



universität
wien

DISSERTATION / DOCTORAL THESIS

Titel der Dissertation /Title of the Doctoral Thesis

„Berufsgeheimnisträger und Telekommunikation“

verfasst von / submitted by

Dipl.Jur. Ermano Geuer

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of
Doktor der Rechtswissenschaften (Dr.iur.)

Wien, am 21.12.2017

Studienkennzahl lt. Studienblatt /
degree programme code as it appears on the student
record sheet:

A 783 101

Dissertationsgebiet lt. Studienblatt /
field of study as it appears on the student record sheet:

Rechtswissenschaften

Betreut von / Supervisor:

ao. Univ.-Prof. Dr. Hannes Tretter

Inhalt

1. Einleitung.....	12
Kapitel I – Die Gruppe der Berufsheimnisträger	15
2. Einfachgesetzlicher Schutz von Berufsheimnissen	15
2.1. Berufsrechtlicher Schutz in Österreich.....	17
2.1.1. Heilberufe.....	17
2.1.2. Geistliche und Seelsorger.....	19
2.1.3. Rechtsberatung	20
2.1.4. Medienmitarbeiter	21
2.2. Berufsrechtlicher Schutz in Deutschland.....	22
2.2.1. Heilberufe.....	22
2.2.2. Geistliche und Seelsorger.....	22
2.2.3. Rechtsberatung	23
2.2.4. Medienmitarbeiter	24
2.3. Strafprozessualer Schutz in Österreich.....	24
2.3.1. Heilberufe.....	25
2.3.2. Geistliche und Seelsorger.....	25
2.3.3. Rechtsberatung	26
2.3.4. Medienmitarbeiter	26
2.4. Strafprozessualer Schutz in Deutschland.....	27
2.4.1. Heilberufe.....	28
2.4.2. Geistliche und Seelsorger.....	28
2.4.3. Rechtsberatung	29
2.4.4. Medienmitarbeiter	30
2.5. Schutz nach sonstigen Vorschriften in Österreich.....	32
2.6. Schutz nach sonstigen Vorschriften in Deutschland	33
3. Verfassungsrechtliche Grundlagen des Berufsheimnisträgerschutzes in Österreich	34

3.1.	Art 6 EMRK – Recht auf ein faires Verfahren	35
3.2.	Art 8 EMRK – Recht auf Achtung des Privat- und Familienlebens	36
3.2.1.	Schutz der Korrespondenz	36
3.2.2.	Schutz der Wohnung	37
3.2.3.	Schutz des Privatlebens	37
3.3.	§ 1 HausrechtsG, Art 9 StGG – Schutz des Hausrechtes	38
3.4.	Art 6 StGG – Erwerbsfreiheit	39
3.5.	Art 14 StGG, Art 9 EMRK – Glaubensfreiheit	39
3.6.	Art 13 StGG, Z 2 Beschluss ProvNV, Art 10 EMRK – Medienfreiheit	40

4. Verfassungsrechtliche Grundlagen des Berufsgeheimnisträgerschutzes in Deutschland 40

4.1.	Art 12 Abs 1 GG – Berufsfreiheit.....	41
4.2.	Art 5 Abs 1 S 2 GG – Presse- und Rundfunk und Filmfreiheit.....	42
4.3.	Art 4 Abs 1 und 2 GG – Religionsfreiheit.....	45
4.4.	Art 13 Abs 1 GG – Grundrecht auf Unverletzlichkeit der Wohnung.....	46

5. Grundlagen des Berufsgeheimnisträgerschutzes in der GRC..... 47

6. Ergebnisse..... 48

Kapitel II – Überwachung von Telekommunikation 50

7. Einzelne Überwachungsmaßnahmen..... 50

7.1.	Technische Beschreibung von digitalen Überwachungsmaßnahmen	51
7.1.1.	„Stummes SMS“	52
7.1.2.	IMSI-Catcher.....	53
7.1.3.	IMEI-Catcher	54
7.1.4.	Abhören von Gesprächen	54
7.1.5.	E-Mail- und Textnachrichtenüberwachung.....	55
7.1.6.	Quellen-Telekommunikationsüberwachung	55
7.1.7.	Online-Durchsuchung	56

7.1.8. Vorratsdatenspeicherung.....	56
7.1.9. Abfrage von Kundendaten	57
7.1.9.1. Funkzellenabfrage	57
7.1.9.2. Rufdatenrück Erfassung / Zielwahlsuche	58
7.1.10. Durchsuchung von Endgeräten der Telekommunikation.....	58
7.2. Strafprozessuale und sicherheitspolizeiliche Telekommunikationsüberwachung in Österreich	58
7.2.1. Auskunft über Stamm- und Zugangsdaten, § 76a StPO	59
7.2.2. Auskunft über Daten einer Nachrichtenermittlung, §§ 135 Abs 2 StPO, 134 Z 2 StPO.....	60
7.2.2.1. Daten einer „Nachrichtenermittlung“	60
7.2.2.2. Voraussetzungen für die Herausgabe.....	62
7.2.3. Auskunft über Vorratsdaten, ehemaliger § 135 Abs 2a StPO.....	64
7.2.4. Überwachung von Nachrichten, § 135 Abs 3 StPO	64
7.2.5. Durchsuchung von Endgeräten der Telekommunikation.....	66
7.2.6. Gerichtliche Bewilligung	67
7.2.7. Befugnisse im SPG	69
7.2.8. Kontrolle durch den Rechtsschutzbeauftragten	71
7.2.9. Zuordnung einzelner Überwachungsmaßnahmen zu strafprozessualen und sicherheitspolizeilichen Ermächtigungsgrundlagen	72
7.3. Die strafprozessuale und polizeirechtliche Telekommunikationsüberwachung in Deutschland	76
7.3.1. Telekommunikationsüberwachung, § 100a Abs 1 dStPO.....	76
7.3.2. Erhebung von Verkehrsdaten, § 100g Abs 1 dStPO	77
7.3.3. Weitere Maßnahmen außerhalb von Wohnraum, § 100h dStPO.....	77
7.3.4. Technische Ermittlungsmaßnahmen bei Mobilfunkendgeräten, § 100i Abs 1 dStPO	77
7.3.5. Bestandsdatenauskunft, §100j dStPO	78
7.3.6. Durchsuchung von Endgeräten der Telekommunikation.....	78
7.3.7. Befugnisse im (bayerischen) Polizeirecht.....	78
7.3.8. Gerichtliche Bewilligung	80
7.3.9. Zuordnung einzelner Überwachungsmaßnahmen zu strafprozessualen und polizeirechtlicher Ermächtigungsgrundlagen	80

7.4. Vergleich.....	83
8. Verfassungsrechtliche Vorgaben für die Überwachung von Telekommunikation in Österreich	84
8.1. Art 10a StGG - Fernmeldegeheimnis	84
8.2. Art 8 EMRK – Recht auf Achtung des Privat- und Familienlebens	87
8.3. § 1 DSG 2000– Grundrecht auf Datenschutz	88
8.4. § 1 HausrechtsG, Art 9 StGG – Schutz des Hausrechts	89
9. Verfassungsrechtliche Vorgaben für die Überwachung von Telekommunikation in Deutschland	90
9.1. Art 10 GG – Fernmeldegeheimnis.....	90
9.2. Art 2 Abs 1 GG iVm Art 1 Abs 1 GG – Grundrecht auf informationelle Selbstbestimmung	94
9.3. Art 2 Abs 1 GG iVm Art 1 Abs 1 GG – Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme	97
9.4. Art 13 Abs 1 GG – Grundrecht auf Unverletzlichkeit der Wohnung.....	100
10. Vorgaben aus der Grundrechtecharta der Europäischen Union.....	101
11. Einfachgesetzlicher Schutz in Österreich.....	102
12. Einfachgesetzlicher Schutz in Deutschland.....	103
13. Ergebnisse.....	104
Kapitel III – Spannungsfeld zwischen verfassungsrechtlichem Telekommunikations- und Berufsgeheimnisträgerschutz und Überwachung im Lichte der Rechtsprechung in Österreich und Deutschland	106
14. Die Rechtslage in Österreich.....	107

14.1. Berufsgeheimnisträgerschutz im Rahmen der Telekommunikation in der Strafprozessordnung	107
14.2. Berufsgeheimnisträgerschutz im Rahmen der Telekommunikation im Sicherheitspolizeigesetz	110
14.3. Berufsgeheimnisträgerschutz im Rahmen der Telekommunikation im Telekommunikationsgesetz	110
15. Die Rechtslage in Deutschland	111
15.1. Aussagen des BVerfG bezüglich Berufsgeheimnisträgern	112
15.2. Gesetzliche Umsetzung von Beweiserhebungsverboten in Deutschland	114
15.2.1. Die Umsetzung in § 160a dStPO	114
15.2.2. Zulässigkeit der Unterscheidung einzelner Berufsgeheimnisträger	116
15.2.2.1. Rechtfertigung der Differenzierung	117
15.2.2.2. Differenzierung im Rahmen des § 160a dStPO	118
15.2.2.3. Bedeutung von absolutem Geheimnisträgerschutz in § 160a Abs 1 dStPO	119
15.2.2.4. Verhältnis zu anderen strafprozessualen Vorschriften in Deutschland	120
15.3. Bewertung	121
15.4. Umsetzung im Polizeirecht	121
16. Die Entscheidung des EuGH zur Vorratsdatenspeicherung	122
17. Die Entscheidung des VfGH zur Vorratsdatenspeicherung	124
18. Die Bedeutung „überwachungsfreier Räume“ in der Rechtsprechung des Bundesverfassungsgerichtes	126
18.1. Relevanz des „Kernbereiches privater Lebensgestaltung“	126
18.1.1. Überschneidungen des Kernbereichs privater Lebensgestaltung mit dem Schutz der Berufsgeheimnisse	128
18.1.2. Parallelen des Kernbereichs privater Lebensgestaltung mit dem Schutz der Berufsgeheimnisse	128
18.2. Notwendigkeit von „überwachungsfreien Räumen“ für Berufsgeheimnisträger	129

19. Ergebnisse.....	132
Kapitel IV – Rechtsvergleichende Aspekte.....	133
20. Interpretation des Schutzbereiches des Fernmeldegeheimnisses.....	134
20.1. Rechtsvergleich des Fernmeldegeheimnisses in Österreich und in Deutschland	136
20.1.1. Inhalte der Telekommunikation während eines laufenden Telekommunikationsvorgangs	136
20.1.2. Inhalte der Telekommunikation nach einem abgeschlossenen Telekommunikationsvorgang	137
20.1.3. Verbindungsdaten während eines Telekommunikationsvorgangs	139
20.1.3.1. Fernmeldegeheimnis in Deutschland betroffen	139
20.1.3.2. Das Fernmeldegeheimnis in der österreichischen Staatsrechtslehre	142
20.1.3.3. Verfassungsvergleichende Aspekte	143
20.1.3.3.1. Einbeziehung von Verkehrsdaten in das Fernmeldegeheimnis	143
20.1.3.3.2. Vorbehalt des richterlichen Befehls für Eingriffe in das Fernmeldegeheimnis?	145
20.1.4. Verbindungsdaten außerhalb eines Telekommunikationsvorgangs	147
20.2. Zwischenergebnis	147
20.3. Folgen der verfassungsrechtlichen Folgerung für die Überwachung der Telekommunikation im Bereich der Gefahrenabwehr und der Strafverfolgung	148
21. Die Rolle der „Menschenwürde“ in der österreichischen Verfassungsrechtsordnung	149
21.1. Übertragbarkeit auf Österreich	149
21.1.1. Grundrechtecharta und europarechtliches Äquivalenzprinzip	150
21.1.2. Einschränkung des Grundrechtsschutzes durch Art 51 GRC	154
21.1.2.1. Art 51 GRC und seine Interpretation durch den VfGH	155
21.1.2.2. Weitere Anwendungsbereiche von Art 51 Abs 1 GRC im Bereich der Grundfreiheiten der Europäischen Union	156

21.1.2.3. Weitere Anwendungsbereiche von Art 51 Abs 1 GRC von der "Fransson"-Entscheidung des EuGH zur „neuen Formel“	156
21.1.2.3.1. Anwendbarkeit der GRC bei auch nur indirektem Bezug	157
21.1.2.3.2. Anwendbarkeit der GRC bei Telekommunikationsüberwachung	160
21.1.2.4. Grundsätzliche Anwendbarkeit der GRC im Bereich der Überwachung der Telekommunikation	162
21.1.3. Neue Bewertung des Begriffs der Menschenwürde im österreichischen Verfassungsrecht.....	163
21.2. Fazit	165
22. Das Grundrecht auf informationelle Selbstbestimmung in der österreichischen Verfassungsrechtsordnung.....	166
22.1. Verwendung durch den VfGH und der Unterschied zum Grundrecht auf Datenschutz	166
22.2. § 1 DSG 2000, Art 8 EMRK, Art 1 und 8 GRC als Rechtsquellen des „Grundrechts auf informationelle Selbstbestimmung“	168
23. Ergebnisse.....	169
Kapitel V – Bedeutung von Kontrollinstanzen im Rahmen von Überwachungsmaßnahmen. Ist der Richtervorbehalt in der heutigen Form zeitgemäß?.....	171
24. Der Richtervorbehalt als Kontrollinstanz	171
25. Die Kontrolle durch den Rechtsschutzbeauftragten	174
26. Reformbedarf bei Kontrollinstanzen	175
26.1. Kritikpunkte am Richtervorbehalt	175
26.2. Kritikpunkte an der Funktion des Rechtsschutzbeauftragten	178
26.3. Lösungsmöglichkeiten	179
27. Ergebnisse.....	182

Kapitel VI – Aktuelle Entwicklungen im Hinblick auf Berufsgeheimnisträger und im Bereich der Telekommunikationsüberwachung in Österreich und Deutschland 184

28. Aktuelle Entwicklungen 185

28.1. Polizeiliches Staatsschutzgesetz (PStSG) - Österreich.....	185
28.1.1. Inhalte des PStSG.....	188
28.1.1.1. Zielsetzung des PStSG	188
28.1.1.2. Datenerhebung im Bereich der Telekommunikation	189
28.1.2. Umsetzung des Berufsgeheimnisträgerschutzes im PStSG	189
28.1.3. Weitere Kritikpunkte aus dem Bereich der Telekommunikationsüberwachung im PStSG.....	192
28.1.4. Reaktion des Gesetzgebers auf die vorgebrachten Kritikpunkte	192
28.1.4.1. Die erste Überarbeitung des Gesetzesentwurfs.....	193
28.1.4.2. Die zweite Überarbeitung des Gesetzesentwurfs	193
28.1.4.3. Die dritte Überarbeitung des Gesetzesentwurfs	194
28.2. „Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden“ – Österreich	195
28.3. „Vorratsdatenspeicherung neu“ in Deutschland	197
28.3.1. Zielsetzung der „Vorratsdatenspeicherung neu“	198
28.3.2. Datenerhebung im Bereich der Telekommunikation	199
28.3.3. Umsetzung des Berufsgeheimnisträgerschutzes bei der „Vorratsdatenspeicherung neu“	200
28.3.4. Bewertung nach der Entscheidung des EuGH	202
28.3.5. Erste gerichtliche Entscheidung	203
28.4. BKA-Gesetz - Deutschland	206
28.4.1. Vergleichbarkeit von Kernbereichsschutz und Berufsgeheimnisträgerschutz 206	
28.4.2. Die Bedeutung einer „unabhängigen Vorabkontrolle“	207
28.4.3. Kernbereichsrelevante Eingriffe außerhalb des Wohnraums.....	209
28.5. Arbeitsprogramm der Bundesregierung 2017/2018 – Österreich.....	209
28.5.1. „Quick-Freeze“-Verfahren	210

28.5.2. Überwachung verschlüsselter Kommunikation und IMSI-Catcher in der StPO	211
28.6. Überwachungspaket neu - Deutschland.....	212
29. Ergebnisse.....	214
Kapitel VII – Zusammenfassung und Schlussbetrachtung.....	216
30. Zusammenfassung der wichtigsten Ergebnisse	216
31. Lösungsvorschläge und Ausblick	219
Literaturverzeichnis.....	225
Monographien	225
Kommentare	227
Aufsätze.....	229
Veröffentlichungen im Internet.....	236
Liste verwendeter Judikatur	240
Österreich	240
Verfassungsgerichtshof.....	240
Ordentliche Gerichte	240
Verwaltungsgerichtshof	240
Deutschland	240
Bundesverfassungsgericht	240
Landesverfassungsgerichte	241
Ordentliche Gerichte.....	241
Verwaltungsgerichte	242
Europäischer Gerichtshof.....	242
Europäischer Gerichtshof für Menschenrechte.....	242
Abkürzungsverzeichnis.....	244

Zusammenfassung.....	246
Abstract	248
Lebenslauf	250

Danksagung

Zunächst möchte ich mich bei meinem Betreuer ao. Univ.-Prof. Dr. Hannes Tretter herzlich für die Betreuung dieser Arbeit bedanken. Seine Anregungen und seine Kritik haben meine Arbeit entscheidend weitergebracht und bereichert. Die Zeit, die ich als Referendar am Boltzmann-Institut für Menschenrechte verbringen konnte, hat meine Begeisterung für viele Themengebiete, die in dieser Arbeit behandelt wurden erst geweckt.

Mein Dank gilt auch Ing. Mag. Dr. Christof Tschohl für seine wertvollen Anregungen. Ebenfalls bedanken möchte ich mich bei RAA Mag. Katharina Windisch und bei meiner Partnerin Mag. Klara Haimberger. Ihr ist diese Arbeit auch gewidmet.

1. Einleitung

Was ich bei der Behandlung oder auch außerhalb meiner Praxis im Umgange mit Menschen sehe und höre, das man nicht weiterreden darf, werde ich verschweigen und als Geheimnis bewahren.

Aus dem Eid des Hippokrates¹

Berufsgeheimnisse hat es von alters her gegeben. Viele Berufe, die besondere Vertrauensverhältnisse erfordern, sind ohne sie undenkbar. Das Beispiel des hippokratischen Eides, welches hier exemplarisch vorangestellt wird, zeigt, dass die Schweigepflicht des Arztes so alt ist, wie die moderne Medizin selbst.

Dies bedeutet jedoch nicht, dass Berufsgeheimnisse, so alt sie auch sein mögen, nicht mit jeder Epoche neuen Veränderungen unterworfen sind. Mit einem Wandel der Berufsbilder, auch durch den Einsatz neuer Informationstechnologie, entwickeln sich auch die Berufsgeheimnisse weiter. Moderne Kommunikationstechnologie ist dabei nicht nur aus dem Blickwinkel zu sehen, dass sie dem Berufsgeheimnisträger neue und bessere Kommunikationsformen erschließen. Jede neue Form der Kommunikation ist auch staatlicherseits neuen, modernen Formen der Telekommunikationsüberwachung ausgesetzt.

Waren es früher die Wohn- bzw. Büroraumüberwachung und das Abhören von Telefonen, die Ermittler und Berufsgeheimnisträger vor Probleme stellten, so sind heutzutage viel tiefgreifendere Grundrechtseingriffe möglich. Schließlich lassen sich, wenn Ermittler Zugriff auf bestimmte Daten erhalten, in vielen Fällen weitaus umfangreichere Informationen über eine bestimmte Person gewinnen. Überwachung ist heutzutage allgegenwärtig und selbst als Bürger, der nicht mit dem Gesetz in Konflikt geraten ist, kann man leicht in das Visier von Ermittlungen im Bereich der Telekommunikation

¹ Zitiert nach *Schubert*, Der hippokratische Eid, 15. Die erste textliche Überlieferung findet sich jedoch erst im 1. Jhdt n Chr bei *Erotian*.

geraten, zumal diese oft nicht einmal einen bestimmten Anlass haben. Was für jeden einzelnen Grundrechtsträger gilt und schon in diesem Bereich problematisch ist, bekommt bei Berufsgeheimnisträgern eine zusätzliche Relevanz. Schließlich vertraut jeder Bürger darauf, dass er sich an diese wenden kann, ohne dass Dritte von der Kontaktaufnahme, geschweige denn vom Grund der Kontaktaufnahme oder gar vom Inhalt des Gespräches erfahren.

Die zunehmende Bedeutung von elektronischer Datenverarbeitung, auch durch Berufsgeheimnisträger, stellt beide Seiten – sowohl die Berufsgeheimnisträger als auch Strafverfolger – vor neuartige Herausforderungen.² Die Abwägung zwischen den Grundrechten der Betroffenen und dem Interesse der Öffentlichkeit an der Strafverfolgung fällt in ein besonders sensibles verfassungsrechtliches Spannungsfeld.

Hierbei ist, bevor auf das verfassungsrechtliche Spannungsfeld und die technischen Methoden eingegangen werden kann, zunächst wichtig, inwiefern sich die einzelnen Berufsgeheimnisträger voneinander unterscheiden.

Ein Rechtsvergleich zwischen Österreich und Deutschland ist dabei insofern förderlich, als beide Rechtsordnungen grundlegende Gemeinsamkeiten aufweisen, sich aber auch in vielen Punkten unterscheiden. Ein systematischer Vergleich zwischen beiden Rechtsordnungen kann zudem im Rahmen der Interpretation von Verfassungsnormen hilfreich sein. Ergänzt wird dies durch eine Einbeziehung der Judikatur des EuGH und des EGMR, die letztlich in beide Rechtsordnungen wieder hinein wirkt.

Ziel dieser wissenschaftlichen Arbeit ist es, rechtliche Leitlinien für die Ermittlungen bei Berufsgeheimnisträgern herauszuarbeiten. Beweiserhebungs- und Beweisverwertungsverbote werden hierbei eine zentrale Rolle spielen. Letztlich wird es hierbei auch eine Rolle spielen, inwiefern sich die Erkenntnisse der Rechte der Berufsgeheimnisträger nicht auch auf andere Berufsträger oder Privatpersonen übertragen lässt.

² Vgl zu dieser Thematik *Kutzner*, Die Beschlagnahme von Daten bei Berufsgeheimnisträgern, NJW 2005, 2652.

Kapitel I – Die Gruppe der Berufsgeheimnisträger

Wer sich mit Berufsgeheimnissen rechtlich auseinandersetzen will, muss zunächst die Gruppe der Berufsgeheimnisträger umreißen. Erst wenn diese von anderen Berufen abgegrenzt sind, kann man anhand der Gruppe über andere rechtliche Fragestellungen diskutieren. Dies lässt sich am besten dadurch bewerkstelligen, dass man Berufsrecht, (Straf-)prozessrecht und gegebenenfalls weitere Regelungen untersucht. Eine verfassungsrechtliche Verankerung einzelner Berufsgeheimnisträger gibt es in direkter Form nicht.

Wie Berufsgeheimnisse letztlich ausgestaltet sind, zeigt deren einfachgesetzlicher Schutz, den es aus verfassungsrechtlicher Perspektive zu beleuchten gilt. Einen direkten Berufsgeheimnisträgerschutz unmittelbar aus dem Verfassungsrecht heraus gibt es nicht, zumindest nicht in der Form, dass sich aus dem Verfassungsrecht ein Schutz für eine bestimmte Berufsgruppe unmittelbar ableiten lässt.³ Daher ist zunächst auf die einfachgesetzlichen Grundlagen des Berufsgeheimnisträgerschutzes einzugehen, bevor man sich den verfassungsrechtlichen Bezugspunkte des Berufsgeheimnisträgerschutzes zuwendet.

2. Einfachgesetzlicher Schutz von Berufsgeheimnissen

Schon beim einfachgesetzlichen Berufsgeheimnisträgerschutz treten viele Unterschiede zutage, die größtenteils historisch bedingt sind. Hierbei ergeben sich auf den ersten Blick nur marginale Unterschiede zwischen Deutschland und Österreich, die aber je nach Berufsgeheimnisträger auch größere Auswirkungen haben können.

Zunächst wird man abgrenzen müssen, was man unter einem Berufsgeheimnis versteht. Gemeinsam ist allen Berufsgeheimnissen, dass den jeweiligen Berufen ein besonderes Vertrauensverhältnis zugrunde liegt. Bei einigen Berufen mag sich dies

³ Nichtsdestotrotz implizieren verschiedene Grundrechte den Schutz von Berufsgeheimnissen, mehr hierzu unter 3.

förmlich aufdrängen, bei einigen mag man diskutieren, ob ein besonderes Vertrauensverhältnis vorliegt. Während es bei Ärzten selbstverständlich ist, sind Steuerberater zwar auch als Berufsgeheimnisträger anerkannt, genießen aber nicht den gleichen Schutz wie beispielsweise Strafverteidiger, obgleich ihre Tätigkeit auch strafrechtliche Aspekte betreffen kann.⁴ Unterschiede rühren hier von den unterschiedlichen Grundrechten her, die betroffen sind.

Der Schutz der Berufsgeheimnisträger spielt sich auf verschiedenen Ebenen ab, die alle verfassungsrechtliche Rückbezüge haben. Zum einen existiert das Berufsrecht, welches die beruflichen Rechte und Pflichten des Geheimnisträgers regelt und bereits Vorschriften zu Vertrauensverhältnissen und zur Geheimhaltung enthält. Zum anderen schützt das Strafrecht teilweise die Pflicht zur Geheimhaltung. Die wichtigste und mit Rückbindung an das Verfassungsrecht sensibelste Ebene ist dabei der Schutz von Berufsgeheimnissen im Rahmen strafprozessualer Ermittlungen. Betreffen die ersten beiden Ebenen, also jene des Berufsrechts und jene des Strafrechts, die Fälle, in denen der Berufsgeheimnisträger von sich aus ein Geheimnis offenbart, so wird im Falle von strafrechtlichen Ermittlungen ein Berufsgeheimnis in der Regel entgegen dem Willen desjenigen, um dessen Tatsachen es geht, und entgegen dem Willen des Berufsgeheimnisträgers den Ermittlern bekannt werden. In diesem Fall haben weder der Geheimnisträger noch der Betroffene eine Möglichkeit die Kenntnisnahme Dritter zu verhindern, was sich für das Vertrauensverhältnis als besonders problematisch darstellt.

Abzugrenzen ist das Berufsgeheimnis auch vom Amtsgeheimnis. Während das Berufsgeheimnis einen berufsspezifischen Bezug aufweist, der Grund für die Geheimhaltung also die Ausübung eines Berufes ist, der ein besonderes Vertrauensverhältnis zwischen dem Hilfesuchenden oder Kunden und dem Berufsgeheimnisträger erfordert, ist die Schutzrichtung beim Amtsgeheimnis eine andere. Hier wird nicht der Beruf etwa des Finanzbeamten oder Polizisten selbst geschützt, sondern die Tatsache, dass etwa eine Zeugenvernehmung im Strafprozess eine Angelegenheit des Staates ist und somit

⁴ Vgl. zum unterschiedlichen Schutzniveau in Deutschland kritisch *Ende*, Verstärkter Schutz von Berufsgeheimnisträgern – auch für Steuerberater!, DStR 2009, 2556.

dieser auch entscheiden kann, ob ihm amtsbekannte Sachen Teil dieses Prozesses sind.⁵ Im Gegensatz zum Berufsgeheimnisträger, der über sein eigenes Berufsgeheimnis nicht disponieren darf, entscheidet hier gerade eine weitere Stelle, nämlich die vorgesetzte Behörde (in Österreich)⁶ bzw der Dienstherr (in Deutschland).⁷

2.1. Berufsrechtlicher Schutz in Österreich

Das Berufsrecht gibt verschiedene Vorgaben für den Schutz von Berufsgeheimnissen. Je nach Beruf finden sich mehr oder weniger explizite Verschwiegenheitsverpflichtungen. Nachfolgend sollen die wichtigsten Regelungen für die wichtigsten Berufsgruppen in Österreich und Deutschland kurz erläutert werden.

2.1.1. Heilberufe

Das ärztliche Berufsgeheimnis ist – wie eingangs bereits angeklungen – historisch gewachsen und sehr weitreichend. Berufsrechtlich verpflichtet § 54 Abs 1 ÄrzteG Ärzte zur Verschwiegenheit. Daneben existieren noch Verschwiegenheitspflichten für Psychotherapeuten, klinische Psychologen und Gesundheitspsychologen, sowie weitere Berufe medizinischer Prägung, die an das ärztliche Berufsgeheimnis angelehnt sind.

Die in § 54 ÄrzteG geregelte Verschwiegenheitspflicht ist umfassend; sie erstreckt sich auch auf nahe Angehörigen, Arztkollegen, staatlichen Dienststellen, etc.⁸ Im Rahmen des „Arztgeheimnisses“ geht es um sämtliche für den Patienten relevante Daten. Dazu zählt nicht nur die Erkrankung oder die Diagnose, sondern in vielen Fällen auch schon allein die Tatsache, dass sich jemand überhaupt in ärztlicher Behandlung befindet.⁹ Eine nur scheinbare Einschränkung erfährt hier das Berufsgeheimnis insoweit, dass der Arzt von dem Geheimnis auch in Ausübung seines Berufes erfahren muss; dieses Merkmal ist sozusagen zugunsten des Patienten weit auszulegen, so dass

⁵ *Leitner*, Vernehmungsverbote im österreichischen Strafprozessrecht, 66.

⁶ Vgl zum Prozedere ausführlich *Leitner*, Vernehmungsverbote im österreichischen Strafprozessrecht, 85.

⁷ Dienstherr im Sinne des BeamStG ist das Land, der Bund, die Gemeinde oder sonstige öffentliche Körperschaft in deren Dienstverhältnis der Beamte nach § 2 BeamStG steht. Die Verschwiegenheitspflicht regelt § 37 Abs 3 BeamStG.

⁸ Details vgl *Stolzlechner*, Überlegungen zur ärztlichen Verschwiegenheits-, Anzeige- und Meldepflicht, RdM 200, 67.

⁹ Dies ist immer dann gegeben, wenn die Behandlung einen besonders intimen und sensiblen Bereich umfasst, wie z B Urologie, Gynäkologie, vgl *Kletečka-Pulker* in *Aigner/Kletečka/Kletečka-Pulker/Memmer*, Handbuch Medizinrecht für die Praxis¹⁸, Kap I.6.9.2.2.

auch eine Äußerung des Patienten dem Arzt gegenüber, die sich außerhalb seiner Ordination abspielt, geheim zu halten ist.¹⁰

Zudem sind besonders strenge Merkmale beim Merkmal der Geheimnisoffenbarung anzulegen: Ein Geheimnis ist darüber hinaus nämlich auch dann bereits offenbart, wenn der Arzt zwar keine direkte Auskunft über den Patienten erteilt, dieser sich aber aufgrund der vom Mediziner verratenen Merkmale (z B seltener Vorname) identifizieren lässt.¹¹

Das ärztliche Berufsgeheimnis, wie es in § 54 Abs 1 ÄrzteG niedergelegt ist, existiert in ähnlicher Form auch für Psychotherapeuten und klinische Psychologen in § 15 PThG und § 14 PG. Es entspricht in wesentlichen Zügen dem Berufsgeheimnis der Ärzte. Es wird hierbei auf den gleichen Geheimnisbegriff abgestellt.¹² Das Berufsgeheimnis im psychologischen und psychotherapeutischen Bereich unterscheidet sich aber vom Arztgeheimnis darin, dass er, aufgrund der besonderen Sensibilität der Informationen noch weitreichender auszulegen ist.¹³

Dies zeigt sich auch daran, dass eine Sonderregelung für einsichtsfähige Minderjährige besteht, die ca. das 14. Lebensjahr vollendet haben: Deren genaue Gesprächsinhalte sind selbst für die Erziehungsberechtigten tabu; der Therapeut oder Psychologe hat lediglich über deren Behandlung und die Therapie Auskunft zu geben hat.¹⁴

Ähnliche Regelungen existieren für weitere medizinische Heilberufe und entsprechende Hilfsberufe. Exemplarisch seien hier Sanitäter (§ 6 SanG), Hebammen (§ 7 HebG) und Zahnärzte (§ 21 ZÄG) genannt.

¹⁰ Also etwa auch dann, wenn Arzt und Patient im Privatleben zufällig aufeinander treffen und der Patient dem Arzt bei dieser Gelegenheit etwas über seinen Gesundheitszustand berichtet, vgl *Kletečka-Pulker* in Aigner/Kletečka/Kletečka-Pulker/Memmer, Handbuch Medizinrecht für die Praxis¹⁸, Kap I.6.9.2.3.

¹¹ *Kletečka-Pulker* in Aigner/Kletečka/Kletečka-Pulker/Memmer¹⁸, Handbuch Medizinrecht für die Praxis, Kap I.6.10.11.

¹² Hierbei fällt die Tatsache, dass überhaupt sich ein Patient überhaupt in Behandlung befindet stets unter den Geheimnisschutz, *Kletečka-Pulker* in Aigner/Kletečka/Kletečka-Pulker/Memmer, Handbuch Medizinrecht für die Praxis¹⁸, Kap I.6.9.2.2.

¹³ *Schmoller*, Zur Reichweite der Verschwiegenheitspflicht von Ärzten, Psychologen und Psychotherapeuten RdM 1996, 131.

¹⁴ *Windisch-Graetz* in Aigner/Kletečka/Kletečka-Pulker/Memmer, Handbuch Medizinrecht für die Praxis¹⁸, Kap III.3.4.3.3.

2.1.2. Geistliche und Seelsorger

Berufsgeheimnisse existieren ebenfalls in der Seelsorge, wobei das Beichtgeheimnis hervorzuheben ist. Es genießt besonderen Schutz und ist seit dem Mittelalter im Kirchenrecht verankert.¹⁵ Ihm kommt damit auch eine rechtshistorisch bedeutende Komponente zu, da es sich um ein kodifiziertes Berufsgeheimnis handelt, das schon über einen langen Zeitraum besteht und welches weitere Berufsgeheimnisse zweifelsohne beeinflusst hat und für deren Etablierung ein wichtiges Vorbild war.

Wie auch das Berufsgeheimnis für medizinische Heilberufe besteht ein Geheimnisschutz für Zeugenaussagen nach Verwaltungsverfahrens- und Zivilprozessrecht ebenso im Bereich der Seelsorge. Dennoch unterliegt dieses Berufsgeheimnis einigen Besonderheiten, die vorliegend erläutert werden sollen.

Für die römisch-katholische Kirche, die hier exemplarisch behandelt werden soll,¹⁶ geht die Beichte nicht nur auf eine direkte biblische Grundlage zurück;¹⁷ auch erfährt das Beichtgeheimnis durch kirchenrechtliche Bestimmungen im CIC eine herausragende Stellung: Nach Can. 983 CIC ist dieses absolut geschützt.¹⁸ Verstöße hiergegen sanktioniert das Kirchenrecht. Verletzt ein Priester das Beichtgeheimnis durch eine Offenbarung der Inhalte des Beichtgespräches mit einem Gläubigen in direkter Weise, so trifft ihn kirchenrechtlich die Strafe der Exkommunikation (vgl. Can. 1388 § 1 CIC), also den Ausschluss aus der kirchlichen Gemeinschaft.¹⁹ Dies bedeutet,

¹⁵ Canon 21, Beschluss des IV. Laterankonzils der römisch-katholischen Kirche aus dem Jahr 1215, abrufbar unter http://www.intratext.com/IXT/ENG0431/_PL.HTM#2D.

¹⁶ Vgl. zum „Beichtgeheimnis“ in Bezug auf andere (christliche) Religionsgemeinschaften *Krömer*, öarr 2010, 198, 218.

¹⁷ Die kirchliche Lehre bezieht sich hierbei auf die Jesus-Worte in *Joh 23,20*, die den Jüngern bei einer Erscheinung nach der Auferstehung im Rahmen einer Aussendung („Wie mich der Vater gesandt hat, so sende ich Euch.“) kundgetan wurden: „Wem ihr die Sünden vergebt, dem sind sie vergeben; wem ihr die Vergebung verweigert, dem ist sie verweigert.“ Die Kirche sieht damit das Beichtsakrament als einen direkten göttlichen Auftrag an. Vgl. hierzu und zur historischen Entwicklung des Beichtgeheimnisses *Schmoeckel* in Witte/Alexander, *Christianity and Law*, 157 f.

¹⁸ Vgl. auch zur historischen Entwicklung des Beichtgeheimnisses *Fischedick*, Das Beicht- und Seelsorgegeheimnis, Zur Legitimation und Reichweite der Zeugnisverweigerungsrechte für Geistliche, DÖV 2008, 584, 584 f.

¹⁹ Diese Strafe kann auch sonstige Personen, wie etwa Dolmetscher, treffen, die an dem Beichtvorgang beteiligt waren, vgl. Can. 1388, § 2 CIC. Vgl. hierzu näher *Leitner*, Vernehmungsverbote, 49; die Exkommunikation geht einher mit dem Verbot Sakramente zu empfangen oder kirchliche Ämter auszuüben.

dass der Exkommunizierte selbst keine Sakramente (wie etwa die Eucharistie, kirchliche Eheschließung oder Krankensalbung) empfangen und keine kirchlichen Ämter ausüben darf; die Mitgliedschaft in der Kirche bleibt gleichwohl aufrecht und kann aus kirchenrechtlicher Sicht ohnehin nicht zurückgenommen werden.²⁰

Die kirchenrechtlichen Vorschriften erlangen durch völkerrechtliche Bestimmungen auch im staatlichen Bereich eine hohe Bedeutung. So hat sich Österreich durch ein Konkordat mit dem Heiligen Stuhl vom 5. Juni 1933 zum Schutz des Beichtgeheimnisses im staatlichen Recht verpflichtet.²¹ Dies überträgt den absoluten Status, den das Kirchenrecht der Regelung zuweist, über das Völkerrecht in die österreichische Rechtsordnung hinein. Dieser Schutz erlangt für alle Religionsgemeinschaften aufgrund des Gleichbehandlungsgrundsatzes eine große Bedeutung, so dass von diesem weitgehenden Schutz alle Religionsgemeinschaften gleichsam profitieren, da ihnen ein ebensolches Schutzniveau einzuräumen ist, wie der römisch-katholischen Kirche.

2.1.3. Rechtsberatung

Österreichs Rechtsanwaltschaft kann auf eine lange berufsrechtliche Tradition zurückblicken. Das Berufsrecht der Anwälte regelt hierbei die RAO, welche bereits 1868 erlassen wurde.²² Auch das Anwaltsgeheimnis ist in Österreich berufsrechtlich hierbei durch die Vorschrift des § 9 Abs 2 S 1 RAO normiert und geschützt, welche als Recht und Pflicht des Rechtsanwalts zugleich verstanden werden kann.²³ Zwar wurde das Anwaltsgeheimnis den Erfordernissen der heutigen Zeit angepasst,²⁴ ist aber ansonsten dem Grunde nach nicht verändert worden.²⁵ Die erste Fassung der RAO enthielt jedoch noch keine Normierung eines Umgehungsverbotes durch Beschlagnahme von Unterlagen oder Befragung von Kanzleipersonal, bei dem es sich nicht um Rechtsanwälte handelt. Diese findet sich heute in § 9 Abs 3 RAO. Zudem enthielt die Ursprungsfas-

²⁰ Vgl näher hierzu *Krause/Müller*, TRE, Band V, 171.

²¹ Vgl BGBl II, 2/1934.

²² Die damalige Bezeichnung lautete „Advocatenordnung“, RGBI Nr. 96/1868, 274 ff; ihren heutigen Namen erhielt die RAO 1919, StGBI. Nr. 95/1919, 165.

²³ *Harbich*, Einige Fragen der anwaltlichen Verschwiegenheit, AnwBl 1983, 671

²⁴ So wurde etwa dem Umstand Rechnung getragen, dass Kanzleien nunmehr auch in der Rechtsform einer GmbH auftreten.

²⁵ RGBI Nr. 96/1868.

sung von § 9 Abs 2 RAO in Satz 2 einen straf- und zivilprozessualen Vorbehalt. Insofern ist das Berufsgeheimnis der Rechtsanwaltschaft im Berufsrecht erheblich aufgewertet worden.

Gleiches gilt für die anderen in § 157 Abs 1 Z 2 StPO erwähnten Berufe, beispielsweise für Notare (vgl § 37 Abs 1 NO), für die es ebenfalls berufsrechtliche Pflichten zur Geheimhaltung gibt.

2.1.4. Medienmitarbeiter

Unabhängige Medien können nur dann existieren, wenn Mitteilungen von Informanten an die Medienmitarbeiter in gewisser Weise als vertraulich betrachtet werden können. Andernfalls entfällt für diese eine wichtige Säule für die Informationsbeschaffung, die eine Recherche in umfassender Weise nahezu unmöglich macht.

Jedoch wirft der Begriff des Medienmitarbeiters, wie er im Gesetz geregelt ist, bereits Fragen auf, was auch darauf zurückzuführen ist, dass sich der Begriff des Medienmitarbeiters nicht so leicht eingrenzen lässt, wie etwa der des Geistlichen oder der des Arztes.

Der Begriff des Medienmitarbeiters ist in § 1 Abs 1 Z 11 MedienG definiert. Dieser lässt jedoch Spielraum für Interpretationen. So lehnt es beispielsweise die Rechtsprechung ab, freie Journalisten zu den Medienmitarbeitern zu zählen, was in der Literatur teilweise zu Recht auf Ablehnung stößt.²⁶ Schließlich ist die journalistische Tätigkeit von freien Mitarbeitern nicht weniger unprofessionell. Inwiefern jemand vom Schutz des Mediengesetzes profitiert, kann nicht von der Art des Beschäftigungsverhältnisses abhängen.

Ein direktes berufsrechtlich verfasstes Berufsgeheimnis für Medienmitarbeiter existiert in Österreich nicht und lässt sich auch aus dem Ehrenkodex des Österreichischen Presserates²⁷ nur indirekt herauslesen. Allerdings regelt das Mediengesetz einen

²⁶ Vgl hierzu *Wittmann/Zöchbauer* in Röggl/Wittmann/Zöchbauer, MedienG PK, § 1 MedienG, Rz 26; *Litzka/Strebing*, Mediengesetz Kurzkommentar⁵, § 31, Rz 1.

²⁷ Vgl hierzu den Ehrenkodex des österreichischen Presserates http://www.presserat.at/rte/upload/pdfs/grundsaeetze_fuer_die_publizistische_arbeit_ehrenkodex_fuer_die_oesterreichische_presse_idf_vom_14.11.2012.pdf.

umfassenden Berufsgeheimnisträgerschutz, welcher sich im Strafprozessrecht und auch in anderen Gesetzen auswirkt.²⁸

2.2. Berufsrechtlicher Schutz in Deutschland

Der berufsrechtliche Schutz, den Berufsgeheimnisträger in Deutschland erfahren, ist mit dem in Österreich gut vergleichbar und unterscheidet sich von diesem nur in Nuancen.

2.2.1. Heilberufe

Das Berufsgeheimnis der Ärzte findet auch in Deutschland seine Verankerung im Berufsrecht. Aufgrund des besonders stark ausgeprägten Föderalismus existiert in jedem Bundesland eine eigene Berufsordnung für Ärzte, die dieses Berufsgeheimnis für die im jeweiligen Bundesland niedergelassenen Ärzte näher regelt. Die Berufsordnungen der Bundesländer gehen jedoch im Wesentlichen auf eine gemeinsame Vorlage, die Musterberufsordnung für Ärzte (MBO), zurück, auf die hier der Einfachheit und Übersichtlichkeit halber Bezug genommen werden soll. Dort ist das ärztliche Berufsgeheimnis in § 9 Abs 1 S 1 MBO geregelt: *Ärztinnen und Ärzte haben über das, was ihnen in ihrer Eigenschaft als Ärztin oder Arzt anvertraut oder bekannt geworden ist – auch über den Tod der Patientin oder des Patienten hinaus – zu schweigen.*

Dabei schützt das Berufsrecht alles, was über den Patienten nicht allgemein bekannt ist.²⁹ Der Arzt muss hierbei – wie in Österreich – nicht direkt im Rahmen einer Behandlung davon erfahren.³⁰ Es kommt nur darauf an, dass er dies in seiner Eigenschaft als Arzt erfährt.³¹ § 9 Abs 1 S 2 MBO stellt klar, dass auch schriftliche Aufzeichnungen vom Patienten an den Arzt davon umfasst sind.

2.2.2. Geistliche und Seelsorger

Das Kirchenrecht in seiner heutigen Form wurde von Papst Johannes Paul II. im Jahr 1983 erlassen und gilt für die römisch-katholische Kirche weltweit, so dass die für

²⁸ Vgl 2.3.4.

²⁹ Scholz in Spickhoff, Medizinrecht, § 9 MBO, Rz 2 mit Verweis auf Ärztliches Berufsgericht Nds. GesR 2006, 37, 38.

³⁰ So ist es auch ausreichend, wenn ihm der Patient bei Gelegenheit etwas über seinen Zustand berichtet.

³¹ Scholz in Spickhoff, Medizinrecht, § 9 MBO, Rz 2.

Österreich festgehaltenen Grundsätze aus dem CIC zur Gänze auf Deutschland übertragen werden können.

Ebenfalls ähnlich ist die völkerrechtliche Transferierung der Regelungen in das nationale Recht. Für das zwischen Österreich und dem Heiligen Stuhl bestehende Konkordat gibt es eine Entsprechung im Konkordat zwischen dem Hl. Stuhl und dem Deutschen Reich,³² welches Bund und Länder in Deutschland völkerrechtlich bindet und damit ebenfalls eine völkerrechtliche Garantie dieser kirchenrechtlichen Regelung beinhaltet.

2.2.3. **Rechtsberatung**

Die BRAO regelt in Deutschland das Berufsrecht der Rechtsanwälte. Die darin enthaltenen Regelungen sind nicht besonders detailreich; einzelne Berufspflichten kommen darin kaum vor.³³ Zentrale berufsrechtliche Regelung war hierbei jahrelang § 43 BRAO, der eine allgemeine Berufspflicht enthält, welche eine gewissenhafte Berufsausübung vom Rechtsanwalt verlangt.

Aufgrund dieser in Bezug auf die einzelnen Pflichten des Rechtsanwalts eher nichtssagenden Vorschrift,³⁴ wurde der Deutsche Anwaltsverein schon im Jahre 1929 selbst aktiv und erließ die *Grundsätze des anwaltlichen Standesrechts* (RichtlRA), welche unter anderem auch Verschwiegenheitspflichten enthielten,³⁵ die das BVerfG jedoch für rechtlich unverbindlich erklärte.³⁶

Als Reaktion auf diese verfassungsgerichtliche Einschätzung wurden die Grundpflichten des Rechtsanwalts in der BRAO novelliert³⁷ und § 43a BRAO eingefügt, welcher in § 43a Abs 2 BRAO die Verschwiegenheitspflicht für alle berufsmäßig

³² dRGBI II 1933, 679; dort Art 9.

³³ Henssler, Das anwaltliche Berufsgeheimnis, NJW 1994, 1817, 1818.

³⁴ Auch die Vorgängerregelungen waren gleich oder ähnlich gefasst. Mit der Novellierung der BRAO im Jahre 1994 hat sich damit die Regelung inhaltlich nicht geändert.

³⁵ Wild, Verschwiegenheitspflicht, 33.

³⁶ BVerfGE 76, 171 = NJW 1988, 191 = JZ 1988, 242.

³⁷ Vgl dBGBI I, 1994, 2278.

bekannt gewordenen Tatsachen enthält, welche nicht ohnehin offenkundig sind.³⁸ Hierbei handelt es sich um Recht und Pflicht zugleich. Somit findet sich auch eine berufsrechtliche Normierung der anwaltlichen Verschwiegenheit, welche Rechtsverbindlichkeit genießt.³⁹

2.2.4. Medienmitarbeiter

Ähnlich wie in Österreich fehlt es an einem direkten gesetzlich normierten Berufsgeheimnis im Berufsrecht. Die Landespressegesetze enthalten hierzu keine oder nur andeutungsweise Regelungen.

Der Pressekodex des Deutschen Presserates⁴⁰ enthält in Ziffer 5 das Berufsgeheimnis der Medienmitarbeiter und verweist auf das gesetzlich gewährleistete Berufsgeheimnis, welches die Presse im Interesse ihrer Informanten grundsätzlich zu wahren habe.

2.3. Strafprozessualer Schutz in Österreich

Zentral für den Berufsgeheimnisträgerschutz ist dessen strafprozessuale Komponente, da dieser für das Vertrauensverhältnis zwischen Berufsgeheimnisträger und Patient, Ratsuchenden, Mandant oder Informant elementar ist. An der Ausgestaltung des strafprozessualen Schutzes im Rahmen des Zeugnisverweigerungsrechtes zeigt sich, mehr als an anderen Ausprägungen des Berufsgeheimnisträgerschutzes, wie stark das Vertrauensverhältnis zwischen Berufsgeheimnisträger und demjenigen, der ihm ein Geheimnis anvertraut, von der Rechtsordnung bewertet wird.

Diese Wertung wird auch unmittelbar auf andere strafprozessuale Bereiche übertragen. Schließlich darf das Verbot zur Aussageverweigerung vor Gericht nicht umgangen werden (§ 157 StPO).⁴¹ Dies darf auch nicht dadurch geschehen, dass Gegenstände

³⁸ Diese Pflicht gilt auch über den Tod des Mandanten hinaus und geht auch nicht auf dessen Rechtsnachfolger über; vgl BGH NJW 1968, 1773; BGH v. 25.11.1974 = DNotZ 1975, 420; OLG München AnwBl 1975, 159, 161.

³⁹ Dieser wird zudem wieder von Standesrichtlinien flankiert. Eine entsprechende Regelung findet sich in § 2 der Berufsordnung für Rechtsanwälte.

⁴⁰ Abrufbar unter <http://www.presserat.info/inhalt/der-pressekodex/pressekodex.html>.

⁴¹ Vgl Bertel/Venier, StPO, § 157, Rz 11 ff.

des Berufsgeheimnisträgers beschlagnahmt werden, die ihm in beruflicher Eigenschaft bekanntgeworden sind.⁴²

2.3.1. Heilberufe

Die Verschwiegenheitspflicht ist durch die StPO geschützt. Dies regeln § 144 Abs 2 und 3 und § 157 StPO. Allerdings bezieht sich die StPO auch nach der Reform nicht auf Ärzte,⁴³ sondern schließt im Rahmen der medizinischen Berufe lediglich Psychiater und Psychotherapeuten mit ein.⁴⁴

Demnach können diese die Aussage verweigern, wobei das Recht zur Aussageverweigerung hierbei nicht dadurch umgangen werden darf, dass der Geheimnisträger entsprechenden Überwachungsmaßnahmen ausgesetzt wird.

2.3.2. Geistliche und Seelsorger

Die bereits in Bezug auf medizinische Heilberufe erläuterten Vorschriften sind, was Geistliche angeht, weitergehend. Die geistliche Amtsverschwiegenheit ist durch § 144 Abs 1 StPO besonders geschützt. Dabei kommt es nicht darauf an, ob es sich um einen Geistlichen einer im Inland anerkannten Kirche oder Religionsgemeinschaft handelt.⁴⁵ Es besteht ein gesetzlich normiertes ausdrückliches Umgehungsverbot.⁴⁶

Der besonders umfassende Schutz – der sogar eine Art „überwachungsfreien Raum“ vorsieht – ist, wie bereits im Rahmen der berufsrechtlichen Vorschriften erwähnt, auch darauf zurückzuführen, dass sich Österreich im Konkordat mit dem Hl. Stuhl verpflichtet hat, die geistliche Amtsverschwiegenheit besonders zu schützen und für alle Religionsgemeinschaften zu einem recht umfassenden Schutz führt. Dies führt bei Ermittlungen im Bereich des Beichtgeheimnisses zu einem Beweisthemenverbot; dies bedeutet, dass sogar dann, wenn – was kirchenrechtlich nicht passieren sollte – der Inhalt des Beichtgespräches in die Hände Dritter gelangt, hierüber kein Beweis geführt

⁴² *Tipold/Zerbes* in Fuchs/Ratz, WK StPO Vor §§ 110 – 115, Rz 13, 18 ff.

⁴³ Dazu zu Recht kritisch *Schmoller*, WK-StPO, altes Vorverfahren § 3 Rz 53.

⁴⁴ Vgl *Kirchbacher*, WK-StPO, § 157, Rz 20ff.

⁴⁵ *Fabrizy*, StPO, § 144, Rz 1.

⁴⁶ *Fabrizy*, StPO, § 144, Rz 2.

werden darf.⁴⁷ Auch im Fall der Entbindung vom Beichtgeheimnis durch einen Straftäter für den Fall seines Todes, wäre eine Vernehmung des Geistlichen nicht zulässig.⁴⁸

2.3.3. Rechtsberatung

Von besonderer Wichtigkeit ist auch das anwaltliche Berufsgeheimnis. Dieses wird gem § 157 Abs 1 Z 2 StPO geschützt. Von der Vorschrift umfasst sind Verteidiger, Rechtsanwälte, Patentanwälte, Notare und Wirtschaftstreuhänder.

Es beinhaltet nicht nur die unmittelbar im Zusammenhang mit einem Rechtsstreit oder einer Strafverteidigung verfassten Schriftstücke und ausgetauschten Informationen, sondern auch beispielsweise anwaltliche Gutachten, Niederschriften und Ratschläge an den Mandanten und ist damit sehr weit auszulegen.⁴⁹

2.3.4. Medienmitarbeiter

Der Schutz des Berufsgeheimnisses der Medienmitarbeiter ist darauf zurückzuführen, dass den Medien in unserer Gesellschaft eine besondere Kontroll- und Aufklärungsfunktion in der Gesellschaft zukommt.⁵⁰

Dieser Schutz ist auch strafprozessual in § 157 Abs 1 Z 4 StPO verankert. Er findet zudem im Medienrecht seine Erwähnung in § 31 MedienG. Das Redaktionsgeheimnis ist hierbei auf Medienmitarbeiter beschränkt, findet also keine Anwendung auf bloße Verfasser von Gastbeiträgen, Leserbriefschreiber, etc.⁵¹ Umfasst vom Redaktionsgeheimnis sind allerdings auch freie Mitarbeiter und Personen, die für Medien tätig sind, ihre Tätigkeit aber nicht in „professioneller“ Weise ausüben.⁵² Auch sie sind Medienmitarbeiter nach der Legaldefinition von § 1 Z 11 MedienG, sofern ihre Tätigkeit keine wirtschaftlich unbedeutende Nebentätigkeit ist. Diese Abgrenzung ist durchaus kritisch zu sehen, da die wirtschaftliche Bedeutung der Tätigkeit für den Medien-

⁴⁷ *Tipold/Zerbes* in Fuchs/Ratz, WK StPO Vor §§ 110 – 115, Rz 13.

⁴⁸ *Leitner*, Vernehmungsverbote im österreichischen Strafprozessrecht, 32.

⁴⁹ Vgl *Stuefer*, Durchsuchung und Beschlagnahme im Strafverfahren, JSt 2011, 134, 138.

⁵⁰ *Berka/Heindl/Höhne/Noll*, Mediengesetz Praxiskommentar³, § 31, Rz 2.

⁵¹ Vgl *Röggla* in Röggla/Wittmann/Zöchbauer, MedienG PK, § 31 MedienG, Rz 1; *Berka/Heindl/Höhne/Noll*, Mediengesetz Praxiskommentar³, § 31, Rz 6.

⁵² Wie etwa Autoren in einer Schülerzeitung, vgl hierzu näher *Litzka/Strebinger*, Mediengesetz Kurzkomentar⁵, § 31, Rz 1.

mitarbeiter nicht unbedingt ein aussagekräftiges Kriterium für die Art der journalistischen Betätigung dar.⁵³

Zum einen regelt § 31 Abs 1 MedienG den Schutz des Redaktionsgeheimnisses, zum anderen stellt § 31 Abs 2 MedienG klar, dass dieser Schutz nicht durch andere Vorschriften umgangen werden darf. Schließlich nimmt § 31 Abs 3 MedienG für die Überwachung von Journalisten auf die Regelungen der StPO Bezug.

2.4. Strafprozessualer Schutz in Deutschland

Auch in Deutschland ist es Berufsgeheimnisträgern möglich, das Zeugnis im Strafprozess zu verweigern. Die Ausgestaltung ähnelt im Ergebnis der in Österreich, ist aber vom legistischen Aufbau her unterschiedlich. Die dStPO knüpft, ähnlich wie in Österreich, an die Aussageverweigerungsberechtigten an. Einziger, wenn auch zunächst für die Praxis wenig relevant scheinender Unterschied, ist, dass die systematische Einordnung nicht bei der Aussageverweigerung (wie in § 157 Abs 2 StPO) erfolgt, sondern direkt bei der Beschlagnahme in § 97 Abs 1 dStPO.⁵⁴ Des Weiteren existiert ein eigener Beschlagnahmeschutz im Bereich der Telekommunikation in § 160a dStPO.⁵⁵

Letztlich schafft er Gesetzgeber damit eine komplexe Situation in einer Art Dreiecksverhältnis zwischen der Aussageverweigerung (§ 53 dStPO), dem Beschlagnahmeverbot (§ 97 dStPO) und den Sondervorschriften für Telekommunikation (§ 160a dStPO),⁵⁶ obwohl diese thematisch zusammengehören.⁵⁷ Es wird also am Ende bei der legistischen Analyse auch darüber zu reden sein, inwiefern dies systematisch vorbildhaft oder eher ablehnenswert erscheint.

⁵³ Vgl hierzu *Rami*, Österreichische Medienprivilegien unter den Messern des EuGH und des EGMR, ÖJZ 2015, 533, 534 zumales bei Medienunternehmen auf diese rein wirtschaftliche Unterscheidung wiederum nicht ankommt.

⁵⁴ Vgl hierzu näher *Park*, Durchsuchung und Beschlagnahme³, Rz 533 ff, insbesondere die Übersicht in Rz 607.

⁵⁵ Dieser wird später näher ausgeführt. Darüber hinaus kann sich ein Beschlagnahmeschutz noch aus anderen Gesetzen, etwa aus Sozialgesetzen, ergeben. Vgl hierzu etwa *Park*, Durchsuchung und Beschlagnahme³, Rz 617.

⁵⁶ Hierbei ist das Verhältnis der einzelnen Vorschriften untereinander nicht abschließend geklärt; vgl hierzu *Park*, Durchsuchung und Beschlagnahme³, Rz 621 ff.

⁵⁷ In der Rechtsprechung ist die Frage, in welcher Beziehung beide Vorschriften zueinander stehen noch ungeklärt; vgl *Park*, Durchsuchung und Beschlagnahme³, Rz 634 ff mit Verweis auf LG Hamburg StV 2011, 148, 149 f. einerseits und LG Mannheim wistra 2012, 400, 407 andererseits.

2.4.1. Heilberufe

Die Vorschrift des § 53 dStPO schützt das Berufsgeheimnis der Ärzte und ähnlicher Berufe. Hierbei wird zwischen einzelnen Fachrichtungen nicht unterschieden. Ebenfalls erstreckt sich § 53 dStPO auf psychologische Psychotherapeuten. Entscheidend ist, dass die Berufsgeheimnisträger approbiert sind.⁵⁸ Das Berufsgeheimnis beschränkt sich auf Tatsachen, die der Berufsgeheimnisträger selbst wahrnimmt und die das Vertrauensverhältnis zum Patienten berühren.⁵⁹

2.4.2. Geistliche und Seelsorger

Die Regelung des § 53 dStPO nennt zunächst den Geistlichen, dessen Berufsgeheimnis zu schützen ist. Hierbei kann es nach der jüngsten Rechtsprechung entgegen früherer Ansichten keine Rolle spielen, ob es sich um ein staatlich anerkanntes Bekenntnis handelt.⁶⁰ Nach einer Literaturansicht, die früher als vorherrschend anzusehen war,⁶¹ genießen Geistliche von „Sekten“ nicht den Schutz des § 53 dStPO, wobei schwer zu definieren sein dürfte, was unter einer solchen zu verstehen ist.⁶² Diese pauschale Unterscheidung wird wohl nach aktueller, in der Rechtsprechung vorherrschender Sicht⁶³ nicht in dieser Form aufrechterhalten werden können.⁶⁴ Vielmehr wird eine Entscheidung im Einzelfall oder zumindest aufgrund sachlicher Kriterien zu treffen sein.⁶⁵

Der strafprozessuale Schutz soll es dem Hilfesuchenden ermöglichen, „sich mit einem Geistlichen zu besprechen, ohne befürchten zu müssen, dass dieser die ihm mitgeteilten Tatsachen und Umstände als Zeuge offenbaren muss. Der Schutz erfolgt

⁵⁸ *Senge* in Karlsruher Kommentar zur StPO⁶, § 53, Rz 17.

⁵⁹ *Senge* in Karlsruher Kommentar zur StPO⁶, § 53, Rz 18; insofern nicht umfasst ist damit, was der Berufsgeheimnisträger von einem Dritten außerhalb des Behandlungsverhältnisses über den Patienten erfährt, da hier kein Bezug zum Vertrauensverhältnis gegeben ist.

⁶⁰ BGH NSTZ 2010, 646.

⁶¹ Zusammenfassend *Senge* in Karlsruher Kommentar zur StPO⁶, § 53, Rz 11.

⁶² Vgl zusammenfassend und zugleich kritisch *Haas*, Zeugnisverweigerungsrecht des Geistlichen, NJW 1990, 3253 zum mangelnden Zeugnisverweigerungsrecht eines Geistlichen der Zeugen Jehovas im Gegensatz zum Geistlichen der Neuapostolischen Kirche, dies jedoch nur im Bundesland Nordrhein-Westfalen, da diese dort staatlicherseits anerkannt ist.

⁶³ BGH NSTZ 2010, 646.

⁶⁴ So vorausgehend schon *Haas*, Zeugnisverweigerungsrecht des Geistlichen, NJW 1990, 3253, 3254.

⁶⁵ So wird es zulässig sein eine Religionsgemeinschaft von einer eher wirtschaftlichen Organisation abzugrenzen. Vgl zu dieser Problematik BVerfG NJW 2002, 3458, 3459 zum Fall der Scientology.

um der Menschenwürde des Gesprächspartners des Seelsorgers willen“⁶⁶. Der Geistliche muss hierfür von seiner Religionsgemeinschaft keine Weihe o.ä. empfangen haben.⁶⁷

Einzige Einschränkung dieses weitreichenden Berufsgeheimnisses ist es, dass der Geistliche von der Tatsache, über die er das Zeugnis verweigern darf, in seiner Tätigkeit als Seelsorger erfährt. Eine Zeugnisverweigerung ist als unzulässig, wenn der Geistliche in eine andere Tätigkeit ausführt, die mit Seelsorge in keinem Zusammenhang stehen, also etwa die Verwaltung kirchlichen Vermögens.⁶⁸ Bei der Seelsorge kann es sich um sakramentale Seelsorge wie beim Beichtgespräch handeln, das bestimmte religiösen Regeln folgt,⁶⁹ oder um ein seelsorgerisches Gespräch ohne eine bestimmte Form handeln.

2.4.3. Rechtsberatung

In der Rechtsberatung überrascht zunächst die Terminologie des Gesetzgebers, der zwischen Verteidigern (§ 53 Abs 1 S 1 Z 2 dStPO) und Rechtsanwälten (§ 53 Abs 1 S 1 Z 3 dStPO) unterscheidet, ihnen jedoch die gleichen Rechte zur Verweigerung des Zeugnisses einräumt. Dies ist zum einen darauf zurückzuführen, dass Verteidiger eine herausgehobene Stellung im Strafverfahren haben und ist außerdem der Tatsache geschuldet, dass in Deutschland auch Konstellationen möglich sind, in denen es Verteidiger gibt, die über keine Anwaltszulassung verfügen.⁷⁰

⁶⁶ BGH NStZ 2010, 646, 647.

⁶⁷ BVerfG NJW 2007, 1865 zum Bestehen des Zeugnisverweigerungsrechts eines römisch-katholischen Gemeindereferenten der für die Seelsorge von Strafgefangenen zuständig ist.

⁶⁸ Huber in BeckOK StPO, § 53, Rz 10.

⁶⁹ RG JW 1928, 2142.

⁷⁰ Denkbar ist hier der durchaus praxisrelevante Fall, dass die vom Beschuldigten gewählte oder vom Gericht bestellte Person des Verteidigers Rechtslehrer an einer deutschen Hochschule ist. Auch diese können als Strafverteidiger auftreten (§ 138 Abs 1 dStPO), sofern sie über die Voraussetzungen nach § 5 DRiG („Befähigung zum Richteramt“) – also über ein Zweites Staatsexamen – verfügen. Andere Personen, die die Voraussetzung des § 5 DRiG erfüllen, können vom Gericht ausnahmsweise bestellt werden (§ 138 Abs 2 dStPO). Auch möglich ist es, dass die Tätigkeit von einem Rechtsanwalt auf den ihm zur Ausbildung zugewiesenen Rechtsreferendar (ein Jurist mit Universitätsstudium und Erster Juristischer Staatsprüfung im Vorbereitungsdienst) nach § 140 dStPO überträgt. Vgl hierzu *Senge* in *Karlsruher Kommentar zur StPO*⁶, § 53, Rz 13.

