



Ludwig Boltzmann Institut
Menschenrechte

An das
Bundesministerium für Verkehr, Innovation und Technologie (BMVIT)
Sektion III, Abteilung PT 2
Ghegastraße 1
A-1030 Wien
(jd@bmvit.gv.at)

Wien, am 15. Jänner 2010

**Stellungnahme des *Ludwig Boltzmann Instituts für Menschenrechte (BIM)*
zum Entwurf BMVIT-630.333/0001-III/PT2/2009
Novelle des TKG 2003 zur Umsetzung der
Richtlinie über die Vorratsdatenspeicherung 2006/24/EG**

Zum Ministerialentwurf 117/ME (XXIV. GP) Änderung des TKG 2003, nimmt das Ludwig Boltzmann Institut für Menschenrechte (BIM) mit dem Ersuchen um Kenntnisnahme und Berücksichtigung wie folgt Stellung:

1) Allgemeines

Der nun zur Begutachtung vorliegende Gesetzesvorschlag wurde bekanntlich durch das BIM mit einer Gruppe von unabhängigen ExpertInnenen ausgearbeitet und vom BMVIT nach sorgfältigem Studium ohne Änderungen in Begutachtung geschickt. Nicht in die Ministerialvorlage aufgenommen wurden das „Vorblatt“ des BIM-Entwurfes.¹ Dieser nicht in die offizielle Begutachtung versandte Teil des Entwurfes enthält eine Beschreibung der Entstehungsgeschichte der Richtlinie 2006/24/EG, eine Analyse der Vereinbarkeit dieser Richtlinie mit der Europäischen Menschenrechtskonvention (EMRK) in der Auslegung durch den Europäischen Gerichtshof für Menschenrechte (EGMR) sowie eine Analyse des Anpassungsbedarfs, der sich durch diese TKG-Novelle für die Strafprozessordnung (StPO), das Sicherheitspolizeigesetz (SPG) und das Datenschutzgesetz (DSG 2000) ergibt. Diese Ausführungen finden sich nun nachfolgend unter Punkt 2 und 3 dieser Stel-

¹ Der vollständige Vorschlag des BIM ist im Internet abrufbar unter:
<http://bim.lbg.ac.at/de/informationsgesellschaft/bimentwurf-zur-vorratsdatenspeicherung-begutachtung>.

lungnahme, damit sie auf diese Weise auch im parlamentarischen Gesetzgebungsprozess dokumentiert sind und berücksichtigt werden können.

Zum Begriff „schwere Straftat“ vorweg einige Anmerkungen (nähere Ausführungen nachfolgend in Punkt 3). Die Definition, was unter einer „schweren Straftat“ zu verstehen ist, hat aus gesetzessystematischen Gründen im Strafrecht zu erfolgen. Dennoch führt der vorliegende Entwurf diesen Begriff, ohne ihn aus dargelegtem Grund näher definieren zu können, ganz bewusst ins TKG ein. Dies ist vor dem Hintergrund zu sehen, dass die Reichweite des dem BIM erteilten Auftrags durch und auf die Zuständigkeit des beauftragenden Ministeriums beschränkt war. Die Ausarbeitung konkreter legislatischer Änderungsvorschläge für den Bereich der StPO und des SPG war mangels Zuständigkeit des BMVIT nicht auftragsgegenständlich. Dennoch behielt sich das BIM die Möglichkeit vor, im Zuge der Ausarbeitung des Entwurfes auch zu prüfen, ob und inwieweit Anpassungen in den Bereichen der StPO sowie des SPG notwendig sind. Die diesbezüglichen Erwägungen finden sich in den weiter unten in die Stellungnahme aufgenommenen Ausführungen.

Zudem hat das BIM im Zuge der Ausarbeitung dieses Vorschlages mehrere intensive und konstruktive Gespräche mit hochrangigen und für die entsprechende Materie zuständigen BeamtInnen aus dem BMJ und BM.I geführt, wie dies im Übrigen auch mit VertreterInnen der betroffenen Branche, der Interessensvertretungen und der Zivilgesellschaft der Fall war. So konnten schon im Vorfeld einige Missverständnisse, aber auch Vorschläge der Praxis abgeklärt werden. Die zu einigen Punkten des Entwurfes harte Kritik bzw. Ablehnung durch BM.I und BMJ, wie in den bereits veröffentlichten Stellungnahmen formuliert, ist aus Sicht des BIM weder überraschend noch neu. Vielmehr handelt es sich gerade um jene Punkte, die mehrfach diskutiert und in der vorgeschlagenen TKG-Novelle letztlich bewusst sehr restriktiv formuliert wurden, weil in den Besprechungen zwischen BMJ, BM.I und BIM klargestellt wurde, dass über konkrete – und aus grundrechtlicher Sicht notwendige – Änderungen des SPG oder der StPO nicht verhandelt wird.

Vor diesem Hintergrund ist insbesondere der vorgeschlagene § 99 TKG und die Kritik zu dieser Bestimmung zu verstehen. Dabei geht es – von dessen praktischer Auswirkung her – primär um IP-Adressen und die bisherige langjährige Praxis, dass die Information, welchem Teilnehmer eine IP-Adresse zu einem bestimmten Zeitpunkt in der Vergangenheit zugewiesen war, von den meisten Betreibern bereits bis zu 6 Monaten gespeichert und auch beauskunftet wurde. Aufgrund der Entscheidung des 11. Senates des OGH (in Strafsachen), GZ 11 Os 57/05z, vom 26.07.2005 wurde diese Information als reine Auskunft über Stammdaten behandelt, war also nicht an die Voraussetzungen der §§ 135 ff StPO gebunden (keine Anordnung des Staatsanwalts, keine richterliche Bewilligung, keine Informationspflichten, keine Beschränkung auf Straftaten mit einer bestimmten Mindeststrafdrohung). Damit korrespondiert die seit 1.1.2008 neugefasste Bestimmung des § 53 Abs 3a SPG, der solche Auskünfte der Betreiber an die Sicherheitsbehörden vorsieht. Es geht also um die Frage, ob die Anonymität im Internet für strafrechtliche Zwecke ausnahmslos aufgehoben sein soll.

Spätestens seit der Entscheidung des 4. Senats des OGH (in Zivilsachen), GZ 4 Ob 41/09x vom 14.7.2009 ist klargestellt, dass die Betreiber diese Daten zu IP-Adressen bisher nicht hätten aufbewahren dürfen, sondern diese Daten zu löschen gewesen wären, sobald sie für den technischen Betrieb nicht mehr notwendig sind, also im Normalfall nach wenigen Tagen. Das bedeutet im Lichte des Entwurfs (vor allem weil im vorgeschlagenen § 92 Abs 3 Z 16 TKG erstmals eine rechtliche Definition des Begriffs „öffentliche IP-Adresse“ erfolgt), dass diese Daten zu Vorratsdaten werden und damit dem deutlich strengeren Auskunftssystem unterliegen. Der eben skizzierte formlose Zugriff auf IP-Adressen wäre somit jedenfalls nicht mehr möglich, was primär den Sturm der Entrüstung des BM.I (und ein wenig abgeschwächter, aber doch auch des BMJ) gegenüber dem BIM-Entwurf verursacht. Insofern stellt der Entwurf für die Sicherheits- und Strafverfolgungsbehörden in Wahrnehmung ihrer Aufgaben zwar keine rechtliche, aber doch eine praktische Verschlechterung im Vergleich zum Status Quo dar, weil mit ihm eine grundrechtskonforme Ausgestaltung der Rechtslage erfolgt und Rechtsschutzlücken geschlossen werden, die in den bisher eher löchrigen datenschutzrechtlichen Bestimmungen des TKG bestanden.

Ein wesentliches Anliegen dieses Entwurfs ist der Schutz vor Missbrauch der Daten. Damit ist die Frage verbunden, was unter Missbrauch zu verstehen ist. Jedenfalls sind davon die Fälle bewussten rechtswidrigen Handelns in schädigender Absicht umfasst. Missbrauch liegt im datenschutzrechtlichen Sinn aber schon vor, wenn Daten und Informationen für Zwecke verwendet werden, für die sie nicht erhoben und auch nicht umgewidmet wurden; dies ist natürlich auch davon abhängig, wie abstrakt die Zwecke definiert sind. Dem Problem bzw. der Gefahr des Datenmissbrauchs kann man aber letztlich durch geeignete Maßnahmen im Rechtsschutzbereich mit unabhängiger Kontrolle und vor allem der Information Betroffener begegnen. Zur Gänze wird sich ein Datenmissbrauch freilich – solange Daten vorhanden sind – niemals verhindern lassen. Selbst wenn noch entsprechende grund- bzw. datenschutzrechtliche Absicherungen im SPG erfolgen und der für die Auskunft über Daten einer Nachrichtenübermittlung bestehende Rechtsschutz der StPO auch auf IP-Adressen erstreckt wird, wäre die Rechtslage im Falle eines Missbrauchs zwar grundrechtlich nicht perfekt, aber vertretbar.

Grundrechtlich irreparabel und daher nicht mit Artikel 8 EMRK bzw. Artikel 8 der EU-Grundrechtecharta vereinbar ist aber die grundsätzliche Gefahr, die aus der systemimmanenten unzuverlässigen Aussagekraft riesiger Datenmengen resultiert, die durch die Vorratsspeicherung von Telekommunikations- und Internetzugangsdaten existieren würde und in einigen europäischen Ländern schon existiert. Die goldene Regel – unter Technikern – zur Optimierung von Datensicherheit ist das Prinzip der Datensparsamkeit. Das Risiko steigt exponentiell zur Menge der gesammelten Informationen. Auch der Schaden, der an der Informationsfreiheit durch die permanente Aufzeichnung des Kommunikationsverhaltens der gesamten europäischen Gesellschaft entsteht, lässt sich mit gleichwohl notwendigen „Safeguards“ nicht beheben. Es ist eine Abkehr vom Grundsatz der Vertrau-

lichkeit der Kommunikation aufgrund eines generellen Misstrauens gegenüber allen Menschen. Die rechtswissenschaftlich fundierten Ausführungen zu dieser These sind nachfolgend Punkt 2) dieser Stellungnahme zu entnehmen.

Was die Umsetzung des in Begutachtung geschickten Entwurfs des BIM anbelangt, so sind seit dessen Erarbeitung bzw. Fertigstellung Entwicklungen auf europäischer Ebene zu berücksichtigen, die in die weiteren Verhandlungen zwischen den betroffenen Ministerien und im Nationalrat einfließen sollten:

Mit dem Inkrafttreten des Vertrags von Lissabon am 1.1.2010 ist auch die EU-Grundrechtecharta unmittelbar anzuwendender Bestandteil des EU-Primärrechts geworden, die in Artikel 8 das Grundrecht auf Schutz personenbezogener Daten, das nach Artikel 8 EMRK zum Recht auf Achtung des Privatlebens zählt, eigenständig garantiert und damit aufwertet.

