Liechtensteinische Juristenzeitung (LJZ):
Für die Redaktion bestimmte Zuschriften und Manuskripte, Besprechungsexemplare und Zeitschriften sind an die Schriftleitung, FL-9490 Vaduz, Spaniagasse 1, zu richten. Die Vereinigung Liechtensteinischer Richter (VLR) behält sich das ausschliessliche Recht der Vervielfältigung und Verbreitung der zum Abdruck gelangenden Beiträge sowie ihre Verwendung für fremdsprachige Ausgaben vor. Für den Inhalt der einzelnen Abhandlungen trägt ausschliesslich der Autor die Verantwortung.

Druck: Gutenberg AG, FL-9494 Schaan
ISSN 1029–1776

Bezugsbedingungen:
Das Jahresabonnement der Liechtensteinischen Juristenzeitung (LJZ), umfassend vier Hefte, Inhaltsverzeichnis, Einbanddecke und Volltext-Suche auf der Homepage www.juristenzeitung.li, beträgt ab 01.01.2007 CHF 150.– zuzüglich Versandkosten.

Abonnements können beim Sekretariat der Vereinigung Liechtensteinischer Richter (VLR), Frau Roswitha Grabher, c/o Obergericht, FL-9490 Vaduz, Spaniagasse 1, Telefon +423 / 236 65 03, E-Mail: Roswitha.Grabher@lg.llv.li, aufgegeben werden.

Anzeigenaufträge werden von der Vereinigung Liechtensteinischer Richter (VLR), FL-9490 Vaduz, Spaniagasse 1, entgegengenommen.

LJZ

LIECHTENSTEINISCHE JURISTEN-ZEITUNG

Offizielles Mitteilungsorgan
der Vereinigung
Liechtensteinischer Richter (VLR)

2009

30. Jahrgang

Abhandlungen

Die Regelung des staatlichen Zugriffs auf Fernmeldedaten im Kommunikationsgesetz aus grundrechtlicher Sicht[1]

Hilmar Hoch[2]

1. Einleitung

Der staatliche Zugriff auf Fernmeldedaten ist eine grundrechtlich sensible Thematik. Allerdings hat die entsprechende Sensibilität in den letzten Jahren im Hinblick auf eine effizientere Bekämpfung von Terrorismus und organisiertem Verbrechen sichtlich nachgelassen. Zumindest im Ausland wird nun aber insbesondere im Zusammenhang mit der – in Liechtenstein schon verwirklichten – sogenannten Vorratsdatenerfassung eine intensive Diskussion geführt. Vor dem Hintergrund dieser ausländischen Debatte sowie der – bisher spärlichen – Rechtsprechung soll hier die einschlägige Regelung im Kommunikationsgesetz (KomG)[3] einer kritischen Würdigung aus grundrechtlicher Sicht unterzogen werden.

2. Rechtsgrundlagen

Die behördliche Erfassung und Verwertung von Fernmeldedaten ist in Liechtenstein ausser im KomG und der zugehörigen Verordnung über elektronische Kommunikationsnetze und -dienste (VKND)[4] auch in der Strafprozessordnung (StPO)[5] geregelt. Auch wenn die einschlägige Regelung im KomG bzw. der VKND primär Gegenstand dieser Untersuchung sind, ist somit auch die StPO einzubeziehen, zumal im KomG und in der VKND auch mehrfach auf das Strafverfahren Bezug genommen wird und sich – wie noch zu zeigen sein wird – auch darüber hinaus die analoge Anwendung diverser Bestimmungen der Strafprozessordnung aufdrängt. Hingegen ist das Datenschutzgesetz (DSG)[6] nur am Rande in seiner den grundrechtlichen Datenschutz konkretisierenden Funktion für die vorliegende Abhandlung von Bedeutung. Im Folgenden sind zunächst die relevanten Bestimmungen des KomG und der VKND sowie der StPO kurz darzustellen.

2.1 KomG- und VKND-Bestimmungen

Die für diese Untersuchung relevanten KomG-Bestimmungen finden sich in Abschnitt XI. «Kommunikations-

[1] Nachstehende Abhandlung wurde vom Verfasser als Gutachten zuhanden der Datenschutzstelle verfasst. Der Text wurde für die Publikation leicht angepasst. Literatur und Rechtsprechung sind bis Ende 2008 berücksichtigt.

[2] Hilmar Hoch, Dr. iur. (Bern), LL.M. (Harvard); Rechtsanwalt FL/NY; Vizepräsident des Staatsgerichtshofes.

[3] vom 17.03.2006, LGBl. 2006/91.