Davon abgesehen gestaltet sich der Schutzbereich der Vorschriften auf den ersten Blick recht einfach, auf den zweiten Blick jedoch komplizierter. Betrachtet man den Schutzbereich aus einer generalisierenden Perspektive, dann sind davon, von den Ausnahmen im Bereich der Verteidigung abgesehen, alle Personen erfasst, die über eine entsprechende Zulassung Verfügung (wie etwa Rechtsanwälte, Steuerberater oder Notare).⁷¹ Grob könnte man diese Personengruppe als „Rechtsanwälte und Gleichgestellte“ bezeichnen. Jedoch ergibt sich hier eine, wenn auch umstrittene, Ausnahme. In Deutschland ist es üblich, dass Juristen, die für ein Unternehmen tätig sind, auch zugelassene Rechtsanwälte sind, und in gewissem Umfang anwaltliche Tätigkeiten für das Unternehmen übernehmen.⁷² Die Tätigkeit wird von den Rechtsanwaltskammern nur genehmigt, wenn der Arbeitgeber dem Rechtsanwalt genügend Freiheiten einräumt, wie etwa ohne Rücksprache mit dem Unternehmen weitere Mandate anzunehmen.⁷³

2.4.4. Medienmitarbeiter

Die Zeugnisverweigerung der Medienmitarbeiter ist in § 53 dStPO geregelt. Neben Geistlichen und Seelsorgern, Verteidigern, rechtsberatenden Berufen, Heilberufen, Schwangerschafts- und Drogenberatungsstellen und Abgeordneten, sieht die Vorschrift auch ein Zeugnisverweigerungsrecht für Medienmitarbeiter vor (§ 53 Abs 1 Z 5 dStPO).⁷⁴

Das Recht zur Zeugnisverweigerung steht allen zu, die berufsmäßig an Verbreitung und / oder Herstellung des Presserzeugnisses beteiligt sind.⁷⁵ Keine Rolle spielt es

⁷¹ *Senge* in Karlsruher Kommentar zur StPO⁶, § 53, Rz 13.

⁷² Hierbei unterliegen sie nur wenigen Einschränkungen; eine der wenigen, wenn auch entscheidenden, ist das Vertretungsverbot, also das Verbot für das Unternehmen im Rahmen eines Rechtsstreits vor Gericht tätig zu werden.

⁷³ Hierbei darf beim Anwalt lediglich keine Interessenkollision vorliegen. Dies hat er ohnehin bei jedem Mandat zu prüfen.

⁷⁴ Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von Druckwerken, Rundfunksendungen, Filmberichten oder der Unterrichtung oder Meinungsbildung dienenden Informations- und Kommunikationsdiensten berufsmäßig mitwirken oder mitgewirkt haben.

⁷⁵ *Huber* in BeckOK, StPO, § 53, Rz 26.

dabei, ob es sich um angestellte Journalisten oder freiberuflich tätige Mitarbeiter handelt.⁷⁶

Das Zeugnisverweigerungsrecht ist vor allem auf die Person des Informanten bezogen, der auch selbst Pressemitarbeiter sein kann.⁷⁷ Es handelt sich also nicht um ein umfassendes Zeugnisverweigerungsrecht, wie es etwa Geistlichen zukommt, sondern um einen reinen Schutz derjenigen, die dem Pressemedium Informationen liefern.

Dieser Informantenschutz ist weitreichend. Damit kann der Journalist nicht nur Fragen nach der Person des Informanten unbeantwortet lassen, sondern darf das Zeugnis über alle Fragen verweigern, welche sich auf die näheren Umstände der Kontaktaufnahme beziehen, die unmittelbar oder auch nur mittelbar zur Enttarnung des Informanten führen könnten.⁷⁸ Der Informant kann auch selbst der Verfasser eines Beitrags sein, der entsprechend abgedruckt oder gesendet wird; so dass keine Verpflichtung bestehen kann, den Namen mit abzudrucken oder auf Nachfrage zu nennen.⁷⁹ Nicht relevant ist, ob der Medienmitarbeiter die erlangten Informationen bereits veröffentlicht hat bzw ob er diese überhaupt veröffentlichen wird.⁸⁰

Seit einer Gesetzesänderung⁸¹ ist auch auf Grundlage von Informantenangaben erarbeitetes selbst erstelltes Material von § 53 dStPO erfasst. Eigene Eindrücke, die sich der Medienmitarbeiter gebildet hat, können, sobald sie zu Papier gebracht, diktiert oder in irgendeiner Weise digital festgehalten sind, somit vom Schutz des Zeugnisverweigerungsrechts umfasst; folglich hat der Verfasser die Möglichkeit das Redaktionsgeheimnis auch in gewisser Weise „gestaltend“ wahrzunehmen und durch entsprechende Verknüpfung von persönlichen Wahrnehmungen oder weiteren Recherchen mit den

⁷⁶ BGH NJW 1999, 2051; jedoch scheiden „Gelegenheitsjournalisten“ wohl aus *Kunert* MDR 1975, 885, 886; nicht relevant ist es jedoch ob die Tätigkeit Haupt- oder Nebenberuflich ausgeübt wird.

⁷⁷ *Huber* in BeckOK, StPO, § 53, Rz 26.

⁷⁸ BGH NSTZ 1990, 135 f; dort weigerte sich ein Journalist gegenüber den Behörden nähere Angaben zu einem Interview mit einem gesuchten Terroristen der Irish Republican Army zu machen, da er dessen Identität schützen wollte. Zu den näheren Angaben gehört z B die Frage danach, in welcher Sprache das Interview geführt wurde, ob Fotos während des Interviews angefertigt wurden oder ob weitere Personen, wie etwa ein Dolmetscher, beteiligt waren.

⁷⁹ *Senge* in Karlsruher Kommentar zur StPO⁶, § 53, Rz 37f.

⁸⁰ *Senge* in Karlsruher Kommentar zur StPO⁶, § 53, Rz 43.

⁸¹ BT-Drucksache 14/5166.

Aussagen des Informanten, diese Informationen ebenfalls dem Redaktionsgeheimnis zu unterwerfen.⁸²

Das soeben erläuterte Zeugnisverweigerungsrecht findet seine gemäß § 53 Abs 2 dStPO seine Grenzen. Diese Regelung ist ebenfalls eine Besonderheit, die sich nur im Zeugnisverweigerungsrecht der Medienmitarbeiter findet.

Eine Zeugnisverweigerung ist dann teilweise unzulässig, wenn bestimmte Straftaten im Raum stehen. Hierfür genügt auch ein Verdacht.⁸³ Allerdings muss die Person des Informanten selbst dann nicht offenbart werden. Offengelegt werden müssen lediglich selbst erstellte Materialien, aus denen sich keine direkten Rückschlüsse auf die Person des Informanten schließen lassen.

2.5. Schutz nach sonstigen Vorschriften in Österreich

Über das Berufsrecht und das Strafprozessrecht hinaus durchzieht der Berufsgeheimnisträgerschutz die Rechtsordnung und findet prozessrechtlichen aber auch strafrechtlichen Niederschlag.

Bei Verletzung des Berufsgeheimnisses durch Personen in Gesundheitsberufen greift § 121 StGB. Dessen Tatbestand ist erfüllt, wenn ein Geheimnis über die Gesundheit eines Patienten einem Dritten, dem dieses nicht bekannt ist, offenbart wird oder sich der Täter das Geheimnis wirtschaftlich nutzbar macht und es damit verwertet.⁸⁴ Strafbar ist das Offenbaren oder Verwerten jedoch letztlich nur dann, wenn dadurch berechnigte Interessen des Patienten verletzt werden.⁸⁵ Die Tat ist ein Privatklagedelikt (§ 71 StPO).⁸⁶

⁸² *Kunert*, Erweitertes Zeugnisverweigerungsrecht der Medienmitarbeiter, Gesetz zur Änderung der Strafprozessordnung vom 15. 2. 2002, NStZ 2002, 169, 172.

⁸³ *Senge* in Karlsruher Kommentar zur StPO⁶, § 53, Rz 44b.

⁸⁴ *Lewisch* in WK-StGB § 121 Rz 7.

⁸⁵ Dies ist z B dann nicht der Fall, wenn der behandelnde Kinderarzt einen sexuellen Missbrauch des Patienten erkennt und den Behörden gegenüber offenbart, vgl *Lewisch* in WK-StGB § 121 Rz 10.

⁸⁶ *Fabrizy*, StGB, § 121, Rz 6.

Ebenso schützen § 49 AVG und § 321 ZPO das Berufsgeheimnis im Verwaltungsverfahrenrecht bzw Zivilprozessrecht.⁸⁷ Der Berufsgeheimnisträger kann nicht dazu gezwungen werden, als Zeuge eine Ausnahme zu machen. Vielmehr kann er den Konflikt mit weiteren Vorschriften, die das Berufsgeheimnis schützen, verhindern.⁸⁸ Gleiches gilt für die Verschwiegenheitspflicht im Finanzstrafverfahren, welche in § 104 FinStrG geregelt ist. Der Schutz des Redaktionsgeheimnisses gilt auch im Verfahren vor den Verwaltungsgerichten oder in abgabenrechtlichen Sachen.⁸⁹

Geistliche fallen nicht unter § 49 AVG, da ihre Vernehmung bereits nach § 48 Z 2 und 3 AVG ausgeschlossen ist. Diese Vorschrift geht als *lex specialis* vor.⁹⁰ Wie in der StPO steht die geistliche Amtsverschwiegenheit damit unter einem besonderen Schutz.⁹¹

2.6. Schutz nach sonstigen Vorschriften in Deutschland

In Deutschland regelt § 203 dStGB die Strafbarkeit der Verletzung von Privatgeheimnissen. Die Vorschrift schützt umfassend die Berufsgeheimnisse in strafrechtlicher Hinsicht und differenziert dabei nicht zwischen einzelnen Berufen. Inhaltlich korrespondiert sie, mit den bereits erläuterten strafprozessualen Vorschriften in Deutschland, auch wenn sie, was den Personenkreis angeht, über diese teilweise hinausgeht, diesen aber auch unterschreitet.⁹²

Normzweck dieser Vorschrift ist die Verhinderung von „informationeller Veruntreuung“ durch den Berufsgeheimnisträger.⁹³ Die Vorschrift deckt zudem Betriebs- und

⁸⁷ Vgl dazu Zenz, "Staatlich anerkannte Pflicht zur Verschwiegenheit" bestimmter Berufsgruppen im Verhältnis zur Zeugnisablegung im Verwaltungs-, Zivil- und Strafverfahren, ZRP 2005, 230.

⁸⁸ Vgl zum ärztlichen Berufsgeheimnis Frauenberger in Fasching/Konecny, Zivilprozessgesetze, § 321 ZPO, Rz 30.

⁸⁹ Langheinrich/Ryda, Beweismittel im Verfahren vor den (Abgaben-)Behörden und den Verwaltungsgerichten (Teil II), FJ 2016, 3, 7.

⁹⁰ Hengstschläger/Leeb, AVG, § 49, Rz 15.

⁹¹ Auch hier ist es unerheblich, ob die Religionsgemeinschaft offiziell anerkannt ist oder nicht, vgl zum Begriff des Geistlichen Hengstschläger/Leeb, AVG, § 49, Rz 22.

⁹² So sind z B auch Mitarbeiter einer Krankenversicherung von § 203 dStGB umfasst. Nicht umfasst sind jedoch Medienmitarbeiter.

⁹³ Cierniak/Pohlitz in MÜKo-StGB, § 203, Rz 1.

Geschäftsgeheimnisse ab und geht damit über den „klassischen“ Schutz der Berufsgeheimnisse weit hinaus.⁹⁴

Die Verletzungshandlung im Sinne des § 203 Abs 1 dStGB ist die „Offenbarung“ des Geheimnisses, also eine Mitteilung an einen unbefugten Dritten.⁹⁵ Das Verwerten stellt § 204 dStGB unter Strafe. Bei den Straftaten handelt es sich nach § 205 dStGB um sog Privatklagedelikte.⁹⁶

Ebenfalls finden sich Regelungen in den weiteren Prozessordnungen neben der dStPO zum Schutz von Berufsgeheimnisträgern, wie etwa in § 383 dZPO, auf den andere Prozessordnungen wiederum verweisen.⁹⁷ Der Schutz stellt sich somit in den sonstigen Regelungen etwas umfassender dar, als dies in Österreich der Fall ist.

Aus rechtspraktischer Sicht scheint diese Unterscheidung aber keine Rolle zu spielen. Die Vorschriften im dStGB zum Schutz von Berufsgeheimnissen haben eine zu vernachlässigende kriminalpolitische Bedeutung.⁹⁸

3. Verfassungsrechtliche Grundlagen des Berufsgeheimnisträgerschutzes in Österreich

Die Tatsache, dass die lediglich einfachgesetzlich definierten Berufsgeheimnisträger besonders geschützt sind, ergibt sich direkt aus verfassungsrechtlichen Vorgaben. Dabei kommen verschiedene Grundrechte in Betracht. Zum einen gibt es Grundrechte, die direkte Bezüge zu Berufsgeheimnisträgern aufweisen, wie etwa Art 6 EMRK (Recht auf ein faires Verfahren), da die Möglichkeit einer anwaltlichen Vertretung für dieses Grundrecht immanent ist. Doch auch andere Grundrechte, wo ein Bezug zu Berufsgeheimnisträgern weniger stark ausgeprägt ist, sind bei dieser Betrachtung relevant. Zu

⁹⁴ Der Schutz von Geschäftsgeheimnissen an diese Stelle wird in der Literatur zur recht für deplatziert an dieser Stelle gehalten; vgl hierzu *Kargl* in Kindhäuser/Neumann/Paeffgen, StGB, § 203, Rz 1.

⁹⁵ Vgl *Kargl* in Kindhäuser/Neumann/Paeffgen, § 203, Rz 19.

⁹⁶ In Deutschland: Antragsdelikte.

⁹⁷ Vgl etwa § 98 VwGO.

⁹⁸ *Cierniak/Pohl* in MÜKo-StGB, § 203, Rz 7.

nennen wäre in diesem Zusammenhang Art 8 EMRK (Recht auf Achtung des Privat- und Familienlebens). Ebenfalls von Bedeutung in diesem Zusammenhang ist die Grundrechte-Charta der EU mit Art 7 GRC⁹⁹, da diese auch in einem verfassungsrechtlichen Verfahren nach Art 139 f B-VG Prüfungsmaßstab sein kann, sofern die Normen im Anwendungsbereich der Charta erlassen wurden.¹⁰⁰ Die grundrechtlichen Grundlagen der Stellung der Berufsgeheimnisträger sollen anhand der spezifischen Grundrechte vorliegend kurz erläutert werden.

3.1. Art 6 EMRK – Recht auf ein faires Verfahren

Das Recht auf ein faires Verfahren ist zweifelsohne eine der wichtigsten Vorschriften der EMRK.¹⁰¹ Zwar betrifft die Vorschrift lediglich das Straf- und Zivilverfahren, jedoch legt der EGMR diese Begriffe selbständig aus, so dass mitunter auch Verfahren, die national dem öffentlichen Recht zugeordnet werden, darunter fallen können. So wird beispielsweise ein berufsrechtliches Disziplinarverfahren bei Anwälten vom EGMR dem Zivilrecht zugerechnet.¹⁰² Das Recht auf ein faires Verfahren berührt von den Berufsgeheimnissen nur das der rechtsberatenden Berufe.

Relevant im Zusammenhang dieser Untersuchung ist dabei Art 6 Abs 3 lit c. Dieser garantiert das Recht auf Verteidigung umfassend. Dazu gehört nicht nur, dass sich ein Angeklagter selbst verteidigen kann und sich durch einen Verteidiger – nötigenfalls unentgeltlich – verteidigen lassen kann, sondern auch dass er ungestört und ohne Überwachungsmaßnahmen fürchten zu müssen mit dem Verteidiger verkehren kann und dies sogar dann, wenn ihm schwere Straftaten zur Last liegen.¹⁰³ Unter bestimmten Umständen ist es zulässig, ausnahmsweise Verteidiger und Mandant zu überwachen: zum einen wenn der Mandant besondere Gefährlichkeit aufweist und zum anderen, wenn der

⁹⁹ Ebenfalls wichtig ist Art 8 EUGR-Charta, der auch eine Teilidentität mit Art 8 EMRK aufweist, vgl dazu *Raschauer* in Raschauer, Datenschutzrecht 2010, 21.

¹⁰⁰ Vgl explizit für den Bereich der Vorratsdatenspeicherung VfGH vom 28.11.2012, G47/12-11, 59/12-10, ua, Rz 24.

¹⁰¹ So ist in mehr als der Hälfte der Fälle des EGMR Art 6 EMRK betroffen, vgl *Meyer-Ladewig*, EMRK, Art 6 Rz 1.

¹⁰² EGMR ÖJZ 2000, 728 – W.R. / Österreich.

¹⁰³ EGMR ÖJZ 1992, 343 = NJW 1992, 3090 = EuGRZ 1992, 298 – S./Schweiz; dazu Anmerkung von Dörr, JuS 1993, 508.

Verdacht der Kollusion zwischen Verteidiger und Mandant besteht.¹⁰⁴ Diese Beschränkungen dürfen zum einen nur kurzfristig sein und bedürfen weiters einer substantiierten Begründung; die Begründungslast steigt hierbei, je länger die Überwachungsmaßnahme andauert.¹⁰⁵ Diese Rechte bestehen auch während einer Untersuchungshaft¹⁰⁶ und damit erst Recht, wenn sich der Mandant auf freiem Fuß befindet. Der EGMR hält die unüberwachte Kommunikation zwischen Verteidiger und Mandant für eine elementare Voraussetzung für ein faires Verfahren.¹⁰⁷

3.2. Art 8 EMRK – Recht auf Achtung des Privat- und Familienlebens

Die Vorschrift des Art 8 EMRK ist sehr weitgehend und ist weniger als ein einzelnes Grundrecht zu verstehen, sondern fasst mehrere Grundrechte zusammen. Sie schützt neben dem Privat- und Familienleben auch die Wohnung und die Korrespondenz.¹⁰⁸

Hierbei ist vor allem die Korrespondenz für das Recht der Berufsgeheimnisträger von Bedeutung, wenn zwischen ihnen und dem Mandanten, Patienten, etc. kommuniziert wird. Jedoch berührt auch die berufliche Tätigkeit der Berufsgeheimnisträger fast alle Schutzbereiche von Art 8 EMRK, was die Vorschrift mit zur wichtigsten verfassungsrechtlichen Schutznorm für Berufsgeheimnisträger macht.

3.2.1. Schutz der Korrespondenz

Der Begriff Korrespondenz im Sinne der Vorschrift steht einer weiten Auslegung offen. Unter Korrespondenz ist dabei nicht nur alles zu verstehen, was in irgendeiner Weise verschriftlicht ist; vielmehr schließt der Begriff alle möglichen Formen der Kommunikation zwischen Personen mit ein, also auch Telefongespräche¹⁰⁹ und elektro-

¹⁰⁴ Meyer in Karpenstein/Mayer, EMRK, Art 6, Rz 195; ebenso besteht im Übrigen auch nahezu keine Möglichkeit auf Grund eines „Kollusionsverdachts“ die Wahl eines bestimmten Verteidigers zu untersagen; vgl hierzu Grabenwarter/Pabel, EMRK⁵, § 24, Rz 111.

¹⁰⁵ Meyer in Karpenstein/Mayer, EMRK⁵, Art 6, Rz 195.

¹⁰⁶ Vgl EGMR NJW 1987, 563.

¹⁰⁷ Vgl Grabenwarter/Pabel, EMRK⁵, § 24, Rz 112.

¹⁰⁸ Meyer-Ladewig, EMRK, Art 8, Rz 1.

¹⁰⁹ EGMR EuGRZ 1992, 298, 300 – Lüdi ./.. Schweiz.

nisch gespeicherte Daten.¹¹⁰ Hierbei gibt es – ebenso wie bei anderen Schutzgütern von Art 8 EMRK (dazu sogleich) – keine scharfe Trennlinie zwischen gewerblichem und privatem Bereich.¹¹¹

3.2.2. Schutz der Wohnung

Auch das Schutzgut Wohnung kann betroffen sein, wenn beispielsweise die Kanzlei eines Rechtsanwaltes oder die Ordination eines Arztes durchsucht wird.¹¹² Dies wird unter anderem damit begründet, dass, würde man den Schutz des Art 8 EMRK demjenigen versagen, der beruflichen und privaten Bereich klar voneinander trennt, würde man mit der Vorschrift denjenigen privilegieren, der beide Bereiche vermischt und so eine Trennung unmöglich macht.

Dies führt in der Konsequenz dazu, dass letztlich auch Räume einer juristischen Person unter den Begriff Wohnung fallen und aus dem Schutz der Wohnung quasi auch ein „Schutz der Geschäftsräumlichkeiten“ wird.¹¹³ Anstatt von Wohnungen zu reden, beschreibt wohl der Begriff „abgeschlossene Räumlichkeit“ den Schutzbereich der Norm an dieser Stelle am besten.

3.2.3. Schutz des Privatlebens

Auch der Schutz des Privatlebens kommt den Berufsgeheimnisträgern zugute. Ein wichtiger Aspekt dieses Grundrechtes ist es, berufliche Kontakte aufzunehmen.¹¹⁴ Somit kennt das Grundrecht auch hier keine Trennung zwischen Berufsleben auf der einen Seite und Privatleben auf der anderen Seite.¹¹⁵ Folglich betrifft auch dieses Schutzgut des Art 8 EMRK das Recht der Berufsgeheimnisträger. Auch die Kenntnisnahme von Kommunikation, die nur berufliche Inhalte enthält, unterfällt damit dem

¹¹⁰ EGMR NJW 2008, 3409 – Wieser u. Bicos Beteiligungen-GmbH ./ Österreich.

¹¹¹ EGMR NJW 2008, 3409, 3410 – Wieser u. Bicos Beteiligungen-GmbH ./ Österreich.

¹¹² Vgl hierzu EGMR NJW 1993, 718 – Niemitz ./ Deutschland; vgl dazu eingehend *Spielmann*, AnwBl 2010, 346, 347.

¹¹³ EGMR JuS 2007, 369 – Buck ./ Deutschland.

¹¹⁴ Näher dazu *Spielmann*, Das anwaltliche Berufsgeheimnis in der Rechtsprechung des EGMR, AnwBl 2010, 346, 347.

¹¹⁵ Geschützt sein kann aber nur die Berufsausübung, nicht unbedingt die freie Wahl des Berufes, vgl *Meyer-Ladewig*, EMRK, Art 8, Rz 31.

Schutz von Art 8 EMRK, weswegen eine Abgrenzung von Privat- und Berufsleben im Rahmen dieses Grundrechts allgemein als kritisch anzusehen ist.¹¹⁶

3.3. § 1 HausrechtsG, Art 9 StGG – Schutz des Hausrechtes

Bereits im Jahre 1862 wurde in Österreich die Durchsuchung von Wohnungen unter einen Richtervorbehalt gestellt.¹¹⁷ Wenige Jahre später wurde das Hausrecht auch Teil des StGG, indem dieses durch Art 9 StGG zum Teil des StGG erklärt wurde.¹¹⁸ Damit steht die Bestimmung gemäß Art 149 B-VG automatisch im Verfassungsrang. Der Gesetzgeber muss damit alle Gesetze, die eine Hausdurchsuchung ermöglichen, mit einem richterlichen Befehl versehen.¹¹⁹

Ähnlich wie bei dem Schutz des häuslichen Bereichs in der EMRK ist der Schutzbereich weit auszulegen und umfasst sämtliche räumlich abgeschlossenen Bereiche.¹²⁰ Das Hausrecht dient damit der Wahrung der Intimsphäre. Hierzu entschied bereits 1933 der Verfassungsgerichtshof:¹²¹

Nun soll durch den Schutz des Hausrechtes verhindert werden, dass ein die persönliche Würde und Unabhängigkeit verletzender Eingriff in den Lebenskreis des Wohnungsinhabers, in Dinge, die man im allgemeinen berechtigt und gewohnt ist, dem Einblick Fremder zu entziehen.

Hierauf nahmen zahlreiche Urteile des VfGH Bezug.¹²² Die Definition vom Schutzbereich des Hausrechtes ist insofern unverändert. Je stärker Dinge dann in einer Wohnung den Blicken der Öffentlichkeit entzogen sind, desto mehr fällt der Schutz des Hausrechtes ins Gewicht.¹²³

¹¹⁶ Vgl Ennöckl, Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung, 58 f.

¹¹⁷ Gesetz zum Schutze des Hausrechts, RGBI Nr. 88/1862.

¹¹⁸ Dies wurde schon in der ersten Fassung des StGG berücksichtigt, RGBI Nr. 142/1867.

¹¹⁹ Berka, Grundzüge des Verfassungsrechts⁴, Rz 1291.

¹²⁰ Berka, Grundzüge des Verfassungsrechts⁴, Rz 1414.

¹²¹ VfSlg 1486/1933.

¹²² VfSlg 5182/1965, 9525/1982, 10.897/1986.

¹²³ Vgl hierzu VfSlg 10.897/1986 in Bezug auf einen Kasten.

3.4. Art 6 StGG – Erwerbsfreiheit

In Österreich ist die Freiheit des Erwerbes durch Art. 6 StGG geschützt. Inwiefern dies für Berufsgeheimnisträger einen verfassungsrechtlichen Vorteil ist von der Judikatur nie behandelt worden. Die Gewährleistung steht unter Gesetzesvorbehalt. Grundsätzlich darf das Grundrecht durch den Gesetzesvorbehalt nicht im Wesensgehalt angetastet werden,¹²⁴ wobei diese Einschränkung anscheinend nur theoretischer Natur ist.¹²⁵

3.5. Art 14 StGG, Art 9 EMRK – Glaubensfreiheit

In Bezug auf bestimmte Berufsgeheimnisse kann auch die Glaubensfreiheit eine Rolle spielen. Diese umfasst die freie Wahl und Ausübung eines religiösen Bekenntnisses, einschließlich der Befolgung von Gebräuchen in der religiösen Praxis.¹²⁶ Hierzu gehört etwa auch die Inanspruchnahme von Seelsorge, welche zum Teil einfach religiöse Praxis, zum Teil jedoch auch Bestandteil der religiösen Lebensführung ist bzw nach der Glaubensauffassung in bestimmten Lebenssituationen geboten ist.¹²⁷

Die Einschränkung des Grundrechts der Glaubensfreiheit ist nur in sehr engen Grenzen möglich, da gemäß Art 63 Abs 2 StV St. Germain die Religionsausübung zu gewährleisten ist, sofern kein Verstoß gegen die öffentliche Ordnung oder die guten Sitten vorliegt.¹²⁸ Insofern ist das Eingreifen in das Berufsgeheimnis bei Seelsorgern an besonders strenge Anforderungen geknüpft. Dies muss sich in der konkreten gesetzgeberischen Ausgestaltung entsprechend niederschlagen.

¹²⁴ VfSlg 7304/1973, 9173/1981, 9233/1981, 9237/1981; vgl zur Entwicklung der Rspr des VfGH krit *Binder*, Der materielle Gesetzesvorbehalt der Erwerbsfreiheit (Art 6 StGG) - Überlegungen zur neuen Judikatur des VfGH, ÖZW 1988, 1 ff.

¹²⁵ Vgl zur Entwicklung der Rspr des VfGH krit *Binder*, Der materielle Gesetzesvorbehalt der Erwerbsfreiheit (Art 6 StGG) - Überlegungen zur neuen Judikatur des VfGH, ÖZW 1988, 1 ff..

¹²⁶ *Berka*, Grundzüge des Verfassungsrechts⁴, Rz 1431f.

¹²⁷ Vgl etwa Katechismus der Katholischen Kirche, Kompendium, 113.

¹²⁸ Da diese Schranke enger ist, als jene in Art 9 Abs 2 EMRK kommt diese nach dem Günstigkeitsprinzip zum Tragen; vgl zum Ganzen *Berka*, Grundzüge des Verfassungsrechts⁴, Rz 1434ff.

3.6. Art 13 StGG, Z 2 Beschluss ProvNV, Art 10 EMRK – Medienfreiheit

Verfassungsrechtlich ist die freie Betätigung der Massenmedien anerkannt. Die freien Medien werden vom Verfassungsgesetzgeber für unerlässlich für die Meinungsbildung der Bevölkerung angesehen.¹²⁹ Dieses Grundrecht wird nicht schrankenlos gewährleistet, sondern unterliegt verfassungsrechtlich gesehen Einschränkungsmöglichkeiten, die ihrerseits wiederum – etwa durch Art 10 Abs 2 EMRK – limitiert sind. Hier weicht, was den Schutz des Berufsgeheimnisses angeht, das Verfassungsrecht stark von der Gesetzeslage in § 31 MedienG ab. Der Gesetzgeber hat mithin die starke Schutzbedürftigkeit des Redaktionsgeheimnisses erkannt, ohne dieses direkt in den Verfassungsrang zu heben. Hier stellt sich die Frage, inwiefern eine solche „absolute“ Verankerung außerhalb des Verfassungsrechts sinnig ist. Gleichwohl sei darauf hingewiesen, dass der EGMR den Schutz von Informanten als Teil des Redaktionsgeheimnisses ansieht; hierbei sieht das Gericht diesen als festen Bestandteil der Pressefreiheit an.¹³⁰ Daher mag man eine Verankerung im Verfassungsrecht auch für überflüssig halten. Meinem Erachten nach, wäre eine solche aber trotzdem geboten. Wenn schon trotz einer verfassungsrechtlichen Regelung ein solch absoluter Schutz im einfachen Gesetz verankert wird und der Schutz des Redaktionsgeheimnisses dort so absolut ausgestaltet wird, sollte man den Anschein vermeiden, dieses würde in der Form zur Disposition des einfachen Gesetzgebers stehen.¹³¹

4. Verfassungsrechtliche Grundlagen des Berufsgeheimnisträgerschutzes in Deutschland

Für den verfassungsrechtlichen Berufsgeheimnisträgerschutz wird als wichtigstes Grundrecht die Berufsfreiheit nach Art 12 GG vorrangige Relevanz entfalten. Die Norm ist sicher der grundlegende verfassungsrechtliche Anker, wenn auch nicht der einzige.

¹²⁹ Berka, Grundzüge des Verfassungsrechts⁴, Rz 1459f.

¹³⁰ EGMR Urt. v. 27.3.1996, Nr. 17488/90; EGMR Urt. v. 22.11.2007, Nr. 20477/05.

¹³¹ Vgl zu entsprechenden Diskussionen und Vergleich mit dem Amtsgeheimnis http://diepresse.com/home/wirtschaft/alpbach2010/1445831/Experten-empfoert_Faellt-mit-Amts-auch-Redaktionsgeheimnis.

Darüber hinaus gewährleisten andere Grundrechte zusätzlich den Schutz bestimmter Berufsgeheimnisse. Dies kann zu einem teilweise unterschiedlichen Schutzniveau führen, was für die einfachgesetzliche Umsetzung wiederum von Bedeutung sein kann.

4.1. Art 12 Abs 1 GG – Berufsfreiheit

Das Grundrecht des Art 12 Abs 1 GG gewährleistet sowohl die Freiheit der Berufswahl als auch der Berufsausübung.¹³² Hierbei beinhaltet das Grundrecht ein subjektives Abwehrrecht gegen staatliche Eingriffe.¹³³ Hierzu kann es auch gehören, dass der Staat bestimmte Berufsgeheimnisse gewährleisten muss. Hintergrund hierfür ist, dass es bei manchen Berufen notwendig ist, dass solche Berufsgeheimnisse existieren, da ansonsten der Berufsgeheimnisträger seinen Beruf nicht in der gebotenen Weise ausüben instande ist.¹³⁴

Das BVerfG führt zu dieser Thematik aus, dass ein Geheimnisschutz nur dann notwendig ist, wenn er ansonsten nicht „sinnvoll oder bestimmungsgemäß“ ausgeübt werden kann.¹³⁵ Es ist also eine Betrachtung des einzelnen Berufsbildes erforderlich. Ein Eingriff in Art 12 Abs 1 GG liegt dann nicht vor, wenn ein Berufsgeheimnis für die Ausübung des Berufes nicht erforderlich ist. Hierbei ist über die geforderten Merkmale der sinnvollen und bestimmungsgemäßen Ausübung nachzudenken. Gemeint sein kann damit nur ein erforderliches Vertrauensverhältnis, ohne dessen Existenz dem Berufsgeheimnisträger die Ausübung seiner Tätigkeit unmöglich ist. Die Existenz des Berufsgeheimnisses muss für den Berufsgeheimnisträger somit elementar sein. Das bedeutet im Umkehrschluss jedoch nicht, dass nicht auch verschiedene Abstufungen möglich sind. Mag es bei mehreren Berufen auf entsprechende Vertrauensverhältnisse ankommen, so können diese im einen Beruf wichtiger und im anderen unwichtiger sein. Daraus folgt, dass es in der konkreten einfachgesetzlichen Ausgestaltung des Berufsgeheimnisträgerschutzes Unterschiede ergeben können. Hierbei kann ein Unterschied auch dadurch gerechtfertigt sein, dass weitere Grundrechte ergänzend hinzutreten.

¹³² Scholz in Maunz/Dürig, GG, Art 12, Rz 1.

¹³³ Ruffert in BeckOK, GG, Art 12, Rz 17 mwN.

¹³⁴ Dazu Henssler, Das anwaltliche Berufsgeheimnis, NJW 1994, 1817, 1819.

¹³⁵ BVerfG NJW 1975, 588, 589 zum fehlenden Zeugnisverweigerungsrecht für Tierärzte. Dabei verneinte das BVerfG, dass einem Tierarzt ein Zeugnisverweigerungsrecht zustehen müsse, da er seinen Beruf auch ohne ein solches problemlos ausüben könne.

Da es sich bei Art 12 GG um ein sogenanntes „Deutschengrundrecht“¹³⁶ handelt, können sich Ausländer grundsätzlich nicht hierauf berufen.¹³⁷ Personen, die nicht Deutsche sind, steht ein entsprechender Schutz auf Grund der allgemeinen Handlungsfreiheit (Art 2 Abs 1 GG) zu, welcher jedoch im Ergebnis leichter eingeschränkt werden könnte.¹³⁸

4.2. Art 5 Abs 1 S 2 GG – Presse- und Rundfunk und Filmfreiheit

Bei Berufen mit Medienbezug tritt ein weiteres Grundrecht ergänzend hinzu. Das Berufsgeheimnis der Medienmitarbeiter geht in Deutschland hierbei auf Art 5 Abs 1 S 2 GG zurück. Dieser schützt die Presse-, Rundfunk-, und Filmfreiheit.

Der Presse- und Rundfunkfreiheit kommt für eine demokratische Gesellschaft eine enorme Bedeutung zu. Presse und Rundfunk erfüllen in einer solchen Gesellschaft eine wichtige Überwachungs- und Kontrollfunktion aus deren Informationen der Bürger zur Meinungsbildung notwendige Erkenntnisse ziehen kann, die sich letztlich auch auf dessen Wahlentscheidung und Teilhabe am politischen Leben auswirken können.¹³⁹

Wer unter den persönlichen Schutzbereich der Pressefreiheit fällt, wird durch den Wortlaut des Grundrechts nicht explizit ausgesagt.¹⁴⁰ Träger des Grundrechts können sowohl natürliche als auch juristische Personen¹⁴¹ sein.¹⁴² Hierbei kommt es nicht darauf an, ob es sich um professionelle Journalisten oder um „Amateure“ handelt.¹⁴³ Der Pressebegriff des Art 5 Abs 1 S 2 GG ist sehr weit und entwicklungs offen.¹⁴⁴ Er

¹³⁶ Hierbei ist nicht unbedingt auf die Staatsbürgerschaft abzustellen. Vielmehr sind Deutsche im Sinne des Grundgesetzes in Art 116 GG definiert. Hierunter können auch Personen fallen, die über keine deutsche Staatsbürgerschaft verfügen (sog „Statusdeutsche“); vgl zusammenfassend *Hillgruber* in BeckOK, GG, Art 116, Rz 5 ff.

¹³⁷ Dies ist bei EU-Ausländern umstritten; vgl *Ruffert* in BeckOK, GG, Art 12, Rz 35 ff. Sie sind Deutschen (nach Art 116 GG) aber jedenfalls gleich zu stellen.

¹³⁸ Bei EU-Bürgern, sofern man sie nicht direkt in den Schutzbereich des Art 12 GG einbezieht, muss der Schutzbereich dem des Art 12 GG vollumfänglich entsprechen.

¹³⁹ *Herzog* in Maunz/Dürig, GG, Art 5, Rz 118.

¹⁴⁰ *Schemmer* in BeckOK, GG, Art 5, Rz 38.

¹⁴¹ Nach Maßgabe von Art 19 Abs 3 GG.

¹⁴² *Schemmer* in BeckOK, GG, Art 5, Rz 39.

¹⁴³ *Herzog* in Maunz/Dürig, GG, Art 5, Rz 162; Sodann in Sodann, GG, Art 5, Rz 19.

¹⁴⁴ *Bethge* in Sachs, Grundgesetz⁶, Art 5, Rz 68; vgl zu einer restriktiven Auslegung und zur Kritik hieran *Herzog* in *Herzog* in Maunz/Dürig, GG, Art 5, Rz 127 f.

reicht von klassischen Druckerzeugnissen über Datenträger bis hin zu Online-Medien,¹⁴⁵ wie etwa Blogs.¹⁴⁶ Geschützt ist das ungehinderte Beschaffen und Verbreiten von Informationen¹⁴⁷ unabhängig davon, ob es sich dabei um reine Berichterstattung oder um Meinungsäußerung handelt.¹⁴⁸ Bei Berichterstattung über Tatsachen sind denklogisch nur wahre Tatsachenbehauptungen geschützt, da die Verbreitung unrichtiger Informationen nicht zum Prozess der Meinungsbildung beitragen soll.¹⁴⁹

Die Pressefreiheit garantiert folglich auch die Unabhängigkeit des Journalismus; Medienmitarbeiter sollen dabei nicht gezwungen sein, ihre Quellen offenzulegen.¹⁵⁰ Wird die Telekommunikation von Journalisten überwacht, so liegt nicht nur ein Eingriff in Art 10 oder Art 2 Abs 1 iVm Art 1 Abs 1 GG vor, sondern es ist zugleich auch Art 5 Abs 1 S 2 GG betroffen.¹⁵¹ Beide Grundrechte stehen also in Idealkonkurrenz nebeneinander.

Vom Schutzbereich der Rundfunkfreiheit, deren Gewährleistung ebenso umfassend ist wie der der Presse, ist jede Übermittlung von Gedankeninhalten mittels elektromagnetischer Wellen umfasst.¹⁵² Diese Definition, die noch aus Zeiten stammt, wo Rundfunk ausschließlich über analoges Antennenfernsehen empfangen werden konnte, wirkt aus heutiger Sicht etwas eng bzw unzeitgemäß.¹⁵³ Auch wenn die Verbreitung über DVB-T, Fernseekabel und SAT-Technik heutzutage noch der Schwerpunkt bilden, so ist der Übertragungsweg nicht auf die Definition beschränkt, sondern kann auch

¹⁴⁵ Vgl zur Entwicklung und der nunmehr immer schwieriger werdenden Abgrenzung zwischen Presse und Rundfunk; *Neuhoff*, Die Dynamik der Medienfreiheit am Beispiel von Presse und Rundfunk, ZUM 2012, 371, 374 f; dadurch kommt es zu presserechtlichen Problemen, wie etwa bei der „Tagesschau-App“ der ARD, vgl LG Köln ZUM-RD 2012, 613; diese Probleme sind jedoch nicht von verfassungsrechtlicher Relevanz.

¹⁴⁶ Vgl *Schemmer* in BeckOK, GG, Art 5, Rz 43 mwN.

¹⁴⁷ *Schemmer* in BeckOK, GG, Art 5, Rz 44 ff.

¹⁴⁸ *Herzog* in Maunz/Dürig, GG, Art 5, Rz 134.

¹⁴⁹ *Sodann* in Sodann, GG, Art 5, Rz 4 mit Verweis auf BVerfGE 54, 208, 219; 85, 1, 15; es kommt jedoch nicht auf die „Seriosität“ des Presseerzeugnisses an; vgl *Sodann* in Sodann, Art 5, Rz 16 mit Verweis auf BVerfGE 34, 269, 283.

¹⁵⁰ *Polenz* in Kilian/Heussen, Computerrechtshandbuch¹⁶, Teil 13, Rz 45.

¹⁵¹ BVerfG NJW 2003, 1787 = ZUM-RD 2003, 284, 295.

¹⁵² *Herzog* in Maunz/Dürig, GG, Art 5, Rz 195.

¹⁵³ Im Übrigen ist die Definition auch etwas missverständlich, da sie auf viele technische Sachverhalte anwendbar ist, die allein durch Art 10 Abs 1 GG geschützt sind.

neuartige Methoden (wie etwa Verbreitung über das Internet) umfassen. Der Rundfunkbegriff ist damit ähnlich technikoffen, wie etwa der Pressebegriff.¹⁵⁴

In der Rechtsprechung hat sich mit der Zeit ein Katalog von geschützten Tätigkeiten herausgebildet, die das BVerfG als vom Redaktionsgeheimnis umfasst bzw nicht umfasst ansieht. Aus dieser Rechtsprechung ergibt sich ein klares Bild, welches verfassungsgerichtlich vom Redaktionsgeheimnis besteht und damit die Vorgaben, welche einfachgesetzlich bei verfassungskonformer Auslegung von Normen zu beachten sind.

Hierbei hat das BVerfG vor allem die folgenden Grundsätze entwickelt: Was ein Journalist durch Täuschung in rechtswidriger Weise erlangt, unterfällt dem Redaktionsgeheimnis im Regelfall nicht.¹⁵⁵ Das Redaktionsgeheimnis soll also nicht als Feigenblatt verwendet werden können, um rechtswidrige Handlungen zu ermöglichen oder im Nachhinein zu verdecken. Inhaltlich gesehen, ist das Redaktionsgeheimnis sehr weit auszulegen. So sind etwa Daten, die zum Organisationsablauf eines Rundfunksenders gehören, aus denen sich Rückschlüsse auf den Namen einzelner Redakteure, die von ihnen bearbeiteten Ressorts und einzelne redaktionelle Abläufe ergeben, durch Redaktionsgeheimnis geschützt.¹⁵⁶ Ferner geht das Gericht davon aus, dass das Redaktionsgeheimnis nicht nur für die „klassischen“ Printmedien gilt. Die Pressefreiheit und damit auch das Redaktionsgeheimnis gelten damit etwa auch für Werkszeitungen¹⁵⁷ oder Blogs.¹⁵⁸ Weiters betrifft das Redaktionsgeheimnis auch Adressen von Kontaktpersonen. Verschafft sich also der Staat durch eine Durchsuchung von Redaktionsräumen oder auf sonstige Weise Kenntnis – denkbar ist also auch ein rein digitaler Zugriff von außen – über die Kontakte, so ist stets das Redaktionsgeheimnis betroffen. Zum einen,

¹⁵⁴ *Sodann* in Sodann, GG, Art 5, 21; so fallen unter den Begriff Rundfunk zum Beispiel auch Erscheinungsformen wie etwa PayTV oder Teletext.

¹⁵⁵ BVerfG NJW 1984, 1741, 1743; hierbei widersprach das BVerfG dem BGH, der angenommen hatte, dass dies möglich sei; BGH NJW 1981, 1089, 1091.

¹⁵⁶ BVerfG ZUM-RD 2001, 142, 144.

¹⁵⁷ BVerfG NJW 1997, 386, 387.

¹⁵⁸ Vgl hierzu *Stadtler*, <http://www.internet-law.de/2010/11/redaktionsgeheimnis-und-quellenschutz-auch-fur-blogger.html>.

weil potentielle Informanten in Zukunft abgeschreckt werden und zum anderen, weil dadurch die Identität von Informanten aufgedeckt werden kann.¹⁵⁹

Aus der Gesamtschau der Rechtsprechung ergibt sich, dass im Verfassungsrecht von einem sehr starken Schutz des Redaktionsgeheimnisses ausgegangen wird. Hervorzuheben ist hierbei der Informantenschutz, der als einer der Hauptbestandteile des Redaktionsgeheimnisses, im einfachen Recht einer entsprechenden Umsetzung bedarf, welche vor allem im strafprozessualen Bereich eine Rolle spielen wird.

4.3. Art 4 Abs 1 und 2 GG – Religionsfreiheit

Das Beicht- und Seelsorgegeheimnis wird verfassungsrechtlich durch das Grundrecht auf Religionsfreiheit in Art 4 Abs 1 und 2 GG geschützt. Dabei sind in den meisten Fällen auch die Artikel der Weimarer Reichsverfassung, welche sich auf die Kirchen beziehen (Art 136 bis 141 WRV), die gemäß Art 140 GG Bestandteil des Grundgesetzes sind, betroffen.¹⁶⁰ Art 4 Abs 1 und 2 GG sind hierbei nicht nur als Abwehrrechte dem Staat gegenüber zu verstehen, sondern begründen gerade auch staatliche Schutzpflichten.¹⁶¹

Hierbei billigen Rechtsprechung und Lehre Beichtgesprächen oder Gesprächen mit Beichtcharakter einen hohen Schutz zu. Nach der Rechtsprechung des BVerfG gehören die Inhalte solcher Gespräche „zum verfassungsrechtlichen Menschenwürdegehalt der Religionsausübung“.¹⁶² Eine Beschränkung dergestalt, dass sich eine Person nicht sicher sein kann, ob ein seelsorgerisches Gespräch Ziel staatlicher Überwachung

¹⁵⁹ BVerfG NJW 2007, 117, 1178 – „Cicero“.

¹⁶⁰ Die sogenannten Kirchenartikel der WRV wurden, da man sich auf keine anderes Staatskirchenrecht einigen konnte, in das Grundgesetz inkorporiert und sind damit vollgültiges Verfassungsrecht; vgl *Germann* in BeckOK, GG, Art 140, Rz 3 mwN. Alle anderen Artikel der WRV galten nach Verkündung des GG als einfaches Bundesrecht fort, sofern sie dem GG nicht widersprachen. Mittlerweile gilt nur noch Art 109 Abs 3 S 2 WRV als einfaches Bundesrecht fort, der regelt, dass Adelsbezeichnungen als Teil des Namens gelten und nicht mehr verliehen werden dürfen.

¹⁶¹ Sodann in *Sodann*, GG, Art 4, Rz 11a; *Morlok* in Dreier, Grundgesetz³, Art 4, Rz 103 ff.

¹⁶² Dies stellte das BVerfG in seiner Entscheidung zum großen Lauschangriff dar; BVerfGE 109, 279, 322; vgl zum sog „Lauschangriff“ in Österreich auch Miklau / Pilnacek, Optische und akustische Überwachungsmaßnahmen und organisierte Kriminalität („Lauschangriff“) – Paradigmenwechsel im Verfahrensrecht, JRP 1997, 286.

sein, wird mithin immer einen Eingriff in das Grundrecht auf Religionsfreiheit darstellen.¹⁶³

Der Schutzbereich des Art 4 GG umfasst freilich nur seelsorgerisches Handeln, wobei die Abgrenzung zu nicht-seelsorgerischem Handeln sich in der Praxis oft als schwierig erweist.¹⁶⁴ Da die Abgrenzung manchmal nicht möglich ist wird man in Zweifelsfällen eher davon auszugehen haben, dass ein Eingriff vorliegt.

4.4. Art 13 Abs 1 GG – Grundrecht auf Unverletzlichkeit der Wohnung

Die Unverletzlichkeit der Wohnung ist in Art 13 GG geregelt. Hierbei handelt es sich um ein „Abwehrrecht zum Schutz der räumlichen Privatsphäre“.¹⁶⁵ Der Begriff ist weit zu fassen und schließt neben allen möglichen Arten von Wohnstätten, wie etwa Wohnräumen, Hotelzimmern, Wohnwägen und ähnlichem, auch Arbeitsräume und Werkstätten,¹⁶⁶ die nicht allgemein zugänglich sind.¹⁶⁷ Geschützt ist im Prinzip nicht die Wohnstätte selbst im Sinne eines Schutzes des Besitzrechts an dieser, sondern die Privatheit des Einzelnen.¹⁶⁸ Können Geschäftsräume ungehindert betreten werden, gilt ein abgeschwächter Schutz.¹⁶⁹

Insofern ist bei jedem staatlichen Einschreiten im Bereich von Geschäftsräumlichkeiten von Berufsheimnisträgern der Schutzbereich des Art 13 GG zunächst eröffnet.

¹⁶³ Polenz in Kilian/Heussen, Computerrechtshandbuch¹⁶, Teil 13, Rz 44.

¹⁶⁴ Fishedick, Das Beicht- und Seelsorgegeheimnis, Zur Legitimation und Reichweite der Zeugnisverweigerungsrechte für Geistliche, DÖV 2008, 584, 590.

¹⁶⁵ Papier in Mainz/Dürig, GG, Art 13, Rz 1.

¹⁶⁶ Und umfriedetes Besitztum, wie etwa Gärten, etc, welches dazugehört; vgl Hermes in Dreier, Grundgesetz³, Art 13, Rz 19.

¹⁶⁷ Papier in Mainz/Dürig, GG, Art 13, Rz 10.

¹⁶⁸ Hermes in Dreier, Grundgesetz³, Art 13, Rz 13 mit Verweis auf BVerfGE 89, 1, 12.

¹⁶⁹ Papier in Mainz/Dürig, GG, Art 13, Rz 10.

5. Grundlagen des Berufsgeheimnisträgerschutzes in der GRC

Ebenfalls – zumindest im weiteren Sinne – sind Normen der GRC aus österreichischer Sicht in Bestimmten Konstellationen¹⁷⁰ als Verfassungsrecht anzusehen, da diese auch im Normenkontrollverfahren Prüfungsmaßstab sind.¹⁷¹ Hierbei ist der Vorlagebeschluss des VfGH von Bedeutung, in dem sich dieser mit der möglichen Verletzung der GRC eingehend auseinandersetzt.

Als Schutznorm für Berufsgeheimnisträger kommt Art 7 GRC in Betracht, der Art 8 EMRK entspricht. Insofern kann auf die Ausführungen zu Art 8 EMRK entsprechend Bezug genommen werden. Jedoch ist vielfach nicht klar, ob das Grundrecht genau wie seine Vorlage auszulegen ist. Während sich beim personellen Schutzbereich keine Unterschiede ergeben und das Grundrecht aus Art 7 GRC, ebenso wie Art 8 EMRK, auch auf juristische Personen anwendbar ist, so ist es umstritten, ob der räumliche Schutzbereich identisch ist.

Während der EGMR Art 8 EMRK dergestalt interpretiert, dass dieser auch auf Geschäftsräume anwendbar sein kann, so ist dies im Rahmen von Art 7 GRC stark umstritten.¹⁷² Zwar hatte der EuGH dahingehend in der Vergangenheit eine abweichende Meinung geäußert¹⁷³, fraglich ist jedoch ob diese Ansicht noch haltbar ist und nicht inzwischen selbst vom EuGH verworfen wurde. Dafür spricht zum einen, dass der EuGH schon seit längerem die Tendenz erkennen lässt, dass er seine alte Argumentationslinie nicht mehr aufrechterhalten möchte.¹⁷⁴ Es dürfte davon auszugehen sein, dass sich der EuGH hinsichtlich der Begrifflichkeiten immer stärker der Rechtsprechung des EGMR annähert.¹⁷⁵ Eine ähnliche Auslegung ist hierbei auch aus rechtlicher Sicht

¹⁷⁰ Vgl hierzu später unter 21.1.2.1.

¹⁷¹ Aus diesem Grunde hat der VfGH die österreichische Umsetzung der Vorratsdatenspeicherung auch gem Art 267 AEUV dem EuGH vorgelegt, vgl VfGH vom 28.11.2012, G47/12-11, 59/12-10.

¹⁷² Vgl zum Streitstand *Jarass*, GRC, Art 7, Rz 34.

¹⁷³ EuGH, Rs. 46/87 – Hoechst, Slg.1989, 2859 Rz 18.

¹⁷⁴ EuGH, NJW 2003, 35.

¹⁷⁵ Bislang gab es wohl vor allem was den Schutz von Geschäftsräumlichkeiten angeht unterschiedliche Auffassungen. Während der EuGH hier einen etwas zurückhaltenden Grundrechtsschutz annahm, schloss der EGMR Geschäftsräume in nahezu allen Fällen in den Schutzbereich von Art 8 EMRK ein; näher

geboten: Alle mit der EMRK unmittelbar korrespondierenden Grundrechte sind vom Schutzbereich her wenigstens wie in der EMRK auszulegen (Art 52 Abs 3 GRC).¹⁷⁶

Außerdem hat der EuGH im Rahmen der Entscheidung über die Vorratsdatenspeicherung¹⁷⁷ nicht zuletzt das Recht der Berufsgeheimnisträger gestärkt, indem er fehlende Ausnahmeregelungen für diese bemängelte. Dabei berief er sich auf Art 7 und 8 der GRC.

Gerade das Beispiel der Kommunikation zeigt, dass zwischen Wohn- und Geschäftsräumen schwer unterschieden werden kann und dass Art 7 GRC – auch – eine Norm ist, die Berufsgeheimnisträger bei der Ausübung ihrer Tätigkeit schützt und zwar unabhängig davon, ob sie diese in allein dazu gewidmeten Geschäftsräumen oder in privaten Räumlichkeiten verrichten.

Damit bliebe letztlich nur die Frage offen, ob das Grundrecht auch auf frei zugängliche Geschäftsräume anwendbar ist.¹⁷⁸ Die Beantwortung dieser Frage, ist für Berufe mit Vertraulichkeitsverhältnissen von untergeordneter Bedeutung, weil entsprechende Geschäftsräume nicht unkontrolliert zugänglich sein können, um die Vertraulichkeit überhaupt gewährleisten zu können.

6. Ergebnisse

Der Schutz der Berufsgeheimnisträger kann als weitreichend bezeichnet werden. Er ist in der österreichischen und in der deutschen Rechtsordnung gleichermaßen verankert und betrifft die gleichen Berufsgruppen. Ebenfalls ist beiden Rechtsordnungen ein Umgehungsverbot bekannt. In seiner Ausprägung unterscheiden sich sowohl

hierzu *Breitenlechner/Kneihs/Segalla* in Holoubek/Lienbacher, GRC, Art 7, Rz 16. Es spricht vieles dafür, dass der EuGH seine Rechtsprechung in Zukunft mehr am weiten Schutzbereich des EGMR ausrichten wird. So hat der EuGH den Schutz von Geschäftsräumlichkeiten mittlerweile anerkannt; vgl. EuGH v. 22.10.2002, C-94/00.

¹⁷⁶ *Breitenlechner/Kneihs/Segalla* in Holoubek/Lienbacher, GRC, Art 7, Rz 20.

¹⁷⁷ EuGH v. 8. April C-293/12 und C-594/12, näheres hierzu unter 16.

¹⁷⁸ Dafür etwa *Kingreen* in Calliess/Ruffert, EUV/AEUV⁴, Art 7 GRC, Rz 9; dagegen *Jarass*, GRC, Art 7, Rz 34.

einfachgesetzlich als auch verfassungsrechtlich die beiden Rechtsordnungen nur marginal. Dies mag zunächst als eine schlechte Ausgangsposition für einen Rechtsvergleich gesehen werden, bietet aber die Chance für einen umfassenden Rechtsvergleich, zumal dann, wenn sich bei der Untersuchung der Telekommunikationsüberwachung Unterschiede ergeben.

Ein Berufsgeheimnisträger kann in Österreich oder Deutschland denselben Überwachungsmaßnahmen staatlicher Stellen ausgesetzt sein. Wenn der verfassungsrechtlich gebotene Schutz in beiden Ländern ähnlich ausgestaltet sein muss, lassen sich dadurch auch Erkenntnisse von einem Land auf das andere übertragen. Würde das Verständnis in beiden Ländern stark divergieren, böte sich ein Vergleich nur in stark eingeschränktem Maße an.

Es ist nun nach der Erkenntnis, dass der Schutz der Berufsgeheimnisträger in beiden Ländern vergleichbar ist, zunächst auf die Telekommunikationsüberwachung in technischer und rechtlicher Hinsicht in beiden Ländern einzugehen, bevor dann die Schnittmengen zwischen Berufsgeheimnisträgerschutz und Telekommunikationsüberwachung näher beleuchtet werden können.

Kapitel II – Überwachung von Telekommunikation

Die Überwachung der Telekommunikation ist aus technischer Sicht in verschiedenster Weise möglich. Strafprozessrecht und Polizeirecht machen Ermittlern diese Mittel zum Teil zugänglich. Ebenso divers sind die Grundrechte, in die aufgrund von Überwachungsmaßnahmen eingegriffen werden kann. Diese Variabilität wird umso größer, wenn man diese Thematik im Rechtsvergleich betrachtet. Schließlich sind die technischen Möglichkeiten, welche Ermittlungsbehörden in der Theorie haben, weltweit gleich. Die verfassungsrechtlichen Vorgaben einzelner Länder können sich jedoch ebenso wie die strafprozessuale und polizeirechtliche Umsetzung stark unterscheiden.

Auch wenn auf den ersten Blick zwischen Deutschland und Österreich nicht viele Unterschiede bestehen, so offenbaren sich diese letztlich in kleinen aber entscheidenden Nuancen. Hierbei kann der Rechtsvergleich für beide Rechtsordnungen dienlich sein, um eine vielleicht festgefahrene Interpretation in beiden Ländern neu zu überdenken. Hierbei ist – vor allem in Hinblick auf das Fernmeldegeheimnis – der Rechtsvergleich nicht als juristische Einbahnstraße zu sehen, bei der die Interpretation der einen Rechtsordnung auf die andere Rechtsordnung übertragen wird, sondern vielmehr als eine Art Rechtsdialog, bei dem beide Rechtsordnungen voneinander lernen können.

7. Einzelne Überwachungsmaßnahmen

Die Möglichkeiten der Überwachung im Bereich der Telekommunikation sind zahlreich und reichen von Maßnahmen, die auf den Inhalt der Gespräche oder Nachrichten gerichtet sind, bis hin zu gezielter Abfrage von Verbindungsdaten, wobei die Aufstellung zeigen wird, dass letztere Maßnahmen durchaus zahlreicher und vielfältiger sind. Die technische Erläuterung der Maßnahmen ist aber auch in juristischer Hinsicht bedeutend, da nur auf diese Weise nachvollzogen werden kann, in welche Grundrechte überhaupt ein Eingriff erfolgt, da dies je nach Art der Maßnahme abweichen kann, obwohl oftmals die gleichen Daten betroffen sind.

7.1. Technische Beschreibung von digitalen Überwachungsmaßnahmen

Nur durch eine kurze technische Beschreibung der einzelnen Vorgänge lassen sich die Maßnahmen entsprechend dem oben entwickelten Schema einordnen. Auch wenn sich viele Überwachungsmaßnahmen ähneln, so sind doch oft unterschiedliche Grundrechte betroffen. Aus diesem Grund sind zunächst einzelne Überwachungsmaßnahmen in technischer Hinsicht zu erläutern, um diese im Nachhinein in (grund-)rechtlicher Hinsicht analysieren zu können.

Während einige Überwachungsmaßnahmen auf den Inhalt der Kommunikation gerichtet sind, richten sich andere auf sog Verkehrsdaten, die zusätzlich zur Kommunikation anfallen. Der Begriff der Verkehrsdaten ist etwa in Österreich in § 92 Z 4 TKG näher definiert. Dies sind solche Daten, „die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden.“ Mithin sind dies alle Daten die bei der Übermittlung anfallen, außer die Nachricht selbst, also etwa Rufnummern, Mailadressen, IP-Adressen, etc. Hiervon abzugrenzen sind Inhaltsdaten (§ 92 Z 5 TKG), die allein auf den Inhalt der Nachricht¹⁷⁹ abstellen. Nach Definition des Gesetzgebers in Deutschland sind Verkehrsdaten alle Daten, „Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden“ (§ 3 Z 30 dTKG). Dies ist im Ergebnis das Gleiche,¹⁸⁰ so dass Verkehrsdaten in beiden Rechtsordnungen synonym verwendet werden kann.

Nachfolgend soll auf die „gängigsten“ Überwachungsmaßnahmen eingegangen werden. Teilweise werden diese Überwachungsmaßnahmen in Österreich und Deutschland angewandt, zum Teil finden die Überwachungsmaßnahmen auch nur in Deutschland Anwendung. Überwachungsmaßnahmen, die nur in Österreich zum Einsatz kommen, gibt es zurzeit nicht. Im Nachgang an die Erläuterung sollen die Überwachungsmaßnahmen ihren gesetzlichen Grundlagen in beiden Ländern zugeordnet werden.

¹⁷⁹ Nachricht ist hierbei nach § 92 Z 7 TKG jeder Inhalt die mittels Telekommunikation ausgetauscht wird. Es sind also sowohl Text- als auch Sprachnachrichten, sowie Bildnachrichten erfasst. Es spielt somit keine Rolle, in welcher Form die Nachricht verkörpert ist.

¹⁸⁰ Vgl zum Begriff der Verkehrsdaten im deutschen TKG *Graf* in BeckOK StPO, § 4, Rz 20.

7.1.1. „Stummes SMS“

Mittels „stummes SMS“ (oftmals auch als „stilles SMS“ oder „verdecktes SMS“¹⁸¹ bezeichnet und in der Polizeipraxis auch als „Ortungsimpuls“¹⁸² bekannt) haben Ermittler die Möglichkeit den Standort von Mobiltelefonen bestimmen.¹⁸³ Dabei wird an eine den Ermittlern bekannte Mobilfunknummer, ähnlich wie bei einem normalen SMS¹⁸⁴, ein Signal von einem Computer oder Mobilgerät der Ermittler gesendet; ist das Handy eingeschaltet, fallen Verbindungsdaten an, über die auch der Standort bestimmt werden kann.¹⁸⁵ Diese Verbindungsdaten können wiederum abgefragt werden. Die Genauigkeit der Standortbestimmung liegt hierbei zwischen 500 m bis hin zu 50 m.¹⁸⁶

Der Inhaber des Mobiltelefons bekommt von diesem Vorgang nichts mit, da ein akustisches oder sonstiges Signal, wie bei einem normalen SMS üblich, nicht erfolgt.¹⁸⁷ Werden in kurzen Abständen stumme SMSen verschickt, können ohne großen Aufwand Bewegungsprofile erstellt werden.¹⁸⁸ Nicht erforderlich ist es hierbei, dass der Überwachte selbst mit seinem Mobiltelefon kommuniziert.¹⁸⁹

Diese Überwachungsmaßnahme hat extrem hohe praktische Relevanz. Nach Auskunft des deutschen Bundesinnenministeriums wurden im Jahr 2008 vom Bundeskriminalamt 96.314, vom Bundesamt für Verfassungsschutz 107.852 und vom Zoll 236.617

¹⁸¹ Vgl. *Eisenberg/Singelstein*, NStZ 2005, 62, Fn. 3.

¹⁸² *Smith*, Kurzer Zwischenstand zu Recht und Praxis der "stillen SMS", VR 2012, 334.

¹⁸³ Kurze Zusammenfassung bei *Graf* in BeckOK StPO, § 100a, Rz 132f.; vgl. auch <http://derstandard.at/2000012472104/Stille-SMS-Ein-Perfektes-Tool-fuer-Ueberwachung>.

¹⁸⁴ Jedoch gibt es in technischer Hinsicht noch einige Unterschiede zur normalen SMS, vgl. *Krüger*, ZJS 2012, 606.

¹⁸⁵ *Eisenberg/Singelstein*, Zur Unzulässigkeit der heimlichen Ortung per „stiller SMS“, NStZ 2005, 62.

¹⁸⁶ *Tiedemann*, Die „stille SMS“ – Überwachung im Mobilfunk, K&R, 63, 64.

¹⁸⁷ Vgl. *Smith*, Kurzer Zwischenstand zu Recht und Praxis der "stillen SMS", VR 2012, 334 mwN. Für Mobiltelefone mit Betriebssystem Android kann die Open-Source-Software SnoopSnitch heimliche Maßnahmen aber erkennen (<https://opensource.srlabs.de/projects/snoopsnitch/wiki/Wiki>); vgl. hierzu <http://derstandard.at/2000009821924/31c3-App-snoopSnitch-spaecht-Handyueberwachung-aus>. Die Applikation erkennt ebenfalls IMSI- und IMEI-Catcher. Eine vergleichbare Applikation für andere Betriebssysteme gibt es allerdings nicht.

¹⁸⁸ *Singelstein*, Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co, NStZ 2012, 593, 601.

