 16 Abs 1 Z 2 SPG.

57 Vgl § 16 Abs 3 SPG.

58 Vgl wieder § 21 Abs 3 SPG.

Freiheit oder Eigentum von Menschen „gegenwärtig gefährdet“ sind oder eine solche gegenwärtige Gefährdung „unmittelbar bevorsteht“, festzustellen, ob eine solche tatsächlich vorliegt und zutreffendenfalls die Gefahrenquelle festzustellen und für unaufschiebbare Hilfe zu sorgen.

Insgesamt zeigt sich also, dass die nach „alter“ Rechtslage bestehende Anknüpfung der hier interessierenden Auskunftsbefugnis an die durch das SPG übertragenen Aufgaben bedeutete, dass die Sicherheitsbehörden unter dem Gesichtspunkt des Anfragezwecks im Prinzip keinen spezifischen Beschränkungen unterworfen waren. Lediglich die „Wesentlichkeit“ („wesentliche Voraussetzung […]“)[59] der angefragten Informationen für die Erfüllung der weiten Aufgabe „Sicherheitspolizei“ hätte eine Rolle spielen können. Angesichts der relativen Unbestimmtheit des Passus „wesentliche Voraussetzung“ kam den Behörden naturgemäß in der Praxis ein nicht zu unterschätzender Ermessensspielraum zu. Auf die Frage der korrekten Auslegung dieses Kriteriums wird noch später im Kontext der Behandlung der geltenden Rechtslage eingegangen.

- *Zum Kriterium der „konkreten Gefahrensituation“*

– Auslegungsfragen

Die vorstehend skizzierte, bis Jahresbeginn 2008 gegebene relative Weite der Anfragebefugnis der Sicherheitsbehörden gegenüber Betreibern öffentlicher bzw öffentlich zugänglicher Telefondienste wurde nun mit Inkrafttreten der jüngsten SPG-Änderungen in einem nicht unwesentlichen Punkt reduziert: Das Auskunftsrecht nach § 53 Abs 3a Z 1 SPG besteht nur, „wenn bestimmte Tatsachen die Annahme einer konkreten Gefahrensituation rechtfertigen und sie diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben benötigen“.

Negativ formuliert bedeutet dies auf den ersten Blick, dass Sicherheitsbehörden Namens- bzw Adressdaten zu einer bestimmten Telefonnummer bei Telefondiensteanbietern nicht mehr für die Wahrnehmung sämtlicher ihnen nach dem SPG übertragenen Aufgaben ermitteln dürfen. Positiv formuliert könnte man zum Schluss kommen, dass den Sicherheitsbehörden die Anfrage für Zwecke der Abwehr von konkreten Gefahren und im Falle, dass es sich bei einer solchen um eine „gegenwärtige“ oder „unmittelbar bevorstehende“[60] handelt, auch für Zwecke der ersten allgemeinen Hilfeleistungspflicht offen steht. Aus dem Rückgriff auf den Passus „konkrete Gefahrensituation“ in § 53 Abs 3a Satz 1 SPG iVm den oben zur sog erweiterten Gefahrenerforschung iSd § 21 Abs 3 SPG (Stichwort „abstrakte Gefahr“) getätigten Ausführungen scheint sich zunächst zu ergeben, dass jedenfalls Letztere keinen legitimen Anfragezweck mehr darstellen kann. Dem ua für die Beobachtung und die Analyse von Gruppen am extremen Rand des politischen Spektrums mit Potential zu verfassungsgefährdenden Aktivitäten zuständigen Bundesamt für Verfassungsschutz (BVT) würden damit bisher zur Verfügung stehende Befugnisse entzogen.

59 Vgl wieder § 53 Abs 3a Satz 1 SPG idF vor BGBl I 2007/114.

60 Vgl in diesem Sinne wieder die Definition der ersten allgemeinen Hilfeleistungspflicht in § 19 Abs 1 und 2 SPG.

Der Passus „konkrete Gefahrensituation“ bedarf jedoch – wie schon die öffentliche Diskussion gezeigt hat[61] – der näheren Betrachtung. Da dieses Kriterium erst im Zuge eines Abänderungsantrages[62] im Parlament eingefügt wurde und dessen Begründung auf diesen Umstand nicht eingeht, fehlen Anhaltspunkte unmittelbar aus der „Entstehungsgeschichte“ der Norm. Das SPG selbst verwendet – von § 53 Abs 3a Satz 1 einmal abgesehen – nur an einer einzigen weiteren Stelle den Begriff „Gefahrensituation“, uzw in § 28a. Dort freilich ohne das Adjektiv „konkret“ und ohne die Gefahrensituation näher zu umschreiben, weshalb keine verwertbaren Rückschlüsse für den hier zu beurteilenden Fall gezogen werden können. Es ist insofern erforderlich, nachstehend eigene (vorläufige) Hypothesen über den Norminhalt zu entwickeln.

So könnte man etwa die Meinung vertreten, es müsse sich dabei um eine „gegenwärtige“ (Bsp: Bedrohung einer Person mit einer Waffe) oder zumindest unmittelbar bevorstehende gegenwärtige Gefahr handeln (Bsp: „Hinweis auf Täter, der kurz vor dem Eintreffen am Ort des geplanten Überfalls ist“; „volltrunkene Person setzt sich ans Steuer eines Kfz und startet“), wie sie von § 19 Abs 1 SPG für das Einschreiten zum Zwecke der ersten allgemeinen Hilfeleistung gefordert wird.[63] Denkbar wäre theoretisch aber auch ein etwas weiteres Begriffsverständnis. Im Sinne des Unterfalls eines gefährlichen Angriffs gem § 16 Abs 3 SPG könnte damit auch noch ein Verhalten, welches noch vor der eigentlichen Tatausführung liegt und in bloßen Vorbereitungshandlungen besteht, sofern sie nur in einem ausreichend engen zeitlichen Konnex zur angestrebten Tatbestandsverwirklichung liegen (Bsp: Beschaffung einer Tatwaffe mit den Ziel demnächst einen Straftatbestand zu verwirklichen), mitumfasst sein.

Nicht übersehen werden darf im vorliegenden Fall freilich die Einbettung des Passus „konkrete Gefahrensituation“ in das „sprachliche Umfeld“. Denn – genau gesehen – wird von § 53 Abs 3a Satz 1 SPG nicht das tatsächliche Vorliegen einer konkreten Gefahrensituation verlangt, sondern nur, „dass bestimmte Tatsachen die Annahme“ einer ebensolchen „rechtfertigen“. Es reicht somit vom Wortlaut her ein „Gefahrverdacht“ aus. Letzterer unterscheidet sich von der tatsächlichen (konkreten) Gefahr dadurch, dass aus der Ex-ante-Sicht des objektiven Beobachters (noch) keine sichere Prognose über den Eintritt eines Schadens für ein Rechtsgut möglich ist.

Das Gegenbeispiel dazu wäre der Täter, der für jedermann in der Umgebung offensichtlich eine Person mit einem gefährlichen Gegenstand oder einer Waffe bedroht („gegenwärtige [konkrete] Gefahr“). Diesfalls liegt – unter Zugrundelegung eines ungehinderten Ablaufes des Geschehens – eine hinreichende Wahrscheinlichkeit eines Schadenseintrittes vor bzw ist geradezu mit an Sicherheit grenzender Wahrscheinlichkeit vom Schadenseintritt auszugehen.

Als Zwischenergebnis ist festzuhalten, dass sich „konkrete Gefahr“ und „Gefahrverdacht“ genau genommen logisch ausschließen. Ein Sachverhalt, der Anlass zu einem Gefahrverdacht gibt, liegt im Vorfeld einer konkreten Gefahr. Daraus folgt weiters, dass die Textierung des § 53 Abs 3a Satz 1 SPG einen

61 Vgl oben nach FN 27.

62 Vgl wieder die Quelle in FN 4.

63 Davon schien etwa der stv. Vorsitzender des Datenschutzrates, Mag. *Maier*, auszugehen (vgl dessen Presseaussendung vom 19.12.2007, OTS0192 5 II 0534 SPK0011 CI Mi, 19.Dez 2007).

inneren Widerspruch aufweist, indem sie nämlich sprachlich das im Vorfeld der konkreten Gefahr angesiedelte Kriterium des Gefahrverdachts eben mit dem Kriterium der konkreten Gefahr verbindet.

In diesem Lichte wird eine Auslegung des § 53 Abs 3a Satz 1 SPG, welche zu einem sinnvollen Ergebnis führt, sehr schwierig. Aus dem Umstand, dass – wie eben dargelegt – ein Gefahrverdacht als (eine) Voraussetzung (neben anderen) für die Inanspruchnahme der Anfragebefugnis bereits ausreichen soll, kann jedenfalls geschlossen werden, dass die „konkrete Gefahrensituation" iS dieser Bestimmung keineswegs mit einer „gegenwärtigen" Gefahr gleichgesetzt werden kann. Am ehesten scheinen dagegen noch Sachverhalte, die unter den Tatbestand des § 16 Abs 3 SPG subsumierbar sind, einschlägig. Genauer Ort und Zeitpunkt der Tat bzw des befürchteten Schadenseintritts müssen hier nicht unbedingt bekannt sein. Schwierig erscheint es diesfalls jedoch, in der Praxis das Vorliegen des Kriteriums des „engen zeitlichen Zusammenhanges mit der angestrebten Tatbestandsverwirklichung", wie dies § 16 Abs 2 SPG verlangt, zu beurteilen.

Auch auf Basis einer derart reduzierenden Auslegung des Passus „konkrete Gefahrensituation" im Sinne der Überwindung der inneren Inkonsistenzen des § 53 Abs 3a Satz 1 SPG erschiene es freilich zu weitgehend, den gesamten Bereich der sog erweiterten Gefahrenerforschung iSd § 21 Abs 3 SPG in den Anwendungsbereich der Norm einzubeziehen.[64]

– Ergänzende systematische Erwägungen

Ergänzend sei an dieser Stelle angemerkt, dass die Einführung des vorstehend diskutierten neuen Kriteriums der „konkreten Gefahrensituation" auch gewisse Probleme aus rechtssystematischer Sicht aufwirft. Die im 2. Hauptstück des 4. Teiles des SPG (§§ 52 ff) geregelte Verwendung personenbezogener Daten „im Rahmen der Sicherheitspolizei" schafft nicht per se Ermächtigungen zur Ermittlung der bezüglichen Daten. Vielmehr stehen die dort vorgesehenen (Teil)Ermächtigungen unter dem Vorbehalt des Eingreifens von Aufgaben nach dem 2. Teil („Aufgaben der Sicherheitsbehörden auf dem Gebiet der Sicherheitspolizei") des SPG iVm Befugnissen auf Grund des 2. Hauptstücks des 3. Teils des SPG („Befugnisse der Sicherheitsbehörden und der Organe des öffentlichen Sicherheitsdienstes im Rahmen der Sicherheitspolizei") im konkreten Einzelfall.[65] Aus der skizzierten inhaltlichen Verschränkung der genannten Teile des SPG folgt, dass jede Einführung neuer Begrifflichkeiten (hier: „konkrete Gefahrensituation") in den 4. Teil des SPG, die sich nicht bereits im 2. Teil bzw im 3. Teil des SPG finden, eine entsprechende Angleichung letzterer Teile nach sich ziehen muss. Dies wurde im vorliegenden Fall offenbar verabsäumt.

• *Zum „Wesentlichkeitskriterium"*

Abschließend verbleibt noch, kurz das Teilkriterium „als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Auf-

64 Zu weitgehend daher die Auslegung der Generaldirektion für die öffentliche Sicherheit in ihrem Erlass GZ 94.762/101-GD/08 v 28.1.2008, Seite 2, in dem ausdrücklich auch auf § 21 Abs 3 SPG Bezug genommen wird.

65 Vgl in diesem Sinne wieder § 52 SPG.

gaben benötigen“[66] zu untersuchen. Genau gesehen wiederholt § 53 Abs 3a Z 1 SPG, was als Prinzip bereits in § 52 SPG verankert ist. Nach letzterer, bereits im Vorabschnitt angesprochener Bestimmung dürfen personenbezogene Daten von den Sicherheitsbehörden gem dem 2. Hauptstück („Ermittlungsdienst“) des 4. Teiles („Verwenden personenbezogener Daten im Rahmen der Sicherheitspolizei“) des SPG nämlich nur verwendet werden, „soweit dies zur Erfüllung der ihnen übertragenen Aufgaben erforderlich ist“. Fraglich könnte nun auf den ersten Blick sein, ob die Begriffe „erforderlich“ (§ 52) und „wesentliche Voraussetzung“ (§ 53) synonym zu verstehen sind oder hier eine inhaltliche Nuancierung beabsichtigt ist. Die Regelung des § 53 Abs 3a Z 1 SPG stellt sich – iVm einer jeweils eingreifenden Befugnisregelung des 2. Hauptstücks des 3.Teiles des SPG – letztlich als gesetzliche Ermächtigung zur behördlichen Ermittlung personenbezogener Daten iSd § 1 Abs 2 Datenschutzgesetz 2000[67] (kurz: DSG 2000) und damit zum Eingriff in das Grundrecht der Betroffenen auf Datenschutz dar. Folgerichtig ordnet § 51 Abs 2 SPG unter Vorbehalt abweichender ausdrücklicher Bestimmungen an, dass „auf das Verwenden personenbezogener Daten die Bestimmungen des DSG 2000 Anwendung finden“.

Von Interesse ist deshalb, dass das DSG 2000 selbst als ein Kernprinzip den „Wesentlichkeitsgrundsatz“ enthält. Gem § 6 Abs 1 Z 3 dürfen Daten nur verwendet werden, „soweit sie für den Zweck der Datenanwendung wesentlich sind und über diesen Zweck nicht hinausgehen“. Davon abgesehen ist stets zu beachten, dass „die Zulässigkeit einer Datenverwendung voraussetzt, dass die dadurch verursachten Eingriffe in das Grundrecht auf Datenschutz nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln erfolgen“.[68] Mit anderen Worten: Die Verhältnismäßigkeit zwischen angestrebtem Ziel und Mitteleinsatz muss gewahrt bleiben. Für das SPG wiederholt diesen Grundsatz im gegebenen Kontext § 51 Abs 1, wonach die Sicherheitsbehörden „beim Verwenden (Verarbeiten und Übermitteln) personenbezogener Daten die Verhältnismäßigkeit (§ 29) zu beachten haben“.

§ 6 Abs 1 Z 3 DSG 2000 kann nun als direkte Umsetzung des Art 6 Abs 1 lit c der EG-Datenschutzrichtlinie (95/46/EG)[69] gesehen werden. Dort wird festgelegt, dass personenbezogene Daten für die Zwecke, für die sie erhoben und/oder weiterverarbeitet werden, „erheblich“ sein müssen „und nicht darüber hinausgehen“ dürfen. „Erheblich“ wiederum ist im gegebenen Kontext bedeutungsgleich mit „wichtig“ bzw „erforderlich“. Daraus folgt, dass anstelle von „Wesentlichkeitsgrundsatz“ ohne weiteres auch von „Erheblichkeits- oder Erforderlichkeitsgrundsatz“ gesprochen werden kann und insofern § 52, wie auch § 53 Abs 3a Satz 1 SPG, als bereichsspezifische Ausprägungen des § 6 Abs 1 Z 3 DSG 2000 begriffen werden können. Die Überlegungen zum Wesentlichkeitsgrundsatz nach dem DSG 2000 sind somit ohneweiters auf die Auslegung des „Wesentlichkeitskriteriums“ in § 53 Abs 3a Satz 1 SPG übertragbar.[70]

66 § 53 Abs 3a Satz 1 letzter Satzteil SPG.

67 BGBl I 1999/165.

68 Vgl § 7 Abs 3 und § 1 Abs 2 letzter Satz DSG 2000. Vgl dazu auch DSK 14.9.2001, K120.705/010-DSK/2001.

69 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 ABl L 281, 31 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

70 Vgl in diesem Sinne DSK 21.06.2005, K121.009/0010-DSK/2005.

Die Frage der Einhaltung des Wesentlichkeitsgrundsatzes muss für jede Ermittlungshandlung gesondert beurteilt werden. Jedenfalls dann, wenn überschießend ermittelt wird (Bsp: alle in privaten Aufzeichnungen eines Verdächtigen, die dieser bei sich führt, enthaltenen Telefonnummern werden unterschiedslos zwecks Klärung der vollständigen Namen beim Telefonbetreiber angefragt) oder nicht das gelindeste Mittel eingesetzt wird (bspw Befragung des Betroffenen selbst), werden Daten ermittelt, die nicht „wesentlich" zur Aufgabenerfüllung sind.[71]

c) Von der Anfragebefugnis erfasste Datenarten

Nach § 53 Abs 3a Z 1 kann Auskunft „über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses" verlangt werden. Diese bereits seit der SPG-Novelle 1999 bestehende Formulierung wurde von den Änderungen ab 1. Jänner 2008 nicht berührt. Mögen die zu beauskunftenden Datenarten auf den ersten Blick auch unproblematisch erscheinen, so bereiten einige davon bei näherer Betrachtung doch erhebliche Auslegungsschwierigkeiten.

- *„Namen und Anschrift"*

Keine wirklichen Probleme bereiten die der Allgemeinsprache entnommenen Begriffe „Namen" und „Anschrift". Gemeint ist/sind im gegebenen Kontext (Anfragetyp 1) offenkundig der/die Name(n) des/der Kunden eines Telefondiensteanbieters und deren Wohnadresse(n) bzw Adresse(n) des Anschlusses (Bsp. Büro, Firma). Unter Namen kann – je nach Anschlussinhaber – sowohl der Name einer natürlichen Person als auch einer juristischen Person bzw Firma verstanden werden.