[4] vom 03.04.2007, LGBl. 2007/67.

[5] vom 18.10.1988, LGBl. 1988/62.

[6] vom 14.03.2002, LGBl. 2002/55.

geheimnis; Datenschutz; Mitwirkungspflichten» (Art 48 bis 53 KomG). Näher zu untersuchen sind dabei die Art 52 und 53.[7]

Gemäss Art 52 KomG haben alle Anbieter die technischen Einrichtungen zur elektronischen Kommunikationsüberwachung in Strafverfahren bereitzustellen und bei dieser Überwachung mitzuwirken (Abs 1). Hierfür sind sämtliche Verkehrsdaten[8] aufzuzeichnen und während sechs Monaten aufzubewahren (Abs 2).

Gemäss Art 53 KomG haben Anbieter öffentlich zugänglicher Kommunikationsdienste sämtliche Teilnehmerdaten aufzuzeichnen und während der gesamten Dauer der vertraglichen Beziehungen mit dem betreffenden Teilnehmer sowie sechs Monate nach deren Beendigung aufzubewahren (Abs 1). Die Anbieter sind hinsichtlich dieser Daten zur unverzüglichen Auskunftserteilung gegenüber dem Untersuchungsrichter und, sofern die Daten zur gesetzlichen Aufgabenerfüllung unbedingt benötigt werden, auch gegenüber der Landespolizei verpflichtet (Abs 2).

Auf die Erörterung der einschlägigen VKND-Bestimmungen in den Abschnitten VII. «Datenschutz» (Art 49 bis 59 VKND) und VIII. «Mitwirkung und Auskunftserteilung» (Art 60 bis 68 VKND) kann verzichtet werden. Abschnitt VII. dient wiederum primär dem Schutz gegen Missbräuche durch die Anbieter. Im Abschnitt VIII. sind insbesondere technische Anforderungen an die Mitwirkung der Anbieter bei der Überwachung geregelt. Diese sind für die gegenständliche Untersuchung ebenfalls nicht wesentlich, zumal sie sich im gesetzlichen Rahmen bewegen und somit auch gesetzeskonform im Sinne der StGH-Rechtsprechung sind (siehe StGH 2003/2, LES 2005, 281 [Erw. 3.2]; StGH 1998/37, LES 2001, 69 [Erw. 2.2]).

Es genügt somit, die mit der Mitwirkung der Anbieter bei der Datenspeicherung und Überwachung der elektronischen Kommunikation verbundenen Grundrechtseingriffe anhand der Regelung im KomG zu überprüfen.

2.2 StPO-Bestimmungen

Die hier wesentlichen StPO-Bestimmungen zur Überwachung einer elektronischen Kommunikation finden sich in § 103 f. Gemäss § 103 Abs 1 StPO ist eine solche Überwachung nur zur Aufklärung einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten Straftat zulässig. Eine Überwachung ist auf drei Monate befristet, kann jedoch jeweils um drei Monate verlängert werden. Gemäss § 104 Abs 3 StPO sind «jedenfalls» Aufzeichnungen von Gesprächen zwischen einem Verdächtigen und seinem Verteidiger zu vernichten, sofern nicht beide die Aufbewahrung verlangen. Blosse Verkehrs- und Standortdaten sind also von diesem Verwertungsverbot nicht erfasst. Generell keine Berücksichtigung finden bei der Überwachung der elektronischen Kommunikation die weiteren in der StPO neben demjenigen des Verteidigers normierten Zeugnisverweigerungsrechte von Berufsgeheimnisträgern. Das Zeugnis verweigern dürfen auch Rechtsanwälte, Rechtsagenten, Wirtschaftsprüfer[9] und Patentanwälte (§ 107 Abs 1 Ziff 3 StPO) sowie Psychiater[10], Psychotherapeuten, Psychologen, Bewährungshelfer und Mediatoren (§ 107 Abs 1 Ziff 4 StPO). Geistliche dürfen zudem gemäss § 106 Abs 1 Ziff 1 von vornherein nicht als Zeugen vernommen werden.[11]

3. Exkurs: EWR-Recht

Die oben angeführten KomG-Bestimmungen dienen gemäss Art 1 Abs 1 lit. f KomG unter anderem auch der Umsetzung der Richtlinie 2002/58/EG, welche im Gegensatz zum strengen Datenschutz gemäss Art 6 der allgemeinen Richtlinie 95/46/EG die Mitgliedstaaten ermächtigte die Anbieter zu verpflichten, die Verkehrsdaten ihrer Nutzer zur Terrorismusbekämpfung und zur Strafverfolgung den Behörden zur Verfügung zu stellen. Eine Verpflichtung zur Vorratsdatenspeicherung enthielt die Richtlinie indessen noch nicht.[12]

Diese Richtlinie ist inzwischen durch die noch weitergehende Richtlinie 2006/24/EG vom 15.03.2006 ergänzt worden, nach deren Art 6 nunmehr eine mindestens sechsmonatige und maximal zweijährige Speicherungsfrist vorgeschrieben ist. Die neue Richtlinie ist in Liechtenstein noch nicht formell, wohl aber – jedenfalls hinsichtlich der sechsmonatigen Vorratsdatenspeicherung – materiell umgesetzt worden.