Zugleich fordert das „Stockholmer Programm“ des Europäischen Rats vom 11.12.2009, das ein sicheres Europa und den Schutz der Bürger und Bürgerinnen propagiert, bei der Umsetzung sicherheitspolitischer Ziele die strikte Einhaltung und weitere Entwicklung der datenschutzrechtlichen Standards der EU. Dies hat die neue Kommissarin für Justiz, Grundrechte und Bürgerschaft, *Viviane Reding*, zum Anlass genommen, im Rahmen ihrer Anhörung vor dem Europäischen Parlament die Forderung aufzustellen, dass dem Recht auf Datenschutz im digitalen Zeitalter Priorität eingeräumt werden muss, selbst gegenüber Antiterrormaßnahmen; dies erfordere auch eine Überprüfung der Speicherung von Daten auf Vorrat anhand des Grundsatzes der Verhältnismäßigkeit.²

Aufgrund erheblicher Probleme, die eine Reihe von EU-Mitgliedstaaten mit der Umsetzung der Richtlinie haben sei deshalb bereits ein Vertragsverletzungsverfahren vor dem EuGH eingeleitet worden), einer Beschwerde von 35.000 Personen vor dem deutschen Bundesverfassungsgericht, mit dem die Umsetzung der Richtlinie in Deutschland angefochten wurde, sowie eines jüngsten Urteils des rumänischen Verfassungsgerichts, mit dem das rumänische Umsetzungsgesetz wegen Verstoßes gegen das grundrechtlich geschützte Kommunikationsgeheimnis für verfassungswidrig erklärt wurde, hält der österreichische Datenschutzrat die Richtlinie für grundrechtswidrig und hofft auf ein Umdenken auf europäischer Ebene.³

Angesichts dieser Entwicklungen schlägt das BIM vor, die Richtlinie nicht genau in der vorliegenden Minimalvariante des Entwurfs umzusetzen, sondern eine modifizierte Vorgangsweise zu wählen, die auf Zeit setzt und die flächendeckende, verdachtsunabhängige Vorratsspeicherung personenbezogener Daten vermeidet, da mit dieser ein unverhält-

² <http://futurezone.orf.at/stories/1636295/>

³ <http://futurezone.orf.at/stories/1636493/>; vgl. die Stellungnahme des Datenschutzrates unter <http://www.bka.gv.at/DocView.axd?CobId=37819>.

nismäßiger Eingriff in das Recht auf Datenschutz und Privatleben aller verbunden ist (siehe die Ausführungen in Punkt 2 dieser Stellungnahme).

Ausgangspunkt der Überlegungen des BIM ist die Entscheidung des rumänischen Verfassungsgerichts vom 8.10.2009 über die innerstaatliche Umsetzung der Richtlinie.⁴ Das Gericht begründet die Aufhebung des Umsetzungsgesetzes vor allem damit, dass nur eine Einschränkung der Speicherpflicht auf konkrete Anlassfälle mit Artikel 8 EMRK in der Rechtsprechung des EGMR vereinbar sei, weswegen nur unter dieser Voraussetzung eine Umsetzung der Richtlinie zulässig sei. Der Wortlaut der Richtlinie lässt auch nach Ansicht des BIM eine solche grundrechtskonforme Auslegung (wie dies in Artikel 4 der Richtlinie sogar vorgesehen ist) durchaus zu, selbst wenn damit der Intention der Richtlinie nicht Rechnung getragen wird. Auch die Speicheranordnung im Einzelfall bleibt eine Vorratsspeicherung. Das BIM empfiehlt der Republik Österreich daher, die Richtlinie auf eben skizzierte Weise umzusetzen, bewusst keine permanente vorrätige Aufzeichnung der Kommunikationsverbindungen aller Menschen zu normieren und im derzeit anhängigen oder in einem möglichen weiteren Vertragsverletzungsverfahren vor dem EuGH diese grundrechtskonforme Auslegung des Sekundärrechts zu argumentieren. Eine Suche nach verbündeten europäischen Mitgliedsstaaten für diese Vorgangsweise wäre mittlerweile wohl nicht vergeblich. Außerdem könnte, wie schon erwähnt, zumindest vorläufig – bis eine endgültige Klärung der Frage der Grundrechtskonformität auf europäischer Ebene erfolgt (allenfalls auch durch den EuGH oder EGMR) – die antizipierte Speicherung personenbezogener Daten aller in Österreich lebender Menschen, die die betreffenden Telekommunikationsdienste nutzen, vermieden werden.

Die vorgeschlagene Modifikation des in Begutachtung befindlichen Entwurfs der TKG-Novelle könnte in Form einer „Quickfreeze-Variante“ durch eine Umgestaltung des § 102a erfolgen:

Dabei wird zwar eine Speicherpflicht vorgeschrieben, die aber erst einsetzt, wenn ein Gericht dies im Einzelfall aufgrund eines konkreten Verdachts anordnet. Davon sollten allerdings die – bisher nicht verfügbaren – E-Mail-Verbindungsdaten (§ 102a Abs 4 TKG) ausgenommen werden, weil diese systembedingt so unzuverlässig sind, dass sie mehr Schaden als Nutzen für die Strafverfolgung verursachen. Gleichzeitig sollte eindeutig definieren werden, welche (dieser Daten) bei Betreibern wie lange für welche Zwecke gespeichert werden dürfen. Der diesbezügliche Ermessensspielraum ist derzeit zu weit und unbestimmt, es braucht vielmehr einheitliche, klare, kontrollierbare und durchsetzbare Regeln. Verfassungspolitisch ist außerdem die Debatte darüber überfällig, ob Verbindungsdaten schutzwürdig genug sind, um unter den Schirm des Fernmeldegeheimnisses zu fallen. Dieser spannt im Artikel 10a Staatsgrundgesetz (StGG) vor allem den Richter-

⁴ <http://futurezone.orf.at/stories/1629089/>

Eine englische Übersetzung findet sich in:

<http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html>

Das BIM verfügt auch über eine inoffizielle deutsche Übersetzung der Entscheidung des Verfassungsgerichts.

vorbehalt im Sinne einer ausschließlichen Justizzuständigkeit über seine Anwendungsbereiche. Da dies in der Praxis unbequeme Umwege und Rückfragen sowie eine Kompetenzaufteilung zwischen Sicherheitsbehörden und der Justiz bedeutet, die den Arbeitsalltag der Polizei erschweren, wird seitens des BM.I lieber auf den – nach Ansicht des BIM – unzureichenden, weil iSd Artikel 13 EMRK nicht ausreichend wirksamen kommissarischen Rechtsschutz des Rechtsschutzbeauftragten im BM.I verwiesen.

§ 102a TKG könnte in einer modifizierten grundrechtskonformen „Quickfreeze-Variante“ im Kern so lauten (Änderung fett hervorgehoben):

*„§ 102a. (1) TKG Über die Berechtigung zur Speicherung oder Verarbeitung gemäß den §§ 96, 97, 99, 101 und 102 hinaus haben Anbieter von öffentlichen Kommunikationsdiensten nach Maßgabe der Abs. 2 bis 3 Daten ab dem Zeitpunkt der Erzeugung oder Verarbeitung bis sechs Monate nach Beendigung der Kommunikation zu speichern, **wenn dies im Einzelfall durch ein Gericht angeordnet wird**. Die Speicherung erfolgt ausschließlich zum Zweck der Ermittlung, Feststellung und Verfolgung schwerer Straftaten.“*

2) Die Richtlinie 2006/24/EG und der Schutz der Privatsphäre

a) Entstehungsgeschichte der Richtlinie 2006/24/EG

Vor dem Jahr 2002 hatten nur wenige europäische Staaten verbindliche Regelungen über die Vorratsspeicherung von Kommunikationsdaten auf nationaler Ebene erlassen. Erst in der zweiten Hälfte des Jahres 2002 – und damit nach den und in Reaktion auf die Ereignisse des 11. September 2001 – wurde erstmals die Einführung einer Vorratsspeicherung von Daten auf europäischer Ebene öffentlich diskutiert. Die britische Bürgerrechtsorganisation „Statewatch“ veröffentlichte einen von belgischer Seite ausgearbeiteten Entwurf eines Rahmenbeschlusses (also eines Vorschlag für eine Gesetzgebung innerhalb „dritten Säule der EU“ gemäß Art. 29-42 EUV) zur europaweiten Einführung der Vorratsdatenspeicherung.

Dieser inoffizielle Entwurf sah eine Pflicht zur Vorratsspeicherung von Daten für mindestens 12 und höchstens 24 Monate vor. Gespeichert werden sollten jene Daten, die erforderlich sind, um die Quelle, das Ziel, den Zeitpunkt und die Teilnehmer einer Kommunikation sowie das Endgerät festzustellen. Der Zugriff auf Daten sollte nur für die Verfolgung ausreichend schwerwiegender Straftaten möglich sein, nicht aber für rein präventive Zwecke. In einem umfangreichen Katalog war vorgegeben, für welche Straftaten der Zugriff möglich sein sollte. Zudem enthielt der Entwurf Regeln für die grenzüberschreitende Zusammenarbeit für Zugriffe auf die gespeicherten Daten zu Strafverfolgungszwecken. Strafverfolgungsbehörden aus jedem Staat der EU sollte der Zugang zu den in den anderen Mitgliedstaaten vorhandenen Vorratsdaten möglich sein.

Nach den Bombenanschlägen vom 11. März 2004 in Madrid beauftragte der Europäische Rat den Ministerrat mit der Prüfung von Maßnahmen für die Erarbeitung von Rechtsvorschriften über die Aufbewahrung von Verkehrsdaten durch Diensteanbieter.⁵ In der Folge erarbeiteten die Regierungen Frankreichs, Irlands, Schwedens und des Vereinigten Königreichs einen gemeinsamen Vorschlag für einen Rahmenbeschluss zur Vorratsspeicherung von Kommunikationsdaten und legten diesen am 29. April 2004 dem Ministerrat vor.⁶ Angesichts zunehmender grenzüberschreitender Kriminalität und als Reaktion auf die in Madrid verübten terroristischen Attentate erachteten sie eine einheitliche europäische Politik der Vorratsdatenspeicherung für erforderlich. Die Initiatoren verstanden die im Entwurf vorgesehenen Maßnahmen als Vorgehen im Bereich der justiziellen Zusammenarbeit in Strafsachen.

Diesem Entwurf zufolge sollten Verkehrs- und Standortdaten einschließlich Teilnehmer- und Nutzerdaten gespeichert werden, die im Rahmen von Telefonie, SMS-Kurzmitteilungen und Internet-Protokollen einschließlich E-Mails, erzeugt werden. Der Vorschlag sah eine Speicherdauer von mindestens 12 und maximal 36 Monaten vor. Er enthielt keine Entschädigungsregelung für entstehende Kosten der Betreiber.

Im Unterschied zum Entwurf von 2002 sah dieser Entwurf die Vorratsdatenspeicherung auch zum Zweck der Vorbeugung von Straftaten und nicht nur zur Untersuchung, Feststellung und Verfolgung von Straftaten vor. Darüber hinaus fehlte eine Beschränkung auf hinreichend schwere Straftaten sowie die Pflicht zur Aufnahme bestimmter Straftaten. Auch enthielt der Entwurf die unpräzise Regelung des Zugriffs durch „zuständige Behörden“, während der Entwurf aus dem Jahr 2002 noch von „Strafverfolgungsbehörden“ sprach.

