Stellungnahme des Ludwig Boltzmann Instituts für Menschenrechte (BIM)

im Begutachtungsverfahren
über die Regierungsvorlage zum „Bundesgesetz,
mit dem das Telekommunikationsgesetz 2003 – TKG 2003 geändert wird"

1. Allgemeines

Grundsätzlich sollte das Verhältnis zwischen einem demokratischen Verfassungsstaat und seiner Gesellschaft von Vertrauen geprägt sein. Der Einzelne kann und soll darauf vertrauen dürfen, dass in seine grundrechtlich geschützten Positionen im Zuge von Ermittlungstätigkeiten bzw. Strafverfolgungsmaßnahmen nur bei Vorliegen entsprechender Verdachtsmomente, als *ultima ratio*, unter Wahrung der rechtstaatlichen Prinzipien, insbesondere unter Beachtung des Verhältnismäßigkeitsprinzips eingegriffen wird. Der Grundsatz, dass gegen eine bestimmte Person ausschließlich bei Vorliegen von Verdachtsmomenten Ermittlungs- bzw. Verfolgungsmaßnahmen gesetzt werden, zieht sich einem roten Faden gleich durch die diesbezüglich relevanten Bestimmungen des VStG, der StPO und des SPG.[1] Hierzu gehört aber nicht eine verdachtsunabhägige, gleichsam antizipierte „Sicherung von Beweismitteln", wie sie nun in der Form der Vorratsspeicherung von Telekommunikationsdaten in das österreichische Rechtssystem Einzug findet. Eingriffe in die grundrechtlich geschützten Bereiche einer beliebigen Person ohne jedes Verdachtsmoment zum Zwecke „der Ermittlung, Feststellung und Verfolgung von schweren Straftaten", wie es in Art. 1 der Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten (die mit der vorliegenden Regierungsvorlage einer TKG-Novelle umgesetzt werden soll) heißt, wären grundsätzlich als Akt der Willkür einzustufen und somit verfassungswidrig.

Zwar wurde schon bislang eine Vielzahl von Daten der EinwohnerInnen dieses Landes erfasst und verarbeitet. Diese Datenanwendungen erfolg(t)en in aller Regel aber entweder (v.a. bei Auftraggebern des privaten Bereichs) zur Erfüllung eines Vertrages und somit zumindest mittelbar auf Wunsch bzw. mit Zustimmung der datenschutzrechtlich Betroffenen oder aber (v.a. bei Auftraggebern des öffentlichen Bereichs) mit dem Ziel, der Gesellschaft die unterschiedlichsten Leistungen der öffentlichen Daseinsversorgung zur Verfügung zu stellen. Davon unterscheidet sich die Vorrats-

[1] Beispielsweise sei nur auf die in § 139ff StPO normierten Voraussetzungen für die Vornahme einer Hausdurchsuchung – die ebenfalls in den Schutzbereich des Art. 8 EMRK fällt und der eine ähnliche Interessens- und Gefährdungslage zu Grunde liegt – verwiesen. Eine Hausdurchsuchung darf nach der eindeutigen Anordnung des § 139 Abs. 1 StPO „nur dann vorgenommen werden, wenn *gegründeter Verdacht* vorliegt, daß sich darin *eine eines Verbrechens oder Vergehens verdächtigte Person* verborgen halte oder daß sich daselbst Gegenstände befinden, deren Besitz oder Besichtigung für eine *bestimmte Untersuchung* von Bedeutung sein könne." (kursive Hervorhebung von den Autoren). Vergleiche auch die – im vorliegenden Zusammenhang besonders beachtenswerte – Regelung des § 149a Abs. 2 Ziff. 3 lit. a StPO, wonach eine Telekommunikationsüberwachung u.a. nur dann zulässig ist, wenn „der Inhaber des Teilnehmeranschlusses selbst *dringend verdächtig* ist, die Tat begangen zu haben". Ob sich nun die Überwachung (auch) auf den Inhalt einer Kommunikation richtet oder „lediglich" die Erfassung von Verkehrs- und Standortdaten zum Gegenstand hat, vermag am Umstand, dass eine jeweils vergleichbare Interessens- und Gefährdungslage vorliegt, nichts zu ändern.

datenspeicherung schon alleine durch ihre Zielsetzung in fundamentaler Weise, da diese auf Grundlage der Richtlinie (und umgesetzt durch die geplante TKG-Novelle) in Ansehung von Telekommunikations- und Bewegungsdaten ohne Unterschied ausschließlich zum Zwecke der Ermittlung, Feststellung und Verfolgung von Straftaten erfolgt.