¹⁸⁹ *Tiedemann*, Die „stille SMS“ – Überwachung im Mobilfunk K&R, 63, 64.

„stumme SMS“ versendet.¹⁹⁰ Im Rahmen dieser Zahlen ist die „alltägliche“ Polizeiarbeit durch die Polizei der Länder nicht einmal berücksichtigt. Die Bundesländer führen darüber zumeist nur ungenaue Statistiken. Im gleichen Jahr wurden zur präventiven und repressiven Polizeiarbeit 610.323 Ortungsimpulse verschickt, wobei die Tendenz in den darauffolgenden Jahren leicht steigend ist.¹⁹¹

7.1.2. IMSI-Catcher

Ein IMSI-Catcher kommt zum Einsatz, um lokal an einem Punkt vorhandene Geräte zu ermitteln.¹⁹² Bei der IMSI (Abkürzung für International Mobile Subscriber Identity) handelt es sich um eine Nummer, die weltweit einmalig an eine jeweilige SIM-Karte vergeben ist.¹⁹³

Der IMSI-Catcher simuliert dabei eine Funkzelle und macht sich damit, ebenso wie das stumme SMS, zu Nutze, dass die meisten Mobiltelefone im Stand-by-Modus sind. Das Mobiltelefon ist immer in der jeweils nächsten Funkzelle angemeldet über die sich das stärkste Signal beziehen lässt. Meldet sich das Telefon in der Funkzelle an, die der Catcher simuliert, kann durch einen IMSI-Request die IMSI der SIM-Karte des Gerätes offengelegt werden.¹⁹⁴

Der IMSI-Catcher ermöglicht es zudem auch, sämtliche Telefongespräche weiter zu vermitteln, so dass er sich quasi bei bestehenden Mobilfunkverbindungen dazwischenschaltet und damit auch ähnlich einem Mobiltelefon agieren kann; dies ermög-

¹⁹⁰ Antwort Bundesministerium des Innern, auf Anfrage des Abgeordneten Hunko, Arbeitsnr. 11/339, 340.

¹⁹¹ BayLT-Drs. 16/11003, 2. Im Jahr 2011 wurden allein im Zeitraum 1. Jänner bis 1. Dezember 747.526 „stumme SMS“ verschickt. Hierbei wurden 2011 3.466 Mobilfunkanschlüsse überwacht, so dass bei der Menge an Ortungsimpulsen, gut 215 pro Anschluss, von der Erstellung detaillierter Bewegungsprofile auszugehen ist. Nicht klären lässt sich im Übrigen, wie viele Ermittlungsverfahren der Überwachungsmaßnahme zu Grunde liegen, da die Daten laut Bayerischem Landeskriminalamt weniger der rechtsstaatlichen Dokumentation sondern vielmehr Abrechnungszwecken dienen.

¹⁹² Graf in BeckOK StPO, § 100a, Rz 122, vgl. Zum Einsatz im präventiven Bereich Huber-Lintner, .SIAK-Journal, 36, 39.

¹⁹³ Eisenberg, StPO, Rz 2507f.

¹⁹⁴ Details bei Eisenberg, StPO, Rz 2507 f.

licht, auch wenn dies nicht beabsichtigt sein mag, in letzter Konsequenz also auch das Mithören von Gesprächen.¹⁹⁵

7.1.3. IMEI-Catcher

Der IMEI-Catcher funktioniert technisch auf gleiche Weise wie der IMSI-Catcher und ermittelt jedoch anstatt der IMSI der SIM-Karte die IMEI (Abkürzung für International Mobile Subscriber Identity) des jeweiligen Gerätes.¹⁹⁶ Hierbei handelt es sich um eine Nummer, welche weltweit einzigartig einem bestimmten mobilen Endgerät zugewiesen ist und demzufolge nicht wie eine SIM-Karte einfach gewechselt werden kann.¹⁹⁷

Mit IMSI und IMEI verknüpft werden können auch Internetverbindungsdaten, die bei der Überwachung von Smartphones anfallen.¹⁹⁸ Dies lässt eine Analyse des Nutzerverhaltens eines bestimmten Gerätes bzw einer bestimmten SIM-Karte zu und damit auf den Benutzer des Gerätes und / oder der SIM-Karte schließen.

7.1.4. Abhören von Gesprächen

Als einzige Überwachungsmaßnahme zielt das Abhören von Gesprächen von Gesprächsteilnehmern, sei es im Rahmen von Festnetz- oder Mobilfunkgesprächen oder bei VOIP-Telefonie, direkt auf den Inhalt der Kommunikation ab. Hierbei geht der Trend dazu, dass vermehrt Telefongespräche außerhalb der eigenen Wohnung geführt werden, was früher technisch nicht möglich war.¹⁹⁹

¹⁹⁵ Gercke, MMR 2003, 453; hierzu auch kritisch *Regenfelder*, Ermittlungsmaßnahmen bei neuen Informationstechnologien im Spannungsverhältnis zum Grundrechtsschutz, 86.

¹⁹⁶ *Eisenberg*, StPO, Rz 2507f.

¹⁹⁷ Die IMEI eines jeden Gerätes kann mit der Tastenkombination *#06# abgefragt werden und Details zu der jeweiligen IMEI sind in öffentlichen Datenbanken frei zugänglich, vgl <https://www.numberingplans.com/?page=analysis&sub=imeinr> . Das Ändern der IMEI ist mit entsprechender Software möglich und in einigen Ländern (z B dem Vereinigten Königreich) strafbar, vgl Sec. 1 Mobile Telephones (Re-programming) Act 2002.

¹⁹⁸ *Kolb*, Jahrbuch Datenschutzrecht, 237, 249.

¹⁹⁹ Vgl zum Verhältnis *Gurlit*, Verfassungsrechtliche Rahmenbedingungen des Datenschutzes, NJW 2010, 1035, 1037.

7.1.5. E-Mail- und Textnachrichtenüberwachung

Im Rahmen der E-Mail-Überwachung und der Überwachung von SMSen und sonstigen Textnachrichten sind zwei Szenarien denkbar, die sich technisch voneinander unterscheiden. Zum einen kann auf ein bereits heruntergeladenes E-Mail am Endgerät des Betroffenen zugegriffen werden.²⁰⁰ Die Überwachung kann aber bereits früher, außerhalb des direkten Herrschaftsbereichs des Empfängers oder Absenders, auf dem Server des E-Mailproviders stattfinden.²⁰¹

Unter Umständen kann, zum Beispiel bei der reinen Nutzung von Webmailern, auch gar keine endgültige Übertragung auf den Rechner des Überwachten erfolgen, was letztlich zu unterschiedlichen rechtlichen Bewertungen und zu Schwierigkeiten bei der Bestimmung des grundrechtlichen Schutzes führen kann.²⁰²

7.1.6. Quellen-Telekommunikationsüberwachung

Unter Quellen-Telekommunikationsüberwachung (kurz: Quellen-TKÜ) fallen sämtliche Überwachungsmethoden, die am Endgerät (PC, Smartphone, etc) des Nutzers ansetzen und nicht auf den Telekommunikationsvorgang selbst gerichtet sind. Die Technik wurde in Deutschland unter den Begriffen „Bundes-“ bzw „Landestrojaner“ bekannt.²⁰³ Hierbei wird von den Ermittlern auf dem Endgerät des Verdächtigen eine Software installiert,²⁰⁴ die den Ermittlern Zugriff auf Inhalte auf dem Endgerät erlaubt.²⁰⁵

Dabei sind verschiedenste Formen der Überwachung möglich. Zum einen können Screenshots von Bildschirminhalten²⁰⁶ angefertigt oder etwa am Mikrophon gesproche-

²⁰⁰ Wie etwa im Fall VGH Kassel, WM 2009, 2004.

²⁰¹ Wie etwa im Fall BVerfG MMR 2009, 673.

²⁰² Park, Durchsuchung und Beschlagnahme³, Rz 809 ff.

²⁰³ Vgl Albrecht/Dienst, JurPC Web-Dok. 5/2012, Rz 4.

²⁰⁴ Die Installation kann dabei entweder von außen erfolgen, indem z B der Verdächtige durch einen Link oder ähnliches dazu verleitet wird, sich die Software selbst herunterzuladen oder auch dadurch, dass sich die Ermittler selbst kurzzeitig Zugriff auf das Endgerät verschaffen und die Software installieren.

²⁰⁵ Albrecht/Dienst, JurPC Web-Dok. 5/2012, Rz 4.

²⁰⁶ Vgl hierzu den Fall des LG Landshut MMR 2011, 690 mit Anmerkung Bär; dazu auch Albrecht, Rechtswidrige Online-Durchsuchung durch das Bayerische Landeskriminalamt, JurPC Web-Dok. 59/2011.

nes aufgezeichnet werden²⁰⁷. Diese Überwachungsmethode erlaubt auch die Überwachung von Kommunikationsvorgängen, deren Kontrolle sich auf Grund von Verschlüsselungstechniken schwierig gestalten würde, weil die Kommunikation auf dem Endgerät stets in unverschlüsselter Form vorliegt. Somit handelt es sich bei der Quellen-TKÜ um eine besonders einschneidende Überwachungsmethode.

7.1.7. Online-Durchsuchung

Von der klassischen Quellen-TKÜ zu unterscheiden ist die Online-Durchsuchung. Hierfür benötigt man ebenfalls einen staatlichen Trojaner, der jedoch nicht darauf ausgelegt ist, Bildschirmfotos oder Aufnahmen anzufertigen, sondern vielmehr bestehende Inhalte auf dem Computer durchzusehen, ohne dass der Überwachte davon Kenntnis erlangt.²⁰⁸ Es ist unerheblich ob die Infizierung des Computers des Verdächtigen hierzu mittels einer (heimlichen) Installation vor Ort erfolgt oder diese ebenfalls über das Internet, etwa durch den Versand einer E-Mail mit Anhang, die der Verdächtige dann öffnet, geschieht.²⁰⁹

Damit hat die Online-Durchsuchung mit der klassischen Quellen-TKÜ das technische Einsatzmittel gemeinsam; zudem setzen beide Überwachungsmethoden an der Quelle, nämlich am Endgerät des Überwachten, an. Jedoch ist die Online-Durchsuchung eine noch einschneidendere Maßnahme, da durch sie quasi die gesamten Inhalte des Endgerätes für die Ermittler zugänglich sind.

7.1.8. Vorratsdatenspeicherung

Bei der Vorratsdatenspeicherung handelt es sich im Grunde nicht um eine zusätzliche Überwachungsmaßnahme im technischen Sinne. Im Rahmen der Vorratsdatenspeicherung werden jedoch Verbindungsdaten von sämtlichen Nutzern von Telekommunikation über einen längeren Zeitraum auf Vorrat gespeichert, so dass den Ermittlern im Falle von anderen Überwachungsmaßnahmen eine erheblich größere Menge an

²⁰⁷ LG Landshut MMR 2011, 690, 691.

²⁰⁸ *Braun/Roggenkamp*, Ozapftis - (Un)Zulässigkeit von "Staatstrojanern", K&R 2011, 681; Definition etwas zu weit bei *Pilnacek/Pscheidl*, Das Strafverfahren und seine Grundsätze (Teil I), ÖJZ 2008, 629, 633.

²⁰⁹ Näher *Park*, Durchsuchung und Beschlagnahme³, Rz 794.

Daten zur Verfügung steht. Verbindungsdaten sollen also damit nicht nach Rechnungserstellung gelöscht werden, sondern darüber hinaus aufbewahrt werden.

Da im Rahmen der Vorratsdatenspeicherung Verbindungsdaten der gesamten Bevölkerung gespeichert werden und damit auch automatisch Daten, die Berufsgeheimnisse betreffen, hat diese auch im Rahmen des verfassungsrechtlichen Spannungsfeldes eine enorme Relevanz. Vorliegend sollen daher kurz die rechtsgeschichtlichen Grundlagen der Vorratsdatenspeicherung auf europäischer Ebene erläutert werden.²¹⁰

7.1.9. Abfrage von Kundendaten

Ferner ist eine Form der Telekommunikationsüberwachung beim Anbieter von Telekommunikationsdienstleistungen allgemein die Daten seiner Kunden abzufragen. Im Gegensatz zur Vorratsdatenspeicherung wird man bei einer solchen Abfrage nicht wissen, über welchen Zeitraum diese Daten vorliegen und welche Daten genau vorliegen.²¹¹ So werden die abgefragten Daten zumeist neuer sein, da diese nicht beliebig vom Provider vorgehalten werden (dürfen). Neben Anfragen eher allgemeiner Natur existieren auch Spezialfälle der Abfrage von Kundendaten, die spezielle Überwachungsmaßnahmen darstellen: die Funkzellenabfrage und die Rufdatenrück Erfassung.

7.1.9.1. Funkzellenabfrage

Die Funkzellenabfrage beim Betreiber der verschiedenen Funkzellen an. Im Rahmen einer Funkzellenabfrage kann abgefragt werden, welche Mobiltelefone zu einem bestimmten Zeitraum in einer bestimmten Funkzelle eingebucht waren.²¹² Auf diese Weise kann der Aufenthaltsort eines bestimmten Mobilfunknutzers in einer Funkzelle ermittelt werden, sofern er sein Gerät eingeschaltet bei sich trägt.²¹³ Bei der Kombination von Abfragen verschiedener nah beieinanderliegender Funkzellen ist eine noch genauere Ortung für die Ermittler möglich.

²¹⁰ Zur aktuellen Umsetzung in Deutschland vgl unter 28.3.

²¹¹ Vgl hierzu entsprechende Gesetzgebung in Deutschland dies zu ändern unter 28.2.

²¹² Eisenberg/Singelstein, Zur Unzulässigkeit der heimlichen Ortung per „stiller SMS“, NStZ 2005, 62.

²¹² Graf in BeckOK StPO, § 100a, Rz 125.

²¹³ Nack in Karlsruher Kommentar StPO⁶, § 100i, Rz 5, Singelstein, NStZ 2012, 593, 602.

7.1.9.2. Rufdatenrückfassung / Zielwahlsuche

Auch die Rufdatenrückfassung setzt beim Telekommunikationsbetreiber an. Im Rahmen einer Rufdatenrückfassung wird festgestellt, wer einen bestimmten Anschluss angerufen hat oder von diesem angerufen wurde.²¹⁴ Damit kommt die Rufdatenrückfassung der Zielwahlsuche in Deutschland sehr nahe.²¹⁵

Bei einer Zielwahlsuche, die in der Literatur auch als „elektronische Rasterfahndung“²¹⁶ bezeichnet wurde,²¹⁷ durchsuchen die Ermittler systematisch die Verbindungsdaten eines Telekommunikationsanbieters, um herauszufinden, wer einen bestimmten Anschluss angerufen hat.²¹⁸

7.1.10. Durchsuchung von Endgeräten der Telekommunikation

Ebenfalls besteht die Möglichkeit, durch eine Durchsuchung und Beschlagnahme beim Betroffenen an dessen Endgeräte, wie etwa Smartphones oder Computer, zu gelangen. Diese können wiederum durchsucht werden und damit Aufschluss über die Telekommunikation gewonnen werden. Dabei handelt es sich letztlich um keine Telekommunikationsüberwachungsmaßnahme im engeren Sinne, da Telekommunikation nur auf die Übertragung abzielt. Dennoch stellen sich auch bei dieser Fallkonstellation wichtige Fragen über die verfassungsrechtliche Einordnung von Telekommunikationsdaten, weswegen diese auch vorliegend näher erläutert werden soll.

7.2. Strafprozessuale und sicherheitspolizeiliche Telekommunikationsüberwachung in Österreich

Eben kurz erläuterte Maßnahmen zur Telekommunikationsüberwachung finden sich – zumindest teilweise – in der StPO und im SPG wieder. Für einige der oben erwähnten Überwachungsmaßnahmen fehlt in Österreich eine gesetzliche Grundlage. Sie dürfen daher von Ermittlungsbehörden oder Gerichten nicht angeordnet werden.

²¹⁴ *Fabrizy*, StPO, § 135, Rzz. 3; vgl auch zu den Pflichten des Kommunikationsdiensteanbieters *Brenn*, ECG, § 18, Z 3. Die Rufdatenrückfassung bezieht sich aber im Gegensatz zur Zielwahlsuche nicht nur auf Telefondaten, sondern auch auf IP-Adressen.

²¹⁵ Vgl *Nack* in *Karlsruher Kommentar StPO*⁶, § 100i, Rz 4.

²¹⁶ Diesen Begriff verwendet auch im Zusammenhang mit der Rufdatenrückfassung *Reindl*, JBl 1999, 791, was die Vergleichbarkeit beider Maßnahmen deutlich macht.

²¹⁷ So *Bär*, MMR 2004, 633, 634.

²¹⁸ Vgl *Sankol*, MMR 2008, XVII.

Diese Überwachungsmaßnahmen gibt es teilweise in Deutschland, teilweise wurden sie dort angewandt, ohne dass es dafür eine Rechtsgrundlage gab. Ermittler verhielten sich mithin bewusst rechtswidrig oder überinterpretierten den Wortlaut bestehender Normen.

7.2.1. Auskunft über Stamm- und Zugangsdaten, § 76a StPO

Diese Norm erfasst die Auskunft über Stamm- und Zugangsdaten. Den Antrag auf Auskunft über Stammdaten²¹⁹ nach § 76a Abs 1 StPO können die Kriminalpolizei, die Staatsanwalt oder ein Gericht – auch mündlich²²⁰ – stellen. Auskünfte über Zugangsdaten kann nur die Staatsanwaltschaft beantragen, dies aber ebenfalls vorläufig auch mündlich; eine Begründung in schriftlicher Form ist zwar auszufertigen, dies kann jedoch auch später geschehen.²²¹ Auf die Schwere des Deliktes kommt es bei der Auskunft nicht an.²²² Als das Gesetz noch die Vorratsdatenspeicherung vorsah, konnte über § 76a StPO auch auf Vorratsdaten zugegriffen werden. Einen Richtervorbehalt gibt es nicht.

Bei der Stammdatenauskunft muss sich die Auskunft, losgelöst von weiterer Datenverarbeitung, etwa durch Blick in die Vertragsunterlagen, erteilen lassen.²²³ Weitergehende Auskünfte sind nicht zulässig. Die verdächtige Person ist den Behörden schließlich bereits bekannt.

Weiter reicht der Eingriff bei einer Auskunft nach § 76a Abs 2 StPO. Polizeibehörden können diesen Antrag daher nicht stellen. Zuständig ist die Staatsanwaltschaft oder im Falle eines laufenden Hauptverfahrens auch das Gericht selbst.²²⁴ Die einzelnen Datenarten sind in § 76a Abs 2 StPO entsprechend abgegrenzt. Da sich die Anordnung nur auf Verkehrsdaten nach § 99 TKG bezieht und deren Speicherung dort abschließend geregelt ist, ergibt sich aus der StPO selbst keine Pflicht zur Speicherung der

²¹⁹ Dazu zählen der Name, der akademische Grad bei natürlichen Personen, die Anschrift, die Teilnehmernummer und sonstige Kontaktinformationen für die Nachricht, Informationen über Art und Inhalt des Vertragsverhältnisses sowie die Bonität.

²²⁰ Bertel/Venier, StPO, § 76a, Rz 3.

²²¹ Bertel/Venier, StPO, § 76a, Rz 4; Lendl in WK-StPO, § 76a, Rz 4.

²²² Pühringer, Vorratsdatenspeicherung, Zugriffsmöglichkeiten durch Sicherheits- und Strafverfolgungsbehörden, JAP 2012/2013/10, 80, 82.

²²³ Lendl in Fuchs/Ratz, WK StPO § 76a, Rz 1.

²²⁴ Lendl in Fuchs/Ratz, WK StPO § 76a, Rz 8.

Daten. Nach dem im TKG verankerten Prinzip bedeutet dies, dass nur solche Daten von der Speicherung umfasst sind, die vom Telekommunikationsanbieter zur Verrechnung von Endkunden- oder Vorleistungsentgelten erforderlich sind gespeichert werden dürfen (§ 99 Abs 2 TKG). Die Speicherung von Verkehrsdaten über diesen Zweck hinaus ist vom Gesetzgeber untersagt, was auf die meisten Flatrate-Tarife im Telekommunikationsbereich zutrifft.²²⁵ Insofern dürften Ermittlungsbehörden vielfach keinen Zugriff auf Daten über § 76a Abs 2 StPO erhalten, da zumindest dann, wenn sich die Provider rechtskonform verhalten, im Regelfall Daten der Teilnehmer nicht (mehr) vorhanden sein dürften.

7.2.2. Auskunft über Daten einer Nachrichtenermittlung, §§ 135 Abs 2 StPO, 134 Z 2 StPO

Die Auskunft über Daten einer „Nachrichtenübermittlung“ ist in § 134 Z 2 StPO legaldefiniert als „die Erteilung einer Auskunft über Verkehrsdaten (§ 92 Abs 3 Z 4 TKG), Zugangsdaten (§ 92 Abs 3 Z 4a TKG), die nicht einer Anordnung gemäß § 76a Abs 2 StPO unterliegen, und Standortdaten (§ 92 Abs 3 Z 6 TKG) eines Telekommunikationsdienstes oder eines Dienstes der Informationsgesellschaft (§ 1 Abs 1 Z 2 des Notifikationsgesetzes)“. Es geht somit nicht um Nachrichteninhalte selbst. Die Definitionen richten sich nach dem TKG. Zugangsdaten sind hierbei ein Unterfall der Verkehrsdaten, nämlich solche, durch die ein Telekommunikationsteilnehmer für den Zugang zu einer Telekommunikation verwendet oder benötigt, wie etwa eine IP-Adresse oder eine Rufnummer.²²⁶ Ferner erfasst die Vorschrift auch Standortdaten. In § 135 Abs 2 StPO selbst sind nur die Voraussetzungen für den Zugriff geregelt.

7.2.2.1. Daten einer „Nachrichtenermittlung“

Nach dem Gesetzeswortlaut wird auf Daten einer „Nachrichtenermittlung“ abgestellt. Das Wort Nachrichtenermittlung ist hierbei eher irreführend. So verweist § 134 Z 2 StPO auf die Datenkategorien, welche vielfach im Rahmen der Telekommunikation anfallen. Jedoch ist Telekommunikation für das Anfallen dieser Daten gerade nicht unbedingt an eine Übermittlung von Daten geknüpft, insbesondere bei Standortda-

²²⁵ Bergauer/Schmölzer in Jahnel/Mader/Staudegger, IT-Recht³, 716 f.

²²⁶ Reindl-Krauskopf/Tipold/Zerbes in Fuchs/Ratz, WK StPO § 134, Rz 33.

ten. Vielmehr ist gerade in Zeiten umfassender mobiler Nutzung von Telekommunikation der Anfall solcher Daten auch außerhalb von Telekommunikationsvorgängen nichts Ungewöhnliches. So fallen Standortdaten regelmäßig dann an, wenn das Mobiltelefon eingeschaltet ist.²²⁷ Hierin sieht die Kommentarliteratur kein rechtliches Problem, da sich der Verweis auf die rechtlich offene Definition des TKG beziehe,²²⁸ was die Erstellung von Bewegungsprofilen zulasse.²²⁹ Hierbei wird argumentiert, dass insbesondere ein entgegenstehender Wille des Gesetzgebers sich aus dem Materialien zur Gesetzgebung nicht ergebe.²³⁰ Es mag zwar zutreffend sein, dass der Gesetzgeber die Abfrage einzelner Standortdaten im Blick hatte, jedoch erlaubt die Vorschrift, was auch die Literatur nicht bezweifelt, umfassende Bewegungsprofile. Diese können aber noch weiter in die Grundrechtssphäre des Überwachten eingreifen, als Verkehrsdaten, da sich auf diese Weise dessen gesamtes Verhalten anhand seiner Aufenthaltsorte lückenlos rekonstruieren lässt.

Dies lässt sich auch nicht durch das Argument entkräften, eine Abfrage von Standortdaten sei bereits durch die Vorgängernorm (§ 149a Abs 1 Z 1 lit a StPO aF) möglich gewesen und es somit dem Gesetzgeber freigestanden hätte, entsprechende Verschärfungen vorzunehmen.²³¹ Diese Argumentation würde nur dann durchgreifen, wenn sich die gesamten Begleitumstände nicht verändert hätten. War früher der Anfall von Standortdaten die Ausnahme, da entsprechende Endgeräte nicht sonderlich weit verbreitet waren, geht nunmehr eher der Trend dazu, dass Personen über mehr als ein Endgerät verfügen, schon allein, weil dies in vielen Berufen erforderlich ist. Insofern würde es sich anbieten, die Erfassung von Standortdaten in eine gesonderte Vorschrift auszulagern, die dem besonderen Charakter einer solchen Überwachung auch gerecht wird. Wenigstens der Verhältnismäßigkeitsgrundsatz in § 5 StPO hat hier als Korrektiv zu wirken.

²²⁷ Reindl-Krauskopf/Tipold/Zerbes in Fuchs/Ratz, WK StPO § 134, Rz 34 f.

²²⁸ Reindl-Krauskopf/Tipold/Zerbes in Fuchs/Ratz, WK StPO § 134, Rz 35.

²²⁹ Bertel/Venier, StPO, § 135, Rz 4.

²³⁰ Reindl-Krauskopf/Tipold/Zerbes in Fuchs/Ratz, WK StPO § 134, Rz 35.

²³¹ Reindl-Krauskopf/Tipold/Zerbes in Fuchs/Ratz, WK StPO § 134, Rz 35.

Der Zugriff ist auf zwei Arten denkbar. Wo hierbei der Zugriff erfolgt, spielt keine Rolle. Er wird regelmäßig beim Anbieter selbst erfolgen; jedoch ist auch ein Zugriff auf die Daten selbst beim Verdächtigen vom Wortlaut der Vorschrift gedeckt.²³²

Jedoch gibt die Norm Ermittlern keine Handhabe, selbst die benötigten Daten zu generieren, indem sie etwa stumme SMS versenden und anhand der Ergebnisse ein Bewegungsprofil erstellen.

7.2.2.2. Voraussetzungen für die Herausgabe

Die Vorschrift des § 135 Abs 2 StPO listet taxativ die Voraussetzungen für die Herausgabe der in § 134 Z 2 StPO aufgeführten Daten auf. Dies ist zunächst vorgesehen, für den Fall einer Entführung (Z 1). Diese Fallgruppe weist keine sonderlichen rechtlichen Probleme auf.

Wesentlich interessanter ist die Fallgruppe von Z 2. Hier kann Telekommunikation überwacht werden, „wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als sechs Monaten bedroht ist, gefördert werden kann und der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Auskunft ausdrücklich zustimmt“. Interessant ist hier die Zustimmung des *Inhabers* der technischen Einrichtung. Als Inhaber ist wohl nicht nur der Sender, Adressat des Endgerätes zu verstehen, sondern jede Person, die die technische Einrichtung rechtmäßig im Besitz hat.²³³ Zwar wird – gerade im Bereich der Cyberkriminalität – oft etwa das Opfer als Empfänger der Nachrichten als Ermittlungsansatz infrage kommen und der Ermittlung zustimmen, jedoch sind auch ganz andere Fallkonstellationen denkbar, insbesondere im Kontext öffentlicher Netze. Wurde diese Thematik früher bei öffentlichen Fernsprechern diskutiert, so hat sich diese Fallkonstellation aufgrund der technischen Entwicklung quasi überholt.²³⁴ Gestattet etwa ein Kaffeehausbetreiber seinen Kunden die Benützung seines W-LANs, so wäre ein Gast des Kaffeehauses zwar der Nutzer, die

²³² Reindl-Krauskopf/Tipold/Zerbes in Fuchs/Ratz, WK StPO § 134, Rz 40.

²³³ Bergauer/Schmölzer in Jahnel/Mader/Staudegger, IT-Recht³, 720f.

²³⁴ Vgl zu diese Fallkonstellation Bergauer/Schmölzer in Jahnel/Mader/Staudegger, IT-Recht³, 717 mit Verweis auf OGH v. 18.01.2011, 12 Os152/00.

Herrschaft über die Anlage übt aber der Kaffeehausbetreiber aus.²³⁵ Stimmt der Kaffeehausbetreiber also zu, dürfte das Surfverhalten der Gäste, sofern die anderen Voraussetzungen der Z 2 vorliegen, letztlich untersucht werden. Eine Untersuchung des Mailverkehrs der Gäste dürfte wiederum nicht erfolgen, weil es sich hierbei um eine „eigene technische Anlage“ handelt.²³⁶

Fragen wirft ebenfalls die Tatsache auf, dass es bei der rechtmäßigen Inhaberschaft nicht darauf ankommt, welche Vertragsverhältnisse dahinter stehen, sondern nur, wer die technische Anlage rechtmäßig benützt. Diese Betrachtungsweise führt dann zu Problemen, wenn mehrere Personen gemeinsam eine solche Anlage rechtmäßig nützen. So ist bei einem W-LAN-Router in einer Wohngemeinschaft im Regelfall ein Mitbewohner Vertragspartner, alle Mitbewohner sind aber zur Nutzung dieses Routers berechtigt, sind also Inhaber der Anlage. Nach der Logik des Gesetzes könnte ein Mitbewohner die Überwachung gestatten. Es ist nach dem Gesetzeswortlaut nicht erforderlich, dass alle rechtmäßigen Inhaber ihre Zustimmung erklären.²³⁷ Dass allein die Frage der Inhaberschaft so viele Fragen und Unschärfen aufweist zeigt deutlich, dass die Vorschrift an legislativen Mängeln leidet. Schließlich handelt es sich im Rahmen von § 135 Abs 2 Z 2 StPO bei der Frage nach der Inhaberschaft um die zentrale, allen auf dieser Vorschrift basierender Ermittlungen, Frage. Solange nicht geklärt ist, wer Inhaber der technischen Einrichtung ist, kann keine Überwachung erfolgen, da dessen ausdrückliche, vorherige Zustimmung erforderlich ist.²³⁸ Letztlich wirft die Zustimmung in Z 2 aufgrund diverser Unschärfen Probleme auf.

Einfacher gestaltet sich der Anwendungsfall von Z 3, da hier gerade keine Zustimmung vonnöten ist. Voraussetzung ist lediglich, dass die Überwachung eine vorsätzlich begangene Straftat aufklären soll, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist und auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können.

²³⁵ *Reindl-Krauskopf/Tipold/Zerbes* in Fuchs/Ratz, WK StPO § 134, Rz 32; *Bergauer/Schmölzer* in Jahnelt/Mader/Staudegger, IT-Recht³, 717.

²³⁶ *Reindl-Krauskopf/Tipold/Zerbes* in Fuchs/Ratz, WK StPO § 134, Rz 32.

²³⁷ Auf diesem Umstand machen auch aufmerksam *Bergauer/Schmölzer* in Jahnelt/Mader/Staudegger, IT-Recht³, 717.

²³⁸ *Reindl-Krauskopf/Tipold/Zerbes* in Fuchs/Ratz, WK StPO § 134, Rz 33.

Ebenfalls nicht von der Zustimmung eines Kommunikationsteilnehmers abhängig ist Z 4. Hier ist es für die Überwachung erforderlich, dass der Aufenthalt eines flüchtigen oder abwesenden Beschuldigten, der einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung dringend verdächtig ist, ermittelt werden kann

7.2.3. Auskunft über Vorratsdaten, ehemaliger § 135 Abs 2a StPO

Diese Behandlung dieser Norm hat nur mehr rechtshistorischen Wert, da die Vorratsdatenspeicherung durch den VfGH nach der Entscheidung des EuGH aufgehoben wurde. Insofern lässt sich anhand des § 135 Abs 2a StPO²³⁹ nur das grundsätzliche Vorgehen des Gesetzgebers erkennen. Zentrale strafprozessuale Norm der Vorratsdatenspeicherung war § 135 Abs 2a StPO. Dieser legte fest, wann auf Vorratsdaten, die nicht zugleich von § 76a StPO erfasst sind, zugegriffen werden darf.

Was eine Auskunft über Vorratsdaten war, wurde in § 134 Z 2a StPO als die Erteilung einer Auskunft über Daten, die Anbieter von öffentlichen Kommunikationsdiensten nach Maßgabe des § 102a Abs 2 bis 4 TKG zu speichern hatten und die nicht nach § 99 Abs 2 TKG einer Auskunft nach Z 2 unterliegen,²⁴⁰ definiert.

Die Vorschrift des § 135 Abs 2a StPO regelte also die Zulässigkeitsvoraussetzungen für die in § 134 Z 2a StPO geregelte Auskunft. Grundsätzlich musste also dem Beschuldigten eine Straftat zur Last gelegt werden, die eine Strafandrohung von einem Jahr und mehr erwarten lässt.²⁴¹

7.2.4. Überwachung von Nachrichten, § 135 Abs 3 StPO

Diese Überwachungsmaßnahme ist direkt auf den Inhalt der Nachrichten gerichtet. Dies können Inhalte von Telefonaten, SMS, MMS oder E-Mails sein. Es kommt nicht darauf an, ob es sich um geschriebenes oder gesprochenes Wort oder um nonver-

²³⁹ Aufhebung nach BGBl I Nr. 44/2014.

²⁴⁰ Die Erteilung einer Auskunft über Daten, die Anbieter von öffentlichen Kommunikationsdiensten nach Maßgabe des § 102a Abs 2 bis 4 TKG zu speichern haben und die nicht nach § 99 Abs 2 TKG einer Auskunft nach Z 2 unterliegen.

²⁴¹ *Pühringer*, Vorratsdatenspeicherung, Zugriffsmöglichkeiten durch Sicherheits- und Strafverfolgungsbehörden, JAP 2012/2013/10, 80, 82.

bale Inhalte handelt.²⁴² Es ist ebenfalls die Definition des § 134 Z 3 StPO maßgeblich, welche wiederum ins TKG verweist (vgl hierzu die Ausführungen unter 7.2.2.1).

Die Fälle, in denen dies zulässig ist, lehnt der Gesetzgeber hierbei direkt an § 135 Abs 2 Z 1, 2 und 4 StPO an. Es stellen sich insofern auch die gleichen rechtlichen Fragen, wie bei § 135 Abs 2 StPO. Weiters ist eine Überwachung von Nachrichten in den Fällen des § 135 Abs 2 Z 3 StPO zulässig; jedoch hat der Gesetzgeber diesen für den Fall der Nachrichtenüberwachung etwas modifiziert, indem er der Vorschrift weitere Voraussetzungen hinzugefügt hat und sie mithin im Vergleich zur reinen Metadatenüberwachung verschärft hat. So ist eine Nachrichtenüberwachung zur Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, oder die Aufklärung oder Verhinderung von im Rahmen einer kriminellen oder terroristischen Vereinigung oder einer kriminellen Organisation (§§ 278 bis 278b StGB) begangenen oder geplanten strafbaren Handlungen ansonsten wesentlich erschwert wäre zulässig, wenn noch zusätzlich die Voraussetzungen von lit a oder lit b vorliegen, nämlich entweder der Inhaber der technischen Einrichtung, Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, oder einer Straftat gemäß §§ 278 bis 278b StGB dringend verdächtig ist oder auf Grund bestimmter Tatsachen anzunehmen ist, dass eine der Tat (lit a) dringend verdächtige Person die technische Einrichtung benützen oder mit ihr eine Verbindung herstellen werde.

Die Überwachung von Nachrichten, betrifft Nachrichten während des Übertragungsvorgangs; aufgrund dieser Ermächtigungsgrundlage können weder Nachrichten vor ihrem Absenden, noch nach ihrem Empfang überwacht werden.²⁴³ Dies wirft aber, in einer immer stärker auf reine Online-Services angelegte Technologien auch Abgrenzungsprobleme auf, da immer mehr Nutzer Services wie E-Mail rein im Browser nutzen und ein Abruf der Daten auf Endgeräte regelmäßig gar nicht (mehr) stattfindet.

²⁴² *Reindl-Krauskopf/Tipold/Zerbes* in Fuchs/Ratz, WK StPO § 134, Rz 22.

²⁴³ *Bertel/Venier*, StPO, § 135, Rz 7.

7.2.5. Durchsuchung von Endgeräten der Telekommunikation

Nicht direkt der Telekommunikationsüberwachung sind jene Maßnahmen zuzuordnen, die direkt am Endgerät der Telekommunikation ansetzen. Hierbei kommen strafprozessual die Beschlagnahme und die Sicherstellung in Betracht. Weiters ist im Rahmen der Sicherstellung oftmals die Durchsuchung von Orten und Gegenständen relevant.

Hierbei beziehen sich die Sicherstellung, welche in § 109 Z 1 StPO definiert ist und die Beschlagnahme, definiert in § 109 Z 2 StPO, zunächst nur auf die Begründung des Gewahrsams durch die Kriminalpolizei auf Anordnung der Staatsanwaltschaft im Rahmen der Sicherstellung bzw auf Anordnung eines Gerichtes im Rahmen der Beschlagnahme. Die Beschlagnahme kann hierbei auch auf einen Gegenstand beziehen der bereits sichergestellt wurde. Hiervon abgesehen gibt es jedoch Ausnahmen, in denen die Polizei von sich aus Gegenstände sicherstellen kann, die auch im Falle von Endgeräten der Telekommunikation relevant sein können. Dies trifft gemäß § 110 Abs 3 StPO zum einen auf Gegenstände zu, die in niemandes Verfügungsmacht stehen (Z 1 lit a), also etwa Fundsachen, sowie solche, die an einem Tatort aufgefunden wurden und zur Begehung der strafbaren Handlung verwendet wurden oder dazu bestimmt worden sein könnten (Z 1 lit c).²⁴⁴ Ebenfalls relevant ist die Sicherstellung von Gegenständen bei Personen, die auf frischer Tat betroffen festgenommen wurden (§ 170 Abs 1 Z 1 StPO), sowie bei Gegenständen, die im Rahmen einer Durchsuchung von Räumlichkeiten nach § 120 Abs 1 StPO aufgefunden wurden. Zudem ist die Sicherstellung bei Gefahr im Vollzug auch ohne Anordnung möglich.²⁴⁵ Bei der Durchsuchung von Orten und Gegenständen (§ 117 Z 2 StPO) sowie Personen (§ 117 Z 3 StPO) muss angegeben werden, was gesucht wird.²⁴⁶ Dies kann zum Beispiel eine bestimmte Nachricht auf einem Endgerät sein, die auf eine Straftat hindeutet. Hierfür benötigt die Kriminalpoli-

²⁴⁴ Bertel/Venier, StPO, § 135, Rz 3; die Variante „geringwertig oder vorübergehend leicht ersetzbar“ (Z 1 lit d) kommt schon allein, weil Telekommunikationsgeräte in der Regel einen Wert von über 100 € aufweisen und zum anderen nicht beliebig ersetzbar sind und, da an ihnen im Regelfall ein privates oder sogar berufliches Geheimhaltungsinteresse besteht, nicht in Betracht.

²⁴⁵ Bertel/Venier, StPO, § 99, Rz 6.

²⁴⁶ Bertel/Venier, StPO, § 119, Rz 3.

zei erste Indizien, im Sinne eines begründeten Verdachts.²⁴⁷ Eine Hausdurchsuchung darf hierbei, im Gegensatz zu den anderen Maßnahmen, nur in sehr eingeschränkten Fällen von der Kriminalpolizei selbst angeordnet werden. Allerdings geht das Gesetz noch zu weit, da das Hausrechtsgesetz noch weitere Beschränkungen in § 2 Abs 2 HausrechtsG enthält. Insofern ist die Vorschrift des § 120 StPO nicht verfassungsgemäß.²⁴⁸

Festzuhalten bleibt, dass stets das mildeste Mittel anzuwenden ist. Eine Sicherstellung von Daten ist nur dann zulässig, wenn dem Gerät auf dem die Daten gespeichert sind, ein zusätzlicher Beweiswert zukommt. Ansonsten sind Kopien der Daten, also auch allfällige auf dem Gerät gespeicherter Verbindungs- oder Inhaltsdaten, anzufertigen.²⁴⁹

7.2.6. Gerichtliche Bewilligung

Eine gerichtliche Bewilligung für Auskünfte nach § 76a StPO, die nicht von einem Gericht angefordert werden, gibt es nicht. Hier können auch Kriminalpolizei und Staatsanwaltschaft (§ 76a Abs 1 StPO) oder auch die Staatsanwaltschaft allein handeln (§ 76a Abs 2 StPO).

Anders ist die Rechtslage bei Auskünften nach § 135 StPO²⁵⁰. Diese werden von der Staatsanwaltschaft angeordnet, nachdem die Maßnahme zuvor gerichtlich bewilligt wurde. Die Anordnung ist hierbei an Formerfordernisse geknüpft, welche in § 138 Abs 1 Z 1 bis 6 StPO aufgeführt sind. Insbesondere sind die Maßnahmen nur in einem festgelegten Zeitraum zulässig (§ 138 Abs 1 Z 4 StPO). Dies ist nicht zuletzt Ausdruck des Verhältnismäßigkeitsgrundsatzes (§ 5 Abs 1 StPO).²⁵¹ Der Name des Beschuldigten muss nicht unbedingt bekannt sein, es reicht aus, wenn sich die Ermittlungen gegen eine

²⁴⁷ Hierbei reicht allein die Tatsache, dass jemand ein ehemaliger Straftäter ist, in Kombination mit einem lediglich anonymen Hinweis nicht aus; vgl *Bertel/Venier*, StPO, § 119, Rz 3 f.

²⁴⁸ So auch *Bertel/Venier*, StPO, § 120 Rz 4.

²⁴⁹ *Bertel/Venier*, StPO, § 110 Rz 6 f.

²⁵⁰ Gleiches gilt für Anordnungen nach § 136 StPO, mit Ausnahme von § 136 Abs 1 Z 1 StPO, welche auch die Kriminalpolizei anordnen kann.

²⁵¹ *Bertel/Venier*, StPO, § 137, Rz 3; dieser Grundsatz ist allgemein anwendbares Recht. Er muss ohnehin stets eingehalten werden. Hierbei kommt es insbesondere nicht darauf an, ob das Gesetz auf § 5 StPO verweist oder nicht, *Bertel/Venier*, StPO, § 5, Rz 3.

eindeutig identifizierbare Person richten,²⁵² oft wird der Name den Ermittlern erst im Laufe der Ermittlungen überhaupt bekannt werden (§ 138 Abs 1 Z 1 StPO).

Hierbei spielt es keine Rolle, ob die Maßnahme eilt, weil etwa benötigte Daten nur für einen bestimmten Zeitraum zur Verfügung stehen, oder nicht. Insbesondere kommt der Kriminalpolizei keine Eilkompetenz zu.²⁵³

Anbieter von Telekommunikation sind zur Mitwirkung und Mitüberwachung verpflichtet (§ 138 Abs 2 StPO) und können zur Geheimhaltung über die Vorgänge in einer gesonderten Anordnung verpflichtet werden (§ 138 Abs 3 StPO), wogegen der Betreiber wiederum vorgehen kann.²⁵⁴ Die Anordnung kann sich auch allein auf die Vergangenheit beziehen.²⁵⁵

Entsprechende Anordnungen greifen jedoch nicht nur in die Rechte der Kommunikationsteilnehmer ein, sondern auch in die Rechte des Telekommunikationsanbieters.²⁵⁶ Er muss daher auch in der Lage sein, die Rechtmäßigkeit der Anordnung untersuchen zu können, da er schließlich auch dem Kunden gegenüber zur Geheimhaltung der Telekommunikation verpflichtet ist (§ 93 TKG).²⁵⁷ Dagegen geht *Reindl-Krauskopf* davon aus, dass der Betreiber „nicht unmittelbar von einem Zwangsmittel betroffen“ sei,²⁵⁸ was sich unter anderem daran zeige, dass die Ermittler entsprechende Überwachungen auch am Anbieter vorbei, etwa mittels IMSI- oder IMEI-Catcher, durchführen könnten.²⁵⁹ Dies überzeugt jedoch nicht, zumal dort die Vorgehensweise eine ganz andere ist. Beim IMSI- oder auch IMEI-Catcher ahmen die Ermittler selbst eine Funkzelle nach und zeichnen dabei Daten auf, sie greifen nicht auf Daten, die beim Telekommunikationsanbieter liegen zu.²⁶⁰ Wer in die staatsanwaltschaftlichen Ermittlungen miteinbezogen wird hat, wenn er per Gesetz zur Geheimhaltung verpflichtet ist, klare

²⁵² *Reindl-Krauskopf/Tipold/Zerbes* in Fuchs/Ratz, WK StPO § 138, Rz 27.

²⁵³ *Reindl-Krauskopf/Tipold/Zerbes* in Fuchs/Ratz, WK StPO § 138, Rz 23.

²⁵⁴ *Bertel/Venier*, StPO, § 138, Rz 3.

²⁵⁵ *Reindl-Krauskopf/Tipold/Zerbes* in Fuchs/Ratz, WK StPO § 138, Rz 24.

²⁵⁶ So auch zutreffend *Bertel/Venier*, StPO, § 138, Rz 3.

²⁵⁷ *Bertel/Venier*, StPO, § 138, Rz 3.

²⁵⁸ *Reindl-Krauskopf/Tipold/Zerbes* in Fuchs/Ratz, WK StPO § 138, Rz 20.

²⁵⁹ *Reindl-Krauskopf/Tipold/Zerbes* in Fuchs/Ratz, WK StPO § 138, Rz 46.

²⁶⁰ Vgl zur Funktionsweise des IMSI-Catchers oben unter 7.1.2 und des IMEI-Catchers oben unter 7.1.3.

Pflichten gegenüber seinen Kunden. Inwiefern das Kommunikationsgeheimnis als Amtsgeheimnis fortbesteht, wenn Ermittler Daten aus einem Kommunikationsvorgang erhalten, bestimmt § 93 TKG nicht. Es ist jedoch, ähnlich wie beim Bankgeheimnis nach § 38 Abs 1 BWG, davon auszugehen, dass ein unverschuldetes Weitergeben von Daten den Telekommunikationsanbieter von der Haftung befreit.²⁶¹

Dies heißt aber im Umkehrschluss, dass auch dieser in der Lage sein muss, Anordnungen der Ermittler zu prüfen. Der Anbieter muss sich zumindest davon überzeugen können, dass die Anordnung die richterliche Bewilligung korrekt wiedergibt; ist dies nicht der Fall, dann ist ein Einspruch nach § 106 Abs 1 Z 2 StPO zulässig.²⁶²

7.2.7. Befugnisse im SPG

Zentrale Norm im SPG ist § 53 Abs 3a und 3b SPG. Auch diese richtet sich, wie die Vorschriften in der StPO, vor allem an die Telekommunikationsanbieter und sonstigen Diensteanbieter selbst.²⁶³ Befugt Auskünfte von diesen zu verlangen sind die Sicherheitsbehörden nach § 4 SPG.²⁶⁴ Das Auskunftsbegehren kann zunächst formlos ergehen, kann dann aber nicht durch Zwang durchgesetzt werden; eine Nicht-Auskunft stellt in diesem Fall auch keine Verwaltungsübertretung dar.²⁶⁵ Die Behörde kann aber einen Bescheid erlassen, der wiederum nach den Regeln des VVG durchgesetzt werden kann.

Grundsätzlich erfragen dürfen Ermittler nach § 53 Abs 3a Z 1 SPG Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses, solange sie diese zur Erfüllung ihrer Aufgaben nach dem SPG benötigen.²⁶⁶ Das Auskunftsrecht ist also, in

²⁶¹ Das Kreditinstitut ist also für die Weitergabe von Bankkundendaten nicht verantwortlich, sofern es an der Weitergabe kein Verschulden trifft; vgl *Laurer* in *Laurer/Borns/Strobl/M. Schütz/O. Schütz*, BWG³, Rz 7.

²⁶² *Bertel/Venier*, StPO, § 138, Rz 3.

²⁶³ Mit den sonstigen Diensteanbietern nach dem ECG, sind etwa Chatroom-Betreiber oder Host-Provider gemeint; *Hauer/Keplinger*, SPG⁴, 566.

²⁶⁴ Vgl zur Zuständigkeit und Hierarchie der Sicherheitsbehörden *Hauer/Keplinger*, SPG⁴, 84 mwN

²⁶⁵ *Hauer/Keplinger*, SPG⁴, 565.

²⁶⁶ *Hauer/Keplinger*, SPG⁴, 565 f.

Bezug auf die Anlässe in denen es angewendet werden kann sehr weitreichend,²⁶⁷ jedoch bezüglich der Daten, welche angefordert werden können, sehr eingeschränkt. Es bezieht sich nur auf einen bestimmten Anschluss und nicht etwa auf weitere, wie etwa die Daten von Angerufenen.²⁶⁸

In § 53 Abs 3a Z 2 SPG können die Behörden Auskunft über die IP-Adresse zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung anfordern, wenn bestimmte Voraussetzungen gegeben sind. Der Gesetzgeber hat also erkannt, dass eine IP-Adresse im Prinzip sensibler zu behandeln ist als eine Telefonnummer, da sich im Zusammenhang mit einer IP-Adresse wesentlich eher ein Profil eines Menschen erstellen lässt. Weiters ist nach § 53 Abs 3a Z 3 SPG die Auskunft über Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, möglich. Beide Ziffern stehen unter den gleichen Voraussetzungen.²⁶⁹ Die Ermittler müssen davon ausgehen können, dass die gewonnenen Daten eine wesentliche Voraussetzung für die Abwehr einer konkreten Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen im Rahmen der ersten allgemeinen Hilfeleistungspflicht (§ 19 SPG), eines gefährlichen Angriffs (§ 16 Abs 1 Z 1 SPG) oder einer kriminellen Verbindung (§ 16 Abs 1 Z 2 SPG) dienen. Die Voraussetzungen sind recht streng. So liegt ein gefährlicher Angriff nur dann vor, wenn die Bedrohung eines geschützten Rechtsgutes durch eine von Amts wegen zu verfolgende Straftat vorliegt.²⁷⁰

Weiters ermöglicht § 53 Abs 3a Z 4 SPG die Auskunft über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses durch Bezugnahme auf ein von diesem Anschluss aus geführtes Gespräch durch Bezeichnung eines möglichst genauen Zeitraumes und der passiven Teilnehmernummer. Dies ermöglicht den Ermittlern festzustellen, wer mit einem bestimmten Anschluss kommuniziert hat, mithin die

²⁶⁷ *Flendrovsky* in Bauer /Reimer, Handbuch Datenschutzrecht, 358.

²⁶⁸ *Hauer/Keplinger*, SPG⁴, 567.

²⁶⁹ Hierbei durfte im Übrigen auch auf Vorratsdaten zugegriffen werden; vgl. *Bergauer/Schmölzer* in Jähnel/Mader/Staudegger, IT-Recht³, 724.

²⁷⁰ *Bergauer/Schmölzer* in Jähnel/Mader/Staudegger, IT-Recht³, 724.

Auswertung passiver Gesprächsdaten.²⁷¹ Diese Abfrage ist zulässig zur Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder zur Abwehr gefährlicher Angriffe.

Schließlich sieht das SPG in § 53 Abs 3b SPG die Möglichkeit zur Standortfeststellung und die Identifizierung eines Mobilfunkteilnehmers mittels IMSI vor. Hierzu hat der Anbieter Auskunft über Standortdaten und IMSI zu erteilen. Die Sicherheitsbehörden dürfen dann die betreffende Person auch orten und mit technischen Mitteln deren genauen Standort ermitteln. Die Mobilfunkanbieter selbst sind nur zur Auskunft verpflichtet und nicht etwa zu weiterer Hilfestellung oder Datenspeicherung.²⁷² Die Standort- oder IMSI-Feststellung ist nach dem SPG nur sehr eingeschränkt zulässig. So kann aufgrund der Vorschrift nur eine Person geortet werden, die sich in unmittelbarer Lebens- oder Gesundheitsgefahr befindet und wenn die Ortung der Gefahrenabwehr und/oder Rettung der Person dient. Das bedeutet im Umkehrschluss, dass nur das Opfer, nicht etwa der Täter geortet werden darf.²⁷³

Eine physische Beschlagnahme im Wege der Sicherstellung nach § 42 SPG stellt bei Telekommunikationsendgeräten keinen tauglichen Weg dar, da keine der Varianten des § 42 SPG einschlägig ist.

7.2.8. Kontrolle durch den Rechtsschutzbeauftragten

Der Rechtsschutzbeauftragte nach dem SPG ist von den Überwachungsmaßnahmen gemäß § 53 Abs 3a Z 2 und Z 3 SPG und § 53 Abs 3a S 2 SPG zu informieren.²⁷⁴ Hierbei handelt es sich um eine nachträgliche Informationspflicht (§ 91c Abs 1 SPG); ohne dass dadurch unmittelbar eine Information der Betroffenen vorgesehen wäre.²⁷⁵ Hierbei sieht der Gesetzgeber in einer Maßnahme nach § 53 Abs 3a SPG noch eine solche auf unterer Eingriffsschwelle, so dass eine nachträgliche Information für ausreichend gehalten wird.²⁷⁶ Für bestimmte Maßnahmen außerhalb der Telekommunikationsüberwachung ist hingegen nach § 91c Abs 2 SPG eine Vorabkontrolle durch den

²⁷¹ *Bergauer/Schmölzer* in *Jahnel/Mader/Staudegger*, IT-Recht³, 725.

²⁷² *Hauer/Keplinger*, SPG⁴, 569.

²⁷³ *Hauer/Keplinger*, SPG⁴, 569.

²⁷⁴ *Hauer/Keplinger*, SPG⁴, 568.

²⁷⁵ *Hauer/Keplinger*, SPG⁴, 899.

²⁷⁶ RV zu BGBl I 85/2000 nach *Hauer/Keplinger*, SPG⁴, 900.

Rechtsschutzbeauftragten vorgesehen.²⁷⁷ Entdeckt der Rechtsschutzbeauftragte, dass Rechte des Betroffenen durch die Überwachungsmaßnahme verletzt wurden, so darf er diese informieren; sofern dies aus Gründen von § 26 Abs 2 des DSG 2000 – mithin beim Vorliegen besonderer öffentlicher Interessen²⁷⁸ – nicht möglich ist, darf er selbst bei der Datenschutzbehörde gegen die Maßnahme vorgehen.²⁷⁹

7.2.9. Zuordnung einzelner Überwachungsmaßnahmen zu strafprozessualen und sicherheitspolizeilichen Ermächtigungsgrundlagen

Zusammenfassend kann für den Bereich des Strafprozessrechts gesagt werden, dass die §§ 134 ff StPO für manche der oben unter 7.1 genannten Überwachungsmaßnahmen als Ermächtigungsgrundlage dienen können. Zum einen immer dann, wenn Metadaten betroffen sind, § 135 Abs 2 StPO, und zum anderen sobald es um Inhalte geht, § 135 Abs 3 StPO. Während es für diverse Metadaten im SPG – wenn auch oft unter strengen Voraussetzungen – Möglichkeiten gibt, diese als Sicherheitsbehörde anzufordern, gibt es keine SPG-Norm zur Überwachung von Nachrichteninhalten. Diese hat allein über die StPO zu erfolgen.²⁸⁰

Die sogenannte Rufdatenrückerfassung ist strafprozessual von § 135 Abs 3 StPO abgedeckt. Sie ist zudem im Polizeirecht in § 53 Abs 3a Z4 SPG geregelt. Hierbei

²⁷⁷ Etwa bei Videoüberwachung von Kriminalitätsschwerpunkten oder öffentlicher Orte wegen einer Veranstaltung mit besonders zu schützenden internationalen Teilnehmern (§ 54 Abs 7 und Abs 6 SPG), Einrichtung von Analysedatenbanken zur Abwehr allgemeiner Gefahren (§ 53a Abs 2 und 6 SPG), Einrichtung einer Staatsschutzdatenbank (§ 12 PStSG), Einsatz von Bild- und Tonaufzeichnungs- sowie von elektronischen Abfertigungsgeräten im Bereich von Grenzübergangsstellen (§ 12 Abs. 2 GrekoG).

²⁷⁸ Dies sind laut § 26 Abs 2 S 2 DSG 2000 insbesondere der Schutz der verfassungsmäßigen Einrichtungen der Republik Österreich, die Sicherung der Einsatzbereitschaft des Bundesheeres, die Sicherung der Interessen der umfassenden Landesverteidigung, der Schutz wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der Europäischen Union oder die Vorbeugung, Verhinderung oder Verfolgung von Straftaten.

²⁷⁹ *Hauer/Keplinger*, SPG⁴, 902; ²⁷⁹ *Klaushofer*, Strukturfragen des Rechtsschutzbeauftragten, 304 f. Mit der Information der Betroffenen endet automatisch auch die Vertretungsbefugnis des Rechtsschutzbeauftragten.

²⁸⁰ *Hauer/Keplinger*, SPG⁴, 590.

dürfen die Ermittler jedoch nicht ins Blaue ermitteln, sondern müssen den Zeitraum der Rufdatenrück Erfassung möglichst genau eingrenzen.²⁸¹

Diese Unterteilung scheint einfach, ist aber in Bezug auf IMSI-Catcher und IMEI-Catcher problematisch. Während seine sicherheitspolizeiliche Einordnung klar ist. Jedoch wird von staatlicher Seite auch davon ausgegangen, dass IMSI-Catcher und IMEI-Catcher von § 135 Abs 2 StPO als Ermächtigungsgrundlage gedeckt sind.²⁸² Auch die Kommentarliteratur geht zum Teil implizit davon aus, dass entsprechende Maßnahme auf § 135 Abs 2 StPO gestützt werden können.²⁸³ Dies mag ein pragmatischer Ansatz sein, der vor allem ermittlungstaktisch und strafprozessual auch stimmig ist. Jedoch wird hierbei übersehen, dass aufgrund der in § 134 StPO für die folgenden Vorschriften festgelegten Definitionen, die Interpretation was ein Telekommunikationsdienst ist, allein dem TKG unterliegen kann, da auch alle Datenarten rein nach dem TKG zu beurteilen sind. Nach dem TKG ist ein Telekommunikationsdienst ein Kommunikationsdienst mit Ausnahme von Rundfunk (§ 3 Z 21 TKG).

Ein Kommunikationsdienst wiederum ist eine gewerbliche Dienstleistung, die ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze besteht, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen, jedoch ausgenommen Dienste, die Inhalte über Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben (§ 3 Z 9 TKG). Durch das Betreiben eines IMSI- oder IMEI-Catcher kann wohl kaum behauptet werden, der Staat würde eine gewerbliche Dienstleistung für Endnutzer erbringen. Insbesondere wird der Staat hierbei nicht zum Betreiber eines Kommunikationsdienstes nach § 3 Z 3 TKG. Mithin ist der Einsatz dieser Mittel zur Strafverfolgung in Österreich nicht zulässig. Die Abfragen haben also über den Anbieter selbst zu laufen.

²⁸¹ Hauer/Keplinger, SPG⁴, 558.

²⁸² Dies kommt durch eine parlamentarische Stellungnahme des Justizministeriums zum Ausdruck (3910/AB 1 von 5 vom 06.05.2015 zu 4087/J (XXV.GP)); im Internet abrufbar unter https://www.parlament.gv.at/PAKT/VHG/XXV/AB/AB_03910/imfname_409316.pdf.

²⁸³ Vgl hierzu die Argumentation bei Reindl-Krauskopf/Tipold/Zerbes in Fuchs/Ratz, WK StPO § 138, Rz 46; näheres vgl oben unter 7.2.6.

Gleichlautend ist die Argumentation beim stummen SMS, welches den Ermittlern ermöglichen würde, Standortdaten zu ermitteln. Anfragen zu Standortdaten richten die Ermittler „ausnahmslos nach den einschlägigen Bestimmungen des Sicherheitspolizeigesetzes und der Strafprozessordnung an den jeweiligen Mobilnetzbetreiber.“²⁸⁴ Hier müssten die Ermittler nämlich zunächst einmal selbst den Ortungsimpuls setzen. Für diese Handlung mangelt es an einer gesetzlichen Ermächtigung.

Im SPG findet sich jedenfalls auch keine Rechtsgrundlage für das stumme SMS. Insbesondere § 53 Abs 3b S 1 SPG kann hier nicht als Rechtsgrundlage dienen. Zwar ist der Einsatz technischer Mittel zur Ortung möglich. Jedoch haben die Ermittler vom Mobilfunkanbieter bereits die Funkzelle bekommen, weitere Informationen lassen sich durch stumme SMS auch nicht ermitteln. Der IMSI-Catcher, dessen Einsatz das SPG vorsieht (dazu sogleich), kann hingegen immer noch dazu herangezogen werden, den Standort des mobilen Endgerätes genauer zu bestimmen. Für den IMSI-Catcher gibt es hingegen eine Ermächtigungsgrundlage im SPG,²⁸⁵ jedoch nur in engen Grenzen. Somit scheidet eine Fahndung aus. Der IMSI-Catcher eignet sich nur als punktuelle Maßnahme, um gezielt den Aufenthaltsort einer bestimmten Person an einem Ort zu bestätigen.

Keine Rechtsgrundlage findet sich hingegen für den IMEI-Catcher, obwohl dieser ähnlich grundrechtsintensiv ist. Dies ist dadurch zu erklären, dass Mobilfunkbetreibern die IMSI ihrer SIM-Karten bekannt ist, jedoch nicht unbedingt die IMEI eines Gerätes zugeordnet werden kann, diese Daten also für Ermittler geringeren Informationsgehalt haben.

In jedem Fall unzulässig sind in Österreich im Bereich der Strafverfolgung Maßnahmen wie die Quellen-Telekommunikationsüberwachung und die Online-Durchsuchung, wie etwa *Pilnacek* zutreffend beschreibt.²⁸⁶ Sie sind insbesondere auch keine Lausch- oder Spähangriffe nach § 136 StPO und können nicht auf diese Grundlage gestützt werden. Vielmehr würden sich die beteiligten Ermittler bei Durchführungen

²⁸⁴ Stellungnahme des Justizministeriums (vom 15.09.2014 zu 2231/J (XXV.GP)); abrufbar unter https://www.parlament.gv.at/PAKT/VHG/XXV/AB/AB_02109/imfname_364266.pdf.

²⁸⁵ Vgl oben unter 7.2.7.

²⁸⁶ *Bertel/Venier*, StPO, § 136, Rz 5; *Reindl-Krauskopf/Tipold/Zerbes* in Fuchs/Ratz, WK StPO § 138, Rz 115.

solcher Ermittlungsmaßnahmen ohne gesetzliche Grundlage sogar strafbar machen.²⁸⁷ Auch nach dem SPG findet sich keine Basis für solche Ermittlungsmaßnahmen.

Pilnacek ist aber insofern nicht zuzustimmen, als dass er eine reine Quellen-Telekommunikationsüberwachung, welche nach seiner Definition auch eine Variante der Online-Durchsuchung ist, für zulässig hält bzw dort lediglich das heimliche Eindringen von außen als Problem ansieht.²⁸⁸ Auch hierbei ist zu betonen, dass § 135 Abs 2 StPO eindeutig beim Anbieter ansetzt und nicht etwa beim Endbenutzer. Wollen Ermittler Zugriff auf die Endgeräte des Telekommunikationsteilnehmers bekommen, dann müssen sie diese auf herkömmlichem Wege unter Einhaltung aller gesetzlichen Regelungen beschlagnahmen oder im Rahmen einer Hausdurchsuchung in Augenschein nehmen.

Damit ergibt sich bei den Überwachungsmaßnahmen für Österreich nach SPG und StPO folgendes Gesamtbild:

Maßnahme	Ermächtigungsgrundlage ²⁸⁹	
	StPO	SPG
„stummes SMS“	keine	
IMSI-Catcher	keine	§ 53 Abs 3b
IMEI-Catcher	keine	
Abfrage von Kundendaten beim Telekommunikationsanbieter	§§ 76a, 135 Abs 2	§§ 53 Abs 3a Z 1 bis 4, 53 Abs 3b
Funkzellenabfrage	§ 135 Abs 2	keine
Rufdatenrückerfassung	§ 135 Abs 2	§ 53 Abs 3a Z 4
Abhören von Gesprächen	§ 135 Abs 3	keine
E-Mail- und Textnachrichtenüberwachung	§ 135 Abs 3	keine
Quellen-Telekommunikationsüberwachung	keine	

²⁸⁷ *Pilnacek/Pscheidl*, Das Strafverfahren und seine Grundsätze (Teil I), ÖJZ 2008, 629, 633.

²⁸⁸ *Pilnacek/Pscheidl*, Das Strafverfahren und seine Grundsätze (Teil I), ÖJZ 2008, 629, 632 f.

²⁸⁹ Alle Paragraphen sind solche der StPO bzw des SPG.

