Information des Vorsitzenden des Datenschutzrates betreffend ein BG, mit dem das TKG 2003 geändert wird (RV 1074 BlgNR 24. GP) sowie betreffend ein BG, mit dem die StPO 1975 und das SPG geändert werden (RV 1075 BlgNR 24. GP)

I. Hintergrund

A. Europäische Ebene – Vertragsverletzungsverfahren (jüngste Entwicklung)

Österreich wurde mit Urteil des EuGH vom 29. Juli 2010 in der Rs. C-189/09 wegen Nichtumsetzung der Richtlinie (RL) 2006/24/EG innerhalb der vorgeschriebenen Frist (bis spätestens 15. September 2007) verurteilt.

In Verfolg der Überwachung der Umsetzung dieses Urteils urgierte die Kommission zuletzt in einem ergänzenden Auskunftsersuchen vom 7. Jänner 2011 die Mitteilung eines konkreten Datums für die Verabschiedung des bezüglichen österreichischen Umsetzungsgesetzes. Österreich hat der Kommission daraufhin mitgeteilt, dass als Beschlusszeitpunkt (Plenum NR) Ende April 2011 in Aussicht genommen ist. Weiters wird Österreich die Kommission über die nunmehr erfolgte Weiterleitung konkreter Gesetzesentwürfe an den Nationalrat per Ministerratsbeschluss vom 22. Februar 2011 unterrichten.

Nicht auszuschließen ist, dass die Kommission trotzdem den Schritt der Beschlussfassung der Einleitung eines Vertragsverletzungsverfahrens nach Art. 260 AEUV (sog. „Sanktionsverfahren“) setzen wird, um den Druck auf Österreich aufrechtzuerhalten. Ob es in weiterer Folge auch zu einer Klagseinbringung beim EuGH kommt, wird nicht zuletzt von der künftigen Chronologie der innerösterreichischen Umsetzungsschritte abhängen. Am Ende eines Sanktionsverfahrens stünde im schlechtesten Fall ein (Zweit-)Urteil des EuGH mit der Verhängung von finanziellen Sanktionen (Pauschalbetrag [mindestens ca. 2,5 Mio Euro] und Zwangsgeld [pro Tag der Nichtumsetzung von € 2.904,- bis € 174.240,-]).

Die Kommission selbst war nach Art 14 der RL 2006/24/EG verpflichtet, bis 15. September 2010 eine Bewertung der Anwendung der Richtlinie und ihrer Auswirkungen auf die Wirtschaftsbeteiligten und die Verbraucher vorzulegen. Darin soll(t)e unter anderem festgestellt werden, ob die Bestimmungen der Richtlinie geändert werden müssen.

Inzwischen hat die Kommission angekündigt, den besagten Evaluierungsbericht bis Mitte März 2011 und im Herbst 2011 konkrete Änderungsvorschläge zur RL 2006/24/EG selbst vorlegen zu wollen. In inhaltlicher Sicht zeichnet sich bis dato allerdings kein ein Abgehen vom Prinzip der Vorratsdatenspeicherung als solchem ab. Aus heutiger Sicht könnte nur ein einschlägiges Urteil des EuGH, welchem die Letztzuständigkeit der Prüfung am Maßstab der Grundrechtecharta zukommt, eine substantielle Änderung der Rechtslage bewirken. Für das österreichische Vertragsverletzungsverfahren käme eine solche Entscheidung freilich jedenfalls zu spät.

Nicht im Letzten klar ist auch, wieweit die Kommission von sich aus allfällige Vorschläge in Richtung der expliziten Erweiterung der Nutzung von Vorratsdaten für andere Zwecke als für den der Aufklärung schwerer Straftaten andenken bzw. vorschlagen wird.

Aktuell ist noch ein Vertragsverletzungsverfahren wegen Nichtumsetzung der Richtlinie 2006/24/EG gegen Luxemburg anhängig.

B. Nationale Ebene

Ein erster Versuch zur Umsetzung der Vorratsdatenspeicher-RL 2006/24/EG wurde in Österreich im Jahre 2007 unternommen. Infolge massiver Kritik am seinerzeitigen Ministerialentwurf (61/ME XXIII. GP) für eine TKG-Novelle im Zuge des Begutachtungsverfahrens (insbesondere in Richtung der Ablehnung der Vorratsdatenspeicherung als solcher wegen Unverhältnismäßigkeit) wurde schließlich vom BMVIT das Boltzmann-Institut für Menschenrechte mit der Ausarbeitung eines völlig neuen Entwurfs beauftragt. Dieser Entwurf wurde im Herbst 2009 vorgelegt. Auch zu diesem Entwurf ergingen zahlreiche Stellungnahmen (190) mit sehr kritischem Tenor ein.

Nach Überarbeitung des Entwurfes auf Basis der Stellungnahmen und zahlreicher ergänzender Konsultationen mit Betroffenenkreisen begannen politische Verhandlungen zwischen BMVIT und BMJ/BMI über offene Detailfragen und insbesondere über die konkrete Ausgestaltung der in Ergänzung zur Normierung der Speicherpflicht als solcher im TKG als erforderlich erachteten logischen „Anschlussstücke“ in SPG und StPO.

Nach Abschluss der vorgenannten politischen Verhandlungen am 21. Februar 2011 konnten dann im Ministerrat vom 22. Februar 2011 zwei gesonderte Regierungsvorlagen (TKG - RV 1074 BlgNR 24. GP sowie StPO / SPG - RV 1075 BlgNR 24. GP) verabschiedet werden.

C. Exkurs: Stand der Überlegungen in Deutschland

In Deutschland wurde die Richtlinie über die Vorratsdatenspeicherung zunächst mit dem Gesetz zur Neuregelung der Telekommunikationsüberwachung vom 21. Dezember 2007 umgesetzt. Die bezüglichen Bestimmungen wurden in der Folge Gegenstand einer Verfassungsbeschwerde beim dt. Bundesverfassungsgericht.

Der Antrag der Beschwerdeführer, die Anordnung der Datenspeicherung im Wege einer der einstweiligen Anordnung außer Kraft zu setzen, hatte teilweise Erfolg. Der Erste Senat des Bundesverfassungsgerichts ließ nämlich die Anwendung der betreffenden Bestimmung, soweit er die Verwendung der gespeicherten Daten zum Zweck der Strafverfolgung regelt, bis zur Entscheidung in der Hauptsache nur modifiziert zu (Beschluss vom 11. März 2008 – 1 BvR 256/08). Diese einstweilige Anordnung wurde in der Folge wiederholt und erweitert mit Beschluss vom 28. Oktober 2008, zuletzt mit Beschluss vom 15. Oktober 2009.

Die einstweiligen Anordnungen bedeuten, dass aufgrund eines Abrufersuchens einer Strafverfolgungsbehörde der Anbieter von Telekommunikationsdiensten die verlangten Daten zwar zu erheben und zu speichern hat. **Sie sind jedoch nur dann an die Strafverfolgungsbehörde zu übermitteln, wenn Gegenstand des Ermittlungsverfahrens eine schwere Straftat im Sinne des § 100a Abs. 2 StPO ist, die auch im Einzelfall schwer wiegt, der Verdacht durch bestimmte Tatsachen begründet ist und die Erforschung des Sachverhalts auf andere Weise wesentlich erschwert oder aussichtslos wäre** (§ 100a Abs. 1 StPO). In den übrigen Fällen ist von einer Übermittlung der Daten einstweilen abzusehen.