Am 27. September 2005 verabschiedete das Europäische Parlament eine legislative Entschließung, in der es die Initiative Frankreichs, Irlands, Schwedens und des Vereinigten Königreichs ablehnte und diese Mitgliedstaaten aufforderte, ihre Initiative zurückzuziehen.⁷ Die ablehnende Haltung des Europäischen Parlaments hatte mehrere Gründe. Zum einen äußerte der zuständige Berichterstatter erhebliche Zweifel an der Wahl der Rechtsgrundlage. Nach Auffassung des Rechtsausschusses des Europäischen Parlaments beinhaltete der Vorschlag verschiedene Maßnahmen, die teils der ersten Säule (EG-Vertrag), teils der dritten Säule (EU-Vertrag) zuzuordnen seien. Es seien daher zwei

⁵ Erklärung des Europäischen Rates zum Kampf gegen den Terrorismus vom 25. März 2004, Ratsdokument 7764/04 vom 28. März 2004.

⁶ „Entwurf eines Rahmenentschlusses über die Vorratsspeicherung von Daten, die in Verbindungen mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus“, Ratsdokument 8958/04 vom 28. April 2004.

⁷ Siehe „Bericht über die Initiative der Französischen Republik, Irlands, des Königreichs Schweden und des Vereinigten Königreichs für einen Rahmenbeschluss des Rates über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus (8958/2004 – C6-0198/2004 – 2004/0813(CNS))“, 31.5.2005, A6 – 0174/2005.

Rechtsakte zu erstellen. Zum anderen bestanden Zweifel an der Verhältnismäßigkeit der Maßnahme. Sie stünde nicht in einer angemessenen Zweck-Mittel-Relation, da sie weder geeignet noch erforderlich sei und eine unzumutbare Härte für die Betroffenen darstellen würde. Insbesondere wurde hervorgehoben, dass die Notwendigkeit der Vorratsdatenspeicherung nicht belegt wäre. Zudem wurde eine Verletzung des Art. 8 der Europäischen Menschenrechtskonvention (EMRK) für möglich gehalten.

Im März 2005 hatte sich die Europäische Kommission der Rechtsauffassung angeschlossen, dass die gebotene Rechtsform für eine allfällige Einführung der Vorratsspeicherung jene der Richtlinie und nicht die des Rahmenbeschlusses wäre. Der damalige EU-Kommissar für Justiz, Freiheit und Sicherheit, *Franco Frattini*, forderte den Rat auf, vom Erlass des geplanten Rahmenbeschlusses abzusehen.

Am 21. September 2005, vorangetrieben durch die Terroranschläge vom 7. Juli 2005 in London, legte die Europäische Kommission schließlich einen eigenen Vorschlag einer Richtlinie zur Vorratsdatenspeicherung auf der Grundlage des Art. 95 EGV vor. Die gewählte Rechtsgrundlage räumte dem Europäischen Parlament das Recht zur Mitentscheidung ein. Dieser Richtlinienentwurf wurde noch am selben Tag an das Parlament übermittelt. Die britische Ratspräsidentschaft⁸ brachte dabei ihr Interesse zum Ausdruck, dass eine Regelung noch vor Ende des Jahres 2005 als Kompromiss in erster Lesung verabschiedet werden solle. Daraufhin nahm das Parlament rasch seine Arbeit auf. In einem Bericht des Europäischen Parlaments wurde der Hoffnung Ausdruck verliehen, dass dieses Vorgehen die Ausnahme bleiben möge und nicht zur Regel werde; es wurde von einem „extrem beschleunigten Gesetzgebungsverfahren“ gesprochen. Folge dieses Schnellverfahrens wären etwa – so der Bericht weiter – fehlerhafte Übersetzungen wie auch unzureichende Beratungszeiten gewesen.⁹

Der Entwurf sah, wie bereits der Entwurf des Rahmenbeschlusses aus dem Jahr 2004, die Verhütung von Straftaten neben der Ermittlung, Feststellung und Verfolgung von Straftaten als Zweck der Vorratsspeicherung vor. Auch die zu speichernden Datenkategorien entsprachen weitestgehend jenen des damaligen Entwurfs, wobei im Richtlinienentwurf eine genauere Umschreibung erfolgte. Ähnlich wie bereits der Entwurf von 2004 sprach der Richtlinienentwurf nur von den „zuständigen Behörden“, die Zugang zu den auf Vorrat gespeicherten Daten haben sollten. Eine Zugriffsmöglichkeit durch Geheimdienste als von den Mitgliedstaaten zu bestimmende zuständige Behörden war somit nicht ausgeschlossen. Im Unterschied zum Entwurf des Rahmenbeschlusses sah der Richtlinienentwurf eine grundsätzliche Speicherfrist von einem Jahr vor, mit Ausnahme von auf das Internet bezogenen Daten, für die eine Speicherdauer von sechs Monaten vorgesehen war. Auch

⁸ 1. Juli 2005 bis 31. Dezember 2005.

⁹ Siehe „Bericht des Europäischen Parlaments über den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rats über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (KOM(2005)0438 – C6 0293/2005 – 2005/0182(COD))“, 28.11.2005, A6-0365/2005, S. 34.

enthielt er eine Erstattungsregelung hinsichtlich zusätzlicher Kosten, welche den Betreibern/Anbietern durch die Vorratsspeicherung entstehen würden.

Der federführende Ausschuss des Parlaments, der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE – Ausschuss), hatte 250 Änderungsanträge zu berücksichtigen. Schließlich verständigte man sich mit den mit beratenden Ausschüssen¹⁰ auf 87 Änderungsanträge, die dem Plenum des Europäischen Parlaments vorgelegt wurden. Fast alle Anträge hatten eine Entschärfung des Kommissionsentwurfs zum Gegenstand.

Abermals wurde Kritik an dem Umstand geübt, dass die Notwendigkeit der Maßnahme nicht hinreichend belegt wäre. So kritisierte der ITRE – Ausschuss: „Ähnlich wie beim diskutierten Rahmenbeschluss führt auch die Kommission nur den sehr pauschalen Nachweis, dass es durch die vorgeschlagenen Maßnahmen tatsächlich zu einer Verbesserung der Verbrechens- und Terrorbekämpfung kommt. Dieser Nachweis ist jedoch Grundvoraussetzung, um die erheblichen Auswirkungen und Belastungen für Bürger und Unternehmen zu rechtfertigen.“¹¹ Es folge nämlich aus Art. 6 Abs. 1 b der Datenschutzrichtlinie 95/46/EG, dass personenbezogene Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen. Dies gebiete bereits der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit, denn verhältnismäßig könne eine Datenverarbeitung nur im Hinblick auf einen legitimen Zweck sein.

Wenige Tage vor der Beschlussfassung verhandelte der Ministerrat inoffiziell mit maßgeblichen EU-Parlamentariern der großen Fraktionen, jedoch ohne Beisein des zuständigen parlamentarischen Berichterstatters *Alexander Alvaro*, den Entwurf. Diese einigten sich im Rahmen einer Absprache mit dem britischen Innenminister *Charles Clarke* informell auf eine Position. Das Ergebnis dieser Verhandlungen wurde schließlich dem Parlament als Kompromissvorschlag zur Abstimmung vorgelegt.

Der zuständige Berichterstatter *Alvaro* äußerte an diesem Vorgehen massive Kritik, erinnerte an den Umstand, dass der Ausschussbericht und somit auch die Änderungsanträge mit deutlicher Mehrheit und fraktionsübergreifend (also auch mit Zustimmung der großen Fraktionen) beschlossen wurden und wies darauf hin, dass diese informelle Einigung die Arbeit des Ausschusses ignoriere.

Am 14. Dezember stimmte das Europäische Parlament mit 378 zu 197 Stimmen für den Kompromissvorschlag. Der Ministerrat stimmte seinerseits am 21. Februar 2006 zu. Schließlich wurde am 15. März 2006 die Richtlinie 2006/24/EG über die Vorratsspeiche-

¹⁰ Mitberatern haben der Ausschuss für Industrie, Forschung und Energie (ITRE – Ausschuss) sowie der Ausschuss für Binnenmarkt und Verbraucherschutz (IMCO – Ausschuss).

¹¹ Siehe „Bericht über den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (KOM(2005)0438 – C6 0293/2005 – 2005/0182(COD))“, 28.11.2005, A6-0365/2005, S. 41.

rung von Daten,¹² die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG vom Europäischen Parlament und vom Rat der Europäischen Union erlassen.

In den Erwägungsgründen der Richtlinie wird zur Begründung ihrer Erlassung im Rahmen der ersten Säule unter anderem ausgeführt, dass die rechtlichen und technischen Unterschiede zwischen den nationalen Vorschriften zur Vorratsdatenspeicherung zum Zwecke der Ermittlung, Feststellung und Verfolgung von Straftaten den Binnenmarkt für elektronische Kommunikation beeinträchtigen, da Diensteanbieter mit unterschiedlichen Anforderungen in Bezug auf die zu speichernden Arten von Verkehrs- und Standortdaten, die für die Vorratsdatenspeicherung geltenden Bedingungen und die Dauer der Vorratsdatenspeicherung konfrontiert sind.¹³ Demnach verfolgt die Richtlinie als – letztlich wettbewerbsrechtliches – Ziel die Harmonisierung der Pflichten für Diensteanbieter bzw. Netzbetreiber in Bezug auf die Vorratsdatenspeicherung, damit diese Daten für die genannten Zwecke auch tatsächlich zur Verfügung stehen, was im Sinne des in Art. 5 EGV normierten Subsidiaritätsprinzip besser auf Gemeinschaftsebene zu erreichen ist.¹⁴ Mit Urteil vom 10. Februar 2009 bestätigte der EuGH in einem von Irland angestrebten Nichtigkeitsverfahren gemäß Art. 230 EGV die für die Richtlinie gewählte Rechtsgrundlage des Art 95 EGV, weil „die Richtlinie 2006/24 in überwiegendem Maß das Funktionieren des Binnenmarkts betrifft“, und lehnte damit die Rechtsmeinung ab, wonach die in der Richtlinie geregelte Materie in den Anwendungsbereich des Titels VI EUV fiele und statt einer Richtlinie ein Rahmenbeschluss zu erlassen gewesen wäre.¹⁵

b) Zur grundrechtlichen Bedenklichkeit der Richtlinie 200/24/EG

Ungeachtet der datenschutzrechtlichen Bestimmungen der Richtlinie – wie insbesondere über Sicherung des Datenzugangs gemäß den Bestimmungen des Art 8 EMRK (Art 4), Datenschutz und Datensicherheit (Art 7), unabhängige Kontrollstellen (Art 9) sowie Rechtsbehelfe, Haftung und Sanktionen (Art 13) – stellt sich angesichts neuester Entwicklungen und Studien die Frage, ob die Richtlinie *per se* mit den grundrechtlichen Anforderungen des Rechts auf Achtung des Privatlebens gemäß Art. 8 der Europäischen Menschenrechtskonvention (EMRK),¹⁶ aus dem der Europäischen Gerichtshof für Menschen-

¹² Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

¹³ Erwägungsgrund (6) der Richtlinie.

¹⁴ Erwägungsgrund (21) der Richtlinie.