4. Rechtsvergleich

Das KomG und die VKND stellen zum grossen Teil schweizerische Rezeptionsmaterie dar. In Österreich ist die Verkehrsdatenerfassung und -verwertung abgesehen vom Telekommunikationsgesetz detailliert in der dortigen Strafprozessordnung geregelt; dies liegt nahe, weil auch die Telekommunikationsüberwachung in Österreich – wie im Übrigen in Liechtenstein – primär in der

[7] Nicht direkt relevant für diese Abhandlung sind die Art 48 («Kommunikationsgeheimnis»), Art 49 («Datenschutz»), Art 50 («Unerbetene Nachrichten») und Art 51 («Mitwirkung bei der Standortfeststellung»). Art 48 bis 50 KomG regeln den Schutz der Teilnehmer bzw. Nutzer gegen Missbräuche durch die Anbieter und betreffen somit nicht die hier einschlägigen staatlichen Massnahmen. Art 51 KomG regelt zwar auch die Weitergabe von elektronischen Kommunikationsdaten an staatliche Behörden, konkret die Verpflichtung der Betreiber, im Falle einer unmittelbaren Gefährdung der physischen Integrität einer Person bei der Feststellung des Standorts eines bestimmten Mobilfunknetzanschlusses mitzuwirken (Abs 1) sowie das Verbot, entsprechende Daten für andere Zwecke zu verwenden (Abs 3). Diese Regelung erscheint aber aus grundrechtlicher Sicht unproblematisch.

[8] Verkehrsdaten betreffen u.a. Datum, Dauer und Teilnehmer einer elektronischen Kommunikation. Sie sind zu unterscheiden von (die Inhalte der übertragenen Nachrichten betreffenden) Inhaltsdaten, Standortdaten (zur Ermittlung des Standortes insbesondere eines Mobilfunkteilnehmers) sowie (personenbezogenen) Teilnehmerdaten; vgl. die entsprechenden Legaldefinitionen in Art 3 Abs 1 KomG.

[9] Nicht aber Bankangestellte und Berufstreuhänder; letzteres gilt auch für Rechtsanwälte, soweit sie in treuhänderischer Funktion tätig sind; siehe StGH 1998/39, Erw. 5.6 ff.

[10] Hingegen gibt es kein generelles Zeugnisverweigerungsrecht für Ärzte (siehe zur analogen österreichischen Regelung Kurt Kirchbacher, Wiener Kommentar StPO, Wien 2007, § 151 RZ 53).

[11] Weniger relevant sind im gegebenen Zusammenhang die Regelungen in § 106 Abs 1 Ziff 2 (Staatsbeamte, welche nicht vom Amtsgeheimnis entbunden sind) und Ziff 3 (Zeugnisunfähige).

[12] Siehe Andreas Gietl, Das Schicksal der Vorratsdatenspeicherung, DuD 5/2008, S. 317.

Strafprozessordnung geregelt ist. Aufgrund dieser engen Verflechtung mit dem schweizerischen und dem österreichischen Recht erscheint es jedenfalls sinnvoll, die dortigen Regelungen rechtsvergleichend heranzuziehen.

4.1 Schweiz

Die Überwachung des Fernmeldeverkehrs ist in der Schweiz primär im Bundesgesetz vom 06.10.2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) und der diesbezüglichen Verordnung vom 31.10.2001 (VÜPF) geregelt.

Gemäss Art 15 BÜPF sind die Anbieter verpflichtet, die für die Teilnehmeridentifikation notwendigen Daten sowie die Verkehrs- und Rechnungsdaten während sechs Monaten aufzubewahren (Abs 3). Während mindestens zwei Jahren nach Aufnahme der Kundenbeziehung müssen sie Auskünfte über Fernmeldeanschlüsse auch über Personen erteilen können, welche die Kundenbeziehung für Mobiltelefone nicht über ein Abonnementverhältnis aufgenommen haben (Abs 5bis).