Mit Urteil des Ersten Senats vom 2. März 2010 (1 BvR 256/08) hat das Bundesverfassungsgericht die einschlägigen **Rechtsgrundlagen** für die Vorratsdatenspeicherung wegen Verstoßes gegen das verfassungsgesetzliche Fernmeldegeheimnis **für nichtig erklärt. Die Verfassungsrichter sprachen von**

einem "besonders schweren Eingriff in das Fernmeldegeheimnis", das Rückschlüsse bis in die Privatsphäre ermögliche.

Zugleich wurde die **Löschung sämtlicher** zwischenzeitlich erhobener und nicht übermittelten **Vorratsdaten angeordnet.**

Der nun zur „Reparatur“ der bisherigen Konzeption vom Gesetzgeber zu beschreitende Weg ist aktuell strittig.

Das dt Jusitizministerium hat ein Konzept vorgelegt, welches eine Umsetzung der Vorratsdatenspeicher-Richtlinie im Wege des sog. **Quick-Freezing-Verfahrens** präferiert. Bei diesem tritt an die Stelle der anlasslos-generellen Speicherung der Telekommunikationsdaten eine Speicherung nur im Einzelfall und erst zu dem Zeitpunkt, zu dem dazu etwa wegen eines bestimmten Tatverdachts konkreter Anlass besteht (Näheres dazu im Eckpunktepapier des dt. BMJ unter http://www.bmj.de/cln_102/DE/Buerger/digitaleWelt/QuickFreeze/quickfreeze_node.html).

II. Zur Frage der Einbindung des Datenschutzrates

Anlässlich seiner Stellungnahme zum damals vorliegenden Entwurf für eine Umsetzung der Vorratsdatenspeicherung im TKG vom 15. Jänner 2010 (BKA-817.386/0003-DSR/2010) hat der Datenschutzrat ausdrücklich bedauert, dass es damals keinen abgestimmten Begutachtungsentwurf zwischen den mit diesen Fragen befassten Bundesministerien (BMVIT, BMI, BMJ) gab. Damit blieben wesentliche Fragen offen. Der Datenschutzrat forderte daher die fachzuständigen Ressorts auf […] ein abgestimmtes legistisches Gesamtpaket zu erstellen […]. Der Datenschutzrat hielt es für **unverzichtbar, dass er auch mit dem überarbeiteten und abgestimmten legistischen Paket rechtzeitig vor der Beschlussfassung einer Regierungsvorlage befasst werde,** um eine qualifizierte Diskussion zu führen und eine fundierte Stellungnahme abgeben zu können. Tatsächlich ist keine solche Befassung erfolgt, was der Datenschutzrat ausdrücklich bedauert. Umso nachdrücklicher fordert der Datenschutzrat die Berücksichtigung seiner nachstehenden Kritik im Zuge der parlamentarischen Behandlung der bezüglichen Regierungsvorlagen.

III. Grundsätzliches zur Vorratsdatenspeicherung

Die grundrechtliche Kernproblematik der Vorratsdatenspeicherung liegt darin, dass die Vorratsspeicherung von Telekommunikations- und Internetzugangsdaten im Sinne der Richtlinie 2006/24/EG die permanente Aufzeichnung des Kommunikationsverhaltens der gesamten europäischen Gesellschaft bedeutet. Die gewonnenen Daten geben detaillierten Aufschluss über Ausmaß und Intensität sozialer Beziehungen und ermöglichen ua. die Erstellung genauer Bewegungsprofile. Das Risiko missbräuchlicher Auswertungen in diese Richtung steigt exponentiell zur Menge der gesammelten Informationen. Auch die Informationsfreiheit im Sinne des Art. 10 EMRK erscheint durch den Überwachungsdruck bedroht.

Die Vorratsdatenspeicherung ist im Grunde eine Abkehr vom Grundsatz der Vertraulichkeit der Kommunikation aufgrund eines generellen Misstrauens gegenüber allen Menschen. Auch mit diversen verbesserten Rechtsschutzmaßnahmen bzw. „technischen Sicherungen“ lässt sich die oben skizzierten Problematik nicht beheben, sondern nur abmildern.

Folgerichtig hat der Datenschutzrat in allen seinen bisherigen Stellungnahmen zur **Vorratsdatenspeicherung** diese (stets einstimmig) **grundsätzlich in Frage gestellt** (vgl. DSR 2.9.2002, GZ 817.222/006-DSR/2002 ua.; zuletzt DSR 15.1.2010, GZ BKA-817.386/0003-DSR/2010).

IV. Zu ausgewählten vorgeschlagenen Änderungen im TKG 2003

A. Vorbemerkung

Vorab ist festzuhalten, dass sich die Nachvollziehbarkeit der datenschutzrechtlichen Relevanz der durch die Umsetzung der Vorratsdatenspeicherung ausgelösten Änderungen im TKG durch die gewählte Verweisungstechnik als sehr schwierig darstellt. Vor diesem Hintergrund wird auf vollumfängliche Zitate aus dem Gesetzestext tendenziell zugunsten einer an Sachthemen anknüpfenden und das jeweilige Problem umschreibenden Darstellungsweise verzichtet.

B. Zu Z 20 (§ 99 Abs 1 bis 5) und Z 22 (§§ 102a f) (Thema „Zweckbindung“)

1. Tendenz zur Aufweichung der Zweckbindungsregeln

Positiv anzumerken ist zunächst, dass der Gesetzgeber in § 99 TKGneu den Versuch unternimmt, eine abschließende Regelung der zulässigen Verwendung von Telekommunikationsdaten durch die Diensteanbieter vorzunehmen. So heißt es in § 99 Abs 1, dass Verkehrsdaten **„außer in den in diesem Gesetz geregelten Fällen“** nicht gespeichert oder übermittelt werden dürfen […]. „Diese Fälle“ sind auf den ersten Blick **abschließend** in § 99 Abs 5 leg cit geregelt, welcher bestimmt, dass „eine Verarbeitung von Verkehrsdaten zu Auskunftszwecken **zulässig ist** zur Auskunft über 1. […]“.

Hiebei fällt auf, dass die Formulierung des Einleitungssatzes des § 99 Abs 5 leg cit **im Vergleich zum Entwurf** aus dem seinerzeitigen Begutachtungsverfahren **abgeschwächt** wurde, indem das Wort „nur“ entfallen ist (ursprünglich: „Eine Verarbeitung von Verkehrsdaten zu Auskunftszwecken ist nur zulässig […]“). Da diese textliche Änderung keine Entsprechung in den Erläuterungen findet, kann über die Motive nur gemutmaßt werden. Betrachtet man § 99 Abs. 5 iVm Abs. 1 macht diese nachträgliche Abschwächung wenig Sinn. Außer es soll damit implizit zum Ausdruck gebracht werden, dass künftige Zweckerweiterungen durchaus intendiert sind.

Im Sinne der Rechtsklarheit und um jeden Zweifel an der systematischen Funktionalität des § 99 TKG neu als **zentrale, materienübergreifende Zweckbindungsregelung** betreffend die Verwendung von Telekommunikationsdaten auszuschließen, ist die Wiederaufnahme des Wortes „nur“ zu fordern.