- *„Teilnehmernummer"*

– Problemstellung

Anlass für Diskussionen lieferten dagegen schon vor dem 1. Jänner 2008 die Termini „Teilnehmernummer" und „Anschluss". Schon bald nach der Einführung der Auskunftsbefugnis gem § 53 Abs 3a SPG stellten sich die Sicherheitsbehörden auf den Standpunkt, die Wendung „Teilnehmernummer eines bestimmten Anschlusses" berechtige sie nicht nur zur Auskunft über Identitätsdaten unter Vorlage von Telefonnummern, sondern auch unter Vorlage von IP-Adressen. Letztere seien nämlich als „zum konkreten Zeitpunkt der Anfrage statisches Element" zu begreifen, weshalb „kein Unterschied zu statischen Telefonnummern bestehe".[72]

Die Anbieter von Internetdiensten teilten diese Rechtsauffassung zwar nicht und verlangten für die Beauskunftung von Nutzerdaten zu IP-Adressen einen Gerichtsbeschluss auf Grundlage der StPO,[73] gerieten aber unter immer stärkeren Druck der Behörden. Dies führte dazu, dass in der Praxis tatsächlich schon

71 Vgl in diesem Sinne (dort am Beispiel Wohnadressen) etwa DSK 7.6.2005, K121.006/0007-DSK/2005. Als Bsp zulässiger Ermittlungen (am Beispiel Anfertigen einer Fotografie) DSK 21.6.2005, K120.942/0008-DSK/2005. Siehe ergänzend zu Art 6 Abs 1 lit c RL 95/46/EG auch Erwägungsgrund 28 dieser RL.

72 Übereinstimmende Auskunft der Rechtsabteilungen von Telekom Austria und Mobilkom in den Jahren 2002.

73 Damals auf Grundlage von § 149a iVm § 149b StPO.

weit vor dem Inkrafttreten der bezüglichen ausdrücklichen Ermächtigungen im neu gefassten § 53 Abs 3a Z 2 und 3 SPG Auskünfte auf Basis von bzw nach IP-Adressen eingeholt und auch erteilt wurden.[74] Für die Öffentlichkeit ersichtlich wurde dieser Usus anlässlich der parlamentarischen Behandlung der hier diskutierten Bestimmungen im Dezember 2007. Die mittels Abänderungsantrag im Plenum des Nationalrates vorgenommene Ausweitung der Datenkategorien auch auf IP-Adressen wurde ebendort nämlich damit begründet, dass diese „den Sicherheitsbehörden zur Abwehr gefährlicher Angriffe oder zur Erfüllung der ersten allgemeinen Hilfeleistungspflicht bereits jetzt zugänglich gemacht wurden". „Nach den erhobenen Unterlagen" handle es sich „um Abfragen in der Größenordnung von etwa 1000 Anfragen pro Jahr".[75]

Mit der nunmehr erfolgten ausdrücklichen Regelung der Frage der Beauskunftung anhand / von IP-Adressen in § 53 Abs 3a Z 2 und 3 SPG stellt sich die Frage der Subsumierbarkeit von IP-Adressen unter § 53 Abs 3a Z 1 SPG auf den ersten Blick zwar nicht mehr. Dennoch verdient diese Frage aus zwei Gründen eine kurze Analyse. Erstens berührt die vorhin angesprochene Praxis vor dem 1. Jänner 2008 – je nachdem, wie die Auslegung durch die Sicherheitsbehörden qualifiziert wird – potentiell Grundfragen der Rechtsstaatlichkeit. Und zweitens könnte der Frage des Verständnisses des Passus „Teilnehmernummer eines bestimmten Anschlusses" insofern Relevanz zukommen, als man in der Praxis versucht sein könnte, § 53 Abs 3a Z 1 SPG gewissermaßen als Auffangtatbestand für Sachverhalte heranzuziehen, die sich nicht ohne weiteres unter § 53 Abs 3a Z 2 SPG subsumieren lassen. Dies ist insofern nicht ganz abwegig, als ein Auskunftsersuchen aufgrund letzterer Norm voraussetzt, dass eine „bestimmte Nachricht" vorgelegt werden kann und eben dieser Begriff wiederum einer engeren oder weiteren Auslegung zugänglich ist (Näheres dazu unten in Abschn V.B.5 nach FN 175).

– Argumente aus dem Zusammenspiel von SPG und TKG

Da das SPG selbst keine Legaldefinitionen von „Teilnehmernummer" bzw „Anschluss" bereit hält, liegt es nahe, einen Blick in das für die Regulierung des Telekommunikationsmarktes einschlägige Materiengesetz, das TKG 2003, bzw – mit Blick auf den Zeitpunkt der Einfügung des § 53 Abs 3a ins SPG mit Wirksamkeit vom 14. August 1999 – in dessen Vorläufer, das bis zum 19. August 2003 gültige TKG 1997[76], zu werfen.

Dass die Autoren des (ursprünglichen) § 53 Abs 3a SPG sich bei der Wahl des Begriffs „Teilnehmernummer" tatsächlich an der Diktion des TKG orientierten, zeigt die Entstehungsgeschichte der Norm. Der ministerielle Erstentwurf vom September 1998[77], mit dem die Einfügung eines neuen Abs 3a in § 53 SPG

74 Vgl dazu etwa den Sachverhalt in DSK 21.06.2005, K121.009/0010-DSK/2005.

75 Vgl die Begründung in AA-89 (XXIII. GP) (FN 4) Seite 3. In diesem Sinne auch die Argumentation von Dr. *Pointner* (FN 41).

76 BGBl I 1997/100.

77 GZ BMI 95.012/473-IV/11/98/Vg vom 22.9.1998: Entwurf eines Bundesgesetzes, mit dem das Sicherheitspolizeigesetz, das Bundesgesetz über die Einführung besonderer Ermittlungsmaßnahmen, das Bundesgesetz über den Schutz vor Straftaten gegen die Sicherheit von Zivilluftfahrzeugen, die Exekutionsordnung und das Tilgungsgesetz geändert werden (SPG-Novelle 1998).

vorgeschlagen wurde, sah nämlich keine Auflistung von zu beauskunftenden Datenarten vor, sondern formulierte (negativ), dass sich die Auskunft (der ersuchten Stellen) „auf die in § 87 Abs 3 Z 4 und 5 TKG [1997] genannten Inhalte zu beschränken hat".[78] § 87 Abs 3 listete in Z 4 als sog „Stammdaten" insbesondere Adresse (lit c) und Teilnehmernummer (lit d) und in Z 5 als sog „Vermittlungsdaten" ua aktive und passive Teilnehmernummern (lit a) sowie die Anschrift des Teilnehmers (lit b) auf. Von der geplanten Regelung wären insofern sowohl Stamm- als auch Vermittlungsdaten erfasst worden. Die massive Kritik im Zuge des Begutachtungsverfahrens durch den Verfassungsdienst im Bundeskanzleramt,[79] aber auch den Datenschutzrat[80], führte letztlich zur Verabschiedung einer Regierungsvorlage (RV), der zufolge sich die Auskunft „auf Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses sowie – mit Zustimmung eines Teilnehmers – auf Teilnehmernummer, Namen und Anschrift in Bezug auf einen bei dem Teilnehmer eingegangenen Anruf zu beschränken hat".[81] Als Adressaten der Auskunftspflicht waren weiterhin Stellen, „die über Stamm- oder Vermittlungsdaten im Sinne des Telekommunikationsgesetzes" verfügen, vorgesehen.[82] Die schließlich im Parlament beschlossene Fassung änderte sich im Zuge der Ausschussberatungen[83] zwar noch gegenüber der RV. Die vorstehend zitierte Auflistung der Datenarten im ersten Satzteil fand aber unverändert Eingang in die Endfassung.[84] Daraus lässt sich unschwer ersehen, dass mit § 53 Abs 3a SPG weder ein spezifisch sicherheitspolizeilicher Begriff der „Teilnehmernummer" noch ein solcher des „Anschlusses" kreiert werden sollte. Vielmehr wurde die bezügliche Terminologie des TKG samt den dahinter stehenden Bedeutungsgehalten übernommen.

Auf Basis dieser Feststellung kann daran gegangen werden, im TKG 1997 nach näheren Anhaltspunkten für die Auslegung der in Frage stehenden Begriffe zu suchen. Das TKG 1997 enthielt seinerseits keine direkte Definition der „Teilnehmernummer" oder des „Anschlusses". Erstere fand sich einmal in der Liste der sog „Stammdaten" aufgeführt.[85] Dies sind jene Daten, die für die Begründung, Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen Benutzer und Anbieter (von öffentlichen Kommunikationsdiensten) oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind.[86] Solche „Teilnehmerverzeichnisse" umfassen grundsätzlich Familienname und Vorname, akademischen Grad, Adresse, Teilnehmernummer des Teilnehmers und, sofern der Teilnehmer dies wünscht, die Berufsbezeichnung.[87] Es handelt sich also hiebei in allererster Linie um herkömmliche Telefonbücher, die Telefonnummern alphabetisch geordneten Namens- bzw Adressdaten zuordnen. Das Ge-

78 Vgl Art I Z 18 des Entwurfs.
79 Vgl etwa GZ BKA 810.057/6-V/3/98 ; Näheres dazu noch unten bei FN 154.
80 Vgl GZ 817.068/3-DSR/98 (Datum der Beschlussfassung).
81 Vgl Art I Z 15 der RV 1479 BlgNR 20. GP, 4.
82 Vgl ebenda.
83 Vgl dazu den Bericht des Ausschusses für innere Angelegenheiten über die Regierungsvorlage (1479 BlgNR) AB 2023 BlgNR 20. GP, 8.
84 Vgl § 53 Abs 3a SPG idF BGBl I 1999/146.
85 Vgl § 87 Abs 3 Z 4 lit a TKG 1997.
86 Vgl § 87 Abs 3 Z 4 TKG 1997 bzw § 92 Abs 3 Z 3 TKG 2003.
87 Vgl § 96 Abs 2 TKG 1997 bzw § 69 Abs 3 TKG 2003.

sagte indiziert, dass „Teilnehmernummer“ iSd TKG mit „Telefonnummer“ gleichzusetzen war/ist.

Verstärkt wurde/wird dieser Eindruck durch den seinerzeitigen § 94 Abs 3 TKG 1997, welcher die Erstellung von sog Einzelentgeltnachweisen regelt. Für Letztere wurde/wird angeordnet, dass „die passiven Teilnehmernummern im Einzelentgeltnachweis nur in verkürzter Form ausgewiesen werden dürfen“, „es sei denn, die Tarifierung einer Verbindung lässt sich nur aus der unverkürzten Teilnehmernummer ableiten“.[88] Und „Anrufe, für die keine Entgeltpflicht entsteht, und Anrufe bei Notrufstellen dürfen nicht ausgewiesen werden“.[89] Auch diese eben zitierten Regelungen lassen sich vernünftigerweise nur so lesen, dass unter „Teilnehmernummer“ eine „Telefonnummer“ verstanden wird.

Die vorhin auf der Basis der seinerzeitigen Rechtslage nach dem TKG 1997 angestellten Überlegungen können sinngemäß auf die Rechtslage nach dem derzeit geltende TKG 2003 übertragen werden. Letzteres enthält ebenfalls keine Legaldefinition des Begriffes „Teilnehmernummer“. Allerdings weicht die gesetzliche Definition der Stammdaten im TKG 2003 in zwei bemerkenswerten Punkten von jener im TKG 1997 ab: Einmal wurde die Datenart „Adresse“ durch den präziseren Begriff „Wohnadresse“ ersetzt,[90] um deutlich zu machen, dass darunter keinesfalls IP- oder E-Mail-Adressen zu verstehen sind.[91] Darüber hinaus wurde die Datenart „Teilnehmernummer“ um die „sonstige Kontaktinformation für die Nachricht“[92] ergänzt. Unter einer solchen Kontaktinformation sind den Erläuterungen zur seinerzeitigen Regierungsvorlage zum TKG 2003 zufolge – in Abgrenzung zur „Teilnehmernummer im Telefoniebereich“[93] – bspw „eine vom Betreiber bereitgestellte Email-Adresse oder sonstige ähnlich individuelle dauerhafte Rufzeichen oder Kennungen […]“ zu verstehen.[94] Anders formuliert: Auch nach dem TKG 2003 spricht alles für ein restriktives Verständnis der „Teilnehmernummer“ iS eines auf die (Sprach)Telefonie gemünzten (technischen) Begriffs, der synonym für „Telefonnummer“ gebraucht wird.

– Argumente aus der (seinerzeitigen) Numerierungsverordung

Begibt man sich – normenhierarchisch gesehen – eine Ebene tiefer, so stößt man auf der Suche nach Anhaltspunkten zur Bestimmung des Inhaltes des Begriffs „Teilnehmernummer“ unweigerlich auf die (bis 11. Mai 2004 in Kraft befindliche) sog Numerierungsverordnung.[95] Diese setzte insbesondere den sog Numerierungsplan für das öffentliche Telekommunikationsnetz fest.[96] Im 2. Abschnitt der Verordnung wurde die „Nummernstruktur“ festgelegt. Die oberste Ebene bildet(e) demzufolge die „Internationale Rufnummer, welche sich aus der Landeskennzahl und der nationalen Rufnummer zusammensetzt“.[97] Unter „Landeskenn-

88 Vgl § 94 Abs 3 Satz 2 TKG 1997 und § 100 Abs 3 Satz 2 TKG 2003.
89 Vgl § 94 Abs 3 TKG 1997 und § 100 Abs 3 letzter Satz TKG 2003.
90 Siehe § 92 Abs 3 Z 3 lit c TKG 2003 im Vergleich zu § 87 Abs 3 Z 4 lit c TKG 1997.
91 So die Erl „Zu Art I“, „Zu § 92“ der RV 128 BlgNR 22. GP, 17.
92 Siehe § 92 Abs 3 Z 3 lit d TKG 2003 im Vergleich zu § 87 Abs 3 Z 4 lit d TKG 1997.
93 So die Erl „Zu Art I“, „Zu § 92“ der RV 128 BlgNR 22. GP, 17.
94 Ebenda.
95 Verordnung BGBl II 1997/416 des Bundesministers für Wissenschaft und Verkehr über die Numerierung (Numerierungsverordnung – NVO).
96 Vgl § 1 leg cit.
97 Vgl § 3 leg cit.

zahl“ (Country Code) ist jene Ziffernfolge zu verstehen, die von der Internationalen Fernmeldeunion (International Telecommunication Union - ITU) Österreich als eindeutiges Ziel im internationalen öffentlichen Telefonverkehr zugewiesen wurde.[98] Die nationale Rufnummer wiederum setzt sich aus „der Regionalkennzahl oder der Bereichskennzahl ohne dem Präfix (Ziffer „0“) und der Teilnehmernummer“ zusammen. Aus eben letzterer Definition (arg: „Ruf“-Nummer) iVm der vorzitierten betreffend die Landeskennzahl (arg: Ziel im öffentlichen „Telefon“-Verkehr) ist erschließbar, dass es sich bei der Teilnehmernummer um die in der Alltagssprache als Telefonnummer bezeichnete „Ziffernfolge handelt, die einem (Telefon)Teilnehmer innerhalb einer Region oder eines anderen Bereiches zugeordnet ist“.[99]

– Argumente aus dem persönlichen Anwendungsbereich des § 53 Abs 3a SPG

Abgesehen von den obenstehenden Argumenten aus dem TKG ließ sich (bis zum 1. Jänner 2008) ein enges Begriffsverständnis der „Teilnehmernummer“ zusätzlich auch aus § 53 Abs 3a SPG selbst begründen: Wie bereits in Abschn V.A.1.a bzw bei der Skizzierung des persönlichen Anwendungsbereiches der Norm erwähnt,[100] werden erst infolge der jüngsten Änderung als Verpflichtete neben den Betreibern öffentlicher Telekommunikationsdienste auch „sonstige Diensteanbieter“ iSd § 3 Z 2 ECG angesprochen. Unter Letztere fallen gem § 3 Z 2 ECG Anbieter von „Diensten der Informationsgesellschaft“. Diese Dienste wiederum sind als „in der Regel gegen Entgelt elektronisch im Fernabsatz auf individuellen Abruf des Empfängers bereitgestellte“ Dienste, wie etwa der Online-Vertrieb von Waren und Dienstleistungen, Online-Informationsangebote , die Online-Werbung, elektronische Suchmaschinen und Datenabfragemöglichkeiten sowie Dienste, die Informationen über ein elektronisches Netz übermitteln (sog „Content-Provider“), die den Zugang zu einem solchen vermitteln (sog „Access-Provider“) oder die Informationen eines Nutzers speichern („Host-Provider“), definiert.[101] Solche Dienste sind strikt von Leistungen zu unterscheiden, die ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze bestehen,[102] eben den „Telekommunikationsdiensten“[103].

Anbieter öffentlicher Telekommunikationsdienste transportieren heute zwar neben Gesprächsinhalten aus der klassischen Telefonie ua IP-Adressen, können aber solche einem bestimmten Nutzer – so sie nicht funktionell gleichzeitig als dessen Access-Provider agieren – gar nicht zuordnen. Als Ansprechpartner von Sicherheitsbehörden, welche Anfragen mit/zu IP-Adressen stellen, kommen reine Telekommunikationsdiensteanbieter insofern gar nicht in Betracht. Wenn nun § 53 Abs 3a SPG vor dem 1. Jänner 2008 ausschließlich auf „Betreiber öffentlicher Telekommunikationsdienste“ abstellte, folgt schon aus deren eben diskutierter spezifischer technischer Funktion, dass diese nur zur Beauskunftung von Telefonnummern, nicht aber IP-Adressen verpflichtet waren/sind. Eine Erweiterung deren

98 Vgl § 2 Abs 1 Z 1 leg cit.
99 Vgl dazu ergänzend die Legaldefinition der Teilnehmernummer in § 2 Abs 1 Z 3 leg cit.
100 Vgl oben bei FN 50.
101 Vgl § 3 Z 1 ECG iVm § 1 Abs 1 Z 2 Notifikationsgesetz 1999 BGBl I 1999/183.
102 Vgl § 3 Z 9 TKG 2003.
103 Vgl § 3 Z 21 TKG 2003.

Auskunftspflicht bzw die Erstreckung des persönlichen Anwendungsbereiches etwa auf (Internet)Diensteanbieter iSd § 3 Z 2 ECG über den Weg einer exzessiven Auslegung der „Teilnehmernummer", wie sie in der Praxis vorgenommen ist, musste demzufolge nicht als sachgerecht, sondern als willkürlich erscheinen.