Solche Auskünfte über Fernmeldeanschlüsse umfassen gemäss Art 14 Abs 1 BÜPF Name, Adresse und gegebenenfalls Beruf des Teilnehmers oder der Teilnehmerin, die Adressierungselemente und die Art der Anschlüsse. Diese Auskünfte sind gemäss Art 14 Abs 2 BÜPF den kantonalen und Bundesbehörden mit der Kompetenz zur Anordnung von Telefonüberwachungen (lit. a), der Polizei für die Erfüllung von Polizeiaufgaben (lit. b) sowie den zuständigen Behörden zur Erledigung von Verwaltungsstrafsachen (lit. c) zu erteilen.

Dagegen ist die Verwendung der Verkehrs- und Rechnungsdaten Teil der Überwachung des Fernmeldeverkehrs (Art 5 Abs 1 BÜPF). Eine solche Überwachung ist nur bei Verdacht auf Begehung einer in Art 3 Abs 2 BÜPF angeführten, abschliessenden Liste von Katalogtaten zulässig. Auskünfte betreffend Teilnehmeridentifikation und Verkehrs- und Rechnungsdaten können auch sechs Monate rückwirkend angeordnet werden (Art 5 Abs 2 BÜPF). Eine Überwachung darf nur durch den Richter oder eine ihm gleichgestellte Behörde (Art 6 BÜPF), nicht aber durch die Polizei angeordnet werden.

Auch bei der Überwachung der elektronischen Kommunikation sind die – durch strafprozessuale Zeugnisverweigerungsrechte geschützten[14]

- Berufsgeheimnisse gemäss der Regelung in Art 8 BÜPF umfassend geschützt. Informationen, welche ein durch ein Zeugnisverweigerungsrecht geschütztes Berufsgeheimnis betreffen, dürfen nicht verwendet werden und sind sofort zu vernichten (Abs 3). Eine Ausnahme besteht nur dann, wenn den Berufsgeheimnisträger selbst ein dringender Verdacht hinsichtlich einer Katalogtat trifft (Abs 4).

[14] So ausdrücklich Art 4 Abs 3 BÜPF. Insbesondere das Treuhänder- und das Bankgeheimnis sind somit nicht erfasst (vgl. zum Bankgeheimnis Maurice Aubert et al., Le secret bancaire suisse, Bern 1995, S. 144 ff.).

4.2 Österreich

Österreich hatte die Telekommunikationsüberwachung bis zum 31.12.2007[15] detailliert in § 149a öStPO geregelt. Die ursprüngliche Regelung i.d.F. BGBl. 1975/631 wurde von Liechtenstein im Rahmen der weitgehend wörtlichen Rezeption der österreichischen StPO im Jahre 1988 übernommen. Hingegen wurden die zahlreichen in der Folge vorgenommenen österreichischen Revisionen der Telefonabhörregelung in Liechtenstein nur teilweise nachvollzogen. Insbesondere hat Österreich im Gegensatz zu Liechtenstein das ursprünglich auf den Verteidiger beschränkte Verwertungsverbot auch für die Telekommunikationsüberwachung sukzessive auf weitere Berufsgeheimnisträger ausgedehnt.[16]

Eine Vorratsdatenerfassung gibt es derzeit in Österreich noch nicht. Zwar enthält § 94 Abs 3 des Telekommunikationsgesetzes eine entsprechende Verordnungsermächtigung, welche aber bisher noch nicht umgesetzt worden ist. Während die Telekommunikationsüberwachung im Rahmen eines Strafverfahrens gemäss § 149a öStPO nur mit richterlicher Bewilligung erfolgen konnte, sieht § 53 des Sicherheitspolizeigesetzes zur Abwehr besonderer Gefahren für die öffentliche Ordnung bzw. zu Fahndungszwecken (Abs 1) vor, dass die Polizei unter anderem von den Betreibern öffentlicher Telekommunikationsdienste die Erteilung von Verkehrsdatenauskünften verlangen kann (Abs 3a). Hiergegen sind aber mehrere, unter anderem von der Grünen Partei Österreichs eingereichte Beschwerden beim Verfassungsgerichtshof hängig.[16]

5. Erfassung und Verwertung von Fernmeldedaten als Grundrechtseingriff

In Liechtenstein stellt der Datenschutz einen Teilbereich der Geheim- und Privatsphäre gemäss Art 32 Abs 1 LV bzw. Art 8 EMRK dar; dies im Einklang mit der Schweiz, aber im Gegensatz zu Österreich und Deutschland, wo jeweils ein entsprechendes spezifisches Grundrecht besteht.[17]

[15] Mit dem am 01.01.2008 in Kraft getretenen sogenannten Strafprozessreformgesetz wurden grosse Teile der österreichischen StPO revidiert bzw. neu redigiert. Da Liechtenstein aber diese Änderungen bisher nicht rezipiert hat, ist hier nicht auf die reformierte Fassung einzugehen. Siehe zur neuen Rechtslage aber Daniel Ennöckl, Der Rechtsschutz gegen sicherheitsbehördliche Massnahmen nach Inkrafttreten des Strafprozessreformgesetzes, JBl. 2008, 409.

