Wien, 30.03.2012

Struktur-Entwurf für einen Individualantrag gemäß § 140 B-VG
des AKVorrat.at gegen die Umsetzung der Vorratsdatenspeicherung in Österreich

A) Vollmachtsbekanntgabe

B) Individualantrag

ZUSAMMENFASSUNG / Punktation

1. Die VDS betrifft alle Nutzer von Kommunikationsdiensten aktuell, unmittelbar und nachteilig in ihrer Grundrechtssphäre

- Die Speicherung der Verbindungsdaten ist schon ein Grundrechtseingriff, nicht erst eine allfällige Auskunft an die Behörden
- Der Dienst-Anbieter hält sich nur an das Gesetz, diesen vor Gericht zu klagen ist nicht erfolgversprechend und daher nicht zumutbar (Prozesskostenrisiko)
- Die Datenschutzkommission ist hier nur für Streitigkeiten zu Auskunftsbegehren zuständig - Anbieter haben regelmäßig keinen Grund, die gesetzeskonforme Speicherung nicht offenzulegen (keine Beschwer) – im Detail aber schwierig (siehe ganz am Ende)
- Fazit: Der einzige zumutbare Weg, die grundrechtsverletzende Vorratsspeicherung zu bekämpfen, führt ohne Umweg zum VfGH --> Zulässigkeit des Individualantrags (die schwierigste rechtliche Hürde!)

2. Die VDS ist gar nicht geeignet, die vorgeblichen Zwecke zu erreichen

- Die von der zugrundeliegenden Richtlinie vorgegebene Bekämpfung schwerer Kriminalität wird durch die VDS nicht merkbar gefördert (belegt durch Studien, keine Gegenstudien, immer nur emotionale Einzelfälle)
- selbst für den mittelschweren Bereich - zB Straftaten mit knapp über einem Jahr Strafrahmen - konnte kein Anstieg der Aufklärungsquote belegt werden, wo die VDS schon umgesetzt wurde
- Geeignet ist die VDS höchstens, ein "diffuses Gefühl der ständigen Überwachung" (dt. BVErfG) zu erzeugen und damit soziale Kontrolle auszuüben (verborgener Zweck ohne echten Plan)

3. Die VDS ist selbst dort, wo sie vielleicht in manchen Einzelfällen die Ermittlungen unterstützt, nicht das schonendste Mittel, den Zweck zu erreichen

- in den meisten Fällen würden schon betrieblich notwendig vorhandene Daten reichen, wenn die Investitionen zur VDS besser in mehr Personal der Exekutive investiert und Ermittlungen beschleunigt würden

- in den übrigen Fällen würde ein abgekürztes Verfahren reichen, bei dem ein Gericht bei entsprechender Verdachtslage anordnet, bestimmte Daten von bestimmten Teilnehmern "einzufrieren" (sog. "Quick-Freeze")

4. Die VDS steht selbst dann, wenn man sie als das gelindeste, noch zum Ziel der Kriminalitätsbekämpfung führende Mittel ansieht, in keinem angemessenen Verhältnis zum Nachteil für die Einzelnen sowie die Gesellschaft

- je fragwürdiger die Eignung und die Notwendigkeit (im Sinne des gelindesten Mittels) erscheinen, desto höher sind die Anforderungen an die Verhältnismäßigkeit im

- die Güterabwägung zeigt - wenn überhaupt - nur einen geringen positiven Effekt in wenigen Einzelfällen gegenüber einem schweren Eingriff in die Privatsphäre praktisch der gesamten Bevölkerung

- Die Unverhältnismäßigkeit der VDS ergibt sich auch daraus, dass die Verwendungszwecke viel zu weit gefasst sind und keine ausreichenden Rechtsschutzmöglichkeiten zur Verfügung stehen

ZULÄSSIGKEIT

1. Anzufechtende Rechtlage

A) Kern der Anfechtung: Speicheranordnung im TKG einschließlich Verwendungszwecke