Nun könnte man aus der mit 1. Jänner 2008 erfolgten Erweiterung des Kreises der auskunftspflichtigen Betreiber im ersten Teil des ersten Satzes des § 53 Abs 3a SPG den Umkehrschluss ziehen und meinen, damit sei legistisch klargestellt, dass unter die Teilnehmernummer in der nunmehrigen Z 1 des § 53 Abs 3a Satz 1 SPG auch IP-Adressen zu subsumieren sind. Um eine inhaltliche Änderung des Begriffs „Teilnehmernummer" auf diesem (subtilen) Wege zu bewerkstelligen, hätte es freilich nicht der zusätzlich erfolgten Einfügung der Z 2 und 3, in denen IP-Adressen explizit angeführt werden, bedurft.

Zugleich ist daran zu erinnern, dass der Erweiterung des Verpflichtetenkreises auf Diensteanbieter iSd ECG auch für die Z 1 des ersten Satzes des § 53 Abs 3a SPG eine gewisse Berechtigung zukommt. Nämlich mit Blick auf die Internet-Telefonie.[104] Auch dort werden von Anbietern Teilnehmerverzeichnisse geführt. Es erscheint daher insgesamt plausibler, anzunehmen, dass aus der hier diskutierten Erweiterung nicht auch auf eine Änderung des Bedeutungsgehaltes der „Teilnehmernummer" geschlossen werden darf.

– Argumente aus § 53 Abs 3a Satz 2 SPG

Anhaltspunkte gegen die Subsumierbarkeit von IP-Adressen unter den Terminus „Teilnehmernummer" ergeben sich auch aus dem Wortlaut des § 53 Abs 3a Satz 2 SPG. Dort heißt es nämlich, dass die Bezeichnung eines „Anschlusses nach Z 1 für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder die Abwehr gefährlicher Angriffe auch durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch" erfolgen kann. Diese Textierung unterstreicht, dass es sich bei der Z 1 des § 53 Abs 3a SPG um eine auf die klassische Sprachtelefonie zugeschnittene Bestimmung handelt.[105]

– Argumente aus der technischen Spezifik von IP-Adressen[106]

Abschließend sei noch kurz auf die zu Beginn der Befassung mit dem Begriff der Teilnehmernummer zitierte Argumentation der Sicherheitsbehörden eingegangen, wonach eine IP-Adresse praktisch mit einer Telefonnummer gleichsetzbar sei.[107] Tatsächlich gibt es eine Parallele zwischen diesen beiden Daten. Beide dienen nämlich dazu, Daten, die über Telekommunikationsnetze transportiert werden, bestimmten Anschlüssen zuzuordnen bzw zuzuleiten (näher zu dieser Funktion unten im „Exkurs II: Anschluss und Adressierung"). Es gibt allerdings auch wesentliche Unterschiede: Telefonnummern werden Teilnehmern bzw Telefonkunden vom Telefondiensteanbieter in der Regel für die gesamte Dauer eines Vertragsverhältnisses zugeteilt und sind insofern gemeinsam mit Namen

104 Siehe dazu auch die Ausführungen zum persönlichen Anwendungsbereich oben bei FN 50. Zu VoIP aus technischer Sicht noch näher unten vor und nach FN 124.

105 Vgl in diesem Sinne bereits DSK 20.7.2007, K121.279/0017-DSK/2007; weiters *Wiederin*, Privatsphäre und Überwachung (2003) 109.

106 Näheres zur technischen Funktionalität der IP-Adressen bei *Einzinger/Schubert/Schwabl/Wessely/Zykan,* Wer ist 217.204.27.214?, MR 2005, 113.

107 Vgl oben bei FN 72.

und Anschrift im entsprechenden Stammdatenverzeichnis gespeichert. Aus Letzterem kann dann insbesondere bei behördlichen Anfragen Auskunft erteilt werden. Einer Heranziehung sonstiger, auf einen konkreten Kommunikationsvorgang bezogener Daten (Vermittlungs- oder Verkehrsdaten) bedarf es nicht.

Grundlegend anders verhält es sich aber bei der Beauskunftung von IP-Adressen. Diese werden einem Internetnutzer von dessen Zugangsdiensteanbieter (Access-Provider) typischerweise lediglich für die Dauer einer Sitzung bzw Verbindung zum Internet zur temporären Nutzung zugewiesen. Man spricht hier in Abgrenzung von – primär Institutionen und Firmen – fest zugewiesenen („statischen") Adressen von „dynamischen" IP-Adressen. Über einen gewissen Zeitraum hinweg gesehen, kann somit eine Vielzahl von Kunden mit ein und derselben (dynamischen) IP-Adresse das Internet nutzen. „Inhaber" bzw Eigentümer von IP-Adressen sind insofern regelmäßig nicht die „Endnutzer", sondern der jeweilige Access-Provider. Zugeordnet werden kann eine bestimmte IP-Adresse mittels Einschau in einschlägige Verzeichnisse[108] daher grundsätzlich nur auf Ebene der Access-Provider. Um nun nachträglich eine Verbindung zwischen einer etwa von der Sicherheitsbehörde vorgelegten IP-Adresse und einem bestimmten Endnutzer herzustellen, muss einmal der genaue Zeitpunkt der Verwendung definiert sein. Darüber hinaus bedarf es der Durchsuchung allenfalls vorhandener Protokolldaten, also sog „Verkehrsdaten" (genauer: „Zugangsdaten"), des Access-Providers, um zu eruieren, welchem Nutzer er die in Frage stehende IP-Adresse zum definierten Zeitpunkt zur Verfügung gestellt hat. Als Verkehrsdaten unterliegen IP-Adressen gem § 93 Abs 1 TKG 2003 dem Kommunikationsgeheimnis.[109] Die Durchführung eines Suchvorganges im vorstehenden Sinn samt Beauskunftung führt im Ergebnis dazu, dass einem Dritten Informationen über Verkehrsdaten (wer hat wann eine IP-Adresse zu welchem Zweck benutzt bzw welche Rechner standen zum gegebenen Zeitpunkt miteinander in Verbindung) zugäng-

108 Vgl dazu das Verzeichnis des für Europa zuständigen regionalen Internetregisters (Regional Internet Registry - RIR), der Réseaux IP Européens Network Coordination Centre (RIPE NCC). Abrufbar unter http://www.ripe.net/db/index.html.

109 Vgl Erl „Zu Art I", „Zu § 92" und „Zu § 99 Abs 3" der RV 128 BlgNR 22. GP, 17, 19; weiters OLG Wien 28.2.2005, 20 Bs 27/05z; OLG Linz 23.2.2005, 9 Bs 35/05v; DSK 29.9.2006, K213.000/0005-DSK/2006; 20.7.2007, K121.279/0017-DSK/2007; auch der EuGH qualifizierte in seinem Urteil v 29.1.2008, Rs C-275/06 - (Promusicae) - RdNr 30 iVm 47 und 48, IP-Adressen als „Verkehrsdaten" iSd Art 2 lit b bzw Art 6 RL 2002/58/EG des Europäischen Parlaments und des Rates v 12.7.2002 ABl L 201, 37 (43 f) über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) idF Art 11 RL 2006/24/EG v 15.3.2006 ABl 2006 L 105, 54 (59). S weiters *Zanger/Schöll*, Telekommunikationsgesetz. Kommentar zum TKG 2003 (2004) § 92 Rz 51; *Einzinger/Schubert/Schwabl/Wessely/Zykan* (FN 106) 116 f, 118; *Wiebe*, Auskunftsverpflichtung der Access Provider - Verpflichtung zur Drittauskunft bei Urheberrechtsverletzungen von Kunden, die an illegalem File-Sharing teilnehmen, Blg zu MR 2005 H 4, 14; nicht überzeugend dagegen *Schanda*, Auskunftsanspruch gegen Access-Provider über die IP-Adressen von Urheberrechtsverletzern, MR 2005, 20, der in der Beantwortung der Frage nach dem Nutzer einer bestimmten IP-Adresse nur eine Stammdatenauskunft sieht, da „nur zwei verschiedene Daten derselben Person" (Identität und IP-Adresse) miteinander verknüpft würden und nicht offengelegt werde, wer mit wem kommuniziert habe; ähnlich *Stomper*, Zur Auskunftspflicht von Internet-Providern, MR 2005, 122.

lich werden und daher in das Kommunikationsgeheimnis des betroffenen Nutzers eingegriffen wird.[110]

Ein weiterer wesentlicher Unterschied zwischen Telefonnummer und IP-Adresse besteht hinsichtlich des potentiellen Aussagewertes der beiden Daten. Nimmt etwa eine Sicherheitsbehörde bei der Anfrage auf eine Telefonnummer Bezug, weiß sie in der Regel nur, „dass" diese bspw von einem observierten Teilnehmer verwendet wurde/wird und möchte die Identität der Person, die Ziel eines Anrufes war oder potentielles Ziel von Anrufen einer observierten Person sein kann, klären. Legt die Behörde dagegen eine IP-Adresse vor, so steht diese in der Regel bereits in Verbindung mit bestimmten Inhalten. Etwa dann, wenn bspw ein Hostprovider zufällig Material (Videos, Fotos) mit strafrechtlich relevantem Inhalt auf einem von ihm betriebenen Rechner („Server") findet und dieses Material unter Mitteilung von IP-Adressen von Nutzern, die dieses Material entweder hochgeladen oder auch nur angesehen haben, den Strafverfolgungsbehörden anzeigt. Diesfalls hätte die Zusammenführung von IP-Adressen und Identitäten von Nutzern für Letztere naturgemäß eine völlig andere Dimension als im Falle einer Rufnummernauskunft. Daraus folgt, dass IP-Adressen sich insofern nicht bloß als Verkehrsdaten darstellen lassen, sondern im Einzelfall (etwa aus der Perspektive des Anfragenden) so stark mit Inhalten verknüpft sein können, dass eine Beauskunftung von Identitätsdaten hiezu funktionell durchaus einer Beauskunftung/Überwachung von Inhaltsdaten nahe kommt.[111]

Zusammenfassend lässt sich festhalten, dass die besseren Argumente nicht nur gegen eine Gleichsetzung von Telefonnummer und IP-Adresse aus technischer Sicht, sondern auch gegen deren rechtliche Gleichbehandlung sprechen.

• *Zum Begriff „Anschluss"*

– Problemstellung

Im Lichte der bereits mehrfach angesprochenen Auslegungspraxis der Sicherheitsbehörden nimmt es nicht weiter wunder, dass auch versucht wurde, nicht nur die Teilnehmernummer, sondern auch den Begriff „Anschluss" in § 53 Abs 3a (alter Fassung) SPG mit einer IP-Adresse gleichzusetzen. Es erscheint insofern von Interesse, auch die Reichweite des Begriffs des Anschlusses einer näheren Betrachtung zu unterziehen.

110 So im Ergebnis auch OLG Linz 23.2.2005, 9 Bs 35/05v; OLG Wien 8.2.2005, 22 Bs 23/05a = MR 2005, 124 (Anm *Daum*) und 28.2.2005, 20 Bs 13/05a; vgl auch *Einzinger/Schubert/Schwabl/Wessely/Zykan* (FN 106) 116, 118. Verfehlt dagegen die Sichtweise des Kommunikationsgeheimnisses durch OGH 26.7.2005, 11 Os 57/05z (11 Os 58/05x, 11 Os 59/05v) = MR 2005, 352 (Anm *Daum*) = ÖJZ 2005/176 (EvBl). Der OGH nimmt dort an, dass die Beantwortung der Frage, welchem Nutzer eine IP-Adresse zu einem Zeitpunkt zugeordnet war, nicht mit einer Rufdatenrückerfassung vergleichbar sei und nicht zur Offenlegung von Kommunikationsverhalten führe. S dazu auch den Erlass BMJ GZ 430.002/15/II.3/05. Ebenfalls unzutreffend: OLG Wien 16.2.2005, 18 Bs 24/05v; 28.2.2005, 17 Bs 19/05a; 7.3.2005, 19 Bs 13/05h = MR 2005, 123 (Anm *Daum*).

111 *Schmidbauer,* Die Metamorphose der Auskunftspflicht, MR 2007, 239, spricht diesbezüglich von „Daten eigener Art, etwa Verkehrsdaten mit Inhaltsbezug".

– Zur Verwendung des Begriffs (Teilnehmer)Anschluss in Normtexten

Zum Terminus „Anschluss“ wurde bereits an anderer Stelle vermerkt, dass das TKG 1997 keine einschlägige Legaldefinition enthielt.[112] Den Zusammenhängen nach (vgl etwa §§ 25 [„Frist zur Erlangung eines Anschlusses an einen Universaldienst“], 87 Abs 3 Z 5 lit h [„Sperren eines Anschlusses“], 93 Abs 4 [„Auswertung von Teilnehmeranschluss nach den von diesem Anschluss angerufenen Teilnehmernummern“], 100 [„Fangschaltung zur Feststellung der Identität (iS von Rufnummer) eines anrufenden Anschlusses“], 101 [„unerbetene Anrufe“]), in welchen das TKG 1997 die Begriffe „Anschluss“ oder „Teilnehmeranschluss“ verwendete, war freilich eine primäre Orientierung an der (Sprach)Telefonie nicht zu übersehen. Damit ist freilich noch nicht die Frage beantwortet, was das TKG 1997 unter „Anschluss“ verstand.

Noch bevor mit der Erlassung des TKG 2003 eine Legaldefinition des Teilnehmeranschlusses (auch) in das TKG Eingang fand, formulierte der Verordnungsgeber, gestützt auf § 89 TKG 1997 in der sog „Überwachungsverordnung“ (ÜVO)[113], den Teilnehmeranschluss als „die technische Einrichtung, die Ursprung oder Ziel der Telekommunikation ist und durch eine Adresse eindeutig gekennzeichnet ist (physikalischer Anschluss), oder die Adresse, die der Teilnehmer einem physikalischen Anschluss fallweise zuordnen kann“.[114] Das sich daran anlehnende[115] und allgemein eine Modernisierung der Begrifflichkeiten auf dem Felde der Überwachung des Fernmeldeverkehrs anstrebende[116] Strafrechtsänderungsgesetz 2002[117] fügte in § 149a StPO („Überwachung einer Telekommunikation“) eine neue Z 3 in dessen Absatz 1 ein. Dieser definierte erstmals auf Gesetzesebene den „Teilnehmeranschluss“ als „die Adresse, welche die technische Einrichtung, die Ursprung oder Ziel einer Telekommunikation ist, kennzeichnet“. Das per 20. August 2003 in Kraft getretene TKG 2003 führte in Form des § 3 Z 20 TKG schließlich eine weitere Legaldefinition des Teilnehmeranschlusses in die Rechtsordnung ein. Diese übernimmt wörtlich die Definition aus Art 2 lit e der sog „Zugangsrichtlinie“[118] der EU. Demnach ist ein „Teilnehmeranschluss“ die „physische Verbindung, mit dem der Netzanschluss in den Räumlichkeiten des Teilnehmers an den Hauptverteilerknoten oder an eine gleichwertige Einrichtung im festen öffentlichen Telefonnetz verbunden wird.“

112 Vgl oben bei FN 85.

113 Verordnung BGBl II 2001/418 idF BGBl II 2003/559 der Bundesministerin für Verkehr, Innovation und Technologie über die Überwachung des Fernmeldeverkehrs (Überwachungsverordnung - ÜVO).

114 Vgl § 2 Z 2 ÜVO.

115 So die Erl „Zu Artikel II“, „Z 4, 7 bis 9, 11 bis 14, 16, 18, 19 und 25 (§§ 149a bis 149c, 149e bis 149h, 149m, 149o, 151 Abs 2, 414a StPO)“ der RV 1166 BlgNR 21. GP, 52.

116 Vgl ebenda, 51.

117 BG BGBl I 2002/134, mit dem das Strafgesetzbuch, die Strafprozessordnung 1975, das Strafvollzugsgesetz, das Suchtmittelgesetz, das Gerichtsorganisationsgesetz, das Waffengesetz 1996, das Fremdengesetz 1997 und das Telekommunikationsgesetz geändert werden.

118 Richtlinie 2002/19/EG des europäischen Parlaments und des Rates vom 7. März 2002 ABl L 108, 7 über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung (Zugangsrichtlinie).

– Exkurs I: Der Anschluss aus technischer Sicht

Die vorzitierten Legaldefinitionen sollen nun an dieser Stelle kurz darauf hinterfragt werden, wie weit sie den technischen Realitäten gerecht werden. Wenn im (Computer- bzw Elektro-)Technikkontext von einem „Anschluss" die Rede ist, dann liegt darin typischerweise eine umgangssprachliche Umschreibung einer sog „Schnittstelle". Mit Letzterer werden im gegebenen Kontext wiederum bestimmte (physikalische) Eigenschaften bezeichnet, die den Austausch von Daten zwischen zwei Geräten, einem Kabel und einem Gerät (bspw Telefonkabel und Telefonapparat) oder einem untergeordneten und einem übergeordneten ganzen System (lokales Netzwerk und regionales Netzwerk) etc ermöglichen. Man könnte eine Schnittstelle insofern als konkreten physikalischen „Übergabepunkt" für Daten begreifen, der sich in (standardisierten bzw genormten) Steckverbindern, Steckdosen, Geräte-Ein- und Ausgängen uä „materialisiert". Im Zusammenhang von Telekommunikationsnetzen spricht man im Übrigen synonym für Schnittstelle(n) auch vom/von „Netzabschlusspunkt(en)".[119]

Neben Hardware-Schnittstellen gibt es aber auch softwareseitige Datenschnittstellen. Letztere sind logische Berührungspunkte in einem Softwaresystem, welche definieren, wie Befehle und Daten zwischen verschiedenen Prozessen und Komponenten ausgetauscht werden. Bestimmte Arten von Softwareschnittstellen ermöglichen etwa die Kommunikation zwischen verschiedenen Programmen („Interprozesskommunikation"/inter-process communication, IPC). Zu dieser Kategorie von Schnittstellen zählen bspw die bekannten Netzwerkprotokolle wie TCP (Transmission Control Protocol)[120] und Http (Hypertext Transfer Protocol).