[16] Siehe vorne unter Punkt 2.2.

[16] Siehe www.ueberwachungsstaat.at/index.php?id=56961.

[17] Vgl. den Hinweis auf die analoge schweizerische Rechtslage in der Entscheidung der liechtensteinischen Datenschutzkommission vom 07.04.2008, DSK 2007/1, S. 9, Erw. 4 mit Verweis auf Arthur Haefliger/Frank Schürmann, Die Europäische Menschenrechtskonvention und die Schweiz, 2. A., Bern 1999, S. 258. In Österreich normiert § 1 öDSG ein Grundrecht auf Datenschutz, wobei diese Bestimmung ihrerseits auf Art 8 EMRK verweist (Susanne Reindl, Wiener Kommentar StPO, Wien 2005, Vor §§ 149 a-c, RZ 10). In Deutschland hat das Bundesverfassungsgericht mit Urteil vom 27.02.2008 («Online-Durchsuchung») ein Grundrecht «auf Vertraulichkeit und Integrität informationstechnischer Systeme» anerkannt. Dieses neue Grundrecht greift allerdings nur Platz, soweit ein hinreichender Schutz des Persönlichkeitsrechts durch andere Grundrechte nicht gewährleistet ist, sodass es nur eine subsidiäre Funktion hat (siehe hierzu Thomas B. Petry, Das Bundesverfassungsgericht zur «Online-Durchsuchung», DuD 7/2008, S. 443 [insb. S. 444]).

Klarerweise greift nicht nur die inhaltsbezogene Telekommunikationsüberwachung, sondern auch die Erhebung von Verkehrs- und Standortdaten in den sachlichen Schutzbereich der Geheim- und Privatsphäre ein.[18] Zwar wird auch die Erhebung von Teilnehmerdaten von diesem Grundrecht erfasst, sie stellt aber nur einen leichten Eingriff dar.

Eingriffe in spezifische Grundrechte sind nach ständiger StGH-Rechtsprechung nur zulässig, wenn sie auf einer genügenden gesetzlichen Grundlage beruhen, verhältnismässig und im öffentlichen Interesse sind sowie den Kerngehalt des betreffenden Grundrechts nicht verletzen.[19] Auch die Datenschutzkommission hat in einer kürzlichen Entscheidung betont, dass datenschutzsensible behördliche Massnahmen den vom Staatsgerichtshof entwickelten Grundrechtseingriffskriterien zu genügen haben.[20] Die Notwendigkeit einer gesetzlichen Grundlage sowie das Verhältnismässigkeitserfordernis für die behördliche Erfassung von personenbezogenen Daten werden auch explizit im DSG normiert.[21]

6. Grundrechtssensible Bereiche der geltenden Zugriffsregelung

6.1 Zeugnisverweigerungsrechte von Berufsgeheimnisträgern

Ein zentrales grundrechtliches Problem beim staatlichen Zugriff auf Fernmeldedaten ist der Schutz der diversen gesetzlich normierten Zeugnisverweigerungsrechte. Diese Zeugnisverweigerungsrechte dienen grossteils der Durchsetzung verschiedener gesetzlich normierter Berufsgeheimnisse[22] und sind somit wiederum Ausfluss des grundrechtlichen Schutzes der Privatsphäre. Die Verwertung von unter Missachtung von Zeugnisverweigerungsrechten und somit widerrechtlich erlangten Beweismitteln in Gerichtsverfahren kann im Weiteren eine Verletzung des Anspruchs auf ein faires Verfahren gemäss Art 6 EMRK darstellen.[23]