2. Ermöglichung der Nutzung der Vorratsdaten für präventive Zwecke

In Z 4 des § 99 Abs 5 TKGneu fällt auf, dass **Vorratsdaten** (bis zu einem Zeitraum von drei Monaten vor Anfrage) nicht nur für Zwecke der Strafverfolgung, sondern **auch für Auskünfte an** nach dem SPG zuständige **Sicherheitsbehörden**, also zur „Prävention“ zur Verfügung stehen sollen. Insbesondere soweit dabei an die erste allgemeine Hilfeleistung durch die Sicherheitsbehörden im Unglücksfall mittels Ermittlung von Standortdaten gedacht ist, erscheint diese Regelung **nicht plausibel.** Die Abdeckung von Unglücksfällen, zu denen ohne Vorratsdatenspeicherung keine aktuellen Standortdaten mutmaßlich mitgeführter Endeinrichtungen mehr verfügbar

wären, wäre **per se** nämlich keine ausreichende Rechtfertigung für eine flächendeckende Speicherung von Standortdaten auf Vorrat.

An dieser Stelle ist daran zu erinnern, dass der Datenschutzrat eine Einbeziehung der **„Prävention“** in die Liste der **Speicherzwecke** (Strafverfolgung, Aufklärung) stets abgelehnt hat (Zitat aus GZ 817.222/0010-DSR/2005).

Aus der Sicht des Datenschutzrates sollte die Nutzung von Vorratsdaten insofern strikt auf Fälle der Aufklärung und Verfolgung von Straftaten beschränkt bleiben.

3. Nutzung der Vorratsdaten für Verfolgung von lediglich mit geringer Strafe bedrohten Handlungen

Gemäß § 102a Abs 1 TKGneu haben Anbieter von öffentlichen Kommunikationsdiensten Vorratsdaten „ausschließlich zur Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs 2a StPO rechtfertigt,“ zu speichern. Eine Beauskunftung über diese Daten ist nach 102b Abs 1 leg cit „ausschließlich aufgrund einer gerichtlich bewilligten Anordnung der Staatsanwaltschaft zur Aufklärung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs 2a StPO rechtfertigt“ zulässig.

Diese Formulierungen bedeuten **in der Zusammenschau** mit den unverändert gebliebenen sonstigen Regelungen der StPO, dass das **in früheren TKG-Entwürfen verfolgte Regelungsziel** der **Beschränkung** der Beauskunftung von Vorratdaten auf Zwecke der **Verfolgung schwerer Straftaten aufgegeben wurde.**

Zufolge § 76a Abs. 2 iVm Abs. 1 iVm § 99 Abs. 5 Z 2 TKG sind Anbieter von Kommunikationsdiensten sind auf Ersuchen von kriminalpolizeilichen Behörden, Staatsanwaltschaften und Gerichten, die sich auf die **Aufklärung** des konkreten **Verdachts einer (nicht näher qualifizierten) Straftat** einer bestimmten Person beziehen, zur Auskunft über […] **Zugangsdaten** (va IP-Adressen) verpflichtet. Als Vorratsdaten gespeicherte IP-Adressen sind also **für die Verfolgung sämtlicher im StGB verzeichneter Straftaten nutzbar.**

Gemäß § 135 Abs 2 Z 2 StPO iVm § 135 Abs 2a StPO kommt ein Zugriff auf Vorratsdaten (Standortdaten, Verbindungsdaten) im Fall, dass der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Auskunft ausdrücklich zustimmt (Bsp:

Rufdatenrückerfassung), bereits dann in Betracht, wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit einer **Freiheitsstrafe von mehr als sechs Monaten** bedroht ist, **gefördert** werden **kann.**

Nach § 135 Abs 2 Z 3 StPO iVm § 135 Abs 2a StPO kann auf Vorratsdaten zugegriffen wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, **die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, gefördert werden kann** und auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können.

Bereits im Jahr 2007 hat der Datenschutzrat hervorgehoben, dass im Rahmen der innerstaatlichen Umsetzung der RL 2006/24/EG der **ursprüngliche Zweck und Anlass für die Erlassung der Richtlinie** zu **beachten** ist, nämlich die **Bekämpfung von Terrorismus und organisierter Kriminalität** (vgl. Erwägungsgründe 7, 8, 9, 10 der RL 2006/24/EG). Innerhalb des durch die verbindlichen Regelungen des Gemeinschaftsrechts vorgegebenen Rahmens komme dem nationalen Gesetzgeber ein rechtspolitischer Gestaltungsspielraum zu, um die konkreten Maßnahmen zur Umsetzung der Richtlinie zu setzen. **Der Datenschutzrat hat daher dazu aufgerufen,** „bei der Ausübung dieses Gestaltungsspielraumes insbesondere den datenschutzrechtlichen Grundsätzen der **Zweckbindung** sowie der **Verhältnismäßigkeit** Rechnung zu tragen (DSR 16.5.2007, GZ BKA-817.304/0003-DSR/2007).

Konkret hat der Datenschutzrat damals vorgeschlagen, etwa an jene **Straftaten anzuknüpfen,** die **explizit** zur **Umsetzung internationaler Übereinkommen** bzw. europäischer **Rahmenbeschlüsse** zur **Bekämpfung organisierter Kriminalität** bzw. des **Terrorismus** in das StGB eingeführt wurden (d.h. §§ 278 sowie 278 a - d StGB). Darüber hinaus hielt er es für denkbar, Verbrechen im Sinne des § 17 Abs. 1 StGB in die Definition aufzunehmen, um Straftaten im oberen Kriminalitätsbereich einzubeziehen (DSR 16.5.2007, GZ BKA-817.304/0003-DSR/2007).

In seiner Stellungnahme vom 15. Jänner 2010 hat der Datenschutzrat das Erfordernis einer **möglichst restriktiven Definition „schwerer Straftaten“,** die sich am grundsätzlichen Ziel und Zweck der Vorratsdatenspeicherrichtlinie (der Bekämpfung organisierter Kriminalität und des Terrorismus) orientiert, betont. Zugleich lehnte er die **generelle Einbeziehung** von **Vergehen**, die **ausschließlich**

im Wege der Telekommunikation begangen werden, in den Kreis jener Straftaten, zu deren Verfolgung auf Vorratsdaten zurückgegriffen werden darf, als **unverhältnismäßig** iSd Art. 1 Abs. 2 DSG 2000 (sowie auch des Art. 8 EMRK) ab (BKA-817.386/0003-DSR/2010).

Der Datenschutzrat sieht keinen Anlass, von seinen obzitierten Positionen abzurücken und bedauert daher die oben skizzierte Inkonsistenz der getroffenen Regelungen.

C. Zu Z 22 (§ 102c Abs. 4) (Thema „Transparenz"; „Berichtspflichten")

Gemäß § 102c Abs. 4 haben die zur Speicherung verpflichteten Anbieter 1. für Zwecke der Kontrolle des Datenschutzes und zur Gewährleistung der Datensicherheit die sog. Protokolldaten gemäß Abs. 2 leg cit an die Datenschutzkommission und den Datenschutzrat sowie 2. zum Zweck der Berichterstattung an die Europäische Kommission und an den Nationalrat die Protokolldaten gemäß Abs. 1 Z 2 bis 4 an den Bundesminister für Justiz zu übermitteln.

Die Übermittlung der Protokolldaten hat auf schriftliches Ersuchen der Datenschutzkommission bzw. des Bundesministers für Justiz zu erfolgen; die Übermittlung an den Bundesminister muss darüber hinaus jährlich bis zum 31. Jänner für das vorangegangene Kalenderjahr erfolgen (§ 102c Abs. 5 leg. cit.).