Für den hier interessierenden spezifischen Fall der Telekommunikation ist im Lichte der obigen Ausführungen zu schlussfolgern, dass (technisch gesehen) strikt insbesondere zwischen (Telekommunikations)Endeinrichtung bzw „Endgerät", Schnittstelle(n) und Übertragungsweg(en) für die bei der Kommunikation anfallenden Signale bzw Daten unterschieden werden muss. Erstere bezeichnet ein technisches Gerät oder Bauteil davon (Festnetztelefonapparat, Mobiltelefon, Faxgerät, usw), welches bei Anschluss an eine Schnittstelle eines öffentlichen Telekommunikationsnetzes Kommunikation ermöglicht.[121] Die Schnittstelle wiederum stellt den physischen Anschlusspunkt (Netzabschlusspunkt/„Telefonanschlussdose") dar, an den ein Endnutzer/Teilnehmer (hier: Telefonkunde) sein Endgerät anschließt und solcherart Zugang zum öffentlichen Telekommunikationsnetz erhält.[122] Als Übertragungsmedien fungieren im Kern nach wie vor Kupferkabel und Glasfaserkabel. Im Mobilfunkbereich dagegen gibt es kein „Medium" im physikalischen Sinne, da die Übertragung mittels elektromagnetischer Wellen arbeitet, welche sich auch im Vakuum ausbreiten.

Die herkömmliche Telefonschnittstelle in Form eines leitungs- und standortgebundenen Festnetzanschlusses tritt heute vielfach zugunsten eines mobilen Telefonanschlusses (Mobilfunkanschlusses) in den Hintergrund. Anstelle der

119 Vgl in diesem Sinne die Definition der „Schnittstelle" in § 2 Z 5 BG BGBl I 2001/134 idF BGBl I 2005/133 über Funkanlagen und Telekommunikationsendeinrichtungen (FTEG). Weiters die Definition des Netzabschlusspunktes in § 3 Z 13 TKG 2003.

120 Näheres dazu noch unten nach FN 169.

121 Vgl dazu die Legaldefinition der „Telekommunikationsendeinrichtung" in § 2 Z 2 FTEG.

122 Vgl dazu die Legaldefinition der „Schnittstelle" in § 2 Z 5 (hier: lit a) FTEG.

„Anschlussdose“ tritt hier eine „Funkschnittstelle“ (auch: „Luftschnittstelle“)[123], die einen drahtlosen Anschluss an das Telekommunikationsnetz ermöglicht. Sie lässt sich – im Gegensatz zur Festnetzschnittstelle – nicht als physikalischen Übergabepunkt, sondern (vereinfacht) primär als ein standardisiertes Verfahren zur Datenübermittlung (mittels elektromagnetischer Wellen durch das Medium Luft) zwischen Endgerät (Mobiltelefon) und der jeweils in Betracht kommenden sog Mobilfunksendeanlage (oder Basis-Sende- und Empfangsstation/„Base Transceiver Station [BTS]“) eines Mobilfunknetzes definieren. Um eine Schnittstelle im vorstehenden zu „aktivieren“, dh eine konkrete Funkverbindung zwischen einem Mobiltelefon und einer Basis-Sende- und Empfangsstation (zwecks „Anmeldung“ als berechtigter Kunde im Mobilfunknetz) aufbauen zu können, muss in das Mobiltelefon des Endnutzers eine sog SIM-Karte (Subscriber Identity Module) eingelegt sein. Dabei handelt es sich um eine Chipkarte, dh einen kleinen Rechner samt Speicher. Über die auf Letzterem gespeicherte sog Mobilteilnehmerkennung („International Mobile Subscriber Identity“, „IMSI“) kann das benützte Mobiltelefon einem bestimmten berechtigten Nutzer (Mobiltelefonkunde) zugeordnet und somit der Zugang zum Mobilfunknetz administriert werden.

Noch weniger Analogien zu einem physikalischen Übergabepunkt bei der Festnetztelefonie weisen Anschlüsse für die sog Internet-Telefonie auf. Sie wird auch als IP-Telefonie (kurz für „Internet-Protokoll-Telefonie“) oder Voice over IP (VoIP) bezeichnet. Im Unterschied zum Fest- oder Mobilnetz werden hier die für die Telefonie typischen Informationen (Sprache und Steuerinformationen) über Computernetzwerke, eben das Internet, übertragen. Die akustischen Signale werden dazu zunächst (via Mikrofon) in analoge und dann in digitale Signale umgewandelt und schließlich zwecks Übertragung über das Internet in Datenpakete unterteilt. Als Endgerät kommen hier sowohl PC iVm einer spezifischen Software („Softphone“) bzw einem Headset, für IP-Telefonie spezialisierte Telefonendgeräte oder über spezielle Adapter für VoIP angeschlossene klassische Telefone in Betracht. Alternativ dazu gibt es bei bestimmten Anbietern noch die Möglichkeit über ein Webportal zu telefonieren. Auf Basis einer Registrierung kann mittels vorhandenem Festnetz- oder Mobiltelefon kommuniziert werden. Vor jedem Gespräch sind auf dem Portal die eigene und jene des gewünschten Gesprächsteilnehmers anzugeben.[124]

Der IP-Telefonanbieter selbst stellt im Unterschied etwa zum Festnetztelefonanbieter keinen „physisch greifbaren“ Netzabschlusspunkt oder sonstige Ausrüstung zur Verfügung. Er betreibt lediglich einen entsprechenden, mit dem Internet verbundenen Rechner (Server), auf dem – vereinfacht gesagt – Teilnehmerkennungen in einer Weise verarbeitet werden, die gewährleisten, dass die über das Internet übertragenen Gesprächs- bzw Vermittlungsdaten den Weg vom Anrufer zum Angerufenen und umgekehrt finden. Dazu muss die jeweils aktuell sowohl vom Anrufenden als auch vom Angerufenen verwendete (dynamische) IP-Adresse auf dem Rechner des IP-Telefonanbieters unter einem entsprechenden Benutzernamen (dazu gleich unten)) hinterlegt sein. Diese Hinterlegung erfolgt jeweils beim Aufbau einer Verbindung zwischen dem vom Nutzer verwendeten Endgerät und dem Server des IP-Telefonanbieters. Letzterer leitet anläss-

123 Vgl dazu § 2 Z 5 lit b FTEG.

124 Vgl dazu etwa die Anbieter Jajah (http://www.jajah.com/) oder Nikotel (http://www.nikotel.de/index.html).

lich eines Anrufes eines Teilnehmers den Verbindungswunsch an das Endgerät des Angerufenen weiter. Im Falle dessen Empfangsbereitschaft erfolgt via Server des IP-Telefonanbieters eine entsprechende Rückmeldung an das Endgerät des anrufenden Teilnehmers. Als Ergebnis ertönt beim Angerufenen ein entsprechendes Anrufsignal, beim Anrufenden ein Freizeichen. Veranlasst wird der Verbindungsaufbau jeweils durch Eingabe der gewünschten Rufnummer auf einer Webseite des Betreibers.

Zu beachten ist nun, dass der Server des IP-Telefonanbieters primär die eben skizzierte sog „Signalisierungsleistung", dh den Auf- und Abbau von Telefonrufen (Rufsteuerung) unter Einsatz eines bestimmten Protokolls (= technischer Standard zum Datenaustausch) erbringt. Die Übertragung der eigentlichen Gesprächsinhalte (Sprachkommunikation) wird dagegen nicht über den Server des IP-Telefonanbieters, sondern auf Basis eines eigenen Protokolls (idR des sog „Real-Time Transport Protocol" [(RTP]) direkt über das Internet zwischen den Endgeräten abgewickelt.

Um Zugang zum Server eines IP-Telefonanbieters zu erhalten, bedarf es eines (mit einem Benutzerkonto [„user account"] verbundenen) Benutzernamens („user name") und eines Kennwortes (auch „Passwort" oder „Losungswort"; engl: „password"). Werden diese korrekt eingegeben, erkennt der Server den Nutzer als „zugangsberechtigten" Teilnehmer und schaltet im Fall eines gewünschten Anrufes – im übertragenen Sinne – eine „Leitung" frei. Um überhaupt Zugang zum Internet und damit zur Webseite bzw zum Server des IP-Telefonanbieters zu erhalten, ist wiederum ein Vertrag mit einem Access-Provider erforderlich.

Fragt man nun im Kontext der IP-Telefonie nach der Bedeutung des „Anschlusses" im hier interessierenden Sinne, so kann auf Basis der obigen Ausführungen allgemein geschlussfolgert werden, dass hier bestenfalls von einem „virtuellen" Anschluss gesprochen werden kann. Dieser manifestiert sich definitiv nicht in einem physikalischen Übergabepunkt. Vielmehr kann er beschrieben werden als Zusammenspiel von durch einen IP-Telefondiensteanbieter vergebene und verwaltete Nutzerdaten (Benutzernamen, Kennwort, Rufnummer) mit einer nur im Falle der konkreten Nutzung einbezogenen (dynamischen), von einem Access-Provider bereitgestellten IP-Adresse, uzw auf der Grundlage bestimmter technischer Übertragungsverfahren für die Signalisierung; dies alles jeweils unter Rückgriff auf einen Internetzugang.

Fernkommunikation über das Internet findet heute nicht nur über Sprachtelefonie, sondern auch mittels sog Instant-Messaging-Programmen wie ICQ (Homophon für „I seek you"; dt: „Ich suche dich") oder MSN (Web) Messenger statt. Mit diesen können – auf Basis eines spezifischen Übertragungsprotokolls – am PC als Texte erstellte Nachrichten in Echtzeit zwischen registrierten Nutzern über das Internet ausgetauscht werden (sog „Chatten"). Voraussetzung ist – abgesehen von einem Zugang zu Internet, etwa auch von einem Internet-Café aus – die Installation eines sog Client (Programm zur automatisierten Aufnahme einer Verbindung mit einem bestimmten Server) am benutzten PC sowie eine Registrierung, bei der man eine Identifizierungsnummer bzw Benutzernamen samt Passwort erhält. Im Unterschied etwa zum Austausch von E-Mail-Nachrichten, die auf speziellen Mail-Servern zum Abruf bereit gehalten werden, geschieht der Datenaustausch im Rahmen der Instant-Messaging ohne Zeitverzögerung, direkt von Nutzer zu Nutzer. Ähnlich wie bei der Internet-Telefonie kann ein „Anschluss" hier wiederum als Kombination aus den auf dem Server des Dienstean-

bieters gespeicherten Nutzerdaten, temporärer IP-Adresse und jeweils erforderlichen technischen Rahmenbedingungen (Protokollstandard, Internetzugang) definiert werden.

Wiewohl im Fokus des § 53 Abs 3a Z 1 SPG die Sprachtelefonie steht, soll aus Gründen des besseren Gesamtverständnisses der in § 53 insgesamt angesprochenen Eingriffsermächtigungen an dieser Stelle noch kurz auf „Anschlüsse" an das Internet im Allgemeinen eingegangen werden. Für einen leistungsfähigen Zugang zum Internet als solchem (Stichwort „Breitband") über eine feste Leitung stehen dem Durchschnittskunden heute technisch gesehen im Wesentlichen Anschlüsse via ADSL („asymmetrischer digitaler Teilnehmeranschluss", engl: „Asymmetric Digital Subscriber Line") oder Kabelfernsehnetz zur Verfügung. Hiebei wird in ersterem Falle ein ADSL-Modem zwischen PC des Nutzers und Festnetztelefonanschluss geschaltet. Dieses Gerät zur Umwandlung von Signalen ermöglicht ua die gleichzeitige Nutzung von Sprachtelefonie und Internetzugang (etwa durch Surfen). Im Falle des Internetzugangs via Kabelfernsehnetz bedarf es ebenfalls eines Modems. Die Aufgabe Letzteren besteht darin, die vom PC kommenden Signale in ein zur Übertragung im Kabelfernsehnetz kompatibles Format umzuwandeln. Beide vorgenannten Modems werden den Kunden vom Access-Provider zur Verfügung gestellt und sind als Teil des von diesem betriebenen (Sub)Netzes zu sehen. Im Netz selbst werden die Modems über eine fest zugewiesene sog „MAC-Adresse" (Media Access Control) identifiziert.

Ähnlich wie bei der klassischen Festnetztelefonie kann bei Breitbandanschlüssen an das Internet die Steckverbindung am jeweiligen Modem, an welches der PC des Nutzers angeschlossen wird, als Anschluss im technischen Sinn verstanden werden.

– Exkurs II: Anschluss und Adressierung

Ergänzend zu den vorstehend diskutierten Komponenten „Endgerät", „Schnittstelle"/ „Anschluss" und „Übertragungsweg" verbleibt noch auf die Frage einzugehen, wie die in einem Telekommunikationsnetz transportierten Daten/Nachrichten jeweils ihre(n) Adressaten finden. Anders gefragt: Wie finden die Sprachsignale beim klassischen Telefon ihren Weg zum Endgerät des Angerufenen? Oder: Wie findet bspw ein bestimmtes Datenpaket im Internet vom Absender zum Empfänger? Die Antwort liegt in der sog „Adressierungsinformation", welche einen „Anschluss" im Netz bezeichnet bzw auffindbar macht.

Beim klassischen Festnetztelefon dient(e) als Übertragungsmedium im Bereich eines Anschlusses („Telefondose") ein verdrilltes Leitungspaar, die sog „Kupfer-Doppelader". Jeder solchen Ader war/ist hier eine bestimmte Nummer zugeordnet. Letztere wiederum wurde/wird im Verzeichnis des Netzbetreibers gemeinsam mit einer bestimmten Telefonnummer, die der Leitungsnummer zugewiesen wurde/wird, gespeichert. Über dieses Verzeichnis lässt sich /ließ sich ein Gespräch zum gewünschten Anschluss weiterleiten bzw der jeweilige Anschlussinhaber namentlich eruieren.

Zur Adressierung eines Mobiltelefonanschlusses dient dagegen grundsätzlich die auf der SIM-Karte gespeicherte IMSI. Diese ist im Verzeichnis der eigenen Kunden des jeweiligen Mobilfunkbetreibers („Home Location Register" – HLR) gemeinsam mit der dem Kunden zugeordneten Mobiltelefonnummer gespeichert. Angemerkt sei allerdings, dass auch mehrer IMSIs einer Mobilrufnummer zuge-

ordnet sein können – etwa wenn der Kunde an mehreren Endgeräten (Autotelefon und Handy) über dieselbe Mobiltelefonnummer erreichbar sein will.

Im Falle der Internet-Telefonie wiederum erfolgt die Zuordnung eines bezüglichen „Gesprächsdatenstroms“ durch eine Verknüpfung von Benutzeranmeldedaten (Authentifizierungsdaten; Benutzername / Passwort) mit einer aktuell verwendeten IP-Adresse. Ähnlich funktionieren Instant-Messaging-Anwendungen.

Internetanschlüsse in Form von Breitbandzugängen schließlich werden über die sog Mac-Adresse, die jeweils einem (dem Nutzer zur Verfügung gestellten) Modem zugeordnet ist, identifiziert.

– Schlussfolgerung zum Verhältnis von „Anschluss“ und „IP-Adresse“

Unter Bezugnahme auf die Ausgangsfrage zeigt sich insgesamt, dass eine (dynamische) IP-Adresse für sich genommen nie einen „Anschluss“ repräsentiert. Vielmehr stellt sie lediglich eine von mehreren Informationen dar, die erforderlich sind, um die Abwicklung konkreter Kommunikationsvorgänge zu ermöglichen.

• *Zwischenergebnis zum Passus „Teilnehmernummer eines bestimmten Anschlusses“ in § 53 Abs 3a Z 1 SPG*

Fügt man nun die auf Ebene der Auslegung der Begriffe „Teilnehmernummer“ und „Anschluss“ gewonnenen Erkenntnisse zusammen, ergibt sich zunächst, dass diese keinesfalls synonym verwendet werden dürfen. Erstere stellt eine Adressierungsinformation dar, die dazu dient, über ein Telekommunikationsnetz übertragene Daten einem bestimmten Anschluss zuzuleiten.

Unter „Teilnehmernummer“ eines bestimmten Anschlusses iSd § 53 Abs 3a Satz 1 Z 1 SPG ist somit (vereinfacht) zu verstehen:

– bei einem klassischen Festnetzanschluss die „Telefonnummer zu einer bestimmten Teilnehmeranschlussleitung“ (in eine Wohnung etc);
– im Falle eines Mobiltelefonanschlusses die „Telefonnummer, die einer oder mehreren Mobilteilnehmerkennung(en) (IMSI) zugeordnet ist;
– im Falle eines Internet-Telefonanschlusses die Telefonnummer, die einem bestimmten Benutzerkonto zugeordnet ist.

Nicht subsumierbar ist dagegen unter „Teilnehmernummer“ eine IP-Adresse. Ebenso wenig besteht eine Gleichsetzbarkeit von „Anschluss“ und (dynamischer) „IP-Adresse“.

d) Zur (äußeren) Form von Anfragen an die Betreiber auf Grundlage von § 53 Abs 3a SPG

§ 53 Abs 3a SPG trifft keinerlei Aussagen zu äußerer Form von darauf gestützten sicherheitsbehördlichen Anfragen oder das allenfalls einzuhaltende nähere Verfahren. Ausdrücklich festgehalten ist lediglich, dass die ersuchte Stelle verpflichtet ist, die Auskunft „unverzüglich und kostenlos zu erteilen“.[125] Auch eine Schriftlichkeit ist nicht ausdrücklich vorgesehen.

125 Vgl § 53 Abs 3a Satz 3 SPG.

- *Überlegungen auf Basis des DSG 2000*

In Ermangelung abweichender Vorgaben greifen allerdings die allgemeinen Datenverwendungsregelungen des DSG 2000 ein. Einschlägig ist im vorliegenden Fall die Bestimmung des § 7 Abs 2 Z 2 DSG 2000. Demnach dürfen Daten insbesondere nur dann übermittelt werden, wenn der Empfänger dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis – soweit diese nicht außer Zweifel steht – im Hinblick auf den Übermittlungszweck glaubhaft gemacht hat […]. Aus der zitierten Textpassage ist für den hier interessierenden Fall zu folgern, dass es den angefragten Betreibern obliegt, die Anfragen der Sicherheitsbehörden nach § 53 Abs 3a SPG auf Plausibilität zu prüfen.