Wie schon ausgeführt, ist nach der StPO-Regelung nur die Verwertung von Inhaltsdaten betreffend Gespräche mit dem Verteidiger (nicht aber entsprechender Verkehrsdaten) vom Gesetzgeber explizit als unzulässig erklärt worden.[24] Dies ist in einem solchen grundrechtssensiblen Bereich problematisch. Nachdem die Zeugnisverweigerungsrechte Ausfluss des Schutzes der Privatsphäre und des Anspruchs auf ein faires Verfahren sind, erscheint eine solche gesetzliche Regelung kaum verfassungskonform. Es ist auch nicht plausibel, dass die Zeugnisverweigerungsrechte mit Ausnahme desjenigen des Verteidigers dann plötzlich nicht mehr gelten sollen, wenn es nicht um die Zulässigkeit bzw. Verwertbarkeit von Zeugenaussagen, sondern von Fernmeldedaten geht. Dies läuft auf eine Aushöhlung des Zeugnisverweigerungsrechts hinaus. Diese inkonsequente Regelung ist besonders gravierend, soweit sie die einen besonders schweren Grundrechtseingriff darstellende Inhaltsdatenerfassung und -verwertung betrifft. Doch auch für die (blosse) Verkehrs- und Standortdatenerfassung lässt sich dies wohl kaum rechtfertigen, zumal im Bezug auf solche Daten, wie ausgeführt, nicht einmal die elektronische Kommunikation des Beschuldigten mit dem Verteidiger zwingend geschützt ist; dies im Gegensatz zur Schweiz und Österreich, wie der vorne vorgenommene Rechtsvergleich zeigt.[25] Insgesamt stellt die weitgehende Nichtbeachtung des Zeugnisverweigerungsrechts bei der Telekommunikationsüberwachung einen unverhältnismässigen Eingriff in die betroffenen Grundrechte dar. Es ist deshalb anzunehmen, dass der Staatsgerichtshof entsprechende Verwertungsverbote mangels gesetzlicher Regelung in analoger Anwendung der gesetzlichen Zeugnisverweigerungsrechte nicht nur für die Inhaltsdatenerfassung und -verwertung, sondern auch hinsichtlich Verkehrsdaten einschliesslich Vorratsdaten anerkennen bzw. direkt aus der Verfassung und der EMRK ableiten würde.[26]

6.2 Vorratsdatenerfassung

Grundrechtlich problematisch ist im Weiteren die Regelung der Vorratsdatenerfassung.[27] Der Staatsgerichtshof hatte sich schon in der StGH-Entscheidung 2006/19 mit

[18] In diesem Sinne offensichtlich auch StGH 2006/19, LES 2008, 1 (5 Erw. 2.2.2). Vgl. auch Susanne Reindl (FN 17), Vor §§ 149 a-c, RZ 4 mit Verweis auf die EGMR-Entscheidung Malone v. UK 8691/79 § 64.

[19] Vgl. anstatt vieler: StGH 1997/19, LES 1998, 269 (273 f. Erw. 3.2 f.); spezifisch zur Telefonabhörung siehe StGH 2006/19, LES 2008, 1 (4 Erw. 2.1).

[20] Siehe Entscheidung der Datenschutzkommission vom 07.04.2008 (DSK 2007/1), S. 9 f., Erw. 5.1.

[21] Zur gesetzlichen Grundlage siehe Art 21 DSG; vgl. hierzu auch DSK 2007/1 (FN 20), S. 10, Erw. 5.2. Der Verhältnismässigkeitsgrundsatz ist in Art 22 DSG normiert.

[22] Vgl. vorne Punkt 2.2 sowie Kurt Kirchbacher (FN 10), § 151, RZ 6.

[23] StGH 2002/38, Erw. 4.3; siehe hierzu auch Hilmar Hoch, Grundrechtliche Verfahrensgarantien in der Rechtsprechung des liechtensteinischen Staatsgerichtshofes, in: DACH-Schriftenreihe Bd. 2, Grundrechtsschutz in gerichtlichen Verfahren, Wien 1994, 105 (112 f.). Der Staatsgerichtshof hat den Anspruch auf ein faires Verfahren auch als Ausfluss des innerstaatlichen Grundrechts auf rechtliches Gehör qualifiziert (StGH 2003/90, LES 2006, 89 [91 Erw. 2.1]; vgl. hierzu auch Tobias Michael Wille, Liechtensteinisches Verfassungsprozessrecht, LPS Bd. 43, Schaan 2007, S. 377 f.).

[24] Siehe vorne Punkt 2.2. Zwar enthält Art 15 des Rechtsanwaltsgesetzes (RAG) eine Verschwiegenheitsbestimmung, welche nach Abs 1 aber ausdrücklich unter den Vorbehalt der verfahrensrechtlichen Bestimmungen steht – welche eben kein entsprechendes Verbot beinhalten. Hieran ändert auch Abs 2 nichts, wonach dieses Verschwiegenheitsrecht auch nicht durch gerichtliche oder sonstige behördliche Massnahmen wie unter anderem die Beschlagnahmung von Datenträgern umgangen werden darf. Denn die restriktive Unverwertbarkeitsregelung in § 104 Abs 3 StPO stellt insoweit eine spezifische verfahrensrechtliche Norm dar, welche der Regelung in Art 15 RAG vorgeht.