Online-Durchsuchung	keine	
Vorratsdatenspeicherung	keine	
Sicherstellung und Beschlagnahme von Endgeräten der Telekommunikation	§§ 110, 115	keine

7.3. Die strafprozessuale und polizeirechtliche Telekommunikationsüberwachung in Deutschland

Strafprozessual weisen die Überwachungsbefugnisse der dStPO eine gänzliche andere Systematik auf als jene der StPO. Die dStPO baut eher auf einem Modell auf, das, ausgehend von den verübten Straftaten, einen schwereren oder leichteren Zugang zu Telekommunikationsdaten ermöglicht. Hierbei ist ein Zugriff grundsätzlich dergestalt geregelt, dass bei besonders schweren Straftaten auf sämtliche Telekommunikationsdaten, in anderen Fällen nur auf Verkehrsdaten zugegriffen werden kann.

Da die Überwachungsmaßnahmen in Deutschland nicht beim Provider ansetzen, steht es den zuständigen Behörden frei, Maßnahmen nach ihren technischen Möglichkeiten auch selbst zu ergreifen. Einzige Ausnahme hierzu hatte die Vorratsdatenspeicherung neu dargestellt, die jedoch nach einem Urteil des OVG Münster von der Bundesnetzagentur ausgesetzt wurde.²⁹⁰ Damit gelangt die Vorratsdatenspeicherung in Deutschland aktuell de facto nicht mehr zur Anwendung.

7.3.1. Telekommunikationsüberwachung, § 100a Abs 1 dStPO

Die zentrale Norm für die Telekommunikationsüberwachung in Deutschland ist § 100a Abs 1 dStPO. Dieser ist von vornherein auf bestimmte schwere Straftaten beschränkt, welche in § 100a Abs 2 dStPO aufgelistet sind. § 100a dStPO bezieht sich auf Verkehrsdaten und Nachrichteninhalte. Die Anordnung zur Überwachung, welche die Staatsanwaltschaft zu treffen hat, muss sich gegen den Beschuldigten oder einen der Tat Verdächtigen richten.²⁹¹ Die Vorschrift ist am Telekommunikationsvorgang orien-

²⁹⁰ Vgl hierzu unter 28.3.5.

²⁹¹ Näher *Graf*, BeckOK StPO, § 100a, Rz 42 ff.

tiert. Damit endet der Grundrechtsschutz am Endgerät.²⁹² Die Maßnahmen werden vom Gericht auf Antrag der Staatsanwaltschaft angeordnet, bei Gefahr im Verzug auch durch diese selbst (§ 100b Abs 1 d StPO).²⁹³

7.3.2. Erhebung von Verkehrsdaten, § 100g Abs 1 dStPO

Die Vorschrift regelt die Erhebung von Verkehrsdaten. Deren Ermittlung ist zwar bereits unter § 100a Abs 1 dStPO möglich, jedoch nicht an den Straftatenkatalog geknüpft. Wollen Ermittler von vornherein nur Verkehrsdaten überwachen, so werden sie sich dieser Norm bedienen, da die Voraussetzungen weit weniger streng sind. Es genügen bereits Straftaten von auch im Einzelfall erheblicher Bedeutung (§ 100g Abs 1 S 1 Z 1 dStPO). Hierbei verweist das Gesetz zwar auf § 100a dStPO und dessen taxative Aufzählung, die jedoch in diesem Fall nicht als abschließend zu verstehen ist. Weiters ist eine Überwachung nach § 100g Abs 1 S 1 Z 2 dStPO möglich, sobald Telekommunikationsmittel als Tatmittel für Straftaten verwendet werden. Hierbei kommt es auf die Schwere der Straftaten nicht an.²⁹⁴

7.3.3. Weitere Maßnahmen außerhalb von Wohnraum, § 100h dStPO

Des Weiteren dürfen die Ermittler außerhalb von Wohnungen besondere, für Observationszwecke bestimmte technische Mittel verwenden. Ein technisches Mittel ist hierbei alles außer Bild- und Tonaufnahme des Betroffenen, was die Observation ermöglicht, etwa ein GPS-Peilsender, der am Auto des Überwachten angebracht wird.²⁹⁵

7.3.4. Technische Ermittlungsmaßnahmen bei Mobilfunkendgeräten, § 100i Abs 1 dStPO

Im Gegensatz zum österreichischen Recht gibt es in der dStPO mit § 101i Abs 1 dStPO eine Ermittlungsnorm für die Feststellung von IMEIs und IMSIs.

²⁹² Pfeiffer, StPO⁵, § 100a StPO, Rz 1 f.

²⁹³ Bruns in Karlsruher Kommentar StPO⁶, § 100b, Rz 2 f.

²⁹⁴ Bruns in Karlsruher Kommentar StPO⁶, § 100g, Rz 7 ff.

²⁹⁵ Graf, BeckOK StPO, § 100h, Rz 6 f.

Zusätzlich können aufgrund dieser Vorschrift Auskünfte bezüglich des Standortes eingeholt werden.²⁹⁶

7.3.5. Bestandsdatenauskunft, §100j dStPO

Die Vorschrift regelt die Auskunft über Bestandsdaten, welche beim Telekommunikationsanbieter vorliegen. Die Voraussetzungen hierfür sind gering; die Maßnahme muss lediglich dazu dienen, dass dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten erforderlich ist. Hierbei nimmt die Vorschrift direkt Bezug auf das dTKG. Anbieter haben demnach Daten nach § 95 bis § 111 TKG herauszugeben. Hierbei handelt es sich um Rechnungsdaten, Verkehrs- und Standortdaten, die der Anbieter aus Gründen der Abrechnung oder aus technischen Gründen, etwa zur Störungsverfolgung, speichert. Dynamische IP-Adressen sind hierbei nicht als Bestandsdaten im Sinne von § 100j Abs 1 dStPO anzusehen, weswegen der Gesetzgeber diese in einer gesonderten Vorschrift in § 100j Abs 2 dStPO aufnahm.²⁹⁷ Die Maßnahme muss von einem Gericht auf Antrag der Staatsanwaltschaft angeordnet werden. Die Betroffenen sind über die Maßnahmen nach § 100j dStPO zu benachrichtigen (§ 100j Abs 4 dStPO), solange der Zweck der Maßnahme hierdurch nicht vereitelt wird und keine Schutzwürdigen Rechte Dritter entgegenstehen.

7.3.6. Durchsuchung von Endgeräten der Telekommunikation

Endgeräte der Telekommunikation können nach § 94 Abs 1 dStPO sichergestellt werden, wenn sie als Beweismittel von Bedeutung sind. In diese kann dann im weiteren Verfahren Einsicht genommen werden. Nach der zurzeit in der strafprozessualen Literatur vertretenen Ansicht, können Daten, auch solche auf Servern und ebenfalls solche, die Teil eines Telekommunikationsvorgangs sind, dort beschlagnahmt werden.²⁹⁸

7.3.7. Befugnisse im (bayerischen) Polizeirecht

Das bayerische Polizeirecht stattet die Landespolizei – etwas umfassender als in den meisten Bundesländern – mit weitreichenden Befugnissen aus. Die Polizei kann

²⁹⁶ *Bruns* in Karlsruher Kommentar StPO⁶, § 100i, Rz 2 ff.

²⁹⁷ *Bruns* in Karlsruher Kommentar StPO⁶, § 100j, Rz 2.

²⁹⁸ *Bruns* in Karlsruher Kommentar StPO⁶, § 94, Rz 4; diese Ansicht wird auch verfassungsgerichtlich in Deutschland vertreten, ist aber unzutreffend.

hierbei Daten und Telekommunikation aufzeichnen (Art 34a Abs 1 PAG), sofern bestimmte Voraussetzungen, wie etwa eine Gefahr für Leib, Leben und Freiheit, vorliegt. Allerdings ist eine Datenerhebung nur dann zulässig, wenn sich die Polizei die Daten anderweitig nur unter erschwerten Bedingungen oder gar nicht beschaffen kann.²⁹⁹ Ferner können Telekommunikationsanbieter bei den Ermittlungen mitwirkungspflichtig sein und müssen entsprechende Anfragen beantworten (Art 34b PAG).

Ebenfalls im Landesrecht geregelt ist der verdeckte Eingriff in informationstechnische Systeme in Art 34d PAG. Hier regelt der Gesetzgeber in einer – aufgrund der zugrundeliegenden verfassungsrechtlichen Rechtsprechung³⁰⁰ sehr komplizierten Vorschrift – den verdeckten Eingriff auf informationstechnische Systeme; mithin ermöglicht diese Vorschrift die Quellen-Telekommunikationsüberwachung und darüber hinaus die noch weiter reichende Online-Durchsuchung.³⁰¹ Zum einen findet eine Einschränkung dergestalt statt, dass ein Einsatz der Ermittlungsmaßnahme nur unter besonderen Voraussetzungen stattfinden darf (den Bestand oder die Sicherheit des Bundes oder eines Landes, Rechtsgüter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, oder Leib, Leben oder Freiheit einer Person; Art 34d Abs 1 S 1 PAG) und zum anderen dadurch, dass die Maßnahme nur dann durchgeführt werden darf, wenn die Polizei sich die Daten nicht anderweitig beschaffen kann.

Eine Sicherstellung von Endgeräten der Telekommunikation wird nach Art 25 PAG nur selten in Betracht kommen. Allenfalls möglich wäre eine Sicherstellung nach Art 25 Z 1 PAG, um eine gegenwärtige Gefahr abzuwehren. Gegenwärtig ist eine Gefahr aber erst dann, wenn die Einwirkung des schädigenden Ereignisses bereits begonnen hat oder wenn diese Einwirkung unmittelbar oder in allernächster Zeit mit an Sicherheit grenzender Wahrscheinlichkeit bevorsteht.³⁰² Mithin wird dies beim Einsatz von Telekommunikation selten der Fall sein, so dass sich eine Sicherstellung mit an-

²⁹⁹ Berner/Köhler/Käβ, PAG²⁰, Art 34a, Rz 12.

³⁰⁰ Berner/Köhler/Käβ, PAG²⁰, Art 34d, Rz 3.

³⁰¹ Berner/Köhler/Käβ, PAG²⁰, Art 34d, Rz 4.

³⁰² Berner/Köhler/Käβ, PAG²⁰, Art 2, Rz 27.

schließender Beweisverwertung für die Polizei aus rein polizeirechtlicher Sicht eher nicht anbietet.

7.3.8. Gerichtliche Bewilligung

Eine gerichtliche Bewilligung ist in mehreren Fällen erforderlich und in Deutschland nicht allein auf die dStPO beschränkt. So sieht das Gesetz eine gerichtliche Anordnung bei Maßnahmen nach § 100a dStPO vor; bei Gefahr im Verzug ist eine richterliche Bestätigung binnen drei Tagen erforderlich (§ 100b Abs 1 dStPO).³⁰³ Entsprechendes gilt für Maßnahmen nach §§ 100i und 100j dStPO, diese verweisen hierbei entsprechend auf § 100b dStPO.

Der Richtervorbehalt beschränkt sich nicht auf den strafprozessualen Bereich. Auch im Polizeirecht ist ein Richtervorbehalt im Fall des Art 34d PAG (Online-Durchsuchung) vorgesehen. Hierbei verweist das Gesetz auf Art 34 Abs 4 PAG, der die Überwachung von Wohnraum regelt und wird damit der Rechtsprechung des BVerfG s zur Online-Durchsuchung gerecht.³⁰⁴

7.3.9. Zuordnung einzelner Überwachungsmaßnahmen zu strafprozessualen und polizeirechtlicher Ermächtigungsgrundlagen

Aufgrund der komplexen Gemengelage an strafprozessualen Vorschriften ist die Zuordnung zu den einzelnen Vorschriften schwierig und dementsprechend teilweise auch umstritten. So ist beispielsweise der IMSI-Catcher vom sachlichen Anwendungsbereich des § 100i dStPO klar abgedeckt, da dieser auf technische Mittel Bezug nimmt, die sich auf die Gerätenummer oder die SIM-Karte beziehen. Diese Norm kann aber nicht Ermächtigungsgrundlage für das stumme SMS sein, da dieses eines zweistufigen Ablaufs bedarf: dem Senden des Impulses und der Abfrage der selbst verursachten Bestandsdaten beim Provider.

³⁰³ Näheres bei *Bruns* in *Karlsruher Kommentar StPO*⁶, § 100b, Rz 2 f.

³⁰⁴ *Berner/Köhler/Käβ*, PAG²⁰, Art 34d, Rz 12 mwN.

Hierbei wird in der Rechtswissenschaft diskutiert, ob sich das stummer SMS auf § 100a dStPO iVm § 100h dStPO stützen lässt, was etwa *Graf* befürwortet.³⁰⁵ *Smith* hingegen bringt die allgemeine Ermittlungsnorm § 161 dStPO ins Spiel, die den Behörden allgemeine Maßnahmen erlaubt, die nötig sind, um Straftaten aufzuklären, wobei er diesen Ansatz selbst kritisch sieht.³⁰⁶ Letztlich muss hierbei die Grundsatzfrage gestellt werden, inwiefern eine einzige Maßnahme auf zwei Ermächtigungsgrundlagen gestützt werden kann, die nicht näher zusammenhängen.

Aus meiner Sicht muss zunächst § 100h dStPO ausscheiden. Dieser gestattet lediglich den Einsatz technischer Mittel, wobei die Überwachung mit dem Mittel selbst zu erfolgen hat und nicht etwa in einem zweiten Schritt aufgrund einer völlig anderen Ermittlungsgrundlage. Damit fehlt es an einer Ermächtigungsgrundlage.

Eine konkrete Norm zur Nachrichtenüberwachung kennt die deutsche StPO nicht. Frühere Ansichten stützten sich hierbei auf § 99 dStPO, der die Postbeschlagnahme regelt.³⁰⁷ Heutzutage wird die Rechtsgrundlage eher in § 94 dStPO gesehen,³⁰⁸ was aber in der Literatur berechtigterweise auf Kritik stößt.³⁰⁹ Auf Grundlage dieser Vorschrift beschlagnahmen Gerichte nunmehr auch Facebook-Nachrichten und jegliche Art von Telekommunikation, die in irgendeiner Weise auf Servern Dritter Spuren hinterlässt, ohne dass es der Gesetzgeber für nötig hält, hierfür eine explizite Maßnahme zu schaffen.

Sicherlich bewegt sich die heutige Kommunikation nicht mehr in den starren Mustern, in denen zwischen dem Absenden einer Nachricht, der Übermittlung und deren Empfang genau getrennt werden kann und selbstverständlich kann ein E-Mail etwa nicht ewig im Schutzbereich des Fernmeldegeheimnisses verbleiben, nur weil es nie vom Server abgerufen, aber längst gelesen wurde. Dies aber zeigt lediglich, dass der Staat hierfür geeignete Vorschriften zu schaffen hat, die entsprechende Abwägungen

³⁰⁵ *Graf*, BeckOK StPO, § 100h, Rz 7 f.

³⁰⁶ *Smith*, Kurzer Zwischenstand zu Recht und Praxis der „stillen SMS“, VR 2012, 314, 336.

³⁰⁷ *Graf*, BeckOK StPO, § 99, Rz 9 ff.

³⁰⁸ Vgl zur verfassungsgerichtlichen Rechtsprechung *Klein*, Offen und (deshalb) einfach – Zur Sicherstellung und Beschlagnahme von E-Mails beim Provider, NJW 2009, 2996.

³⁰⁹ Eine Übersicht zur Kritik am Gesetzgeber, dem dieses Problem bereits seit Jahren bekannt ist, findet sich bei *Graf*, BeckOK StPO, § 99, Rz 9 ff.

zulassen. Insbesondere fehlt gerade eine Vergleichbarkeit mit der Postbeschlagnahme. Die beschlagnahmte Post ist für den Empfänger nicht mehr greifbar. Dies ist einerseits gravierender, als wenn sich die Ermittler eine Kopie von einem oder mehreren Mails machen, andererseits liegen bei einem E-Mailpostfach in der Regel eine Vielzahl von E-Mails vor, erst recht dann, wenn diese nie abgerufen werden oder dann, wenn diese zwar abgerufen werden, aber eine Kopie auf dem Server verbleibt. Damit kann, mangels entsprechender Regelung, ein Abruf nur unter den strengen Voraussetzungen des § 100a dStPO erfolgen. Die Quellen-Telekommunikationsüberwachung hingegen dürfte zwar noch von § 100a dStPO umfasst sein, auch wenn gemeinhin kritisiert wird, dass eine explizite gesetzliche Regelung notwendig wäre.³¹⁰ Keine Ermächtigung gibt es – anders als etwa im bayerischen Polizeirecht – in der dStPO für Online-Durchsuchungen.

Damit ergibt sich aus deutscher Sicht folgendes Gesamtbild:

Maßnahme	Ermächtigungsgrundlage ³¹¹	
	dStPO	PAG
„stummes SMS“	keine	
IMSI-Catcher	§ 100i	Art 34a
IMEI-Catcher	keine	
Abfrage von Kundendaten beim Telekommunikationsanbieter	§ 100a	Art 34b, 34a
Funkzellenabfrage	§ 100a / § 100g	Art 34b, 34a
Zielwahlsuche	§ 100a / § 100g	Art 34b, 34a
Abhören von Gesprächen	§ 100 a	
E-Mail- und Textnachrichtenüberwachung	Keine, zurzeit wenigstens § 100a	Art 34b, 34a
Quellen-Telekommunikationsüberwachung	§ 100a	Art 34d

³¹⁰ Graf, BeckOK StPO, § 100a, Rz 107e. In der Praxis dürfte aber zwischen einer reinen Quellen-Telekommunikationsüberwachung und einer Online-Durchsuchung oft schwer zu trennen sein.

³¹¹ Alle Paragraphen in dieser Tabelle ohne nähere Angabe sind solche der dStPO bzw alle Artikel, solche des PAG.

Online-Durchsuchung	keine ³¹²	Art 34d
Vorratsdatenspeicherung	§ 100a iVm § 113b TKG ³¹³	Art 34b, 34a iVm § 113b TKG
Sicherstellung und Beschlagnahme von Endgeräten der Telekommuni- kation	§ 94	Art 25 Z 1

7.4. Vergleich

Deutschland setzt auf wesentlich weitreichendere Überwachungsmaßnahmen und hat (teilweise) entsprechende Rechtsgrundlagen geschaffen, wohingegen für viele Überwachungsmaßnahmen in Österreich keine Rechtsgrundlage besteht, mithin diese von den Ermittlern auch nicht eingesetzt werden dürfen. Das deutsche Recht hat einen etwas differenzierteren Ansatz, indem etwa die Straftaten, wegen denen auf bestimmte Telekommunikationsdaten zugegriffen werden darf, stark eingeschränkt sind, wohingegen es in Österreich für den Zugriff genügt, wenn die Straftat mit einer mehr als einjährigen Freiheitsstrafe bedroht ist, was den Katalog in Betracht kommender Straftaten ungleich größer macht. Umgekehrt ist das österreichische Recht viel stärker am TKG orientiert, was bei den Datenarten eine viel klarere Struktur vorgibt. Beide Ansätze haben damit ihre legislativen Stärken und Schwächen. In beiden Staaten besteht jedenfalls ein komplexes System an Überwachungsmaßnahmen.

³¹² Auf Bundesebene existiert jedoch mit § 20k BKAG eine Ermächtigungsnorm für diese Maßnahme. In der normalen Ermittlungstätigkeit der Staatsanwaltschaften und der Polizei spielt diese Überwachungsmaßnahme also zurzeit keine Rolle. Näheres zum BKAG und dem dortigen Schutz der Berufsgeheimnisträger siehe 28.4.

³¹³ Details hierzu siehe 28.2. Nach einer Entscheidung des OVG Münster (siehe hierzu unter 28.3.5) gelangt diese aber de facto nicht mehr zu Anwendung.

8. Verfassungsrechtliche Vorgaben für die Überwachung von Telekommunikation in Österreich

Zunächst gilt es, die betroffenen Grundrechte im österreichischen Verfassungsrecht herauszuarbeiten, da nur dies die Unterschiede im Rahmen der Rechtsvergleichung offenbart und nur auf diese Weise ein Vergleich mit der deutschen Grundrechtsordnung erfolgen kann.

Welche Grundrechte im Einzelnen betroffen sind, ist von Überwachungsmaßnahme zu Überwachungsmaßnahme sehr differenziert zu sehen. Hierfür muss zunächst der Schutzbereich dieser Grundrechte und ihre nähere Auslegung weiter umrissen werden.

8.1. Art 10a StGG - Fernmeldegeheimnis

In Österreich wird in der Staatsrechtslehre davon ausgegangen, dass der Schutzbereich von Art 10a StGG eher eng auszulegen ist. Das Fernmeldegeheimnis in seiner jetzigen Form wurde 1975 eingeführt; zu dieser Zeit fielen bei einem Kommunikationsvorgang noch verhältnismäßig wenige Daten an. Dennoch kann die Einführung als originäres österreichisches Grundrecht als spät bezeichnet werden, da Fernmeldevorgänge bereits in der Nachkriegszeit in größerem Maße existierten. Man sah jedoch erst an der Schwelle zum Kommunikationszeitalter die Notwendigkeit, das Fernmeldegeheimnis parallel zum Briefgeheimnis legislativ nachzuziehen.³¹⁴

Das Fernmeldegeheimnis schützt hierbei jedenfalls den Inhalt des Fernmeldevorgangs.³¹⁵ Vom Schutzbereich umfasst ist somit, was Personen geschützt vor dem Zugriff Dritter untereinander kommunizieren. In welcher Form kommuniziert wird (Telefongespräch, Chat, E-Mail, etc), ist dabei nicht von Belang. Das Fernmeldegeheimnis erweist sich insofern als technikoffen. Der Schutzbereich endet dann, wenn der Kom-

³¹⁴ Morscher/Waitz, Zum Schutz des Briefgeheimnisses, JBl. 2008, 424, 425 f. Gleichwohl bestand 1975 bereits ein Schutz über Art 8 EMRK.

³¹⁵ Vgl Berka, Grundzüge des Verfassungsrechts⁴, Rz 1428; Hengstschläger / Leeb, Grundrechte, Rz 15/4.

munikationsvorgang beendet ist, mithin die Nachricht beim Empfänger angekommen ist.³¹⁶

Sehr umstritten ist, ob auch Verkehrsdaten in den Schutzbereich des Fernmeldegeheimnisses fallen.³¹⁷ Verkehrsdaten sind Daten, die bei Erbringung von Telekommunikationsdiensten anfallen; mithin alle Daten, die bei dem Kommunikationsvorgang anfallen, außer der Nachricht selbst. Dies wird – vor allem im Bereich der strafrechtlichen Rechtsprechung – teilweise angenommen³¹⁸ und erfuhr in der Literatur teilweise Unterstützung,³¹⁹ stieß aber in der Verfassungsrechtslehre in Österreich mehrheitlich auf Ablehnung.³²⁰

Hierbei wird oft historisch argumentiert und darauf abgestellt, welchen Schutzzumfang der Gesetzgeber bei Gesetzeserlass im Auge hatte.³²¹ In diesem Zusammenhang wird vielfach darauf abgestellt, dass Art 10a StGG dem Briefgeheimnis in Art 10 StGG nachgebildet ist und dieses nur den Inhalt der Nachricht schützt.³²² Diese Vorgehensweise mag bei unveränderten Sachverhalten folgerichtig sein. Schließlich spricht nichts dafür, eine unveränderte Sachlage einer neuen Bewertung zu unterziehen, wenn der Gesetzgeber im Rahmen des Gesetzgebungsprozesses bereits alles abgewogen und berücksichtigt hat; umgekehrt konnte der Gesetzgeber des Jahres 1975 nicht die Entwicklung der modernen Kommunikation in ihrer jetzigen Form voraussehen.

³¹⁶ Dies schlägt sich auch strafprozessual nieder. Ein Durchsehen gespeicherter Nachrichten auf einem beschlagnahmten Mobiltelefon ist nicht als „Überwachung von Nachrichten“ im Rahmen des § 134 Nr. 3 StPO zu verstehen, vgl hierzu *Reindl-Krauskopf* in WK-StPO, § 134, Rz 55 mwN.

³¹⁷ Zusammenfassend *Regenfelder*, Ermittlungsmaßnahmen bei neuen Informationstechnologien im Spannungsverhältnis zum Grundrechtsschutz, 19.

³¹⁸ OGH 26.7.2005, 11 Os 57/05Z; OGH 6.12.1995, 13 Os 161/95 ; OGH v. 17.6.1998, 13 Os 68/98.

³¹⁹ *Reindl*, Telefonüberwachung zweimal neu?, JBl 2002, 69; *Satenig*, Stille Nacht, heimliche Macht Zur SPG-Novelle 2007 und der Erweiterung sicherheitspolizeilicher Ermittlungsbefugnisse, *juridikum* 2008, 130.

³²⁰ Vgl *Wessely*, Das Fernmeldegeheimnis - ein unbekanntes Grundrecht?, *ÖJZ* 1999, 491; *Wiederin* in *Korinek/Holoubek*, Österreichisches Bundesverfassungsrecht, Bd III, Art 10a StGG, Rz 12; *Himberger*, Fernmeldegeheimnis und Überwachung, 49 ff.

³²¹ Ausführlich bei *Wessely*, Das Fernmeldegeheimnis - ein unbekanntes Grundrecht?, *ÖJZ* 1999, 491. Dieser setzt das Fernmeldegeheimnis des StGG mit dem FG in Beziehung und versucht daraus abzuleiten, dass nur Inhaltsdaten umfasst sind.

³²² Zur Vergleichbarkeit beider Grundrechte vgl *Feiler* in *Zankl*, Überwachungsstaat, 67.

Nunmehr hat der VfGH entschieden, dass Verkehrsdaten im Falle von IP-Adressen, die nach § 53 Abs 3a Z 2 und 3 SPG ermittelt werden, nicht dem Schutzbereich des Art 10a StGG unterfallen.³²³ Hierbei nimmt der VfGH wohl eine Abgrenzung vor, die Verkehrsdaten grundsätzlich nicht zum Inhalt von Art 10a StGG macht, die aber wiederum diese Daten nicht völlig vom Schutzbereich des Grundrechtes ausnimmt.³²⁴ Der VfGH hat sich hierbei geschickt die Hintertür zur Einbeziehung von Verkehrsdaten in den Schutzbereich von Art 10a StGG offen gehalten. Zwar ist er der Ansicht, dass ein einzelnes Verkehrsdatum nicht unter den Schutz von Art 10a StGG fällt, jedoch bleibt bewusst offen, wie diese Frage bei einer Bündelung von Verkehrsdaten zu beurteilen ist. Mag man zugestehen, dass ein einzelnes Verkehrsdatum für sich genommen noch keinen vertieften Hinweis auf die Lebensführung und Lebensgestaltung liefert, so ist dies bei einer Vielzahl von Verkehrsdaten aus einem bestimmten Zeitraum der Fall.

Die Einbeziehung von Verkehrsdaten in den Schutzbereich von Art 10a StGG ist damit auch nach der jüngsten Entscheidung des VfGH umstritten und nicht durch die Rechtsprechung des Gerichtshofs ausgeschlossen. Zumindest die rein historische Interpretation gerät bei einem technikoffenen Grundrecht in jedem Fall zu kurz. Anhand der Überwachung von Mobiltelefonen und dem Rechtsvergleich mit Deutschland wird die Interpretation des Schutzbereiches von Art 10a StGG einer näheren Betrachtung zu unterziehen sein. Hierbei ist zu untersuchen, inwiefern eine wahrhaft technikoffene Auslegung nicht Verkehrsdaten generell mit einbeziehen muss.

Im Übrigen beantwortet auch eine Einbeziehung von Art 8 EMRK die Frage nicht zufriedenstellend. Zwar schützt Art 8 EMRK gleichermaßen den Inhalt von Telefongesprächen und darüber hinaus auch Verkehrsdaten,³²⁵ jedoch besteht insofern ein Unterschied, als dass Art 8 EMRK nicht unter einem Richtervorbehalt steht. Von daher ist die Frage, inwiefern Verkehrsdaten Art 10a StGG trotz des Grundrechtsschutzes durch die

³²³ VfGH 29. 06. 2012, B 1031/11.

³²⁴ Metzler, Verkehrsdaten nicht vom Fernmeldegeheimnis erfasst, ZTR 2012, 170, 173.

³²⁵ Brandstetter, Die Fernmeldeüberwachung öffentlicher Telefonzellen, JBl 1984, 457.

EMRK unterfallen, von großer praktischer Relevanz. Gleiches gilt für § 1 DSG 2000³²⁶, der ebenfalls im Verfassungsrang steht.³²⁷ Eingriffe in das Fernmeldegeheimnis bedürfen ohne Ausnahme eines richterlichen Befehls.³²⁸ Daher erlangt die Frage, wie weitreichend Art 10a StGG ist, an dieser Stelle Bedeutung, da der Richtervorbehalt, wenn man sich rein auf den Inhalt der Kommunikation beschränkt, nur sehr eingeschränkt Anwendung findet, wohingegen eine weite Auslegung des Schutzbereiches auch zu vielen Anwendungen des Richtervorbehaltes führen würde.

8.2. Art 8 EMRK – Recht auf Achtung des Privat- und Familienlebens

Das Recht auf Achtung des Privat- und Familienlebens in Art 8 EMRK spielt nicht nur im Rahmen des Schutzes der Berufsgeheimnisträger,³²⁹ sondern auch im Rahmen des originären Schutzes des Grundrechts der Telekommunikation eine zentrale Rolle.

Die Vorschrift des Art 8 EMRK hebt hierbei die Korrespondenz als Schutzgut hervor. Unter diese fällt jegliche Telekommunikation unabhängig davon, ob diese in geschriebener oder gesprochener Form erfolgt.³³⁰ Es können im Rahmen der Telekommunikationsüberwachung aber auch die anderen Schutzgüter von Art 8 EMRK betroffen sein.³³¹

Hier kann auf die bereits gewonnenen Erkenntnisse zum Berufsgeheimnisträgerschutz Bezug genommen werden. Die Vorschrift des Art 8 EMRK zeigt sich damit als Grundrecht, dessen Vielgestaltigkeit für den Berufsgeheimnisträgerschutz von herausragender Bedeutung ist.

³²⁶ Die Verfassungsnorm des § 1 Abs 1 DSG normiert das Geheimhaltungsinteresse an Personenbezogenen Daten; vgl *Dohr/Pollirer/Weiss/Knyrim*, § 1 Anm 2.

³²⁷ Vgl hierzu *Schmölzer*, JBl 1997, 211, die ebenfalls einen Schutz von Verbindungsdaten durch Art 10a StGG bejaht.

³²⁸ *Hengstschläger/Leeb*, Grundrechte, Rz 15/4 mwN.

³²⁹ Vgl näher hierzu unter 3.2.

³³⁰ *Meyer-Ladewig*, EMRK, Art 8, Rz 92.

³³¹ *Meyer-Ladewig*, EMRK, Art 8, Rz 33.

8.3. § 1 DSG 2000– Grundrecht auf Datenschutz

Das DSG 2000 ist nicht nur die österreichische Umsetzung der RL 95/46/EG³³² zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.³³³ Dem Gesetz ist auch eine Verfassungsnorm in § 1 DSG vorangestellt, die wiederum an Art 8 EMRK angelehnt ist,³³⁴ allerdings bedarf eines keines Bezugs zum Privatleben des Betroffenen, was § 1 DSG 2000 wiederum von Art 8 EMRK unterscheidet. Diese gibt die Grundlinien des Datenschutzes vor und ist als Verbot mit Erlaubnisvorbehalt zu sehen.³³⁵ Eingriffe von staatlicher Seite stehen gemäß § 1 Abs 1 S 1 DSG 2000 unter einem Gesetzesvorbehalt, wobei sich dieser wiederum an Art 8 Abs 2 EMRK messen lassen muss.³³⁶

Das Grundrecht auf Datenschutz ist jedoch keine Erfindung des DSG 2000, sondern war bereits in der Vorgängerregelung, dem § 1 DSG 1978, enthalten. Dies bedeutet aber nicht, dass § 1 DSG 2000 nur eine datenschutzspezifische Wiederholung von Art 8 EMRK darstellt. Vielmehr verbreitert § 1 DSG 2000 den Schutz im Vergleich zu Art 8 EMRK, indem das Grundrecht auf Datenschutz nicht nur explizit die Geheimhaltung personenbezogener Daten statuiert, sondern auch Auskunfts- und Löschungsansprüche Betroffener beinhaltet³³⁷ und diesen Verfassungsrang zuweist.³³⁸ Auch nach Inkrafttreten der Datenschutzgrundverordnung wird Art 1 DSG 2000 als neuer Art 1 DSG³³⁹ unverändert fortbestehen.

³³² Auch durch die DSGVO kommt es beim österreichischen Datenschutz hier zu keiner Änderung. Im DSG, dem reformierten DSG 2000, wird § 1 DSG unverändert bleiben. Ursprünglich sollte das Grundrecht auf Datenschutz ebenfalls reformiert werden, unter anderem dadurch, dass juristische Personen aus dem Schutzbereich von § 1 DSG ausgenommen werden, aufgrund der fehlenden Verfassungsmehrheit wurden aber nur jene Teile des DSG, die nicht im Verfassungsrang stehen, an die DSGVO angepasst. Vgl zum Gesetzgebungsverfahren den Bericht des Verfassungsausschusses über die Regierungsvorlage 1761 der Beilagen (abrufbar unter https://www.parlament.gv.at/PAKT/VHG/XXV/II/I_01761/index.shtml).

³³³ Sog EG-Datenschutzrichtlinie.

³³⁴ Knyrim, Datenschutzrecht², 7.

³³⁵ Knyrim, Datenschutzrecht², 9.

³³⁶ Dazu näher Auer, Grundrecht auf Datenschutz, 40.

³³⁷ Vgl zu diesen Nebenrechten Hengstschläger/Leeb, Grundrechte, Rz 13/7 ff.

³³⁸ Hengstschläger/Leeb, Grundrechte, Rz 13/1.

³³⁹ Ursprünglich waren Änderungen geplant, wie etwa die Entfernung von juristischen Personen aus dem Schutzbereich. Da es jedoch an einer Verfassungsmehrheit fehlte wurde das Datenschutzanpassungsge-

Dass hier eine besondere Art des Grundrechtsschutzes vorliegt wird dadurch deutlich, dass, ein Aspekt des Verhältnismäßigkeitsgrundsatzes in § 1 Abs 2 S 3 DSG 2000 explizit festgeschrieben³⁴⁰ ist: „*Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.*“ Dies ist für ein Grundrecht eher unüblich. Bereits der Verweis auf Art 8 Abs 2 EMRK statuiert ein Verhältnismäßigkeitsgebot, welches durch die nochmalige Erwähnung im DSG 2000 quasi gedoppelt wird.³⁴¹ Durch diese Verdoppelung der Verhältnismäßigkeit ist insgesamt ein strengerer Maßstab anzulegen als bei Art 8 EMRK.³⁴²

8.4. § 1 HausrechtsG, Art 9 StGG – Schutz des Hausrechts

Im Rahmen der Telekommunikationsüberwachung liegt dieses Grundrecht zunächst eher fern, müssen doch Ermittler gerade nicht in die Wohnung eines Verdächtigen eindringen, sondern können sich Zugriff von außen verschaffen. Inwiefern dieser Eingriff nicht grundrechtsintensiver ist, wurde bislang in der österreichischen Judikatur und Literatur nicht näher behandelt. Parallelen zu anderen Grundrechten wurden noch nicht aufgezeigt.

Hier kann, soviel kann vorweg genommen werden, die Rechtsprechung des deutschen BVerfG zum sog „Online-Grundrecht“³⁴³ für Österreich insofern interessant sein, als dass zu diskutieren sein wird, ob sich nicht verfassungsrechtliche Parallelen in Österreich auch anbieten, bzw geradezu aufdrängen.

setz ohne Änderung der Verfassungsbestimmung beschlossen, vgl Ministerialentwurf Gesetzestext 322/ME XXV. GP.

³⁴⁰ Dazu *Hengstschläger/Leeb*, Grundrechte, Rz 13/5 mit Verweis auf VfSlg 18.146/2007.

³⁴¹ So auch *Öhlinger*, Verfassungsrecht⁸, Rz 830.

³⁴² Vgl auch VfSlg 16.369/2001.

³⁴³ Vgl hierzu unter 9.3.

9. Verfassungsrechtliche Vorgaben für die Überwachung von Telekommunikation in Deutschland

Die verfassungsrechtlichen Vorgaben in Deutschland speisen sich zum Teil aus dem geschriebenen, teils aus dem ungeschriebenen Verfassungsrecht. Im Folgenden soll ein Überblick über die betroffenen Grundrechte aus Sicht der deutschen Verfassungsrechtsordnung gegeben werden.

In Deutschland sind teilweise gleiche, teils andere Grundrechte betroffen. Hierbei ist jedoch auf den exakten Schutzbereich zu achten; nur weil ein Grundrecht, wie etwa das Fernmeldegeheimnis, durch eine ähnlich lautende Vorschrift geschützt ist, heißt das nicht, dass die Interpretation zum Schutzbereich des Grundrechts nicht stark abweicht, was sich wiederum unmittelbar auf den Grundrechtsschutz auswirken kann.

9.1. Art 10 GG – Fernmeldegeheimnis

Auch das deutsche Verfassungsrecht kennt den Schutz des Fernmeldegeheimnisses in Art 10 GG. Diese Vorschrift geht historisch bereits auf Art 117 WRV zurück,³⁴⁴ was das deutsche Fernmeldegeheimnis zu einem Grundrecht macht, das wesentlich älter ist, als sein österreichisches Pendant. Der Schutzbereich des Grundrechts ist hierbei sehr weit zu fassen. Art 10 GG stellt einen wichtigen Teil der menschlichen Privatsphäre dar und schützt damit letztlich auch die Menschenwürde.³⁴⁵

Umfasst sind sowohl die Inhalte als auch die Umstände der Kommunikation. Un-
erheblich sind die Übertragungsart³⁴⁶ und Ausdrucksform.³⁴⁷ Auch Internetnutzung fällt darunter.³⁴⁸ Der Schutz geht also im Unterschied zu Österreich über bloße Inhalte der Kommunikation weit hinaus. Umfasst werden alle näheren Umstände der Telekommu-

³⁴⁴ Durner in Maunz/Dürig, GG, Art 10, Rz 81.

³⁴⁵ Baldus in BeckOK, GG, Art 10, Rz 1.

³⁴⁶ Dies stellte das BVerfG in seiner Entscheidung zur Online-Durchsuchung dar, vgl BVerfG MMR 2008, 315, 316.

³⁴⁷ BVerfGE 106, 28, 36; vgl hierzu auch Pagenkopf in Sachs, Grundgesetz⁶, Art 10, Rz 14.

³⁴⁸ BVerfG MMR 2008, 315, 316 mit Verweis auf BVerfGE 113, 348, 383, wo entschieden wurde, dass sich Art 10 GG auch auf E-Mails erstreckt.

nikation. Hiervon sind alle Daten erfasst, die darauf schließen lassen, ob, mit wem und wann kommuniziert wurde.³⁴⁹

Der Schutz des Fernmeldegeheimnisses beginnt, sobald der Telekommunikationsvorgang seinen Anfang nimmt. Er endet mit Abschluss des Vorgangs, also dann, wenn der Empfänger die Nachricht erhalten hat und die Übertragung beendet ist.³⁵⁰ Er kann enden, wenn der Empfänger die Nachricht zur Kenntnis genommen hat, dies muss aber nicht zwingend der Fall sein.³⁵¹

Das Fernmeldegeheimnis ist, obwohl ursprünglich nur für Telefon- und Telegrafendienste eingeführt, technikoffen.³⁵² Entscheidend ist lediglich, dass im Verborgenen kommuniziert wird, die Kommunikation also nicht öffentlich zugänglich ist.³⁵³ Das Fernmeldegeheimnis soll umfassend gewährleistet werden und den Effekt erzielen, dass kein Beteiligter an einem Telekommunikationsvorgang diesen unterlässt, weil er eine staatliche Überwachung in diesem Bereich fürchtet.³⁵⁴ Dies gilt im Übrigen auch bei Überwachungen mit Auslandsbezug, da die deutsche Staatsgewalt aufgrund von Art 1 Abs 3 GG stets grundrechtsgebunden ist.³⁵⁵ Das Fernmeldegeheimnis gilt dabei nicht nur im Staat-Bürger-Verhältnis, sondern erfährt durch Normen des Zivil- und Strafrechts auch in gewissem Umfang unter Privaten Anwendung.³⁵⁶

Hervorzuheben bei den bisherigen Ausführungen ist, dass sämtliche Verkehrsdaten vom Fernmeldegeheimnis erfasst sind. Dies waren früher recht wenige, relativ „bedeutungsarme“ Daten³⁵⁷: So wurden während der Telefonverbindung Schaltungen durch elektromechanische Stellgeräte bewirkt, die nach Ende eines Telefonats in die

³⁴⁹ BVerfG MMR 2008, 315, 316 mit Verweis auf die ständige Rechtsprechung des Gerichts.

³⁵⁰ *Baldus* in BeckOK, GG, Art 10, Rz 8; dazu klarstellend *Käß*, BayVBl. 2007, 135.

³⁵¹ Zum Beispiel dann, wenn ein Mail nicht abgerufen wird, sondern auf dem Mailserver verbleibt, vgl *Baldus* in BeckOK, GG, Art 10, Rz 10.3.

³⁵² Vgl *Pagenkopf* in Sachs, Art 10, Rz 14.

³⁵³ Vgl *Pagenkopf* in Sachs, Art 10, Rz 14a.

³⁵⁴ BVerfGE 100, 313, 358.

³⁵⁵ Vgl *Pagenkopf* in Sachs, Art 10, Rz 14a mit Verweis auf BVerfGE 6, 290, 295; 57, 1, 23.

³⁵⁶ So z B bei Abtretung von Forderungen aus Verträgen aus Telekommunikationsverträgen. Vgl hierzu *Geuer*, Das Fernmeldegeheimnis als gesetzliches Verbot, ZD 2012, 515; vgl hierzu auch *Schatzschneider*, Fernmeldegeheimnis und Telefonbeschattung, NJW 1981, 268.

³⁵⁷ Vgl *Welp*, Strafprozessuale Zugriffe auf Verbindungsdaten des Fernmeldeverkehrs, NStZ 1994, 209, 209 f.

Ausgangsposition zurückkehrten. Lediglich das Entgelt wurde gezahlt, der Kommunikationsvorgang war im Anschluss an die Verbindung nicht mehr nachvollziehbar. Folglich erlangten diese Daten erst mit fortschreitender Digitalisierung und der Verbreitung neuer Technologien, wie Mobilfunk, immer größere Wichtigkeit.

Die Einbeziehung von Verkehrsdaten in den Schutzbereich von Art 10 GG stellt sich als folgerichtig dar und ist an die technischen Möglichkeiten der heutigen Zeit angepasst. So ist die Tatsache, dass zwei Personen miteinander kommuniziert haben, oftmals ebenso brisant, wie der Inhalt der Kommunikation selbst,³⁵⁸ zumal bei Mobilfunktelefonaten auch Standortdaten anfallen. Damit zeigt sich Art 10 GG als modernes, wirklich technikoffenes Grundrecht, das den Fernmeldeverkehr wirksam schützt.

Die Vorschrift des Art 10 GG enthält keinen Richtervorbehalt. Eingriffe in das Fernmeldegeheimnis nach Art 10 Abs 1 GG sind „auf Grund eines Gesetzes“ möglich. Der fehlende präventive Richtervorbehalt ist rechtshistorisch gesehen überraschend,³⁵⁹ findet sich aber auch in den Verfassungen der deutschen Bundesländer nicht.³⁶⁰

Die Ansichten bezüglich eines Richtervorbehalts schienen bis vor kurzem einheitlich zu sein. Bislang wurde sowohl von Seiten der Judikatur³⁶¹ als auch von Seiten der Literatur³⁶² überwiegend nicht davon ausgegangen, dass im Rahmen von Art 10 GG ein Richtervorbehalt in ungeschriebener Form besteht. Insofern wird vom klaren Wortlaut der Vorschrift ausgegangen,³⁶³ der den Richtervorbehalt *expressis verbis* nicht vorsieht.³⁶⁴ Als Argument hierfür kann auch herangezogen werden, dass ein richterlicher Vorbehalt dem Grundgesetz nicht fremd ist, sondern zum Beispiel bei der Unverletz-

³⁵⁸ Vgl hierzu die Entscheidung des BVerfG über das Verhältnis von Art 10 GG und dem Redaktionsgeheimnis von Journalisten, BVerfG NJW 2003, 1787.

³⁵⁹ Dazu Durner in Maunz/Düring, GG, Art 10, Rz 152.

³⁶⁰ Lediglich in der Verfassung des Landes Brandenburgs findet sich der Richtervorbehalt, jedoch nicht als präventive Maßnahme, vgl Art 16 Abs 2 BbgVerf.

³⁶¹ Vgl BVerfG NJW 2005, 1637, 1639.

³⁶² Vgl Kutscha, Rechtsschutzdefizite bei Grundrechtseingriffen von Sicherheitsbehörden, NVwZ 2003, 1296, 1299.

³⁶³ Dazu auch Badura in Bonner Kommentar, Art 10, Rz 59, der klarstellt, dass auch andere Schranken, die dem Grundgesetz bekannt sind, z B jene von Art 2 GG, nicht sinngemäß auf Art 10 GG angewendet werden können.

³⁶⁴ So zusammenfassend Durner in Maunz/Düring, GG, Art 10, Rz 152.

lichkeit der Wohnung in Art 13 Abs 2 GG ausdrücklich vorgesehen ist.³⁶⁵ Wäre also ein entsprechender Vorbehalt vom Gesetzgeber gewollt, hätte er ihn in die Vorschrift entsprechend eingefügt. Für eine weitergehende Interpretation verbleibt somit schlichtweg kein Raum.

Diese jahrelang unumstrittene Ansicht könnte durch die jüngere Rechtsprechung des BVerfG es nunmehr einem teilweisen Paradigmenwechsel unterliegen. Hierbei hat sich das Gericht zu weiteren Grundrechten geäußert, die bei Überwachungen ebenfalls betroffen sind, und – relativ überraschend – einen Richtervorbehalt angenommen. Zu nennen wäre zunächst das Urteil zur sog „Online-Durchsuchung“³⁶⁶, bei dem das BVerfG das sog Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme³⁶⁷ als besondere Auswirkung des allgemeinen Persönlichkeitsrechts und der Menschenwürde (Art 2 Abs 1 GG iVm Art 1 GG) entwickelt hat. Dies ist nicht zuletzt deswegen geschehen, um Rechtsschutzlücken dort zu schließen, wo das Fernmeldegeheimnis nicht greift.³⁶⁸

Insofern drängt sich in einem „Erst-Recht-Schluss“ auf, dass, wenn für das Grundrecht, welches die Lücken schließt, die bei Art 10 GG verbleiben, ein Grundrechtseingriff unter „den Vorbehalt richterlicher Anordnung zu stellen“³⁶⁹ ist, dies denklogisch bei Art 10 GG auch der Fall sein muss. Diese Ansicht ist insofern überzeugend, als dass sie das Grundrecht und die Schwere der Eingriffe in einen modernen

³⁶⁵ Auch dies ist nicht selbstverständlich, da ein Richtervorbehalt an dieser Stelle auch vielen Landesverfassungen nicht bekannt ist. So gewährt die Bayerische Verfassung in Art 106 Abs 1 BV ein zunächst soziales Grundrecht auf angemessenen Wohnraum, das in Art 106 Abs 3 BV eine, über den Programmsatz hinausgehende, Grundrechtskomponente ergänzt wird. Ein Richtervorbehalt fehlt ebenfalls und kann allenfalls im Rahmen der Verhältnismäßigkeitsabwägung berücksichtigt werden, vgl hierzu *Lindner* in *Lindner/Möstl/Wolf*, BV, Art 106, Rz 36.

³⁶⁶ BVerfGE 120, 274 ff.

³⁶⁷ In der Praxis zumeist kurz als „IT-Grundrecht“ bezeichnet, wobei diese Bezeichnung strenggenommen nicht ganz korrekt ist, da es sich ja nicht um ein ganz neues Grundrecht handelt, sondern lediglich um eine bislang unbekannte Ausprägung von Art 2 Abs 1 GG iVm Art 1 Abs 1 GG; Näheres zum „IT-Grundrecht“ sogleich.

³⁶⁸ Vgl dazu *Britz*, Vertraulichkeit und Integrität informationstechnischer Systeme, DÖV 2008, 411, 413 f. Das „neue Grundrecht“ schließt die Lücke zwischen Art 10 GG und Art 13 GG (Unverletzlichkeit der Wohnung).

³⁶⁹ BVerfGE 120, 274, 331 ff.

rechtlichen Kontext stellt, der die technische Entwicklung der letzten Jahre mit berücksichtigt. Ein Eingriff in Art 10 GG mag heute schwerer wiegen als vor einigen Jahren.

Als weiteres Argument kann Art 13 GG (Unverletzlichkeit der Wohnung) herangezogen werden, für den in Art 13 Abs 2 GG ein Richtervorbehalt vorgesehen ist. Dieser schützt die Wohnung und demgemäß auch dort getätigte Äußerungen, jedoch erlaubt und begünstigt moderne Kommunikation, dass Telekommunikation, die früher ortsgebunden nur aus der eigenen Wohnstätte erfolgen konnte, mittlerweile von jedem Ort aus erfolgen kann.

9.2. Art 2 Abs 1 GG iVm Art 1 Abs 1 GG – Grundrecht auf informationelle Selbstbestimmung

Deutschland ist ein explizites Grundrecht auf Datenschutz oder Ähnliches im geschriebenen Verfassungsrecht fremd. Ein entsprechendes Grundrecht, das sich spezifisch auf den Schutz persönlicher Daten richtet existiert im Grundrechtekatalog des GG nicht. Trotzdem genießen personenbezogene Daten einen umfassenden grundrechtlichen Schutz. In seiner Rechtsprechung hat das deutsche BVerfG aus dem allgemeinen Persönlichkeitsrecht in Art 2 Abs 1 GG iVm mit der Menschenwürde in Art 1 Abs 1 GG das *Grundrecht auf informationelle Selbstbestimmung* abgeleitet³⁷⁰ und seither kontinuierlich ausdefiniert und fortentwickelt.³⁷¹

Das Gericht trat hierbei – wie so oft³⁷² – als eine Art „Ersatzgesetzgeber“³⁷³ auf und entwickelte auf Grundlage bestehender Verfassungsnormen eine Art eigenes

³⁷⁰ Erstmals entwickelt im sog. „Volkszählungs-Urteil“, BVerfGE 65, 1 = NJW 1984, 419; Grundlagen bereits bei *Rüpke*, Der verfassungsrechtliche Schutz der Privatheit, 25.

³⁷¹ Vgl hierzu *di Fabio* in Maunz/Dürig, GG, Art 2, Rz 173 mwN.

³⁷² Vgl krit zur Rolle von Gerichten als „Gesetzgeber“ *Steiner*, NJW 2001, 2919; *Schlaich/Korioth*, Das Bundesverfassungsgericht⁵, Rz 426.

³⁷³ *Di Fabio* spricht hierbei auch von einem „Grundrecht auf Datenschutz“, welches eigentlich vom Gesetzgeber zu schaffen sei und kritisiert dessen Untätigkeit auf dem Gebiet scharf; vgl *di Fabio* in Maunz/Dürig, GG, Art 2, Rz 173 mwN; Kritik findet sich auch bei *Albers*, Informationelle Selbstbestimmung, 176 f. Hierbei kritisiert *Albers* vor allem, dass es eine Diskrepanz zwischen der Herleitung des Rechts auf informationelle Selbstbestimmung und der Beschreibung des Schutzgehaltes gibt. Im Rahmen des Umreißen des Schutzbereiches werde nicht klar, inwiefern die Selbstbestimmungsidee in Bezug auf persönliche Daten überhaupt folgerichtig ist.

Grundrecht,³⁷⁴ welches von sich vom Charakter her verselbständigt hat.³⁷⁵ Hierbei mag man aus rechtsdogmatischen Gründen nicht von einem eigenen Grundrecht sprechen, jedoch wird man de facto davon ausgehen müssen, dass das BVerfG durch seine Praxis Verfassungsrecht schafft, welches der Verfassungsgesetzgebung wenigstens vorauseilt, in den Fällen in denen der Bundestag ex post noch tätig wird, oder, was zumeist der Fall ist, diese ersetzt, da im Nachhinein keine Änderung des GG erfolgt.

In seiner Entscheidung greift das BVerfG eine ältere Entscheidung, den „Mikrozensus-Beschluss“³⁷⁶, wieder auf. In dieser Entscheidung befasste sich das Gericht mit der Verfassungsmäßigkeit der Erstellung einer Repräsentativstatistik. Dabei hielt das BVerfG vor allem fest, dass durch seine statistische Erfassung (von staatlicher Seite) der Mensch nicht zum Objekt degradiert werden dürfe.³⁷⁷ Nunmehr ging das BVerfG im „Volkszählungs-Urteil“ weit über die im „Mikrozensus-Beschluss“ entwickelten Grundsätze hinaus.

Das dabei herausgearbeitete Grundrecht umfasst in seinem Kern das Selbstbestimmungsrecht des Individuums über seine personenbezogenen Informationen.³⁷⁸ Der Begriff des personenbezogenen Datums ist hierbei laut Gericht sehr weit zu ziehen und umfasst auch StimmAufnahmen oder Bilder einer Person.³⁷⁹ Hierbei umfasst das Grund-

³⁷⁴ Rein dogmatisch entwickelte das BVerfG kein neues Grundrecht, sondern entwickelte in seiner Rechtsprechung ein bereits bestehendes Grundrecht entsprechend weiter, vgl. *Simitis*, Datenschutz und Neue Medien, NJW 1984, 394, 399. Aus Gründen der Praktikabilität wird jedoch in Rechtsprechung und Literatur stets vom „Grundrecht auf informationelle Selbstbestimmung“ gesprochen.

³⁷⁵ Vgl. *Lorenz* in Bonner Kommentar GG, Art 2, Rz 334 f.; dies wird dadurch deutlich dass Art 2 Abs 1 GG in Form der informationellen Selbstbestimmung nicht mehr reines Auffanggrundrecht ist, sondern auch dann, wenn der Grundrechtsangriff zusätzlich andere Grundrechte betrifft (z. B. Art 13 GG) ergänzend hinzutritt und damit wie eine eigenes Grundrecht behandelt wird.

³⁷⁶ BVerfGE 27, 1 = JW 1969, 1707.

³⁷⁷ Zusammenfassend hierzu *Albers*, Informationelle Selbstbestimmung, 153 f.

³⁷⁸ *Di Fabio* in Maunz/Dürig, GG, Art 2, Rz 175 mwN; *Murswiek* in Sachs, Grundgesetz⁶, Art 2, Rz 73.

³⁷⁹ Vgl. zum Umfang *Jarass*, Das allgemeine Persönlichkeitsrecht im Grundgesetz, NJW 1989, 857, 858; zur näheren Eingrenzung auch *Geuer*, Digitale Identität, 24 f.

recht das Erheben, Verarbeiten, Speichern, Verwenden,³⁸⁰ sowie darüber hinaus auch das Weitergeben personenbezogener Daten.³⁸¹

Außerdem geht das BVerfG davon aus, dass ein privater Kernbereich besteht, der jeglicher staatlicher Einsichtnahme entzogen ist.³⁸² Spiegelbildlich zum besonderen Schutz für den Kernbereich der Lebensführung gibt es keinen „schutzlosen“ Raum für besonders profane Daten; auch diese unterfallen dem Schutzbereich.³⁸³ Lediglich dann, wenn personenbezogene Daten für eine extrem kurze Zeitspanne anfallen und dann sofort wieder unwiederbringlich gelöscht werden, ist ein Eingriff in den Schutzbereich zu verneinen.³⁸⁴

Auch im Rahmen der Telekommunikation erlangt das Grundrecht auf informationelle Selbstbestimmung insofern Relevanz, als dass es auch Kommunikationsverbindungsdaten schützt, die nach Abschluss des Übertragungsvorgangs noch im Machtbereich des Kommunikationsteilnehmers vorhanden sind; hierbei wird das Grundrecht gegebenenfalls von Art 13 GG (Unverletzlichkeit der Wohnung) flankiert.³⁸⁵

³⁸⁰ Geschützt sind Daten dabei auch vor Zweckentfremdung *Polenz* in Kilian/Heussen, Computerrechtshandbuch³¹, Teil 13, Rz 25.

³⁸¹ Zusammenfassend *Jarass*, Das allgemeine Persönlichkeitsrecht im Grundgesetz, NJW 1989, 857, 858; welche Daten letztlich personenbezogen sind, ist nicht unumstritten und kann in Einzelfällen schwierig zu bestimmen sein; vgl hierzu *Forgó/Krügel*, Der Personenbezug von Geodaten - Cui bono, wenn alles bestimmbar ist?, MMR 2010, 17, 18 ff und *Meyerdierks*, Sind IP-Adressen personenbezogene Daten?, MMR 2009, 8, 11 ff. Zur Frage, welche Vorkehrungen bei der Anonymisierung und Pseudonymisierung von Daten getroffen werden müssen, also wann diese ausreichend vom Personenbezug getrennt sind, vgl *Roßnagel/Scholz*, Datenschutz durch Anonymität und Pseudonymität - Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, 721, 730.

³⁸² BVerfG NJW 1990, 563 zur Nichtverwertbarkeit von Tagebuchaufzeichnungen; hierzu *Strömer*, Verwertung tagebuchartiger Aufzeichnungen, NStZ 1990, 397.

³⁸³ Vgl *Polenz* in Kilian/Heussen, Computerrechtshandbuch³¹, Teil 13, Rz 24; zusammenfassend *Hornung*, Zwei runde Geburtstage: Das Recht auf informationelle Selbstbestimmung und das WWW, MMR 2004, 3, 4.

³⁸⁴ BVerfG MMR 2008, 308, 309 für den Fall der automatisierten Kennzeichenerfassung. Hierbei ist das Grundrecht auf informationelle Selbstbestimmung dann nicht betroffen, wenn Daten erhoben werden, ein Abgleich mit einer Datenbank stattfindet und die Daten dann, mangels „Treffer“ sofort gelöscht wurden und damit nur ein paar Sekunden vorlagen. Das Grundrecht ist aber dann betroffen, wenn die Daten entweder nicht sofort gelöscht werden, um sie später nochmals auszuwerten (Speicherung auf Vorrat) oder in den Fällen, in denen ein „Treffer“ vorliegt und die Daten deswegen dauerhaft gespeichert werden sollen.

³⁸⁵ Vgl *Polenz* in Kilian/Heussen, Computerrechtshandbuch³¹, Teil 13, Rz 22 mit Verweis auf BVerfGE 115, 166, 183 = NJW 2006, 976.

9.3. Art 2 Abs 1 GG iVm Art 1 Abs 1 GG – Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme

Neue technische Sachverhalte zwangen das BVerfG, das Persönlichkeitsrecht nochmals weiterzuentwickeln, damit keine Grundrechtslücken entstanden. In der Entscheidung³⁸⁶ zur sog Online-Durchsuchung im Verfassungsschutzgesetz des deutschen Bundeslandes Nordrhein-Westfalen, erkannte das BVerfG den grundrechtlichen Schutz auf Integrität und Vertraulichkeit informationstechnischer Systeme an.³⁸⁷ Es wird auch kurz als „IT-Grundrecht“³⁸⁸ oder „Computer-Grundrecht“³⁸⁹ bezeichnet.³⁹⁰

Diese Entwicklung ist konsequent und erschließt sich im historischen Kontext. Vor einer allgegenwärtigen Vernetzung von Computern, waren die meisten Daten, sofern diese überhaupt auf Computern gespeichert waren, nur „offline“ verfügbar. Um in diese Daten Einsicht zu nehmen, waren die Ermittler grundsätzlich gezwungen, einen richterlichen Durchsuchungsbeschluss zu erwirken; eine Rahmenbedingung, die verfassungsrechtlich Art 13 GG vorgibt.

In dem Ausgangsfall zur Online-Durchsuchung in Nordrhein-Westfalen, war es dem dortigen Landesverfassungsschutz gestattet worden, Computer von Verdächtigen, die mit dem Internet verbunden sind, ohne Beschlagnahme „von außen“ mithilfe des Internet heimlich zu durchsuchen. Diese Fallgestaltung lieferte auch den Präzedenzfall für den Schutzbereich des Grundrechts: Der Schutzbereich umfasst alle vernetzten IT-Systeme,³⁹¹ die eine Vielzahl personenbezogener Daten enthalten, so dass sich durch ein Bild über die Persönlichkeit des Überwachten gewinnen lässt.³⁹² Dies ist also bei gewöhnlichen Personal Computern ohne Weiteres der Fall, ebenso wie bei Smartphones oder ähnlichen technischen Geräten; aus dem Schutzbereich fallen lediglich technische

³⁸⁶ BVerfGE 120, 274 = NJW 2008, 822 = MMR 2008, 315.

³⁸⁷ BVerfG NJW 2008, 822, 825.

³⁸⁸ So etwa *Lang* in BeckOK, GG, Art 2, Rz 46.

³⁸⁹ Vgl *Murswiek* in Sachs, Grundgesetz⁶, Art 2, Rz 73b.

³⁹⁰ Wie bereits in Fn 375 erläutert handelt es sich um kein „neues“ Grundrecht, sondern – wie beim Grundrecht auf informationelle Selbstbestimmung – um eine neue Interpretation und Ausprägung aus Art 2 Abs 1 GG und 1 Abs 1 GG.

³⁹¹ *Polenz* in Kilian/Heussen, Computerrechtshandbuch³¹, Teil 13, Rz 29.

³⁹² *Roßnagel/Schnabel*, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, NJW 2008, 3534, 3535.

Systeme, die nur einen geringen Bezug zum Überwachten haben.³⁹³ Geschützt wird vorrangig das Nutzerinteresse, dass von außen nicht heimlich³⁹⁴ auf dessen System zugegriffen wird.³⁹⁵

Das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme ist also immer dann berührt, wenn dem berechtigten³⁹⁶ Nutzer die Verfügungsgewalt über das System entzogen wird; dieser muss das System als sein eigenes gebrauchen können und kann folglich auch Dritte, und damit auch staatliche Stellen, von der Nutzung ausschließen können.³⁹⁷

Hinsichtlich des „IT-Grundrechts“ ergeben sich große Abgrenzungsschwierigkeiten zu anderen Grundrechten. Deutlich ist die Abgrenzung zum Fernmeldegeheimnis aus Art 10 GG. Im Rahmen von Maßnahmen, die das „IT-Grundrecht“ betreffen, findet keine Telekommunikation statt, so dass auch Art 10 GG nicht betroffen ist. Viel unschärfer ist die Abgrenzung zum Grundrecht auf informationelle Selbstbestimmung.

Zu Recht weist *Britz* darauf hin, dass die Abgrenzung zwischen dem Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme und dem Grundrecht auf informationelle Selbstbestimmung mehr als unscharf sei, da das BVerfG offenbar davon ausgeht, dass durch das Grundrecht auf informationelle Selbstbestimmung lediglich ein Schutz des Betroffenen gegenüber einzelnen Datenzugriffen gewährt wird, wohingegen das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme eine Lücke schließe, da es eine umfassende Privatheit gewährleiste.³⁹⁸ Diese

³⁹³ *Roßnagel/Schnabel* nennen hier beispielsweise Anlagen der Haustechnik; *Roßnagel/Schnabel*, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, NJW 2008, 3534, 3535; dazu auch *Polenz* in Kilian/Heussen, Computerrechtshandbuch³¹, Teil 13, Rz 33.

³⁹⁴ Hierin sieht *Polenz* ein Problem, der den Schutz auch bei nicht-heimlichem Beobachten bejaht, da sich dadurch auch ein aussagekräftiger Datenbestand gewinnen ließe; vgl. *Polenz* in Kilian/Heussen, Computerrechtshandbuch³¹, Teil 13, Rz 32. Diese Problematik dürfte jedoch von sehr geringer Praxisrelevanz sein, da die meisten Überwachungsmaßnahmen in der Regel darauf angelegt sein werden, dass der Zugriff auf das informationstechnische System heimlich erfolgt.

³⁹⁵ *Brink* in BeckOK, BDSG, Syst. C., Rz 147.

³⁹⁶ Zweifelnd *Hoeren*, Was ist das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme?, MMR 2008, 365, 366.

³⁹⁷ *Polenz* in Kilian/Heussen, Computerrechtshandbuch³¹, Teil 13, Rz 36.

³⁹⁸ *Britz*, Vertraulichkeit und Integrität informationstechnischer Systeme, DÖV 2008, 411, 412.