Grundsätzlich sind die vorstehend zitierten Ansätze zur Stärkung der Transparenz im Umgang mit Vorratsdaten **zu begrüßen.** Allerdings weisen sie gewisse Inkonsistenzen und Lücken auf. So ist zunächst darauf hinzuweisen, dass der **Datenschutzrat kein Organ** der **Kontrolle** des Datenschutzes und zur Gewährleistung der Datensicherheit darstellt, sondern ein Beratungsorgan. Er kommt insofern nicht als Empfänger **personenbezogener** Daten, wie offenbar mit Z 1 des Abs 4 des § 102c leg cit intendiert, in Betracht, sondern wäre systematisch in Z 2 einzubringen.

Um zu verdeutlichen, dass sich der Kontrollzweck „Kontrolle durch die Datenschutzkommission" in § 102c Abs. 4 Z 1 leg cit auf Einzelfälle bezieht, wäre Abs. 5 entsprechend umzuformulieren („auf schriftliches Ersuchen der Datenschutzkommission im **Einzelfall"**).

Weiters ist darauf hinzuweisen, dass sich aus der Bestimmung selbst nicht ergibt, ob und inwieweit sich Pflichten des BMJ zur berichtsmäßigen **Aufbereitung** des von den Diensteanbietern übermittelten **Datenmaterials** ergeben. Die Erläuterungen gehen einfach davon aus (vgl. die Erl „Zu § 102c Abs. 2“). Unklar bleibt auch, inwieweit ohne nähere Ausführungen die Gewährleistung des Zwecks „Berichterstattung an den Nationalrat“ erfolgen soll (vgl. § 102c Abs. 4 Z 2 leg cit). Insgesamt wäre hier ggf. eine ausdrückliche Verordnungsermächtigung zweckmäßig, welche etwa die Struktur bezüglicher Berichte vorgeben könnte.

Im Übrigen ist an dieser Stelle aus datenschutzpolitischer Sicht festzuhalten, dass sich die Bemühungen um Transparenz nicht in der Umsetzung der statistischen Berichtspflichten nach Art. 10 der RL 2006/24/EG erschöpfen dürfen. Vielmehr erscheint es unverzichtbar **über die Fälle des behördlichen Zugriffs auf Vorratsdaten hinaus** auch die Fälle der Zugriffe auf Kommunikationsdaten zu erfassen, die noch nicht in diese Kategorie fallen, weil sie (auch/noch) für technische bzw. Rechnungslegungszwecke gespeichert sind bzw. verwendet werden. Nur auf diese Weise kann ein **vollständiges Bild** über die Eingriffe in das Kommunikationsgeheimnis im Interesse der Strafverfolgung bzw. Gefahrenabwehr entstehen und letztlich einer datenschutzpolitischen Bewertung zugeführt werden.

D. Zu Z 22 (§ 102a Abs. 8) (Thema „De facto-Speicherdauer 7 Monate“)

Nach § 102a Abs. 8 TKGneu sind die als Vorratsdaten zu speichernden Daten nach Ablauf der Speicherfrist zwar grundsätzlich unverzüglich zu löschen. Zugleich wird es den Diensteanbietern gestattet, diese Frist um einen Monat zu überziehen. Aus den Erläuterungen ist zu entnehmen, dass diese Regelung primär dem Komfort der Diensteanbieter dient. Diese Vorgangsweise führt somit in der Praxis dazu, dass **faktisch eine 7-monatige Speicherdauer** eingeführt.

Die **Erteilung einer Auskunft** nach Ablauf der Speicherfrist ist gleichwohl ausdrücklich für **unzulässig** erklärt. Ob diese gesetzliche Anordnung nicht insofern umgangen werden könnte, als Zwangsmitteln nach der StPO (Bsp: Beschlagnahme) eingesetzt werden, bleibt dahingestellt (vgl. dazu die Äußerung des Bundeskanzleramt-Verfassungsdienstes vom Jänner 2010, GZ BKA-810.022/0001-V/3/2010). Erwägenswert erschiene insofern eine ausdrückliche Klarstellung, dass

dieses Auskunftsverbot nicht durch Zwangsmaßnahmen im Rahmen des strafprozessualen Ermittlungsverfahrens umgangen werden darf.

E. Sonstiges (Thema „Datensicherheit“)

Wie dem Datenschutzrat bekannt wurde, ist in Umsetzung der Vorratsdatenspeicherrichtlinie geplant, eine Art technische Plattform einzurichten, welche eine standardisierte Abwicklung des Datenverkehrs zwischen auskunftspflichtigen Diensteanbietern und Sicherheits- bzw. Justizbehörden gewährleisten soll. Entsprechende Vorgaben sollen mittels Verordnung des BMVIT erfolgen. Soweit ersichtlich wäre im Falle der Umsetzung die Teilnahme für Diensteanbieter zwingend vorgesehen. Schon vor diesem Hintergrund erschiene eine entsprechende Vorherbestimmung einer solchen Verordnung durch das TKG mit Blick auf Art. 18 B-VG geboten.

IV. Zu ausgewählten vorgeschlagenen Änderungen in der StPO

A. Vorbemerkung

Vorab ist festzuhalten, dass sich die datenschutzrechtliche Bedeutung bzw. die Effektivität der „verfahrensrechtlichen Sicherungen“ der neuen Regelungen in der StPO jeweils nur in der Zusammenschau mit den oben diskutierten Vorgaben des TKG ergeben. In der Praxis neigen die Strafverfolgungsbehörden freilich erfahrungsgemäß dazu, sich verfahrenstechnisch ausschließlich an der StPO zu orientieren. Es stellt sich insofern die Frage des Erfordernisses begleitender Maßnahmen (Schulungen etc) um einen möglichst grundrechtsschonenden Vollzug des Instrumentariums der Vorratsdatenspeicherung und –nutzung zu gewährleisten.

Der Datenschutzrat erinnert in diesem Zusammenhang an seine Schlussfolgerung vom 15. Jänner 2010 (BKA-817.386/0003-DSR/2010), wonach er der Überzeugung ist, dass insbesondere im Lichte des Instruments der Vorratsdatenspeicherung **Begleitmaßnahmen** erforderlich erscheinen, um das **Bewusstsein der zuständigen Organe in den Sicherheitsbehörden und in der Justiz für die Sensibilität von Eingriffen in das Fernmeldegeheimnis zu stärken und so einen verhältnismäßigen Einsatz der bezüglichen Instrumente zu gewährleisten.**

B. Zu Art 1 Z 1 (§ 76a StPO) (Thema: „Bindung der Nutzung der Vorratsdaten an gerichtliche Bewilligung“)

1. Zum Gesetzestext

Betrachtet man § 102b Abs 1 TKGneu, so **scheint** es, als komme eine **Auskunft über Vorratsdaten nur aufgrund einer gerichtlichen Bewilligung** in Betracht. Eine Auskunft über Vorratsdaten ist demnach nämlich „ausschließlich aufgrund einer gerichtlich bewilligten Anordnung der Staatsanwaltschaft zur Aufklärung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs 2a StPO rechtfertigt, zulässig“.