[25] Siehe vorne Punkt 4.1, letzter Absatz; Punkt 4.2, 2. Absatz sowie Punkt 2.2.

[26] Siehe vorne Punkt 5.2.

[27] Der Begriff «Vorratsdatenerfassung» bezieht sich darauf, dass Telekommunikationsdaten voraussetzungslos für eine gewisse Zeit gespeichert werden. Der Begriff sagt an sich noch nichts darüber aus, um welche Art von Daten es sich dabei handelt. Indessen sind Inhaltsdaten hiervon faktisch nicht umfasst, da eine voraussetzungslose Speicherung von Inhaltsdaten von vornherein unverhältnismässig und somit verfassungswidrig wäre. Aus grundrechtlicher Sicht weitgehend unproblematisch ist auf der anderen Seite die Speicherung von Teilnehmerdaten (siehe vorne Punkt 5.1). Wenn hier von Vorratsdatenerfassung die Rede ist, ist primär die voraussetzungslose Speicherung von Verkehrsdaten gemeint.

der Vorratsdatenerfassung gemäss Art 16 AllKV[28] zu befassen. Er warf dabei allerdings die Frage von deren Verfassungskonformität nicht auf.[29] Auch wenn man aus dieser StGH-Entscheidung eine implizite Bejahung der Verfassungsmässigkeit der Vorratsdatenerfassung ableiten wollte, so kann sie wohl nicht als definitive Stellungnahme des Staatsgerichtshofes zu dieser Frage qualifiziert werden; dies zumal die Vorratsdatenerfassung, welche sich gerade dadurch auszeichnet, dass sie ohne jeglichen Verdacht auf eine Straftat erfolgt, aus grundrechtlicher Sicht heikel ist.[30] So ist in Deutschland derzeit eine Vielzahl von Verfassungsbeschwerden gegen ein entsprechendes Gesetz hängig.[31] Es ist auch bezeichnend, dass in Deutschland der Bundesrat zwar schon im Jahre 1996 eine Vorratsdatenerfassung forderte, Bundestag und Bundesregierung dies aber während Jahren wegen verfassungsrechtlichen Bedenken ablehnten.[32] Der deutsche Datenschutzbeauftragte erachtet eine solche Vorratsdatenspeicherung jedenfalls als verfassungswidrig.[33] Grosse Bedenken hat auch die sogenannte «Art 29-Arbeitsgruppe», das Gremium von Datenschutzbeauftragten des EWR-Raumes gemäss der Richtlinie 95/46/EG.[34] In Deutschland wird im Übrigen die generelle Verfassungswidrigkeit der Vorratsdatenerfassung gerade auch damit begründet, dass dadurch die verschiedenen gesetzlich normierten Berufsgeheimnisse ausgehöhlt würden.[35] Dabei sieht die dortige Regelung – anders als in Liechtenstein, aber ähnlich wie in der Schweiz und in Österreich – ein weitgehendes Verwertungsverbot für Telekommunikationsdaten betreffend zeugnisverweigerungsberechtigte Personen vor.[36]

Die noch ausstehende Entscheidung des Bundesverfassungsgerichts, aber auch zukünftige Entscheidungen des österreichischen Verfassungsgerichtshofes oder des schweizerischen Bundesgerichts werden zweifellos einen wesentlichen Einfluss auf die Position haben, welche der Staatsgerichtshof bei einer allfälligen erneuten Befassung mit der Frage der Verfassungsmässigkeit der Vorratsdatenerfassung einnehmen wird; dies zumal es der Staatsgerichtshof in einem Kleinstaat wie Liechtenstein als «durchaus gerechtfertigt (erachtet), die Rechtsvergleichung als eigentliche ‹fünfte Auslegungsmethode› zu bezeichnen».[37]

6.3 Verwertung von Vorratsdaten

Wenn die Vorratsdatenerfassung, weil sie voraussetzungslos erfolgt, aus grundrechtlicher Sicht schon von vornherein problematisch ist, muss jedenfalls der Zugriff auf solche Daten – soweit Verkehrsdaten betroffen sind[38] – an strenge Voraussetzungen gebunden sein. In Liechtenstein ist denn auch wie in der Schweiz[39] für den Zugriff auf entsprechende Vorratsdaten das gleiche Bewilligungsprozedere wie für eine inhaltsbezogene Telekommunikationsüberwachung einzuhalten.[40] Doch auch diese strengen Zugriffs- bzw. Verwertungsvorschriften können die grundrechtliche Problematik der voraussetzungslosen Vorratsspeicherung von Verkehrsdaten letztlich nicht ausräumen.