Interpretation wäre aber nicht zwingend gewesen und hat das Grundrecht auf informationelle Selbstbestimmung zu eng ausgelegt.³⁹⁹

In diesem Zusammenhang erweist es sich auch als Widerspruch, dass das BVerfG im Jahr 2005 die Kopie aller Daten auf der Festplatte eines Strafverteidigers als vom Grundrecht auf informationelle Selbstbestimmung umfasst angesehen.⁴⁰⁰ Hierbei ist fraglich, wie das Gericht einen solchen Zugriff werten würde, wenn er heimlich von außen erfolgt. Nach Ansicht des BVerfG sollen das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme und das Grundrecht auf informationelle Selbstbestimmung dergestalt voneinander abgegrenzt werden, dass beim „IT-Grundrecht“ das gesamte System betroffen ist, während die informationelle Selbstbestimmung eher punktuelle Eingriffe schützt.⁴⁰¹ Vor diesem Hintergrund dürfte eine Beschlagnahme des gesamten Datenbestandes auch als vom „IT-Grundrecht“ umfasst anzusehen sein.

Unabhängig davon, ob diese Einteilung dogmatisch sauber und sinnvoll sein mag, sticht doch ein wesentlicher Unterschied ins Auge, der auch in der Rechtspraxis bedeutsam ist: das Gericht hat das „Computer-Grundrecht“ unter einen Richtervorbehalt gestellt, insofern ein IT-System „heimlich infiltriert“ wird,⁴⁰² und hebt es damit sogar vom Fernmeldegeheimnis in Art 10 Abs 1 GG ab, welches nur unter einem Gesetzesvorbehalt steht. Dieser Widerspruch heizte die Diskussion um einen ungeschriebenen Richtervorbehalt im Rahmen von Art 10 GG an. Daher wird in der Praxis genau darauf zu achten sein, inwiefern der Eingriff punktueller Natur ist, oder das System in größerem Umfang erfasst. Hierbei wird man bei der Annahme punktueller Eingriffe äußerst zurückhaltend sein müssen.

³⁹⁹ Britz, Vertraulichkeit und Integrität informationstechnischer Systeme, DÖV 2008, 411, 413; die dies kritisch sieht und die Schutzgüter lieber beim Grundrecht auf informationelle Selbstbestimmung angesiedelt hätte.

⁴⁰⁰ BVerfGE 113, 29, 45.

⁴⁰¹ Polenz in Kilian/Heussen, Computerrechtshandbuch³¹, Teil 13, Rz 36 mit Verweis auf BVerfGE 120, 274, 313.

⁴⁰² Diese Beschränkung blieb auch nicht ohne Kritik. So kritisiert Kutscha, dass der richterliche Vorbehalt nicht entsprechend ausgeweitet wird; vgl Kutscha, Mehr Schutz von Computerdaten durch ein neues Grundrecht?, NJW 2008, 1042, 1044.

9.4. Art 13 Abs 1 GG – Grundrecht auf Unverletzlichkeit der Wohnung

Das bereits oben unter 4.4 erläuterte Grundrecht auf Unverletzlichkeit der Wohnung hat auch eine Ausprägung, die sich auch auf den Schutz der Telekommunikation auswirkt. Insofern kann das Grundrecht sowohl als Schutzrecht gegen Überwachung als auch zum Schutz von Berufsgeheimnisträgern wirken.

Die Einordnung von Art 13 GG als Schutzrecht gegen Überwachung mag zunächst überraschen, denn dieses Grundrecht mag zunächst völlig losgelöst von telekommunikationstechnischen Kontexten erscheinen, hat aber im Rahmen von Telekommunikationsüberwachung Relevanz. Im Rahmen von Telefonüberwachungen (sog. „Lauschangriff“) war Art 13 Abs 1 GG lange Zeit das wichtigste Grundrecht, welches, um zusätzliche Überwachungen zu ermöglichen, Ende der 1990er-Jahre um einige Absätze erweitert wurde.⁴⁰³ Die Unverletzlichkeit der Wohnung schützt auch vor informationellen Eingriffen.⁴⁰⁴

In gewisser Weise stand Art 13 GG auch Pate für das neue Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme, da Art 13 GG früher einen Bereich abdeckte, der heute nicht mehr so leicht von seiner Umgebung abzugrenzen ist. War es früher die Wohnung, in der sich das Privatleben eines Menschen abspielte und in der sich sensible Daten befanden, so sind es heute IT-Systeme, die diese Privatheit aus dem Wohnungsbereich in einen nicht abgrenzbaren Bereich hinaustragen. So kann das Durchsuchen eines IT-Endgerätes von außen für den Betroffenen mittlerweile ein gravierenderer Eingriff sein, als die Durchsuchung seiner Wohnung. So übernimmt das „Computer-Grundrecht“ den Richtervorbehalt⁴⁰⁵ des Art 13 GG, was die Vorbildfunktion von Art 13 GG unterstreicht.

Untersucht man die Relevanz von Art 13 GG im Rahmen der Überwachung der Telekommunikation, so ist festzuhalten, dass dieses Grundrecht zumeist nicht direkt

⁴⁰³ Vgl hierzu im Überblick *Leipold*, Der „große Lauschangriff“, NJW-Spezial 2005, 135; die Grundgesetzänderung musste auf Grund der Rechtsprechung des BVerfG jedoch entsprechend angepasst werden; vgl BVerfG NJW 2004, 999.

⁴⁰⁴ *Polenz* in Kilian/Heussen, Computerrechtshandbuch³¹, Teil 13, Rz 50.

⁴⁰⁵ Dazu näher *Hermes* in Dreier, Grundgesetz³, Art 13, Rz 80.

betroffen sein wird. Einzig denkbare Variante ist jene, dass Ermittler eine Wohnung durchsuchen und dabei ein Endgerät der Telekommunikation finden, auf dem sich noch Spuren oder Abbilder des Telekommunikationsvorgangs befinden.⁴⁰⁶ Hierbei handelt es sich aber streng genommen gar nicht mehr um Telekommunikation, da diese bereits abgeschlossen ist. Das Grundrecht auf Unverletzlichkeit der Wohnung schützt damit nur im Nachhinein vor Überwachung bereits getätigter Telekommunikation, sofern sich die Geräte im häuslichen Bereich befinden.

10. Vorgaben aus der Grundrechtecharta der Europäischen Union

Wie schon bei den Vorgaben der GRC zu Berufsgeheimnisträgern⁴⁰⁷ erläutert, schützt selbstverständlich auch Art 7 GRC die private (Tele-)kommunikation. Da gerade Art 8 EMRK mit Art 7 GRC unmittelbar korrespondiert, der schon lange Teil des österreichischen Verfassungsrechts ist, wird die Implikation von Art 7 GRC auf Österreich eher geringe Auswirkungen haben.⁴⁰⁸ Spannender stellt sich der Einfluss von Art 8 GRC dar, der personenbezogene Daten⁴⁰⁹ schützt. Vom Schutzbereich umfasst sind, wie in der Datenschutzrichtlinie und auch der zukünftigen Datenschutzgrundverordnung, das Verarbeiten von personenbezogenen Daten.⁴¹⁰ Der Begriff des Verarbeitens ist hierbei weit gefasst. Er wird in Zukunft im Sinne der Datenschutzgrundverordnung zu definieren sein, welche in Art 4 Z 2 DS-GVO die Verarbeitung als *das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder*

⁴⁰⁶ Etwa eine Anrufliste in einem Telefon, SMS, heruntergeladene E-Mails, Chatprotokolle.

⁴⁰⁷ Siehe hierzu unter 5.

⁴⁰⁸ Breitenlechner/Kneihs/Segalla in Holoubek/Lienbacher, GRC, Art 7, Rz 24.

⁴⁰⁹ In Einklang mit der Datenschutzrichtlinie (95/46/EG) werden unter „personenbezogenen Daten“ nur jene natürlicher Personen zu verstehen sein. Hieran wird sich auch durch die Datenschutzgrundverordnung nichts verändern (Verordnung 2016/679). Der grundrechtliche Schutz von Daten juristischer Personen ist damit nur auf nationaler Ebene in Art 1 DSG 2000 vorgesehen; aA wohl Raschauer/Riesz in Holoubek/Lienbacher, GRC, Art 8, Rz 20.

⁴¹⁰ Die Datenschutzgrundverordnung nimmt in Erwägungsgrund 1 ausdrücklich auf das Grundrecht aus Art 1 GRC Bezug. Hierbei heißt es: „Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht.“

Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Daten definiert. Somit ist im Prinzip jede Art, bei der personenbezogene Daten staatlicherseits auf irgendeine denkbare Weise verarbeitet werden, als Eingriff in den Schutzbereich von Art 8 Abs 1 GRC zu sehen.⁴¹¹ Im Wesentlichen wird Art 8 GRC aber keinen nennenswerten zusätzlichen Schutz für Betroffene bringen, da § 1 DSG 2000 eine nahezu gleiche Schutzwirkung hat.⁴¹²

Noch wenig geklärt und von Literatur und Wissenschaft beachtet ist die Auswirkung von Art 1 GRC, der für die deutsche Verfassungsrechtsordnung keine Neuerung darstellt, aber für Österreich eine Verstärkung des verfassungsrechtlichen Schutzes im Hinblick auf die informationelle Selbstbestimmung bedeuten kann. Inwiefern dies der Fall ist, wird im Laufe der Arbeit zu untersuchen sein.

11. Einfachgesetzlicher Schutz in Österreich

Auch einfachgesetzlich ist die Telekommunikation geschützt. Ist durch das Verfassungsrecht der Staat gebunden, so trifft die Verpflichtung hier vor allem die Telekommunikationsanbieter.⁴¹³ Hier spielen vor allem das TKG und das StGB eine Rolle.

So schützt § 93 TKG das Kommunikationsgeheimnis. Bemerkenswert in diesem Zusammenhang ist, dass sich dieses vom Begriff des Fernmeldegeheimnisses in Art 10a StGG insofern unterscheidet, als dass die Inhaltsdaten, die Verkehrsdaten und die Standortdaten in § 93 Abs 1 S 1 TKG klar zum Schutzbereich gezählt werden.

⁴¹¹ Vgl zum weiten Schutzbereich auch *Raschauer/Riesz* in Holoubek/Lienbacher, GRC, Art 8, Rz 13.

⁴¹² *Raschauer/Riesz* in Holoubek/Lienbacher, GRC, Art 8, Rz 35.

⁴¹³ Seit die Telekommunikationsanbieter nicht mehr direkt dem Staat zuzuordnen sind (wie das etwa bis 01.03.1996 bei der Post- und Telegraphenverwaltung der Fall war), sind diese auch nicht mehr direkt grundrechtsverpflichtet, so dass es allenfalls zu einer mittelbaren Drittwirkung der Grundrechte kommen kann. Vgl hierzu *Himberger*, Fernmeldegeheimnis und Überwachung, 64 f.

Insofern ist dieser nicht umstritten.⁴¹⁴ Die Vorschrift des § 93 TKG setzt beim Anbieter an und allen, denen er sich zur Ausführung seiner Dienstleistung bedient, also etwa Angestellten und Gehilfen. Zur unmittelbaren Absicherung von § 93 TKG existiert in § 108 Abs 1 Z 1 TKG eine Strafnorm, die es unter Strafe stellt, wenn die Geheimhaltungsverpflichtungen nach § 93 TKG gebrochen werden.

Für den Fall, dass sich eine Person Kenntnis vom Inhalt⁴¹⁵ der Kommunikation verschafft, tritt § 108 Abs 1 TKG hinter § 119 Abs 1 StGB zurück.⁴¹⁶ Die Vorschrift des § 119 Abs 1 StGB bestraft das unbefugte Sich-Verschaffen des Nachrichteninhaltes mittels Benützung einer Vorrichtung.⁴¹⁷ Sowohl bei § 108 TKG als auch bei § 199 StGB handelt es sich um Ermächtigungsdelikte.

12. Einfachgesetzlicher Schutz in Deutschland

Ähnlich wie in Österreich⁴¹⁸ gestaltet sich der telekommunikationsrechtliche und strafrechtliche Schutz in Deutschland. So enthält § 88 dTKG eine Geheimhaltungsverpflichtung für den Diensteanbieter mit im Ergebnis gleichem Schutz wie in Österreich.⁴¹⁹ Die Verbreitung von Verkehrsdaten allein stellt eine Ordnungswidrigkeit dar (vgl § 96 Abs 2 iVm §§ 97, 99, 100 und 101 dTKG).⁴²⁰

⁴¹⁴ Ihren historischen Ursprung hat diese Vorschrift hierbei in der Telephonordnung 1887 des k.k. Handelsministeriums in § 33, die der Post- und Telegraphenverwaltung aufgab, für die Sicherstellung des „Telefon-Geheimnis“ in beiden Richtungen Sorge zu trage. Vgl zu den historischen Hintergründen *Himberger*, Fernmeldegeheimnis und Überwachung, 5.

⁴¹⁵ *Lewisch in Höpfel/Ratz*, WK² StGB, § 119, Rz 9.

⁴¹⁶ *Lewisch in Höpfel/Ratz*, WK² StGB, § 119, Rz 14 ff.

⁴¹⁷ Details hierzu bei *Lewisch in Höpfel/Ratz*, WK² StGB § 119, Rz 4 ff.

⁴¹⁸ Wohl bedeutendster Unterschied, neben dem unterschiedlichen Schutzbereich im dStGB, ist die Ausnahme für Luft- und Wasserfahrzeuge in § 88 Abs 4 dTKG, dem Führer dieser Fahrzeuge gegenüber, sofern sich die Kommunikationsanlage an Bord dieses Fahrzeugs befindet. Hiermit sollten wohl Konflikte zwischen Bordfunker und Kapitän vermieden werden. Die Vorschrift ist veraltet und wird für entbehrlich gehalten. Vgl hierzu *Bock in Geppert/Schütz*, Beck-TKG⁴, § 88 TKG, Rz 48.

⁴¹⁹ Näheres vgl *Bock in Geppert/Schütz*, Beck-TKG⁴, § 88 TKG, Rz 1 ff.

⁴²⁰ *Bock in Geppert/Schütz*, Beck-TKG⁴, § 88 TKG, Rz 49.

Auch das deutsche Strafrecht, stellt eine Verletzung des Fernmeldegeheimnisses unter Strafe,⁴²¹ wobei es hier – im Gegensatz zu Österreich – nicht nur auf die Inhalte, sondern auch auf die Verkehrsdaten ankommt.

Der einfachgesetzliche Schutz in Deutschland ist unlängst in die Kritik geraten, da bei neuen Technologien in der Judikatur teilweise umstritten ist, inwiefern § 88 dTKG greift. Unklar ist dies etwa bei modernen Over-the-top-Diensten, dabei handelt es sich um Dienste, die auf verschiedensten Wegen ihren Nutzern Kommunikation ermöglichen, also Mailportale (wie etwa Google-Mail, Gmx.at), Messagingdienste (wie etwa WhatsApp, Telegram oder Facebook-Messenger) oder auch Internettelefonie (wie beispielsweise Skype oder Google Hangout). Meines Erachtens kommt es hier nicht zu einer Lücke in der Gesetzgebung, da § 88 dTKG greift. Da dies aber von Gerichten höchst unterschiedlich behandelt wird, wird in der Literatur der Ruf laut, der Gesetzgeber möge hier legislativ eine Nachschärfung vornehmen und eine entsprechende Klarstellung im Bereich des Telekommunikationsrechts aufnehmen.⁴²²

13. Ergebnisse

Grundsätzlich ist die Telekommunikation durch das Verfassungsrecht geschützt. Sowohl der Telekommunikationsvorgang selbst, als auch die gespeicherte Telekommunikation am Endgerät eines Betroffenen unterliegt dem Schutz von zahlreichen Grundrechten. Nennenswerte Lücken liegen hier weder in Österreich noch in Deutschland vor. In Deutschland hat sich – bedingt durch die umfassendere Rechtsprechung des BVerfG in diesem Bereich – der Grundrechtsschutz in vielen Bereichen weiter entwickelt und es haben sich weitere Grundrechte etabliert, bei denen das Gericht als eine Art Ersatzgesetzgeber tätig wurde. Dafür fehlt im Gegensatz zu Österreich ein direkt niedergeschriebenes Grundrecht, das personenbezogene Daten schützt. .

⁴²¹ Vgl zum Verhältnis zwischen dTKG und dStGB *Bock* in Geppert/Schütz, Beck-TKG⁴, § 88 TKG, Rz 7.

⁴²² Deusch/Eggendorfer, Das Fernmeldegeheimnis im Spannungsfeld aktueller Kommunikationstechnologien, K&R 2017, 93, 96.

Durch den unterschiedlichen Aufbau beider Verfassungsrechtsordnungen existieren teilweise gleiche, teilweise völlig unterschiedliche Grundrechte in Österreich und Deutschland. Gleiches gilt im Hinblick auf die europäische Ebene, wo Grundrechte teilweise dem österreichischen Verfassungsrecht ähnlich sind, wie etwa Art 8 GRC, oder dem deutschen, wie etwa Art 1 GRC.

Im Rahmen der Rechtsvergleichung wird zu betrachten sein, wie stark die eine Verfassungsrechtsordnung mit der jeweils anderen verglichen werden kann und inwiefern die GRC hier im Rahmen des Verfassungsvergleiches hilfreich sein kann. Denn nur dann, wenn eine Vergleichbarkeit beider Rechtsordnungen vorliegt, ist es möglich, Erkenntnisse von der einen auf die andere Rechtsordnung zu übertragen.

Kapitel III – Spannungsfeld zwischen verfassungsrechtlichem Telekommunikations- und Berufsgeheimnisträgerschutz und Überwachung im Lichte der Rechtsprechung in Österreich und Deutschland

Das Spannungsfeld zwischen Telekommunikationsüberwachung und Berufsgeheimnissen ist an sich kein neues Phänomen, welches erst durch die Vorratsdatenspeicherung auftrat. Die Einführung der Vorratsdatenspeicherung in der EU hat jedoch dazu geführt, dass sich Gerichte stärker als bisher mit dem Schutz der Berufsgeheimnisträger auseinandergesetzt haben. Dies betrifft vor allem das deutsche BVerfG, dessen Aussagen zur Vorratsdatenspeicherung dazu geführt haben, dass eine neue Vorschrift (§ 160a dStPO) eingeführt wurde. Über diese Rechtsprechung hinaus geht der EuGH, der sich nach Vorlage des VfGH und des Irischen High Court mit der Thematik ebenfalls auseinandergesetzt hat und die Vorratsdatenspeicherung in der von der RL

Die Erkenntnisse aus den beiden vorangegangenen Kapiteln sind nun zusammen zu führen. Die Telekommunikationsüberwachung unterliegt hierbei verfassungsrechtlichen Schranken, die durch die verfassungsrechtlichen Schranken zum Berufsgeheimnisträgerschutz in bestimmten Bereichen eine Verstärkung erfahren. Diese gestalten sich in beiden Ländern ähnlich. In der legislatischen Umsetzung findet sich jedoch nur in Deutschland bislang eine entsprechende Regelung in der Strafprozessordnung (§ 160a dStPO), die bestimmte Berufsgruppen von Überwachungsmaßnahmen ganz oder teilweise ausnimmt.

Waren früher die Hauptanwendungsgebiete für den Schutz der Berufsgeheimnisträger die Berechtigung zur Verweigerung der Aussage im Verfahren vor den Strafgerichten, so wird durch die Gesetzgebung nunmehr erkannt, dass eine ähnliche, teilweise weitaus größere Gefährdungslage im Rahmen der Überwachung besteht, welche – was, wie gezeigt wurde, auch verfassungsrechtlich geboten ist – eingegrenzt werden muss.⁴²³

⁴²³ *Bertheau*, § 160a StPO neuer Fassung – doch offene Fragen bleiben, StV 2012, 313.

Insofern ist die Analyse einer verfassungsgerichtlichen Entscheidung des BVerfG zu § 160a dStPO hilfreich, weil sich dieses vertieft mit dem Spannungsfeld von Berufsgeheimnisträgerschutz und Telekommunikationsüberwachung auseinandersetzt. Dessen Erkenntnisse lassen sich aber auch auf andere Überwachungsmaßnahmen übertragen. Schließlich stellen sich die Probleme nicht erstmalig. Zwar wurde die entsprechende Regelung aus Anlass der Vorratsdatenspeicherung eingefügt und in diesem Lichte auch vom BVerfG interpretiert, jedoch ist sie nicht vorratsdatenspeicherungsspezifisch und gilt ebenso für andere Arten der Telekommunikationsüberwachung.

Hervorzuheben ist hierbei, dass eine entsprechende Regelung in Österreich nicht vorhanden ist, weswegen sich hier erneut ein rechtlicher Vergleich zwischen beiden Ländern anbietet. Die Rechtsprechung des deutschen BVerfG war dem österreichischen Gesetzgeber zwar bewusst, eine Übertragung einer ähnlichen Regelung auf das österreichische Recht wurde aber abgelehnt. Ziel dieses Kapitels soll es sein, die Regelung des § 160a dStPO zum einen auf ihre Verfassungsmäßigkeit zu untersuchen und dabei zum anderen die grundrechtliche Bedeutung von überwachungsfreien Räumen näher zu erforschen.

14. Die Rechtslage in Österreich

In Österreich sind Berufsgeheimnisse in der StPO und im SPG geschützt, wobei der Schutz im SPG sich allerdings nicht auf den Bereich der Telekommunikationsüberwachung erstreckt.

14.1. Berufsgeheimnisträgerschutz im Rahmen der Telekommunikation in der Strafprozessordnung

Wie bereits erwähnt, fehlt es im Rahmen der Telekommunikationsüberwachung an einer entsprechenden Regelungen, welche klare Beweiserhebungsverbote regeln. Zwar dürfen gemäß § 144 Abs 1 und 2 StPO die in der StPO normierten Zeugnisver-

weigerungsrecht durch Überwachungsmaßnahmen nicht ohne weiteres umgangen werden,⁴²⁴ dies läuft jedoch nicht auf einen absoluten Schutz hinaus.

Absolut geschützt ist in Österreich in diesem Zusammenhang nur das Beichtgeheimnis durch § 145 Abs 1 StPO. Dieses darf etwa nicht durch technische Überwachungsmaßnahmen im Beichtstuhl ausgehebelt werden.⁴²⁵ Zwar bedeutet ein Umgehungsverbot, wie es sich in der StPO findet, einen Schutz vor gezielten Überwachungsmaßnahmen, dies lässt aber jene Überwachungsmaßnahmen außen vor, die sich gegen die gesamte Bevölkerung richten. Auch ist nicht im engeren Sinne die Überwachung des Berufsgeheimnisträgers per se verboten, sondern vielmehr ist nur deren Verwertbarkeit im Rahmen eines Strafprozesses eingeschränkt.

Es bleibt damit festzuhalten, dass die StPO den Ermittlungen bei Berufsgeheimnisträgern gewisse Grenzen setzt. Zumindest wird davon ausgegangen werden können, dass bei der Überwachung erlangte Erkenntnisse über eine Person, die sich hilfesuchend an den Berufsgeheimnisträger gewandt hat, da diese das Zeugnisverweigerungsrecht des Berufsgeheimnisträgers wohl betreffen werden, nicht verwendet werden dürfen.⁴²⁶ Insofern kann ein Hilfesuchender sich zwar sicher sein, dass alles, was er dem Berufsgeheimnisträger mitteilt, nicht gegen ihn in einem Strafprozess verwendet werden kann, jedoch kann er sich nicht sicher sein, dass nicht Ermittlungspersonen von dem, was er dem Berufsgeheimnisträger mitteilt, Kenntnis erhalten.

Zu erwähnen ist, dass sich das Umgehungsverbot nicht nur auf den Inhalt der Nachrichten des Berufsgeheimnisträgers, sondern auch auf dessen Verkehrsdaten auswirkt.⁴²⁷

Positiv zu erwähnen ist, dass es einer Genehmigung durch den Rechtsschutzbeauftragten bedarf, bevor ein Berufsgeheimnisträger überwacht werden darf.⁴²⁸ Somit ist eine gewisse Art der Vorabkontrolle gewährleistet.

⁴²⁴ *Bergauer/Schmölzer* in *Jahnel/Mader/Staudegger*, IT-Recht³, 723.

⁴²⁵ Auch dann nicht, wenn der Geistliche davon weiß und dieses – entgegen der innerkirchlichen Vorschriften – gestattet, vgl *Bertel/Venier*, StPO, § 144, Rz 6.

⁴²⁶ Vgl *Zerbes*, Anwaltsverschwiegenheit: überkommenes Privileg oder rechtsstaatliches Erfordernis?, AnwBl 2013, 565, 568 f.

⁴²⁷ *Reindl-Krauskopf/Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO § 135, Rz 36.

Auch haben Berufsgeheimnisträger die Möglichkeit, der Beschlagnahme von Unterlagen oder Datenspeichern im Rahmen von Durchsuchungen nach § 112 StPO zu widersprechen.⁴²⁹ Die Unterlagen oder Datenträger sind dann zu versiegeln und dem Berufsgeheimnisträger müssen wenigstens 14 Tage Zeit gegeben werden, um nähere Umstände zu bezeichnen, warum die beschlagnahmten Dinge seine berufliche Verschwiegenheitspflicht tangieren.⁴³⁰ Der Berufsgeheimnisträger hat das Recht, bei der Sichtung durch Gericht oder Staatsanwaltschaft⁴³¹ anwesend zu sein.⁴³² Fällt nach der Sichtung eine Entscheidung zugunsten des Berufsgeheimnisträgers aus, sind die beschlagnahmten Gegenstände auszufolgen, andernfalls zum Akt zu nehmen, wogegen dem Berufsgeheimnisträger wiederum der Einspruch zusteht (§ 112 Abs 3 StPO).⁴³³ Zentral für diese Norm ist es, eine Prüfung ob das jeweilige Berufsgeheimnis berührt ist durchzuführen, bevor die Unterlagen zum jeweiligen Akt gelangen. Hierbei ist sich der Gesetzgeber auch bewusst, dass, einmal zur Kenntnis genommen und zum Akt gelangt, auch bei Beweisverwertungsverbieten entsprechende Unterlagen die Ermittlungen in erheblichem Maße in ihrer Arbeit beeinflussen.

Telekommunikationsrechtlich entfaltet die Norm nur teilweise Relevanz, da nur Gegenstände und auch Datenträger umfasst sind, auf denen Gedanken festgehalten sind.⁴³⁴ Das können beispielsweise SMS, E-Mails oder andere Nachrichten auf einem Smartphone als Datenträger sein. Allerdings bezieht sich diese Norm nur auf Daten, die auch einen Inhalt haben. Die Anrufliste, also die Verkehrsdaten, oder andere automatisch angelegten Protokolle, wie etwa die Speicherung des Standortes, welche aber unter

⁴²⁸ Bertel/Venier, StPO, § 147, Rz 3.

⁴²⁹ Stricker, Schutz von Berufsgeheimnissen, ÖJZ 2016, 539, 541. Die Widerspruchsmöglichkeit steht hierbei nicht nur dem Berufsgeheimnisträger, sondern auch dem Hilfspersonal des Berufsgeheimnisträgers zu. Im Fall der Durchsuchung einer Kanzlei hat ohnehin ein Vertreter der RAK anwesend zu sein.

⁴³⁰ Stricker, Schutz von Berufsgeheimnissen, ÖJZ 2016, 539, 542 f. Unterlässt der Berufsgeheimnisträger seine Mitwirkung oder wirkt er unzureichend mit, werden die Unterlagen oder Daten zum Akt genommen.

⁴³¹ Ob Gericht oder Staatsanwaltschaft die Sichtung gemeinsam mit dem Berufsgeheimnisträger vornehmen, hängt vom Berufsgeheimnisträger ab, der beantragen kann, dass die Unterlagen nicht bei Gericht unter Verschluss sondern bei der Staatsanwaltschaft, getrennt vom Ermittlungsakt, aufbewahrt werden. Näher hierzu Stricker, Schutz von Berufsgeheimnissen, ÖJZ 2016, 539, 544.

⁴³² Stricker, Schutz von Berufsgeheimnissen, ÖJZ 2016, 539, 542 mwN.

⁴³³ Stricker, Schutz von Berufsgeheimnissen, ÖJZ 2016, 539, 544.

⁴³⁴ Tipold/Zerbes in Fuchs/Ratz, WK StPO § 112, Rz 5.

Umständen ebenso aussagekräftig sind wie ein Nachrichteninhalt, sind nicht hiervon umfasst.

14.2. Berufsgeheimnisträgerschutz im Rahmen der Telekommunikation im Sicherheitspolizeigesetz

Im Bereich der präventiven Maßnahmen von Ermittlern finden sich hingegen keine wirksamen Beschränkungen. Lediglich bei der Durchsuchung von Grundstücken, Räumen und Fahrzeugen geht das SPG in diesem Zusammenhang auf Berufsgeheimnisse ein. So regelt § 39 Abs 7 SPG, dass diese Durchsuchung nach Möglichkeit nicht in Berufsgeheimnisse eingreifen soll. Somit fordert das Gesetz eine besonders wirksame Verhältnismäßigkeitsprüfung.⁴³⁵ Bei der Überwachung von Telekommunikation und beim Zugriff auf Metadaten nach § 53 Abs 3a SPG findet hingegen eine solche Abwägung nicht statt.⁴³⁶

Im Gegensatz zur StPO, wo dem Rechtsschutzbeauftragten eine aktive Rolle zukommt, ist dessen Rolle im polizeirechtlichen Bereich anders ausgestaltet. Hier ergeht an den Rechtsschutzbeauftragten eine Information.⁴³⁷ Der Rechtsschutzbeauftragte wird hierbei nachträglich über die Maßnahme der Ermittler in Kenntnis gesetzt (§ 91c Abs 1 SPG).⁴³⁸

14.3. Berufsgeheimnisträgerschutz im Rahmen der Telekommunikation im Telekommunikationsgesetz

Die Norm des § 93 Abs 5 TKG normiert den Schutz der Berufsgeheimnisträger in Bezug auf das Kommunikationsgeheimnis gegenüber Telekommunikationsanbietern.⁴³⁹ Die Umsetzung sah in Österreich aber keinen umfassenden Schutz durch § 93 Abs 5 TKG vor, sondern stellt nur zu dem ohnehin geltenden Kommunikationsgeheimnis klar, dass Telekommunikationsanbieter diese zu beachten habe. Der Gesetzgeber war sich hierbei auch der Rechtsprechung des BVerfG zur deutschen Umsetzung

⁴³⁵ Hauer/Keplinger, SPG⁴, 429.

⁴³⁶ Näher Hauer/Keplinger, SPG⁴, 565 ff.

⁴³⁷ Hauer/Keplinger, SPG⁴, 565

⁴³⁸ Hauer/Keplinger, SPG⁴, 899.

⁴³⁹ Vergleichbare Regelungen bestehen auch in Deutschland, vgl Geuer, Das Fernmeldegeheimnis als gesetzliches Verbot, ZD 2012, 515.

der Richtlinie zur Vorratsdatenspeicherung bewusst. Er unterstellte dem Gericht aber, dass dieses sich mit der Problematik nicht vertieft auseinandergesetzt habe; schließlich bestünden auch bei einer Art „Whitelist“ für Berufsgeheimnisträger datenschutzrechtliche Probleme.⁴⁴⁰ Diese lägen etwa darin, dass dann ein Verzeichnis existieren würde, in dem sämtliche Berufsgeheimnisträger aufgeführt wären. Worin die „datenschutzrechtliche“ Problematik hier liegen soll, erfährt man bei Lektüre der Gesetzesmaterialien leider nicht. Auch in anderen Staaten steht man dem offenbar ablehnend gegenüber.⁴⁴¹

Jedenfalls zutreffend war die gesetzgeberische Anmerkung, dass es sich hierbei um keine neuartige Problematik handele, sondern dass diese bereits seit längerem bestehe, nämlich seitdem es Auskünfte über Verkehrsdaten an Gerichte gibt, sodass die damals eingeführte Vorratsdatenspeicherung ein bestehendes Problem verstärke und kein neues schüfe.⁴⁴²

15. Die Rechtslage in Deutschland

Die dStPO wählt eine gänzlich andere Herangehensweise an diese Problematik. Dies ist letztendlich auf ein Urteil des BVerfG zur Vorratsdatenspeicherung zurückzuführen. Dies ist insofern besonders interessant, als dass die Vorratsdatenspeicherung eine Überwachungsmaßnahme ist, die die gesamte Bevölkerung inklusive aller Berufsgeheimnisträger umfasst. Demgemäß lassen sich für den Berufsgeheimnisträgerschutz bedeutende Schlüsse ziehen. Das Gericht hat hierbei insbesondere die Schutzwürdigkeit der Berufsgeheimnisträger betont und seine Ansichten sind unmittelbar in den darauffolgenden Gesetzgebungsprozess eingeflossen.

Kurz zusammengefasst lässt sich zur Entscheidung des BVerfG zur Vorratsdatenspeicherung sagen, dass dieses die Vorratsdatenspeicherung an sich für vereinbar mit

⁴⁴⁰ RV zu § 93 (1074 Blg NR 24. GP) zitiert nach *Dohr/Pollirer/Weiss/Knyrim*, DSG, § 93 TKG, Gesetzesmaterialien.

⁴⁴¹ *Rogalski*, Verpflichtung zur Vorratsspeicherung und Bereitstellung von Telekommunikationsdaten in Polen, WiRO 2015, 50, 51.

⁴⁴² RV zu § 93 (1074 Blg NR 24. GP) zitiert nach *Dohr/Pollirer/Weiss/Knyrim*, DSG, § 93 TKG, Gesetzesmaterialien.

dem Grundgesetz hält. Als betroffenes Grundrecht kommt nach deutscher Rechtslage Art 10 GG in Betracht, welches das Fernmeldegeheimnis schützt.⁴⁴³ Das BVerfG wog beim Grundrechtsschutz umfassend ab und schloss eine grundgesetzkonforme Regelung zwar nicht aus, machte aber entsprechend strenge Vorgaben.

Die im Urteil des BVerfG geäußerten Bedenken können ebenfalls erkenntnisleitend für die rechtliche Umsetzung in Österreich sein, sollte an eine Wiedereinführung der Vorratsdatenspeicherung auf nationaler Ebene gedacht werden, auch wenn – wie bereits erläutert – der Grundrechtsschutz einer anderen Systematik folgt. Unabhängig davon, dass Art 10 GG in Deutschland auf jeden Fall Verkehrsdaten schützt, was bei Art 10a StGG oft verneint wird schützt beispielsweise Art 8 EMRK gleichermaßen Inhaltsdaten und darüber hinaus auch Verkehrsdaten.⁴⁴⁴ Auch § 1 DSG 2000⁴⁴⁵, der ebenfalls im Verfassungsrang steht, sichert diese grundrechtlich ab.⁴⁴⁶

15.1. Aussagen des BVerfG bezüglich Berufsgeheimnisträgern

Bezüglich der Berufsgeheimnisse hat das BVerfG in einem Urteil klar Stellung bezogen. Grundlage war diesmal nicht die Überwachung im Rahmen der Vorratsdatenspeicherung an sich, sondern die Überwachung der Berufsgeheimnisträger. Hierbei bezieht sich das Gericht auf bestehende „besondere Vertrauensbeziehungen“⁴⁴⁷. Zwischen einzelnen Berufsgeheimnissen wird in dieser Entscheidung nicht differenziert, es

⁴⁴³ Zusammenfassend *Tschohl*, BIM –Studie, 34.

⁴⁴⁴ Vgl zum Verhältnis beider Normen und zur historischen Entwicklung auch *Brandstetter*, Die Fernmeldeüberwachung öffentlicher Telefonzellen, Rückwirkende Überprüfung von Vermittlungsdaten im Fernmeldeverkehr, Anmerkungen zu OGH 6. 12. 1995, 13 Os 161/95, JBl 1984, 457. Nachdem zunächst ungeklärt war, inwiefern Art 8 EMRK überhaupt Fernmeldevorgänge schützt, wurde, bevor dies durch den EGMR bestätigt wurde, das Grundrecht des Art 10a StGG geschaffen. Vgl hierzu auch *Schmölzer*, Rückwirkende Überprüfung von Vermittlungsdaten im Fernmeldeverkehr, JBl 1997, 211, die ebenfalls einen Schutz von Verbindungsdaten durch Art 10a StGG bejaht.

⁴⁴⁵ Die Verfassungsnorm des § 1 Abs 1 DSG normiert das Geheimhaltungsinteresse an personenbezogenen Daten; sie geht damit über das Fernmeldegeheimnis hinaus und normiert auch die informationelle Selbstbestimmung, vgl *Dohr/Pollirer/Weiss/Knyrim*, DSG, § 1 Anm 2.

⁴⁴⁶ Die Unterscheidung ist zwar von großer Bedeutung, da nur Art 10a StGG, was ihn im Übrigen von Art 10 GG grundlegend unterscheidet, unter einem Richtervorbehalt steht und somit eine Erfassung von Verkehrsdaten über Art 8 EMRK und § 1 DSG keinen äquivalenten Schutz bietet. Diese Fragestellung geht jedoch über die Themensetzung dieser Arbeit weit hinaus.

⁴⁴⁷ BVerfG NJW 2010, 833, 842.

werden lediglich exemplarisch einige vertrauliche Bereiche aufgezählt, ohne dass sich daraus eine Wertung direkt ablesen lässt.

Damit gibt es mittlerweile zu der Thematik eine klare verfassungsgerichtliche Position. Der Berufsgeheimnisträgerschutz hat eine angemessene Berücksichtigung zu finden. Hierbei führt das deutsche BVerfG an den entscheidenden Stellen aus:⁴⁴⁸

[E]s kann in Blick auf das Eingriffsgewicht einen Unterschied machen, ob bei der Datenübermittlung Filter zwischengeschaltet werden, mit denen bestimmte Telekommunikationsverbindungen zum Schutz von besonderen Vertrauensbeziehungen ausgesondert werden. [...]

Verfassungsrechtlich geboten ist als Ausfluss des Verhältnismäßigkeitsgrundsatzes jedoch, zumindest für einen engen Kreis von auf besondere Vertraulichkeit angewiesenen Telekommunikationsverbindungen ein grundsätzliches Übermittlungsverbot vorzusehen. Zu denken ist hier etwa an Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit anderen Verschwiegenheitsverpflichtungen unterliegen.

Aus diesen Ausführungen lässt sich folgern, dass das BVerfG im Rahmen der Vorratsdatenspeicherung explizit Bedarf an Beweiserhebungsverboten bei Berufsgeheimnisträgern sieht. Ein reines Beweisverwertungsverbot reicht wohl nicht aus. Ohne dabei die genauen Anforderungen näher zu konkretisieren, wird davon ausgegangen, dass es Fälle gibt, in denen von vornherein eine Datenübermittlung über Telekommunikationsvorgänge auszuschneiden hat. Dabei wird – wie bereits angedeutet – auch bezüglich der Berufsgruppen keine wirkliche Differenzierung vorgenommen. Allenfalls lässt sich herauslesen, dass ein derartiger Schutz vielleicht nicht in jeder Vertrauensbeziehung gleichermaßen gefordert ist. Inwiefern eine Differenzierung notwendig ist, wird somit auf anderen Überlegungen fußen müssen.

⁴⁴⁸ BVerfG NJW 2010, 833, 842.

15.2. Gesetzliche Umsetzung von Beweiserhebungsverboten in Deutschland

Nach der ersten Einführung der Vorratsdatenspeicherung in Deutschland⁴⁴⁹, wurde im Rahmen des Gesetzgebungsprozesses auch die dStPO entsprechend geändert und an die neuen Maßnahmen angepasst. Die Regelungen zur Vorratsdatenspeicherung selbst wurden für verfassungswidrig erklärt (§§ 113a, 113b dTKG und § 100g dStPO). Für Berufsgeheimnisse wurde die Regelung des § 160a dStPO geschaffen; diese Regelung, für die die Vorratsdatenspeicherung nur den Anlassfall darstellt, besteht weiterhin.

Das BVerfG hat gesondert zu dieser Regelung Stellung bezogen und sie für verfassungskonform erklärt.⁴⁵⁰ Daher ist davon auszugehen, dass das BVerfG seine im Urteil zur Vorratsdatenspeicherung vorgesehenen Vorgaben in § 160a dStPO für verwirklicht ansieht.

15.2.1. Die Umsetzung in § 160a dStPO

Um damals einen Ausgleich für die Überwachung durch die Vorratsdatenspeicherung zu schaffen, hat der Gesetzgeber in Deutschland die Norm des § 160a dStPO eingeführt.⁴⁵¹ Diese sollte ursprünglich nicht an dieser Stelle in die dStPO eingefügt werden, sondern als § 53b dStPO, in direkter Nachbarschaft zu den Zeugnisverweigerungsrechten.⁴⁵² Dies hätte der Vorschrift aus systematischer Sicht besser zu Gesicht gestanden. Nunmehr befindet sie sich in einem eher sachfremden Umfeld im 2. Abschnitt des 2. Buches der dStPO unter „Vorbereitung der öffentlichen Klage“. Dies passt von der Systematik her nicht zu der Vorschrift. Sie ist daher eher ein Fremdkörper in diesem Teil der dStPO und ist losgelöst von diesem Kontext zu betrachten.

Die Vorschrift des § 160a dStPO wurde zum Schutz der Interessen zeugnisverweigerungsberechtigter Berufsgeheimnisträger (§§ 53, 53a dStPO) eingefügt und

⁴⁴⁹ Vgl zur neuerliche Einführung unter 28.3.

⁴⁵⁰ BVerfG NJW 2012, 833, 840 f.

⁴⁵¹ Mittlerweile ist § 160a dStPO aktueller denn je, da der Gesetzgeber die Vorratsdatenspeicherung in Deutschland wieder eingeführt hat. Vgl zu den aktuellen Entwicklungen unter 28.3.

⁴⁵² *Sackreuther* in BeckOK StPO, § 160a, Rz 2.

normiert ein umfassendes Beweisverwertungs- und Beweiserhebungsverbot.⁴⁵³ Die Regelung gilt nicht nur für die – mittlerweile erneut eingeführte – Vorratsdatenspeicherung,⁴⁵⁴ sondern für sämtliche Ermittlungsmaßnahmen, wurde aber im Rahmen der Umsetzung der damals gültigen Vorratsdatenspeicherungsrichtlinie in die dStPO eingefügt.⁴⁵⁵ Die Einführung der Vorratsdatenspeicherung stellte also lediglich den Anlassfall für den Erlass der Regelung dar. Die Regelung weist dabei bei den verschiedenen Berufsgeheimnisträgern eine Zweiteilung auf. Ein Teil der Berufsgeheimnisträger genießt absoluten Schutz⁴⁵⁶ vor Beweiserhebungen, die anderen lediglich relativen Schutz.

Grundsätzlich unzulässig sind nach § 160a Abs 1 dStPO Ermittlungsmaßnahmen, die sich gegen in § 53 Abs 1 S 1 Z 1, 2 und 4 dStPO genannte Person oder einen Rechtsanwalt⁴⁵⁷ richten. In § 53 Abs 1 S 1 Z 1, 2 und 4 dStPO sind Geistliche, Verteidiger und Abgeordnete erwähnt. Dabei normiert die Vorschrift des § 160a Abs 1 dStPO für einen Teil der Berufsgeheimnisträger ein absolutes Beweiserhebungs- und Beweisverwertungsverbot. Bereits angefertigte Aufzeichnungen über diese Berufsgeheimnisträger sind somit zu löschen, die Löschung wiederum muss protokollarisch festgehalten werden.

Für die übrigen Berufsgeheimnisträger regelt § 160a Abs 2 dStPO, dass Ermittlungsmaßnahmen grundsätzlich zulässig sind, die Stellung des Berufsgeheimnisträgers aber in die Verhältnismäßigkeitsprüfung miteinzufließen hat. Damit wurde ein relatives Beweiserhebungs- und Beweisverwertungsverbot normiert. Im Rahmen der Verhältnismäßigkeit spielt es dann z B eine Rolle, welche Straftat dem Betroffenen zur Last

⁴⁵³ *Sackreuther* in BeckOK StPO, § 160a, Rz 1.

⁴⁵⁴ Vgl hierzu unter 28.3.

⁴⁵⁵ *Sackreuther* in BeckOK StPO, § 160a, Rz 2.

⁴⁵⁶ Vgl hierzu auch *Roxin/Schünemann*, Strafverfahrensrecht²⁷, § 36, Rz 12. Der Schutz ist sehr weitreichend. In diesem Zusammenhang verwiesen *Roxin/Schünemann* auch auf § 148 dStPO, der die Überwachung des Fernmeldeverkehrs zwischen Strafverteidiger und Mandant auch dann untersagt, wenn gegen den Verteidiger der Verdacht der Strafvereitelung (§ 258 dStGB) besteht.

⁴⁵⁷ Mit Rechtsanwälten gleichgestellt sind nach § 206 BRAO aufgenommene Personen aus ausländischen Staaten, die Mitglieder in einer der Anwaltskammern sind.

liegt; es muss sich dabei mithin um Straftaten von erheblicher Bedeutung⁴⁵⁸ handeln.⁴⁵⁹ Somit ist jede Beweiserhebung oder auch Beweisverwertung am Ende eine Frage der Abwägung.

Die Regelung des § 160a dStPO war von Anfang an in der Kritik. Kritik wurde verstärkt von Seiten der Bundesrechtsanwaltskammer geäußert. Dies ging darauf zurück, dass Rechtsanwälte in der Ursprungsfassung nicht von § 160a Abs 1 dStPO erfasst waren, sondern lediglich von § 160a Abs 2 dStPO. Ermittlungen im Umfeld von Rechtsanwälten unterfielen damit nur dem relativen Beweisverwertungs- und Beweis-erhebungsverbot,⁴⁶⁰ während Strafverteidiger von Anfang an dem Schutz von § 160a Abs 1 dStPO unterfielen.⁴⁶¹

15.2.2. Zulässigkeit der Unterscheidung einzelner Berufsgeheimnis-träger

Der Gesetzgeber hat nach der aufkommenden Kritik § 160a dStPO einer Novellierung unterzogen, jedoch auf die Kritikpunkte nur partiell reagiert. Auch nach der Neufassung riss folglich die Kritik an § 160a dStPO nicht ab. Begründet wurde dies damit, dass der Rechtsanwalt seinen Mandanten umfassend berät. Ein zivilrechtliches Beratungsgespräch kann schnell strafrechtliche Aspekte aufweisen, welche es erforderlich machen, sich auf eine Strafverteidigung einzustellen. Die einzelnen Rechtsgebiete lassen sich in der anwaltlichen Praxis nur schwer trennen.⁴⁶²

Doch auch nach Aufnahme der Rechtsanwälte in die Gruppe des § 160a Abs 1 dStPO bleiben Fragen offen. Zum einen, ob eine Differenzierung überhaupt gerechtfertigt ist und, falls dem so ist, ob die jetzige Umsetzung verfassungskon-

⁴⁵⁸ Was unter einer Straftat von erheblicher Bedeutung zu verstehen ist, ist nicht gesetzlich normiert. Voraussetzung ist, dass die Straftat „mindestens dem Bereich der mittleren Kriminalität zuzurechnen [ist], den Rechtsfrieden empfindlich stör[t] und dazu geeignet [ist], das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen“, vgl BVerfG, NJW 879, 880 mwN.

⁴⁵⁹ *Griesbaum* in *Karlsruher Kommentar StPO*⁶, § 160a, Rz 14.

⁴⁶⁰ Vgl zu dieser Kritik auch *Szuba*, *Vorratsdatenspeicherung*, 161.

⁴⁶¹ Vgl hierzu auch *Müller*, *Durchsuchung einer Rechtsanwaltskanzlei - Verhaltenshinweise, Mitteilungen der Rechtsanwaltskammer München* 03/2013, 4.

⁴⁶² Vgl zur Neuregelung auch *Müller-Jacobsen*, *Schutz von Vertrauensverhältnissen zu Rechtsanwälten im Strafprozess, Ein erster Schritt zum Abschied vom „Zwei-Klassen-Recht“*, NJW 2011, 257.

form ist oder ob aus verfassungsrechtlichen Gründen eine andere Einteilung der Berufsgeheimnisträger geboten ist.

15.2.2.1. *Rechtfertigung der Differenzierung*

Das BVerfG hat sich in seiner Rechtsprechung bereits vor seiner Judikatur zu § 160a dStPO zu Berufsgeheimnisträgern geäußert. Diese Rechtsprechung muss mit der Entscheidung im Kontext betrachtet werden.

Bereits in der Entscheidung zum großen Lauschangriff⁴⁶³ hatte das Gericht zwischen einzelnen Berufsgeheimnisträgern zu differenzieren, welche von §§ 52, 53 dStPO geschützt sind. Das BVerfG bezog sich dabei darauf, dass der Grundrechtsschutz beim Abhören von Gesprächen verschieden zu beurteilen sei, auch wenn die gleiche Vorschrift betroffen sei. Es sei vielmehr bei der Kommunikation mit Berufsgeheimnisträgern entscheidend, ob die Menschenwürde betroffen ist:⁴⁶⁴

Wird beispielsweise ein Beichtgespräch mit einem Seelsorger abgehört, so ist direkt die Menschenwürde⁴⁶⁵ betroffen und zwar der Menschenwürdegehalt der Religionsausübung, der in Art 4 Abs 1 und 2 GG seine verfassungsrechtliche Ausprägung findet. Wird ein Gespräch zwischen Strafverteidiger und Mandant abgehört, so ist auch direkt die Menschenwürde betroffen. Dies gilt auch bei Gesprächen mit Ärzten. Dort kann die Menschenwürde in vielen Fällen betroffen sein.⁴⁶⁶ Keine Ausprägung der Menschenwürde sei es hingegen, mit Medienmitarbeitern oder Parlamentsabgeordneten zu kommunizieren. Diese seien von § 53 dStPO nur um der Funktionsfähigkeit der Institutionen und nicht um der Menschenwürde willen geschützt.

Die Unterscheidung des BVerfG ist in sich konsequent. Der sogenannte Kern der privaten Lebensgestaltung ist Ausfluss der Menschenwürde und darf daher nicht angetastet werden. Dies bestätigt auch das BVerfG in seinem Urteil zur Verfassungskonformität des § 160a dStPO und zieht erneut den Kern der privaten Lebensgestaltung

⁴⁶³ BVerfG MMR 2004, 302 = BeckRS 2004, 21087.

⁴⁶⁴ BVerfG BeckRS 2004, 21087, Rz 148.

⁴⁶⁵ Vgl hierzu auch *Fishedick*, Das Beicht- und Seelsorgegeheimnis, Zur Legitimation und Reichweite der Zeugnisverweigerungsrechte für Geistliche, DÖV 2008, 584, 590 f.

⁴⁶⁶ Hierbei verweist das BVerfG auf seine Entscheidung BVerfGE 90, 255, 260.

heran.⁴⁶⁷ Hierbei sollte jedoch nicht direkt auf die Menschenwürde und deren Ausflüsse abgestellt werden. Diese Abgrenzung mag etwas unscharf wirken, ist doch letztlich der gesamte Grundrechtskatalog auf der Menschenwürde aufgebaut. Statt Menschenwürde und ihre direkte Ausflüsse sollte vielleicht davon gesprochen werden, dass einige Grundrechte ein besonders Näheverhältnis zur Menschenwürde aufweisen, zB die Religionsfreiheit, was bei anderen Grundrechten nicht der Fall ist.

15.2.2.2. Differenzierung im Rahmen des § 160a dStPO

Die ursprünglich herausgearbeitete Rechtsprechungslinie verfolgt das BVerfG jedoch nicht in vollständiger Konsequenz. Zwar bestätigt das BVerfG im Wesentlichen die im Urteil zum Großen Lauschangriff gewonnen Erkenntnisse und konkretisiert sie weiter, jedoch überrascht das BVerfG dann teilweise bei der Differenzierung.

In die Rechtsprechung des BVerfG reiht sich der absolute Schutz für Geistliche und Strafverteidiger ein.⁴⁶⁸ Auch die Gleichstellung von Rechtsanwälten mit Strafverteidigern ist dabei folgerichtig nicht unter dem Gesichtspunkt des Gleichheitssatzes in Art 3 Abs 1 GG zu beanstanden, da eine saubere Trennung von beidem quasi nicht möglich ist und auch die rechtsstaatliche Bedeutung des Anwaltsberufes von großer Bedeutung ist.⁴⁶⁹

Dafür lassen sich die Aussagen zur Gruppe der Abgeordneten nicht in eine saubere Linie mit der bisherigen Rechtsprechung einreihen, auch wenn das Gericht versucht, dies zu tun. Der Gesetzgeber gewährt ihnen den absolute Schutz des § 160a Abs 1 dStPO.⁴⁷⁰ Dies wird mit Art 47 GG begründet,⁴⁷¹ also mit der Funktionsfähigkeit der Institutionen. Dies passt zwar insofern zur bisherigen Rechtsprechung des BVerfG, als dass die Vorschrift des § 53 Abs 4 dStPO nicht dem Persönlichkeitsschutz oder der Menschenwürde dient, sondern der institutionellen Funktionsfähigkeit.

⁴⁶⁷ BVerfG NJW 2012, 833, 841.

⁴⁶⁸ BVerfG NJW 2012, 833, 842.

⁴⁶⁹ Dies hat wohl mittlerweile auch der Gesetzgeber erkannt, vgl BT-Drucksache 17/2637, 6.

⁴⁷⁰ Mitglieder des Deutschen Bundestages, der Bundesversammlung, des Europäischen Parlaments aus der Bundesrepublik Deutschland oder eines Landtages (vgl § 53 Abs 4 dStPO).

⁴⁷¹ *Griesbaum* in Karlsruher Kommentar zur StPO⁶, § 160a, Rz 3 mit Verweis auf BT-Drucksache 16/5846, 35.

Im Rahmen des § 160a dStPO muss aber aus Gleichheitsgesichtspunkten kritisch gesehen werden, dass der Gesetzgeber beispielsweise Art 47 GG als Grund für die Privilegierung von Abgeordneten heranzieht, dann aber wiederum die Pressefreiheit in Art 5 Abs 1 GG⁴⁷² als Schutzgut außen vor lässt, welche den Schutz von Medienmitarbeitern in § 53 Abs 1 Nr 5 dStPO bedingt.⁴⁷³ Das Gericht übersieht letztlich noch einen weiteren Aspekt. Es lehnt – auch eine partielle – Gleichbehandlung von Anwälten und Steuerberatern ab. Lediglich Steuerberater, die zugleich Rechtsanwälte sind, können sich auf § 160a Abs 1 dStPO berufen.⁴⁷⁴ Eine Kritik der Steuerberater über einen „Zwei-Klassen“-Berufsgeheimnisträgerschutz ist hierbei nicht von der Hand zu weisen.⁴⁷⁵ Grund dafür ist das Steuerstrafrecht, in dem Steuerberater für ihre Mandanten tätig werden. Ein beratungsrechtliches Mandat kann jederzeit fließend in ein Verteidigungsmandat übergehen.⁴⁷⁶ Hier zeigt sich die Parallele zum Rechtsanwalt und Strafverteidiger deutlich, weswegen die Abwägungen des BVerfG in diesem Punkt unausgewogen sind.⁴⁷⁷

15.2.2.3. Bedeutung von absolutem Geheimnisträgerschutz in § 160a Abs 1 dStPO

Hinsichtlich der Bedeutung des absoluten Geheimnisträgerschutzes muss auch auf die Zwecksetzung des § 160a Abs 1 dStPO abgestellt werden. Sinn des § 160a dStPO ist es auch, dass sich der Grundrechtsträger sicher sein kann, dass wenn er den Berufsgeheimnisträger aufsucht, er auch vor staatlicher Überwachung sicher ist und frei von dem Gedanken, Inhalte könnten Dritten gegenüber bekannt werden, sich diesem anvertrauen kann. Für ein solches Vertrauensverhältnis ist es nicht förderlich und sogar höchst schädlich, wenn sich der Ratsuchende dem nicht sicher sein kann, da er geneigt

⁴⁷² Vgl dazu *Szuba*, Vorratsdatenspeicherung, 163.

⁴⁷³ *Huber* in BeckOK, § 53, Rz 23.

⁴⁷⁴ *Goez*, Keine Gleichheit von Steuerberatern mit Rechtsanwälten als Verteidiger, *SteuK* 2012, 107.

⁴⁷⁵ *Vinken*, Ausdehnung des § 160a StPO auf Steuerberater zum Schutz der Mandanten, *DStR-KR* 2011, 13.

⁴⁷⁶ *Becherer*, Zum Seminar B: Der Schutz des Berufsgeheimnisses bei Steuerberatern in Deutschland, *IStR* 2010, 555, 557.

⁴⁷⁷ Aus diesem Grund hält die Bundessteuerberaterkammer auch an ihrer Forderung fest, den Schutz des § 160a Abs 1 dStPO auch auf Steuerberater auszudehnen, vgl zu entsprechenden Initiativen *Vinken*, Praxistauglichkeit verbessern – mehr Rechtssicherheit im Steuerrecht schaffen, Beihefter zu *DStR* 22 2012, 81.

sein wird, sich im Zweifel gar keinen Rat zu holen. Daran ändert auch die Tatsache nichts, dass nachträgliche Beweisverwertungsverbote bestehen.

Hat sich jemand beispielsweise einem Seelsorger anvertraut⁴⁷⁸ und wurde dieses Gespräch von Ermittlern mitgehört, wird der Betroffene, auch wenn ein Beweisverwertungsverbot besteht, beim nächsten Konfliktfall allein aus Angst, dass ein Dritter vom Gespräch Kenntnis nimmt, weniger geneigt sein, diesen aufzusuchen. Der Betroffene wird in eine psychische Zwangslage geraten, die ihm eine Inanspruchnahme seelsorgerischer Hilfe erschwert oder unmöglich macht und ihn damit in seinen Grundrechten beschneidet.

Hierbei ist die Bedrohungslage für das Vertrauensverhältnis sogar ungleich größer als im Rahmen strafprozessualer Ermittlungen. Beschränkt sich dort der Schutz allein auf strafprozessual relevante Vorgänge, so erfasst die Überwachung – potentiell – den gesamten Lebensbereich.

15.2.2.4. *Verhältnis zu anderen strafprozessualen Vorschriften in Deutschland*

In bestimmten Bereichen, die sich jedoch alle außerhalb der Telekommunikation bewegen, namentlich beim Mithören des gesprochenen Worts in Wohnungen (§ 100c Abs 6 dStPO) und bei der Beschlagnahme von Schriftstücken, Ton-, Bild- und Datenträgern, Abbildungen und anderen Darstellungen, die sich , die sich im Gewahrsam einer zur Zeugnisverweigerung berechtigten Person oder einer Redaktion, eines Verlages, einer Druckerei oder Rundfunkanstalt befinden ist zunächst § 97 Abs 5 dStPO einschlägig. Hier tritt aber je nach Fallkonstellation § 160a dStPO ergänzend hinzu.⁴⁷⁹ Insofern beeinflusst § 160a dStPO, der ja eigentlich nur für die verdeckte Überwachung geschaffen wurde, auch andere Vorschriften der dStPO.

⁴⁷⁸ Was hierbei unter Beichte oder Seelsorgegespräch zu verstehen ist, darf nicht zur Disposition des Gesetzgebers stehen, sondern bleibt allein der Religionsgemeinschaft überlassen; vgl *Fishedick*, Praxistauglichkeit verbessern – mehr Rechtssicherheit im Steuerrecht schaffen, DÖV 2008, 584, 590.

⁴⁷⁹ *Sackreuther* in BeckOK StPO, § 160a, Rz 17.

15.3. Bewertung

Aus der Rechtsprechung des BVerfG und der gesetzlichen Umsetzung in Deutschland lassen sich folgende Schlüsse ziehen: Eine Unterscheidung zwischen den einzelnen Berufsgeheimnisträgern ist nicht schlechthin aus Gründen des Grundrechtsschutzes verboten. Jedoch muss der Gesetzgeber, wenn er differenziert, eine einheitliche Linie fahren. Aus Gründen des Gleichheitssatzes kann etwa schwerlich begründet werden, warum Parlamentsabgeordnete unter den Schutz des § 160a Abs 1 dStPO fallen, Psychologen hingegen aber nicht.

Hier schert das BVerfG aus seiner bisherigen Rechtsprechungslinie aus und kommt zu einem Abwägungsergebnis, welches in sich nicht völlig durchdacht ist.⁴⁸⁰ Praktisch wird dies nach meiner Ansicht verfassungskonform nur insofern zu lösen sein, als dass die relativen Beweiserhebungsverbote in § 160a Abs 2 dStPO in solchen Fällen sehr restriktiv zu handhaben sind, so dass beispielsweise bei Steuerberatern und Psychologen in einen nahezu gleichen Schutz wie im Rahmen von § 160a Abs 1 dStPO kommen.

Darüber hinaus gebietet auch die EMRK eine sehr restriktive Auslegung von § 160a dStPO, da ansonsten ein hinreichender Schutz nach Art 8 EMRK nicht als gewährleistet angesehen werden kann. Der EGMR hatte hierbei einen Fall zu entscheiden⁴⁸¹, in dem in die Bankverbindung eines Anwalts aufgrund von § 160 Abs 4 dStPO mehrfach Einsicht genommen wurde, da aus Sicht der Ermittler *bestimmte Tatsachen den Verdacht begründeten*, dass der Verteidiger selbst einer Straftat verdächtig ist. Diese Vorschrift sei zu unbestimmt, um zu eine Aufhebung aller in § 160a dStPO vorgesehenen Rechte zu führen.⁴⁸²

15.4. Umsetzung im Polizeirecht

Auch bei der präventiven Arbeit von Ermittlern tragen die Polizeigesetze des Bundes und der Länder der Stellung der Berufsgeheimnisträger Rechnung. Bei Daten-

⁴⁸⁰ Kritisch hierzu auch *Sachs*, Grundrechte: Fernmeldegeheimnis und Unverletzlichkeit der Wohnung, Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen im Strafprozess, JuS 2012, 374, 376.

⁴⁸¹ EGMR v 27/04/2017, 73607/13 – Sommer ./, Deutschland.

⁴⁸² EGMR v 27/04/2017, 73607/13, Rz 61.

erhebungen im Telekommunikationsbereich ist darauf zu achten, dass diese Berufsgeheimnisträger im Sinne der dStPO nicht betreffen. Stellt sich erst während der Ermittlung heraus, dass ein Berufsgeheimnisträger betroffen ist, macht dies die Datenerhebung unzulässig.⁴⁸³

Hierbei wird auf das Zeugnisverweigerungsrecht der Berufsgeheimnisträger in §§ 53, 53a dStPO verwiesen. Diese sind etwa nach Art 34a Abs 1 S 3 PAG ebenso bei Datenerhebungen ausgenommen, wie die Intimsphäre der Überwachten. Somit dürfen sich Überwachungen der Exekutive gegen diese gar nicht richten; stellt sich dies erst während der Überwachung heraus, so sind die Daten zu löschen. Diese Norm findet sich beim verdeckten Eingriff auf informationstechnische Systeme, mithin einer Online-Durchsuchung, ebenfalls (Art 34d Abs 1 S 3 PAG). Erst recht ist eine weitere Verwendung, etwa in einem Strafverfahren, verboten (Art 34c Abs 4 PAG).

Die strafprozessuale Wertung wird damit zur Gänze in den polizeirechtlichen Bereich übertragen. Es besteht keine Möglichkeit, hiervon – etwa nach Einschaltung einer neutralen Stelle – abzuweichen. Einzige Ausnahme stellt der Fall dar, in dem der Berufsgeheimnisträger selbst der Straftat verdächtig ist, etwa dann, wenn er als Komplize der Person agiert, gegen die ermittelt werden soll.⁴⁸⁴ Dies stellt aber ohnehin keinen Fall des Berufsgeheimnisträgerschutzes dar.

16. Die Entscheidung des EuGH zur Vorratsdatenspeicherung

Auch der Entscheidung des EuGH über die Vorratsdatenspeicherung auf Vorlage des VfGH und des High Court of Ireland⁴⁸⁵ lässt sich entnehmen, dass im Rahmen der Vorratsdatenspeicherung Ausnahmen für Berufsgeheimnisträger bestehen müssten. Deren Fehlen wirkte sich in der Entscheidung des EuGH im Rahmen der Verhältnismäßigkeit aus.

⁴⁸³ Die Überwachung war damit nicht unrechtmäßig, jedoch dürfen die Ermittler die Daten nicht verwenden und haben diese umgehend zu löschen. Vgl etwa zur Regelung in Bayern, *Berner/Köhler/Käß*, Polizeiaufgabengesetz, Art 34a, Rz 10 ff.

⁴⁸⁴ *Berner/Köhler/Käß*, PAG²⁰, Art 34a, Rz 15.

⁴⁸⁵ EuGH v 08.04.2012, C-293/12 und C-594/12.

Hierbei stellte der EuGH bezüglich der Vorratsdatenspeicherung im Hinblick auf Berufsgeheimnisträger fest:⁴⁸⁶

Die Richtlinie 2006/24 betrifft nämlich zum einen in umfassender Weise alle Personen, die elektronische Kommunikationsdienste nutzen, ohne dass sich jedoch die Personen, deren Daten auf Vorrat gespeichert werden, auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte. Sie gilt also auch für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte. Zudem sieht sie keinerlei Ausnahme vor, so dass sie auch für Personen gilt, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen.