Gemäß der neu einzufügenden Bestimmung des § 76a Abs. 2 iVm Abs 1 StPO sind künftighin Anbieter von Kommunikationsdiensten **auf bloße Anordnung** der **Staatsanwaltschaft** zur **Auskunft** über Stammdaten und **Zugangsdaten** nach § 99 Abs. 5 Z 2 TKG (dh insbesondere IP-Adressen) **verpflichtet.**

An dieser Stelle erinnert der Datenschutzrat einmal daran, dass Eingriffe in das verfassungsgesetzlich gewährleistete Fernmeldegeheimnis zufolge Art. 10a StGG nur auf Grund einer richterlichen Genehmigung zulässig sind. Die Einstufung von sog. IP-Adressen ist umstritten. Eine Judikatur des Verfassungsgerichtshofes zur genauen Reichweite des Schutzbereiches des Fernmeldegeheimnisses gemäß Art. 10a StGG existiert bis dato nicht. Die strafgerichtliche Praxis behandelte IP-Adressen bis dato als bloße „Stammdaten“ ohne jeden Bezug zum Fernmeldegeheimnis. Mit der nunmehrigen ausdrücklichen Bindung der Abfrage von IP-Adressen an eine staatsanwaltliche Anordnung lässt die Regierungsvorlage erkennen, dass sie dieser grob vereinfachenden Sicht der Strafgerichte nicht folgt bzw. korrigierend eingreift. Dieser Schritt geht allerdings nicht weit genug.

Bei genauerer Betrachtung zeigt sich nämlich, dass IP-Adressen, zu denen beim Provider Identitätsdaten erfragt werden, bzw. IP-Adressen, nach denen anhand anderer Kriterien beim Provider gefragt wird, typischerweise bereits im Anfragezeitpunkt **mit** bestimmten **inhaltlichen Daten** (gepostete Nachricht etc.) **verbunden** sind und deshalb zutreffender als „Nachrichten“ bzw. Inhaltsdaten behandelt werden sollten – mit entsprechenden Konsequenzen für den Rechtsschutz bzw. die strafprozessualen Sicherungen.

Unabhängig von der noch zu klärenden verfassungsrechtlichen Frage der inhaltlichen Reichweite des verfassungsgesetzlich gewährleisteten Fernmeldegeheimnisses nach Art 10a StGG erschiene es insofern konsequent, auch Informationseingriffe durch Beauskunftung von (dynamischen) IP-Adressen an eine gerichtliche Bewilligung zu binden.

Im Übrigen erscheint es **systematisch** verfehlt, den Regelungsinhalt des § 76a im 2. Abschnitt („Amts- und Rechtshilfe“) des 5. Hauptstücks der StPO zu platzieren. Es geht hier definitiv nicht um Amts- und Rechtshilfe, sondern um Ermittlungsmaßnahmen, wie sie im 6. Hauptstück der StPO normiert sind.

2. Zu den Erläuterungen („Zu Z 1 [§ 76a StPO]):

Die Erläuterungen sind insofern irreführend, als dort behauptet wird, dass die Strafverfolgungsbehörden im Zuge der Ermittlung von IP-Adressen „keine Kenntnis über der vorsorglich zu speichernden Daten erhalten“. Die Staatsanwaltschaft rufe im Rahmen einer Auskunftsanordnung nicht Verkehrsdaten selbst ab, sondern erhalte lediglich personenbezogene Auskünfte über den Inhaber eines bestimmten Anschlusses. Dabei bleibe die Aussagekraft dieser Daten eng begrenzt. Diese Ausführungen fußen offenbar auf einem Missverständnis. Wie im Vorabsatz bereits angedeutet, gibt es de facto keine Anfragen, ausschließlich auf Basis des Vorliegens einer IP-Adresse. Stets ist ein bestimmter damit verbundener der zu verbindender Inhalt (bspw. Droh-E-Mail; Posting im Internet etc.) Anlass der Auskunftsanordnung. Zudem ist jede Handhabung von solcherart erlangten Informationen durch die Kriminalpolizei der zuständigen Staatsanwaltschaft als datenschutzrechtlicher Auftraggeberin zuzurechnen, der die volle Weisungsbefugnis und damit der Zugang zu dieser Information zukommt.

Nicht nachvollziehbar sind weiters die – auch systematisch völlig verfehlten - Ausführungen in den Erl. zu § 76a StPO, soweit sie den behaupteten ausreichenden Rechtsschutz gegen staatsanwaltlich (ohne Gerichtsbewilligung) angeordnete Überwachungsmaßnahmen betreffen. Tatsächlich besteht etwa im Falle der allfälligen überschießenden Ermittlung von IP-Adressen bzw. darauf Bezug habender Daten für strafprozessuale Zwecke eine **Rechtschutzlücke.** Werden nämlich die Ermittlungen gegen die Betroffenen eingestellt und erfahren diese (typischerweise) erst nach Ende des Ermittlungsverfahrens von der Überwachungsmaßnahme, steht

ihnen kein Rechtsbehelf zur Überprüfung der Rechtmäßigkeit des Informationseingriffs mehr zu. Nur Personen, gegen die nach Abschluss der Ermittlungen das strafgerichtliche Anklageverfahren eröffnet wird, können sich in diesem Verfahren bei Gericht noch gegen Rechtsverstöße im Ermittlungsverfahren beschweren. Dies ergibt sich aus dem Wortlaut der §§ 106 Abs 1 und 107 Abs 1 StPO. Der in den Erläuterungen skizzierte komplizierte Weg über die Erneuerung des Strafverfahrens bleibt versperrt, da er eine belastende **gerichtliche** Entscheidung voraussetzt. Gerade im Falle der IP-Adressen wird aber auch künftig keine gerichtliche Bewilligung benötigt.

V. Zu den ausgewählten vorgeschlagenen Änderungen im SPG

A. Vorbemerkung

Die Regelungen zum Eingriff in das Kommunikationsgeheimnis für Zwecke der Sicherheitspolizei wurden teilweise neu gefasst und ergänzt. An den Grundsatzproblemen, die sich bei diesen Bestimmungen seit der SPG-Novelle 2008 aus rechtsstaatlicher und datenschutzrechtlicher Perspektive stellen, hat sich dabei wenig geändert. Durch die oben angesprochenen Nutzung von **Vorratsdaten auch für polizeiliche Zwecke** (IP-Adressauskünfte, Standortdaten) kann insgesamt von einer Verschärfung der Problemlage gesprochen werden.

B. Zu Art 2 Z 1 (§ 53 Abs 3a SPG) (Thema: „Eingriffsschwelle“)

Zufolge der Z 2 und 3 des § 53 Abs 3a SPG soll ein sicherheitsbehördlicher Zugriff auf IP-Adressen zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung bzw. ein solcher Zugriff auf Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, für Zwecke der **ersten allgemeinen Hilfeleistung** sowie zur **Abwehr allgemeiner Gefahren** (§ 16 SPG) zulässig sein. Die nach dem derzeit geltenden Wortlaut des § 53 Abs 3a noch bestehende Anknüpfung an eine „konkrete Gefahr“ soll entfallen.

Während gegen den Verwendungszweck der Hilfeleistung, die ja per se eine gegenwärtige Bedrohungslage voraussetzt, keine grundsätzlichen Einwände bestehen, stößt der Zweck der Abwehr allgemeiner Gefahren im Sinne des § 16 SPG auf umso gravierendere Bedenken. Dies deshalb, da dies vereinfacht gesagt eine

Möglichkeit der **Durchbrechung des Kommunikationsgeheimnisses** für **sämtliche** den Sicherheitsbehörden nach dem SPG übertragenen **Aufgaben** (außer reine Ordnungsstörungen) bedeutet. Zu diesen Aufgaben zählt nicht nur die Abwehr unmittelbar drohender Gefahren, etwa durch **jegliche** Arten gerichtlich **strafbarer** Handlungen (ohne Schwelle), sondern bspw. auch die Beobachtung von bloß abstrakt bzw potentiell „gefährlichen" sozialen Gruppen (Bsp: militante Tierschützer uä). Mithin werden die Sicherheitsbehörden punktuell auch **weit im Vorfeld** von Kriminalität tätig.