Dass eine solche Prüfung nur auf Basis entsprechender Mindestangaben der Behörden möglich ist, versteht sich von selbst. Dazu wird sich die anfragende Behörde zunächst mit ihrer genauen amtlichen Bezeichnung und einschlägigen Adress- bzw Kontaktdaten sowie dem Namen des zuständigen Sachbearbeiters „vorzustellen" haben. Dies schon deshalb, um bei Zweifeln im Wege der Rückfrage feststellen zu können, ob tatsächlich eine befugte Stelle, dh eine Sicherheitsbehörde iSd § 4 SPG,[126] angefragt hat. Um die Fallbezogenheit nachvollziehen zu können, wird weiters – soweit bereits verfügbar – die korrespondierende Geschäfts-/Aktenzahl anzugeben sein.

Um die Prüfung iSd § 7 Abs 2 Z 2 DSG 2000 vornehmen zu können, muss der Auskunftspflichtige weiters die genaue Rechtsgrundlage, auf welche sich die behördliche Anfrage stützt, kennen. Eine entsprechende Differenzierung anhand der im Rahmen dieses Beitrags vorgestellten Anfragetypen erscheint insofern geboten. Naturgemäß muss die anfragende Behörde weiters jene Informationen mitteilen, auf deren Basis sie entsprechende Auskünfte begehrt (bspw vollständige Telefonnummer). Fraglich erscheint, welche Angaben aus Sicht der Betreiber erforderlich sind, um beurteilen zu können, ob das Kriterium der „konkreten Gefahrensituation" erfüllt ist.

Dies ist insofern keine rein theoretische Frage, als sich im Einzelfall schwierige Abgrenzungsfragen dahin stellen können, ob nicht anstelle des SPG die Strafprozessordnung anzuwenden ist, mit der Konsequenz entsprechend erhöhter Formerfordernisse (Stichwort „richterliche Genehmigung"; vgl § 135 ff StPO). Denkbar wäre eine zumindest stichwortartige Umschreibung des Anlassfalles. Zu bedenken ist in diesem Kontext aber auch, dass den Betreibern im Zuge einer Anfrage im hier interessierenden Sinne Informationen über ihre eigenen Kunden zugänglich werden, die aus der Sicht Letzterer potentiell sehr nachteilig sein können (Verdachtsmomente hinsichtlich strafbaren Verhaltens). Gleichzeitig unterliegen die Betreiber keinen spezifischen, etwa der Amtsverschwiegenheit vergleichbaren Verschwiegenheitspflichten gegenüber den von einer Anfrage betroffenen Kunden. In diesem Spannungsfeld von Interessen bedürfte es insofern möglichst klarer Vorgaben für die Praxis, welche freilich dem Gesetz selbst nicht zu entnehmen sind.

126 Oberste Sicherheitsbehörde ist der Bundesminister für Inneres (§ 4 Abs 1 SPG). Diesem unmittelbar unterstellt sind die Sicherheitsdirektionen in den Ländern, diesen nachgeordnet wiederum sind Bezirksverwaltungsbehörden und Bundespolizeidirektionen (§ 4 Abs 2 SPG).

Erfährt ein betroffener Kunde – auf welchem Weg auch immer – von einer ihn betreffenden Anfrage, steht ihm grundsätzlich ein Auskunftsanspruch nach § 26 DSG 2000 gegenüber übermittelnder und empfangender Stelle und im Verweigerungsfall ein Beschwerderecht nach § 31 Abs 1 DSG 2000 zu. Damit die im Verweigerungsfall bzw Streitfall über die Rechtmäßigkeit einer Auskunftsverweigerung bzw -erteilung gem § 31 Abs 2 leg cit zuständige Datenschutzkommission eine entsprechende Sachverhaltsermittlung und Entscheidung vornehmen kann, bedarf es der Nachvollziehbarkeit von Anfrage und Auskunftserteilung. Dies kann naturgemäß nur durch entsprechende Aufzeichnungen sowohl auf Seite der Sicherheitsbehörde als auch auf Seite des angefragten Betreibers sichergestellt werden. Folgerichtig bestimmt § 14 Abs 2 Z 7 iVm Abs 1 DSG 2000, dass alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, je nach Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit spezifische Datensicherheitsmaßnahmen zu treffen haben, wozu es erforderlichenfalls gehört, „Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können". Die Erforderlichkeit einer Protokollierung im vorliegenden Fall steht im Lichte des oben Gesagten außer Zweifel.

Aus all den vorgenannten Erwägungen ergibt sich im Übrigen, dass als äußere Form einer Anfrage nach § 53 Abs 3a SPG im Grunde nur die Schriftlichkeit in Betracht kommt.[127]

- *Exkurs: Überlegungen zur Zulässigkeit einer Online-Abfrage für Fälle des § 53 Abs 3a Satz 1 Z 1 SPG*

Ein Blick über die Grenzen zeigt, dass etwa in Deutschland die Beauskunftung von Stammdaten gegenüber Sicherheitsbehörden und Gerichten im Rahmen eines sog „automatisierten Auskunftsverfahrens" erfolgt. Dieses ist auf gesetzlicher Ebene entsprechend detailliert geregelt.[128] Der Zugriff auf die Kundendateien der Betreiber erfolgt dabei über den Umweg der gewissermaßen als zentrale „Schnittstelle fungierenden Bundesnetzagentur.[129] Letztere kann die Zulässigkeit der Anfragen aufgrund der Automatisierung gar nicht im Einzelfall prüfen. Gesetzlich ist folglich bestimmt, dass „die Verantwortung für die Zulässigkeit der Übermittlung" von den anfragenden Stellen zu tragen ist[130] und eine Prüfung nur vorgenommen wird, „soweit hierzu ein besonderer Anlass besteht".[131] Zugleich ist jedoch ausdrücklich angeordnet, dass die Bundesnetzagentur „für Zwecke der Datenschutzkontrolle durch die jeweils zuständige Stelle bei jedem Abruf den Zeitpunkt, die bei der Durchführung des Abrufs verwendeten Daten, die abgeru-

127 Anders aber das derzeit in Verwendung befindliche Formular in Anlage 1 zum Erlass GZ 94.762/101-GD/08 der Generaldirektion für öffentliche Sicherheit v 28.1.2008, welches als eine Auskunftsmöglichkeit Fernmündlichkeit vorsieht.

128 Vgl § 112 Telekommunikationsgesetz (dTKG) v 22.6.2004 dBGBl I 1190, zuletzt geändert durch Art 2 des G v 21.12.2007 BGBl I 3198.

129 Vgl § 112 Abs 2 und 4 dTKG.

130 Vgl § 112 Abs 4 Satz 3 dTKG.

131 Vgl § 112 Abs 4 Satz 2 dTKG.

fenen Daten, ein die abrufende Person eindeutig bezeichnendes Datum sowie die ersuchende Stelle, deren Aktenzeichen und ein die ersuchende Person eindeutig bezeichnendes Datum“ zu protokollieren hat. Eine Verwendung der Protokolldaten für andere Zwecke als die Datenschutzkontrolle, also etwa für nachträgliche Auswertungen für nachrichtendienstliche oder sicherheitspolizeiliche Zwecke, wird ausdrücklich für unzulässig erklärt.[132]

Vor diesem Hintergrund erhebt sich die Frage, wie nach aktueller österreichischer Rechtslage eine auf die Stammdatenabfrage iSd § 53 Abs 3a Satz 1 Z 1 SPG beschränkte automatisierte Form der Anfrage, bspw direkt bei den Betreibern, zu beurteilen wäre. Gegen deren Zulässigkeit spricht aus datenschutzrechtlicher Sicht zunächst, dass die Einräumung eines Online-Zugriffs de facto eine Plausibilitätsprüfung iSd § 7 Abs 2 Z 2 DSG 2000 in Echtzeit ausschließen würde und damit das Risiko des Datenmissbrauchs erhöhen und damit auch die Dimension der Eingriffsermächtigung als solche beträchtlich verändern würde. Andererseits kann das im Einzelfall zum Tragen kommende Bedürfnis der Sicherheitsbehörden nach einer möglichst raschen Abklärung von Telefonnummern nicht völlig außer Betracht gelassen werden.

Betrachtet man die von der Auskunft nach § 53 Abs 3a Satz 1 Z 1 SPG betroffenen Datenarten, so wäre im Lichte der Tatsache, dass es sich „nur“ um eine „Stammdatenabfrage“ handelt, eine Einräumung eines Online-Zugriffs mit Blick auf die Anforderungen aus § 1 Abs 2 DSG unter folgenden Bedingungen vorstellbar: 1. müsste insbesondere aus Gründen der Vorhersehbarkeit und Transparenz eine ausdrückliche gesetzliche Grundlage geschaffen werden, 2. wäre eine automatisierte Protokollierung sämtlicher Zugriffe nach Vorbild des § 112 Abs 4 dTKG durch eine von den Sicherheitsbehörden unabhängige Stelle vorzusehen und 3. müsste durch entsprechende gesetzliche Anordnung sichergestellt sein, dass laufend eine Auswertung und datenschutzrechtliche Rechtmäßigkeitsprüfung der anfallenden Protokolldateien auf Basis einer gezogenen Stichprobe durch eine unabhängige Datenschutzbehörde vorgenommen wird. Es liegt auf der Hand, dass hier zusätzliche Kosten anfallen würden. Daraus ergibt sich im Umkehrschluss: Sollten bereits derzeit Online-Zugriffsmöglichkeiten im vorstehenden Sinne für österreichische Sicherheitsbehörden bestehen, würden diese einer gesetzlichen Grundlage entbehren.

e) Resümee und Bewertung aus grundrechtlicher Sicht

Im Ergebnis ist einmal festzuhalten, dass die Sicherheitsbehörden im Rahmen von hier als „Anfragetyp 1“ bezeichneten Fällen bei Betreibern nur Namen und Wohnadresse einer Person erfragen dürfen, der im Stammdatenverzeichnis dieser Betreiber eine bestimmte, von den Behörden zu benennende Telefonnummer zugeordnet ist. Keinen Unterschied macht es, ob es sich um Festnetznummern, Mobilrufnummern oder (fest zugeteilte) Internet-Telefonnummern handelt. Im Lichte der technischen Analogie sind auch Inhaber von Faxnummern zu beauskunften.[133] Nicht zulässig wäre hingegen unter dieser Ziffer die Frage nach Namens- bzw Adressdaten auf Basis einer sog IP-Adresse. Soweit sich die

132 Vgl § 112 Abs 4 Satz 4b und 5 dTKG.

133 So im Ergebnis auch *Hauer/Keplinger*, Sicherheitspolizeigesetz. Kommentar (2005) 601.

Praxis in der Vergangenheit bei solchen Anfragen auf § 53 Abs 3a Satz 1 (alter Fassung) SPG berufen hatte, geschah dies ohne gesetzliche Grundlage.

Auf Ebene der Anfragezwecke wirft die Einfügung des Kriteriums der gerechtfertigten „Annahme einer konkreten Gefahrensituation" Probleme auf. Die aufgezeigte Widersprüchlichkeit des Kriteriums in sich sowie der Ausschluss der Stammdatenauskunft für Zwecke von „Vorfeldermittlungen" durch das Bundesamt für Verfassungsschutz müssen als legistische Fehlleistung qualifiziert werden.

Unter Zugrundelegung der gebotenen restriktiven Auslegung zielt der Anfragetyp 1 lediglich auf die Bekanntgabe von Stammdaten iSd § 92 Abs 2 Z 3 TKG 2003 ab, welche der angefragte Betreiber allein schon durch die Konsultation seines jeweiligen Kundenverzeichnisses (iS eines „Stammdatenverzeichnisses") ersehen kann. Solche Daten unterliegen zufolge der Definition des § 93 Abs 1 TKG 2003 nicht dem (einfachgesetzlichen) Kommunikationsgeheimnis. Auch ein Eingriff in das verfassungsgesetzlich verbürgte Fernmeldegeheimnis (zu dessen Inhalt noch näher unten in Absch V.A.3.e nach FN 150) liegt hier nicht vor.

Die Verwendung der Stammdaten unterfällt allerdings dem Datenschutzgrundrecht nach § 1 Abs 1 DSG 2000. Dies deshalb da Telefonnummern über öffentliche Telefonbücher (von „Geheimnummern" abgesehen) zwar grundsätzlich frei zugänglich sind, in diesen idR aber nur anhand des Familien- bzw Firmennamens, nicht aber auch anhand der Telefonnummer gesucht werden kann. Eine den Geheimhaltungsanspruch ausschließende allgemeine Verfügbarkeit iSd § 1 Abs 1 Satz 2 DSG 2000 liegt insofern nicht vor. Beschränkungen des Datenschutzgrundrechts durch behördliche Eingriffe setzten gem § 1 Abs 2 DSG 2000 eine gesetzliche Ermächtigung voraus, die aus den in Art 8 Abs 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK)[134] genannten Gründen (ua „öffentliche Ruhe und Ordnung", „Verteidigung der Ordnung und Verhinderung strafbarer Handlungen") notwendig ist. Der in § 53 Abs 3a Satz 1 SPG angesprochene Zweck, dh – vereinfacht – die Wahrnehmung der Sicherheitspolizei (zu deren Inhalt siehe oben ab FN 54) lässt sich ohne Schwierigkeit unter die in Art 8 Abs 2 EMRK als zulässig genannten Zwecke subsumieren. Auch bestehen keine Zweifel daran, dass die Sicherheitsbehörden in Verfolgung dieses Zwecks im Einzelfall, wie dies § 53 Abs 3a Satz 1 Z 1 SPG vorsieht, Auskünfte nach Anfragetyp 1 benötigen. Die bezügliche Ermächtigung erscheint somit innerhalb des verfassungsrechtlich zulässigen Rahmens liegend. Probleme stellten sich erst dann, wenn die Sicherheitsbehörden sich Zugang zu Rufnummern auf nicht vorgesehenen Wegen verschafften (bspw illegales Auslesen von Telefonnummern mittels IMSI-Catcher) und dann Identitätsklärungen über den hier interessierenden Weg vornähmen.

2. Anfragetyp 2: Frage nach Telefonnummer(n) auf Basis von Name(n)/Anschrift de/r/s Teilnehmer(s) oder genauer Angaben zur Position eines Festnetzanschlusses

a) Verpflichtete, Zwecke und inhaltliche Reichweite, Form

Wiewohl die textliche Struktur des § 53 Abs 3a Satz 1 Z 1 SPG offenbar nicht explizit auf verschiedene denkbare Auskunftsszenarien abstellt, bereitet es keine

134 BGBl 1958/210 idF BGBl III 2002/179.

besonderen Schwierigkeiten, auch den Anfragetyp 2, dh Fragen anhand von Angaben zur Person oder zu einem bestimmten Anschluss unter diese Norm zu subsumieren.

Hinsichtlich des Kreises der Auskunftspflichtigen kann an dieser Stelle sinngemäß auf die Ausführungen zum Anfragetyp 1 verwiesen werden. Auch hier geht es im Wesentlichen um Anbieter von Sprachtelefonie, sei es in Form von Festnetz- oder Mobilfunkanschlüssen oder virtuellen Anschlüssen für die Internet-Telefonie. Ebenfalls keine Unterschiede bestehen hinsichtlich der zulässigen Zwecke.

Hinsichtlich der Reichweite der zulässigen Anfragen ist anzumerken, dass aus dem Wortlaut (arg: kein Hinweis auf Zulässigkeit der Anfrage mit unvollständige Daten) zu schließen ist, dass die zur Person vorgelegten Angaben ausreichen müssen, um auf Seite des Betreibers einen bestimmten Kunden in dessen Stammdatenverzeichnis zu identifizieren. Vor- und Zuname können hier im Einzelfall unzureichend sein und müssten diesfalls durch Zusatzangaben (Anschrift oder zumindest ungefähre Anschrift) ergänzt werden.

Fraglich könnte bei Anfragetyp 2 wiederum sein, welche Daten – von Namens- und Adressdaten des Inhabers einmal abgesehen – die Behörde vorlegen darf, um dazu vom Betreiber eine Telefonnummer zu erhalten. Legt man die anlässlich der Diskussion der Reichweite der Anfragebefugnisse beim Anfragetyp 1 gewonnenen Erkenntnisse[135] auf den hier interessierenden Fall um, lassen sich nachstehende Fälle unterscheiden:

– Zur Ermittlung einer Festnetznummer könnte die genaue Position des Anschlusses (Wohnungsadresse, sofern nur ein Anschluss vorhanden) hinreichen; kaum verfügen wird die Behörde idR dagegen über die Nummer einer „Kupfer-Doppelader“[136].
– Zur Ermittlung einer Mobiltelefonnummer könnte die Mobilteilnehmerkennung (IMSI) vorgelegt werden. Zugang zu einer solchen könnten die Sicherheitsbehörden allerdings in der Praxis nur über den Weg einer gerichtlich angeordneten Überwachungsmaßnahme nach der StPO erlangen.
– Im Falle eines Internet-Telefonanschlusses könnte die Behörde den Benutzernamen eines VoIP-Kunden vorlegen, sofern schon damit ein bestimmter Kunde eruiert werden kann. Auch dieser Fall ist aber wenig realistisch.

Kein zulässiges Anfragedatum stellt hingegen eine IP-Adresse dar, da sie – wie bereits an anderer Stelle ausgeführt[137] – für sich keine ausreichende Individualisierung eines Anschlusses ermöglicht.

In Bezug auf formale Aspekte der Anfrage ist wiederum auf die analog zum Tragen kommenden Überlegungen unter V.A.1.d ab FN 125 zu verweisen, allerdings mit der Maßgabe, dass die Problematik einer allfälligen automatisierten Abfragemöglichkeit beim Anfragetyp 2 deutlich anders zu sehen ist. Einerseits mit Blick auf die hier als Anfragekriterien (wenngleich eher theoretisch) zusätzlich in Betracht kommende IMSI bzw eine Benutzerkennung. Andererseits stellte der Abruf von (in öffentlichen Verzeichnissen aufscheinenden) Telefonnummern

135 Vgl dazu vor allem die Ausführungen zum Begriff „Anschluss“ und dessen Adressierung etwa ab FN 112 und vor FN 125.
136 Dazu oben im „Exkurs II: Anschluss und Adressierung“ auf Seite 110.
137 Siehe die Schlussfolgerungen zu ebendiesem Exkurs auf Seite 111.

mittels vollständigen Namens- und Adressdaten von vornherein kein Datenschutzproblem dar.

b) Bewertung

Auch hier kann, insbesondere hinsichtlich der grundrechtlichen Implikationen des Anfragetyps 2, sinngemäß auf die Ausführungen unter V.A.1.e nach FN 133 verwiesen werden.