Auf gespeicherte Teilnehmerdaten kann der Untersuchungsrichter hingegen gemäss Art 53 Abs 2 lit. a KomG unabhängig von der Schwere der vom Verdacht erfassten Straftat greifen. Auch die Polizei kann dies gemäss lit. b dieser Bestimmung ohne richterliche Bewilligung tun, «sofern sie die Daten zur Erfüllung ihrer gesetzlichen Aufgaben unbedingt benötigt».[41] Diese Regelung entspricht ebenfalls derjenigen in der Schweiz.[42] Da die Erfassung und Verwertung von Teilnehmerdaten, wie erwähnt, nur einen leichten Eingriff in die Privat- und Geheimsphäre darstellt, erscheint diese Regelung verhältnismässig und somit grundrechtskonform.

6.4 Fazit

Wegen des ungenügenden gesetzlichen Schutzes des Zeugnisverweigerungsrechts bei der Überwachung der elektronischen Kommunikation wird hier der Staatsgerichtshof voraussichtlich die in der Strafprozessordnung verankerten Zeugnisverweigerungsrechte von Berufsgeheimnisträgern analog anwenden. Im Weiteren ist die voraussetzungslose Vorratserfassung von Verkehrsdaten trotz den strengen Kriterien für den Zugriff auf solche Daten grundrechtlich jedenfalls problematisch. Ob sie der Staatsgerichtshof als verfassungswidrig qualifizieren wird, dürfte auch wesentlich von der zukünftigen einschlägigen ausländischen Grundrechtsprechung abhängen.

---

[28] Verordnung vom 13.01.2004 über die für die Allgemeinheit bestimmte Konzessionsordnung nach dem Telekommunikationsgesetz sowie dem Gesetz über Radio und Fernsehen (AllKV), LGBl. 2004/45; inzwischen durch Art 73 lit. h VKND aufgehoben.

[29] StGH 2006/19, LES 2008, 1 (5 f., Erw. 2.2.2).

[30] Vgl. auch die schon mehrfach erwähnte Entscheidung der Datenschutzkommission DSK 2007/1 (FN 20). Diese Entscheidung betraf die Videoüberwachung öffentlicher Räume sowie die Speicherung dieser Daten und somit auch eine Variante der voraussetzungslosen «Vorratsdatenspeicherung». Die Datenschutzkommission rügte neben der fehlenden gesetzlichen Grundlage auch die mangelnde Verhältnismässigkeit der Massnahme (DSK 2007/1, S. 10 f., Erw. 5.2 und 5.4).

[31] Andreas Gietl (FN 12), S. 321.

[32] Andreas Gietl (FN 12), S. 317 f.

[33] Hans-Jörg Albrecht/Adina Grafe/Michael Kilchling, Rechtwirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO. Forschungsbericht im Auftrag des Bundesministeriums für Justiz, S. 63.

[34] Stellungnahme 3/2006 vom 25.03.2006; http://europa.eu.int/comm/justice_home/fsi/privacy/index_de.htm.

[35] Stellungnahme vom 13.07.2007 zum Regierungsentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmassnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (im Internet abrufbar unter www.vorratsdatenspeicherung.de), S. 1.

[36] § 53d StPO i.d.F. 26.12.2007 (in Kraft seit 01.01.2008); vgl. Stellungnahme vom 13.07.2007 (FN 35), S. 15.

[37] StGH 2000/6, Erw. 5.1 mit Verweis auf Wolfram Höfling, Die liechtensteinische Grundrechtsordnung, LPS Bd. 20, Vaduz 1994, S. 46; dieser wiederum mit Verweis auf Peter Häberle.

[38] Siehe FN 27.

[39] Siehe vorne Punkt 4.1. In Österreich gibt es derzeit noch keine Vorratsdatenerfassung (siehe vorne Punkt 4.2).

[40] Gemäss § 103 Abs 1 StPO setzt dies u.a. eine vorsätzliche mit mehr als einjähriger Freiheitsstrafe bedrohte Straftat voraus; siehe vorne Punkt 2.2; insoweit anders, wie erwähnt, die Regelung in der Schweiz, wo eine abschliessende Liste von Katalogtaten gilt; siehe vorne Punkt 4.1.

[41] siehe vorne Punkt 2.1.

[42] siehe vorne Punkt 4.1.