- § 102a TKG: Ordnet die Vorratsspeicherung an und zählt die Datenkategorien auf
  ➔ Anfechtung zur Gänze: Verbleibender Rumpf (zB Ausnahme kleiner Anbieter nach Abs. 6) ergibt sonst keinen Sinn mehr

- § 102b TKG: Regelt die Verwendung von Vorratsdaten
  ➔ Anfechtung zur Gänze:

- § 99 (5) Z 2, 3 und 4 TKG: beinhaltet Ausnahmen vom Grundprinzip des § 102b TKG zur Verwendung von Vorratsdaten, d.h. insb. auch Ausnahmen vom „Richtervorbehalt“ (Z2: insb. IP-Adressen u.a. für Strafprozess gem. § 76a StPO; Z 3: Standortdaten gem. § 53 Abs. 3b SPG; Z4: insb. IP Adressen, auch IMSI, IMEI,… für Sicherheitspolizei gem. § 53 Abs. 3a SPG)

- § 90 Abs. 8 TKG: Verpflichtung zur Führung von historischen Aufzeichnungen über die Standorte von Funkzellen – Voraussetzung zur Beauskunftung von Standortdaten als Vorratsdaten (evtl. als Antrag in eventu, weil vom Wortlaut her durchaus alleinstehen möglich)

B) Anfechtung von Bestimmungen im TKG, weil untrennbarer Zusammenhang mit A)
- § 92 Abs. 3 Z 6b TKG: Legaldefinition „Vorratsdaten“
- § 94 Abs. 4 TKG: Vorgaben zur technischen Einrichtung für die Datenübermittlung bei Auskünften nach StPO und SPG; betrifft Betriebsdaten und Vorratsdaten, daher nur Aufhebung der Wortfolge: „einschließlich der Übermittlung von Vorratsdaten,“ sowie im letzten Satz: „so-

wie die näheren Bestimmungen betreffend die Speicherung der gemäß § 102c angefertigten Protokolle“

- § 102c TKG: Datensicherheitsbestimmungen bzgl. Vorratsdaten – obwohl grundsätzlich eigentlich zur Verminderung des Grundrechtseingriffs, weil diese keinen Sinn mehr machen, wenn es keine Anordnung zur Vorratsspeicherung mehr gibt
- § 109 Abs. 3 Z 22 bis 26 TKG: Verwaltungsstrafbestimmungen iZm der VDS

C) Anfechtung von korrespondierenden Bestimmungen in StPO und SPG

System der abschließenden Aufzählung von Fällen der zulässigen Verwendung von Verkehrsdaten (einschl. Vorratsdaten) in § 99 Abs. 1 TKG → Aufzählung im TKG dem Grunde nach → Details in StPO bzw. SPG

- § 135 Abs 2 StPO → § 99 Abs 5 Z 1 TKG (Auskunft über Daten einer NÜ)
- **§ 135 Abs 2a StPO → § 102b TKG (Auskunft über Vorratsdaten)**
- § 135 Abs 3 StPO → § 94 Abs 4 TKG („Begleitende Rufdaten“ bei Inhaltsüberwachung)
- § 76a Abs 1 StPO → § 90 Abs 7 TKG („echte“ Stammdatenauskunft)
- **§ 76a Abs 2 StPO → § 99 Abs 5 Z 2 TKG (Zugangsdaten, insb. IP-Adr.)**
- § 53 Abs 3a Z 1 SPG → § 90 Abs 7 TKG („echte“ Stammdatenauskunft)
- **§ 53 Abs 3a Z 1 SPG → § 99 Abs 5 Z 3 TKG (Bezug auf ein best. Gespräch)**
- **§ 53 (3a) Z 2 u 3 SPG → § 99 Abs 5 Z 4 TKG (Zugangsdaten, insb. IP-Adr.)**
- **§ 53 Abs 3b SPG → § 99 Abs 5 Z 3 TKG (bezüglich Standortdaten)**

Argumentation in eventu:

Falls die VDS nicht schon dem Grunde nach als unverhältnismäßig gesehen wird, ergibt sich die mangelnde Verhältnismäßigkeit daraus, dass die Normen, welche die Verwendungszwecke regeln, eine überschießende Verwendungsmöglichkeit einräumen:

- → Insb. bzgl. IP-Adressen: überhaupt keine Einschränkung, Ermittlung bzw. Gefahrenabwehr bzgl. jeder gerichtlich strafbaren Handlung, keine Einschränkung auf überragende Rechtsgüter, zB Leben, Gesundheit, Freiheit (§ 76a Abs. 2; § 53 Abs. 3a SPG)
- → Bzgl. Standortdaten: § 53 Abs. 3b SPG: kein effektiver Rechtsschutz, keine Sicherstellung, dass Abfragen tatsächlich auf den von § 53 Abs. 3b SPG beschriebenen Zweck beschränkt bleibt (Abwehr einer Gefahr vom Inhaber der lokalisierten Endeinrichtung, zB Tourengeher, Lawinenopfer) → nur die Information durch den Anbieter selbst wäre ein effektiver Schutzmechanismus (Ermittlungszweck kann bei Hilfeleistung kaum gefährdet werden; Argumentation zum Sonderfall der Entführung)

2. Betroffenheit der AntragstellerInnen (durch 1.)

- unmittelbare Betroffenheit
  - Warum ist schon die Speicherung von Verkehrsdaten zur Telekommunikation ein Grundrechtseingriff?
  - Verträge auf den Namen der AntragstellerInnen mit Mobilfunkanbieter, Festnetz, Internetzugangsanbieter, e-mail Dienstanbieter, Voice over IP

- aktuelle Betroffenheit
  - Warum wird der Grundrechtseingriff gegenwärtig durch das Gesetz selbst bewirkt, ohne durch einen Bescheid oder ein Gerichtsurteil aktualisiert zu werden?

- Gesetz per 01.04.2012 in Kraft
- Sofortige Anwendbarkeit der neuen Rechtlage auf sämtliche bestehenden Verträge: Verbindungsdaten, die am 1.4.2012 beim Anbieter noch aus betrieblichen Gründen vorliegen und mangels weiterer betrieblicher Rechtfertigung eigentlich gelöscht werden müssten, sind nun aufgrund § 102a TKG zu speichern
- Es entstehen bei jedem/jeder AntragstellerIn tatsächlich Verbindungsdaten, welche der Speicherung unterliegen – die AntragstellerInnen haben die Verträge abgeschlossen, weil sie die Kommunikationsdienste auch tatsächlich nutzen

- rechtliche Betroffenheit
  - Warum bewirkt die angefochtene Rechtslage nicht bloß faktische/wirtschaftliche Interessen der BeschwerdeführerInnen? Betroffene subjektive Grundrechte der AntragstellerInnen (welche Grundrechte? –kurzer Abriss + Judikaturnachweise EGMR, VfGH):
    - Art. 8 EMRK (Privatleben und Schutz der Korrespondenz)
    - Art. 10 EMRK (Meinungs- und Informationsfreiheit, Redaktionsgeheimnis)
    - Art. 1 § 1 DSG 2000 (Grundrecht auf Datenschutz)
    - Art 10a StGG (Fernmeldegeheimnis)
    - in eventu Art. 7 (Privat- und Familienleben) und Art 8 (Grundrecht auf Datenschutz) und Art 11 (Meinungs- und Informationsfreiheit) EU Grundrechtecharta

- Unzumutbarkeit eines Umweges
  - möglicher Umweg wäre ein Zivilverfahren gemäß §§ 1 Abs. 5 in Verbindung mit 27 (Recht auf Löschung) und 32 (Zivilrechtsweg) DSG
  - Auskunftsbegehren gemäß § 26 DSG an die DSK?