3. Anfragetyp 3: Frage nach Telefonnummer(n) bzw Name(n)/ Anschrift(en) von Anrufer(n) auf Basis einer angerufenen (passiven) Telefonnummer und des Anrufzeitraumes

Gem § 53 Abs 3a Satz 2 SPG kann die Bezeichnung eines Anschlusses nach Z 1 des Satzes 1 leg cit für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder die Abwehr gefährlicher Angriffe auch durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch durch Bezeichnung eines möglichst genauen Zeitraumes und der passiven Teilnehmernummer erfolgen. Dieser, hier als Anfragetyp 3 bezeichnete Auskunftsfall war bereits vor dem 1. Jänner 2008 in § 53 Abs 3a SPG enthalten[138] und blieb bis auf den Passus „eines möglichst genauen Zeitraumes“ unverändert.

a) Zum Kreis der Verpflichteten

Schon mit Blick auf die ausdrückliche Bezugnahme auf ein „(Telefon)Gespräch“ in Satz 2 des § 53 Abs 3a SPG erscheint klar, dass als Adressaten der bezüglichen Auskunftspflicht im Grunde nur Telefondiensteanbieter iSd § 3 Z 16 TKG 2003 in Betracht kommen. Zusätzlich werden aber auch Internet-Telefonieanbieter, die sich auf die Vermittlung zwischen Internetnutzern beschränken und nur deshalb nicht als „öffentliche Telefondienste“ iSd vorzitierten Bestimmung, sondern „nur“ als sonstige Diensteanbieter iSd § 3 Z 2 ECG eingestuft werden,[139] in Betracht kommen.

b) Zulässige Anfragezwecke

Im Vergleich zu den Anfragetypen nach Satz 1 des § 53 Abs 3a SPG fällt bei Satz 2 auf, dass nicht auf die Annahme einer „konkreten“ Gefahrensituation, sondern neben der „Erfüllung der ersten allgemeinen Hilfeleistungspflicht“ (Unterfall 1) auch ganz allgemein auf „die Abwehr gefährlicher Angriffe“ (2. Unterfall) abgestellt wird. Auf den ersten Blick erscheint die Zweckumschreibung in § 53 Abs 3a Satz 2 SPG insofern weiter als jene nach Satz 1 leg cit. Was unter einem gefährlichen Angriff zu verstehen ist, kann § 16 Abs 2 und 3 SPG entnommen werden. Ein gefährlicher Angriff ist demnach die Bedrohung eines Rechtsgutes durch die rechtswidrige Verwirklichung des Tatbestandes einer gerichtlich strafbaren Handlung, die vorsätzlich begangen und nicht bloß auf Begehren eines Beteiligten verfolgt wird, sofern es sich – vereinfacht – um einen Straftatbestand

138 Vgl § 53 Abs 3a Satz 2 SPG idF vor BGBl I 2007/114.
139 Vgl dazu oben bei FN 50.

nach dem Strafgesetzbuch (StGB),[140] nach dem Verbotsgesetz, nach dem Fremdenpolizeigesetz oder nach dem Suchtmittelgesetz (SMG)[141] handelt.[142] Ebenfalls als gefährlicher Angriff ist ein Verhalten zu werten, das darauf abzielt und geeignet ist, eine solche Bedrohung im vorstehenden Sinne vorzubereiten, sofern dieses Verhalten nur „in engem zeitlichen Zusammenhang mit der angestrebten Tatbestandsverwirklichung" gesetzt wird.[143]

Vergegenwärtigt man sich freilich die oben (Abschn V.A.1.b nach FN 59) angestellten Überlegungen zum Gehalt des Passus „wenn bestimmte Tatsachen die Annahme einer konkreten Gefahrensituation rechtfertigen" in § 53 Abs 3a Satz 1 SPG, so relativiert sich der erste Eindruck beträchtlich. Tatsächlich besteht nämlich unter Zugrundelegung der hier vertretenen Auslegung[144] des bezüglichen Passus in Satz 1 weitestgehende inhaltliche Deckungsgleichheit mit den Zwecken nach § 53 Abs 3a Satz 2 SPG.

Der Vollständigkeit halber sei erwähnt, dass sich aus der Textierung der beiden Sätze des § 53 Abs 3a SPG bzw deren inhaltlicher Verschränkung ergibt, dass das sog „Wesentlichkeitskriterium"[145] aus Satz 1 auch für die Zulässigkeit von Anfragen iSd Typs 3 maßgeblich ist.

Als mögliche praktische Anwendungsbeispiele für den Anfragetyp 3 sind Selbstmordankündigungen oder Attentatsdrohungen per Telefon zu nennen. In Ermangelung einer entsprechenden sprachlichen Nuancierung im Gesetzestext muss es sich bei Fällen des Anfragetyps 3 allerdings nicht unbedingt um Fälle einer „unmittelbaren" bzw „gegenwärtigen" Gefährdung handeln.

c) Der Auskunftspflicht unterliegende Daten

- *Die abfragbaren Datenarten*

Eine Spezifik des Anfragetyps 3 kann darin erblickt werden, dass hier stets die gesamte Liste der in § 53 Abs 3a Z 1 SPG genannten Datenarten („Namen, Anschrift und Teilnehmernummer") Ziel des Auskunftsbegehrens der Behörde ist. In den meisten Fällen der Anfragetypen 1 und 2 muss nämlich der anfragenden Stelle typischerweise zumindest eines dieser Elemente bekannt sein.

- *Die zur Anfragebeantwortung verwendeten Daten*

Der wesentliche Unterschied zu den Anfragetypen 1 und 2 besteht beim Anfragetyp 3 darin, dass es sich hier nicht um eine bloße Abfrage von „Stammdaten" iSd § 92 Abs 2 Z 3 TKG 2003 handelt. Anders als bei den erstgenannten beiden Varianten wird ein Anschluss hier nämlich nicht mittels von der Sicherheitsbehörde vorgelegter rein „statischer" Informationen (Telefonnummer, Namen, Anschrift) bezeichnet, mit welchen ein Betreiber bloß sein Kundenverzeichnis konsultieren muss. Vielmehr kann sich die Behörde beim Anfragetyp darauf be-

140 Ausgenommen die Tatbestände nach den §§ 278 („Kriminelle Vereinigung"), 278a („Kriminelle Organisation") und 278b StGB („Terroristische Vereinigung").
141 Ausgenommen Erwerb und Besitz zum Eigengebrauch.
142 Vgl § 16 Abs 2 SPG.
143 Vgl § 16 Abs 3 SPG.
144 Vgl oben nach FN 58.
145 Zu diesem wieder oben nach FN 65.

schränken, grobe Anhaltspunkte für eine sog Rufdatenrückerfassung[146] zu liefern. Zur Bewerkstelligung Letzterer muss der angefragte Betreiber sämtliche Telefonate, die innerhalb eines von der Behörde zu spezifizierenden („möglichst genauen") Zeitraumes an einem durch die Telefonnummer bestimmten Telefonanschlusses eingegangen sind („passive Teilnehmernummer"), feststellen. Technisch kann dies nur unter Rückgriff auf sog Verkehrs- bzw „Vermittlungsdaten" iSd § 92 Abs 2 Z 4 TKG 2003 erfolgen.

Im Zuge der Beantwortung einer Anfrage nach § 53 Abs 3a Z 1 SPG werden den Sicherheitsbehörden auf den ersten Blick zwar nur Stammdaten bekannt gegeben. Genauer betrachtet erschließen sich diesen aber zugleich Verkehrsdaten, nämlich von welchen Anschlüssen aus innerhalb eines bestimmten Zeitraums eine bestimmte (passive) Teilnehmernummer angerufen wurde. Damit kommt es jedenfalls zu einem Eingriff ins einfachgesetzliche Kommunikationsgeheimnis nach § 93 Abs 1 TKG.[147]

- *Zum Kreis der von einer Anfrage Betroffenen („Beauskunfteten")*

Wie bereits erwähnt wird in § 53 Abs 3a Satz 2 SPG seit 1. Jänner 2008 für die zeitliche Eingrenzung eines zu ermittelnden Anrufes nicht mehr die Bezeichnung „des Zeitpunktes", sondern lediglich „eines möglichst genauen Zeitraumes" verlangt. Damit ändert sich die Dimension der Eingriffsermächtigung gravierend: Anstelle der Identifizierung einer bestimmten Zielperson wird potentiell eine unbestimmte Zahl an (unbeteiligten) Telefonteilnehmern in die Rufdatenrückerfassung einbezogen. Wie lange ein Zeitraum sein kann, um noch als „möglichst genau" iSd § 53 Abs 3a Satz 2 SPG gelten zu können, bleibt im Dunkeln. Nicht gefolgt werden kann jedenfalls der in den Erläuterungen zur RV vertretenen Auffassung, wonach diese „aus Gründen der Verhältnismäßigkeit nicht mehr als eine Stunde betragen darf".[148] Ein so langer Zeitraum erscheint insofern unplausibel, als davon auszugehen ist, dass die hier primär interessierenden Anlassfälle (Stichwort „Drohanruf") nach der allgemeinen Lebenserfahrung zu einer sofortigen Veranlassung seitens des Angerufenen führen und somit bestenfalls Minuten bis zur Kontaktierung der Behörde vergehen. Ist eine Sicherheitsbehörde selbst Ziel eines bezüglichen Anrufes, ist schon mit Blick auf deren professionelle Auseinandersetzung mit derartigen Fällen mit einer genauen Dokumentation des Anrufzeitpunktes zu rechnen.

d) Zur Form der Anfrage

Auf Ebene der Frage der äußeren Form von Anfragen nach Anfragetyp 3 stellen sich im Grunde dieselben Herausforderungen wie sie bereits bei Anfragetyp 1

146 Es wird auch von „nachträglicher Rufdatenerfassung" gesprochen (vgl bspw OGH 6.12.1995, 13 Os 161/95; OLG Innsbruck, 13.10.1998, 6 Bs 219/98 ua). Näheres zur Rufdatenrückerfassung (aus Sicht der StPO) bei *Schmölzer*, Rückwirkende Überprüfung von Vermittlungsdaten im Fernmeldeverkehr. Anmerkungen zu OGH 6. 12. 1995, 13 Os 161/95, JBl 1997, 211; *Reindl*, Die nachträgliche Offenlegung von Vermittlungsdaten des Telefonverkehrs im Strafverfahren („Rufdatenrückerfassung"), JBl 1999, 791.

147 Vgl dazu (auf Basis der Vorläuferbestimmung des § 88 Abs 1 TKG 1997) auch OLG Innsbruck, 13.10.1998, 6 Bs 219/98 ua ; OGH 18. 01. 2001, 12 Os 152/00 (12 Os 153/00).

148 Vgl Erl „Zu Art 1 Z 4 (§ 53 Abs 3a)" der RV 272 BlgNR 23. GP, 5.

diskutiert wurden.[149] Mit Blick auf die spezifische technische Seite der Rufdatenrückerfassung kann ein direkter Zugriff durch Sicherheitsbehörden von vornherein nicht in Betracht kommen. Dies würde jedenfalls das einfachgesetzliche Kommunikationsgeheimnis ad absurdum führen.

e) Bewertung aus grundrechtlicher Sicht

• *Überlegungen aus Sicht des Grundrechts auf Datenschutz*

Nicht zuletzt angesichts der potentiell großen Zahl an Telefonteilnehmern, die von einer auf § 53 Abs 3a Satz 2 SPG gestützten Rufdatenrückerfassung betroffen sein können, erscheint die Frage berechtigt, wie in der Praxis ohne unabhängige Kontrolle die von § 1 Abs 2 letzter Satz DSG geforderte Verhältnismäßigkeit des Eingriffs in das Datenschutzgrundrecht der Betroffenen sichergestellt werden soll. Eine bloße Informationspflicht gegenüber dem (de facto nicht ausreichend unabhängigen) Rechtsschutzbeauftragten beim Bundesminister für Inneres[150] erscheint insofern nicht ausreichend.

• *Überlegungen aus Sicht des Fernmeldegeheimnisses*

– Zur Diskussion um die Reichweite des Art 10a StGG

Artikel 10a Abs 1 StGG erklärt, dass das „Fernmeldegeheimnis nicht verletzt werden darf". Ausnahmen davon sind „nur auf Grund eines richterlichen Befehles in Gemäßheit bestehender Gesetze zulässig" (Abs 2 leg cit).

Über die genaue Bedeutung und Reichweite dieser Bestimmung bestehen nach wie vor gravierende Auffassungsunterschiede in Literatur, Judikatur und Staatsverwaltung.

Die Mehrheit der Literaturstimmen vertritt die Auffassung, das Fernmeldegeheimnis iSd Art 10a StGG schütze lediglich Gesprächsinhalte.[151] Begründet wird dies im Wesentlichen aus der Entstehungsgeschichte. Art 10a StGG sei erkennbar aus der älteren Gewährleistung des Briefgeheimnisses heraus entwickelt worden.[152]

Einschlägige Judikatur des Verfassungsgerichtshofes liegt aktuell noch nicht vor. Die ordentliche Gerichtsbarkeit ist jedenfalls bis dato überwiegend von einem

149 Siehe oben bei FN 120.

150 Vgl § 91c Abs 1 Satz 3 SPG.

151 Vgl mwN *Wiederin*, Art 10a StGG, in *Korinek/Holoubek* (Hrsg), Bundesverfassungsrecht (1999) Rz 12 ff und die Nachweise in FN 56 sowie *Grabenwarter*, Verfassung und Informationsgesellschaft, in *Österreichische Juristenkommission (Hrsg)*, Grundrechte in der Informationsgesellschaft (2001) 65 vor FN 60; *Schanda* (FN 109) 19; *Stomper* (FN 109) 119, 120; *Hofer*, datenschutz@internet. Die Privatsphäre im Informationszeitalter (2002) 96 f; *Himberger*, Fernmeldegeheimnis und Überwachung (2004) 57 ff, 62, 63 f, 310; zu den Befürwortern eines auch auf Verkehrsdaten bezogenen Schutzbereiches siehe wieder die Nachweise bei *Wiederin,* Art 10a StGG, in FN 57 und 68 f sowie *Zanger / Schöll* (FN 109) § 93 Rz 8 f; *Einzinger/Schubert/Schwabl/Wessely/Zykan* (FN 106) 116, 118; *Reindl,* Vor §§ 149 a–c StPO, in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur StPO (2005) Rz 9; *Wiebe* (FN 109) 13; *Damjanovic et al*, Handbuch des Telekommunikationsrechts (2006) 243.

152 Vgl *Wiederin* (FN 151) ab Rz 12 ab FN 60.

weiteren Inhalt des Art 10a StGG ausgegangen, welcher auch Vermittlungsdaten umfasse.[153]

Die Praxis der legistisch mit der Frage befassten Bundesministerien war/ist wiederum uneinheitlich. Gerade die „Geschichte" des § 53 Abs 3a SPG demonstriert dies eindrucksvoll.

So äußerte der Verfassungsdienst des Bundeskanzleramtes (kurz: BKA-VD) im Begutachtungsverfahren zum damaligen Ministerialentwurf für die spätere „SPG-Novelle 1999"[154] „schwerwiegende verfassungsrechtliche Bedenken" gegen den darin enthaltenen Vorschlag des BMI, den Sicherheitsbehörden Zugriff auf Verkehrsdaten zu gewähren,[155] ohne gleichzeitig die Einholung einer richterlichen Ermächtigung vorzusehen.[156] In den an eine richterliche Genehmigung gebundenen parallelen Ermächtigungen in der damals gültigen StPO (§§ 149a ff) sah er dabei (hinsichtlich des Richtervorbehalts auch bei Eingriffen durch Verwendung von Verkehrsdaten) durch Art 10a StGG zwingend vorgegebene Ausführungsbestimmungen. Ebenfalls Anhaltspunkte sah man in der Legaldefinition des einfachgesetzlichen Fernmeldegeheimnisses (§ 88 TKG 1997).[157]

Das Bundesministerium für Inneres reagierte darauf, indem in den Erläuterungen des dann folgenden Entwurfs einer Regierungsvorlage zu § 53 Abs 3a SPG ausdrücklich festgehalten wurde, dass der darin vorgesehene „Zugriff auf die so genannten ‚äußere Gesprächsdaten' wohl eine Überwachung analog zu § 149a StPO, jedoch keinen Eingriff in das Fernmeldegeheimnis gem Art 10a StGG darstellt".[158] Dieser Ansatz wurde – wie die Erläuterungen zur RV für die jüngste SPG-Novelle zeigen[159] – bis zum heutigen Tage beibehalten.

Nach weiterer Kritik schlug das BMI dann anstelle des zuerst vorgesehenen pauschalen Abstellens auf „Inhalte nach (dem damals geltenden) § 87 Abs 3 Z 4 („Stammdaten") und 5 („Vermittlungsdaten") TKG" 1997 einen Text vor, wonach die „Auskunft sich auf Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses sowie – mit Zustimmung eines Teilnehmers – auf Teilnehmernummer, Namen und Anschrift in Bezug auf einen bei dem Teilnehmer eingegangenen Anruf zu beschränken hat".[160] Dazu hielt das BKA-VD[161] sinngemäß fest, dass die Zustimmung des passiven Teilnehmers nicht Eingriffe in das Fernmelde-

153 OGH 6.12.1995, 13 Os 161/95 = JBl 1997, 260; 17.6.1998, 13 Os 68/98 = EvBl 1998/191; s auch die in OGH 18.1.2001, 12 Os 152/00 (12 Os 153/00) zitierten Ausführungen des Generalprokurators.

154 Ministerialentwurf betreffend Bundesgesetz, mit dem das Sicherheitspolizeigesetz […] geändert werden (SPG-Novelle 1998), GZ BMI 95.012/474-IV/11/98/Vg v 1.10.1998.