¹⁵ EuGH Urteil vom 10.2.2009, Rs. C-301/06, Irland (unterstützt von der Slowakischen Republik) gegen Europäisches Parlament und Rat der Europäischen Union.

¹⁶ Die in der Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) garantierten Rechte stellen gemäß Art. 6 EUV allgemeine Grundsätze des Gemeinschaftsrechts dar und bilden so einen primärrechtlichen Prüfungsmaßstab für das Sekundärrecht, insbesondere für Verordnungen und Richtlinien.

Art. 8 EMRK („Recht auf Achtung des Privat- und Familienlebens“) lautet:

„(1) Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.

(2) Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das

rechte (EGMR) auch ein Recht auf Datenschutz ableitet, sowie dem Recht auf Achtung des Privatlebens und dem Recht auf Schutz personenbezogener Daten gemäß Art. 7 und 8 der Charta der Grundrechte der EU¹⁷ insbesondere im Hinblick auf den Grundsatz der Verhältnismäßigkeit in Einklang gebracht werden kann. Auf Grundlage der Entstehungsgeschichte¹⁸ und des Verweises in Art. 52 Abs. 3 der Charta auf die EMRK als grundrechtlichem Mindeststandard kann davon ausgegangen werden, dass die Tragweite der Schutzbereiche der Art. 7 und 8 der Charta sich im Wesentlichen mit Art 8 EMRK in der Auslegung durch den EGMR deckt.

Es stellt sich mit anderen Worten die Frage, ob die mit der Richtlinie verfügte Vorratsspeicherung – also die verdachtsunabhängige Speicherung von Kommunikations- und Standortdaten zum Zweck der Ermittlung, Feststellung und Verfolgung schwerer Straftaten – einerseits aus grundrechtlicher Perspektive als geeignetes Mittel zur Erreichung dieses Zwecks angesehen werden kann und andererseits, ob die grundrechtlichen Konsequenzen für den Einzelnen, aber auch die Auswirkungen auf die Gesellschaft insgesamt, in einem angemessenen Verhältnis zu den öffentlichen Interessen stehen, die mit dem genannten Zweck verfolgt werden.

Grundsätzlich sollte das Verhältnis zwischen einem demokratischen Verfassungsstaat und seiner Gesellschaft von Vertrauen geprägt sein. Der Einzelne soll darauf vertrauen können, dass in seine grundrechtlich geschützten Positionen im Zuge von Ermittlungstätigkeiten bzw. Strafverfolgungsmaßnahmen grundsätzlich nur bei Vorliegen entsprechender Verdachtsmomente, also als *ultima ratio*, unter Wahrung der rechtsstaatlichen 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 wohl alle rechtsstaatlichen Gesetzgebungen. Die vorliegende Richtlinie geht von diesem Grundsatz nun ab, indem sie eine verdachtsunabhängige, gleichsam antizipierte „Sicherung von Beweismitteln“ vorschreibt.

Zwar werden schon derzeit vielfältig personenbezogene Daten ermittelt und verarbeitet. Diese Datenanwendungen erfolgen in aller Regel aber entweder zur individuellen Aufklä-

wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.“

¹⁷ Die Charta ist nach dem In Kraft treten des Vertrags von Lissabon für die Organe der EU, für deren Rechtssetzung und für die Mitgliedstaaten in der Umsetzung von EU-Recht verbindliches Primärrecht.

Art. 7 der Charta der Grundrechte der EU („Achtung des Privat- und Familienlebens“) lautet:

„Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.“

Art. 8 der Charta der Grundrechte der EU („Schutz personenbezogener Daten“) lautet:

„(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.“

¹⁸ Siehe dazu Bernsdorff in Jürgen Meyer (Hrsg.), Kommentar zur Charta der Grundrechte der Europäischen Union, 155 ff.

rung und Verfolgung konkret begangener Straftaten, zur Erfüllung eines Vertrages und somit zumindest mittelbar auf Wunsch bzw. mit Zustimmung der datenschutzrechtlich Betroffenen, oder aber mit dem Ziel, der Gesellschaft die unterschiedlichsten Leistungen der öffentlichen Daseinsversorgung zur Verfügung zu stellen. Davon unterscheidet sich die Vorratsdatenspeicherung im Sinne der Richtlinie schon alleine durch ihre Zielsetzung in fundamentaler Weise, da personenbezogene Telekommunikations- und Bewegungsdaten aller Kunden, die Dienste eines Telekommunikationsunternehmens in Anspruch nehmen, präventiv zum Zwecke der Ermittlung, Feststellung und Verfolgung von Straftaten ohne irgendeinen konkreten Tatverdacht gesammelt und verarbeitet werden.

Mit der eingangs beschriebenen, grundrechtliche Eingriffe minimierenden rechtsstaatlichen Tradition bricht die Richtlinie. Während verarbeitete Verkehrs- und Standortdaten derzeit noch teilweise sofort, grundsätzlich aber jedenfalls dann gelöscht werden müssen, wenn und soweit sie etwa für die Bereitstellung von Telekommunikationsdiensten und in weiterer Folge für die Abrechnung nicht mehr erforderlich sind, wird diese im Sinne eines effektiven und grundrechtskonformen Datenschutzes normierte Lösungsverpflichtung nun in eine verdachtsunabhängige, flächendeckende Speicherungspflicht verkehrt, um „schwere Straftaten“, insbesondere Terrorakte und organisierte Kriminalität, bekämpfen zu können. Dies stellt im Ergebnis einen Paradigmenwechsel dar, der aus grundrechtlicher Sicht einer entsprechenden Rechtfertigung bedarf.

Es ist also der Frage nachzugehen, ob der Regelungsgehalt der Richtlinie durch die Eingriffsvorbehalte des Art. 8 EMRK gedeckt ist. Eingriffe in diese Rechte sind nach der Rechtsprechung des EGMR und des Verfassungsgerichtshofes (VfGH) nur dann zulässig, wenn diese zur Erreichung einer der in Art 8 Abs 2 EMRK genannten Ziele in einer demokratischen Gesellschaft notwendig sind. Zweifellos fällt die „Ermittlung, Feststellung und Verfolgung von schweren Straftaten“, wie es Art. 1 Abs. 1 der Richtlinie als Zweck der Vorratsdatenspeicherung bestimmt, unter die in Art. 8 Abs. 2 genannten zulässigen Ziele, insbesondere – aus generalpräventiver Sicht – zur „Verhinderung von strafbaren Handlungen“.¹⁹

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 grundrechtlich geschützte Positionen eingreift: Im Vergleich zum Inhalt aufgezeichneter Gespräche können die gewonnen Verkehrs- und Standortdaten elektronisch unterstützt ungleich leichter, in kürzerer Zeit und größerem Umfang ausgewertet werden. Soziale Netzwerke können bis in Details ebenso nachvollzogen werden, wie – je nach Kommunikationsverhalten – mehr oder weniger genaue Bewegungsprofile jedes Men-

¹⁹ Bei strenger Lesart dieses Eingriffsziels könnte die Ermittlung, Feststellung und Verfolgung von schweren Straftaten nicht darunter fallen, da in diesem Fall eine strafbare Handlung ja schon begangen wurde, eine systematische Interpretation aller Eingriffstatbestände begründet jedoch die Zulässigkeit der Maßnahme.

schen erstellt werden können. Schließlich können Verkehrsdaten auch Rückschlüsse über sensible Inhalte einer Kommunikation ermöglichen.²⁰

Weder im Vorfeld noch im Zuge der Beschlussfassung der Richtlinie wurde allerdings – wie bereits ausgeführt – ein aussagekräftiger Nachweis der Notwendigkeit bzw. des Mehrwerts der Vorratsdatenspeicherung zum Zweck der Ermittlung, Feststellung und Verfolgung von schweren Straftaten geführt.²¹ Dafür 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 verstrich.

Bei näherer Analyse der Richtlinie im Zuge der Vorarbeiten zu ihrer innerstaatlichen Umsetzung in Österreich zeigte sich, dass dem klaren Eingriff in die Grundrechte der Betroffenen ein nur ausgesprochen bescheidener Mehrwert für die Strafverfolgung gegenüber steht, wie sich nicht zuletzt anhand neuerer Studien nachweisen lässt.²² So ist es etwa für den Bereich der Festnetz- aber auch Mobiltelefonie ein Leichtes, durch Verwendung von öffentlichen Telefonzellen oder Wertkarten- bzw. im (nicht EU-)Ausland angemeldeter Handys der unmittelbar auf konkrete Personen rückführbaren Datenaufzeichnung zu entgehen. Die Aufzeichnung von E-Mail-Daten im Rahmen der Vorratsspeicherung kann etwa durch Verwendung außereuropäischer E-Mail-Provider leicht vermieden werden. Sollte zum Beispiel ein Angehöriger einer Terrororganisation oder ein Mitglied einer anderen kriminellen Vereinigung der Vorratspeicherung seiner Daten (bzw. genauer: der Möglichkeit der Rückführung der Daten auf seine Person) entgehen wollen, so ist dies ohne jedes technische Spezialwissen mit einfachsten Mitteln möglich. Stehen diese und ähnliche Möglichkeiten schon jedem „Normalverbraucher“ zur Verfügung, verfügen – und davon kann wohl mit gutem Grund ausgegangen werden – terroristische oder andere kriminelle Vereinigungen, deren Bekämpfung die Vorratsspeicherung ja in erster Linie bezweckt, über ungleich bessere technische Möglichkeiten und Kenntnisse der Umgehung der Speicherung ihrer Daten. Letztendlich werden somit fast ausschließlich Daten jener Personen erfasst, die entweder keine Kenntnis vom Umstand der Vorratsdatenspeicherung haben oder aber kein Interesse an den Tag legen, der Datenaufzeichnung zu entgehen, also die Daten ganz normaler Bürger und Bürgerinnen oder anders gesagt, sogenannter „Durchschnittsverbraucher und -verbraucherinnen“.

Nach der Rechtsprechung des EGMR stellen die Ermittlung und Aufbewahrung von Informationen über das Privatleben einer Person in einer elektronischen Datenbank sowie die Verwendung personenbezogener Daten durch eine öffentliche Behörde einen Eingriff

²⁰ Dazu ausführlich Nathan Eagle, Alex Pentland, David Lazer, Inferring Social Network Structure using Mobile Phone Data, Proceedings of the National Academy of Sciences 2007; vgl. die Erläuterungen zum Besonderen Teil zu § 94 Abs. 4.

²¹ Dazu *Westphal*, Die Richtlinie zur Vorratsdatenspeicherung von Verkehrsdaten – Brüsseler Stellungnahme zum Verhältnis von Freiheit und Sicherheit in der „Post-911-Informationsgesellschaft“, EuR 2006/5, 706 ff (715 mwN); *Westphal* war zum damaligen Zeitpunkt Referent beim deutschen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI).