Aus grundrechtlichen Schranken, dem allgemeinen Verhältnismäßigkeitsgebot, aber auch der Regelungslogik des SPG erfließt allerdings, dass **mit der Zuweisung von bestimmten Aufgaben im SPG nicht** jeweils automatisch die **gesamte Bandbreite an Ermittlungsinstrumenten zur Verfügung stehen kann.** Diese Sichtweise unterstreicht etwa § 28a SPG, der sich mit der Erforschung von Gefahren beschäftigt. Zufolge dessen Abs. 2 dürfen die Sicherheitsbehörden und die Organe des öffentlichen Sicherheitsdienstes zur Erfüllung der ihnen in diesem Bundesgesetz übertragenen Aufgaben alle rechtlich zulässigen Mittel einsetzen, **die nicht in die Rechte eines Menschen eingreifen.** Und gemäß Abs 3 leg cit dürfen sie bei der Erfüllung dieser Aufgaben **in die Rechte eines Menschen nur dann eingreifen,** wenn eine solche **Befugnis** in diesem Bundesgesetz vorgesehen ist **und** wenn entweder **andere Mittel** zur Erfüllung dieser Aufgaben **nicht ausreichen** oder wenn der Einsatz anderer Mittel **außer Verhältnis** zum sonst gebotenen Eingriff steht.

Die Beobachtung etwa von „Gruppen" im vorstehenden Sinne kann typischweise weitestgehend durch die Auswertung offener Quellen (inklusive Webites) erfolgen. Ein zusätzlicher Rückgriff auf den einzelnen identifizierende Mittel (bspw. Aufdeckung der Identität von Leserbriefschreibern auf der Seite eines Online-Mediums mittels IP-Adressen-Anfrage) erschiene nicht nur **unverhältnismäßig,** sondern auch mit **ernsten Gefahren** für Privatsphäre, Meinungs- und Pressefreiheit der Bürger insgesamt verbunden – mit potentiell negativen Folgen für den demokratischen Willenbildungsprozess.

Aus dem Gesagten folgt, dass aus Verhältnismäßigkeitsgründen eine **Einschränkung** des **Anwendungsbereiches** der Möglichkeiten zur sicherheitsbehördlichen Durchbrechung des Kommunikationsgeheimnisses im Falle

der IP-Adressen **dringend geboten** erscheint. Dies könnte etwa durch Abstellen auf das Erfordernis der Abwehr einer **gegenwärtigen** Gefahr für das Leben, die Gesundheit, Freiheit oder Eigentum eines Menschen, die von einem gefährlichen Angriff im Sinne des § 16 Abs 2 Z 1, 2 und 4 SPG ausgeht, erfolgen.
An dieser Stelle sei daran erinnert, dass der Datenschutzrat in seiner Stellungnahme vom 15. Jänner 2010 ua. festgehalten hat, dass in einem liberalen demokratischen Rechtsstaat die Wahrung eines angemessenen Gleichgewichts zwischen dem Recht auf Privatsphäre und dem öffentlichen Interesse an der Aufrechterhaltung der öffentlichen Ordnung und Sicherheit sowie einer angemessenen Verfolgung von Straftaten bedingt, **dass mit der Ermittlung personenbezogener Daten verbundene Ermittlungs- bzw. Verfolgungsmaßnahmen grundsätzlich nur bei Vorliegen von ausreichend konkreten Verdachtsmomenten gesetzt werden dürfen** (Vgl. BKA-817.386/0003-DSR/2010).

C. Zu Art 2 Z 1 (§ 53 Abs 3a SPG) (Thema: „rechtssystematische Gesichtspunkte“)

Regelungssystematisch ist der gewählte Ansatz in den Ziffern 2 bis 4 verfehlt. Die polizeilichen Aufgaben sind im 2. Teil des SPG geregelt. Die darauf Bezug habenden Befugnisse finden sich in Teil 3 und 4 des SPG. Im hier interessierenden Teil 4 („Verwenden personenbezogener Daten“) ginge es darum, festzulegen, **für welche Aufgaben** im Sinne des 2. Teils des SPG nun genau **welche Befugnisse** nach § 53 Abs 3a f SPG zur Verfügung stehen sollen. Zweckmäßig und logisch nachvollziehbar wäre es also, auf die **erste allgemeine Hilfeleistung** durch Verweis auf die Stelle des SPG, in welcher sie **als Aufgabe** normiert ist (§ 19 SPG) Bezug zu nehmen. Eine Bezugnahme auf die Aufgabe der **Gefahrenabwehr** hätte dann folglich nicht bloß durch Verweis auf § 16 SPG, sondern auf den ersten Blick durch Zitierung der **Aufgabennorm** des § 21 SPG zu erfolgen. Mit Blick auf die im Vorabschnitt skizzierten Bedenken, wäre freilich ein **selektiver bzw. differenzierender** Rückverweis unter Bezugnahme auf die Definition in § 16 SPG ein gangbarer Weg (siehe oben).

D. Zu Art 2 Z 1 (§ 53 Abs 3b SPG) (Thema: „Missbrauchsprävention beim Einsatz von technischen Mitteln zur Lokalisierung [IMSI-Catchern]“)

§ 53 Abs 3b SPG gestattet den Sicherheitsbehörden (bereits bisher) ua. „technische Mittel zur Lokalisierung“ einer „Endeinrichtung zum Einsatz zu bringen“. Mit technischen Mittel sind sog. IMSI-Catcher gemeint. Dies sind Geräte, die primär dazu konstruiert sind, bestimmte Mobilfunkgespräche abzuhören. In einer „abgeschlankten“ Version können sie auch bloße Lokalisierungsfunktionen aufweisen. Um sicherzustellen, dass nicht etwa im Falle einer Lokalisierung auf der Grundlage von § 53 Abs 3b SPG irrtümlich Gesprächsinhalte abgehört werden, sollte klargestellt werden, dass für die hier interessierenden Zwecke überhaupt nur die Geräte mit reiner Lokalisierungsfunktion eingesetzt werden dürfen. Folgende Ergänzung am Ende des § 53 Abs 3b SPG sollte insofern erfolgen: „In letzterem Falle **dürfen keine technischen Mittel eingesetzt werden,** die **auch eine Überwachung der über eine solche Endeinrichtung übermittelten Nachrichten ermöglichen.“**

E. Zu Art 2 Z 1 (§ 53 Abs 3c StPO) (Thema: „Rechtsschutzgarantien bei heimlicher Überwachung“)

1. Allgemeines – Betroffeneninformation als Grundprinzip

Die Information Betroffener über die Erhebung und Verwendung ihrer Daten ist ein **datenschutzrechtliches Grundprinzip** und hat zudem **hohe rechtsstaatliche** Bedeutung, da sie Voraussetzung zur Wahrnehmung von Rechtsbelfen und damit einen funktionierenden Rechtsschutz ist. Dieses Prinzip gilt auch im Bereich der inneren Sicherheit. So sieht bspw. Art 16 des sog. EU-Rahmenbeschlusses (RB) für den Datenschutz in der 3. Säule (RB 2008/977/JI) ausdrücklich vor, dass die Mitgliedstaaten sicherstellen, dass die betroffene Person im Einklang mit dem innerstaatlichen Recht über die Erhebung oder Verarbeitung personenbezogener Daten durch ihre zuständigen Behörden informiert wird.