→ Gem. der Judikatur des VfGH ist nicht zumutbar dass die AntragstellerInnen:
Ein strafbares Verhalten provozieren, nur um einen Weg zum VfGH zu finden
Ein Verfahren (vor allem bei Kostenrisiko) allein deshalb führen, um einen Weg zum VfGH zu finden
Einen Feststellungsbescheid allein deshalb begehren, um einen Weg zum VfGH zu finden

BESONDERES PROBLEM zum „Umweg“ Auskunftsbegehren gem. § 26 DSG:

- ➔ Der Wortlaut des TKG lässt keine Selbstauskunft zu. Die Zulässigkeit einer Auskunft nach § 26 DSG würde sich nur ergeben, wenn man diesem in verfassungskonformer Interpretation (§ 1 (3) DSG) den Vorrang vor den TKG Bestimmungen (§99 (1) iVm 102b (1)) einräumt, obwohl diese sowohl lex specialis als auch lex posterior sind. Beispiel: Ein Beschuldigter im Strafverfahren begehrt Auskunft über seine eigenen Vorratsdaten, um sich im Strafverfahren freibeweisen zu können (zB „ich war gar nicht am Tatort zu dem Zeitpunkt“) → hier würde der verfassungsrechtliche Interpretations-"Hebel" wohl auch in Art 6 EMRK liegen (Waffengleichheit).
- ➔ Problem: Einige Anbieter gehen in der Praxis davon aus, dass sie ein Auskunftsbegehren nach § 26 DSG wegen der abschließenden Aufzählung im TKG nicht beantworten dürfen!

MATERIELLER TEIL

Argumentation I: Zweck der durch RL vorgegeben, ist mit dem Eingriff nicht verhältnismäßig (Geeignetheit, Notwendigkeit, Adäquanz, Rechtsschutz)

Argumentation II: Falls Vorratsdatenspeicherung abstrakt zulässig sein soll, ist die konkrete Ausführung in § 135 Abs. 2a, § 76a Abs. 2 StPO und § 53 Abs. 3a und 3b SPG nicht verhältnismäßig (zu weit, keine Schutzmaßnahmen etc.)

1. § 102a TKG
   - Art …. Eingriff
   - Art ….Eingriff

2. § 102b und § 102c TKG
   - Art …. Eingriff
   - Art ….Eingriff

ANTRÄGE

1. = aufzuhebende Wortfolge in den jeweiligen Bestimmungen.
2. in eventu – Anregung zur Einleitung eines Vorabentscheidungsverfahrens beim EuGH
3. Kosten beantragen

SCHWIERIGKEIT:

Ein Antrag auf Normenaufhebung erfordert, dass die AntragstellerInnen exakt bezeichnen, welche Normen aus dem Rechtsbestand auszuscheiden sind, um die Grundrechtsverletzung zu beseitigen. Der VfGH ist dabei an die Anträge und deren Argumentation gebunden (keine Ausdehnung von Amts wegen!) Dabei gibt die Rechtssprechung des VfGH sehr enge Vorgaben, die teilweise sehr schwer miteinander Vereinbar sind:

- Es darf nicht mehr aufgehoben werden, als unbedingt notwendig ist, um das Ziel (Beseitigung der Grundrechtsverletzung) zu erreichen
- Die Aufhebung gemäß dem Antrag muss die Grundrechtsverletzung aber auch wirklich beseitigen (nicht zu viel, aber auch nicht zu wenig anfechten!)
- Der nach der Aufhebung verbleibende Rechtsbestand darf nicht sinnverändert oder überhaupt sinnlos sein (sinnlos wäre zB ein Verweis auf eine Norm, die nach der Aufhebung gar nicht mehr existiert)

Arbeitskreis Vorratsdaten Österreich (AKVorrat.at) A-1070 Wien Westbahnstraße 46/1A
ZVR-Zahl: 140062668 UID: ATU66502037 Erste Bank BLZ 20111 Kto. 29420544100
Web: http://www.akvorrat.at | E-Mail: info@akvorrat.at | Twitter: @AKVorrat_at