²² Siehe dazu etwa Deutsches Bundeskriminalamt (Autorin: *Eva Mahnken*), Mindestspeicherungsfristen für Telekommunikationsdaten, 2005.

in das durch Art 8 EMRK geschützte Recht auf Achtung des Privatlebens dar.²³ Ein solcher Eingriff liegt jedoch nicht erst dann vor, wenn Inhaltsdaten verarbeitet oder aus Stamm- und Verkehrsdaten Rückschlüsse auf Inhaltsdaten gezogen werden können,²⁴ sondern schon bei einer Verarbeitung von Stamm- und Verkehrsdaten selbst. Jede Anwendung personenbezogener Daten schlechthin führt nach Ansicht des EGMR zu einem Eingriff in dieses Recht. Sogar das Sammeln und Speichern personenbezogener Daten ohne deren weitere Verwendung,²⁵ die Aufbewahrung öffentlich zugänglicher personenbezogener Informationen, wenn sie von Behörden systematisch erfasst werden,²⁶ sowie die Speicherung personenbezogener Daten ohne konkreten Verdacht strafbarer Handlungen²⁷ fällt demnach in den Schutzbereich des Art 8 EMRK.

Diese (nach eigenen Worten des EGMR: weite) Interpretation des Schutzbereichs des – das Recht auf Datenschutz einschließenden – Art 8 EMRK folgt unter anderem daraus, dass der EGMR in den Urteilen *Amann* und *Rotaru* zur Begründung auf Art 1 und 2 der Datenschutzkonvention des Europarates Bezug nimmt, die sich auf jede Form automatischer Verarbeitung personenbezogener Daten erstreckt.²⁸ Schon im Urteil *Malone* hielt

²³ Siehe EGMR, 2.8.1984, Urteil *Malone gegen Vereinigtes Königreich* (Telefonüberwachung und Weitergabe von Verkehrsdaten durch die Postverwaltung an die Polizei), Z 62 ff (vor allem 64, 83-89); EGMR, 26.3.1987, Urteil *Leander gegen Schweden* (Speicherung in einem Sicherheitsdatenregister), Z 47-48; EGMR, 16.2.2000, *Amann gegen Schweiz* (Speicherung nach polizeilicher Telefonüberwachung), Z 68-70; EGMR, 4.5.2000, Urteil *Rotaru gegen Rumänien* (Speicherung in einem Geheimdienstregister), Z 43; EGMR, 6.6.2006, Urteil *Segerstedt-Wiberg u.a. gegen Schweden* (Speicherung in einer elektronischen Datenbank der Sicherheitspolizei), Z 70-72; EGMR, 29.6.2006, Unzulässigkeitsentscheidung *Weber und Saravia gegen Deutschland* (strategische Überwachung und Speicherung von Telekommunikationsbeziehungen aufgrund des „G 10“), Beschwerde-Nr. 54.934/00, Z 76-79 (insb. Z 79), deutschsprachige Zusammenfassung und Fundstelle der Entscheidung in: Newsletter des Österreichischen Instituts für Menschenrechte, NL 2006, 177 f (www.menschenrechte.at → online-Archiv), siehe dazu auch das vorangegangene Urteil des EGMR zu „G 10“ vom 6.9.1978 im Fall *Klass u.a. gegen Deutschland* (Telefonüberwachung wegen des Verdachts strafbarer Handlungen); EGMR, 1.8.2008, Urteil *Liberty u.a. gegen Vereinigtes Königreich* (systematische polizeiliche Überwachung der gesamten Telekommunikation), Z 56-57; EGMR 4.12.2008, Urteil *S. und Marper* (Speicherung von Fingerabdrücken und DANN-Proben nach einem Freispruch).

²⁴ Zur Überwachung von Inhaltsdaten siehe weiters EGMR, 24.4.1990, Urteil *Huvig gegen Frankreich*; EGMR, 24.4.1990, Urteil *Kruslin gegen Frankreich*; EGMR, 25.6.1997, Urteil *Halford gegen Vereinigtes Königreich*; EGMR, 25.3.1998, Urteil *Kopp gegen Schweiz*; EGMR, 24.8.1998, Urteil *Lambert gegen Frankreich*; EGMR, 3.4.2007, *Copland gegen Vereinigtes Königreich* (dieses bezieht sich auch auf E-Mail-Kommunikation und die Verwendung des Internet, die vom Schutzbereich des Art. 8 EMRK mit umfasst sind).

²⁵ So der EGMR im Urteil *Copland*, Z 43.

²⁶ EGMR Urteil *Rotaru*, Z 43; Urteil *Segerstedt-Wiberg u.a.*, Z 72; Urteil *Copland*, Z 43.

²⁷ Siehe EGMR Urteil *Segerstedt-Wiberg u.a.*, Z 49, wobei die Angaben der schwedischen Regierung in Richtung verdachtsunabhängiger Speicherung von Vorratsdaten zur Erfüllung präventiver Aufgaben der Sicherheitspolizei gehen. Zur grundrechtlichen Bedenklichkeit von Vorratsdatenspeicherungen siehe auch *European Union Agency for Fundamental Rights (FRA)*, Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, 28 October 2008 (<http://fra.europa.eu> → Products → FRA Opinions).

Siehe dazu auch das laufende Verfahren vor dem deutschen BVerfG zur Umsetzung der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten (www.vorratsdatenspeicherung.de).

²⁸ Urteil *Amann*, Z 65; Urteil *Rotaru*, Z 43. Siehe dazu das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Jänner 1981 (ETS No. 108), ergänzt durch das Zusatzprotokoll vom 8. November 2001 (ETS No. 181).

Dessen Art. 1 („Gegenstand und Zweck“) lautet:

„Zweck dieses Übereinkommens ist es, im Hoheitsgebiet jeder Vertragspartei für jedermann ungeachtet seiner Staatsangehörigkeit oder seines Wohnorts sicherzustellen, daß seine Rechte und Grundfreiheiten, insbesondere sein Recht auf einen Persönlichkeitsbereich, bei der automatischen Verarbeitung personenbezogener Daten geschützt werden („Datenschutz“).“

Und Art. 2 („Begriffsbestimmungen“) lautet:

„In diesem Übereinkommen:

der EGMR fest, dass Art 8 EMRK nicht nur die Überwachung von Inhaltsdaten, sondern auch die Registrierung von Verkehrsdaten schützt.²⁹ „... Die Registrierung unterscheidet sich daher von der Natur der Sache her von der Kommunikationsüberwachung, die, falls nicht gerechtfertigt, zumeist unerwünscht und illegitim ist in einer demokratischen Gesellschaft. Dennoch ist der Gerichtshof nicht der Meinung, dass die Nutzung derart zusammengetragener Fakten niemals zu Problemen im Bereich des Art. 8 EMRK führen könnte. Ein so zusammengestelltes Verzeichnis enthält Informationen – insbesondere die angewählten Nummern – die Bestandteil der Telefongespräche sind. In den Augen des Gerichtshofs führt die Freigabe dieser Informationen an die Polizei ohne Zustimmung des Teilnehmers zu einem Eingriff in ein von Art. 8 EMRK garantiertes Recht.“³⁰ Im neueren Urteil *Copland* bestätigte der EGMR seine Rechtsauffassung aus dem Urteil *Malone* und weitet sie auf E-Mail-Korrespondenz und Nutzung des Internet aus: „Der Gerichtshof erinnert daran, dass die Verwendung von Informationen über den Zeitpunkt und die Länge eines Telefongesprächs und im Besonderen über die gewählten Nummern einen Aspekt des Art 8 EMRK betreffen, da diese Informationen einen ‚integralen Bestandteil der Telefontelekommunikation darstellen‘. ... Daher erachtet der Gerichtshof das Sammeln und Speichern persönlicher Informationen sowohl in Bezug auf die Telefongespräche der Beschwerdeführerin als auch ihre E-Mail- und Internet-Nutzung ohne ihr Wissen als Eingriff in ihr Recht auf Achtung ihres Privatlebens und Korrespondenz im Sinne des Art 8 EMRK.“³¹

Schon in den Urteilen *Klass u.a.* und *Malone* als auch zuletzt in der Unzulässigkeitsentscheidung *Weber und Saravia* sowie im Urteil *Liberty u.a.* führt der EGMR aus, dass selbst das bloße Bestehen von Gesetzen, die ein System der geheimen Überwachung der Kommunikation erlauben, als solche für alle Personen, auf die sie Anwendung finden können, die Gefahr einer Überwachung mit sich bringt. Diese Gefahr greift nach dem EGMR notwendigerweise in die Freiheit der Kommunikation zwischen Benutzern von Telekommunikationseinrichtungen ein und stellt daher ungeachtet tatsächlich gegen sie ergriffener Maßnahmen einen Eingriff in Art 8 EMRK dar.³²

a. bedeutet ‚personenbezogene Daten‘ jede Information über eine bestimmte oder bestimmbare natürliche Person (‚Betroffener‘);

b. bedeutet „automatisierte Datei/Datensammlung“ jede zur automatischen Verarbeitung erfaßte Gesamtheit von Informationen;

c. umfaßt ‚automatische Verarbeitung‘ die folgenden Tätigkeiten, wenn sie ganz oder teilweise mit Hilfe automatisierter Verfahren durchgeführt werden: das Speichern von Daten, das Durchführen logischer und/ oder rechnerischer Operationen mit diesen Daten, das Verändern, Löschen, Wiedergewinnen oder Bekanntgeben von Daten;

d. bedeutet ‚Verantwortlicher für die Datei/Datensammlung‘ die natürliche oder juristische Person, die Behörde, die Einrichtung oder jede andere Stelle, die nach dem innerstaatlichen Recht zuständig ist, darüber zu entscheiden, welchen Zweck die automatisierte Datei/Datensammlung haben soll, welche Arten personenbezogener Daten gespeichert und welche Verarbeitungsverfahren auf sie angewendet werden sollen.“

²⁹ EGMR Urteil *Malone*, Z 56, 64 und 83-89 („Metering“).

³⁰ *Ibid*, Z 84 (deutsche Übersetzung aus EuGRZ 1985, 23).

³¹ EGMR Urteil *Copland*, Z 43 und 44, unter Zitierung des Urteils *Malone*, Z 84 (deutsche Übersetzung vom Autor).

³² EGMR Urteil *Klass u.a.*, Z 41; EGMR Urteil *Malone*, Z 64; EGMR Beschluss *Weber und Saravia*, Z 78, sowie Urteil *Liberty u.a.*, Z 56.