155 Vgl ebenda, Art I Z 20.

156 Vgl BKA GZ 601.598/1-V/98 v bzw 810.057/6-V/3/98 v 21.10.1998 (hier Seite 3 f). Siehe übereinstimmend auch die Stellungnahme des Datenschutzrates (DSR) v 3.11.1998, GZ 817.068/3-DSR/98 (Datum der Beschlussfassung).

157 § 88 Abs 1 TKG 1997 lautete: „Dem Fernmeldegeheimnis unterliegen die Inhaltsdaten und die näheren Umstände der Kommunikation, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war."

158 Vgl Erl „Zu Z 20 (§ 53 Abs 3a)", Seite 11 der Entwurfsfassung der Erläuterungen zur RV betreffend die SPG-Novelle 1998 (GZ BMI 95.012/487-IV/11/98/Vg v 30.10.1998).

159 272 BlgNR 23. GP, 5

160 Vgl Art I Z 15 der RV 1479 BlgNR 22. GP, 4.

161 Vgl BKA GZ 601.598/5-V/A/5/98 v 4.11.1998.

geheimnis des aktiven Teilnehmers legitimieren könne. Gegen die letztlich verabschiedete Version der RV wurde seitens des BK-VD in der Folge kein „Veto" eingelegt. An der grundsätzlichen Aufrechterhaltung einer weiten Auslegung des Anwendungsbereiches des Art 10a StGG wurde aber in der Praxis der Folgejahre festgehalten.

Das Bundesministerium für Justiz vertritt bis heute ebenfalls einen weiten Anwendungsbereich des verfassungsrechtlichen Fernmeldegeheimnisses. Dies wurde im Begutachtungsverfahren zur jüngsten SPG-Novelle sichtbar.[162] Auch die Erläuterungen zu den einschlägigen Eingriffsbestimmungen betreffend die Überwachung von Telekommunikationsdaten (§§ 135 ff) in der seit 1. Jänner 2008 in Kraft befindlichen Fassung der StPO unterstreichen diesen Interpretationsansatz.[163]

– Weitere Überlegungen

Bereits an früherer Stelle wurde angedeutet, welche Aussagekraft im Einzelfall auch „reine" Verkehrsdaten, wie etwa IP-Adressen haben können.[164] Aber auch herkömmliche Telefonnummern geben je nach Fall weit reichende Aufschlüsse.[165] Die hohe Dichte von (temporär) bei den Betreibern verfügbarer Verbindungsdaten ermöglicht bspw die Ermittlung von Menschen mit „Meinungsführereigenschaft". Eine solche lässt sich ohne Schwierigkeit aus dem Kommunikationsverhalten ableiten (Wer hat besonders viele stabile Kontakte zu anderen) und auch für Überwachungszwecke verwerten. Zudem lassen bestimmte Kategorien von Nummern aufgrund ihrer Spezifik indirekte Schlüsse auf Gesprächsinhalte zu („Sexhotline", „Psychotherapeut", „Telefonseelsorger" etc).

Wenn man sich an der Entstehungsgeschichte des Fernmeldegeheimnisses orientiert, sollte man nicht ganz außer Acht lassen, dass zur Zeit der handvermittelten Telefonie bzw später beim mechanisierten Selbstwählverkehr so gut wie keine (nachträglich) ver- bzw auswertbaren Verbindungsdaten anfielen. Erst die Digitalisierung schaffte ein spezifisches Gefahrenpotential, dem durch eine unzeitgemäße Auslegung, die sich nicht am Schutzbedürfnis der Telekommunikationsnutzer orientiert, freilich nicht Rechnung getragen werden kann.

Am Rande vermerkt sei, dass das deutsche Bundesverfassungsgericht (BVerfG) auf Basis der im entscheidenden Punkt nicht wesentlich von Art 10a StGG abweichenden Gewährleistung des Fernmeldegeheimnisses[166] nach Art 10 Grundgesetz[167] in ständiger Rechtsprechung davon ausgeht, dass dieses „nicht nur Kommunikationsinhalte, sondern auch die näheren Umstände der Telekommunikation erfasst". Zu Letzteren gehöre insbesondere, ob, wann und wie oft

162 Vgl die Stellungnahme des BMJ zum bezüglichen Ministerialentwurf v 1.10.2007, GZ BMJ-L707.000/0017-II 3/2007.

163 ErläutRV zu §§ 137 bis 140 StPO der RV 25 BlgNR 22. GP, 190.

164 Dazu oben bei FN 110.

165 Auf die Möglichkeit, von Verkehrsdaten auf Gesprächsinhalte rückzuschließen, wiesen schon *Funk/Krejci/Schwarz,* Zur Registrierung von Ferngesprächsdaten durch den Dienstgeber, DRdA 1984, 289, hin. S auch *Himberger* (FN 151) 63.

166 BGBl 1, zuletzt geändert durch G v. 28.8.2006 BGBl I 2034.

167 Art 10 Abs 1 GG lautet „Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.".

zwischen welchen Personen oder Endeinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist.[168]

- *Ergebnis*

Ingesamt sprechen systematische und teleologische Überlegungen für die Einbeziehung auch von Verkehrsdaten in den Schutzbereich des (verfassungsgesetzlichen) Fernmeldegeheimnisses. Zutreffendenfalls müssten auch die Rufdatenrückerfassungen nicht nur für strafprozessuale (vgl § 135 Abs 2 Z 2 iVm § 137 StPO), sondern auch für sicherheitspolizeiliche Zwecke der richterlichen Genehmigung unterworfen werden. Unabhängig von der Auslegung des Art 10a StGG spricht viel dafür, die richterliche Kontrolle auch über sicherheitspolizeilich motivierte Eingriffe in das Kommunikationsgeheimnis zu erstrecken. Dies ist keine Frage der Praktikabilität (Stichwort: Richter mit Rufbereitschaft), sondern der rechtspolitischen Überzeugung.

B. Zweite Hauptgruppe: Anfragen auf Basis von „Nachricht(en)“ oder IP-Adresse(n) (§ 53 Abs 3a Z 2 und 3 SPG)

1. Allgemeines, technische Hintergründe

Mittels Abänderungsantrag im Plenum des Nationalrates, uzw am Tage der Beschlussfassung der jüngsten Änderungen zum SPG, wurden als völlig neue sicherheitsbehördliche Ermächtigungen die Z 2 und 3 des § 53 Abs 3a SPG kreiert. Demnach können die Sicherheitsbehörden nunmehr Auskunft verlangen „über Internetprotokolladresse (IP-Adresse) zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung“ (Z 2; „Anfragetyp 4“) sowie „über Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war“ (Z 3; „Anfragetyp 4“). Damit versuchte das de facto hinter dem Abänderungsantrag stehende BMI, quasi einen Schlussstrich unter die im Grunde seit Inkrafttreten der SPG-Novelle 1999 schwelenden juristischen Auseinandersetzungen (insbesondere mit den Internetdiensteanbietern) um die Subsumierbarkeit von IP-Adressen unter § 53 Abs 3a Satz 1 SPG alter Fassung zu ziehen.[169]

Allgemein zielen diese Ermächtigungen darauf ab, den Sicherheitsbehörden selbstständige, dh von gerichtlicher Kontrolle entbundene Ermittlungen betreffend Handlungen, die unter Nutzung des Internets gesetzt wurden, zu ermöglichen. Zu denken ist hier neben der Nutzung von E-Mail etwa an Kommunikationsvorgänge im Rahmen von sog „Internetforen“ oder „Chaträumen“ („chat rooms“), aus denen sich Anhaltspunkte für eine konkrete Gefahr für die öffentliche Sicherheit oder auch Hinweise auf Suizidabsichten einer Person ergeben. Zum besseren Verständnis der in § 53 Abs 3a Satz 1 Z 2 und 3 SPG angesprochenen Befugnisse soll nachstehend exkursorisch auf die technische Seite der Internetnutzung eingegangen werden.

Um überhaupt sicherheitspolizeilich relevante Handlungen im Internet setzten zu können, bedarf es vereinfacht gesagt eines Rechners (PCs) (samt einschlä-

168 Vgl BVerfGE 67, 157 (172); 85, 286 (396); BVerfG 1 BvR 330/96 v 12.3.2003 ua.
169 Vgl zu dieser Frage oben ab FN 72.

giger Software, va eines sog „Webbrowsers“) mit entsprechendem Zugang zum Internet. Letzterer wird von Access-Providern vermittelt. Um in einem Verbund von Computernetzwerken wie dem Internet über lokale Netzwerke hinaus kommunizieren zu können, bedarf es bestimmter (technischer) Regeln über den Datenaustausch („Übertragungs- oder Kommunikationsprotokolle“).

Maßgebend im gegebenen Kontext ist heute das sog TCP/IP-Referenzmodell (Transmission Control Protocol/Internet Protocol). Grundprinzip dieses Modells ist die Zerlegung der zu übertragenden Daten in kleine „Datenpakete“. Im IP ist ua festlegt ist, dass jedem mit dem Internet verbundenen Rechner eine eindeutige Zahlenfolge zugeordnet wird, die sog „IP-Adresse“. Diese ermöglicht – wie bereits an anderer Stelle diskutiert – die (logische) Adressierung von PCs und anderen Endgeräten im Internet. Indem in die via Internet übermittelten „Datenpakete“ sowohl die IP-Adresse des sendenden als auch des empfangenden Endgerätes eingetragen werden, kann eine Verbindung zwischen diesen beiden Einheiten über viele Zwischenstationen des Internets aufgebaut bzw aufrechterhalten werden.[170]

Auch der Versand und Empfang von E-Mails läuft über das Internet, allerdings auf Basis eines spezifischen Protokolls (sog Simple Mail Transfer Protocol - SMTP). Für die Zustellung von E-Mails werden neben den E-Mail-Adressen von Absender und Empfänger wiederum ua IP-Adressen (insbesondere jene von versendendem /empfangendem Rechner benötigt.

2. Die Anfragetypen im Einzelnen

a) Frage nach IP-Adresse und Zeitpunkt ihrer Verwendung auf Basis von E-Mails, Beiträgen in Internetforen / Chaträumen, Bild- bzw Videodateien uä

Bringt sich ein Internetnutzer bspw unter einem Benutzernamen („user name“, „nickname“) in eine Diskussionsplattform (Internetforum) oder einen Chatraum ein, lädt er bestimmte Inhalte (Bild-, Videodateien) von einer Webseite, stellt er selbst eine Videodatei auf eine Website oder versendet er E-Mails, so hinterlässt er am Rechner, auf dem die betreffende Webseite (technisch) untergebracht ist („gehostet“ wird), dh dem „Webserver“ bzw auf den betreffenden E-Mail-Servern, elektronische Spuren, insbesondere in Form seiner IP-Adresse. Über die Auswertung allenfalls vorhandener Protokolldaten (Logfiles) des (von einem sog „Host-Provider“ betriebenen) Webservers bzw von E-Mail-Servern kann eine Zuordnung eines Benutzernamens/einer E-Mailadresse zu einer bestimmten IP-Adresse und dem Zeitpunkt/-raum, zu dem diese verwendet wurde, erfolgen.

Auf den vorstehend skizzierten Sachverhalt stellt nun typischerweise die Ermächtigung § 53 Abs 3a Satz 1 Z 2 SPG ab. Danach können die Sicherheitsbehörden die IP-Adresse zu einer bestimmten Nachricht, dh etwa zu einem E-Mail, und den Zeitpunkt ihrer Verwendung erfragen (Anfragetyp 4).

170 Zu den technischen Hintergründen s wieder *Einzinger/Schubert/Schwabl/Wessely/Zykan* (FN 106) 113 ff.

b) Anfragetyp 5: Frage nach Name(n) und Anschrift(en) auf Basis von IP-Adresse und Zeitpunkt der Verwendung ebendieser

Mit den nach § 53 Abs 3a Satz 1 Z 2 SPG ermittelten Daten kann freilich nicht automatisch die reale Identität eines bestimmten Internetnutzers geklärt werden. Weder einem Forenbetreiber noch dem Betreiber des zugehörigen Webservers muss diese nämlich bekannt sein. Im Übrigen sind die von privaten Internetnutzern verwendeten IP-Adressen – wie bereits an anderer Stelle ausgeführt - nicht diesen direkt, sondern primär Anbietern von Internetzugangsdiensten („Access-Providern“) zugeordnet. Letztere weisen ihren Endkunden in der Regel eine solche IP-Adresse anlässlich jedes Aufbaus einer Verbindung vom Endkunden-PC zum Internet neu zu (sog „dynamische Adressierung“). Die bei diesem Vorgang anfallenden Daten fallen unter die sog „Zugangsdaten“ iSd § 92 Abs 3 Z 4a TKG 2003. Erst der Rückgriff auf diese Daten iVm den Stammdaten iSd § 92 Abs 3 Z 3 TKG 2003 ermöglicht letztlich die Feststellung der realen Identität von Nutzern einer IP-Adresse zu einem bestimmten Zeitpunkt. Der als Auskunftspflichtige in Betracht kommende Inhaber einer bestimmten IP-Adresse kann von den Sicherheitsbehörden einfach über das jeweilige regionale Internetregister eruiert werden (Regional Internet Registry – RIR).[171]

In diesem Kontext wird die in § 53 Abs 3a Satz 1 Z 3 SPG verankerte Befugnis verständlich, wonach die Sicherheitsbehörden „Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war,“ erfragen dürfen (Anfragetyp 5).

3. Zum Kreis der Auskunftspflichtigen

Aus dem in beiden vorangegangenen Abschnitten Gesagten ergibt sich, dass im Fokus der Auskunftspflicht nach § 53 Abs 3a Satz 1 Z 2 SPG primär sog Host- oder Content-Provider und jener nach § 53 Abs 3a Satz 1 Z 3 SPG in erster Linie sog Access-Provider stehen. Wiewohl sich aus der Umschreibung des persönlichen Anwendungsbereiches des § 53 Abs 3a Satz 1 SPG ergibt, dass im Allgemeinen nur kommerzielle Diensteanbieter (arg: Diensteanbieter iSd „3 Z 2 ECG“) erfasst sind,[172] kommen unter bestimmten Bedingungen auch Betreiber privater Webseiten als Adressaten für Anfragen in Betracht. Dann nämlich, wenn ein wirtschaftlicher Hintergrund iS einer zumindest indirekten Ertragserzielungsabsicht gegeben ist (Bsp: Webseite eines Hobbymusikers, der dort ua auf die Möglichkeit, ihn fallweise gegen Entgelt für Veranstaltungen zu buchen, hinweist).[173]

---

171 Vgl dazu wieder FN 108.

172 Vgl idS § 3 Z 2 iVm § 3 Z 1 ECG iVm RV 817 BlgNR 21. GP 17 f bzw § 1 Abs 1 Z 2 Notifikationsgesetz 1999 sowie den Vorschlag KOM (1998) 586 endg der Kommission v 23. 12. 1998 für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt, Seite 21 (Kommentar zu Art 2); *Blume/Hammerl*, E-Commerce-Gesetz (2002) 41, 56.

173 Dies reicht für eine Subsumierbarkeit unter den „Dienst in der Informationsgesellschaft“ aus. Vgl idS Erwägungsgrund 18 Satz 4 RL 2000/31/EG ABl 2000 L 178, 1 (3); RV 817 BlgNR 21. GP 18; mwN *Blume/Hammerl* (FN 172) 41, 47.

4. Zulässige Anfragezwecke

Als zulässiger Anfragezweck kommt analog den Anfragetypen 1 und 2 wiederum der Fall in Betracht, dass „bestimmte Tatsachen die Annahme einer konkreten Gefahrensituation rechtfertigen“ und die angefragten Daten „wesentliche Voraussetzung“ für deren Bewältigung sind.[174] Zu den damit verbundenen Auslegungsproblemen ist insofern sinngemäß auf die Überlegungen unter Abschn V.A.1.b zu verweisen.[175]

5. Zur Reichweite des Begriffs „Nachricht“

Auslegungsfragen wirft in Ermangelung einer im SPG selbst enthaltenen Definition der Begriff „bestimmte Nachricht“ in § 53 Abs 3a Satz 1 Z 2 SPG auf. In den Materialien finden sich hiezu schon deshalb keine Hinweise, da die bezügliche Regelung erst unmittelbar vor Beschlussfassung im Plenum in den Text des § 53 Abs 3a SPG Eingang gefunden hat. Auch die Begründung des Abänderungsantrages vermag keinen Aufschluss zu geben.[176] Insoweit scheint es zunächst naheliegend, auf das TKG 2003 zurückzugreifen. § 92 Abs 3 Z 7 TKG 2003 definiert Nachricht als „jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird“.

Unter Zugrundelegung dieses Begriffsverständnisses bereitet die Subsumtion von E-Mails sowie Diskussionsbeiträgen in Chaträumen oder Onlineforen, die nur registrierten Benutzern zugänglich sind, unter § 53 Abs 3a Z 2 SPG keine besonderen Probleme.[177] Fraglich könnte aber sein, ob von diesem Nachrichtenbegriff auf eine allgemein zugängliche Webseite hochgeladene Fotos, Dokumente oder Videodateien erfasst sind.[178] Nach zutreffender Ansicht ist nicht auf die Tatsache der öffentlichen Zugänglichkeit derartiger Informationen, sondern auf die Zuordenbarkeit des jeweiligen Hochlade- bzw Abrufvorganges zu einem bestimmten Internetnutzer abzustellen.[179] Im Übrigen erscheint es schon mit Blick auf die praktischen Bedürfnisse der Sicherheitsbehörden (Stichwort: „Drohvideo“) wenig plausibel, dass die Autoren des § 53 Abs 3a Z 2 SPG von einem allzu engen Begriffsinhalt ausgegangen sind. Im Falle von Meinungsverschiedenheiten zwischen Betreibern und Sicherheitsbehörden über die Reichweite der

174 Vgl wieder § 53 Abs 3a Satz 1 letzter Satzteil SPG.

175 Siehe oben nach FN 58.

176 Vgl wieder AA-89 (XXIII. GP).

177 So in Bezug auf die Reichweite des § 92 Abs 3 Z 7 TKG 2003 auch *Zanger/Schöll* (FN 109) § 92 Rz 32.

178 Verneinend die WKÖ (siehe das Informationsblatt „Recht der Sicherheitsbehörden auf Herausgabe der Kundendaten von Telekommunikationsunternehmen und E-Commerce-Diensteanbietern“, Seite 1). Für ein weites Begriffsverständnis, das neben Inhalten von Homepages auch Aufrufstatistiken von Webseiten mit umfassen soll, dagegen *Zanger / Schöll* (FN 109) § 92 Rz 32. Einen weiteren Anwendungsbereich indiziert auch Erwägungsgrund 15 der mit dem TKG 2003 umgesetzten RL 2002/58/EG v 12.7.2002 ABl L 201, 37 (38), welcher davon spricht, dass „eine Nachricht alle Informationen über Namen, Nummern oder Adressen einschließen kann, die der Absender einer Nachricht oder der Nutzer einer Verbindung für die Zwecke der Übermittlung der Nachricht bereitstellt“.