Aus diesen Ausführungen lässt sich zwar nicht konkret herauslesen, wie sich der der Gerichtshof den Schutz der Berufsgeheimnisträger vorstellt, es ist aber festzuhalten, dass ein solcher Schutz existieren muss und dieser im Falle heimlicher Überwachung in irgendeiner Weise mit Ausnahmen einherzugehen hat. Der EuGH diskutierte diese Fragestellung im Rahmen der Verhältnismäßigkeit. Insofern seien Eingriffe in Art 7 und 8 GRC auf das Nötigste zu beschränken.

Auch diese gerichtliche Entscheidung bestätigt die These, dass es im Rahmen von Telekommunikationsüberwachung für Berufsgeheimnisträger entsprechende Ausnahmen geben muss. Auch an dieser Stelle ist die Vorratsdatenspeicherung nur als Beispiel heranzuziehen. Vielmehr lassen sich aus der Aussage des EuGH auch allgemeingültige Ansichten für die Überwachung von Berufsgeheimnisträgern herauslesen. Die Definition, wer Berufsgeheimnisträger ist, überlässt der EuGH an dieser Stelle dem nationalen Gesetzgeber. Es ist aber wohl davon auszugehen, dass ihm dabei der bekannte Kanon der Berufsgeheimnisträger, wie etwa Rechtsanwälte, Journalisten, Ärzte oder Seelsorger, vorschwebte.

⁴⁸⁶ EuGH v 08.04.2012, C-293/12 und C-594/12, Rz 58.

17. Die Entscheidung des VfGH zur Vorratsdatenspeicherung

Letztlich hatte auch der VfGH auf Grundlage der Entscheidung des EuGH über die Vorratsdatenspeicherung zu urteilen. Hierbei bezieht sich der VfGH⁴⁸⁷ auf die oben erwähnten Artikel der GRC und auf nationales Verfassungsrecht, namentlich Art 8 EMRK und § 1 DSG 2000.⁴⁸⁸ Im Folgenden soll auf die Entscheidung des VfGH in Bezug auf Berufsgeheimnisträger eingegangen werden.

Auf Berufsgeheimnisträger wird hierbei – auch wenn dies von klägerischer Seite explizit angeführt wurde – nicht Bezug genommen. Allerdings trifft der VfGH einige Grundaussagen, die sich auf die Überwachung von jedermann beziehen. Insbesondere sei bei solch umfassenden Überwachungsmaßnahmen der Missbrauchsprävention eine entsprechend hervorgehobene Stellung einzuräumen.⁴⁸⁹ Weiters müssten die Geheimhaltungsinteressen der Betroffenen in angemessener Weise garantiert werden.⁴⁹⁰

Bemerkenswert an der Entscheidung ist, dass der VfGH in der Form erstmalig das Grundrecht auf informationelle Selbstbestimmung, welches in der Rechtsprechung des deutschen BVerfG schon seit Jahren Anwendung findet⁴⁹¹ und letztlich auch für den Berufsgeheimnisträgerschutz bedeutend ist, als Grundrecht anerkennt. Hierzu führt der VfGH aus:⁴⁹²

Bedeutung und Gewicht der mit der Vorratsdatenspeicherung verfolgten Ziele, wie sie der Gesetzgeber auch mit der Zweckbindung in § 102a Abs 1 letzter Satz TKG 2003 zum Ausdruck bringt, sind erheblich. Doch auch wenn die Regelung ausweislich des Wortlauts des Abs 1 einem wichtigen öffentlichen Interesse dient [...], ist es angesichts der "Streubreite" des Eingriffs [...], des Kreises und der Art der betroffenen Daten [...] und der daraus folgenden Schwere des Eingriffs in das Recht auf informationelle Selbstbestimmung (es kann auf Daten zu-

⁴⁸⁷ VfGH v. 27.06.2014 – G 47/2012-49, ua, Rz 136 ff.

⁴⁸⁸ Zu Art 10a StGG und dessen Anwendbarkeit oder Nichtanwendbarkeit auf Metadaten schweigt sich die Entscheidung leider aus.

⁴⁸⁹ VfGH v. 27.06.2014 – G 47/2012-49, ua, Rz 188 f.

⁴⁹⁰ VfGH v. 27.06.2014 – G 47/2012-49, ua, Rz 148.

⁴⁹¹ Vgl zur informationellen Selbstbestimmung 9.2.

⁴⁹² VfGH v. 27.06.2014 – G 47/2012-49, ua, Rz 168.

gegriffen werden, welche im Falle ihrer Verknüpfung nicht nur die Erstellung von Bewegungsprofilen ermöglichen, sondern auch Rückschluss auf private Vorlieben und den Bekanntenkreis einer Person zulassen; [...]) erforderlich, dass der Gesetzgeber durch geeignete Regelungen sicherstellt, dass diese Daten nur bei Vorliegen eines vergleichbar gewichtigen öffentlichen Interesses im Einzelfall für Strafverfolgungsbehörden zugänglich gemacht werden und dies einer richterlichen Kontrolle unterliegt.

Leider lassen sich aus der Entscheidung des VfGH keine näheren Erkenntnisse zur normativen Verankerung dieses für die österreichische Rechtsordnung von der Terminologie her fremden Grundrechtes finden. Der VfGH hat allerdings aus Deutschland bekannte Wertungen dieses Grundrechts übernommen und im Vergleich zum BVerfG sogar etwas ausgebaut. Während das BVerfG im Rahmen der informationellen Selbstbestimmung (Art 2 Abs 1 iVm Art 1 Abs 1 GG) nicht unbedingt einen richterlichen Vorbehalt verlangt, scheint dies beim VfGH der Fall zu sein. Möglich scheint hier, dass dem VfGH in Wirklichkeit eher das neu entwickelte Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (sog „IT-Grundrecht“)⁴⁹³, welches ja vom BVerfG unter einen richterlichen Vorbehalt gestellt wurde, vorschwebt, als das klassische Recht auf informationelle Selbstbestimmung. Beide Grundrechte lassen sich nicht scharf voneinander abgrenzen. Dies ist auch insofern denkbar, als dass das IT-Grundrecht eine rechtliche Entwicklung neueren Datums ist und bereits an die aktuellen grundrechtlichen Herausforderungen angepasst ist. Es ist davon auszugehen, dass der VfGH den aktuellen Grundrechtseingriffen, die zur Entwicklung des Grundrechts auf informationelle Selbstbestimmung in der Form und Intensität gar nicht möglich gewesen wären, Rechnung tragen wollte.

⁴⁹³ Vgl zur Herkunft und zur schwierigen Abgrenzung zum Grundrecht auf informationelle Selbstbestimmung unter 9.3.

18. Die Bedeutung „überwachungsfreier Räume“ in der Rechtsprechung des Bundesverfassungsgerichtes

Die Vorratsdatenspeicherung zeigt, als eine Art Negativbeispiel, eine Welt, mit im digitalen Bereich nicht mehr vorhandenen überwachungsfreien Räumen. Ist es außerhalb des digitalen Bereiches bei Unbescholtenheit relativ leicht, nicht in das Visier der Ermittler zu geraten, machte dies die Vorratsdatenspeicherung im digitalen Umfeld unmöglich.⁴⁹⁴ Doch selbst dann, wenn Personen nicht unbedingt als unbescholten bezeichnet werden können, stehen ihnen überwachungsfreie Räume zu. Überwachung darf etwa dort nicht stattfinden, wo die absolute Intimsphäre der Betroffenen angetastet würde. Hierbei ergeben sich eindeutige Parallelen zu dem Recht, bestimmte Berufsheimnisträger zu kontaktieren.

Aus der Rechtsprechung des BVerfG und der allgemeinen Konzeption des § 160a dStPO lassen sich für den grundrechtlichen Schutz der Vertrauensbeziehungen der Berufsheimnisträger allgemeingültige Lehren ziehen. Zum einen ist es eine wichtige Grunderkenntnis, dass es dort, wo es Überwachung gibt, auch überwachungsfreie Räume geben muss. Dies bedeutet nicht nur, dass unter Umständen im Nachhinein gewonnene Erkenntnisse durch Ermittlungsbehörden nicht ausgewertet werden dürfen, sondern dass es in einem Rechtsstaat auch Vertraulichkeitsverhältnisse geben muss, die nur in absoluten Ausnahmefällen überhaupt einer Überwachung unterliegen.

18.1. Relevanz des „Kernbereiches privater Lebensgestaltung“

In diesem Zusammenhang ist in Deutschland die Bedeutung des „Kernbereiches privater Lebensgestaltung“⁴⁹⁵ näher zu untersuchen. Dieser unterliegt nach der Rechtsprechung des BVerfG ebenfalls nicht der Überwachung. Das BVerfG hat schon sehr früh im sogenannten Elfes-Urteil die Bedeutung dieses Kernbereichs für die persönliche Lebensgestaltung eines jeden Menschen hervorgehoben. Hierbei stellte das Gericht klar, dass *ein letzter unantastbarer Bereich menschlicher Freiheit besteht, der der Einwir-*

⁴⁹⁴ Auf diesem Umstand verwies auch explizit ein Antragsteller, der mit dem Gesetz noch nie in Konflikt gekommen ist; VfGH v. 27.06.2014 – G 47/2012-49, ua, Rz 138.

⁴⁹⁵ Hierzu näher Möstl, Datenverfügbarkeit als Voraussetzung für innere Sicherheit, Ein Bericht aus Deutschland, SIAK-Journal 2010 H 2, 61, 65 ff.

*kung der gesamten öffentlichen Gewalt entzogen ist. Ein Gesetz, das in ihn eingreifen würde, könnte nie Bestandteil der ‚verfassungsmäßigen Ordnung‘ sein; es müsste durch das BVerfG für nichtig erklärt werden.*⁴⁹⁶ Das BVerfG schafft damit mehrere Schutzsphären. Je näher sich ein Vorgang am Kernbereich der Menschenwürde befindet, desto eher muss dieser unangetastet bleiben. Befindet man sich im Kernbereich selbst, so ist dieser staatlichen Eingriffen zur Gänze entzogen. Hierüber findet dann auch keine Abwägung mehr statt.

Sobald festgestellt wird, dass eine Überwachung auf diesen Bereich abzielt, ist sie sofort zu beenden. Dieser ist unmittelbar aus der Menschenwürde abzuleiten.⁴⁹⁷ Dies wiederum kommt in verschiedensten Gesetzen zum Ausdruck. Parallel zum relativ neuen § 160a dStPO existieren zahlreiche Vorschriften, die den Kernbereich der privaten Lebensgestaltung von der Überwachung ausnehmen.⁴⁹⁸ In diesem Kernbereich, der die Intimsphäre umfasst, gibt es keine Abwägung; der Bereich ist für Dritte unantastbar.⁴⁹⁹ Der Kernbereich der privaten Lebensgestaltung beinhaltet die Intimsphäre des Grundrechtsträgers. Zur Intimsphäre zählt alles, was zu dessen innerster Lebensführung zählt, wie etwa Sexualität oder innerste Gedanken.⁵⁰⁰

Dies bedeutet für überwachungsfreie Räume folgendes: Zum einen ist deren Existenz kein neues Phänomen, was erst im Laufe der Zeit durch immer fortschrittlichere Überwachungsmethoden aufkam, sondern findet sich bereits früh in der verfassungsgerichtlichen Rechtsprechung.⁵⁰¹ Zum anderen ergeben sich bezüglich der überwachungsfreien Räume Überschneidungen und Parallelen zu dem gebotenen Schutz der Berufsgeheimnisträger.

⁴⁹⁶ BVerfGE 6, 32, 41 = NJW 1957, 297.

⁴⁹⁷ Näheres zum Kernbereich der privaten Lebensführung vgl. *Hillgruber*, BeckOK GG, Art 1, Rz 27 mwN.

⁴⁹⁸ Etwa § 100a Abs 4 dStPO oder § 3a S 1 G 10 G; vgl. *Roggan*, G 10 G, § 3a, Rz 4.

⁴⁹⁹ *Kretschmer*, § 160a StPO – gelungene oder misslungene Gesetzgebung?, HRRS 2010, 551, 556f.

⁵⁰⁰ BVerfG NJW 2004, 999, 1002. Das in BVerfG NJW 1969, 1707 entwickelte Kriterium, dass es sich hierbei um Geheimnisse handelt, welche auf anderem Wege nicht ermittelt werden können, ist angesichts der umfangreichen Überwachungsmaßnahmen, welche heutzutage möglich sind, wohl nicht mehr praktikabel.

⁵⁰¹ BVerfGE 6, 32, 41 = NJW 1957, 297.

18.1.1. Überschneidungen des Kernbereichs privater Lebensgestaltung mit dem Schutz der Berufsgeheimnisse

Der Kernbereich privater Lebensgestaltung kann sich in vielen Fällen mit dem Berufsgeheimnisträgerschutz überschneiden. Hierbei wären natürlich zum einen besondere Vertrauensverhältnisse zu Berufsgeheimnisträgern zu nennen. Gespräche mit ihnen sind grundsätzlich geeignet dem Kernbereich der privaten Lebensgestaltung zu unterfallen.⁵⁰² Je intimer das Gespräch ist, desto eher wird der Kernbereich betroffen sein. Die Übergänge zwischen schlichter Privatsphäre und dem Kernbereich sind fließend, so dass es leider unmöglich ist, bei jedem Sachverhalt von vornherein zu sagen, ob dieser dem Kernbereich unterfällt.⁵⁰³

18.1.2. Parallelen des Kernbereichs privater Lebensgestaltung mit dem Schutz der Berufsgeheimnisse

Selbst in Fällen, in denen es keine Überschneidung zwischen Kernbereich der privaten Lebensgestaltung und dem Berufsgeheimnisträgerschutz gibt, ergeben sich zwischen beiden letztlich auch Parallelen, deren Bedeutung näher zu diskutieren ist. Für den Kernbereich ist es in gewisser Weise kennzeichnend, dass für diesen – unabhängig davon auf welche Grundrechte man diesen im Einzelnen stützen mag – im Grunde die Menschenwürde aus Art 1 Abs 1 GG⁵⁰⁴ den Rahmen vorgibt, der – teils durch andere Grundrechte wie etwa Art 2 Abs 1 GG oder Art 13 Abs 1 GG gestützt – den Schutz bedingt.

Insofern speisen sich sowohl der elementare Berufsgeheimnisträgerschutz als auch der Kernbereichsschutz im deutschen Verfassungsrecht aus derselben Quelle und sind damit auch vergleichbar. Dies zeigt sich auch in der legislativen Praxis, etwa in Art 34a PAG,⁵⁰⁵ da dort der Schutz der Intimsphäre und jeder der Berufsgeheimnisträger gleich ausgestaltet wird. Dies bewirkt, dass Schutzvorschriften für private Räumlichkeiten sich auch auf Räumlichkeiten zur Berufsausübung auswirken können. Weiters gibt es verfassungsrechtliche Parallelen zwischen dem Schutz der privaten Lebens-

⁵⁰² Vgl etwa zu ärztlichen Unterlagen OLG Braunschweig BeckRS 2009, 87886.

⁵⁰³ Eisenberg, StPO, Rz 388f.

⁵⁰⁴ Mehr oder weniger Wortgleich hierzu Art 1 GRC.

⁵⁰⁵ Vgl hierzu 15.4.

gestaltung und dem Recht, sich an Berufsgeheimnisträger zu wenden. Aus diesen beiden an sich völlig unterschiedlichen Gründen, wird man diese Grundsätze und Grundgedanken des Grundrechtsschutzes in gewisser Weise übertragen müssen.

18.2. Notwendigkeit von „überwachungsfreien Räumen“ für Berufsgeheimnisträger

Überwachungsfreie Räume haben sowohl im Berufsgeheimnisträgerschutz als auch im Kernbereichsschutz der privaten Lebensgestaltung eine Bedeutung. Ihre Existenz ist auch per se nichts Neues. Genau wie es im täglichen Leben einer Privatperson Situationen gibt, die dem Kernbereich zuzuordnen sind, so sind bei Berufsgeheimnisträgern Gespräche und die Korrespondenz mit demjenigen, der ihn um seines Berufes willen aufsucht, mit einem gleichwertigen Schutz auszustatten und damit im Ergebnis überwachungsfrei.

Dieses grundrechtlich gebotene Vorgehen hat auch Konsequenzen. Eine Wohnraumüberwachung, bei der man nicht ausschließen kann, dass auch Geräusche aus dem Schlafzimmer des Überwachten zu hören sind, ist unzulässig, da dieses zum Kernbereich der privaten Lebensgestaltung gehört, was letztlich durch die Menschenwürde so geboten ist.⁵⁰⁶ Ähnlich liegt der Fall bei vielen Berufsgeheimnisträgern in Bezug auf bestimmte berufliche Tätigkeiten, so dass sich hier eine Parallele aufdrängt.⁵⁰⁷

Das verfassungsrechtliche Problem bei der Überwachung von Telekommunikation, sei es während, vor oder auch nach Abschluss des Telekommunikationsvorgangs, ist die Schwierigkeit abzugrenzen, wann entsprechende Kommunikation vorliegt, die diesen Schutz verdient. Im eigentlichen Sinne fällt private Kommunikation, die ein Berufsgeheimnisträger etwa über seinen dienstlichen E-Mail-Account tätigt, nicht unter dessen Berufsgeheimnisträgerprivileg, weswegen es auch von grundrechtlicher Seite keines „überwachungsfreien Raumes“ hierfür bedarf.

⁵⁰⁶ Vgl nur *Polenz* in Kilian/Heussen, Computerrechtshandbuch³¹, Teil 13, Rz 39 mwN.

⁵⁰⁷ Etwa Geistliche während der Beichte; vgl *Leisner*, Das neue „Kommunikationsgrundrecht“ – Nicht Alibi für mehr, sondern Mahnung zu weniger staatlicher Überwachung NJW 2008, 2902, 2904 mwN.

Allerdings darf auch in einem solchem Fall nicht dazu übergegangen werden, zunächst zu überwachen und dann erst die Überwachung zu unterlassen, wenn eventuell berufsrelevante Themen zur Sprache kommen. Solange der Berufsgeheimnisträger seine private und berufliche Sphäre trennt, spricht nichts dagegen, den privaten Bereich nach den rechtsstaatlichen Grundsätzen unter Ausnahme des Kernbereichs zu überwachen, wie bei jedem anderen Bürger. Wenn etwa ein Strafverteidiger über ein berufliches und ein privates Mobiltelefon verfügt, so spricht nichts dagegen, das private Mobiltelefon nach rechtsstaatlichen Grundsätzen zu überwachen. Bekommen die Ermittler im Laufe der Ermittlung mit, dass es sich doch ausnahmsweise um ein Gespräch mit (auch) beruflichem Charakter handelt, hat die Überwachung ab diesem Zeitpunkt zu unterbleiben. Hier liegt der Fall nicht anders als bei einer Wohnraumüberwachung, die das Schlafzimmer ausspart, nicht aber die Küche. Bekommen die Ermittler mit, dass Handlungen und Gespräche, die der Intimsphäre des Überwachten zuzuordnen sind, in der Küche stattfinden, hat ab diesem Zeitpunkt deren Überwachung ebenfalls zu unterbleiben.

Allerdings kann kein Berufsgeheimnisträger dazu gezwungen werden, Privat- und Berufsleben klar zu trennen. Ebenso wie eine Person, die überwacht werden soll in einer Garçonnière wohnen kann, was eine Wohnraumüberwachung nach rechtsstaatlichen Gesichtspunkten schwierig bis unmöglich machen kann, kann ein Berufsgeheimnisträger ein Mobiltelefon, einen Internetanschluss oder ein E-Mail-Postfach für seine berufliche und private Kommunikation nutzen, anstatt hier zu separieren. In einem solchen Fall kann, aufgrund der Vergleichbarkeit beider Fälle, nichts anderes gelten, wie für denjenigen der ein Einzelapartment bewohnt. Letztlich bedeutet dies, dass auch bestimmte Grundsätze aus der Überwachung des privaten Wohnraums auch auf Berufsgeheimnisträger anzuwenden sein werden, weil eine Trennung zwischen privatem und beruflichem Bereich oft unmöglich ist und der Trend allgemein in die Richtung geht, dass privates und berufliches weniger strikt getrennt wird, als dies früher der Fall war. So mag es zwar umstritten sein, ob der Trend zum Teleworking zunimmt,⁵⁰⁸ jedoch ist

⁵⁰⁸ Vgl etwa https://www.nytimes.com/2014/03/08/your-money/when-working-in-your-pajamas-is-more-productive.html?_r=1 und im Gegensatz dazu <http://derstandard.at/2000054819239/IBM-schafft-Home-Office-wieder-ab>.

allein durch gemeinsame Verwendung von technischen Endgeräten für private und berufliche Zwecke

19. Ergebnisse

Die Analyse von Rechtsprechung in Österreich, Deutschland und auf europäischer Ebene zeigt, dass es verfassungsrechtlich geboten ist, für Berufsgeheimnisträger Überwachungsfreie Räume zu schaffen. Auch wenn sich der VfGH hierzu nicht im Detail und auch nicht in Bezug auf Berufsgeheimnisträger äußert, so nimmt er doch an, dass dann, wenn die Überwachung lückenlos ist, es Ausnahmen geben muss. Ebenso sieht es auch der EuGH, der Berufsgeheimnisträger explizit erwähnt.

Die deutsche Rechtsprechung ist etwas detaillierter und geht konkret darauf ein, dass Berufsgeheimnisträger die Möglichkeit haben müssen, ungestört mit Ratsuchenden zu Kommunizieren und dies in einer Umgebung zu tun, die von vornherein keinen Überwachungen unterliegt, mithin in „überwachungsfreien Räumen“. Die Tatsache, dass es Bereiche gibt, die nicht der Überwachung unterliegen, ist insofern keine neue verfassungsrechtliche Entwicklung. Bereits im Rahmen des Schutzes der Intimsphäre hat das Bundesverfassungsgericht Räume definiert, die von der Überwachung ausgenommen sind. Hier ergibt sich also eine Parallele zu bereits bekannten verfassungsrechtlichen Prinzipien. Zudem ergeben sich und teils Überschneidungen.

Kapitel IV – Rechtsvergleichende Aspekte

Österreichische und deutsche Rechtsordnung unterscheiden sich gerade im Verfassungsrecht in einigen entscheidenden Punkten. Zum einen sind die Interpretationen vom Schutzbereich der Grundrechte teilweise anders, obwohl beide Rechtsordnungen vergleichbare Grundrechte kennen und zudem die EMRK und GRC in der Rechtsprechung der beiden europäischen Höchstgerichte, EGMR und EuGH, zu beachten haben. Hier kann Rechtsvergleichung ein sehr hilfreiches Instrument sein, da auf diese Weise neu über die Schutzrichtung eines Grundrechtes nachgedacht werden kann.

Zum anderen ist die Frage von Bedeutung, inwiefern gewisse verfassungsrechtliche Grundprinzipien von einer Rechtsordnung in die andere übertragen werden können. Wenn man die aus der deutschen und europäischen Rechtsordnung herausgearbeiteten Erkenntnisse analysiert, so kommt man zu dem Ergebnis, dass es zumindest in einigen Bereichen überwachungsfreie Räume für Berufsgeheimnisträger geben muss, damit diese in einem vertrauensvollen Umfeld ihrem Beruf nachgehen können. Hierbei kommt vor allem in der deutschen Rechtsordnung der Menschenwürde und deren unantastbarem Kernbereich eine entscheidende Bedeutung zu. Die Rechtsprechung des deutschen BVerfG stützt einen Teil ihrer Judikate, welche mit Telekommunikationsüberwachung zu tun haben, teilweise oder auch überwiegend auf Art 1 Abs 1 GG. Fraglich ist nun, ob diese Grundsätze aus dem deutschen Verfassungsrecht auf Österreich einfach übertragen werden können oder ob sich die Übertragung aufgrund der Unterschiede zwischen deutschem und österreichischem Verfassungsrecht hier eher nicht anbietet.

Weiters existieren bestimmte Grundrechte nicht in jeder Verfassungsrechtsordnung des jeweils anderen Landes. Auch diese Tatsache ist aus rechtsvergleichender Sicht interessant, da – und dies gilt gerade für Österreich – bestimmte verfassungsrechtliche Begriffe der jeweils anderen Rechtsordnung auch in der Verfassungsrechtsprechung Verwendung finden können, ohne dass näher auf ihre verfassungsrechtliche Verankerung eingegangen werden kann. Dies ist vor allem im Bereich des „Grundrechts auf informationelle Selbstbestimmung“ der Fall, von dessen Existenz der VfGH offenbar ausgeht, ohne sich jedoch näher zu dessen verfassungsrechtlicher Verankerung zu äußern.

20. Interpretation des Schutzbereiches des Fernmeldegeheimnisses

Um den Vergleich der Rechtsordnungen näher zu beleuchten, bedarf es zunächst aufgrund vorhergehend gewonnener Erkenntnisse einer Darstellung, welche Telekommunikationsdaten zu welchem Zeitpunkt durch welches Grundrecht geschützt werden und wo im Einzelnen juristische Meinungsverschiedenheiten bestehen.

Hierbei ist – je nach Rechtsordnung – der Telekommunikationsvorgang rechtlich nicht als Einheit zu betrachten, sondern besteht aus einer Vielzahl von Schritten. Zunächst ist nach der Art der Daten in inhaltlicher Form zu differenzieren. Es kann sich hierbei um den Inhalt des Telekommunikationsvorgangs selbst handeln oder aber auch um Metadaten über die Umstände der Kommunikation, also etwa über das Kommunikationsmittel, den Zeitpunkt, sowie die beteiligten Kommunikationsteilnehmer.

Ferner ist nach der Art der Daten in temporärer Hinsicht zu unterscheiden. Es kann sich hierbei um Daten handeln, die außerhalb eines bereits abgeschlossenen Telekommunikationsvorgangs, mithin nach Ende des Telekommunikationsvorgangs, etwa am Endgerät des Überwachten, erhoben werden. Ebenso kann es sich um Daten handeln, die während des Telekommunikationsvorgangs, somit auf dem Transportweg von einem Telekommunikationsempfänger zum anderen erhoben werden. Zwar handelt es sich bei erster Kategorie nicht um Telekommunikation im engeren Sinne, da die Übertragung der Daten bereits beendet ist, jedoch gibt es Überwachungsmaßnahmen, welche genau auf die Endgeräte der Kommunizierenden angesetzt sind. Auch nach der Kommunikation sind die ausgetauschten Inhalte und Metadaten verfassungsrechtlich geschützt, wenn auch zum Teil über andere Vorschriften als der Kommunikationsvorgang selbst.

Kombiniert man diese temporäre und die inhaltliche Komponente ist letztlich nach vier unterschiedliche „Datenarten“ zu differenzieren:

„Datenart“	Österreich	Deutschland	EU
Inhalte der Telekommunikation während eines Telekommunikationsvorgangs	Art 10a StGG; Art 8 EMRK; § 1 DSG 2000	Art 10 GG	Art 7, 8 GRC

Inhalte der Telekommunikation außerhalb eines Telekommunikationsvorgangs	Art 8 EMRK; § 1 DSG 2000	Art 2 Abs 1 GG iVm Art 1 Abs 1 GG; evtl auch Art 13 GG ⁵⁰⁹	Art 7, 8 GRC
Verkehrsdaten während eines Telekommunikationsvorgangs	Art 10a StGG (str); Art 8 EMRK; § 1 DSG	Art 10 GG	Art 7, 8 GRC
Verkehrsdaten außerhalb eines Telekommunikationsvorgangs	Art 8 EMRK; § 1 DSG 2000	Art 2 Abs 1 GG iVm Art 1 Abs 1 GG; evtl auch Art 13 GG	Art 7, 8 GRC

Diesen Datenarten wiederum können die konkreten Überwachungsmaßnahmen⁵¹⁰ zugeordnet werden. Die Zuordnung erfolgt dort, wo die Daten anfallen:

Maßnahme	Datenart
„stummes SMS“	Verkehrsdaten außerhalb eines Telekommunikationsvorgangs
IMSI-Catcher	Verkehrsdaten außerhalb eines Telekommunikationsvorgangs
IMEI-Catcher	Verkehrsdaten außerhalb eines Telekommunikationsvorgangs
Abfrage von Kundendaten beim Telekommunikationsanbieter	Verkehrsdaten während eines Telekommunikationsvorgangs
Funkzellenabfrage	Verkehrsdaten während eines Telekommunikationsvorgangs
Rufdatenrückerfassung	Verkehrsdaten während eines Telekommuni-

⁵⁰⁹ Dies hängt davon ab, ob sich die IT-Infrastruktur innerhalb einer Wohnung befindet oder ob außerhalb von Wohnraum auf die IT zugegriffen wird.

⁵¹⁰ Vgl hierzu 7.2.9.

	kationsvorgangs
Abhören von Gesprächen	Inhalte der Telekommunikation während eines Telekommunikationsvorgangs
E-Mail- und Textnachrichtenüberwachung	Inhalte der Telekommunikation während eines Telekommunikationsvorgangs
Quellen-Telekommunikationsüberwachung	Inhalte (und ggf Verkehrsdaten) der Telekommunikation während eines Telekommunikationsvorgangs
Online-Durchsuchung	Inhalte der Telekommunikation außerhalb eines Telekommunikationsvorgangs
Vorratsdatenspeicherung	Verkehrsdaten während eines Telekommunikationsvorgangs
Durchsuchung von Endgeräten	Inhalte und Verkehrsdaten der Telekommunikation außerhalb eines Telekommunikationsvorgangs

20.1. Rechtsvergleich des Fernmeldegeheimnisses in Österreich und in Deutschland

Nunmehr gilt es, die bereits gewonnenen Erkenntnisse dergestalt zusammen zu führen, dass die einzelnen Überwachungsmaßnahmen im Hinblick auf den Grundrechtseingriff eingeordnet werden. Hierbei ergeben sich im Rechtsvergleich zwischen Österreich und Deutschland viele Gemeinsamkeiten aber auch Unterschiede, die teilweise von großer praktischer Relevanz sind. Aus diesen Unterschieden sollen letztlich auch Schlussfolgerungen für die Auslegung der Rechtsnormen und gesetzgeberischen Reformbedarf auf verfassungsrechtlicher Ebene gezogen werden.

20.1.1. Inhalte der Telekommunikation während eines laufenden Telekommunikationsvorgangs

Ist die Telekommunikationsüberwachung inhaltsbezogen und findet der Zugriff auf den Inhalt der Telekommunikation statt, während der Telekommunikationsvorgang läuft, wird klassischerweise in das Fernmeldegeheimnis eingegriffen, welches den Inhalt der Kommunikation schützt. Hierbei ergeben sich zwischen Österreich und Deutschland vom Schutzbereich her keine Unterschiede. Die verfassungsrechtliche

Umsetzung in Art 10a StGG in Österreich und Art 10 GG in Deutschland unterscheidet sich jedoch durch den richterlichen Befehl, den Art 10a StGG vorsieht, welcher in Art 10 GG jedoch fehlt. Insofern kann davon ausgegangen werden, dass das Fernmeldegeheimnis in Bezug auf Inhaltsdaten⁵¹¹ in Österreich einen stärkeren Schutz erfährt als in Deutschland.

Umgekehrt wird zu diskutieren sein, ob ein solcher Vorbehalt nicht im Rahmen des Fernmeldegeheimnisses geboten ist. Die meisten Telekommunikationsüberwachungsmaßnahmen betreffen das Fernmeldegeheimnis nicht oder zumindest nicht direkt, da diese entweder nicht auf den Inhalt der Kommunikation gerichtet sind, sondern auf Verbindungsdaten oder zwar auf den Inhalt einer Kommunikation gerichtet sind, die aber schon abgeschlossen ist, so dass die Daten bei der überwachten Person bereits vorliegen. Von den untersuchten Überwachungsmaßnahmen unterfällt nur das Mithören von Gesprächen und je nach Fallkonstellation die E-Mail-Überwachung darunter. Letztere nur in den Fällen, in denen auf den Inhalt der E-Mail auf dem Server zugegriffen wird.

20.1.2. Inhalte der Telekommunikation nach einem abgeschlossenen Telekommunikationsvorgang

Viele Überwachungsmaßnahmen sind zwar auf den Inhalt der Telekommunikation gerichtet, der Vorgang der Telekommunikation ist aber zum Zeitpunkt des Zugriffs der Ermittler bereits abgeschlossen. Hier ist das Fernmeldegeheimnis sowohl in Österreich als auch in Deutschland nicht mehr anwendbar, da dieses voraussetzt, dass ein Fernmeldevorgang stattfindet, also zum Zeitpunkt der Überwachung zwei oder mehr Personen miteinander über einen von außen nicht einsehbaren Übertragungsweg miteinander kommunizieren.⁵¹²

Charakteristisch für den Fernmeldevorgang ist es, dass Kommunikation über einen von außen nicht einsehbaren Kanal stattfindet. Da dieser Kanal nur erschwert

⁵¹¹ Nur auf diese bezieht sich das Fernmeldegeheimnis in Art 10a StGG nach der herrschenden Auffassung in der Staatsrechtslehre in Österreich; vgl. *Wiederin*, in: Korinek/Holoubek, Österreichisches Bundesverfassungsrecht, Bd. III, Art 10a StGG, Rz 12.

⁵¹² Vgl. zur Abgrenzung *Eckhardt*, Wie weit reicht der Schutz des Fernmeldegeheimnisses (Art 10 GG)?, DuD 2006, 365, 366.

einsehbar ist, setzen Überwachungsmaßnahmen oft beim Nutzer selber an, wenn der Kommunikationsvorgang bereits abgeschlossen ist. Hier sind alle Überwachungsmaßnahmen, die direkt auf die Endgeräte der Nutzer zugreifen anzusiedeln. Darunter fällt also, sowohl das Durchsuchen der Festplatte durch Zugriff von außen, als auch das Anfertigen von Screenshots während eines Chatvorgangs oder Keylogging.

Die Einordnung dieser Maßnahmen ist in Deutschland, da hierfür kein spezifisches Grundrecht existiert, über das sog „Auffanggrundrecht“ in Form von Art 2 Abs 1 GG iVm Art 1 GG gewährleistet. Hierfür hat das BVerfG⁵¹³ zuletzt das „Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme“ entwickelt, welches auch unter einem richterlichen Vorbehalt steht.

Hier stellt sich, mangels praktischer Relevanz,⁵¹⁴ nur die verfassungstheoretische Frage, ob Eingriffe solcher Art in Österreich nicht auch eines richterlichen Befehls bedürften. Der verfassungsrechtliche Vergleich zwischen beiden Ländern und die Interessenlage der Betroffenen legt dieses freilich nahe. Daher soll diese Frage hier zumindest kurz angedacht werden, für den Fall, dass der Gesetzgeber in Österreich in Zukunft die Einführung solcher Maßnahmen beabsichtigt.⁵¹⁵ Nach einem Bericht von BMJ und BM.I stehen einer Einführung in Österreich jedoch große verfassungsrechtliche Hürden entgegen.⁵¹⁶ Neben einer Verletzung des Verhältnismäßigkeitsgrundsatzes⁵¹⁷ wurde unter anderem bemängelt, dass sich – ähnlich wie in Deutschland – wenn

⁵¹³ Vgl oben unter 9.3

⁵¹⁴ Zur Unzulässigkeit der sog „Online-Überwachung“ vgl zusammenfassend Bertel/Venier, StPO, § 136, Rz 5f.

⁵¹⁵ Die Technologie, welche für den Einsatz eines Staatstrojaners notwendig ist, wurde vom deutschen Softwareunternehmen DigiTask nach Österreich an das BM.I geliefert und steht damit – technischer Hinsicht – den Ermittlern zur Verfügung; vgl <http://www.heise.de/tp/blogs/8/150615>. Hierbei fand auch ein Einsatz – ohne jegliche Rechtsgrundlage – wohl statt; <http://www.profil.at/articles/1142/560/310153/bundestrojaner-trojanische-sitten>.

⁵¹⁶ Details zur fehlenden Rechtsgrundlage und zu den verfassungsrechtlichen Bedenken im Bericht der interministeriellen Arbeitsgruppe Online-Durchsuchung von BMJ und BM.I; der Bericht ist zwischenzeitlich nicht mehr über die Ministerialhomepages abrufbar, findet sich aber noch an anderer Stelle im Internet unter <http://docplayer.org/18876703-Erweiterung-des-ermittlungsinstrumentariums-zur-bekaempfung-schwerer-organisierter-und-terroristischer-kriminalitaetsformen.html>.

⁵¹⁷ Vgl Bericht Arbeitsgruppe Online-Durchsuchung, 67 ff.

auch unter anderen verfassungsrechtlichen Vorzeichen, die Frage nach einem Eingriff in den Kernbereich des Privaten stellt.⁵¹⁸

Bei einigen Überwachungsmaßnahmen greift also das Fernmeldegeheimnis nicht ein. Der grundrechtliche Schutz erfolgt dann aus österreichischer Sicht über das Grundrecht auf Datenschutz (§ 1 DSG 2000) und das Recht auf Achtung des Privat- und Familienlebens (Art 8 EMRK).

Dies betrifft vor allem die Quellen-TKÜ und die Online-Durchsuchung und in vielen Fällen die E-Mail und Textnachrichtenüberwachung, sofern diese auf dem Endgerät des Nutzers unabhängig von einem Telekommunikationsvorgang stattfindet.

20.1.3. Verbindungsdaten während eines Telekommunikationsvorgangs

Während der Inhalt während einer Telekommunikation in Österreich durch Art 10a StGG und in Deutschland durch Art 10 GG, mithin durch das Fernmeldegeheimnis, geschützt wird, so ergeben sich zwischen beiden Ländern bezüglich des Schutzes von Verbindungsdaten, die während eines Telekommunikationsvorgangs anfallen, Unterschiede.

20.1.3.1. Fernmeldegeheimnis in Deutschland betroffen

Legt man den engen Fernmeldebegriff, der in der Staatsrechtslehre in Österreich wohl herrschend ist,⁵¹⁹ zugrunde, sind Daten außerhalb des Inhalts der Kommunikation nicht vom Fernmeldegeheimnis umfasst. Ihr Schutz bestimmt sich allein aus Art 8 EMRK, mit der Konsequenz, dass kein Richtervorbehalt besteht.⁵²⁰ Somit ist, wenn von Verkehrsdaten im Rahmen von Überwachung von Mobiltelefonen die Rede ist, zunächst nur davon auszugehen, dass diese lediglich dem Schutzbereich von Art 10 GG unterfallen.

⁵¹⁸ Vgl Bericht Arbeitsgruppe Online-Durchsuchung, 70 ff. Die Autoren erblicken hier einen Eingriff in den Wesensgehalt der betroffenen Grundrechte.

⁵¹⁹ Vgl Wessely, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht?, ÖJZ 1999, 491; Wiederin, in Korinek/Holoubek, Österreichisches Bundesverfassungsrecht Bd. III, Art 10a StGG, Rz 12.

⁵²⁰ Hengstschläger/Leeb, Grundrechte, Rz 15/4.

Jedoch sind auch in Deutschland, wie nachfolgend festzustellen ist, nicht alle denkbaren Überwachungsmaßnahmen vom Fernmeldegeheimnis umfasst. Wie bereits festgestellt, erstreckt sich der Schutzbereich des Fernmeldegeheimnisses auf Kommunikationsvorgänge, also die unkörperliche Übermittlung von Informationen mittels Kommunikationstechnik.⁵²¹ Nicht bei allen Überwachungsmaßnahmen findet Kommunikation statt oder sind Kommunikationsvorgänge betroffen.

Ob und inwiefern Kommunikation vorliegt, liegt keineswegs bei jeder Überwachungsmaßnahme klar auf der Hand und ist zunächst für jede Maßnahme einzeln zu ermitteln. Beim stummen SMS zum Beispiel ist es umstritten, inwiefern dort Kommunikation stattfindet. Dies mag man auf den ersten Blick verneinen. Schließlich geht vom Inhaber des Mobiltelefons keine Kommunikation dergestalt aus, dass dieser mit seinem Gerät aktiv und wissentlich an einem Vorgang zur Kommunikation teilnimmt. Das positive Wissen um einen Kommunikationsvorgang kann aber gerade nicht entscheidend sein.⁵²² Käme es für den Grundrechtsschutz darauf an, ob sich das Individuum bestimmter Tatsachen bewusst ist, bestünde in vielen Fällen kein Schutz. Es kann schließlich für den Grundrechtsschutz nach Art 13 GG auch keine Rolle spielen, ob sich der „Bewohner“ eines Zimmers in einem Krankenhaus bewusst ist, dass auch das von ihm bewohnte Zimmer eine Wohnung im Sinne des Art 13 GG ist.⁵²³ Dies muss erst recht dann gelten, wenn es sich um eine heimliche Maßnahme handelt. Sonst wäre dem Staat die Möglichkeit gegeben, über den Grundrechtsschutz zu disponieren. In Fällen, wo das stumme SMS zum Einsatz kommt, wird ja gerade ein Kommunikationsvorgang in Gang gesetzt, indem vom georteten Handy ein Signal gesendet wird. Damit unterfällt auch die Ortung von Mobiltelefonen mittels stummes SMS dem Fernmeldegeheimnis.

Anders sind IMEI- und IMSI-Catcher zu bewerten.⁵²⁴ Beim Einbuchten in eine simulierte Funkzelle handelt es sich gerade um keinen Kommunikationsvorgang. Anders als beim stummen SMS fallen die Daten nicht im Herrschaftsbereich eines Telekommu-

⁵²¹ Baldus in BeckOK, GG, Art 10, Rz 7.

⁵²² So auch *Nachbaur*, Standortfeststellung und Art 10 GG - Der Kammerbeschluss des BVerfG zum Einsatz des „IMSI-Catchers“, NJW 2007, 335, 336.

⁵²³ Vgl hierzu BGH NStZ 2006, 176.

⁵²⁴ Die Unterschiede zum stummen SMS werden näher beleuchtet von *Smith*, Kurzer Zwischenstand zu Recht und Praxis der „stillen SMS“, VR 2012, 314.

nikationsunternehmens an, sondern bei der simulierten Funkzelle der Ermittler.⁵²⁵ Der Datenaustausch zwischen Mobiltelefon und dem Catcher erfolgt auf dieselbe Weise, wie wenn das Telefon in einer normalen Funkzelle eingebucht ist, nur um seine Betriebsbereitschaft zu signalisieren. Hierfür müssen die Ermittler auch keinen Kommunikationsvorgang in Gang bringen, wie beim stummen SMS.⁵²⁶ Die Interaktion zwischen Mobiltelefon und Catcher findet allein aufgrund technischer Gegebenheiten statt.⁵²⁷ Wiederum anders stellt sich die Situation bei der Funkzellenabfrage dar. Hier liegt ein Eingriff in Art 10 GG vor, da dieser auch die Verbindungsdaten schützt zu denen auch der Aufenthalt in einer bestimmten Funkzelle zählt.⁵²⁸ Weiters als Eingriff in Art 10 GG aufzufassen ist die Zielwahlsuche. Schließlich wird hierbei durch die systematische Analyse der Kommunikationsvorgänge offengelegt, wer mit einer bestimmten Person zu welchem Zeitpunkt kommuniziert hat.⁵²⁹

Auch wenn IMSI- und IMEI-Catcher mangels Relevanz hier außer Betracht bleiben, so ist die Menge der an für das Fernmeldegeheimnis relevanten Daten enorm. Zum einen fällt auf, dass Maßnahmen wie stummes SMS oder Funkzellenabfrage die Ortung einer Person ermöglichen. Ein genaues Bewegungsprofil der Person lässt sich damit leicht erstellen. Zum anderen ist die Funkzellenabfrage, gerade in städtischen Räumen insofern ein Eingriff von besonders hoher Intensität, da in kurzer Zeit eine extrem hohe Zahl von Datensätzen anfällt.⁵³⁰ Viele Datensätze Unbeteiligter werden zudem von der Zielwahlsuche miteinbezogen.

⁵²⁵ BVerfG NJW 2007, 351, 354.

⁵²⁶ A.A. wohl bei *Nachbaur*, Standortfeststellung und Art 10 GG - Der Kammerbeschluss des BVerfG zum Einsatz des „IMSI-Catchers“, NJW 2007, 335f.

⁵²⁷ BVerfG NJW 2007, 351, 354.

⁵²⁸ Vgl hierzu das Fachgutachten des Sächsischen Datenschutzbeauftragten zur rechtlichen Bewertung der Funkzellenabfrage bei einem Polizeieinsatz in Dresden als Bericht an den Sächsischen Landtag (http://www.saechsdsb.de/images/stories/sdb_inhalt/behoerde/oea/bericht-funkzellenabfragen.pdf, 10).

⁵²⁹ *Polenz* in Kilian/Heussen, Computerrechtshandbuch³¹, Kap 13, Rz 9.

⁵³⁰ Vgl hierzu den Abschlussbericht des Berliner Datenschutzbeauftragten zur Praxis der Funkzellenabfrage, http://www.datenschutz-berlin.de/attachments/896/Pr__fbericht.pdf?1346753690.

20.1.3.2. Das Fernmeldegeheimnis in der österreichischen Staatsrechtslehre

Das Fernmeldegeheimnis wird in Deutschland und Österreich unterschiedlich interpretiert und unterscheidet sich hinsichtlich des Richtervorbehalts, den es in geschriebener Form nur in Österreich gibt. Im Rahmen des Verfassungsvergleichs sollen diese Zusammenhänge näher untersucht werden. In den Schutzbereich des Fernmeldegeheimnisses fallen sowohl in Österreich nach Art 10a StGG als auch in Deutschland nach Art 10 GG Inhaltsdaten. Der Inhalt des Fernmeldevorgangs, also das konkrete Gespräch oder der Nachrichteninhalt, ist also stets erfasst. Interessant im Rahmen eines Verfassungsvergleichs sind somit zwei Punkte:

Zum einen ist fraglich, inwiefern die Verkehrsdaten in den Schutzbereich des Fernmeldegeheimnisses fallen sollten oder ob eine solche Ansicht, den Begriff des Fernmeldegeheimnisses überdehnt. Davon unabhängig zu betrachten ist, ob ein Eingriff in das Fernmeldegeheimnis eines richterlichen Befehls bedarf. Beide Fragen werden in beiden Rechtsordnungen kontrovers diskutiert und letztlich unterschiedlich beantwortet. Die Beantwortung dieser zwei Fragen kann indes auch nicht offengelassen werden, da sie grundlegend sind für die Frage, wie Überwachung der Telekommunikation geregelt sein soll.

Legt man den engen Fernmeldebegriff, der in der Staatsrechtslehre in Österreich wohl herrschend ist,⁵³¹ zugrunde, sind Daten außerhalb des Inhalts der Kommunikation nicht vom Fernmeldegeheimnis umfasst. Ihr Schutz bestimmt sich allein aus Art 8 EMRK und § 1 DSG 2000, mit der Konsequenz, dass kein Richtervorbehalt besteht.⁵³² Somit ist, wenn von Verkehrsdaten im Rahmen von Überwachung der Telekommunikation die Rede ist, im Rahmen des Rechtsvergleichs zunächst nur davon auszugehen, dass diese lediglich dem Schutzbereich von Art 10 GG unterfallen.

⁵³¹ Vgl. Wessely, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht?, ÖJZ 1999, 491; Wiederin in Korinek/Holoubek, Österreichisches Bundesverfassungsrecht, Bd. III, Art 10a StGG, Rz 12; zusammenfassend Himberger, Fernmeldegeheimnis und Überwachung, 49 ff.

⁵³² Hengstschläger/Leeb, Grundrechte, Rz 15/4.

20.1.3.3. *Verfassungsvergleichende Aspekte*

Der bereits dargelegte Widerspruch in der Auslegung legt offen, dass ein verfassungsrechtlich gewährleisteter Schutz des Fernmeldegeheimnisses in Österreich und Deutschland begrifflich auf den ersten Blick den gleichen Schutzzumfang verheißt, durch Auslegung in Österreich aber teilweise einen engeren Schutzbereich erhält.

Bei der Antwort auf die Frage, inwiefern beide Rechtsordnungen hierbei etwas voneinander lernen können, ist meines Erachtens auf folgende Thesen im Rahmen des Verfassungsvergleiches einzugehen:

- Das Fernmeldegeheimnis ist ein technikoffenes und modernes Grundrecht. Es ist das Grundrecht, welches dem Schutz der Telekommunikation am sachnächsten ist. Andere Grundrechte sollten höchstens ergänzend hinzutreten.
- Die Überwachung von Verkehrsdaten weist eine hohe Eingriffsintensität auf, da eine Kumulierung vieler Verkehrsdaten eine Offenlegung der privaten Lebensverhältnisse bedeutet.
- Der richterliche Befehl bei Eingriffen in das Fernmeldegeheimnis, wie in Art 10a StGG vorgesehen, stellt eine notwendige Hürde für Ermittlungen dar. Er muss jedoch, um den Gegebenheiten in Ermittlungspraxis Rechnung zu tragen, fortentwickelt werden.

Diese Thesen bedingen sich in gewisser Weise gegenseitig: Hält man Eingriffe in das Fernmeldegeheimnis für besonders gravierend, ist dies ein Argument für den Richtervorbehalt. Dies mag wiederum ein Grund dafür sein, warum man Verkehrsdaten miteinbezogen wissen will.

20.1.3.3.1. Einbeziehung von Verkehrsdaten in das Fernmeldegeheimnis

Diese Trennung ist aus technischer Sicht zunächst kritisch zu sehen. Wer Inhalt und Verkehrsdaten im Rahmen des Fernmeldegeheimnisses trennen will, nimmt eine künstliche Trennung vor. Inhalt der Kommunikation und die dabei entstehenden Verkehrsdaten gehören beim technischen Übertragungsvorgang untrennbar zusammen. Die mangelnde Bedeutung von Verkehrsdaten in der Vergangenheit ist darauf zurückzuführen, dass diese Daten aufgrund der geringeren Zahl an Kommunikationsvorgängen nicht in der Masse anfielen. Durch die Änderungen bedingt durch technische Neuerungen kommt diesen Daten aber eine gesteigerte Bedeutung zu. Je mehr Kommunikation über

Fernkommunikationsmittel abläuft, desto aussagekräftiger ist eine Auswertung aller Verkehrsdaten. Hieran ändert auch die Tatsache nichts, dass den Provider Inhaltsdaten interessieren und er nur, sei es aus technischen Gründen oder zu Abrechnungszwecken, Verkehrsdaten speichert.

Verkehrsdaten weisen oft eine wesentlich höhere Eingriffsintensität auf als der Inhalt der Nachricht selbst. Dies gilt vor allem dann, wenn nicht nur die Kommunikationspartner, sondern auch deren Standorte ermittelt werden können. Dabei macht es insbesondere auch keinen Unterschied, wenn die Kommunikation den Ermittlern rechtmäßig bereits bekannt ist.⁵³³ Tatsache ist, dass ohne den Fernmeldevorgang auch die Verkehrsdaten nicht existieren würden. Schließlich ist der Zusammenhang beider Datenarten, Inhalts- und Verkehrsdaten, eng und die Aussagekraft über den Kommunikationsvorgang ist es ebenso.⁵³⁴ Der Inhalt der Kommunikation reißt gewissermaßen die mindestens ebenso sensiblen Verkehrsdaten mit in seinen Schutzbereich hinein. Daher empfiehlt sich auch keine andere juristische Behandlung dieser Datenarten. Ihre technische Verknüpfung ist so eng und die Eingriffsintensität so ähnlich, dass eine unterschiedliche juristische Betrachtungsweise im Prinzip nur wie ein schlechter Kunstgriff wirkt.

Insofern ist der Verfassungsvergleich zwischen Österreich und Deutschland hilfreich, weil der Schutzbereich des Fernmeldegeheimnisses nach Art 10 GG die Meinung der Strafrechtslehre in Österreich stützt, und das Fernmeldegeheimnis in Art 10a StGG entsprechend weit auslegt. Es gibt keinen Anlass einer entsprechenden Beschränkung.

Auch widerspricht eine solche Interpretation nicht der in Österreich üblichen Art und Weise der Verfassungsinterpretation, welche sehr normfixiert ist.⁵³⁵ Der Wortlaut des Art 10 a StGG schließt Verkehrsdaten weder explizit ein noch nimmt er diese klar vom Schutzbereich der Norm aus. Vielmehr ähnelt der Wortlaut dem von Art 10 GG in

⁵³³ So argumentierte der VfGH, 29. 6. 2012, B 1031/11.

⁵³⁴ Vgl. hierzu *Feiler* in Zankl, Überwachungsstaat, 67, der einen Eingriff in Art 10a StGG in den Fällen bejaht, in denen neben den Inhaltsdaten auch Verkehrsdaten von einem Auskunftsbefehl umfasst sind. Für den Fall, dass Verkehrsdaten ohne Inhaltsdaten abgefragt werden, verneint Feiler, dass der Schutzbereich des Fernmeldegeheimnisses eröffnet ist.

⁵³⁵ *Wiederin* in Lienbacher, Verfassungsinterpretation in Europa, 82 f.

diesem Punkt, so dass dem Verfassungsvergleich der Wortlaut der Norm nicht entgegensteht.

Zwar spielen im Rahmen der Verfassungsinterpretation auch historische Elemente eine große Rolle, jedoch sollte diesen kein zu großer Spielraum eingeräumt werden. Zum einen spricht allgemein dagegen, dass Verfassungsnormen stets für die Dauer ihrer Geltung Sachverhalte regeln; zwar sind sie zu einem früheren Zeitpunkt entstanden, regeln jedoch auch Inhalte, die zu diesem Zeitpunkt undenkbar waren.⁵³⁶ Wieso hätte sich der Gesetzgeber des Jahres 1975 Gedanken über Verkehrsdaten machen sollen, die damals quasi kaum anfielen, als er das Fernmeldegeheimnis ins Staatsgrundgesetz aufnahm? Noch weniger vermag das Argument der Anlehnung an das Briefgeheimnis in Art 10 StGG zu überzeugen, welches am 23. Dezember 1867 in Kraft trat. Insofern widerspricht ein solcher Verfassungsvergleich – grade bei einem Grundrecht, das Bereiche berührt, die einem ständigen technischen Wandel unterworfen sind⁵³⁷ – nicht den Grundsätzen der Verfassungsinterpretation.

20.1.3.3.2. Vorbehalt des richterlichen Befehls für Eingriffe in das Fernmeldegeheimnis?

Auch aus deutscher Sicht kann der Verfassungsvergleich zwischen Art 10a StGG und Art 10 GG jedoch hilfreich sein, denn die Rechtslage in Österreich kann auch für die in Deutschland im Vordringen befindliche Ansicht, Eingriffe in das Fernmeldegeheimnis bedürften eines richterlichen Befehls, als unterstützendes Argument herangezogen werden. Der Richtervorbehalt dient der Wahrung der Interessen der Betroffenen.⁵³⁸ Die Benützung technischer Kommunikationsmittel mag durch unterschiedliche Grundrechte geschützt sein, die Interessenlage ist aber jedes Mal ähnlich zu beurteilen. Somit stellt es sich nicht als sinnvoll dar, im Rahmen der Integrität und Vertraulichkeit infor-

⁵³⁶ Vgl hierzu auch *Wiederin* in Lienbacher, Verfassungsinterpretation in Europa, 88; der sich gegen eine Überinterpretation von historischen Kontexten wendet. Vielmehr plädiert *Wiederin* zu Recht dafür, sich über eine Norm und den Willen ihres Schöpfers nicht mehr Gedanken zu machen als dieser selbst, zumal die meisten Schöpfer von Verfassungsnormen – gerade bei älteren Verfassungen wie der österreichischen – längst verstorben sind.

⁵³⁷ Ein solcher dynamischer und evolutiver Ansatz in der Verfassungsinterpretation erlaubt Verfassungsgerichten, sich an aktuellen gesellschaftlichen Entwicklungen zu orientieren. Entsprechend geht auch der EGMR vor, Vgl hierzu *Mensching*, in Menzel/Pierlings/Hoffmann, Völkerrechtsprechung, 54.

⁵³⁸ *Durner* in Maunz/Dürig, GG, Art 10, Rz 154.

mationstechnischer Systeme einen Richtervorbehalt zu fordern⁵³⁹ und diesen beim Fernmeldegeheimnis dann zu verneinen.

Die richterliche Kontrolle zwingt die Ermittler, ihr Auskunftsbegehren umfassend zu begründen und den Umfang der angeforderten Daten genau zu bezeichnen.⁵⁴⁰ Dies verhindert Ermittlungen in sensiblen Bereichen, die „ins Blaue hinein“ geführt werden und in die viele Unbeteiligte miteinbezogen werden können. Ein umfassender und moderner Grundrechtsschutz gebietet somit einen Schutz des Fernmeldegeheimnisses, der sich sowohl auf Verkehrsdaten erstreckt als auch unter einem Richtervorbehalt steht.⁵⁴¹ Insofern ergibt sich damit letztlich auch im Rahmen des Verfassungsvergleichs eine Wechselwirkung, da sowohl die österreichische als auch die deutsche Rechtsordnung hier voneinander lernen können.

Der Vorbehalt eines richterlichen Befehls für bestimmte Ermittlungsmaßnahmen ist ein wichtiges rechtsstaatliches Mittel der Kontrolle gegenüber Polizeibehörden und Staatsanwaltschaft,⁵⁴² seine Anwendung sieht sich aber stets großer Kritik gegenübergestellt. Diese Kritik sollte man nicht gleich als „nicht rechtsstaatlich“ zurückweisen.

Die geäußerte Kritik sollte zum Anlass genommen werden, den Richtervorbehalt im Rahmen der Telekommunikationsüberwachung fortzuentwickeln. Hierbei soll es keineswegs darum gehen, dass rechtsstaatliche Elemente in Zukunft vermindert werden. Vielmehr sollte man eine Art Systemfrage stellen, die darauf abzielt zu untersuchen, inwiefern eine Kontrollinstanz zwingend bei einem Gericht angesiedelt sein muss.

⁵³⁹ Durner in Maunz/Dürig, GG, Art 10, Rz 59.

⁵⁴⁰ Vgl zu den Begründungserfordernissen ausführlich *Reindl-Krauskopf*, WK-StPO §§ 137, 138, Rz 25 ff.

⁵⁴¹ Dem wird die StPO auch gerecht, indem Sie zwischen Verkehrs- und Inhaltsdaten in § 137 StPO nicht unterscheidet, vgl *Reindl-Krauskopf*, WK-StPO §§ 137, 138 Rz 23.

⁵⁴² Vgl zur Wichtigkeit des Richtervorbehalts als Element der Rechtsstaatlichkeit im Rahmen des sog „großen Lauschangriffs“ nur *Braun*, Der so genannte „Lauschangriff“ im präventivpolizeilichen Bereich, Die Neuregelung in Art 13 IV-VI GG, NvWZ 2000, 375, 376.

20.1.4. Verbindungsdaten außerhalb eines Telekommunikationsvorgangs

Auch bei den Teilnehmern eines Telekommunikationsvorgangs können nach Abschluss desselben in deren Herrschaftsbereich noch Verbindungsdaten vorliegen, auf welche Ermittler zugreifen können. Hierbei kann zwar nicht mehr vom Fernmeldegeheimnis ausgegangen werden, da der Telekommunikationsvorgang bereits abgeschlossen ist. Jedoch hafteten diese Daten dem Fernmeldevorgang an, so dass sein Schutz in gewisser Weise noch auf diese ausstrahlen kann, zumindest in der Form, dass andere Grundrechte an dessen Stelle treten.⁵⁴³ Dies wäre in Österreich vor allem das Grundrecht auf Datenschutz aus § 1 DSG 2000 und in Deutschland das Recht auf informationelle Selbstbestimmung aus Art 2 Abs 1 GG iVm Art 1 Abs 1 GG.

Diese Kategorie von Daten entfaltet am meisten Relevanz, wenn eine Durchsuchung bei einem Verdächtigen stattfindet und dessen Endgeräte von den Ermittlern sichergestellt werden, auf denen sich dann noch Verbindungsdaten befinden, die vom Inhaber der Endgeräte nicht gelöscht wurden. Insofern kann auch eine gewöhnliche Hausdurchsuchung im Rahmen der Telekommunikationsüberwachung entsprechende Relevanz entfalten.

20.2. Zwischenergebnis

Die vorliegenden Ergebnisse lassen zum einen darauf schließen, dass es beim Fernmeldegeheimnis einer modernen und technikoffenen Interpretation bedarf, die zudem die Effektivität des Grundrechtsschutzes beachtet, wie sie etwa vom EGMR im Hinblick auf Art 13 EMRK, aber auch aus den materiellen Grundrechten abgeleitet, verlangt wird. Zumindest bei einer Kumulation von verschiedenen Metadaten einer Person wird man, bei einer zeitgemäßen Auslegung der verfassungsrechtlichen Normen zum Ergebnis kommen müssen, dass das Fernmeldegeheimnis betroffen ist.

Umgekehrt wird man davon ausgehen können, dass ein Eingriff in das Fernmeldegeheimnis einer unabhängigen Kontrollinstanz bedarf. War es früher notwendig direkt in die Wohnung eines Überwachten einzudringen, sei es mit Abhörvorrichtungen

⁵⁴³ Vgl hierzu BVerfG MMR 2006, 217.

oder mittels Durchsuchung, um umfassende Informationen über diesen zu erhalten, so ist es nunmehr möglich, über diesen Informationen ähnlicher Qualität allein durch Eingriff in das Fernmeldegeheimnis zu erhalten.

Dies ist mithin erst Recht vonnöten, wenn sich die Überwachung der Telekommunikation im Umfeld von Berufsgeheimnisträgern abspielt. Hier wird nun näher das Spannungsfeld der Überwachungen von Berufsgeheimnisträgern und dem verfassungsrechtlichen Schutz der Telekommunikation zu beleuchten sein.

20.3. Folgen der verfassungsrechtlichen Folgerung für die Überwachung der Telekommunikation im Bereich der Gefahrenabwehr und der Strafverfolgung

Praktische Auswirkungen auf die strafprozessualen Überwachungsmaßnahmen in Österreich hat diese Erkenntnis nach dem heutigen Stand nicht. Sie kann jedoch dann relevant werden, falls – was aus grundrechtlicher Sicht nicht unbedingt empfohlen werden kann – weitere Überwachungsmethoden, wie etwa die Online-Durchsuchung,⁵⁴⁴ für die bislang keine Rechtsgrundlage existiert, eingeführt werden.

Für Österreich ergeben sich jedoch Auswirkungen im Bereich des SPG. Sammelt die Polizei Metadaten, die während eines Kommunikationsvorgangs anfallen, über einen Verdächtigen, wird zumindest dann von einem Eingriff in das Fernmeldegeheimnis auszugehen sein, wenn es sich nicht um ein einzelnes Datum, sondern um eine Datensammlung handelt. Gerade bei modernen Ermittlungsmethoden wird es in der Regel nicht so sein, dass die Beamten ein einzelnes Datum ermitteln – wie etwa eine Telefonnummer bei der Rufdatenrück Erfassung – sondern eine Vielzahl von Daten vorliegen. Dies würde bedeuten, dass ein Richtervorbehalt im SPG für solche Fälle eingeführt werden muss, wie er in Deutschland in den Polizeigesetzen der Bundesländer existiert. Ausnahmen hierzu wären nur in Extremfällen, etwa bei Gefahr im Verzug zulässig.

⁵⁴⁴ Vgl hierzu unter 28.2.

21. Die Rolle der „Menschenwürde“ in der österreichischen Verfassungsrechtsordnung

Die entwickelten Grundsätze und Erkenntnisse sind nun auf ihre Übertragbarkeit auf Österreich zu überprüfen. Falls eine Übertragbarkeit schließlich in Frage kommt ist darauf einzugehen, inwiefern der Gesetzgeber den herausgearbeiteten verfassungsrechtlichen Vorgaben gerecht werden kann und ob diese vom Gesetzgeber – vielleicht bereits implizit – in Gesetzgebungsvorhaben hinreichend berücksichtigt wurden.

21.1. Übertragbarkeit auf Österreich

Bevor jedoch im Einzelnen geprüft wird, wie die österreichische Gesetzgebung die entwickelten Grundsätze umgesetzt hat und ob es hier legislativen Nachholbedarf gibt, muss man zunächst diskutieren, inwiefern die vom deutschen BVerfG entwickelte Dogmatik, die es hier gedanklich weiterzuentwickeln gilt, überhaupt auf Österreich angewendet werden kann, ob sie angewendet werden sollte oder ob sie eventuell sogar angewendet werden muss.