Von der Vorratsdatenspeicherung sind durch die Richtlinie und deren nationale Umsetzungsgesetze alle Menschen im EU-Raum betroffen, in deren Grundrechtssphäre dadurch eingegriffen wird. Zu bedenken ist auch, dass im Fall einer konkreten Datenanwendung durch Strafverfolgungsbehörden aber nicht nur in die Rechtssphäre etwa eines möglichen Straftäters oder dessen Komplizen eingegriffen wird, sondern auch in die Rechtssphäre derjenigen Personen, die mit den Adressaten der Maßnahme über Telekommunikationseinrichtungen nur zufällig in Verbindung standen oder stehen.³³ Dies schafft aber nach der Ansicht des EGMR ein System der Überwachung zum Schutz der Sicherheit des Staates und der Gesellschaft, das die Demokratie bzw. die Rechtsstaatlichkeit, die es schützen soll, aushöhlen bzw. umgehen könnte.³⁴

Aus all dem folgt in systematischer Auslegung der Rechtsprechung des EGMR, dass die Vorratsdatenspeicherung einen Eingriff in das Recht auf Achtung des Privatlebens gemäß Art 8 EMRK und das daraus abgeleitete Recht auf Datenschutz bewirkt. Zur Beantwortung der Frage, ob die verdachtsunabhängige Speicherung von Daten auf Vorrat aber mit Art 8 EMRK in Einklang steht, sind vor allem zwei Urteile des EGMR zu beachten:

Im Urteil *S. und Marper gegen Vereinigtes Königreich* zur Speicherung von Fingerabdrücken und DNA-Proben nach einem Freispruch hat der EGMR die Bedeutung des Datenschutzes für das Privatleben, wie es in Art 8 EMRK gewährleistet ist, noch einmal ausdrücklich betont und auf die Notwendigkeit des Schutzes dieser Daten bei ihrer Anwendung durch das nationale Recht hingewiesen.³⁵ Fingerabdrücke enthalten einmalige Informationen über eine Person, die ihre präzise Identifizierung erlauben. Sie sind nach Auffassung des EGMR daher geeignet, ihr Privatleben zu beeinträchtigen. Die Speicherung solcher Informationen ohne Zustimmung der betroffenen Person könne nicht als neutral oder unbedeutend abgetan werden. Die Speicherung von Fingerabdrücken in den Aufzeichnungen der Behörden im Zusammenhang mit einer identifizierbaren Person kann daher für sich gewichtige Bedenken hinsichtlich ihres Privatlebens aufwerfen. Im vorliegenden Fall wurden die Fingerabdrücke in einem Strafverfahren abgenommen und in einer landesweiten Datenbank gespeichert, um dort für Zwecke der Ausforschung von Straftätern aufbewahrt und regelmäßig verarbeitet zu werden. Wenngleich hinsichtlich der Rechtfertigung zwischen der Speicherung von Zellproben und DNA-Profilen einerseits und Fingerabdrücken andererseits unterschieden werden muss, begründet auch die Speicherung von Fingerabdrücken einen Eingriff in das Recht auf Achtung des Privatlebens.

Zur Rechtfertigung des Eingriffs führt der EGMR aus, dass die Speicherung der Fingerabdrücke und DNA-Informationen dem legitimen Ziel der Aufklärung und damit der Verhütung von Straftaten dient. Ohne Zweifel bedürfe, so der EGMR, der Kampf gegen das Verbrechen der Verwendung moderner wissenschaftlicher Methoden der Ermittlung und Identifizierung. Die Frage sei nicht, ob die Aufbewahrung von Fingerabdrücken, Zellpro-

³³ Vgl. dazu BVerfGE 109, 279 (308).

³⁴ Siehe in diesem Sinn den EGMR im Urteil *Leander*, Z 60; und im Urteil *Klass u.a.*, Z 49.

³⁵ EGMR 4.12.2008, Urteil *S. und Marper*.

ben und DNA-Profilen im Allgemeinen als konventionskonform angesehen werden kann. Die einzige zu prüfende Frage ist, ob die Speicherung der Fingerabdrücke und DNA-Daten bestimmter Straftaten verdächtiger, aber nicht verurteilter Personen nach Art 8 Abs 2 EMRK gerechtfertigt ist. Unter Berücksichtigung des Rechts und der Praxis der Konventionsstaaten führt der EGMR aus, dass die Grundprinzipien des Datenschutzes verlangen, dass die Speicherung von Daten im Hinblick auf den Zweck der Datensammlung verhältnismäßig und die Aufbewahrung zeitlich beschränkt ist. Der EGMR verweist darauf, dass die meisten Staaten sich dazu entschieden haben, der Speicherung und Verwendung solcher Daten Grenzen zu setzen, um einen angemessenen Ausgleich mit dem Interesse am Schutz des Privatlebens zu erreichen. Der starke Konsens zwischen den Konventionsstaaten engt nach Ansicht des EGMR den Ermessensspielraum der Staaten auf diesem Gebiet ein. Der EGMR anerkennt, dass eine Datenbank zur Aufklärung und Verhütung von Straftaten beitragen kann. Dennoch bleibe die Frage offen, ob eine solche Speicherung verhältnismäßig ist und einen gerechten Ausgleich zwischen den widerstreitenden öffentlichen und privaten Interessen trifft. Der EGMR gelangt zum Schluss, dass die umfassende und wahllose Befugnis zur Speicherung von Fingerabdrücken, Zellproben und DNA-Profilen von verdächtigten, aber nicht verurteilten Personen, keinen gerechten Ausgleich zwischen den widerstreitenden öffentlichen und privaten Interessen trifft und der belangte Staat in dieser Hinsicht jeden akzeptablen Ermessensspielraum überschritten hat. Die umstrittene Speicherung begründe daher einen unverhältnismäßigen Eingriff in das Recht auf Achtung des Privatlebens, der nicht als in einer demokratischen Gesellschaft notwendig angesehen werden kann. Daher stellte der EGMR in diesem Fall einstimmig eine Verletzung von Art 8 EMRK fest. Das Urteil ist im vorliegenden Zusammenhang deshalb von besonderem Gewicht, weil selbst die Speicherung personenbezogener Daten von Personen, die einmal im Verdacht standen, eine strafbare Handlung begangen zu haben, vom EGMR als Verletzung des Art 8 EMRK betrachtet wird. Umso mehr wirft die völlig verdachtsunabhängige Speicherung von Vorratsdaten die Frage nach einer Verletzung dieses Konventionsrechts auf.

Aus diesen Überlegungen folgt, dass die Frage, ob die Richtlinie mit Art 8 EMRK in Einklang steht, derzeit noch nicht endgültig beantwortet werden kann. Eine rechtsverbindliche Antwort darauf werden mit großer Wahrscheinlichkeit entweder das deutsche Bundesverfassungsgericht (BVerfG) und/oder der Europäische Gerichtshof (EuGH) und/oder der Europäische Gerichtshof für Menschenrechte (EGMR) geben:

Zum einen ist beim BVerfG derzeit eine Beschwerde von ca. 30.000 Personen anhängig, die sich gegen das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“³⁶ wendet, in der unter anderem auch ein Verstoß der Richtlinie gegen das aus Art. 8 Abs. 2 EMRK abgeleitete Recht auf Datenschutz geltend gemacht wird.³⁷ Der Antrag hatte vorläufig teilweise Erfolg und führte zur Erlassung einer einstweiligen Anord-

³⁶ BGBl I 70/2007 vom 31.12.2007, S. 3198.

³⁷ Siehe die Dokumentation des Verfahrens in www.vorratsdatenspeicherung.de

nung, mit der die Anwendung einiger der angefochtenen gesetzlicher Bestimmungen bis zur Entscheidung über die Verfassungsbeschwerde außer Kraft gesetzt wurden.³⁸ Denkbar ist, dass das BVerfG zur Klärung dieser Frage ein Vorabentscheidungsverfahren vor dem EuGH anstrengt, in der Sache selbst entscheidet und/oder im Fall der Abweisung der Beschwerde die Angelegenheit von den nicht erfolgreichen Beschwerdeführern und Beschwerdeführerinnen dem EGMR vorgelegt wird.

Zum anderen hat die Republik Österreich im ebenfalls derzeit laufenden und von der Europäischen Kommission eingeleiteten Vertragsverletzungsverfahren gemäß Art. 226 Abs. 2 EGV wegen Nichtumsetzung der Richtlinie³⁹ in ihrer Klagebeantwortung gemäß Art. 241 EGV Einwände im Hinblick auf die Vereinbarkeit der Richtlinie mit dem Recht auf Datenschutz gemäß Art. 8 EMRK und Art. 8 der EU-Grundrechtecharta vorgebracht.

Vor diesem Hintergrund ergibt sich, dass in absehbarer Zeit mit einer verbindlichen Entscheidung über die Frage der Grundrechtskonformität der Richtlinie gerechnet werden kann, die bis dahin zum Rechtsbestand der Europäischen Union zählt und von den Mitgliedstaaten umzusetzen ist, soweit dies noch nicht geschehen ist. Die innerstaatliche Umsetzung der Richtlinie hat rasch zu erfolgen, um eine Verurteilung Österreichs durch den EuGH im Vertragsverletzungsverfahren möglichst zu vermeiden.

3) Innerstaatlicher Anpassungsbedarf

a) *Strafprozessordnung (StPO)*

Die vorgeschlagene TKG-Novelle erfordert jedenfalls deshalb eine Anpassung der StPO, weil die neue Bestimmung des § 99 Abs. 5 TKG eine Verarbeitung von Verkehrsdaten für Auskünfte über Daten einer Nachrichtenübermittlung (§ 134 StPO) nur aufgrund einer gesetzlichen Bestimmung erlaubt, die „auf diesen Absatz zu verweisen, die konkreten Datenkategorien aufzuzählen, die berechtigten Behörden zu benennen und den Datenumfang auf das notwendige und verhältnismäßige Ausmaß zu beschränken“ hat. Außerdem darf gemäß der neuen Bestimmung § 102b TKG „eine Auskunft über Vorratsdaten (...) nur nach Maßgabe einer ausdrücklich auf § 102a verweisenden gesetzlichen Bestimmung erteilt werden. Dadurch ist zumindest ein insofern „formeller“ Verweis auf die genannten Bestimmungen des TKG in der StPO perpetuiert, als ansonsten eine Verarbeitung von Verkehrsdaten zu Auskunftszwecken nicht zulässig ist. Darüber hinaus scheint im Hinblick

³⁸ BVerfG, 1 BvR 256/08 vom 11.3.2008 http://www.bverfg.de/entscheidungen/rs20080311_1bvr025608.html, BGBl I 13/2008, S. 659; unter den GZ 1 BvR 263/08 und 1 BvR 586/08 sind weitere Beschwerden beim BVerfG erfasst, die Verfahren werden unter einem geführt. Mit Beschluss vom 1.10.2008, 1 BvR 256/08 verlängerte das BVerfG diese einstweilige Anordnung um weitere sechs Monate, längstens jedoch bis zur Entscheidung in der Hauptsache. Erneuert und erweitert wurde die einstweilige Anordnung durch Beschluss des BVerfG vom 28.10.2008, 1 BvR 256/08: http://www.bverfg.de/entscheidungen/rs20081028_1bvr025608.html, BGBl I 53/2008, S. 2239. Zuletzt wurde mit Beschluss des BVerfG vom 22.04.2009, 1 BvR 256/08, die einstweilige Anordnung wiederholt: http://www.bverfg.de/entscheidungen/rs20090422_1bvr025608.html, BGBl I 27/2009, S. 1139.