Zu erinnern ist weiters an die Empfehlung des Europarates Nr R (87) 15 aus 1987 betreffend die Nutzung personenbezogener Daten im Polizeibereich. Dort heißt es ausdrücklich in Punkt 2.2: „Werden personenbezogene Daten **ohne Wissen des Betroffenen gesammelt** und gespeichert, und sofern diese Daten nicht gelöscht werden, **sollte der Betreffende,** falls durchführbar, **darüber informiert werden,**

dass Daten über ihn gespeichert werden, **sobald der Gegenstand der polizeilichen Ermittlungen dadurch vermutlich nicht mehr beeinträchtigt wird.“**

Auch nach der stRsp des EGMR ist die nachträgliche Information des Betroffenen ein wesentliches Element der Anti-Missbrauchsgarantie bei geheimen Überwachungen (vgl. bspw. EGMR U 6.9.1978 - Klass – Serie A Bd 28 Rn 50 ff).

Der Datenschutzrat hat im Übrigen in seiner Stellungnahme vom 15. Jänner 2010 festgehalten, dass er nicht die Notwendigkeit ausreichender Instrumente für strafrechtliche Ermittlungen sowie zur polizeilichen Aufgabenerfüllung verkennt, **sofern** diese **in rechtsstaatlich einwandfreier Form eingesetzt werden** und sofern je nach Eingriffsintensität der **Rechtsschutz** Betroffener und die **Informationsverpflichtungen** ausgebaut werden (BKA-817.386/0003-DSR/2010).

2. Unzureichende Information nach § 53 Abs 3c SPGneu

a) Zu selektive Einbeziehung von Überwachungsfällen

Aktuell bestehen nach dem Regelungssystem des § 53 Abs 3a SPG keinerlei Verpflichtungen der Sicherheitsbehörden zur nachträglichen Information Betroffener über **heimliche Überwachungen.** Vor diesem prekären Hintergrund ist zunächst ausdrücklich zu begrüßen, dass im Zuge der Neustrukturierung des § 53 SPG gewisse nachträgliche Informationspflichten gegenüber den Betroffenen vorgesehen wurden.

Diese Informationspflichten nach § 53 Abs 3c SPGneu bleiben aber aus folgenden Gründen **völlig unzureichend.**

Zunächst ist festzuhalten, dass **nur die Fälle** nach § 53 Abs 3a Z 3 (Frage nach Namen und Anschrift auf Basis einer IP-Adresse) und Abs 3b (Standortdatenermittlung) SPG einer nachträglichen Informationspflicht unterliegen sollen. Dies ist nicht einsichtig. **Auch** in den Fällen nach § 53 Abs 3a Z 2 (Frage nach IP-Adresse zu einer Nachricht [Bsp. E-Mail]) und Z 4 (Rufdatenrückerfassung) SPG besteht ein **Informationsinteresse** der Betroffenen. Der Fall der Z 2 sollte schon deshalb einbezogen werden (ggf. iVm Z 3), da es sich hier um eine logische ermittlungstechnische Vorstufe zum Anwendungsfall der Z 3 und ggf. auch Z 4 handelt.

Hinsichtlich des Falles der Rufdatenrückerfassung nach § 53 Abs 3a Z 4 SPG ist va. zu bedenken, dass bei der Ermittlung von Anrufen auf eine bestimmte passive Nummer innerhalb eines **Zeitfensters** (Stichwort: vages Kriterium des "möglichst genauen Zeitraums" in § 53 Abs 3a SPG) eine **durchaus große Zahl von Anrufen** (etwa in einem Hotel oder öff Gebäude etc) **zum Gegenstand der Ausforschung werden können.** Je nach passiver Teilnehmernummer (Bsp: Drohanruf bei Abtreibungsklinik) kann **allein die Tatsache**, dass ein Teilnehmer diese angerufen hat, hohe Aussagekraft haben. Ergeben sich im Gefolge der Ermittlung der Identitätsdaten eines Anrufes und ggf. weiterer Daten keinerlei Verdachtsmomente und wurde er nicht persönlich kontaktiert, bleibt dem Betroffenen der Umstand seiner Ausforschung nach der vorgesehenen Rechtslage verborgen. Auch wenn keine Ermittlungsschritte gegen die Person gesetzt werden, könnte ihr Informationsinteresse darin bestehen, damit erst die Gelegenheit zur Nachfrage zu erhalten, ob die sie betreffenden Daten bspw. aus einer fallbezogenen Analysedatei wieder gelöscht wurden oder werden, zu erhalten.

b) Faktische Beschränkung bzw. Ausschluss durch Beschränkung auf Vorratsdaten

Indem § 53 Abs 3c SPGneu die Informationspflicht strikt auf jene Fälle begrenzt, in denen „die Verwendung von **Vorratsdaten** gemäß § 99 Abs. 5 Z 3 oder 4 iVm § 102a TKG 2003 erforderlich war“, läuft diese Pflicht faktisch vielfach ins Leere. Gerade im Falle von IP-Adressen wird nämlich einmal die Abgrenzung zwischen solchen, die als Vorratsdaten gespeichert sind, und solchen, die als „Rechnungsdaten“ gespeichert sind, schwer fallen. Damit wird einer willkürlichen bzw. restriktiven Auslegung der Informationspflicht Tür und Tor geöffnet. Zudem werden die Sicherheitsbehörden in vielen Fällen mit kurzfristig noch für Rechnungszwecke gespeicherten Daten das Auslangen finden. Die besagte Restriktion hätte daher **ersatzlos zu entfallen.**

c) Wertungswiderspruch im Vergleich der Informationspflichten nach SPG und StPO

Nachdrücklich zu betonen ist, dass sämtliche Betroffene nach § 138 Abs. 5 StPO nach Beendigung geheimer Ermittlungsmaßnahmen (§§ 135 Abs. 2 und 3 sowie 136) von der Staatsanwaltschaft über die Anordnung und gerichtliche Bewilligung solcher Maßnahmen unverzüglich zu informieren sind. Dies hat durch Zustellung der

Anordnung zu erfolgen. Ein Aufschub ist zulässig, solange durch sie der Zweck dieses oder eines anderen Verfahrens gefährdet wäre. Eine **Einschränkung** nach der Art der verwendeten Daten („Vorratsdaten“ oder andere) oder der Art der Überwachungsmaßnahme **besteht insofern nicht.** Auch vor diesem Hintergrund sind die im SPG vorgesehenen oben diskutierten Restriktionen in keiner Weise nachvollziehbar.