Während sich Vergleiche einzelner Grundrechte – etwa des Fernmeldegeheimnisses in Art 10a StGG und in Art 10 GG⁵⁴⁵ – ohne weiteres anbieten, stößt die Rechtsvergleichung dort an ihre Grenzen, wo ein entsprechendes Pendant in der jeweils anderen Verfassung fehlt. Noch schwieriger gestaltet sich der Rechtsvergleich bei einer gänzlich anderen Systematik. Diese Frage stellt sich vorliegend beim Begriff der Menschenwürde, die im Grundgesetz in Art 1 Abs 1 GG als wichtigstes Grundrecht allen anderen Grundrechten vorangestellt wird. Zunächst einmal ist festzuhalten, dass Österreich eine dem Grundgesetz ähnliche Systematik in Bezug auf die aufgeworfenen Fragen vollkommen fremd ist. Man kann es insofern als umstritten ansehen, ob die vorliegenden Thesen übertragbar sind. Da die österreichische Verfassungsordnung keinen direkten Menschenwürdeschutz wie in Art 1 GG kennt,⁵⁴⁶ die Menschenwürde demzufolge auch

⁵⁴⁵ Siehe hierzu unter 20.2

⁵⁴⁶ Gleichwohl ist im bürgerlichen Recht, in § 16 ABGB, die Menschenwürde im Kernbereich geschützt (vgl. OGH 13.06.2002, 8ObA288/01p). Ebenfalls Erwähnung findet die Menschenwürde in § 47 Abs 1 S 2 SPG im Fall der Anhaltung (zudem nochmals im zugehörigen § 4 Abs 1 Anhalteordnung).

nicht in verschiedene Sphären einteilt, wie es das BVerfG tut, stellt sich die allgemeine Frage der Übertragbarkeit vergleichbarer Konstellationen aus Deutschland.⁵⁴⁷

Könnte man bereits rechtsdogmatisch eine Übertragbarkeit ablehnen, so müssten die Gedanken des deutschen BVerfG zwar nicht zur Gänze verworfen werden, eine Übertragung in das österreichische Verfassungsrecht wäre jedoch nur erschwert möglich. Es ließen sich allenfalls einzelne Rechtsgedanken in einer anderen verfassungsrechtlichen Ordnung unter einem anderen Normenregime fortdenken.

Zunächst mag man einer direkten Anwendung aus dem Grunde widersprechen, dass die Argumentationslinie des BVerfG, die sich stark auf die Menschenwürde in Art 1 Abs 1 GG stützt, in der Form, aufgrund der verfassungsrechtlichen Unterschiede zumindest keine direkte Anwendung finden kann. Schließlich mag man sich bei einem auf die Menschenwürde so stark ausgerichteten Grundrechtsschutz im österreichischen Verfassungsrecht schwer tun, da weder die EMRK noch die sonstigen im Verfassungsrang stehenden Grundrechte hiermit vergleichbar sind. Freilich wird die Existenz der Menschenwürde von all diesen Normen vorausgesetzt⁵⁴⁸ und allein die Tatsache, dass sich diese nicht in geschriebener Form dort wiederfindet, ist somit letztlich kein Hinweis darauf, dass es einem Grundrechtssubjekt verwehrt bleibt, sich direkt auf diese zu berufen oder einem österreichischen Gericht, ein Judikat hierauf zu stützen, jedoch mag man eine direkte Anwendbarkeit schon aus diesem Umstand kritisch sehen oder gar ablehnen. Wenn man sich für diese Argumentationslinie entscheidet, könnte dann untersucht werden, ob nicht andere Grundrechte einen Berufsgeheimnisträgerschutz im Rahmen von Ermittlungen gebieten, der einem direkten Schutz durch die Menschenwürde nahe kommt.

21.1.1. Grundrechtecharta und europarechtliches Äquivalenzprinzip

Zunächst ist jedoch zu klären, welchen Rang die GRC der EU in Österreich genießt, da in dieser, im Gegensatz zu den Normen des österreichischen Verfassungs-

⁵⁴⁷ Vgl. *Höhne* in Berka/Grabenwarter/Holoubek, Persönlichkeitsschutz in elektronischen Massenmedien, 38.

⁵⁴⁸ Auch der EuGH bezog sich – wenn auch erst in den letzten Jahren – verstärkt auf die Menschenwürde direkt; vgl. EuGH Slg 2001, I-7149, 7168 Rz 70 = EuZW 2001, 691, 695 = NJW 2002, 2455.

rechts, der Schutz der Menschenwürde direkt verankert ist. Dies könnte grundrechtliche Argumentationen, die sich (zum Teil) auf die Menschenwürde beziehen, aus österreichischer Sicht in einem neuen Licht erscheinen lassen.

Eine Ablehnung der Anwendbarkeit des Begriffs der Menschenwürde als eigenes Grundrecht im österreichischen Verfassungsrecht scheint nach einer Entscheidung des VfGH überholt zu sein. Der VfGH anerkennt mittlerweile, unter bestimmten Voraussetzungen, dass die Regelungen der GRC der Europäischen Union auch als Normen des Verfassungsrechts anzusehen sind,⁵⁴⁹ auf die sich ein Antragsteller im Verfahren vor dem VfGH auch direkt berufen kann. Damit die in der GRC enthaltenen Verbürgungen herangezogen werden können, müssen zwei Voraussetzungen erfüllt sein. Zum einen muss es sich um echte Grundrechte handeln und nicht nur um bloße Grundsätze.⁵⁵⁰ Dies ist nur eine formale Klarstellung des Gerichts. Selbstverständlich können nur tatsächliche Grundrechte geprüft werden und nicht bloße Grundsätze. Diese Voraussetzung erfüllt die Menschenwürde ohne weiteres, da es sich nicht um einen bloßen Programmsatz handelt, sondern um ein Grundrecht. Diskussionswürdig ist freilich, inwiefern das Grundrecht als verfassungsmäßig gewährleistetes Recht im Sinne von Art 144 B-VG anzusehen ist, da es im österreichischen Verfassungsrecht hierfür kein Pendant oder vergleichbares Grundrecht gibt. Entscheidend ist aber laut VfGH, ob das Grundrecht der Charta in „Formulierung und Bestimmtheit verfassungsgesetzlich gewährleisteten Rechten der österreichischen Bundesverfassung gleicht“. Hiervon wird man ausgehen dürfen, da Art 1 GRC sich nicht signifikant von österreichischen Grundrechten unterscheidet.⁵⁵¹

Was den Prüfungskatalog bei verfassungsgerichtlichen Verfahren angeht, ändert das Gericht diesen nicht pauschal durch seine Entscheidung ab, sondern bleibt beim bisherigen Verfahren, in dem Normen des Europarechts keinen tauglichen Prüfungs-

⁵⁴⁹ VfGH 14.03.2012 U 466/11.

⁵⁵⁰ Hierzu zählt der VfGH etwa Art 22 GRC (Vielfalt der Kulturen, Religionen und Sprachen); vgl VfGH 14.03.2012 U 466/11.

⁵⁵¹ So auch *Fuchs/Segalla* in Holoubek/Lienbacher, GRC, Art 1, Rz 40.

maßstab darstellen. Hierzu hielt der VfGH im bezeichneten Verfahren zusammenfassend zunächst nachfolgendes fest⁵⁵²:

Die auf dem Gipfel von Nizza im Jahr 2000 proklamierte Grundrechte-Charta ist Teil des Vertrags von Lissabon, der von Österreich am 13. Mai 2008 ratifiziert wurde. Seit dem Inkrafttreten des Vertrags von Lissabon am 1. Dezember 2009 [...] ist die Grundrechte-Charta auf Grund ausdrücklicher Anordnung des Art 6 Abs 1 EUV mit den Verträgen rechtlich gleichrangig und daher Teil des Primärrechts der Europäischen Union.

Hierbei alteriert der VfGH nicht die Tatsache, dass Unionsrecht kein tauglicher Prüfungsmaßstab in einem Verfahren vor dem VfGH ist. Ein Verfahren kann demgemäß nicht etwa allein auf EUV oder AEUV oder auf eine EU-Richtlinie gestützt werden, nur weil es sich dabei im Vergleich zu nationalen Rechtsvorschriften um höherrangiges Recht handelt.⁵⁵³

Es ist und bleibt damit grundsätzlich allein Sache des EuGH, österreichische Gesetze auf ihre Europarechtskonformität zu überprüfen. Hieran kann der VfGH auch denklogisch nichts ändern, da diese Kompetenzordnung selbst im europäischen Recht festgeschrieben ist,⁵⁵⁴ die Zuständigkeiten des VfGH hingegen ergeben sich allein aus Art 137 ff B-VG.

Allerdings hat der VfGH auch den unionsrechtlichen Äquivalenzgrundsatz zu beachten. Dieser soll verhindern, dass sich innerstaatliche Gerichte aus der Rechtsprechung zu europäischen Normen quasi zurückziehen. Es muss für einen Rechtsschutzsuchenden auch grundsätzlich möglich sein, sich auf Normen des Unionsrechts zu berufen.⁵⁵⁵ Dies führt letztlich dazu, dass nationale Gerichte passende oder naheliegende

⁵⁵² VfGH 14.03.2012 U 466/11, Rz 18.

⁵⁵³ VfGH 14.03.2012 U 466/11, Rz 22.

⁵⁵⁴ Der VfGH bezieht sich hierbei auch auf die Judikate VfSlg. 15.753/2000, 15.810/2000. Vgl auch *Vcelouch*, Auswirkungen der österreichischen Unionsmitgliedschaft auf den Rechtsschutz vor dem VwGH und dem VfGH, ÖJZ 1997, 721, 724.

⁵⁵⁵ Der VfGH bezieht sich hierbei auf die die Rechtssache *Levez*, EuGH 1.12.1998, Rs. C-326/96, die wiederum die vorangegangenen Entscheidungen zitiert. Vgl VfSlg 15.753/2000, 15.810/2000, Rz 19.

innerstaatliche Normen anwenden und im Sinne des Unionsrechts zu Anwendung bringen, wenn diese ein unionsrechtliches Mindestmaß unterschreiten.⁵⁵⁶

Dieser Grundsatz macht auch vor dem Verfassungsrecht nicht Halt. So können verfassungsrechtliche Normen letztlich nicht hinter der GRC zurückbleiben. Daraus folgt der VfGH:⁵⁵⁷

Nach der österreichischen Bundesverfassung ist gemäß Art 144 B-VG der Verfassungsgerichtshof berufen, letztinstanzliche Bescheide von Verwaltungsbehörden daraufhin zu überprüfen, ob durch sie verfassungsgesetzlich gewährleistete Rechte verletzt werden; Art 144a B-VG enthält die entsprechende Kompetenz für den Bereich des Asylverfahrens. Gemäß Art 133 Z 1 B-VG sind Beschwerdesachen, in denen eine Verletzung von verfassungsgesetzlich gewährleisteten Rechten behauptet wird, von der Zuständigkeit des Verfassungsgerichtshofs ausgeschlossen. Das Rechtsschutzsystem des B-VG beruht darauf, dass die Geltendmachung der Verletzung verfassungsgesetzlich gewährleisteter Rechte im Allgemeinen bei einer Instanz, nämlich dem Verfassungsgerichtshof, konzentriert werden soll, [...]. Dies kann den Grundrechtsschutz also auch über bislang bekannte Maßstäbe hinaus erweitern. Insofern kann auch die Menschenwürde direkt herangezogen werden, wenn diese in der Charta entsprechend verankert ist. [...]

Der Verfassungsgerichtshof kommt daher zum Ergebnis, dass auf Grund der innerstaatlichen Rechtslage der Äquivalenzgrundsatz zur Folge hat, dass auch die von der Grundrechte-Charta garantierten Rechte vor dem Verfassungsgerichtshof als verfassungsgesetzlich gewährleistete Rechte gemäß Art 144 bzw. Art 144a B-VG geltend gemacht werden können und sie im Anwendungsbereich der Grundrechte-Charta einen Prüfungsmaßstab in Verfahren der generellen Normenkontrolle, insbesondere nach Art 139 und Art 140 B-VG bilden. Dies gilt jedenfalls dann, wenn die betreffende Garantie der Grundrechte-Charta in ihrer Formulierung und Bestimmtheit verfassungsgesetzlich gewährleisteten Rechten der österreichischen Bundesverfassung gleicht.

⁵⁵⁶ Vgl hierzu etwa OVG Berlin-Brandenburg, BeckRS 2015, 47831, Rz 16; VG Düsseldorf, BeckRS 2014, 51325; VwGH 2015/04/0002, Rz 37.

⁵⁵⁷ VfGH 14.03.2012 U 466/11, Rz 33 und 35.

Wer sich an den VfGH wendet, kann sich folglich auch direkt und wohl auch ausschließlich auf die GRC berufen, solange er sich auf Grundrechte beruft. Dieser entscheidet ohne Vorabentscheidungsverfahren, es sei denn es ist eine Auslegungsfrage auf europäischer Ebene zu klären.⁵⁵⁸ Selbstverständlich ist diese Entscheidung des VfGH nicht ohne Widerspruch geblieben. Der EuGH hat sich in dieser Sache jedenfalls noch nicht ablehnend geäußert.⁵⁵⁹

Die Entscheidung führt zu einer direkten Anwendung der GRC im österreichischen Verfassungsrecht und damit zu einer Erweiterung des Grundrechtekatalogs. Dies wird bei vielen Grundrechten aus der Charta keine allzu große praktische Relevanz haben, da diese in irgendeiner Form bereits Teil des österreichischen Verfassungsrechts sind. Das ist nicht zuletzt darauf zurückzuführen, dass die EMRK für viele Grundrechte der Charta Pate gestanden ist, was sich daran erkennen lässt, dass diese oft nahezu wortgleich sind und zudem auch in der Charta festgeschrieben ist, dass diese im Sinne der Charta zu interpretieren sind (Art 52 Abs 3 GRC und Art 54 GRC). Eine verfassungsrechtliche Erweiterung der Grundrechte kann also nur dort stattfinden, wo die Charta ein Mehr an Grundrechten bietet, sich also aus österreichischer Sicht auf grundrechtlichem Neuland bewegt.

21.1.2. Einschränkung des Grundrechtsschutzes durch Art 51 GRC

Nun zu verkünden, die Charta sei damit was ihren Grundrechtegehalt angeht, für jeden erdenklichen Sachverhalt vom VfGH in den Verfassungsrang gehoben worden, greift zu kurz. Hiermit würde der VfGH auch seine Kompetenzen überschreiten, da genau dies von der GRC selbst nicht vorgesehen ist. Inwiefern die Charta überhaupt anwendbar ist, wird durch Art 51 GRC bestimmt. Der VfGH lässt die Einschränkung des Art 51 GRC nicht unerwähnt, auch wenn er sich nicht sonderlich ausführlich hierzu äußert, was aber – zumindest nach Ansicht des VfGH – auch dem Fall geschuldet ist.

⁵⁵⁸ VfGH 14.03.2012 U 466/11, Rz 43. Ebenfalls scheidet eine Vorlagepflicht aus, wenn es auf die Norm letztlich nicht ankommt.

⁵⁵⁹ Vgl hierzu die Ausführungen von *Muzak*, Wer darf die GRC prüfen: EuGH oder VfGH?, *ecolex* 2014, 1113.

21.1.2.1. Art 51 GRC und seine Interpretation durch den VfGH

Die Vorschrift des Art 51 Abs 1 GRC legt zunächst den Geltungsbereich der Grundrechtecharta fest. Diese bindet nicht etwa alle Mitgliedsstaaten als eine Art Unionsverfassungsrecht, sondern zunächst nur die Europäische Union und ihre Organe selbst. Gleichwohl sind alle Mitgliedsstaaten zur chartakonformen Umsetzung von Unionsrecht verpflichtet. Weiters ist in Art 51 Abs 2 GRC festgelegt, dass die Charta den Geltungsbereich nicht ausdehnt. Rein vom Wortlaut her lassen die Vorschriften auf eine eher restriktive Auslegung bezüglich des Anwendungsbereiches der Charta schließen. Die GRC wäre damit für die meisten Sachverhalte eher nicht anwendbar, erst recht dann nicht, wenn es sich um österreichische Gesetze oder Handlungen österreichischer Behörden oder weiterer staatlicher Einrichtungen auf Grundlage dieser Gesetze handelt. Diese Ansicht greift aber zu kurz. Der VfGH führt in seiner vorliegenden Entscheidung zum Anwendungsbereich der Charta wie folgt aus:⁵⁶⁰

Die Anwendbarkeit der Grundrechte-Charta auf Akte der Organe der Mitgliedstaaten setzt freilich voraus, dass diese in "Durchführung des Rechts der Europäischen Union" handeln (Art 51 Abs 1 GRC), also die Beschwerdesache, in der ein Recht der Grundrechte-Charta geltend gemacht wird, in den Anwendungsbereich des Unionsrechts fällt [...]. Dieser ist nach der Rechtsprechung des Gerichtshofs der Europäischen Union weit zu verstehen. In den Anwendungsbereich fällt neben der Vollziehung unmittelbar wirksamen Unionsrechts durch Gerichte oder Verwaltungsbehörden der Mitgliedstaaten [...] auch die Vollziehung von mitgliedstaatlichen Umsetzungsvorschriften [...].

Damit ist zunächst festzuhalten, dass die Charta der Grundrechte zunächst in jedem Fall für Gesetze gilt, die auf Grundlage von EU-Richtlinien erlassen wurden.⁵⁶¹ Hier bestehen zwar nationale Gesetze, aber im Prinzip vollziehen die Mitgliedsstaaten hier Europarecht, welches sie in ihre Rechtsordnung zu überführen haben. Damit fallen im Bereich der Überwachung etwa jüngste Vorhaben wie die frühere Vorratsdatenspeicherungs-Richtlinie in jedem Fall in den Bereich, in dem die Charta der Grundrechte

⁵⁶⁰ VfGH 14.03.2012 U 466/11, Rz 47.

⁵⁶¹ Denklogisch gilt dies auch für die Anwendung und vor allem die Auslegung von EU-Verordnungen.

voll zur Anwendung kommt. Der dem VfGH vorliegende Fall stammt aus dem Bereich des Asylrechts, welches eine Regulierung durch europäische Richtlinien erfährt und daher in jedem Fall dem Schutzbereich der Charta unterfällt, zumal der EuGH auch dieser Ansicht ist.⁵⁶² Zu weiteren Möglichkeiten in denen die Charta anwendbar ist, äußert sich der Gerichtshof mangels Relevanz für das vorliegende Verfahren nicht.

21.1.2.2. Weitere Anwendungsbereiche von Art 51 Abs 1 GRC im Bereich der Grundfreiheiten der Europäischen Union

Der EuGH hat sich bereits mehrfach mit Art 51 Abs 1 GRC auseinandergesetzt.⁵⁶³ Aus seiner Rechtsprechung ist zu entnehmen, dass der Anwendungsbereich der Charta, wenn er auch noch nicht vollständig und grundlegend vom Gericht aufgezeigt wurde, für „weitere Anwendungsbereiche“ offen ist.⁵⁶⁴ Ein im vorliegenden Fall eher nicht, aber ansonsten sehr praxisrelevanter Fall, wäre etwa die Beschränkung von Grundfreiheiten, bei denen eine Berufung auf die GRC ebenfalls möglich sein soll.⁵⁶⁵

21.1.2.3. Weitere Anwendungsbereiche von Art 51 Abs 1 GRC von der „Fransson“-Entscheidung des EuGH zur „neuen Formel“

Für Aufsehen hat der EuGH durch die Rechtssache „Fransson“ gesorgt, da dort der Anwendungsbereich der Charta massiv erweitert wurde.⁵⁶⁶ In dem Fall wurde ein schwedischer Fischer der Steuerhinterziehung angeklagt. Für die ihm zur Last gelegte Hinterziehung von Umsatzsteuern hatte er bereits eine Verwaltungsstrafe bezahlt, die zum Zeitpunkt der strafrichterlichen Verhandlung bereits in Rechtskraft erwachsen war. Das Strafgericht legte dem EuGH den Sachverhalt vor, damit dieser beurteile, ob der Sachverhalt gegen den Grundsatz „ne bis in idem“ verstößt, welcher sich in der Charta der Grundrechte in Art 50 GRC findet und die Verurteilung in einem Strafverfahren innerhalb der Europäischen Union für den Fall verbietet, indem der Angeklagte wegen

⁵⁶² VfGH 14.03.2012 U 466/11, Rz 48 mwN.

⁵⁶³ Auch bei den Verhandlungen im Konvent wurde um die endgültige Regelung hart gerungen; vgl *Borowski* in Meyer, Europäische GRC⁴, Art 51, Rz 2 ff.

⁵⁶⁴ *Danda*, Die Anwendung der Charta der Grundrechte der Europäischen Union im österreichischen Grundrechtsschutz, *migralex* 2013, 14

⁵⁶⁵ *Danda*, Die Anwendung der Charta der Grundrechte der Europäischen Union im österreichischen Grundrechtsschutz, *migralex* 2013, 14 mit Verweis auf die Rspr des EuGH.

⁵⁶⁶ EuGH C-617/10 – *Fransson*; vgl hierzu auch ausführlich *Tamblé*, Der Anwendungsbereich der GRC, 23.

dieser Sache bereits verurteilt wurde. Auf den ersten Blick betrachtet wird man hier die Entscheidungskompetenz des EuGH ablehnen müssen, da die Charta der Grundrechte dem Wortlaut von Art 51 Abs 1 GRC nach nicht anwendbar ist.

Es handeln weder Organe der Union, noch geht die Bestrafung des Angeklagten unmittelbar auf eine EU-Richtlinie zurück. Sowohl im Bereich des Strafrechts als auch bei der Erhebung nationaler Abgaben sind die Mitgliedsstaaten, solange nicht der Wettbewerb innerhalb der Union verzerrt oder behindert wird, der Union keine Rechenschaft schuldig. Zwar haben sich die Mitgliedsstaaten der Union verpflichtet, gewisse Harmonisierungen im Umsatzsteuerrecht einzuführen, welche sich jedoch nur darauf beziehen, dass bestimmte Umsätze in der Union der Umsatzsteuer unterliegen und andere nicht.⁵⁶⁷ Hiermit wollte die Union augenscheinlich bezwecken, dass eine unterschiedliche Gesetzgebung der Mitgliedsstaaten bei der Umsatzsteuer den Wettbewerb innerhalb der Europäischen Union beschränkt. Es handelt sich damit eindeutig um eine Richtlinie, die auf den gemeinsamen Wirtschaftsraum bezogen ist.

21.1.2.3.1. Anwendbarkeit der GRC bei auch nur indirektem Bezug

Der EuGH hat aber überraschenderweise die RL 2006/12/EG und Art 325 AEUV zum Anlass genommen, die Vorlage zu entscheiden. Die Begründung vermag auf den ersten Blick weit hergeholt erscheinen, lässt aber einen umfassenden Einblick dahingehend zu, wie der EuGH den Anwendungsbereich der Charta versteht. So führt der Gerichtshof aus:⁵⁶⁸

In Bezug auf die Mehrwertsteuer geht zum einen aus den Art 2, 250 Abs 1 und 273 der Richtlinie 2006/12/EG des Rates vom 28. November 2006 über das gemeinsame Mehrwertsteuersystem (ABl. L 347, S. 1), die den Wortlaut der Art 2 und 22 Abs 4 und 8 der Richtlinie 77/388 in der Fassung des Art 28h dieser Richtlinie übernommen haben, und zum anderen aus Art 4 Abs 3 EUV hervor, dass jeder Mitgliedstaat verpflichtet ist, alle Rechts- und Verwaltungsvorschriften zu erlassen, die geeignet sind, die Erhebung der gesamten in seinem Hoheitsgebiet geschuldeten Mehrwertsteuer zu gewährleisten und den Betrug zu bekämpfen [...].

⁵⁶⁷ Richtlinie 2006/12/EG des Rates vom 28. 11.2006 über das gemeinsame Mehrwertsteuersystem.

⁵⁶⁸ EuGH C-617/10 = HRRS 2013 Nr. 335, Rz 50.

Außerdem sieht der EuGH in Art 325 AEUV einen Grund für seine Zuständigkeit. In diesem verpflichten sich die Mitgliedsstaaten abstrakt „Betrügereien“ zu bekämpfen, welche gegen die finanziellen Interessen der Union gerichtet sind. Während der Wortlaut eher darauf schließen lässt, dass hierbei direkte EU-Mittel, wie etwa EU-Subventionen, gemeint sind, zieht der Gerichtshof den Kreis wesentlich weiter. Hierzu führt er konkret aus:⁵⁶⁹

Außerdem sind die Mitgliedstaaten nach Art 325 AEUV verpflichtet, zur Bekämpfung von rechtswidrigen Handlungen, die sich gegen die finanziellen Interessen der Union richten, abschreckende und wirksame Maßnahmen zu ergreifen, insbesondere müssen sie zur Bekämpfung von Betrug, der sich gegen die finanziellen Interessen der Union richtet, dieselben Maßnahmen ergreifen wie zur Bekämpfung von Betrug, der sich gegen ihre eigenen finanziellen Interessen richtet [...]. Da die Eigenmittel der Union gemäß dem Wortlaut von Art 2 Abs 1 des Beschlusses 2007/436/EG, Euratom des Rates vom 7. Juni 2007 über das System der Eigenmittel der Europäischen Gemeinschaften (ABl. L 163, S. 17) u. a. die Einnahmen umfassen, die sich aus der Anwendung eines einheitlichen Satzes auf die nach den Unionsvorschriften bestimmte einheitliche Mehrwertsteuer-Eigenmittelbemessungsgrundlage ergeben, besteht ein unmittelbarer Zusammenhang zwischen der Erhebung der Mehrwertsteuereinnahmen unter Beachtung des einschlägigen Unionsrechts und der Zurverfügungstellung entsprechender Mehrwertsteuermittel für den Haushalt der Union, da jedes Versäumnis bei der Erhebung Ersterer potenziell zu einer Verringerung Letzterer führt [...].

Aus Sicht des EuGH reicht also ein extrem weiter Bezug zur Union und ihren Rechtsakten aus, um zur Anwendbarkeit der GRC zu kommen. Ein Bezug ist mithin bei einem nur indirekten Bezug zu europäischen Richtlinien oder in den Verträgen festgelegten Zielen der Union gegeben. Dies führt selbstredend dazu, dass der Anwendungsbereich der Charta massiv erweitert wird und durch die Interpretation des EuGH über den eigentlichen Wortlaut hinaus reicht. In Anbetracht der Tatsache, dass das gesamte Recht von europäischen Einflüssen durchdrungen ist, dürfte es schwer fallen, einzelne

⁵⁶⁹ EuGH C-617/10 = HRRS 2013 Nr. 335, Rz 51.

Rechtsbereiche mit Sicherheit vom Anwendungsbereich der GRC auszunehmen, so dass diese im Zweifel dann anzuwenden wäre.⁵⁷⁰

Schon bei seiner Entscheidung, in der der EuGH die Vorratsdatenspeicherung auf die Binnenmarktkompetenz der EU stützte,⁵⁷¹ ließ das Gericht erkennen, dass es Kompetenzen der Union sehr weit zu interpretieren vermag. Insofern ist die Rechtsprechung des EuGH, bei aller Kritik die diese Rechtsprechung insbesondere im Rahmen der Vorratsdatenspeicherung erfahren hat,⁵⁷² in sich nur konsequent. Bringt nämlich diese weite Interpretation nunmehr auch einen stärkeren Grundrechtsschutz mit sich. Insofern ist nun zur weiten kompetenziellen Auslegung eine entsprechende grundrechtliche Flankierung hinzugetreten.

Dem ist nicht zuletzt das deutsche BVerfG entgegengetreten, da es von einer sehr engen Auslegung des Unionsrechts in Verfassungsfragen ausging.⁵⁷³ Letztlich veranlasste dies den EuGH dazu eine „neue Formel“ zu entwickeln, in der dieser folgendes festhielt:⁵⁷⁴

Um festzustellen, ob eine nationale Regelung die Durchführung des Rechts der Union im Sinne von Art 51 der Charta betrifft, ist u. a. zu prüfen, ob mit ihr eine Durchführung einer Bestimmung des Unionsrechts bezweckt wird, welchen Charakter diese Regelung hat und ob mit ihr nicht andere als die unter das Unionsrecht fallenden Ziele verfolgt werden, selbst wenn sie das Unionsrecht mittelbar beeinflussen kann, sowie ferner, ob es eine Regelung des Unionsrechts gibt, die für diesen Bereich spezifisch ist oder ihn beeinflussen kann.

Der EuGH prüft somit, inwiefern eine mitgliedstaatliche Regelung mit dem Unionsrecht in Verbindung steht; etwa dergestalt, dass die zu regelnde Materie unionsrecht-

⁵⁷⁰ So im Ergebnis auch *Wegner*, Die "Fransson"-Entscheidung des EuGH - Eine Erschütterung im System der europäischen Grundrechte?, Anmerkung zum Urteil des Europäischen Gerichtshofs vom 26. Februar 2013 (EuGH C-617/10 - Fransson), HRRS 2013, 126

⁵⁷¹ EuGH v. 10.02.2009 – C-301/06.

⁵⁷² *Simitis*, Der EuGH und die Vorratsdatenspeicherung oder die verfehlte Kehrtwende bei der Kompetenzregelung, NJW 2009, 1782.

⁵⁷³ BVerfG v. 24.4.2013, 1 BvR 1215/07, Rz 88f; näher hierzu *Holoubek/Lechner/Oswald* in *Holoubek/Lienbacher*, GRC, Art 51, Rz 27.

⁵⁷⁴ EuGH v. 6.03.2014 - C-206/13.

lichen Beschränkungen unterliegt oder das Unionsrecht eine gewisse Regelungsdichte für den vorliegenden Sachverhalt aufweist.⁵⁷⁵

21.1.2.3.2. Anwendbarkeit der GRC bei Telekommunikationsüberwachung

Somit ist es erforderlich, um eine sinnvolle Anwendung der Rechtsprechung des EuGH zu prüfen, ob es Anzeichen gibt, dass sich die Inhalts- und Verkehrsdatenüberwachung der Telekommunikation in irgendeiner Weise dem EU-Recht zuordnen lässt. Hierfür gibt es, wenn man die Argumentation des EuGH gedanklich fortentwickelt mehrere Anhaltspunkte. Hierfür kann die Entscheidung des EuGH über die Einordnung der Vorratsdatenspeicherung⁵⁷⁶ herangezogen werden, wo der Gerichtshof, obwohl sich die Richtlinie klar auf die Speicherung von Verbindungsdaten zum Zwecke der Weitergabe an Ermittler im Verdachtsfall bezog, diese auf die Binnenmarktkompetenz gestützt hat, da diese Richtlinie nur Tätigkeiten regelt, „die unabhängig von der Durchführung jeder eventuellen Maßnahme polizeilicher oder justizieller Zusammenarbeit in Strafsachen sind“; damit harmonisiere die Richtlinie zur Vorratsdatenspeicherung „weder die Frage des Zugangs zu den Daten durch die zuständigen nationalen Strafverfolgungsbehörden noch die Frage der Verwendung und des Austauschs dieser Daten zwischen diesen Behörden“.⁵⁷⁷

Somit wird man, wenn dieser Gedankengang konsequent weiterverfolgt wird, zu dem Ergebnis kommen, dass Gesetzgebungsmaßnahmen – auch solche, die nicht direkt Umsetzung einer EU-Richtlinie, sind – welche Telekommunikationsüberwachung betreffen, grundsätzlich Binnenmarktrelevanz haben können. Schließlich sind von diesen Maßnahmen alle Anbieter betroffen – auch solche aus dem EU-Ausland – die in Österreich eine Niederlassung betreiben. Selbst wenn man diese Ansicht für verfehlt halten würde, da man diese Argumentationskette entgegenhalten mag, dass diese aufgrund der mangelnden Kausalität zwischen Gesetzgebung im Bereich der Überwachung der Telekommunikation und dem Binnenmarkt, ohne dass hierbei direkt eine Richtlinie im Spiel ist, zu weit hergeholt ist, so mag man sich nur schwer dem Argument verschließen, dass die EU-Verträge auch auf die gemeinsame Arbeit im Bereich

⁵⁷⁵ *Holoubek/Lechner/Oswald* in *Holoubek/Lienbacher*, GRC, Art 51, Rz 31.

⁵⁷⁶ EuGH v 10.02.2009 – C-301/06, Rz 61.

⁵⁷⁷ EuGH v 10.02.2009 – C-301/06, Rz 83.

von Polizei und Justiz ausgerichtet sind. Spätestens hier wird man sich einer Geltung der GRC nicht mehr verschließen können. So regelt etwa Titel V des AEUV den „Der Raum der Freiheit, der Sicherheit und des Rechts“. Hierbei vereinbaren die Mitgliedsstaaten der Union eine enge Kooperation bei Polizei und Justiz.

Werden neue Gesetze erlassen, die Überwachung ermöglichen, bezieht man sich in den Erläuterungen stets auf globale Gefahren, wie etwa den internationalen Terrorismus oder die organisierte Kriminalität, die es abzuwehren gelte.⁵⁷⁸

Die Abwehr gegen solche globalen Bedrohungen wird kaum in einem nationalen Alleingang Österreichs erfolgen können, zumal nationale Grenzen für diese Arten der Bedrohung kein wirksames Hindernis darstellen. Eine nachhaltige Kriminalitätsbekämpfung lässt sich, wenn überhaupt, nur in einer Zusammenarbeit der europäischen Staaten in diesem Bereich realisieren. In Österreich ermittelte Daten aus einer Telekommunikationsüberwachung verbleiben damit nicht unbedingt im Machtbereich einheimischer Behörden, sondern werden mit nicht geringer Wahrscheinlichkeit auch mit Ermittlungsbehörden aus anderen EU-Staaten geteilt oder etwa über die internationale Polizeibehörde EUROPOL ausgetauscht,⁵⁷⁹ ebenso wie umgekehrt Österreich Informationen aus anderen Mitgliedsstaaten der EU erhält.

Darüber hinaus hat die Union diverse Rechtsakte erlassen, um Terrorismus und internationale Kriminalität zu bekämpfen. Hierbei fördert sie etwa Projekte im Rahmen der Kriminalprävention und Kriminalitätsbekämpfung und des Krisenmanagements finanziell⁵⁸⁰ oder erlässt Strategien zur gemeinsamen Terrorismusbekämpfung.⁵⁸¹ Hiermit nimmt sich die Union intensiv eines Themas an, das die Arbeit von Polizei und Justiz in allen Mitgliedsstaaten beeinflusst.

⁵⁷⁸ Diese Argumentation findet sich etwa auch im Gesetzesentwurf zum neuen PStSG; vgl hierzu unter 28.1.1.

⁵⁷⁹ Vgl hierzu den Beschluss des Rates 2009/371/JI zur Errichtung des Europäischen Polizeiamtes EUROPOL. Vgl auch *Lachmayer*, Transnationales Polizeihandeln – Demokratische und rechtsstaatliche Herausforderungen der europäischen Polizeikooperation, JBl. 409, 410 ff.

⁵⁸⁰ Verordnung (EU) Nr. 513/2014.

⁵⁸¹ Vgl hierzu die übersichtsartige Aufstellung unter <http://register.consilium.europa.eu/doc/srv?l=DE&f=ST%2011778%202008%20REV%201>.

21.1.2.4. Grundsätzliche Anwendbarkeit der GRC im Bereich der Überwachung der Telekommunikation

Folglich ist ein Konnex zum Recht der Union nach der Rechtsprechung des EuGH gegeben. Im Bereich der präventiven und repressiven Überwachung der Telekommunikation kann somit angenommen werden, dass sich Betroffene damit auch auf die GRC berufen können. Hier und in vielen anderen Bereich der Gesetzgebung, stehen den Bürgern Europas in den Mitgliedsstaaten jetzt mehr Grundrechte – nämlich jene der Charta – zur Durchsetzung ihrer Rechte zu. Ihre Anwendung wird eine Herausforderung für die nationalen Verfassungsgerichte.

Hierbei ist es durchaus positiv hervorzuheben, dass der VfGH sich in der Lage sieht, neben den bekannten Grundrechten des österreichischen Verfassungsrechts auch solche der Charta anzuwenden, es damit zu einer parallelen Anwendung kommt. Dem steht auch keine Rechtsprechung auf europäischer Ebene entgegen. Der EuGH hält sogar ausdrücklich fest, dass eine parallele Anwendung von GRC und nationalen Grundrechten möglich und auch durchaus erwünscht ist.⁵⁸² Beide Grundrechtssphären, die europäische und die nationale, haben damit eine Berechtigung in der Rechtsprechung der nationalen Verfassungsgerichte berücksichtigt zu werden. Freilich wird dies in der Rechtsprechung einzelner Verfassungsgerichte auf Ebene der Mitgliedsstaaten nicht als unproblematisch gesehen. Gerade in Deutschland etwa möchte das BVerfG beide Sphären des Verfassungsrechts strikt trennen.⁵⁸³

Diese Entwicklung ist auch aus grundrechtlicher Sicht insofern zu begrüßen, als den Menschen in der EU ein grundrechtlicher Ausgleich zu den zahlreichen Gesetzgebungstätigkeiten der Union im Bereich der Kriminalprävention und der Verfolgung von Straftaten an die Hand gegeben wird. Dies hebt den Grundrechtsschutz in den Staaten der EU auf ein einheitliches Niveau und beeinflusst in diesem Fall auch die Bewertung und Bedeutung des Menschenwürdebegriffs im Rahmen des österreichischen Verfassungsrechts, da dieser in Art 1 GRC enthalten ist.

⁵⁸² EuGH Rs.C-399/11 = NJW 2013, 1215.

⁵⁸³ *Tamblé*, Der Anwendungsbereich der GRC, 28.

21.1.3. Neue Bewertung des Begriffs der Menschenwürde im österreichischen Verfassungsrecht

Die Regelung des Art 1 GRC beinhaltet einen fast wortgleichen Menschenrechtsschutz wie in Art 1 Abs 1 GG.⁵⁸⁴ Hiermit wurde auch aus europäischer Sicht Neuland betreten, da die Menschenwürde zwar vom EuGH als existent anerkannt war, jedoch nie in Form einer Norm im Europarecht existiert hat.⁵⁸⁵ Die Menschenwürde hat damit mit Art 1 GRC erstmal konkret Eingang in die europäische Rechtsordnung gefunden. Dies führt also nicht nur dazu, dass Normen wie Art 7 GRC, der den Schutz der Kommunikation beinhaltet, im Rahmen einer verfassungsrechtlichen Prüfung herangezogen werden müssen, weil diese Normen in Bezug auf die Telekommunikationsüberwachung als verfassungsrechtliche Norm anzusehen ist; vielmehr spielt es darüber hinaus auch eine Rolle in welchem Naheverhältnis⁵⁸⁶ in Bezug auf die Menschenwürde ein Eingriff von Ermittlern im Rahmen einer Überwachung steht.

Hierbei ist die Regelung des Art 1 GRC nicht als leerer Programmsatz zu sehen.⁵⁸⁷ Vielmehr wurde die Norm bewusst in die Charta eingefügt, da die Menschenwürde als Basis aller Grundrechte nicht in allen Verfassungsrechtsordnungen der Mitgliedsstaaten als durchsetzbares Grundrecht oder generelles, voraussetzungsvolles Grundprinzip mit Ausstrahlungswirkung auf alle Grundrechte geläufig war.⁵⁸⁸ Sie ist

⁵⁸⁴ Die Norm des Art 1 GG ist dabei nicht als schlichter Programmsatz zu sehen, sondern als verfassungsrechtliches Leitbild, in dessen Lichte alle Normen (auch andere des Verfassungsrechts) zu interpretieren sind; vgl hierzu *Tinnefeld*, MMR 2004, 797, 798 f. Sie ist dabei nicht nur vom deutschen Verfassungsrecht beeinflusst, sondern auch von der Präambel der Allgemeine Erklärung der Menschenrechte von 1948, in der es heißt, dass [...] „die Anerkennung der allen Mitgliedern der menschlichen Familie innewohnenden Würde und ihrer gleichen und unveräußerlichen Rechte die Grundlage der Freiheit, der Gerechtigkeit und des Friedens in der Welt bildet.“.

⁵⁸⁵ Vgl hierzu *Borowski* in Meyer, Europäische GRC⁴, Art 1, Rz 26.

⁵⁸⁶ Vgl hierzu bereits unter 15.2.2.1.

⁵⁸⁷ *Fuchs/Segalla* in Holoubek/Lienbacher, GRC, Art 1, Rz 3 f.

⁵⁸⁸ In der Entstehungsgeschichte der GRC gab es in diesem Punkt durchaus starke Meinungsverschiedenheiten, welche auf konträre grundrechtliche Auffassungen in einzelnen Mitgliedsstaaten der EU zurückzuführen sind. Während vor allem britische Stimmen nicht davon überzeugt waren, dass man aus der Menschenwürde direkt persönliche Rechte des Individuums ableiten könne, war es vor allem Deutschland, das aus seiner Verfassungstradition heraus dafür eintrat, die Menschenwürde als Grundrecht und nicht etwa nur als einen schlichten Programmsatz in einer der Charta vorangestellten Präambel aufzunehmen. Vgl zu dieser Entstehungsgeschichte die Zusammenfassung bei *Callies* in *Callies/Ruffert*, EUV/AEUV⁴, Art 1 GRC, Rz 4 mwN; *Borowski* in Meyer, Europäische GRC⁴, Art 1, Rz 32 f; *Fuchs/Segalla* in Holoubek/Lienbacher, GRC, Art 1, Rz 7.

ferner kein Grundrecht, das in irgendeiner Form von staatlichen Institutionen verliehen oder gewährt wird, sondern wird als inhärent angesehen,⁵⁸⁹ was auch mit ein Grund dafür ist, dass ihr Wesensgehalt nicht angetastet werden darf.⁵⁹⁰ Die Vorschrift des Art 1 GRC ist damit grundsätzlich einklagbar, wenn dies auch in argumentationstechnischer Hinsicht in jedem Einzelfall eine Herausforderung darstellen mag.⁵⁹¹ Eine Einschränkung wird hierbei jedoch wenigstens zu machen sein: Die Existenz von Art 1 GRC darf keinesfalls in der Form verstanden werden, als handle es sich um ein Auffanggrundrecht, welches immer dann greift, wenn es kein „passendes“ Grundrecht gibt und das fehlende Grundrechte stets zu ersetzen vermag;⁵⁹² jedoch kann es unter Umständen bei bestehenden Grundrechten schutzverstärkend wirken.⁵⁹³

Damit ist zunächst festzustellen, dass Art 1 GRC und Art 1 Abs 1 GG nicht nur wortgleich sind, sondern auch von der rechtsdogmatischen Einordnung vergleichbar sind. Der Menschenwürdebegriff ist in der deutschen Verfassungsgeschichte bei Einführung des Grundgesetzes auf Bundesebene gleichwohl ein Novum gewesen, war jedoch schon in verschiedenen Länderverfassungen der Nachkriegszeit zu finden,⁵⁹⁴ wobei sich insbesondere die Verfassungstradition des Freistaates Bayern und dessen Verfassungsgerichtshof das Grundrecht entscheidend geprägt hat.⁵⁹⁵

Weil damit in der GRC eine Norm geschaffen wurde, die mit Art 1 Abs 1 GG absolut vergleichbar und auch an diese Norm angelehnt ist,⁵⁹⁶ spricht auch nichts dagegen, deutsche Judikate, welche Art 1 Abs 1 GG eine maßgebende Bedeutung in ihrer Rechtsprechung einräumen, grundsätzlich auch auf Österreich zu beziehen und daraus etwas

⁵⁸⁹ *Borowski* in Meyer, Europäische GRC⁴, Art 1, Rz 27.

⁵⁹⁰ *Borowski* in Meyer, Europäische GRC⁴, Art 1, Rz 31. Dies führt beim Menschenwürdeschutz auch zu einer Ewigkeitsgarantie.

⁵⁹¹ Dazu näher *Borowski* in Meyer, Europäische GRC⁴, Art 1, Rz 33.

⁵⁹² *Fuchs/Segalla* in Holoubek/Lienbacher, GRC, Art 1, Rz 28.

⁵⁹³ *Borowski* in Meyer, Europäische GRC⁴, Art 1, Rz 33 f.

⁵⁹⁴ *Herdegen* in Maunz/Düring, GG, Art 1, Rz 15.

⁵⁹⁵ Art 100 BV lautete in der Ursprungsfassung etwa: „Die Würde der menschlichen Persönlichkeit ist in Gesetzgebung, Verwaltung und Rechtspflege zu achten.“ Vgl hierzu die Entscheidungen BayVerfGHE 1, 29, 32 und 2, 85, 91. Die heutige Fassung des Art 101 BV wurde wiederum an die Formulierung des GG angeglichen, um klarzustellen, dass es in der Interpretation des Menschenwürdebegriffs keine Unterschiede gibt.

⁵⁹⁶ Vgl zur deutschen Vorbildwirkung für dieses Grundrecht *Fuchs/Segalla* in Holoubek/Lienbacher, GRC, Art 1, Rz 15 ff.

für die österreichische Rechtsordnung abzuleiten. Insofern können die Überlegungen des BVerfG zu Beweiserhebungs- und Beweisverwertungsverböten auch entsprechend herangezogen und österreichische Grundrechte im Licht von Art 1 GRC interpretiert werden, sofern die Charta der Grundrechte auf den Sachverhalt Anwendung findet. Darüber hinaus besteht die grundsätzliche Möglichkeit, dass Art 1 GRC bereits existierenden Grundrechtsschutz verstärkt oder nationale Grundrechte in einem anderen verfassungsrechtlichen Licht erscheinen lässt.

Dies bedeutet nämlich in letzter Konsequenz für die Überwachung von Telekommunikation vor allem eines: Es existiert auf der Ebene der europäischen Grundrechte und damit automatisch auf der Ebene der österreichischen Verfassungsrechtsordnung sehr wohl ein Kernbereich, der staatlicherseits freizubleiben hat und nicht angetastet werden darf und auch nicht zur Disposition stehen kann.⁵⁹⁷ Je näher ein Grundrecht sich an der Menschenwürde bewegt,⁵⁹⁸ desto mehr wird dann auch Art 1 GRC für dieses schutzverstärkend wirken. Dies wird man in Zukunft auch für Österreich gelten lassen müssen.

Folglich kann der Judikatur des deutschen BVerfG und deren hier erfolgten gedanklichen Weiterentwicklung eine diesbezügliche Anwendbarkeit nicht grundsätzlich abgesprochen werden. Nun ist zu fragen, ob diese Anwendung sich lediglich im Sinne eines guten Menschenrechtsschutzes empfiehlt oder ob eine ähnliche Umsetzung in Österreich nicht sogar zwingend geboten ist.

21.2. Fazit

Verfassungsrechtlich gesehen sind damit österreichische Grundrechte, wie etwa das Fernmeldegeheimnis nach Art 10a StGG oder das Grundrecht auf Datenschutz nach § 1 DSG 2000, auch im Lichte der GRC zu interpretieren und anzuwenden, wenn dies nach Art 51 GRC geboten ist. Hiervon ist im Rahmen der Telekommunikationsüberwachung auszugehen. Schließlich handelt es sich beim Schutz der Persönlichkeitssphäre

⁵⁹⁷ Vgl zur GRC aus medizinrechtlicher aber auch aus allgemeiner Perspektive *Müller-Terpitz* in Spickhoff, Medizinrecht, Rz 54.

⁵⁹⁸ Vgl hierbei zum GG *Herdegen* in Maunz/Düring, GG, Art 1, Rz 26.

um eine klassische Ausprägung der Menschenwürde.⁵⁹⁹ Dies eröffnet grundrechtlich auch neue rechtliche (?) Möglichkeiten.⁶⁰⁰

22. Das Grundrecht auf informationelle Selbstbestimmung in der österreichischen Verfassungsrechtsordnung

Das in Deutschland bereits seit langem etablierte Grundrecht auf informationelle Selbstbestimmung⁶⁰¹ ist, wie auch das neuere sog „IT-Grundrecht“⁶⁰², kein ausdrücklich in der Verfassung niedergeschriebenes Grundrecht, sondern wurde vom BVerfG unter Heranziehung bestehender Grundrechte schwerpunktmäßig aus der Menschenwürde (Art 1 Abs 1 GG) und aus der allgemeinen Handlungsfreiheit (Art 2 Abs 1 GG) und deren Kombination entwickelt. Ein entsprechend benanntes Grundrecht kennt auch das österreichische Verfassungsrecht nicht. Allerdings war das Grundrecht auf informationelle Selbstbestimmung bislang in der österreichischen Rechtsordnung kein Thema, während es in Deutschland in allen verfassungsrechtlichen Fallkonstellationen, in denen es um die Verarbeitung personenbezogener Daten geht, zur Anwendung kommt.

22.1. Verwendung durch den VfGH und der Unterschied zum Grundrecht auf Datenschutz

Im Zuge der Rechtsprechung zur Vorratsdatenspeicherung hat der VfGH erstmals einen Eingriff in die „informationelle Selbstbestimmung“ im Sinne des BVerfG bejaht, ohne dieses auf ein konkretes Grundrecht zu stützen. Hierzu gibt es kritische Stimmen, die eine Herleitung aus § 1 DSG 2000 für nur schwer begründbar halten,⁶⁰³ zumal sich der VfGH in bestimmten Fällen auch einen Richtervorbehalt vorstellen kann, was wiederum mehr an das sog „IT-Grundrecht“ erinnert, womit sehr fraglich ist, ob er

⁵⁹⁹ Vgl hierzu zur Rechtslage in Deutschland *Herdegen* in Maunz/Düring, GG, Art 1, Rz 84.

⁶⁰⁰ Vgl zu den möglichen Auswirkungen auf Österreich *Fuchs/Segalla* in *Holoubek/Lienbacher*, GRC, Art 1, Rz 37 ff.

⁶⁰¹ Vgl unter 9.2.

⁶⁰² Vgl unter 9.3

⁶⁰³ *Hattenberger/Klingbacher*, Bemerkenswertes zur Entscheidung des VfGH zur Vorratsdatenspeicherung, *Jahrbuch Öffentliches Recht* 2015, 179, 198.

tatsächlich das Grundrecht auf informationelle Selbstbestimmung, so wie es das deutsche Verfassungsrecht kennt, gemeint hatte. Zwar sieht auch die Kommentarliteratur in § 1 DSG 2000 die österreichische Umsetzung des Grundrechtes auf informationelle Selbstbestimmung,⁶⁰⁴ geht hierbei aber nicht auf die Tatsache ein, dass viele verfassungsdogmatische Unterschiede zu Art 2 Abs 1 GG iVm Art 1 Abs 1 GG bestehen.

Für eine Unterscheidung zwischen beiden Grundrechten spricht auch, dass das Grundrecht auf Datenschutz nicht zugleich als Grundrecht auf informationelle Selbstbestimmung erhalten kann, auch wenn es ihm nahe kommt. Das Grundrecht auf informationellen Selbstbestimmung kennt auch keinen Eingriffsvorbehalt, wie in § 1 Abs 2 DSG 2000.⁶⁰⁵ Zudem kann eine Rechtsquelle allein kaum Grundlage für zwei Grundrechte darstellen, die sich innerhalb der gleichen Materie bewegen. Es handelt sich bei beiden auch nicht um Synonyme. Hierfür spricht auch, dass der Begriff in der Verfassungsrechtsprechung in Österreich bislang nicht in Erscheinung trat. Wären das Grundrecht auf Datenschutz und das Grundrecht auf informationelle Selbstbestimmung Synonyme oder wäre die informationelle Selbstbestimmung eine Teilausprägung von § 1 DSG, wäre dies bereits zuvor aus der Rechtsprechung des VfGH hervorgegangen, da es hierfür genügend geeignete Anlassfälle gegeben hätte.

Vielmehr ist das Grundrecht auf informationelle Selbstbestimmung betroffen, wenn der Kernbereich von § 1 DSG 2000 verletzt wird, die Eingriffe also eine Vielzahl von persönlichen Daten umfassen. Hierbei spielt auch die Menschenwürde eine Rolle, deren Wirkung auf das österreichische Verfassungsrecht unter den oben geschilderten Umständen gegeben ist. So ist die Materie des Datenschutzrechts auf Grundlage einer europäischen Richtlinie, der sog „Datenschutzrichtlinie“, ⁶⁰⁶ eindeutig der europäischen Rechtsmaterie zuzuordnen. Der Bezug zum EU-Recht ist damit noch enger als im Bereich der Telekommunikationsüberwachung.⁶⁰⁷

⁶⁰⁴ Dohr/Pollirer/Weiss/Knyrim, DSG², § 1, Rz 2.

⁶⁰⁵ So auch *Hattenberger/Klingbacher*, Bemerkenswertes zur Entscheidung des VfGH zur Vorratsdatenspeicherung, Jahrbuch Öffentliches Recht 2015, 179, 198.

⁶⁰⁶ RL 95/46/EG.

⁶⁰⁷ Vgl unter 21.1.2.4.

22.2. § 1 DSG 2000, Art 8 EMRK, Art 1 und 8 GRC als Rechtsquellen des „Grundrechts auf informationelle Selbstbestimmung“

Nach der Entscheidung des VfGH wurden unterschiedliche Schlüsse aus der Erwähnung des Grundrechts auf informationelle Selbstbestimmung gezogen. Während vorbenannte Quellen vor allem die Auswirkungen diskutieren, die Einführung des Grundrechtes in die österreichische Rechtsordnung aber wohl annehmen, gibt es auch kritische Stimmen, die dessen Einführung ablehnen bzw davon ausgehen, durch die Erwähnung des Grundrechts auf informationelle Selbstbestimmung sei keine Einführung eines solchen Grundrechts in die österreichische Rechtsordnung erfolgt. So sieht *Grabenwarter* durch die Stellung in der Entscheidung im Rahmen der Verhältnismäßigkeitsprüfung bestätigt, dass hier nicht etwa die Dogmatik des BVerfG übernommen werden soll, sondern eine „teleologische Erweiterung und Einbettung in den systematischen Zusammenhang im Hinblick auf den Privatsphärenschutz insgesamt“ erfolgt.⁶⁰⁸ Im Ergebnis führt dies aber zu keinem grundsätzlichen Unterschied. Auch *Grabenwarter* sieht letztlich das Grundrecht auf informationelle Selbstbestimmung als eigenständiges grundrechtliches Schutzgut im Rahmen von Art 8 EMRK und § 1 DSG 2000 an.⁶⁰⁹

Hierbei ist zu bedenken, dass die Berücksichtigung von Art 1 GRC⁶¹⁰ im österreichischen Verfassungsrecht auch die Voraussetzungen für einen Kernbereichsschutz schafft. Somit dürfte es auch rechtsdogmatisch möglich sein, ohne pauschal auf einen Rechtsbegriff aus dem deutschen Verfassungsrecht zurückzugreifen, das Grundrecht auf informationelle Selbstbestimmung auf entsprechende Rechtsquellen des österreichischen Verfassungsrechts zu stützen.

Dies eröffnet den Weg zu einem für Österreich neuen Grundrechtsschutz, der nicht nur auf der Grundlage von § 1 DSG 2000 und Art 8 EMRK steht, sondern das (auch) auf die GRC als Rechtsquelle zurückgreifen kann, namentlich auf Art 1 GRC und Art 8 GRC. Insbesondere durch die Einbeziehung von Art 1 GRC kann ein ähnli-

⁶⁰⁸ *Grabenwarter*, Das Recht auf informationelle Selbstbestimmung im Europarecht und im Verfassungsrecht, Österreichisches Anwaltsblatt 2015, 404, 405.

⁶⁰⁹ *Grabenwarter*, Das Recht auf informationelle Selbstbestimmung im Europarecht und im Verfassungsrecht, Österreichisches Anwaltsblatt 2015, 404, 406.

⁶¹⁰ Vgl hierzu unter 21.

ches Schutzniveau wie in Deutschland letztlich begründet werden. Ob es sich hierbei nun um ein gänzlich neues Recht aus österreichischer Sicht handelt oder um eine spezielle Ausprägung des Kernbereichs des Grundrechts auf Datenschutz kann hierbei offenbleiben, weil diese Frage für das Schutzniveau insoweit keine Rolle spielt. Durch die Einbeziehung von Art 1 GRC werden die Einschränkungsmöglichkeiten in § 1 DSG 2000 noch weiter limitiert. Ob dies zu einem Richtervorbehalt immer dann führen muss, wenn das Grundrecht auf informationelle Selbstbestimmung betroffen ist, wie es der VfGH anklingen ließ, ist meines Erachtens nach nicht unbedingt zwingend. Jedoch muss auf den Einzelfall und weitere betroffene Grundrechte abgestellt werden. Jedenfalls bedarf es bei einem Eingriff in das Grundrecht auf informationelle Selbstbestimmung eines besonders gewichtigen Rechtfertigungsgrunds.

23. Ergebnisse

Auch wenn Deutschland und Österreich sehr unterschiedliche Verfassungstraditionen haben, bietet sich ein Rechtsvergleich an und ist sogar durch neuere Entwicklungen noch leichter möglich geworden. Einige der relevanten Grundrechte gibt es in beiden Ländern, die vom Wortlaut her auch vergleichbar sind, wie etwa Art 10a StGG und Art 10 GG. Hier kann ein Vergleich insofern dienlich sein, als dass dieser die Möglichkeit eröffnet, sich von im jeweiligen Land festgefahrenen Auslegungsmustern zu entfernen und entsprechend neue Auslegungswege zu gehen.

Im Hinblick auf das Fernmeldegeheimnis bedeutet dies, dass davon auszugehen ist, dass zumindest eine große Häufung von Metadaten dazu führt, dass dieses auch aus österreichischer Sicht betroffen ist. Umgekehrt ist der Rechtsvorbehalt aus dem österreichischen Verfassungsrecht ebenfalls für das deutsche Verfassungsrecht anzudenken. Hier bewegt sich auch die Rechtsprechung in Deutschland immer stärker in diese Richtung, gleichwohl ohne letztlich den Richtervorbehalt für anwendbar zu erklären.

Wesentlich schwieriger ist ein verfassungsrechtlicher Vergleich, wenn lediglich in einer Rechtsordnung eine Norm vorhanden ist, in der anderen Rechtsordnung, mit der verglichen werden soll, diese Norm aber in der Form nicht vorhanden ist. Eine direkte Übertragbarkeit bietet sich in einem solchen Fall eher nicht an. Allerdings ist auch das Verfassungsrecht einem stetigen Wandel unterworfen. Hierbei stellt die GRC für alle

Verfassungsrechtsordnungen der Mitgliedsstaaten eine Herausforderung dar, da sich diese nun teilweise mit neuen Grundrechten konfrontiert sehen. Der VfGH hat bereits herausgearbeitet, unter welchen Umständen die Grundrechte der GRC zu den Grundrechten des österreichischen Verfassungsrechts hinzutreten und auch vom VfGH überprüft werden. Ist dies der Fall, kann dies wieder zu einer besseren Vergleichbarkeit des Verfassungsrechts führen. So verhält es sich auch mit der für diese Arbeit wichtigen Menschenwürde, die in Deutschland im GG verankert ist, sich ebenfalls in der GRC findet und damit nun auch Eingang in das österreichische Verfassungsrecht gefunden hat.

Dies hat auch unmittelbare Auswirkungen auf die Übertragbarkeit von Erkenntnissen zu weiteren Grundrechten aus der deutschen Verfassungsrechtsordnung, für die kein österreichisches Pendant besteht, sofern diese ein Pendant in der GRC haben. Grundrechte, für welche die Menschenwürde eine Rechtsquelle darstellt, wie etwa das „Grundrecht auf informationelle Selbstbestimmung“ sind so leichter in die österreichische Verfassungsrechtsordnung übertragbar. Hierbei lassen sich mehr als nur Leitlinien ablesen,⁶¹¹ sondern es ist auch an die Anwendbarkeit einzelner Grundrechte zu denken, erst recht, wenn der VfGH diese explizit erwähnt. Dies wird in Fällen, wo die GRC Anwendung findet, zu einem teilweise stärkeren Grundrechtsschutz führen.

⁶¹¹ So leitet *Zerbes* etwa aus dem Urteil des Bundesverfassungsgerichts zum sog IT-Grundrecht Leitlinien für das österreichische Verfassungsrecht ab; *Zerbes*, Das Urteil des deutschen Bundesverfassungsgerichts zur Online-Durchsuchung und Online-Überwachung Grundrechtlicher Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme - auch in Österreich, ÖJZ 2008, 843, 841 f.

Kapitel V – Bedeutung von Kontrollinstanzen im Rahmen von Überwachungsmaßnahmen. Ist der Richtervorbehalt in der heutigen Form zeitgemäß?

Wann immer Telekommunikation einer Überwachung unterliegt, stellt sich die Frage, welche Instanz die Ermittler, welche die Zielpersonen überwachen, kontrolliert. Im Gegensatz zu vielen anderen Maßnahmen im präventiven oder repressiven Bereich wird der Betroffene von der entsprechenden Maßnahme nichts mitbekommen. Dies ist auch nicht weiter verwunderlich, da Telekommunikationsüberwachung grundsätzlich verdeckt erfolgt, da sie ansonsten wirkungslos wäre. Die Heimlichkeit der Maßnahme gehört also zu deren Wesen.

Bereits im Rahmen des Rechtsvergleiches zwischen Deutschland und Österreich im Bereich des Fernmeldegeheimnisses nach Art 10a StGG bzw Art 10 GG drängte sich die Frage auf, inwiefern die Kontrollinstanz des Richtervorbehaltes im Rahmen von Eingriffen in das Fernmeldegeheimnis Bedeutung hat. Im Rahmen der präventiven Überwachung durch Ermittler stellt sich in Österreich die Frage, inwiefern die dort eingeführte Kontrolle durch den Rechtsschutzbeauftragten entsprechende verfassungsrechtliche Vorgaben erfüllen kann.

24. Der Richtervorbehalt als Kontrollinstanz

Der Richtervorbehalt dient als Kontrollinstanz und ist ein rechtsstaatlicher Ausgleich für die heimliche Überwachung. Hierbei kann man beim Richtervorbehalt auf eine lange Geschichte zurückblicken, da sich dieser sowohl in der Paulskirchenverfassung als auch im StGG findet.⁶¹² Insofern ist den Verfassungstraditionen in Österreich

⁶¹² Wie auch das StGG kannte bereits die Paulskirchenverfassung von 1848, bei der eine Geltung auch in der österreichischen Reichshälfte vorgesehen war (da diese im Gegensatz zur ungarischen Reichshälfte Teil des Deutschen Bundes war), an mehreren Stellen bereits einen Richtervorbehalt, wobei sich oft Parallelen zum StGG ergeben, wie etwa bei beschlagnahmten Briefen (§ 141 Paulskirchenverfassung). Hierbei weist das StGG von 1867 oder auch im Hausrechtsgesetz von 1862 durchaus moderne Züge auf. Anders hat sich das Verfassungsrecht in Deutschland entwickelt. Noch in der WRV von 1919 überließ etwa der Verfassungsgesetzgeber sämtliche Eingriffe in Grundrechte der Disposition des einfachen

und Deutschland der Richtervorbehalt und dessen Anwendung schon seit langer Zeit bekannt. Es handelt sich damit also um kein Novum der letzten Jahrzehnte, sondern um ein Institut, dessen Existenz bereits weit zurückreicht. Taugliches Mittel zur Verteidigung der Betroffenenrechte kann der Richtervorbehalt nur kraft seiner verfassungsrechtlich garantierten Unabhängigkeit sein, die in Österreich ihren Ursprung bereits in der Märzverfassung von 1849 findet, die die selbständige Ausübung der richterlichen Gewalt den Gerichten zubilligt.⁶¹³

In seiner praktischen Ausgestaltung heutzutage wird er vielfach kritisch gesehen. *Zerbes* sieht hierin im Bereich der Telekommunikationsüberwachung etwa nur ein Trostpflaster für die Betroffenen.⁶¹⁴ Sie bezieht sich hierbei auf *Asbrock*, der den Begriff bereits 1998 in den rechtspolitischen Diskurs einbrachte und dessen Kritik sich – anlässlich des damals in Deutschland eingeführten „großen Lauschangriffs“ – vor allem auf großen Zeitdruck wegen Eilbedürftigkeit, einer hohen Anzahl an komplexen Verfahren, die es einem einzelnen Richter schwer machen, sich näher mit dem Sachverhalt zu befassen, einer oft selektiven Darstellung von Beweisen durch die Staatsanwaltschaft und nicht zuletzt auf mangelndes Fachwissen in komplexen oft technischen Fragestellungen.⁶¹⁵

Zunächst einmal ist hierbei zu bekräftigen, dass der Richtervorbehalt stets dann anzuwenden ist, wenn in bestimmte Grundrechte eingegriffen wird, wobei es nicht unbedingt erforderlich ist, dass sich der, in dessen Grundrecht eingegriffen wird, selbst im Einklang mit der Rechtsordnung befindet.⁶¹⁶

Gesetzgebers. Vgl hierzu näher *Kamann*, Der Richtervorbehalt in Art 13 Abs 2 GG und seine Bedeutung für den Grundrechtsschutz im Ermittlungsverfahren in *Kammeier/Michalke*, Streben nach Gerechtigkeit, 183.