Dem TKG in der derzeit (noch) geltenden Fassung ist nun eine beschränkte Speichermöglichkeit nicht unbekannt. Im Sinne des oben angesprochenen Vertrauensgrundsatzes konnte der Einzelne aber bisher davon ausgehen, dass nur im unbedingt zur Erfüllung des auf seinen Wunsch (und somit mit seiner Zustimmung) abgeschlossenen Vertrages erforderlichen Ausmaß in grundrechtliche geschützte Positionen eingegriffen wird. Mit dieser eingriffsminimierenden rechtsstaatlichen Tradition bricht der gegenständliche Entwurf in Umsetzung der beschlossenen Richtlinie. Während Daten grundsätzlich gelöscht werden müssen, wenn und soweit sie für die Bereitstellung des Telekommunikationsdienstes und in weiterer Folge für die Abrechnung nicht mehr erforderlich sind, wird diese im Sinne eines effektiven und grundrechtskonformen Datenschutzes normierte Löschungsverpflichtung nun in eine verdachtsunabhängige, flächendeckende Speicherungspflicht verkehrt. Jeder Kommunikationsvorgang ist nunmehr potentiell terrorverdächtig und muss daher erfasst werden. Dies stellt im Ergebnis einen Paradigmenwechsel dar, der insbesondere aus grundrechtlicher Sicht einer entsprechenden Rechtfertigung bedarf.

Damit erhebt sich die Frage, ob nicht der Regelungsgehalt der Richtlinie selbst einen unverhältnismäßigen Eingriff in das durch Art. 8 EMRK geschützte Recht auf Achtung der Privatsphäre bewirkt, das auch das Recht auf Datenschutz sowie der Korrespondenz (des „Briefverkehrs") umfasst, denn Eingriffe in dieses Recht sind nach der Rechtsprechung (des EGMR, aber auch nationaler Höchstgerichte) nur zulässig, sofern diese zur Erreichung einer der in Art. 8 Abs. 2 EMRK genannten zulässigen Ziele in einer demokratischen Gesellschaft unbedingt erforderlich sind. Auch wenn das Speichern von Verkehrs- und Standortdaten auf den ersten Blick harmlos erscheinen mag, offenbart sich doch bei genauerem Hinsehen, dass die Vorratspeicherung in ausgesprochen massiver Weise in die grundrechtlich geschützten Positionen eingreift: Im Vergleich zum Inhalt aufgezeichneter Gespräche können die gewonnen Verkehrs- und Standortdaten computerunterstützt ungleich leichter, in kürzerer Zeit und größerem Umfang ausgewertet werden. Soziale Netzwerke können bis in letzte Detail ebenso nachvollzogen werden, wie - je nach Telefonierverhalten – mehr oder weniger genaue Bewegungsprofile jedes/r Österreichers/in, der/die ein Mobiltelefon sein Eigen nennt, erstellt werden können. Schließlich geben auch Verkehrsdaten mitunter Aufschluss über den Inhalt der Kommunikation (Anruf bei Aidshilfe, Sexhotline, Rat auf Draht etc.).

2. Gefährdete Inhaltsdaten

Nach der eindeutigen Anordnung des Art. 5 Abs. 2 dürfen keinerlei Daten gespeichert werden, „die Aufschluss über den Inhalt einer Kommunikation geben". Mit gutem Grund stellt sich daher hier die Frage, ob nicht aus den erfassten Daten mitunter Rückschlüsse auf den Inhalt möglich sind. So wird ein Anruf in einer Anwaltskanzlei regelmäßig eine anwaltliche Konsultation, ein Anruf bei der „Aids-