Zu Recht hat der Datenschutzrat daher bereits an früherer Stelle klargestellt, dass das **Schutzniveau für Betroffene**, **in deren Kommunikations- bzw. Fernmeldegeheimnis eingegriffen wird,** grundsätzlich **nicht davon abhängen darf, ob der Eingriff aus präventiven oder repressiven Gründen erfolgt.** Diesbezüglich sei insbesondere sicherzustellen, dass etwa das Schutzniveau nach der Strafprozessordnung **in der Praxis nicht** durch ein **willkürliches Ausweichen auf Befugnisse nach anderen Materiengesetzes unterlaufen werden kann** (BKA-817.386/0003-DSR/2010). **Diese Positionierung ist im gegebenen Kontext zu bekräftigen.**

3. Zur Frist innerhalb der Informationen vorzunehmen sind

Hier ist anzumerken, dass die Vorgabe der „ehestmöglichen“ Information aus sachlogischen Gründen bereits im 4. Satz des § 53 Abs 3c SPGneu eingebracht werden sollte, anstelle erst im 5. Satz darauf Bezug zu nehmen. Der Passus hätte also zu lauten:

> […] In den Fällen des Abs. 3a Z 3 sowie Abs. 3b ist die Sicherheitsbehörde verpflichtet, den Betroffenen **ehestmöglich** darüber zu informieren, dass eine Auskunft zur Zuordnung seines Namens oder seiner Anschrift zu einer bestimmten IP-Adresse (§ 53 Abs. 3a Z 3) oder zur Standortbeauskunftung (§ 53 Abs. 3b) eingeholt wurde, sofern hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 3 oder 4 iVm § 102a TKG 2003 erforderlich war. Dabei sind dem Betroffenen nachweislich ~~und ehestmöglich~~ die Rechtsgrundlage sowie das Datum und die Uhrzeit der Anfrage bekannt zu geben.

4. Zu den Ausschlussgründen betreffend Information der Betroffenen

Während im Gesetzestext die Rede davon ist, dass die Information und unterbleiben kann, wenn der Betroffene nachweislich Kenntnis erlangt hat oder die Information des Betroffenen unmöglich ist, sind die Erläuterungen vergleichsweise klarer formuliert. Dort heißt es: "In den Fällen, wo eine Kenntnisnahme durch den Betroffenen auf Grund dessen Ablebens oder Abgängigkeit **nachweislich** nicht möglich ist, hat eine Verständigung durch die Sicherheitsbehörden zu unterbleiben".

Zur Verdeutlichung dessen, was laut Erläuterungen meinen, sollte das Adjektiv „nachweislich“ im Gesetzestext zusätzlich auch vor dem Wort "unmöglich" stehen. Der Passus hätte also zu lauten:

Die Information Betroffener kann aufgeschoben werden, solange durch sie der Ermittlungszweck gefährdet wäre, und kann unterbleiben, wenn der Betroffene bereits nachweislich Kenntnis erlangt hat oder die Information des Betroffenen **nachweislich** unmöglich ist.“

5. Kontrolle der rechtmäßigen Handhabung des Aufschubes der Information

Unklar ist, ob und wie in der Praxis verhindert werden soll, dass sich die Sicherheitsbehörden in bestimmten Fällen auf Dauer auf den Ausschlussgrund der Gefährdung des Ermittlungszwecks berufen und die Information unterbleibt. Hier bedarf es einer entsprechenden **Konkretisierung,** etwa in Form der Verankerung der Pflicht zur Neuvorlage an den Rechtsschutzbeauftragten nach Ablauf einer festzulegenden Frist. Eine einmalige Information des Rechtsschutzbeauftragten, dass wegen Gefährdung der Ermittlungen nicht informiert wird, kann hier keineswegs genügen. Grundsätzlich ist anzumerken, dass eine langfristige Nichtinformation Betroffener unter Berufung auf Ermittlungen nur unter Einschaltung einer gerichtlichen Kontrollinstanz verantwortbar erschiene.

F. Zu Art 2 Z 3 (§ 53 Abs 3c StPO) (Thema: „Rechtsschutzgarantien bei heimlicher Überwachung“)

Gemäß § 91c Abs 1 3. Satz SPGneu ist der Rechtsschutzbeauftragte ua. über „die Information Betroffener (§ 53 Abs. 3c)“ […] ehestmöglich zu informieren.“ Aus den Erläuterungen ergibt sich, dass unter den Passus „Information Betroffener“ **auch die Fälle des Unterbleibens der Information bzw. des Aufschubs zu subumieren sind.** Im Sinne der Rechtsklarheit ist eine ensprechende Ergänzung des Gesetzestextes wie folgt zu fordern:

Darüber hinaus ist der Rechtsschutzbeauftragte über Auskunftsverlangen (§ 53 Abs. 3a Z 2 bis 4 und 3b), die Information Betroffener **sowie das Unterbleiben oder den Aufschub einer solchen** (§ 53 Abs. 3c), den Einsatz technischer Mittel zur Lokalisierung einer Endeinrichtung (§ 53 Abs. 3b) sowie den Einsatz von Kennzeichnerkennungsgeräten (§ 54 Abs. 4b) ehestmöglich zu informieren."

G. Zu Art 2 Z 4 (§ 91c Abs 1 letzter Satz SPGneu) (Thema: „Aufgaben des Rechtsschutzbeauftragten")

Nach dieser Bestimmung „obliegt" dem Rechtschutzbeauftragten die Prüfung der nach diesem Absatz erstatteten Meldungen." Unklar bleibt freilich, **was** der Rechtsschutzbeauftragte **als Ergebnis der Prüfung** unternehmen soll. Logisch wäre es, ihn zu verpflichten, bei Rechtsverstößen bzw. nicht mehr gerechtfertigtem Aufschub der Information der Betroffenen die ursprünglich meldende Sicherheitsbehörde **zu informieren**, welche dann von sich aus den rechtskonformen Zustand herzustellen hätte. Eine Präzisierung in diesem Sinne wird dringend angeregt.

Im Übrigen ist festzuhalten, dass die bloße **Pflicht zur Information** des Rechtsschutzbeauftragten im gegebenen Kontext kritisch zu sehen ist. Grundsätzlich sollten **geheime Überwachungsmaßnahmen** ab einer gewissen Schwelle, wie etwa beim Eingriff in das bedeutsame Kommunikationsgeheimnis, einer (bei Gefahr in Verzug: nachträglichen) **Genehmigung** unterworfen werden sollten und damit im Falle der (auch: nachträglich) nichtgenehmigten Vornahme automatisch rechtswidrig werden.

Überdacht sollte angesichts der in Aussicht genommenen Zusatzaufgaben auch die Stellung des Rechtsschutzbeauftragten insgesamt, uzw. insbesondere unter dem Gesichtspunkt der ausreichenden Ressourcenausstattung und Gewährleistung des äußeren Anscheins der Unabhängigkeit und Unparteilichkeit.

Der Datenschutzrat erinnert an dieser Stelle an seine Feststellung vom Jänner 2010, wonach ein **wesentlicher Gesichtspunkt** jedes **staatlichen Informationseingriffs** – abgesehen von dessen Verhältnismäßigkeit im allgemeinen – die Relation zwischen der jeweiligen Eingriffstiefe bzw. -breite einerseits und den gleichzeitig in Betracht kommenden **unabhängigen Kontrollinstanzen** sowie **wirksamen Rechtsschutzinstrumenten** andererseits ist. Als **unbestritten gilt,** dass eine

ununabhängige Kontrolle am ehesten durch Gerichte oder vergleichbare **gerichtsförmige Einrichtungen** gewährleistet werden kann (DSR 15.1.2010, GZ BKA-817.386/0003-DSR/2010).

H. Sonstiges

Angemerkt sei schließlich, dass im SPG bis dato ausreichende Regelungen über die Zulässigkeit der Weiterverwendung einmal erhobener Daten ebenso fehlen bereichsspezifischere Löschungsregelungen analog zur StPO. Schließlich wird zuwenig auf Schriftlichkeit von Ersuchen abgestellt. Diese Defizite werden naturgemäß auch auf dem Felde der Vorratsdatenspeicherung schlagend.