179 Vgl *Himberger* (FN 151) 54 f, 56.

Auskunftspflicht im Einzelfall bestünde allerdings gerade im Falle eines Drohvideos (vollendete Straftat) ohneweiters die Möglichkeit, bei der Staatsanwaltschaft die Beantragung einer gerichtlichen Bewilligung nach § 137 Abs 1 iVm Abs 2 iVm § 135 Abs 2 Z 3 StPO anzuregen (arg: „Nachrichtenübermittlung"). Im Falle der Erteilung wäre eine solche mit Zwang durchsetzbar.

Jedenfalls obliegt es aber den Sicherheitsbehörden, ausreichend präzise Angaben zu tätigen, um angefragten Providern (Bsp Host-Provider) eine zielgerichtete Suche nach der gewünschten Information zu ermöglichen (Bsp: Welcher Benutzername?, Welcher Inhalt?, Welches Forum?).

6. Zur Form der Anfrage

In punkto Anfrageform ist wiederum sinngemäß auf die Ausführungen unter Abschn V.A.1.d bzw V.A.3.d zu verweisen.[180]

7. Kritik

Wie im Falle der Rufdatenrückerfassung nach § 53 Abs 3a Satz 2 SPG erfordern Auskunftserteilungen auf der Grundlage von § 53 Abs 3a Z 2 und 3 SPG eine Auswertung von sog „Verkehrsdaten". Es kommt diesfalls zu einem Eingriff ins Kommunikationsgeheimnis iSd § 93 Abs 1 TKG[181] und nach der hier vertretenen Auffassung auch in die Rechte nach Art 10a StGG[182]. Auf die Verknüpfung von IP-Adressen mit Inhaltsinformationen und die daraus resultierende spezifische Dimension von im Einzelfall erfolgenden Eingriffen wurde bereits an anderer Stelle hingewiesen.[183] Die Problematik der fehlenden richterlichen Kontrolle der sicherheitsbehördlichen Zugriffe stellt sich auch hier.

C. Dritte Hauptgruppe: Anfragen auf Basis einer Mobiltelefonnummer nach Standortdaten und IMSI (§ 53 Abs 3b SPG)

1. Allgemeines, technische und sachliche Hintergründe

Die dritte Hauptgruppe sicherheitsbehördlicher Anfragen stellen nun die Fälle des neu eingeführten § 53 Abs 3b SPG dar. „Ist auf Grund bestimmter Tatsachen anzunehmen, dass eine gegenwärtige Gefahr für das Leben oder die Gesundheit eines Menschen besteht, sind die Sicherheitsbehörden zur Hilfeleistung oder Abwehr dieser Gefahr berechtigt, von Betreibern öffentlicher Telekommunikationsdienste Auskunft über Standortdaten („Anfragetyp 6") und die internationale Mobilteilnehmerkennung (IMSI) der von dem gefährdeten Menschen mitgeführten Endeinrichtung zu verlangen (der Fall der gleichzeitigen Anforderung beider Datenarten kann als „Anfragetyp 7" eingestuft werden) sowie technische Mittel zu ihrer Lokalisierung zum Einsatz zu bringen".

180 Siehe oben bei FN 125 bzw FN 149.
181 Siehe dazu oben bei FN 109.
182 Siehe dazu oben bei FN 151.
183 Siehe oben nach FN 110.

a) Abgrenzung zur Anfragemöglichkeit nach § 98 TKG

Schon vor dem 1. Jänner 2008 war es Betreibern von Notrufdiensten möglich, unter Berufung auf § 98 TKG 2003 von Betreibern öffentlicher Telekommunikationsdienste Auskünfte über Standortdaten iSd § 92 Abs 3 Z 6 TKG unter der Bedingung zu erhalten, dass ein Notfall nur durch Bekanntgabe dieser Informationen abgewehrt werden konnte.

Auch das Bundesministerium für Inneres konnte als Notrufdienstebetreiber[184] diese Privilegierung in Anspruch nehmen. Wenn allerdings nicht eine in Not befindliche Person selbst bei den Sicherheitsbehörden anrief, sondern Letztere nur indirekt – etwa über den Anruf besorgter Angehöriger – kontaktiert wurde, kam § 98 TKG nicht zum Tragen. Diese „Lücke" schließt quasi § 53 Abs 3b Satz 1 SPG.

Darüber hinaus freilich ist es den Sicherheitsbehörden aber auch möglich, Standorte von Personen zu ermitteln, die mutmaßlich Ziel eines noch andauernden gefährlichen Angriffs auf ihr Leben oder ihre Gesundheit durch (eine/n) „Kriminelle(n)" sind. Und schließlich ist den Behörden die Möglichkeit eröffnet, vom jeweiligen Mobilfunknetzbetreiber unabhängig, dh mit eigenen „technischen Mitteln", die Lokalisierung von Mobiltelefonen zu bewerkstelligen.

b) Zur technischen Funktionalität

Unter den im Vorabschnitt angesprochenen „technischen Mitteln" sind im gegebenen Kontext sog „IMSI-Catcher" zu verstehen.[185] Dabei handelt es sich um Geräte, die eine Mobilfunkzelle simulieren. Die Auffindbarkeit von Mobiltelefonen in einem Mobilfunknetz wird dadurch gewährleistet, dass jede Basis-Sende- und Empfangsstation auf einer für sie festgelegten Frequenz ein permanentes Signal aussendet, welches von im Funkbereich der Anlage befindlichen eingeschalteten Mobiltelefonen erkannt wird. In Reaktion darauf sendet das betreffende Mobiltelefon seine eigene Kennung, genauer die IMSI (in verschlüsselter Form) an diese Basisstation bzw meldet sich dort an. Letztere gibt diese Information an eine Vermittlungsstelle weiter, sodass dem Netz nun bekannt ist, wo sich ein Teilnehmer befindet. Solcherart kann ein für diesen Teilnehmer bestimmter Anruf an diesen weitergeleitet werden.

Ein Mobiltelefon misst zudem laufend die Empfangsqualität „seiner" Basis-Sende- und Empfangsstation und sucht sich automatisch eine neue, wenn sich der Teilnehmer etwa aus dem Bereich der bisherigen Funkzelle hinausbewegt. Auch dieser Zellenwechsel wird dem Netz mitgeteilt.

Auf diese Interaktion zwischen Mobiltelefon und Basis-Sende- und Empfangsstation setzt nun der IMSI-Catcher auf. Indem er durch ein entsprechend starkes Funksignal die reguläre örtliche Funkzelle überlagert, veranlasst er die in seinem Einzugsbereich befindlichen Mobiltelefone, sich bei ihm anstatt bei der regulären Basisstation „einzubuchen" und zugleich seine eigenen Signale in nicht verschlüsseltem Modus an den IMSI-Catcher zu senden. Dies ermöglicht in weiterer Folge die Auslegung der IMSI sämtlicher beim IMSI-Catcher eingebuch-

184 Vgl dazu § 5 Abs 4 SPG iVm § 16 Kommunikationsparameter-, Entgelt- und Mehrwertdiensteverordnung - KEM-V idF BGBl II 2007/219 iVm Bescheid der Rundfunk & Telekom Regulierungs-GmbH GZ TRPV0637-002/2007 v 23.3.2007.

185 Vgl in diesem Sinne Vorblatt zu RV 272 BlgNR 23. GP, 2.

ten Mobiltelefone. Ist die IMSI eines Mobiltelefons bekannt, kann so auch gezielt nach diesem gesucht werden, dh festgestellt werden, ob es sich in Reichweite des IMSI-Catchers befindet.

Voraussetzung für den effizienten Einsatz eines IMSI-Catchers zur gezielten Suche im vorstehenden Sinne ist die Kenntnis der Funkzelle bzw des Funkzellenverbundes, in dem sich das gesuchte Mobiltelefon befindet. Dazu muss zuerst eine Anfrage nach „Anfragetyp 6" an den jeweiligen Mobilfunknetzbetreiber gerichtet werden.

2. Zum Kreis der Auskunftspflichtigen

Als Adressaten der Auskunftspflicht gem § 53 Abs 3b SPG kommen – sachlogisch bedingt – nur Betreiber von Mobilfunknetzen in Betracht. Im Falle ortsgebundener Anschlüsse reicht zur Feststellung des Standortes bereits ein Blick in die Kundendatei.

3. Zulässige Anfragezwecke

Ähnlich wie in den Fällen des § 53 Abs 3a Satz 1 SPG werden in § 53 Abs 3b leg cit zwei an sich widersprüchliche Tatbestandselemente miteinander verbunden, nämlich der Verdachtsansatz („auf Grund bestimmter Tatsachen anzunehmen") und die „gegenwärtige Gefahr". Als denkbare Anwendungsfälle kommen hier Situationen in Betracht, in denen eine Person, die mutmaßlich ein empfangsbereites Mobiltelefon mit sich führt (1. Kriterium), dieses jedoch nicht (mehr) selbst bedienen kann/will (2. Kriterium), sich entweder verirrt hat oder verunfallt ist oder aktuell einem Angriff auf ihre körperliche Integrität bzw Gesundheit ausgesetzt ist (3. Kriterium).

Mit Blick auf die in § 53 Abs 3 b SPG vorgenommene klare Einschränkung auf die „Opferrolle" der gesuchten Person, kommen Standortermittlungen von Tätern weiterhin nur nach Maßgabe der Regelungen der StPO in Betracht.[186]

4. Zur Form der Anfrage

In Anknüpfung zu den Ausführungen in Abschn V.A.1.d (nach FN 125) betreffend die einen Übermittelnden aus dem DSG 2000 allgemein treffenden Pflichten zur Prüfung einer Anfrage auf „Plausibilität" ist im Kontext des § 53 Abs 3b SPG auf die ausdrückliche Anordnung, die dieser in Satz 2 trifft, hinzuweisen: Danach „trifft die Sicherheitsbehörde die Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehrens".[187] Diese Bestimmung kann quasi als lex specialis zu § 7 Abs 2 Z 2 DSG 2000 gelesen werden und würde insofern letztere Norm verdrängen. Dies erscheint im Ergebnis insofern problematisch, als sich für einen Betreiber stets die Grundsatzfrage stellen muss, ob eine an ihn herangetragene Anfrage zur Standortdatenermittlung sich auf einen Fall bezieht, der tatsächlich unter § 53 Abs 3b SPG subsumierbar ist oder ob aber eine auf § 135

186 Vgl § 135 Abs 2 iVm § 137 f StPO.

187 Das aktuell in Verwendung befindliche Anfrageformular verwendet diese „Verantwortungsklausel" undifferenziert für alle Anfragetypen. Siehe wieder den Anlage 1 zu Erlass GZ 94.762/101-GD/08 v 28.1.2008.

Abs 2 StPO gestützte gerichtliche Bewilligung erforderlich ist. Zumindest eine grobe Plausibilitätsprüfung auf Seite des Übermittelnden erschiene mit Blick auf die Dimension des Eingriffs insofern geboten.

Immerhin ist die Behörde trotz der ihr dem Gesetzeswortlaut nach allein zufallenden Verantwortlichkeit für die Rechtmäßigkeit des Auskunftsbegehrens verpflichtet, dessen Dokumentation dem Betreiber unverzüglich, spätestens innerhalb von 24 Stunden, nachzureichen.[188] Wie gleich nachstehend erläutert, ist diese Dokumentation jedoch nicht mit jener nach § 98 Abs 3 TKG 2003 gleichzusetzen.

5. Kritik

Die neue Ermächtigung in § 53 Abs 3b gibt in mehrfacher Hinsicht Anlass zu Kritik. Zunächst fällt auf, dass diese Bestimmung im Gegensatz etwa zu § 98 Satz 3 TKG 2003 streng genommen keine Verpflichtung vorsieht, die „Notwendigkeit der Informationsübermittlung" zu dokumentieren, um diese den Betreibern nachträglich vorzulegen und so das tatsächliche Vorliegen eines entsprechenden Anlassfalles nachvollziehbar zu machen. Denn § 53 Abs 3b Satz 2 SPG verlangt nur die „Dokumentation des Auskunftsbegehrens", also eine Art schriftlicher Bestätigung, ohne dass dem Gesetzeswortlaut zufolge dessen „Erforderlichkeit" begründet werden müsste.

Angemerkt sei weiters, dass ein IMSI-Catcher in den in der RV als typisch angeführten Anwendungsfällen (vermisste Tourengeher oder Wanderer)[189] sehr rasch im betreffenden Einsatzgebiet verfügbar sein müsste. Dazu dürfte der geplante Ankauf eines einzigen IMSI-Catchers, wie dies die RV ankündigt,[190] freilich nicht hinreichen.

Von besonderer Relevanz ist schließlich, dass IMSI-Catcher – je nach Bauart – auch eine – nach SPG selbstverständlich unzulässige – inhaltliche Überwachung der Gespräche, die von Mobilfunktelefonen in deren Einzugsbereich geführt werden, ermöglichen. Um dies technisch auszuschließen, wäre daher die gesetzliche Anordnung zu fordern, dass die für SPG-Zwecke eingesetzten IMSI-Catcher jenen Mobiltelefonen, die sich bei ihnen einbuchen, keine Dienste anbieten dürfen, die in der Folge eine Inhaltsüberwachung ermöglichen.

Nicht zuletzt vor dem vorgestellten technischen Hintergrund erscheint die bloße Mitteilungspflicht des Einsatzes von IMSI-Catchern an den Rechtsschutzbeauftragten beim BMI (vgl § 91c Abs 1 Satz 3 SPG) im Falle des Rückgriffs auf die Befugnisse aus § 53 Abs 3b SPG völlig unzureichend.

Folgte man der hier vertretenen Auffassung, dass „Standortdaten" als Unterfall der „Verkehrsdaten" nicht nur dem einfachgesetzlichen Kommunikationsgeheimnis, sondern auch dem Anwendungsfall des Art 10a StGG unterliegen, wäre wiederum die Abwesenheit jeglicher richterlicher Kontrolle zu beanstanden.

188 Vgl § 53 Abs 3b Satz 2 SPG.
189 Vgl ErläutRV 272 BlgNR 23. GP, 5.
190 Vgl Vorblatt zu RV 272 BlgNR 23. GP, 2.

VI. Resümee

Auf Basis der obigen Ausführungen können im Wesentlichen folgende Schlussfolgerungen gezogen werden:

– Grundsätzlich ist anzuerkennen, dass gesetzliche Eingriffsermächtigungen zugunsten staatlicher Behörden von Zeit zu Zeit daraufhin überprüft werden müssen, ob sie im Lichte des technischen Fortschritts einer Anpassung bedürfen.
– Der Wunsch, für sicherheitspolizeiliche Zwecke neben einer Stammdatenabfrage im Einzelfall auch Verkehrsdaten heranzuziehen, ist bis zu einem gewissen Grad nachvollziehbar
– Die bis 31. Dezember 2007 bestehende Praxis betreffend Anfragen an Betreiber mittels IP-Adressen für sicherheitspolizeiliche Zwecke hatte keine Deckung in § 53 Abs 3a SPG.
– Der Rückgriff auf technische Mittel der Kommunikationsüberwachung für präventive Zwecke stellt angesichts der Eingriffsdimension (heimliche Überwachung usw) jedoch ein grundsätzliches rechtsstaatliches Problem dar, welches ohne Vorkehrungen für eine vorgehende bzw begleitende unabhängige (richterliche) Kontrolle nicht befriedigend lösbar erscheint.
– Die Ermächtigung zum Einsatz von IMSI-Catchern für sicherheitspolizeiliche Zwecke erscheint aus grundrechtlicher Sicht insbesondere in Ermangelung ausdrücklicher Restriktionen in punkto deren technischer Beschaffenheit („Ausschluss der Abhörfähigkeit“) mit schwer kalkulierbaren Risiken behaftet.
– Die Ablehnung formalisierter Kontrollmechanismen (Stichwort „Richtervorbehalt“) für Eingriffe in das Kommunikations- bzw Fernmeldegeheimnis seitens der Sicherheitsbehörden unter Verweis auf die Gefährdung der Effizienz der Mittel vermag gerade mit Blick auf moderne Kommunikationsverbindungen zwischen Sicherheitsbehörden und Justiz nicht zu überzeugen. Darin manifestiert sich seit geraumer Zeit die – auch auf internationaler Ebene zu beobachtende – Tendenz der Sicherheitsbehörden, sich der justiziellen Kontrolle mehr und mehr zu entziehen.
– Eine zeitgemäße Sichtweise des Fernmeldegeheimnisses (Art 10a StGG) legt es nahe, neben Inhalts- auch Verkehrsdaten in dessen Schutzbereich einzubeziehen. In diesem Lichte fehlt es den durch § 53 Abs 3a SPG ermöglichten Eingriffen in das Kommunikationsgeheimnis durchgehend an der Bindung an eine richterliche Genehmigung.
– Die bloßen Informationspflichten gegenüber dem internen und im Übrigen nicht ausreichend unabhängigen Rechtsschutzbeauftragten beim Bundesminister für Inneres bei sicherheitspolizeilich motivierten Eingriffen in das Fernmelde- bzw Kommunikationsgeheimnis stellen kein adäquates Kontrollinstrument dar.
– Im Zuge der parlamentarischen Behandlung der „SPG-Novelle 2008“ sind in § 53 Abs 3a zusätzliche textliche Inkonsistenzen hinzugetreten, welche die Handhabbarkeit der Bestimmung in Frage stellen. Die Vollzugspraxis zeigt erkennbar die Tendenz, diese Probleme durch Auslegungen zu lösen, die mit dem Gesetzeswortlaut schwer in Einklang zu bringen sind.