hilfe", der „Aktion Leben" oder etwa bei „Rat auf Draht" in aller Regel eine entsprechende Beratung oder Hilfestellung zum Inhalt haben. Nun könnte argumentiert werden, dass ja nicht der Inhalt der Gespräche, sondern nur die Verbindungsdaten erfasst würden und ein derartiger Rückschluss nicht zwingend (inhaltlich) richtig wäre. Diesem Einwand könnte leichter Folge gegeben werden, wenn der Richtliniengeber nicht selbst die Formulierung „Aufschluss über den Inhalt" gewählt hätte. Diese Formulierung weist in auffallender Weise Parallelen zu Art. 8 Abs. 1 der Richtlinie 95/46/EG auf. Dieser Bestimmung zu Folge dürfen Daten, „aus denen die rassische und ethnische Herkunft, politische Meinungen (...) hervorgehen sowie (...) Daten über die Gesundheit oder Sexualleben" (sog. sensible Daten) grundsätzlich nicht verarbeitet werden. Für die „Sensibilität" eines Datum ist es nun keinesfalls erforderlich, dass das sensible Faktum, also etwa die ethnische Herkunft oder die politische Meinung, selbst Gegenstand des Datums ist, sondern genügt es, wenn auf dieses rückgeschlossen werden kann. Als Beispiel sei auf die Mitgliedschaft bei einer Vereinigung, der die Nähe zu einer Partei nachgesagt wird, verwiesen. Das Datum „Mitgliedschaft" bei dieser Vereinigung wäre ein sensibles, obgleich die „politische Meinung", also das die Sensibilität begründende Faktum, nicht selbst Gegenstand des Datums ist, sondern aus der Mitgliedschaft auf diese rückgeschlossen würde. Ähnlich verhält es sich mit dem Datum "Besuch beim Lungenfacharzt". Dieses Datum wird als sensibles angesehen,[2] obwohl es sich ja auch um einen Freundschaftsbesuch bei Kaffee und Kuchen handeln könnte. In beiden Fällen ist also das die Sensibilität begründende Faktum nicht selbst Inhalt des Datums, sondern kann mit einiger Wahrscheinlichkeit auf dieses rückgeschlossen werden. Da in eingangs beispielhaft genannten Fällen die erfassten Verkehrsdaten – wie es in Art. 5 Abs. 2 der Richtlinie heißt – „Aufschluss über den Inhalt der Kommunikation geben", sollten die Daten in diesen wie auch ähnlich gelagerten Fällen nicht auf Vorrat gespeichert werden und daher entsprechende Ausnahmeregelungen in den Gesetzesentwurf aufgenommen werden. Dies gilt insbesondere im Hinblick auf Berufsgruppen und Institutionen, deren Kommunikation mit der Außenwelt typischerweise sensible Inhalte zum Gegenstand hat (wie zB in den Bereichen Gesundheit, Medizin, Psychologie/Psychiatrie, Recht und Soziales etc.).

3. Konventionswidrigkeit der Richtlinie

Betrachtet man nun die auf europäischer Ebene im Zuge der Erarbeitung der Richtlinie veröffentlichen Dokumente, so verwundert zunächst, dass weder im Vorfeld noch im Zuge der Beschlussfassung ein aussagekräftiger Nachweis der Notwendigkeit bzw. des Mehrwertes der Maßnahme geführt wurde. Die Aussage, dass Telefondaten zur Aufklärung der ausgesprochen tragischen Madrider Terroranschläge beigetragen haben, vermag eine aussagekräftige Notwendigkeitsanalyse der Vorratsspeicherung nicht einmal ansatzweise zu ersetzen. Für eine solche hätte über einen längeren Zeitraum hinweg beobachtet werden müssen, in wie vielen Fällen welche Daten in welchem Umfang zur Aufklärung welchen Vergehens und/oder Verbrechens beigetragen haben und wie viel Zeit zwischen der Erfassung und der An- bzw. Abfrage verstrichen ist.

[2] Vgl. etwa Recht der Datenverarbeitung, RDV 2003, Heft 6, S 308 f.

Betrachtet man die beschlossene Maßnahme genauer, so zeigt sich, dass dem massiven Eingriff in die Grundrechte der Betroffenen nur ein ausgesprochen bescheidener Mehrwert für die Strafverfolgung gegenüber steht. So ist es etwa für den Bereich der Festnetz- aber auch Mobiltelephonie ein Leichtes, beispielsweise durch Verwendung von öffentlichen Telefonzellen oder Wertkarten- bzw. im (nicht EU-)Ausland angemeldeter Handys der auf konkrete Personen rückführbaren Datenaufzeichnung zu entgehen. Der Aufzeichnung von Email-Daten im Rahmen der Vorratsspeicherung kann durch Verwendung außereuropäischer Emailprovider entgangen werden. Sollte jemand also der Vorratspeicherung seiner Daten (bzw. genauer: der Möglichkeit der Rückführung der Daten auf seine Person) entgehen wollen, so ist ihm/ihr dies ohne jedes technisches Spezialwissen mit einfachsten Mitteln (so man den geringen Zusatzaufwand in Kauf nimmt) möglich. Stehen diese und ähnliche Möglichkeiten schon jedem „Normalverbraucher" zu Verfügung, verfügen – und davon kann wohl mit gutem Grund ausgegangen werden – terroristische oder andere kriminelle Vereinigungen, deren Bekämpfung die Vorratsspeicherung ja in erster Linie dient, über ungleich bessere technische Möglichkeiten und Kenntnisse. Für Angehörige solcher Vereinigungen ist es daher unzweifelhaft ein Leichtes der auf sie rückführbaren Datenaufzeichnung zu entgehen. Letztendlich werden somit fast ausschließlich Daten jener Personen erfasst, die entweder keine Kenntnis von der Datenaufzeichnung haben oder aber kein Interesse an den Tag legen, der Datenaufzeichnung zu entgehen, also die Daten ganz normalen „Durchschnittsverbraucher".