³⁹ EuGH Rs. C-189/09, Kommission der Europäischen Gemeinschaften gegen Republik Österreich.

auf die Zulässigkeit der Verwendung von Vorratsdaten eine Anpassung der StPO aus nachfolgenden Erwägungen indiziert:

Die Richtlinie sieht vor, dass bestimmte Kommunikationsdaten zum Zweck der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie jeweils vom nationalen Recht bestimmt werden, gespeichert werden sollen. Die vorgeschlagene Novellierung des TKG zur Umsetzung der Richtlinie verweist zwar auf den Zweck der Vorratsdatenspeicherung und legt fest, dass diese nur zur Ermittlung, Feststellung und Verfolgung von „schweren Straftaten“ erfolgen darf (§ 102a TKG), was aber unter einer „schweren Straftat“ zu verstehen ist, kann aus Gründen der Sachzuständigkeit nicht über das TKG, könnte aber wohl im Rahmen des 5. Abschnitts der StPO geregelt werden (§§ 134 StPO). Um diesbezüglich schon von Gesetzes wegen Rechtssicherheit herzustellen und die Auslegung des Begriffs nicht der Rechtsprechung zu überlassen, ergibt sich ein entsprechender Anpassungsbedarf, der von folgenden Überlegungen geleitet sein könnte:

Auch wenn die Richtlinie die Definition ins nationale Recht verweist, so ergeben sich doch aus der Entstehungsgeschichte Hinweise darauf, woran der europäische Gesetzgeber gedacht hat. Ursprünglich dominierte der Gedanke der Bekämpfung des Terrorismus und schwerer Kriminalität als Zweckbindung der Vorratsdatenspeicherung. Im ursprünglichen Vorschlag der Kommission hieß es sogar im Normtext ausdrücklich „... Verfolgung von schweren Straftaten wie Terrorismus und organisierter Kriminalität“.⁴⁰ Auch in den Erwägungsgründen (7)-(9) der beschlossenen Richtlinie wird der Zusammenhang mit der Bekämpfung von Terrorismus und organisierter Kriminalität nach wie vor mehrfach deutlich. In der Gemeinsamen Erklärung des Rates und der Kommission vom 17. Februar 2006⁴¹ findet sich schließlich die Aussage, dass die Mitgliedstaaten bei der Auslegung der schweren Straftat die Taten im Sinne des Art. 2 Abs. 2 des Rahmenbeschlusses über den Europäischen Haftbefehl⁴² sowie Straftaten unter Einsatz von Telekommunikationseinrichtungen angemessen zu berücksichtigen haben. Zu Taten im Sinne des Art. 2 Abs. 2 des Rahmenbeschlusses zählen nun die folgenden 32 Deliktsgruppen:

1. Beteiligung an einer kriminellen Vereinigung,
2. Terrorismus,
3. Menschenhandel,
4. sexuelle Ausbeutung von Kindern und Kinderpornografie,
5. illegaler Handel mit Drogen und psychotropen Stoffen,
6. illegaler Handel mit Waffen, Munition und Sprengstoffen,
7. Korruption,
8. Betrugsdelikte, einschließlich Betrug zum Nachteil der finanziellen Interessen der Europäischen Gemeinschaften im Sinne des Übereinkommens vom 26. Juli 1995 über den Schutz der finanziellen Interessen der Europäischen Gemeinschaften,

⁴⁰ KOM (2005) 438 endg.

⁴¹ 5777/06 ADD 1 REV 1 COPEN 7 TELECOM 3 CODEC 78.

⁴² Rahmenbeschluss des Rates vom 13.06.2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten, ABI L 190, 1 vom 18.07.2002.

9. Wäsche von Erträgen aus Straftaten,
10. Geldfälschung, einschließlich der Euro-Fälschung,
11. Cyberkriminalität,
12. Umweltkriminalität, einschließlich des illegalen Handels mit bedrohten Tierarten oder mit bedrohten Pflanzen- und Baumarten,
13. Beihilfe zur illegalen Einreise und zum illegalen Aufenthalt,
14. vorsätzliche Tötung, schwere Körperverletzung,
15. illegaler Handel mit Organen und menschlichem Gewebe,
16. Entführung, Freiheitsberaubung und Geiselnahme,
17. Rassismus und Fremdenfeindlichkeit,
18. Diebstahl in organisierter Form oder mit Waffen,
19. illegaler Handel mit Kulturgütern, einschließlich Antiquitäten und Kunstgegenständen,
20. Betrug,
21. Erpressung und Schutzgelderpressung,
22. Nachahmung und Produktpiraterie,
23. Fälschung von amtlichen Dokumenten und Handel damit,
24. Fälschung von Zahlungsmitteln,
25. illegaler Handel mit Hormonen und anderen Wachstumsförderern,
26. illegaler Handel mit nuklearen und radioaktiven Substanzen,
27. Handel mit gestohlenen Kraftfahrzeugen,
28. Vergewaltigung,
29. Brandstiftung,
30. Verbrechen, die in die Zuständigkeit des Internationalen Strafgerichtshofs fallen,
31. Flugzeug- und Schiffsentführung,
32. Sabotage.

Selbst wenn aber ein Tatbestand in eine der genannten Deliktgruppen einzuordnen ist, bedarf es zusätzlich noch einer Höchststrafe von mindestens drei Jahren Freiheitsstrafe. Schon diese Überlegungen auf europäischer Ebene zeigen, dass das neue Ermittlungsinstrument nicht für jede, sondern – gemessen an der österreichischen Rechtsordnung – nur für wegen ihrer Verbindung zu Terrorismus und besonderer Kriminalität schwerer wiegende Delikte eingesetzt werden sollte. Auch wenn die Richtlinie letztlich zur Definition auf das nationale Recht verweist, ist den Vorarbeiten und der Gemeinsamen Erklärung doch eine gewisse der europäischen Gesetzgebung immanente Wertung dahingehend erkennbar, welcher Art die Taten sein müssen, die den Einsatz der Vorratsdatenspeicherung erlauben sollen – nämlich terroristische Straftaten, organisierte Kriminalität, signifikante Formen von Vermögens- und Gewaltdelikten sowie staatsgefährdende Handlungen.

Vor dem Hintergrund des Zwecks der Richtlinie und des mit der Vorratsdatenspeicherung verbundenen Grundrechtseingriffs ist die nationale Umschreibung der schweren Straftat als jede Vorsatz- oder Fahrlässigkeitstat mit einer Strafdrohung von mehr als einem Jahr Freiheitsstrafe iSd § 17 SPG (ergänzt um die gefährliche Drohung und beharrliche Verfol-

gung, wie dies noch im Ministerialentwurf einer TKG-Novelle vorgeschlagen worden war⁴³) jedenfalls problematisch. Es besteht im Übrigen auch keine Notwendigkeit, auf die Definition des SPG zurückzugreifen: Erstens hat der österreichische Strafgesetzgeber selbst für Zwecke der Strafverfolgung in § 17 StGB eine Einteilung in leichtere und schwere Straftaten getroffen: nämlich in Vergehen und Verbrechen. Letztere sind nur Vorsatztaten, die mit mehr als drei Jahren Freiheitsstrafe geahndet werden. Und zweitens berücksichtigt das Kriminalstrafrecht schon seit langem auch bei der Einteilung in Vergehen und Verbrechen Gefahrenabwehraspekte: Grundsätzlich hat jede Strafverfolgung auch die Funktion der Gefahrenabwehr und Prävention. Im Besonderen bezwecken Vorbereitungs- und Organisationsdelikte, gerade auch im Bereich des Terrorismus, die Erfassung und Abwehr von Gefahren im Vorfeld. Zu nennen sind dabei die Delikte der kriminellen Organisation (§ 278a StGB) und terroristischen Vereinigung (§ 278b StGB) sowie der Terrorismusfinanzierung (§ 278d StGB), die allesamt den Verbrechensbegriff erfüllen. Insofern wäre es konsequent und sachgerecht, die Definition des Verbrechens als Umschreibung der schweren Straftat zu verwenden.⁴⁴

Zu bedenken sind bei der Auslegung weiters prozessuale Aspekte, die diese Definition der schweren Straftat als Verbrechen zu stützen vermögen: Der Gesetzgeber öffnet geheime Maßnahmen in unterschiedlicher Breite für Ermittlungen. Schon für die traditionelle Überwachung der Telekommunikation zieht er eine Schwelle, die oberhalb des § 17 SPG liegt. Denn ohne Zustimmung des Betroffenen ist eine Überwachung nur bei Vorsatztaten und nur bei mehr als einem Jahr Freiheitsstrafandrohung zulässig. Betrachtet man die weiteren geheimen Maßnahmen, so fällt auf, dass der Gesetzgeber bei der derzeit wohl eingriffsintensivsten geheimen Maßnahme die Eingriffsschwelle sehr hoch anlegt: Immerhin geht es beim großen Lauschangriff (§ 136 Abs 1 Z 3 StPO) um Organisationsdelikte und Verbrechen mit mehr als zehn Jahren Freiheitsstrafe. Dass die Vorratsdatenspeicherung nicht mit dem großen Lauschangriff gleichgesetzt werden kann, liegt auf der Hand. Immerhin geht es bei der Vorratsdatenspeicherung um „bloße“ äußere Kommunikations- und Standortdaten, wohingegen beim großen Lauschangriff im Überwachungszeitraum sowohl Äußerungen wie auch das Verhalten der überwachten Person umfassend erhoben werden. Daher wäre es nicht sachgerecht, die Verwendung von Vorratsdaten auf die Fälle des großen Lauschangriffs zu beschränken.

Für den Bereich zwischen § 17 SPG und § 17 StGB hat sich der Gesetzgeber erst kürzlich dahingehend geäußert, dass ein schwerwiegendes Verbrechen in der Regel dann vorliegt, wenn es um ein Verbrechen mit einer Strafdrohung von mehr als fünf Jahren Freiheitsstrafe geht oder sonst ein schwerer Schaden oder Nachteil verursacht wurde.⁴⁵ Obgleich es in diesem Zusammenhang um die Berichtspflicht der Kriminalpolizei an die Staatsanwaltschaft geht, lässt sich dennoch auch daraus eine Gewichtung erkennen. Eine solche Bedeutung, dass von Anfang an die Staatsanwaltschaft ins Verfahren involviert

⁴³ BMVIT, ZI. 630.333/0001-III/PT2/2007.

⁴⁴ Ähnlich BKA-VD, Stellungnahme zum Ministerialentwurf einer TKG-Novelle, 10 SN-61/ME XXIII.GP.

⁴⁵ EBRV 25 BlgNR XXII.GP 133.

sein muss, haben nicht alle Straftaten, nicht einmal alle Verbrechen, sondern nur schwere Verbrechen. Bei ihnen bedarf es offensichtlich besonderer Verfahrensführung und besonderer Maßnahmen. Daher ist davon auszugehen, dass bei Verbrechen mit einer Strafdrohung von mehr als fünf Jahren Freiheitsstrafe jedenfalls eine schwere Straftat im Sinne des nationalen Rechts vorliegt.⁴⁶ Einzuräumen ist allerdings, dass diese Schwelle weit über den Vorstellungen der Gemeinsamen Erklärung von Rat und Kommission liegt, weshalb dieser Zugang zur Begriffsdefinition vor dem Hintergrund europäischer Wertungen eher problematisch erscheint.

Freilich ließe aber auch eine Festlegung auf den Verbrechensbegriff des § 17 StGB zur Definition des Begriffs „schwere Straftat“ Wertungswidersprüche und Probleme zu Tage treten: So wäre etwa der Entzug der persönlichen Freiheit gemäß Art. 2 Abs. 2 Z. 1 des Bundesverfassungsgesetzes über den Schutz der persönlichen Freiheit oder die Überwachung von Nachrichten gemäß § 135 StPO, also die Überwachung von Gesprächsinhalten, unter geringeren Anforderungen zulässig als der Zugriff auf Vorratsdaten. Und schließlich könnte es die Strafverfolgung in ein Dilemma bringen, wenn eine Auskunft über Verkehrsdaten ab dem Moment nur mehr bei Verbrechen – und nicht bei sonstigen, „niederschwelligeren“ Straftaten – zulässig wäre, ab dem diese nicht mehr für Verrechnungszwecke benötigt werden und zu Vorratsdaten werden.