Zwar können gespeicherte Daten erheblich zur Aufklärung von Straftaten beitragen und als Beweise im Strafverfahren dienen, zur Ermittlung von Straftaten – insbesondere mit terroristischem Hintergrund und im Zuge organisierter Kriminalität – sind sie auch nach den bisherigen Erfahrungen alleine schon aufgrund der kaum zu bewältigenden Datenmengen wenig geeignet. Da nach den Erwägungen der Richtlinie Letzteres im Vordergrund zu stehen scheint, um den oben beschriebenen Paradigmenwechsel zu begründen, scheint die Vorratsdatenspeicherung im Sinne der grundrechtlich gebotenen Verhältnismäßigkeitsprüfung schlicht *nicht geeignet* zu sein, einen Grundrechtseingriff zu rechtfertigen. Und was den Zweck der Verfolgung von Straftaten anbelangt, so sind Zugriffe auf bestehende Datenanwendungen sicherlich grundsätzlich gerechtfertigt, jedoch wird es hier zweifellos genügen, auf diejenigen Verkehrsdaten zurückzugreifen, die die Netzwerkbetreiber für Zwecke der Abrechnung ohnehin rechtlich zulässig erfassen und verarbeiten sowie für beschränkte Zeit aufbewahren dürfen. Eine darüber hinaus gehende Speicherung dürfte auch für Zwecke der Verfolgung schwerer Straftaten im Sinne der Eingriffstatbestände des Art. 8 Abs. 2 EMRK nicht erforderlich sein.

Angesichts dieses Befunds, der sich gegen die – von allen EU-Mitgliedstaaten umzusetzende – Richtlinie wendet, sind die Autoren der Ansicht, dass die Umsetzung nur im derzeit unbedingt erforderlichem Ausmaß erfolgen, sich also an den Mindestvorgaben der Richtlinie orientieren sollte.

Zu erwarten ist, dass Betroffene gestützt auf Art. 8 EMRK sowie Netzwerkbetreiber aus dem Blickwinkel einer mit gutem Grund argumentierbaren Verletzung des Rechts auf Achtung des Eigentums iSd Art. 1 des 1. Zusatzprotokolls zur EMRK – da die Kosten der Vorratsdatenspeicherung auf

sie überwälzt werden – rechtliche Schritte ergreifen werden, die zu einer Überprüfung der TKG-Novelle vor dem Verfassungsgerichtshof führen könnten, der dabei allerdings den Vorrang des Gemeinschaftsrechts zu beachten hätte. Jedenfalls aber verblieben den Betroffenen wie den Netzwerkbetreibern die Möglichkeit, gegen eine auf die TKG-Novelle gestützte letztinstanzliche Entscheidung des VfGH und unbeachtlich einer Entscheidung des EuGH in einem allfälligen Vorabentscheidungsverfahren vor dem EGMR Beschwerde zu erheben. Dieser könnte im Zuge der Überprüfung des innerstaatlichen Rechtsakts zum Ergebnis gelangen, dass die Richtlinie – für deren Erlassung alle EU-Mitgliedstaaten Verantwortung tragen – Art. 8 EMRK und Art. 1 des 1. ZPEMRK verletzt, woraus die Notwendigkeit ihrer Aufhebung folgen könnte.

4. Umsetzung der Richtlinie durch die geplante TKG-Novelle 2007

Im Folgenden wird auf einige Bestimmungen des Begutachtungsentwurfs näher eingegangen:

a. zu Z 5:

Österreich hat von der in Art. 15 der Richtlinie (RL) vorgesehenen Möglichkeit, die Anwendung der RL auf die Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie und Internet-Email bis zum 15.03.2009 aufzuschieben, Gebrauch gemacht. Wie oben dargelegt steht die RL in einem Spannungsverhältnis insbesondere zu Art. 8 EMRK, weshalb anzunehmen ist, dass mittelfristig, möglicherweise vor März 2009, durch den EGMR über die Rechtmäßigkeit der Maßnahme abgesprochen wird. Da darüber hinaus auch Verfahren, die die Rechtmäßigkeit der Rechtssetzung in Richtlinienform zum Gegenstand haben, vor dem EuGH anhängig sind, ist aus grundrechtlichen Erwägungen, aber auch angesichts des durch die frühzeitige Umsetzung verursachten (möglicherweise sodann frustrierten) finanziellen Mehraufwands, nicht nachvollziehbar, dass Österreich ohne rechtliche Verpflichtung bereits jetzt die Speicherung der Internet-Daten teilweise einzuführen beabsichtigt.

b. zu § 102a:

Ausdrücklich begrüßt wird, dass die beabsichtigte Speicherdauer sich an den Mindestvorgaben der Richtlinie orientiert. In grundrechtlicher Hinsicht unverhältnismäßig und der Ratio der RL nicht entsprechend wird hingegen angesehen, dass Daten „für die Ermittlung, Feststellung und Verfolgung von mit beträchtlicher Strafe bedrohten Handlungen", wie in § 17 SPG definiert wird, zu speichern sind. Wie nicht nur dem Werdegang der Richtlinie (vom inoffiziellen belgischen Entwurf eines Rahmenbeschlusses über den Rahmenbeschlussentwurf des Jahres 2004 bis zum Kommissionsentwurf und der darüber geführten Diskussion im Europäischen Parlament), sondern auch den Erwägungsgründen (siehe EG 7, EG 8, EG 9, EG 10) zu entnehmen ist, wird die Notwendigkeit und somit der Zweck der Vorratspeicherung wiederholt mit der Bekämpfung organisierten Kriminalität und des internationalen Terrorismus argumentiert. Delikte wie die Störung der Religionsausübung (§ 189 StGB), Bigamie (§ 192 StGB), Adoptionsvermittlung (§ 194 StGB), Versetzung von Grenzzeichen (§ 230 StGB), Verleumdung (§ 297 StGB), Begünstigung (§ 299 StGB), Geschenkannahme durch einen Beamten (§ 304 StGB), Geschenkannahme durch leitende Angestellte eines öffentlichen Unternehmens (§ 305

StGB), unbefugter Gebrauch von Fahrzeugen (§ 136 StGB), bestimmte Formen der Unterschlagung und der dauernden Sachentziehung (§§ 134 135 StGB), Entziehung von Energie (§ 132 StGB), aber auch bestimmte Fahrlässigkeitsdelikte, also Vergehen, bei denen der (meist Einzel-)Täter es nicht einmal für möglich hielt, einen strafbaren „Erfolg" zu verwirklichen, werden wohl in aller Regel nicht unter die vom Richtliniengeber beabsichtigten Ausnahmetatbestände fallen.

Da zudem auch die Übermittlung einen Eingriff in grundrechtlich geschützte Positionen darstellt, stellt sich auch hier die Frage der Rechtfertigung. Dieser Eingriff wird umso eher gerechtfertig sein, je schwerer das Delikt wiegt, weswegen angefragt wird. Beim Verdacht des Vorliegens der vorgenannten Delikte ist mehr als zweifelhaft, ob ein Eingriff in die grundrechtlich geschützten Positionen Rechtfertigung findet.

Zudem sollte diese über den Speicherungszweck wohl beabsichtigte Zugriffs- bzw. Übermittlungsbeschränkung aus gesetzessystematischer Sicht zusätzlich expressis verbis als solche eingefügt bzw. bezeichnet werden. Andernfalls könnte argumentiert werden, dass der Zugriff auch bei geringerer Strafdrohung oder zu anderen Zwecken zu gestatten sei. Es wird daher vorgeschlagen, den Zugriff – wie vom Richtliniengeber intendiert – auf Fälle der organisierten Kriminalität und des Terrorismus, allenfalls auf Verbrechen iSd § 17 StGB zu beschränken.

Wien, am 21. Mai 2007

Für das Ludwig Boltzmann Institut für Menschenrechte:

Ao. Univ.Prof. Dr. *Hannes Tretter* und Mag. *Christian Schmaus*