Dennoch scheint die Festlegung auf den Verbrechensbegriff des § 17 StGB zur Definition einer „schweren Straftat“ im Sinne der Richtlinie aus grundrechtlichen Erwägungen heraus geboten: Da die Verwendung von Vorratsdaten einen über die traditionelle Überwachung hinausgehenden Grundrechtseingriff darstellt, ist damit auch aus dem bisherigen System heraus zwingend, dass für diese neue Maßnahme keine niedrigere Eingriffsschwelle möglich ist. Bedenkt man auch die Zielsetzung der Richtlinie einerseits und die Reichweite des Grundrechtseingriffs andererseits, so erscheint das Verständnis der schweren Straftat als Verbrechen iSd § 17 StGB als adäquate, verhältnismäßige Auslegung. Auch wenn die Strafdrohung als Schwelle damit nicht mit Art. 2 Abs. 2 des Rahmenbeschlusses zum Europäischen Haftbefehl identisch ist, so können diese Taten im Sinne der Gemeinsamen Erklärung ebenso angemessene Berücksichtigung finden wie Straftaten, die unter dem Einsatz von Telekommunikationsmitteln begangen werden, vorausgesetzt, sie haben den im österreichischen Wertesystem traditionell erforderlichen Störwert, der sie zum Verbrechen macht. Das ist allerdings aufgrund der zumeist vorgesehenen Erfolgs- und Handlungsqualifikationen häufig der Fall. Und schließlich können auch Vergehen im Sinne des § 17 StGB weiterhin unter Zuhilfenahme von Verkehrsdaten ermittelt und verfolgt werden, soweit diese Daten – so wie bisher auch – für betriebsnotwendige-, insbesondere Verrechnungszwecke mindestens drei Monate bei den Telekommunikationsbetreibern gespeichert sind, bevor sie zu löschen sind, und den Strafverfol-

⁴⁶ Ähnlich *Otto/Seitlinger*, Die „Spitzel“-Richtlinie – Zur (Umsetzungs)Problematik der Data Retention Richtlinie 2006/24/EG, MR 2006, 227, die als Kriterium für die schwere Straftat entweder eine deutlich höhere Strafdrohung als die Verbrechensschwelle fordern oder auch eine taxative Aufzählung der Delikte für möglich halten.

gungsbehörden in diesem Zeitraum für Auskünfte zur Verfügung stehen. Jedenfalls im Bereich der Telefonrufdaten würde sich damit zur bisherigen Situation praktisch nichts ändern. In Bezug auf IP-Adressen muss hier festgehalten werden, dass nicht wenige Anbieter von Internet-Zugangsdiensten in den letzten Jahren auf Druck der Justiz diese Daten länger aufbewahrt haben, als sie diese für Zwecke der Störungsbehebung oder sonstige betrieblich notwendige Zwecke benötigt hätten, damit ohne ausdrückliche rechtliche Grundlage. Diese Daten werden künftig nach einigen Tagen (je nach System des Betreibers) ausschließlich als Vorratsdaten vorhanden sein, sodass nach dem vorgeschlagenen TKG-Entwurf für den Bereich der „niederschwelligeren“ Straftaten in Bezug auf IP-Adressen tatsächlich weniger Daten zur Verfügung stünden als nach der bisherigen grundrechtswidrigen und insbesondere datenschutzrechtswidrigen Praxis.

Im Übrigen empfiehlt sich aber für allfällige weitere gesetzgeberische Schritte die Erhebung, in welchen Verfahren die Möglichkeit, auf Vorratsdaten zuzugreifen, in der Praxis tatsächlich genutzt wird. Im Idealfall sollte auch eine Auswertung über den Nutzen der Erhebung durchgeführt werden. Ein erster Schritt zur Sammlung der für solche Evaluierungen notwendigen Daten könnte die Erfassung der Maßnahme in den jeweiligen Endverfügungen zu den Verfahren sein.

b) Sicherheitspolizeigesetz (SPG) und Datenschutzgesetz 2000 (DSG 2000)

Ähnlich wie zur StPO unter a) ausgeführt, erfordert die vorgeschlagene TKG-Novelle jedenfalls deshalb eine Anpassung des SPG, weil nach der neuen Bestimmung des § 99 Abs. 5 TKG der „Auskunft über Verkehrsdaten und zur Auskunft über Stammdaten, wenn hierfür die Verarbeitung von Verkehrsdaten erforderlich ist, sowie zur Auskunft über Standortdaten an nach dem SPG zuständige Sicherheitsbehörden“ eine gesetzliche Bestimmung zugrunde liegen muss, die „auf diesen Absatz zu verweisen, die konkreten Datenkategorien aufzuzählen, die berechtigten Behörden zu benennen und den Datenumfang auf das notwendige und verhältnismäßige Ausmaß zu beschränken“ hat. Außerdem darf gemäß der neuen Bestimmung § 102b TKG „eine Auskunft über Vorratsdaten (...) nur nach Maßgabe einer ausdrücklich auf § 102a verweisenden gesetzlichen Bestimmung“ erteilt werden. Die gemäß § 102b TKG grundsätzlich nur „zum Zweck der Ermittlung, Feststellung und Verfolgung schwerer Straftaten an die nach den Bestimmungen der StPO (...) zuständigen Behörden“ zulässige Auskunft über Vorratsdaten ist nur deshalb auch für den Anwendungsbereich des SPG relevant, weil § 99 Abs. 5 Z 2 eine eng determinierte Ausnahme für Standortdaten, nämlich einen Zugriff auf gemäß § 102a Abs. 3 Z 6 lit d) gespeicherte Vorratsdaten vorsieht. Dadurch ist aber zumindest ein insofern „formeller“ Verweis auf die genannten Bestimmungen des TKG im SPG perpetuiert, als ansonsten die in diesem Fall notwendige Verarbeitung von Verkehrsdaten zur Auskunft über Standortdaten nicht zulässig ist. Darüber hinaus scheint im Hinblick auf die Zulässigkeit der Verwendung von Verkehrsdaten ein Anpassungsbedarf des SPG aus nachfolgenden Erwägungen indiziert:

Mit den durch die Novelle BGBl Nr. I 114/2007 neu geschaffene Bestimmungen des SPG werden die Sicherheitsbehörden im Rahmen der Sicherheitspolizei unter näher bestimmten Voraussetzungen zum Zweck der Abwehr von Gefahren unter anderem ermächtigt, von Betreibern öffentlicher Telekommunikationsdienste näher bestimmte personenbezogene Auskünfte über Stamm-, Verkehrs- und Standortdaten zu verlangen und zu verarbeiten, ohne dass die Betroffenen im Nachhinein – nachdem der Zweck der Datenanwendung weggefallen ist – von den Sicherheitsbehörden über die Datenverwendung informiert werden.

Im Hinblick auf die im Entwurf vorgeschlagene Ermächtigung von Sicherheitsbehörden, unter bestimmten Voraussetzungen auch auf Vorrat gespeicherte Standortdaten beauskunften zu lassen (siehe den vorgeschlagenen § 99 Abs. 5 Z. 2 TKG), stellt sich angesichts des Umstands, dass die davon betroffenen Personen über die Datenverwendung auch im Nachhinein nicht informiert werden, ein grundrechtliches und rechtsstaatliches Problem. Dieses Problem ist auch in allen Fällen evident, in denen die Sicherheitsbehörden gemäß § 53 SPG von Betreibern öffentlicher Telekommunikationsdienste zwar personenbezogene Auskünfte verlangen können, die davon Betroffenen aber nicht einmal nach Erreichen oder Wegfall des Zwecks der Maßnahme über diese informiert werden, um allenfalls in einem Verfahren vor der DSK überprüfen lassen zu können, ob die Datenabfrage gesetzeskonform gewesen ist oder nicht. Dies wirft erhebliche Bedenken im Hinblick auf Art. 8 EMRK und das Recht auf eine wirksame Beschwerdemöglichkeit vor einer nationalen Instanz im Sinne des Art. 13 EMRK auf.⁴⁷

Grundsätzlich haben Auftraggeber einer Datenanwendung (und hier fungieren die Sicherheitsbehörden als solche) aus Anlass der Ermittlung von Daten die Betroffenen gemäß § 24 DSG 2000 (der nach § 51 Abs 2 SPG subsidiär anzuwenden ist) in geeigneter Weise über den Zweck der Datenverwendung sowie den Namen und die Adresse des Auftraggebers zu informieren. Nur stellt sich das Problem, dass § 24 DSG im vorliegenden Zusammenhang nicht zur Anwendung kommt. Werden nämlich Daten durch Übermittlung von Daten aus Anwendungen anderer Auftraggeber (hier: die Betreiber von Telekommunikationsdiensten) ermittelt, darf die Information gemäß § 24 DSG 2000 entfallen, wenn die Datenanwendung durch Gesetz oder Verordnung vorgesehen ist. Dies wird in der Praxis auch so gehandhabt.⁴⁸

Eine Reparatur des § 24 DSG 200 könnte derart erfolgen, dass einerseits die Informationspflicht nicht nur aus Anlass der „Ermittlung“, sondern auch der „Übermittlung“ von Daten vorgeschrieben wird. Andererseits könnte geregelt werden, dass die Information eines

⁴⁷ Siehe zu diesem Thema ausführlich *Tretter*, Grundrechtliche Probleme der Anwendung personenbezogener Daten durch Sicherheitsbehörden, in: ÖJK, Alles unter Kontrolle, Überwachung – Privatsphäre – Datenschutz, 2009, 55 ff.; *Feiler und Raschhofer in Zankl* (Hg.), Auf dem Weg zum Überwachungsstaat? – Neue Überwachungsmaßnahmen im Bereich der Informations- und Kommunikationstechnologie, 2009, 43 ff und 91 ff.

⁴⁸ Bestätigt vom BM.I durch die Beantwortung der Parlamentarischen Anfrage 4148/AB vom 23. Juni 2008 zu 4130/J, XXIII. GP.-NR.

Betroffenen dann, wenn ansonsten der Zweck der Datenanwendung (zB Gefahrenabwehr) gefährdet wäre, erst nach Erreichen oder Wegfall des Zwecks erfolgen kann. Schließlich sollte jedenfalls der in § 24 Abs. 4 DSG 2000 pauschal normierte Entfall der Informationspflicht bei Datenanwendungen gemäß § 17 Abs. 3 DSG 2000 aufgehoben oder zumindest materiell eingeschränkt werden. Damit würde die Informationspflicht, die in § 99 Abs. 5 Z 2 TKG vorgeschlagen wird, sachgerecht bei den Sicherheitsbehörden liegen und müsste nicht im TKG substituiert werden, um eine grundrechtskonforme Rechtslage zu schaffen.

Für das Ludwig Boltzmann Institut für Menschenrechte:

ao. Univ.Prof. Dr. Hannes Tretter

Mag. Ing. Christof Tschohl