⁶¹³ Auch vor der Märzverfassung wurde bereits in der Pillerdorff'schen Verfassung die richterliche Unabhängigkeit wohl vorausgesetzt. Später wurde diese immer mehr weiterentwickelt, was heute die richterliche Unabhängigkeit ausmacht, also etwa die Unabsetzbarkeit und Unversetzbarkeit (eingeführt durch das „StGG über die richterliche Gewalt“ von 1867. Vgl hierzu *Piska* in *Korinek/Holoubek*, Österreichisches Bundesverfassungsrecht, Bd. I/333, Art 87 B-VG, Rz 6.

⁶¹⁴ *Zerbes*, Spitzeln Spähen Spionieren, 334.

⁶¹⁵ *Asbrock*, Der Richtervorbehalt – prozedurale Grundrechtssicherung oder rechtsstaatliches Trostpflaster, ZRP 1998, 17, 19.

⁶¹⁶ *Werwigk*, Zur Geltung des Richtervorbehalts bei der Durchsuchung von besetzten Häusern, NJW 1983, 2366, 2367 f.

Nicht zu unterschätzen ist, dass der Richtervorbehalt, zumindest dann, wenn dieser ernst genommen wird, auch eine Hürde bedeutet, eine Art „stummen Grundrechtsschutz“, zumindest wenn er ohne Einschränkungen ausgestaltet ist, welcher Ermittler bei bestimmten Fällen auch davon abhält, bestimmte Grundrechtseingriffe überhaupt einem Richter vorzulegen.⁶¹⁷

Unabhängig davon, ob man den Richtervorbehalt nach der jetzigen Praxis für ein nützliches und effektives Mittel oder für ein juristisches Feigenblatt hält,⁶¹⁸ ist sein Zweck klar. Er ist Schutz dort, wo der Betroffene sich nicht wehren kann, etwa wenn der Eingriff heimlich ist und / oder explizit gegen oder ohne den Willen des Betroffenen erfolgt, mithin in der Regel dann, wenn ein Grundrechtsschutz auf andere Weise gar nicht oder nur in mangelhafter Weise gewährleistet ist. Auf die Kritik am Richtervorbehalt wird einzugehen sein, da dieser auch im Berufsgeheimnisträgerschutz von Relevanz ist.

Immerhin ist zu begrüßen, dass bei Fehlen des richterlichen Befehls in Österreich nunmehr auch direkt unabhängige Gerichte angerufen werden können, so dass eine richterliche Überprüfung im Nachhinein auch möglich ist.⁶¹⁹ Da eine Überwachung durch Ermittler ohne richterlichen Befehl stets einen Verwaltungsakt darstellt,⁶²⁰ können Betroffene gegen diesen nach Art 130 Abs 1 Z 2 B-VG vor den Verwaltungsgerich-

⁶¹⁷ So war es früher in Deutschland etwa bis 1985 bei Wohnungsdurchsuchungen gängige Praxis, gar nicht erst im Falle mittlerer Kriminalität (etwa bei Ladendiebstahl oder Suchtmitteldelikten kleineren Ausmaßes) die Wohnung des Verdächtigen zu durchsuchen, sondern diesen zunächst polizeilich vorzuladen. Insofern wirkte der Richtervorbehalt schützend, ohne dass er in diesen Fällen überhaupt zur Anwendung kam. Ermittler stellten zwar gelegentlich derartige Anträge, waren aber geneigt, diese mit Hinweis auf den Verhältnismäßigkeitsgrundsatz wieder zurück zu nehmen. In dem ab Mitte der 1980er Jahre die Gerichte zunehmend mit – teilweise kaum begründeten – Anträgen geflutet wurden, verkam der Richtervorbehalt mehr und mehr zu einer Farce. Vgl hierzu *Kamann*, Der Richtervorbehalt in Art 13 Abs 2 GG und seine Bedeutung für den Grundrechtsschutz im Ermittlungsverfahren in *Kammeier/Michalke*, Streben nach Gerechtigkeit, 185 ff.

⁶¹⁸ *Helmken* etwa sieht den Richtervorbehalt in Deutschland in seiner jetzigen Form bei Haftprüfungen als standardisiertes Palliativum an; *Helmken*, Reform des Richtervorbehalts: Vom Palliativum zum effektiven Grundrechtsschutz, StV 2003, 193.

⁶¹⁹ Vor Einführung der Verwaltungsgerichte waren die UVS zuständig.

⁶²⁰ Vgl zur Gleichstellung von verwaltungsbehördlicher Befehls- und Zwangsgewalt mit Verwaltungsakten durch den Verfassungsgesetzgeber im Jahr 1975 *Korinek*, Grundrechte und Verfassungsgerichtsbarkeit, 30 mwN.

ten klagen.⁶²¹ Voraussetzung hierfür ist freilich, dass diese überhaupt von der Überwachungsmaßnahme erfahren.

25. Die Kontrolle durch den Rechtsschutzbeauftragten

Die Institution des Rechtsschutzbeauftragten existiert im österreichischen Recht vier Mal. Zum einen als Rechtsschutzbeauftragter für die Sicherheitspolizei (§ 91a ff SPG), als Rechtsschutzbeauftragter nach der StPO und jenem nach dem Militärbefugnisrecht.⁶²² Neu eingeführt wurde zudem im Zuge der Steuerreform 2014/2015 und der damit einhergehenden Einführung des § 99 Abs 3 FinStrG (Beaufkundung von IP Adressen)⁶²³ der Rechtsschutzbeauftragte nach dem FinStrG.⁶²⁴ Die Rechtsschutzbeauftragten sind Kontrollorgane, die der Kontrolle der Gesetzmäßigkeit der Verwaltung dienen und weisungsfrei sind (Art 20 Abs 2 B-VG). Die Einführung erfolgte 1997 in der StPO⁶²⁵ und 2000 im SPG.⁶²⁶

Sowohl in der StPO als auch im SPG war die Einführung von Überwachungsmaßnahmen im Bereich der optischen und akustischen Überwachung Anlass für die Einführung; bald trat die Telekommunikationsüberwachung als Betätigungsfeld hinzu.⁶²⁷ Der Rechtsschutzbeauftragte nach dem Sicherheitspolizeirecht wird auch für die heimlichen Überwachungen nach dem PStSG zuständig sein (§ 14 ff PStSG).

Für den Berufsgeheimnisträgerschutz in der StPO kommt dem Rechtsschutzbeauftragtem eine herausgehobene Stellung zu. Seine Stellung und die Möglichkeiten zur Mitwirkung bezüglich heimlicher Überwachungsmaßnahmen werden hierbei oft kritisiert, da dieser Schutz nicht lückenlos und konsistent ist.⁶²⁸ Bei Berufsgeheimnisträgern wird er dafür konsequent herangezogen wird (§ 144 Abs 3 S 2 StPO). Hierbei

⁶²¹ Vgl noch zur alten Rechtslage *Marent*, Das Fernmeldegeheimnis und die Telefonüberwachungsregelungen der StPO, 47 f.

⁶²² *Hauer/Keplinger*, SPG⁴, 895.

⁶²³ Die Vorschrift ist § 53 Abs 3a StPO nachgebildet.

⁶²⁴ Näheres hierzu bei *Kronig/Stieglitz* in Marschner/Stefaner, Steuerreform 2015/2016, Rz 8/75 ff.

⁶²⁵ *Zerbes*, Spitzeln Spähen Spionieren, 158.

⁶²⁶ *Hauer/Keplinger*, SPG⁴, 895.

⁶²⁷ *Fuchs/Ratz*, WK StPO § 47a StPO, Rz 1.

⁶²⁸ Vgl näher *Zerbes*, Spitzeln Spähen Spionieren, 186.

muss der Rechtsschutzbeauftragte nicht nur in Kenntnis gesetzt werden, so dass er im Nachhinein eingreifen kann, sondern vielmehr ist von seiner Genehmigung die Maßnahme insgesamt abhängig.⁶²⁹

26. Reformbedarf bei Kontrollinstanzen

Unstrittig sein dürfte, dass es in bestimmten Fällen, in denen eine Überwachung heimlich erfolgt, eine Kontrollinstanz notwendig ist, da ansonsten die Betroffenenrechte nicht wahrgenommen werden können und die Überwachung sich damit langfristig auch außerhalb rechtsstaatlicher Konventionen bewegt. Dennoch mag man sowohl beim heute bestehenden Richtervorbehalt als auch bei dem neuen Institut der Rechtsschutzbeauftragten sowohl die beiden Einrichtungen in ihrer Art selbst, als auch hinsichtlich ihres rechtlichen Rahmens, ihrer Transparenz und Arbeitsweise einer kritischen Betrachtung unterziehen.

26.1. Kritikpunkte am Richtervorbehalt

An der Existenz des Richtervorbehalts ist oft Kritik geäußert worden. So wurden Stimmen laut, die vorbrachten, der Richtervorbehalt hemme bei den modernen Ermittlungsmethoden ein sachgerechtes und rasches Vorgehen der Ermittler, da viele Ermittlungsmethoden in gewisser Weise zeitkritisch seien und nicht in einem beliebigen Zeitraum nachgeholt werden können; bis der richterliche Befehl vorliege, vergehe zu viel Zeit und die Daten seien zu diesem Zeitpunkt dann nicht mehr verfügbar.⁶³⁰ In vielen Fällen stelle der Richtervorbehalt somit eine „verzichtbare Belastung“ dar, welche es für ein rechtsstaatliches Verfahren gar nicht bedürfe.⁶³¹

Diese Stimmen, die allesamt aus der Ermittlerperspektive stammen, sind scharf zurückzuweisen. Nur die Einschaltung einer Kontrollinstanz kann in bestimmten Situationen verhindern, dass die Grundrechte des Betroffenen ihres Wesensgehaltes beraubt werden. Die Argumentationen erfolgen zumeist aus ermittlungstaktischen Gründen.

⁶²⁹ Bertel/Venier, StPO, § 144, Rz 5, Zerb, Spitzeln Spähen Spionieren, 163.

⁶³⁰ Dazu Schaefer, Kommentar: Richtervorbehalt, NJW 2005, 1332 f in Bezug auf DNA-Analysen.

⁶³¹ Krumm, Richtervorbehalt bei der Blutprobe: Weg damit!, ZRP 2009, 71.

Sicher ist es für die Ermittler aufwendig, in jedem Einzelfall die Gerichte einzubinden, aber wer so argumentiert, stellt Grundrechte auf eine Stufe mit Praktikabilitätsabwägungen. Dies kann gerade im Sinne einer rechtsstaatlichen Vorgehensweise kein Maßstab sein. Das soll nicht heißen, dass es nicht möglich wäre, in bestimmten Fällen eine unabhängige Kontrollinstanz anders zu gestalten. Allein beziehen sich die meisten der kritischen Stellungnahmen aus ermittlungstaktischen Gründen darauf, dass sie sich in manchen Situationen keine richterliche Kontrolle wünschen. Dies muss – gerade wenn es um den Schutz der Berufsgeheimnisse geht – als Lösungsmöglichkeit auf Probleme bei der Umsetzung des Richtervorbehaltes klar ausscheiden.

Zugleich gibt es auf der anderen Seite Stimmen, die die Wichtigkeit dieses rechtsstaatlichen Elements unterstreichen und sich dagegen wenden, der Richtervorbehalt sei eine „bloße Formalie“.⁶³² Scharf formuliert es *Albrecht* mit den Worten:⁶³³

Das praktische Versagen des Richtervorbehalts steht in Zusammenhang mit dem Zeitdruck, den der sicherheitspolitische Wettbewerb den Gerichten auferlegt. Aufgrund dieses Zeitdrucks wird auf der Grundlage von Sachverhalten entschieden, die nur aus der Sicht von Polizei und Staatsanwaltschaft aufbereitet wurden. Im Ergebnis stellt der Richtervorbehalt ein dünnes Feigenblatt des Rechtsstaats für die verfassungsrechtliche Zumutung des Geheimprozesses dar.

Dieser Ansatz ist nicht grundsätzlich aus rechtsstaatlichen Erwägungen als bedenklich anzusehen. Die Kritiker verweisen auf die im Grundsatz bestehende Wichtigkeit des richterlichen Vorbehaltes, verweisen aber darauf, dass dessen Effektivität zur Wahrung der Betroffenenrechte in der letzten Zeit auch gelitten hat.⁶³⁴ Diese Kritik macht auch am Richtervorbehalt im Zusammenhang mit der Telekommunikationsüber-

⁶³² *Leipold*, Der Richtervorbehalt in der Praxis, NJW-Spezial 2010, 504, der sich auf eine Entscheidung des BVerfG über Blutentnahme durch die Polizei bei Verdacht auf Trunkenheitsfahrten bezieht. Zu Reformbemühungen in diesem Bereich *Busch*, Vorschlag zur Neuordnung der Anordnungscompetenz für die Entnahme von Blutproben, ZRP 2012, 79.

⁶³³ *Albrecht*, Die vergessene Freiheit. Strafrechtsprinzipien in der europäischen Sicherheitsdebatte, 160.

⁶³⁴ So bereits *Brüning*, Der Richtervorbehalt – ein zahnlöser Tiger?, ZIS 2006, 29, die eine richterliche Kontrolle für verfassungsrechtlich geboten hält, aber seine Ineffektivität in der Praxis anprangert.

wachung nicht Halt.⁶³⁵ So sie zwar vielfach ein richterlicher Befehl erforderlich und wird – wie etwa in der Rechtsprechung des deutschen BVerfG zum „IT-Grundrecht“ – in das Verfassungsrecht hineingelesen, jedoch sei dies nicht unbedingt auch eine Garantie für einen wirksamen Schutz der Grundrechte.⁶³⁶

Im richterlichen Alltag wird sich ein Richter mit einer Vielzahl von Überwachungsanfragen konfrontiert sehen. Ihm wird kaum die Zeit zur näheren Überprüfung bleiben. Außerdem ist es dem Richter selbst überlassen, ob er sich näher mit dem doch recht komplexen Spannungsfeld des Rechts, der Informationstechnologie und der Grundrechte beschäftigt, oder nicht.

Dieser Eindruck wird in der Praxis bestätigt. Der deutsche Mailpostfachbetreiber posteo veröffentlicht behördliche Anfragen und macht Zahlen und Hintergründe hierzu öffentlich.⁶³⁷ Demnach kam es im Jahr 2014 zu 22 behördlichen Anfragen, von denen dieser 15 wegen teils grober rechtlicher Mängel zurückwies, obwohl diese größtenteils zuvor durch ein Gericht angeordnet wurden. Daher sieht der Betreiber den Richtervorbehalt ebenfalls kritisch, da er in der zurzeit in der Praxis gelebten Form seiner Aufgabe nicht gerecht wird.⁶³⁸

Hierbei gibt es in der rechtswissenschaftlichen Debatte gerade in Deutschland viele Stimmen, die dem Richtervorbehalt in seiner jetzigen Form sehr kritisch gegenüberstehen. Der Richtervorbehalt, der schon allgemein erheblicher Kritik ausgesetzt ist, mag somit vor allem im Bereich der Telekommunikationsüberwachung zum zahnlosen Tiger verkommen. Dies ist im Sinne eines effektiven Grundrechtsschutzes kein wünschens-

⁶³⁵ Vgl etwa *Stadler*, Der Richtervorbehalt – ein stumpfes Schwert oder ein rechtsstaatlich gebotenes Instrument?, ZRP 2013, 179, 180 ff.

⁶³⁶ So schon *Gusy*, Überwachung der Telekommunikation unter Richtervorbehalt, Effektiver Grundrechtsschutz oder Alibi?, ZRP 2003, 275, der auf den Zustand verweist, dass Überwachungsmaßnahmen im Bereich der Telekommunikation von Gerichten zumeist genehmigt werden, ohne dass nähere Auskünfte eingeholt werden.

⁶³⁷ Transparenzbericht posteo 2014, abrufbar unter: https://posteo.de/site/transparenzbericht_2014.

⁶³⁸ So wurden etwa in Berlin nach dem Jahr 2007 sämtliche Anträge auf Telekommunikationsüberwachung richterlich genehmigt; vgl Abgeordnetenhaus Berlin Drs 17/2401, 2 ff. Daten aus anderen Bundesländern sind nur schwer zu bekommen, da diese nicht erfasst oder zumindest nicht veröffentlicht werden. Dem stehen ca 2800 überwachte Anschlüsse in Berlin gegenüber.

werter Zustand, da Überwachungsmaßnahmen in diesem besonders sensiblen Bereich oft komplette Lebenssachverhalte der Betroffenen gegenüber den Ermittlern offenlegen.

Insofern lässt sich die Situation wohl wie folgt zusammenfassen: Der Richtervorbehalt wird von den Kritikern, die dessen Wirkungslosigkeit bemängeln, trotzdem als Kontrollinstanz im Grunde für unverzichtbar gehalten. Jedoch dürften sich diese eine andere, mehr auf die Grundrechte der Überwachten bedachte, Ausgestaltung wünschen.

26.2. Kritikpunkte an der Funktion des Rechtsschutzbeauftragten

Auch am Institut des Rechtsschutzbeauftragten wurde Kritik geäußert. Da eine entsprechende Einrichtung in Deutschland in dieser Form nicht existiert, ist insofern nur Kritik aus österreichischer Sicht zu berücksichtigen.

Überhaupt handelt es sich beim Rechtsschutzbeauftragten um ein Konstrukt, für das es keine internationalen Vorbilder gab⁶³⁹ und dessen Verortung im staatlichen Aufbau vom Gesetzgeber nicht genau bedacht wurde.⁶⁴⁰ Der Rechtsschutzbeauftragte nimmt zwar, ähnlich wie beim Richtervorbehalt,⁶⁴¹ Kontrollfunktionen wahr, ist aber nach Ansicht des VfGH Teil der Verwaltung.⁶⁴²

Die Arbeit des Rechtsschutzbeauftragten nach der StPO und auch die des Rechtsschutzbeauftragten nach dem SPG wird zuweilen außerhalb des Berufsgeheimnisträgerschutzes kritisiert. Bisweilen würden zu viele der Überwachungsmaßnahmen durch den Rechtsschutzbeauftragten nicht aufgegriffen; in Fällen, in denen dieser sich einschalte,

⁶³⁹ *Klaushofer*, Strukturfragen des Rechtsschutzbeauftragten, 11.

⁶⁴⁰ Zusammenfassend *Vogl*, Der Rechtsschutzbeauftragte in Österreich, 44.

⁶⁴¹ Manche Stimmen sind auch geneigt zu sagen, der Rechtsschutzbeauftragte sei eher mit einem Rechtsanwalt zu vergleichen, der die Interessen seiner Partei, in dem Fall des Überwachten, der über die Überwachung nichts weiß, wahrnimmt. Dies lehnt *Klaushofer* aber zurecht ab. Unabhängig davon, ob es sich um gewillkürte oder amtlich bestellte Rechtsvertreter eines Betroffenen handelt, so ist es das Wesen eines solchen, dass dieser stets mit Wissen des Betroffenen agiert. Genau dies ist im Rahmen der Wahrnehmung der Interessen durch den Rechtsschutzbeauftragten nicht möglich, vgl. *Klaushofer*, Strukturfragen des Rechtsschutzbeauftragten, 53.

⁶⁴² *Klaushofer*, Strukturfragen des Rechtsschutzbeauftragten, 44 ff; vgl. auch *Vogl*, Der Rechtsschutzbeauftragte in Österreich, 45. Während *Klaushofer* eher der Meinung des VfGH zuneigt, so gelangt *Vogl* zu dem Ergebnis, es handle sich um eine Figur *sui generis*, die weder Legislative, noch Exekutive oder Judikative zugeordnet werden kann.

blieben dessen Beschwerden erfolglos.⁶⁴³ Im Rahmen der Überwachung von Berufsgeheimnisträgern ist die Kritik zurückhaltend, weil deren Überwachung, wenn man auf die verfügbaren Quellen vertraut, bislang nicht stattgefunden hat.⁶⁴⁴ Insofern ist es schwer einzuschätzen, wie effektiv sich dieser Schutz in der Praxis gestalten würde. Die Erfahrungen aus anderen Bereichen lassen jedoch nicht unbedingt darauf hoffen, dass es sich um ein besonders wirksames Institut zum Schutze der Betroffenenrechte handelt.

Ein weiterer Kritikpunkt ist die mangelnde Transparenz, die eine Überprüfung der Arbeit des Rechtsschutzbeauftragten nach der StPO quasi unmöglich macht. Zudem wird vielfach beklagt, dass aufgrund von Arbeitsüberlastung und fehlenden personellen Ressourcen die Rechtsschutzbeauftragten nach der StPO und nach dem SPG nur schwer ihrer Arbeit im grundrechtlich erforderlichen Ausmaß nachkommen können.⁶⁴⁵

Die Kritikpunkte sind damit ähnlich wie die beim Richtervorbehalt. Dabei muss klar sein, dass die Kontrolle durch den Rechtsschutzbeauftragten den richterlichen Befehl, zumindest bei der jetzigen Ausgestaltung, nicht ersetzen kann. So ist er nicht mit den richterlichen Privilegien nach Art 87 ff B-VG⁶⁴⁶ ausgestattet, was einen deutlichen Unterschied zum Richter aufzeigt.⁶⁴⁷ Es wird somit zum einen nach gemeinsamen Lösungen für Rechtsschutzbeauftragte und Richter zu suchen sein, da es strukturelle Defizite bei beiden Figuren gibt, aber es wird auch zu hinterfragen sein, wie es in Zukunft mit der Kontrolle heimlicher Überwachungsmaßnahmen weitergehen soll.

26.3. Lösungsmöglichkeiten

In der jetzigen Form scheinen weder der „klassische“ Richtervorbehalt, noch neuere Institute, wie das des Rechtsschutzbeauftragten, für eine hinreichende Wahrung der Betroffenenrechte dauerhaft geeignet zu sein. Erst recht gewinnt dieses Problem zusätzliche Vehemenz, wenn Überwachungsmethoden zu- anstatt abnehmen. Dadurch werden sich nämlich auch die zu beurteilenden Fälle häufen.

⁶⁴³ *Zerbes*, Spitzeln Spähen Spionieren, 164.

⁶⁴⁴ *Zerbes*, Spitzeln Spähen Spionieren, 163.

⁶⁴⁵ *Klaushofer*, Strukturfragen des Rechtsschutzbeauftragten, 476.

⁶⁴⁶ Vgl zu den Ausprägungen richterlicher Unabhängigkeit auch *Piska* in Korinek/Holoubek, Österreichisches Bundesverfassungsrecht, Bd. I/333, Art 87 B-VG, Rz 6.

⁶⁴⁷ *Klaushofer*, Strukturfragen des Rechtsschutzbeauftragten, 69.

Dies liegt zum Teil an praktischen Gegebenheiten. Hat die zuständige Stelle kaum Möglichkeiten sich bei einer Vielzahl von Verfahren näher mit einem einzelnen Verfahren zu beschäftigen, verkommt jeglicher Rechtsschutz zur Farce. Die zuständige Stelle benötigt, unabhängig von ihrer näheren Ausgestaltung, durch entsprechende personelle Ausstattung die Möglichkeit, sich mit den einzelnen Fällen, die ja oft von recht komplexer Natur sind, auseinanderzusetzen.

Langfristig ist über eine Weiterentwicklung und Modernisierung des richterlichen Befehls im Rahmen der Telekommunikationsüberwachung nachzudenken. Zwar ist es nach heutiger Rechtslage notwendig, diesen einzufordern, weil nur auf diese Weise eine Kontrolle von Überwachungsmaßnahmen mit Relevanz im Bereich der Telekommunikation überhaupt gewährleistet werden kann, jedoch ist auch dabei kritisch zu fragen, ob nicht ein effektiverer Schutz möglich sein kann.

Insofern kann die jüngste Rechtsprechung und Gesetzgebung auf europäischer Ebene zur *völligen* Unabhängigkeit von Datenschutzkontrollstellen eine neue Perspektive eröffnen,⁶⁴⁸ die eine Weiterentwicklung des Richtervorbehalts in einer modernen, von Technik durchdrungenen Gesellschaft möglich macht. Nach der Regelungen des Art 28 Abs 1 S 2 der RL 95/46/EG⁶⁴⁹ müssen Datenschutzkontrollstellen ihre Aufgaben „in *völler* Unabhängigkeit“ versehen. Dies sieht auch die DS-GVO vor, die in allen EU-Staaten im Mai 2018 in Kraft tritt.⁶⁵⁰

Der EuGH hat den Begriff der „völligen Unabhängigkeit“ bereits interpretiert. Dabei stellte sich der Gerichtshof in seinen Entscheidungen gegen Deutschland⁶⁵¹ und Österreich⁶⁵² eine Datenschutzkontrolle vor, deren Unabhängigkeit nicht in den sonst in

⁶⁴⁸ Vgl. Geuer, Zur Bedeutung des Kriteriums „in völliger Unabhängigkeit“ bei Datenschutzkontrollstellen, ZIR 2013, 8.

⁶⁴⁹ Sog. „Datenschutzrichtlinie“.

⁶⁵⁰ In der DS-GVO sieht Erwägungsgrund 117, sowie Art 52 ff DS-GVO ebenfalls die „völlige Unabhängigkeit der nationalen Datenschutzbehörden vor. Die DS-GVO hat hierbei einige Leitlinien des Urteils aufgenommen und in den Verordnungstext einfließen lassen. So heißt es in Art 52 Abs 2 DS-GVO: *Das Mitglied oder die Mitglieder jeder Aufsichtsbehörde unterliegen bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse gemäß dieser Verordnung weder direkter noch indirekter Beeinflussung von außen und ersuchen weder um Weisung noch nehmen sie Weisungen entgegen.*

⁶⁵¹ EuGH v 9.3.2010, C-518/07 = EuZW 2010, 296 = EuGRZ 2010, 58.

⁶⁵² EuGH v 16.10.2012, C-614/10 = ZD 2012, 563.

Österreich oder Deutschland üblichen Behördenaufbau mit klaren Weisungsverhältnissen passt. Vielmehr scheint dadurch, dass Weisungsverhältnisse wie sie sonst in Behörden üblich sind, nicht vorkommen dürfen, dem EuGH eine neue Art von Behörde vorzuschweben.⁶⁵³ Dies mag aus verwaltungstechnischer Sicht ein Novum darstellen, eröffnet aber zugleich auch neue Chancen, welche es zu nutzen gilt.

Ist eine Datenschutzkontrollstelle eine „völlig unabhängige“ Behörde, deren Beamte keiner behördenexternen Weisung unterliegen, so ist die gewährleistete Unabhängigkeit mit der eines Richters vergleichbar. Aufgrund dieser besonderen Unabhängigkeit können dieser Behörde auch Aufgaben übertragen werden, deren Übertragung bislang nur auf ein Gericht möglich war. Es müsste nur sichergestellt werden, dass die Beamten der Behörde mit allen anderen sonstigen Privilegien der richterlichen Unabhängigkeit, die das Verfassungsrecht vorsieht, sinngemäß ausgestattet werden.⁶⁵⁴

Sinn des richterlichen Befehls ist es, die Überprüfung der Anordnungen der Ermittlungsbehörde durch eine unabhängige Instanz, die keiner direkten Weisung unterliegt, zu gewährleisten. Durch die Unabhängigkeit bei Datenschutzkontrollstellen könnten Aufgaben im Rahmen der Telekommunikationsüberwachung auch auf diese übertragen werden.

Dies hätte den Vorteil, dass die Datenschutzbehörde sachnäher ist und die Maßnahmen besser einschätzen kann. Selbstverständlich würde dies nur dann zu einem besseren Grundrechtsschutz führen, wenn die Behörde personell entsprechend ausgestattet ist, so dass die Anfragen der Ermittler auch tatsächlich fachlich hoch kompetent und in angemessenem zeitlichem Rahmen beantwortet werden können. Zudem ist auch zu bedenken, dass – neben der technologischen Kompetenz – der juristische Ausbildungsstand der Beamten in jedem Fall dem der Richter zu entsprechen hat, um Vergleichbarkeit zu gewährleisten.⁶⁵⁵

⁶⁵³ Zu den Einzelheiten *Geuer*, Zur Bedeutung des Kriteriums „in völliger Unabhängigkeit“ bei Datenschutzkontrollstellen, ZIR 2013, 8, 9f.

⁶⁵⁴ Vgl zum Fehlen dieser Privilegien beim Rechtsschutzbeauftragten unter 25.

⁶⁵⁵ Der Gedanke weitere nationale Institutionen zu schaffen, die dienst- und haushaltsrechtlich unabhängig sind ist unkonventionell, aber nicht neu; vgl hierzu nur den Vorschlag von *Tretter und Novak* zur Errichtung einer finanziell und weisungsmäßig unabhängigen nationalen Menschenrechtsinstitution in

In jedem Fall muss durch handlungsfähige Behörden oder Gerichte ein Gegengewicht zur polizeilichen Überwachung geschaffen werden. Behörden, die überwachen, müssen also gleichwertige Behörden gegenüber stehen, um die Grundrechte zu schützen.⁶⁵⁶

27. Ergebnisse

Der Richtervorbehalt ist ein unverzichtbares Instrument der Kontrolle verdeckter Überwachungsmaßnahmen.⁶⁵⁷ Ohne eine Kontrollinstanz, die mit den beschriebenen Privilegien ausgestattet ist, werden verdeckte Ermittlungsmaßnahmen ausgenutzt. Leider bewährt sich der Richtervorbehalt in der Praxis offenbar nicht und verkommt zum rechtsstaatlichen Feigenblatt.

Dies lässt meines Erachtens nur zwei Möglichkeiten: Entweder wird der Richtervorbehalt in der Praxis gestärkt und wieder zu einem echten Instrument rechtsstaatlicher Kontrolle. Dies setzt voraus, dass die betroffenen Richter in der Lage sind ohne Druck, mit der nötigen Sachkenntnis und mit einer dem Einzelfall gebührenden Zeit über die jeweilige verdeckte Ermittlungsmaßnahme zu entscheiden oder, sofern sich eine solche Praxis innerhalb der Justiz nicht etablieren lässt, weiterentwickelt, indem die Entscheidungskompetenz einer anderen „völlig unabhängigen“ Stelle übertragen wird, die sich – wenigstens im Rahmen der Telekommunikationsüberwachung – verdeckten Ermittlungsmaßnahmen mit der ausreichenden Zeit und Sachkunde widmet. Diese Stelle muss freilich über alle Privilegien eines Richters nach der Verfassung verfügen, da der Schutz ansonsten nie gleichwertig sein kann.

Beide Reformansätze sind hierbei als gleichwertig anzusehen. Entscheidend ist, dass der Gesetzgeber den Tatsachen ins Auge sieht und eine Reform anstrebt. In seiner

Österreich; *Tretter/Nowak*, Vorschläge zur Errichtung einer nationalen Menschenrechtsinstitution in Österreich, JRP 2007, 1.

⁶⁵⁶ In diese Richtung auch *Albrecht*, Neue Behörde soll Licht ins Dunkel bringen, LTO v. 18.07.2016, http://www.lto.de/persistent/a_id/20038/.

⁶⁵⁷ So im Ergebnis auch *Brüning*, Der Richtervorbehalt – ein zahnloser Tiger?, ZIS 2006, 29 ff.

jetzigen Form wird der Richtervorbehalt den verfassungsrechtlichen Vorgaben nicht gerecht.

Das Institut des Rechtsschutzbeauftragten hat sich in der österreichischen Rechtsordnung zwar bewährt, darf aber den Richtervorbehalt nicht ersetzen, zumindest nicht, wenn es bei der jetzigen Ausgestaltung des Rechtsschutzbeauftragten bleibt. Möglich bleibt es freilich, beide Rechtsinstitute langfristig unter einer neuen unabhängigen Stelle zusammenzuführen.⁶⁵⁸

Möchte man solch tiefgreifende Änderungen im System der Kontrollinstanzen nicht durchführen, dann gilt hinsichtlich des Instituts des Rechtsschutzbeauftragten das, was auch zum Richtervorbehalt zu sagen ist, nämlich dass eine hinreichende Ausstattung mit Personal- und Sachmitteln gegeben sein muss, um den gebotenen Grundrechtsschutz sicherzustellen.⁶⁵⁹ Das Budget des jeweiligen Rechtsschutzbeauftragten darf hierbei nicht (allein) vom Wohlwollen des zuständigen Ministeriums abhängen, so wie es etwa beim Rechtsschutzbeauftragten für das SPG der Fall ist.⁶⁶⁰ Hier sollte man sich die Ausgestaltung beim Rechtsschutzbeauftragten für die StPO zum Beispiel nehmen, da dieser sein Budget aus Mitteln über die Geschäftsstelle des OGH erhält und damit vom BMJ unabhängig ist.⁶⁶¹

⁶⁵⁸ Vgl hierzu 26.1.

⁶⁵⁹ So bereits *Klaushofer*, Strukturfragen des Rechtsschutzbeauftragten, 273.

⁶⁶⁰ So auch *Klaushofer*, Strukturfragen des Rechtsschutzbeauftragten, 271. So heißt es in § 91b Abs 3 SPG: *Der Bundesminister für Inneres stellt dem Rechtsschutzbeauftragten die zur Bewältigung der administrativen Tätigkeit notwendigen Personal- und Sacherfordernisse zur Verfügung.* Damit liegt es auch in seinem Ermessen, welche Mittel das sind. Hierin liegt eindeutig eine Schwachstelle.

⁶⁶¹ *Klaushofer*, Strukturfragen des Rechtsschutzbeauftragten, 272.

Kapitel VI – Aktuelle Entwicklungen im Hinblick auf Berufsgeheimnisträger und im Bereich der Telekommunikationsüberwachung in Österreich und Deutschland

Gerade in Zeiten, in denen sich Staaten immer stärker mit dem Problem des internationalen Terrorismus konfrontiert sehen, bei dem sich die Täter auch modernster Technik im Rahmen der Planung von Terrorakten bedienen, in denen aber im Gegenzug auch die technischen Überwachungsmöglichkeiten immer vielfältiger werden, verschärfen Staaten zahlreiche Regelungen im präventivpolizeilichen und strafprozessualen Bereich. Diese Entwicklung macht auch vor Österreich und Deutschland nicht Halt.

Dies ist aus rechtspolitischer Sicht ein Problem, da sich der Gesetzgeber von einem gewissen Aktionismus getrieben zum Eingriff in die Freiheitsrechte *aller* hinreißen lässt, was Terrorakte jedoch nur unwesentlich bekämpft,⁶⁶² die Freiheit des Einzelnen aber erheblich beschränkt. Dies zeigt sich nicht zuletzt, wenn es Auswirkungen auf Berufsgeheimnisträger gibt. Bei jedem Gesetzesvorhaben dieser Art stellt sich die Frage, inwiefern der Berufsgeheimnisträgerschutz entsprechend berücksichtigt wurde. Die bereits gewonnenen Erkenntnisse können insofern direkt auf neue Gesetzgebungsvorhaben angewandt werden. Aus den bereits gewonnenen Erkenntnissen lassen sich gewisse Leitlinien für den Schutz der Berufsgeheimnisträger ableiten. Ebenso lassen sich aus aktuellen gerichtlichen Entscheidungen weitere Erkenntnisse gewinnen bzw. bereits gewonnene Erkenntnisse untermauern.

⁶⁶² Hierbei ist nicht zuletzt auf die Straftatbestände hinzuweisen, wegen denen im Rahmen der Vorratsdatenspeicherung in Österreich letztlich ermittelt wurde. Hierbei kam es etwa vom 1.4.2012 bis zum 31.3.2013 zu 106 Zugriffen auf Vorratsdaten wegen §§ 127 ff StGB (Diebstahl), 40 wegen § 28a SMG (Suchtmittelhandel) oder 29 wegen §§ 146 ff StGB (Betrug). Hingegen kam es nur zu einem Zugriff mit einem klar terroristischen Hintergrund (§ 278b StGB); vgl 14397/AB XXIV. GP - Anfragebeantwortung über die Anwendung des § 135 Abs 2a StPO iVm §§ 102a und 102b TKG.

28. Aktuelle Entwicklungen

Als Entwicklungen der letzten Jahre lassen sich sowohl in Österreich als auch in Deutschland mehrere Gesetzgebungsverfahren ausmachen, die auf die Überwachung von Telekommunikation abzielen. Dies sind in Österreich das Polizeiliche Staatsschutzgesetz (PStSG)⁶⁶³ und der – noch im Anfangsstadium befindliche – Gesetzgebungsprozess zum Polizeitrojaner und in Deutschland die Neueinführung der Vorratsdatenspeicherung, sowie das BKA-Gesetz, welches auch Regelungen zum Einsatz des sog „Bundestrojaners“ enthält. Zu letzterem Gesetz existiert bereits verfassungsgerichtliche Judikatur, die völlig neue Vorgaben für die Überwachung macht und die Ermittler vor Herausforderungen stellt.

28.1. Polizeiliches Staatsschutzgesetz (PStSG) - Österreich

Mit dem Gesetzgebungsentwurf zum PStSG verfolgt der Gesetzgeber das Ziel, erweiterte Gefahrenforschung zu betreiben und *wahrscheinliche verfassungsgefährdende Angriffe* präventiv zu verfolgen (§ 6 Abs 1 PStSG). Hierzu sollen den Ermittler umfassende Ermittlungsmaßnahmen zur Verfügung stehen, die über die zurzeit bestehenden Befugnisse hinausgehen.⁶⁶⁴ Darüber hinaus werden das PStSG und das SPG eng miteinander verzahnt. Träte das Gesetz in der Form in Kraft, wären Berufsheimnisträger – ebenso wie alle anderen Bürger – hiervon betroffen. Insofern ergeben sich Parallelen zur Einführung der Vorratsdatenspeicherung in Österreich. Der Unterschied zur Vorratsdatenspeicherung besteht darin, dass der Gesetzgeber nunmehr nach den Entscheidungen des VfGH, des EuGH, den Entscheidungen von Verfassungsgerichten im Ausland und der flankierenden Behandlung der Materie in wissenschaftlicher Literatur im Prinzip in der Lage sein sollte, die grundrechtlichen Belange der Betroffenen entsprechend zu berücksichtigen.

⁶⁶³ Bundesgesetz, mit dem das Bundesgesetz über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz - PStSG) erlassen und das Sicherheitspolizeigesetz geändert wird; vgl RV 763 d.B. XXV. GP.

⁶⁶⁴ Diese sind in § 12 PStSG aufgelistet und umfassen die Observation (§ 54 Abs 2 SPG), verdeckte Ermittlung (§ 54 Abs 3 und 3a SPG), Einsatz von Bild- und Tonaufzeichnungsgeräten (§ 54 Abs 4 SPG), Einsatz von Kennzeichenerkennungsgeräten (§ 54 Abs 4b SPG), Einholen von Auskünften nach §§ 53 Abs 3a Z 1 bis 3 und 53 Abs 3b SPG, Einholen von Auskünften von Beförderungsunternehmen, Einholen von Auskünften über Verkehrsdaten (§ 92 Abs 3 Z 4 TKG 2003), Zugangsdaten (§ 92 Abs 3 Z 4a TKG 2003) und Standortdaten (§ 92 Abs 3 Z 6 TKG 2003).

Zu kritisieren ist bereits die Bezeichnung des Gesetzes. Allein diese vermag zunächst etwas zu irritieren. So ist nunmehr nicht mehr wie bisher von „Verfassungsschutz“ sondern von „Staatsschutz“ die Rede, obwohl das Bundesamt und die Landesämter für Verfassungsschutz weiter bestehen und auf Grundlage dieses Gesetzes tätig werden sollen, also keine Umbenennung erfahren. Weitaus mangelhafter in gesetzgeberischer Hinsicht ist jedoch die Tatsache, dass historisch betrachtet der Name „Staatsschutzgesetz“ aus österreichischer Sicht sogar mehr als nur zu irritieren mag, da der Begriff „Staatsschutzgesetz“ in der österreichischen Gesetzgebungsgeschichte schon einmal Verwendung gefunden hat, dies aber zur Zeit der Regierung *Schuschnigg* und zur damaligen Zeit mit dem Gesetz die Absicht verfolgend, Gegner des Ständestaates mit schweren Kerkerstrafen zu belegen.⁶⁶⁵ Aus rechtshistorischer Sicht erweist sich damit bereits die Benennung des Gesetzes wohl eher als Fehlgriff. Der Gesetzgeber wäre hier mit einer anderen Gesetzesbezeichnung – zum Beispiel „polizeiliches Verfassungsschutzgesetz“ – besser beraten gewesen.

Letztlich greift das Gesetz auf bestehende Behörden zu, ordnet deren Zuständigkeiten teils neu und gibt ihnen zusätzliche Befugnisse, die im PStSG näher geregelt sind. So kann die Situation eintreten, dass eine Behörde bei einem bestimmten Fall nach dem SPG handelt und in einem anderen Fall nach dem PStSG.⁶⁶⁶

Die Gesetzesbegründung für das PStSG⁶⁶⁷ geht unter anderem von nachfolgender Annahme aus und beschreibt dabei die gesetzgeberische Aufgabenstellung:⁶⁶⁸

⁶⁶⁵ Bundesgesetz über den Schutz des Staates (Staatsschutzgesetz), BGBl 223/1936, 455. Das damalige Staatsschutzgesetz war eher dem Strafrecht zuzuordnen und sah für verschiedene „staatsfeindliche Betätigungen“ schwere Kerkerstrafen von bis zu 5, in schweren Fällen sogar bis zu 10 Jahren, vor. Das Gesetz diene vorgeblich dem Schutz des inneren Friedens, der Verhinderung eines geheimen Nachrichtendienstes zum Nachteil Österreichs und dem Schutz der gesetzgebenden Organe. Einzelheiten zum damaligen Staatsschutzgesetz bei *Talós*, Das austrofaschistische Herrschaftssystem², 271.

⁶⁶⁶ Kritisch zu der gesamten Konstruktion des PStSG die Stellungnahme des Österreichischen Rechtsanwaltskammertages zum Gesetzesentwurf 110/ME XXV. GP., 4.

⁶⁶⁷ Wie oben bereits erwähnt wird nicht nur das PStSG erlassen, sondern es werden auch einzelne Vorschriften des SPG geändert. Der Einfachheit halber bezieht sich PStSG in dieser Arbeit auf den gesamten Gesetzesentwurf.

⁶⁶⁸ Erläuterungen 110/ME XXV. GP, abrufbar im Internet unter http://www.parlament.gv.at/PAKT/VHG/XXV/ME/ME_00110/.

Die globalisierte Welt führt zu internationalen Verflechtungen und gegenseitigen Abhängigkeiten in allen Lebensbereichen. In diesem fortschreitenden Prozess wandelt sich die Auffassung von territorialen Beschränkungen und staatlichen Grenzen und zeigt sich in den letzten Jahren das verstärkt erkennbare Phänomen der Internationalisierung lokaler und nationaler Ereignisse. [...]

Aufgabe des polizeilichen Staatsschutzes muss es sein, die im Staatsgebiet lebenden Menschen und die verfassungsmäßige Grundordnung zu schützen. Der verfassungsmäßig garantierte Schutz des Individuums steht in Teilbereichen in einem Spannungsverhältnis mit den Aufgaben der inneren Sicherheit. Dabei kann ein Eingriff in die individuellen Grundrechte nur unter Abwägung des Grundrechtsschutzes und den Erfordernissen der Aufrechterhaltung der inneren Sicherheit erfolgen.

Das Gesetzesvorhaben hat damit wie jedes Gesetzesvorhaben eine bestimmte Zielsetzung, nämlich *die im Staatsgebiet lebenden Menschen und die verfassungsmäßige Grundordnung zu schützen*. Ob diese Umsetzung gelungen ist, hängt nicht zuletzt davon ab, wie der Schutz der Berufsheimnisträger ausgestaltet ist. Auch dieser ist, wie bereits ausführlich dargelegt, Teil der verfassungsmäßigen Grundordnung und die Existenz des Berufsheimnisträgerschutzes dient nicht zuletzt allen Menschen, die im Staatsgebiet leben. Unabhängig davon, dass die verfassungsmäßige Grundordnung und die im Staatsgebiet lebenden Menschen auch vor anderen Gefahren zu schützen sind, was wohl das vordringliche Ziel des Gesetzesvorhabens ist, darf auch der Berufsheimnisträgerschutz nicht vergessen werden.

Verwundern mag, dass der Gesetzgeber im ersten Entwurf gewillt war, zehn verschiedene Geheimdienste in einem Staat wie Österreich zu schaffen. Dies mag von der Anzahl der Ämter und den dahinterliegenden Ressourcen verwundern, da schließlich in vergleichbaren Ländern, wie etwa Deutschland, für eine wesentlich größere Bevölke-

rungsgruppe, weniger Geheimdienste existieren,⁶⁶⁹ es jedoch im Gegenzug nicht zu beobachten ist, dass das Sicherheitsniveau in Deutschland wesentlich niedriger wäre.

Nachfolgend soll kurz auf die Inhalte des Gesetzesvorhabens eingegangen werden, sowie weiters auf die Umsetzung des Berufsgeheimnisträgerschutzes und im Anschluss auf weitere Schwachpunkte im Rahmen der Überwachung der Telekommunikation.

28.1.1. Inhalte des PStSG

Neben organisatorischen Aspekten (§§ 2 bis 5 PStSG), die man zwar auch kritisieren kann, die vorliegend mangels jedoch Relevanz für den Schutz der Berufsgeheimnisträger nicht näher behandelt werden sollen, enthält das Gesetz in § 1 Abs 2 PStSG eine klare Zielsetzung, die Aufgabenverteilung unter verschiedenen Sicherheitsbehörden, sowie eine Liste, die aufführt, auf welche Daten auf Grundlage dieses Gesetzes zugegriffen werden darf (§§ 10, 12 PStSG).

28.1.1.1. Zielsetzung des PStSG

Wie bereits die Erläuterungen vermuten lassen, ist die Zielsetzung des PStSG zuvorderst die „Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit“ (§ 1 Abs 2 S 1 PStSG). Gefahren werden erblickt in terroristisch, weltanschaulich oder religiös motivierter Kriminalität, Gefährdungen durch Spionage, durch nachrichtendienstliche Tätigkeit und durch Proliferation. Geschützt werden sollen neben den verfassungsmäßigen Einrichtungen Vertreter ausländischer Staaten, internationaler Organisationen und andere Völkerrechtssubjekte nach Maßgabe völkerrechtlicher Verpflichtungen, kritische Infrastruktur und die Bevölkerung. Die Zielsetzung ist also nicht nur in den Erläuterungen beschrieben, sondern hat auch unmittelbar Eingang in das Gesetz gefunden.

⁶⁶⁹ Vom Aufbau her, sind die im Inland tätigen Nachrichtendienste in Deutschland ähnlich organisiert. Neben den Landesämtern für Verfassungsschutz existiert noch das Bundesamt für Verfassungsschutz. Somit kommt man in Deutschland auf eine Zahl von 17 Behörden, dies allerdings bei einer zehnfach höheren Bevölkerungsanzahl als in Österreich. In Deutschland operieren diese Ämter allerdings streng getrennt von den Polizeibehörden des Bundes und der Länder.

28.1.1.2. Datenerhebung im Bereich der Telekommunikation

Das PStSG enthält neben vielen Regelungen im organisatorischen Bereich auch Vorschriften, die sich explizit auf die Ermittlung und Verarbeitung von Daten durch Ermittlungsbehörden beziehen. Zentrale Norm für die Datenermittlung ist § 12 PStSG. Dieser zählt hierbei taxativ die Überwachungsmethoden und Quellen auf, auf die aufgrund des Gesetzes zugegriffen werden darf. Welche dies im Bereich der Telekommunikation sind, ist hierbei in § 12 Z 5 und 7 PStSG näher geregelt. Hierbei greift der Gesetzgeber in § 12 Z 5 PStSG auf bereits bestehende Ermittlungsmethoden nach dem SPG⁶⁷⁰ zurück, während er in § 12 Z 7 PStSG, quasi als Auffangtatbestand, den Ermittlern umfangreichen Zugriff auf weitere Daten einräumt.

Hierbei normiert die Vorschrift des § 12 Z 7 PStSG das Einholen von Auskünften über Verkehrsdaten (§ 92 Abs 3 Z 4 TKG 2003), Zugangsdaten (§ 92 Abs 3 Z 4a TKG 2003) und Standortdaten (§ 92 Abs 3 Z 6 TKG 2003) durch Ermittler. Hiermit sichert sich der Gesetzgeber den Zugriff auf die wichtigsten Daten rund um die Kommunikation eines jeden Bürgers.

In diesem Zusammenhang sind die Bestimmungen des § 12 PStSG als *lex specialis* zu § 10 PStSG zu sehen. Dieser ist die eigentliche Ermächtigungsnorm, welche die Verarbeitung von personenbezogenen Daten ermöglicht, deren Ermittlung im Rahmen der Telekommunikation wiederum im Rahmen des § 12 Z 7 PStSG erfolgt.⁶⁷¹ Ähnlich wie auch im SPG⁶⁷² vorgesehen, ist der Rechtsschutzbeauftragte zu informieren (§ 15 Abs 2 PStSG). Eine Überwachung von Berufsgeheimnisträgern ist nicht von vornherein ausgeschlossen, so dass zu fragen ist, wie der Gesetzgeber deren Schutz konkret ausgestaltet hat bzw ob er ihren Schutz überhaupt bedacht hat.

28.1.2. Umsetzung des Berufsgeheimnisträgerschutzes im PStSG

Gesetzgebung im Bereich der (Telekommunikations-)Überwachung sollte eigentlich voraussetzen, dass bei einer entsprechenden Überwachung auch an eine ausreichende Beschränkung einer solchen zu denken ist, um die Rechte der Bürger, deren

⁶⁷⁰ Namentlich auf §§ 53 Abs 3a Z 1 bis 3 und 53 Abs 3b SPG.

⁶⁷¹ Vgl hierzu die Erläuterungen zum Gesetzesentwurf 110/ME XXV. GP, 5 f.

⁶⁷² Näheres Erläuterungen zum Gesetzesentwurf 110/ME XXV. GP, 9.

Wohl das Gesetz ja vorgeblich dienen soll, bestmöglich zu wahren. Die Auseinandersetzung bis zu diesem Punkt hat bereits gezeigt, dass es auch zur notwendigen Lebensgestaltung eines jeden Bürgers gehört, ungestört und soweit wie möglich frei von jeder Überwachung durch Ermittler mit Berufsgeheimnisträgern zu kommunizieren. Was im Rahmen der Vorratsdatenspeicherung in Österreich und Deutschland in jedem Fall misslang, wurde auch im PStSG nicht umgesetzt. Vielmehr stehen erneut umfassende Überwachungsmöglichkeiten einem mangelnden bzw nicht vorhandenen Berufsgeheimnisträgerschutz gegenüber. Im PStSG findet dieser weder gesonderte Erwähnung, noch ist er durch Verweise auf andere Vorschriften⁶⁷³ abgesichert. Dies ist insofern problematisch, als dass eine Überwachung prinzipiell möglich wird, ohne dass der Betroffene davon erfährt und ohne dass bei der Überwachung die Gruppe der Berufsgeheimnisträger Berücksichtigung findet.⁶⁷⁴

Dieser Kritik ist man sich aus Regierungssicht auch gewahr, da von berufsständischer Seite darauf aufmerksam gemacht wurde. So macht auf diesen Umstand etwa der *Österreichische Rechtsanwaltskammertag* aufmerksam, der den Gesetzesentwurf aus mehreren Gründen umfassend ablehnt.⁶⁷⁵ Bei der Ermittlung von Daten aus nicht-öffentlichen Quellen wäre ein besonderer Schutz der Berufsgeheimnisträger in § 10 PStSG vorzunehmen, da es sich dort um die Regelung handelt, die den Zugriff auf die Daten ermöglicht. Allerdings unterliegt § 10 PStSG gerade keinen näheren Beschränkungen. Damit leidet das Gesetz an einem grundlegenden legislatischen Konstruktionsfehler. Vielmehr ist, wie die Vertreter des *AK-Vorrat* folgerichtig feststellen, der Zugriff der Ermittler umfassend. Hierbei sei vor allem hervorgehoben, dass die sog kleine Rasterfahndung nach § 141 Abs 2 StPO de facto ermöglicht wird, ohne sich

⁶⁷³ Wie etwa in Deutschland in den Polizeigesetzen des Bundes und der Länder durch Verweise auf Berufsgeheimnisträgervorschriften in der dStPO geschieht.

⁶⁷⁴ Auf diesen Umstand macht auch aufmerksam die Stellungnahme der Österreichischen Bischofskonferenz zum Gesetzesentwurf 110/ME XXV. GP, 2.

⁶⁷⁵ Stellungnahme des Österreichischen Rechtsanwaltskammertages zum Gesetzesentwurf 110/ME XXV. GP. So wird insbesondere bemängelt, dass der Gesetzesentwurf allgemein dazu geeignet ist, den Grundrechtsschutz der Bevölkerung auszuhöhlen und Überwachungsmaßnahmen der Kontrolle der ordentlichen Gerichte zu entziehen und stattdessen auf eine geheimdienstliche Ebene zu heben (zu finden auf Seite 2).

jedoch an die strengeren Vorgaben der StPO halten zu müssen.⁶⁷⁶ Bereits bestehende grundrechtliche Kritikpunkte im Bereich der StPO im Bereich des SPG werden im Entwurf zum PStSG noch verschärft.⁶⁷⁷

In mehreren Stellungnahmen wurde nach dem ersten Entwurf des Gesetzes um Ausnahmeregelungen für Berufsgeheimnisträger ersucht, da deren Rechte und die Rechte derjenigen, die sich an sie wenden, den Zielen des PStSG ohne Abwägung untergeordnet werden.⁶⁷⁸

Den Stellungnahmen war unbedingt beizupflichten. Der Berufsgeheimnisträgerschutz hatte nicht nur keine Berücksichtigung gefunden. Er wurde auch im Gegensatz zum TKG nicht einmal bedacht und auch für nicht notwendig erachtet. Der Gesetzgeber übergeht den Berufsgeheimnisträgerschutz in seinen Erläuterungen, als ob sich die Frage in diesem Kontext nicht stellen würde oder als ob der Berufsgeheimnisträgerschutz gar nicht existieren würde.⁶⁷⁹

Erst in quasi letzter Minute⁶⁸⁰ lenkte der Gesetzgeber doch noch ein und nahm einen Berufsgeheimnisträgerschutz in das Gesetz auf. Dies zeigt vor allem, dass es keinen Sinn machen kann, den Berufsgeheimnisträgerschutz in jedem Überwachungsgesetz neu zu verorten. Es kann nicht bei jedem Gesetz erneut der Schutz der Berufsgeheimnisse zur Disposition stehen und neu diskutiert werden.

⁶⁷⁶ Stellungnahme des Österreichischen Rechtsanwaltskammertages zum Gesetzesentwurf 110/ME XXV. GP., 5. Auf diese Tatsache macht ebenfalls aufmerksam die Stellungnahme des AK-Vorrat zum Gesetzesentwurf 110/ME XXV. GP., 42.

⁶⁷⁷ Auf diesen Umstand verweist etwa die Stellungnahme des AK-Vorrat zum Gesetzesentwurf 110/ME XXV. GP., 42.

⁶⁷⁸ Stellungnahme des Österreichischen Journalistenclubs zum Gesetzesentwurf 110/ME XXV. GP.; Stellungnahme des Generalsekretariats der Österreichischen Bischofskonferenz zum Gesetzesentwurf 110/ME XXV. GP., 2. Vgl insbesondere auch die Ausführungen des AK-Vorrat zum Redaktionsgeheimnis; Stellungnahme des AK-Vorrat zum Gesetzesentwurf 110/ME XXV. GP., 44.

⁶⁷⁹ Vgl Erläuterungen zum Gesetzesentwurf 110/ME XXV.

⁶⁸⁰ Vgl unten 28.1.4.3.

28.1.3. Weitere Kritikpunkte aus dem Bereich der Telekommunikationsüberwachung im PStSG

Die übermittelten Stellungnahmen sprechen eine klare Sprache. Auch unabhängig von dem mangelnden Schutz für Berufsgeheimnisträger finden sich viele Kritikpunkte. So wird oft allgemein kritisiert, dass völlig unklar scheine, was konkret ein verfassungsgefährdender Angriff sein soll, auf den der Gesetzesentwurf abstellt.⁶⁸¹ Auch leide der Gesetzesentwurf allgemein an Unschärfen.⁶⁸²

Ferner werde mit dem Gesetzesentwurf gegen bisherige Gesetzgebungssystematik verstoßen. Eine Auskunft über Verkehrsdaten wird im TKG ausschließlich über § 99 Abs 5 TKG abgewickelt. Der Gesetzesentwurf passt diesen aber nicht an, sondern regelt den Zugriff auf Daten des TKG in § 12 Abs 1 Z 7 PStSG selbst. Dieser widerspricht der bisherigen Systematik und schafft damit eine Rechtsunsicherheit.⁶⁸³

Ferner wird der nicht bestehende Richtervorbehalt bemängelt. Hierbei sei insbesondere der Rückgriff auf den Rechtsschutzbeauftragten nicht als gleichwertig anzusehen.⁶⁸⁴ Dieser und die weiteren Kritikpunkte können ebenfalls hilfreich sein, da hier zu klären sein wird, inwiefern diese Kritikpunkte nicht in einen Gesetzgebungsprozess einfließen müssten.

28.1.4. Reaktion des Gesetzgebers auf die vorgebrachten Kritikpunkte

Der Gesetzgeber hat auf die Kritikpunkte mit insgesamt zwei Überarbeitungen reagiert. Die erste Überarbeitung des Gesetzes enthielt hierbei nur marginale Anpassungen.⁶⁸⁵ Einzig beachtenswert im Rahmen der Telekommunikationsüberwachung war es

⁶⁸¹ Stellungnahme des AK-Vorrat zum Gesetzesentwurf 110/ME XXV. GP., 38.

⁶⁸² Stellungnahme der ISPA zum Gesetzesentwurf 110/ME XXV. GP., 2.

⁶⁸³ Vgl hierzu auch Stellungnahme der ISPA zum Gesetzesentwurf 110/ME XXV. GP., 3.

⁶⁸⁴ Stellungnahme der ISPA zum Gesetzesentwurf 110/ME XXV. GP., 4 mit Verweis auf *Burgstaller*, Sicherheitspolizeiliche Ermittlungshandlungen unter Kontrolle des Rechtsschutzbeauftragten beim BMI, Informationen zur Praxis 2010 und 2009, ÖJZ 2011, 644, 656. Vgl hierzu auch *Giese*, Sicherheitspolizeirecht in Bachmann ua (Hrsg), Besonderes Verwaltungsrecht⁵, überarbeitete und ergänzte Fassung, 31; *Zerbes*, Spitzeln Spähen Spionieren, 158.

⁶⁸⁵ Vgl hierzu die Gegenüberstellung des AK Vorrat, abrufbar unter http://akvorrat.at/sites/default/files/AKVorrat_PStSG_Stellungnahme_RV.pdf

hierbei, dass sensible Daten nach § 4 Z 2 DSG 2000 nur noch in Ausnahmefällen gespeichert werden dürfen. Bei der zweiten Überarbeitung ging der Gesetzgeber auf weitere Kritikpunkte ein und überarbeitete den Gesetzesentwurf stärker, ließ jedoch die Grundkonstruktion des Gesetzes unverändert, so dass grundsätzliche Kritikpunkte aufrecht bleiben.

28.1.4.1. Die erste Überarbeitung des Gesetzesentwurfs

In Bezug auf § 12 PStSG, nunmehr § 11 PStSG, hat man einzelne Überwachungsbefugnisse sogar explizit ausgedehnt.⁶⁸⁶ So ist die Ermittlung von IP-Adressen nach Z 5 nun gegen Gruppierungen möglich, was es leichter macht, in das Visier von Ermittlern zu geraten, wenn man einer bestimmten „Gruppierung“ angehört. Dies gilt im Übrigen auch für Daten, welche auf Grundlage des TKG ermittelt werden, da die Änderungen von Z 5 sinngemäß in Z 7 übernommen wurden. Im Ergebnis wurde nur der Zugriff auf Daten von Beförderungsunternehmen eingeschränkt.

Bezüglich des Schutzes der Berufsheimnisträger wurde die vorgebrachte Kritik vollkommen außer Acht gelassen. Dies überrascht aber insofern eher wenig, als dass der Gesetzgeber die Endfassung im Vergleich zum ersten Gesetzesentwurf eher verschärft als entschärft hat und sich der geäußerten Kritik nur sehr punktuell angenommen hat. Insofern hat sich auch durch die Stellungnahmen am fehlenden Berufsheimnisträgerschutz, trotz entsprechender Hinweise von verschiedenster Seite, in diesem Fall nichts geändert.

28.1.4.2. Die zweite Überarbeitung des Gesetzesentwurfs

In einer weiteren Überarbeitung ging der Gesetzgeber insofern auf die Kritiker des Gesetzes ein, als dass nunmehr nun noch ein Amt für Verfassungsschutz auf Bundesebene die Aufgaben des polizeilichen Staatsschutzes koordinieren soll.⁶⁸⁷ Eine Gegenüberstellung der Letztversion des Gesetzes zeigt aber, dass die Änderungen ansonsten nur marginaler Natur sind und für den Grundrechtsschutz keine echten

⁶⁸⁶ Gegenüberstellung des AK Vorrat, abrufbar unter http://akvorrat.at/sites/default/files/AKVorrat_PStSG_Stellungnahme_RV.pdf, 21 f.

⁶⁸⁷ Vgl. Parlamentskorrespondenz Nr. 1364 vom 01.12.2015, abrufbar unter https://www.parlament.gv.at/PAKT/PR/JAHR_2015/PK1364/index.shtml.

Verbesserungen bringen.⁶⁸⁸ Insbesondere bleiben die Überwachungsmöglichkeiten für die Ermittler unverändert. Ein echter Berufsgeheimnisträgerschutz findet ebenfalls nicht statt.

Als grundrechtliche Verbesserung hat die Regierung Änderungen im SPG präsentiert. So würde demnächst nicht der Rechtsschutzbeauftragte, sondern ein aus drei Personen bestehender „Rechtsschutzsenat“ entscheiden.⁶⁸⁹ Dies suggeriert, dass einem ein Gericht ähnliches neutrales Gremium in Zukunft die Aufgaben des Rechtsschutzbeauftragten wahrnimmt, was zu einem Mehr an Rechtsschutz und Rechtsstaatlichkeit führen würde. In Wirklichkeit bekommt der Rechtsschutzbeauftragte zwei Stellvertreter mit denen er sich abstimmen soll, aber nicht muss.⁶⁹⁰ Es ist weder Einstimmigkeit noch Entscheidung durch Stimmenmehrheit, bei der etwa die Stellvertreter den Rechtsschutzbeauftragten überstimmen könnten, gefordert. Ein verbesserter Grundrechtsschutz wurde mithin nicht erzielt. Hieran ändert auch die Tatsache nichts, dass zumindest ein Stellvertreter zehn Jahre Erfahrung als Richter oder Staatsanwalt haben muss und den beteiligten Personen getrennte Räumlichkeiten zur Verfügung gestellt werden.⁶⁹¹

28.1.4.3. Die dritte Überarbeitung des Gesetzesentwurfs

In einer dritten Überarbeitung hat die Regierungskoalition versucht, das Gesetz im Schulterschluss mit den Oppositionsparteien zu beschließen, was letztlich fehlschlug. Dennoch wurden einige Änderungen in das Gesetz eingearbeitet, die im Endeffekt zu einem höheren Grundrechtsschutz führen und auch die Probleme bezüglich der Berufsgeheimnisträger entschärfen. Das Gesetz wurde in dieser Überarbeitung letztlich vom Nationalrat beschlossen.

Die entscheidende Änderung ergibt sich im Wege des Berufsgeheimnisträgerschutzes. Dort wurde festgehalten, dass der in der StPO festgelegte Berufsgeheimnisträgerschutz nicht durch Maßnahmen nach dem PStSG umgangen werden darf, indem ein neuer § 9 Abs 1 PStSG aufgenommen wurde, in dem es heißt: „Bei Ermittlungen von

⁶⁸⁸ Vgl. Stellungnahme des AK-Vorrat vom 11.01.2016, *Kargl/Tschohl/Czadilek*, <https://akvorrat.at/sites/default/files/PStSG-3.pdf>, 35 f.

⁶⁸⁹ <http://derstandard.at/2000026665430/Neuer-Rechtsschutz-Senat-kommt-etwas-spaeter>.

⁶⁹⁰ *Kargl/Tschohl/Czadilek*, <https://akvorrat.at/sites/default/files/PStSG-3.pdf>, 31.

⁶⁹¹ *Kargl/Tschohl/Czadilek*, <https://akvorrat.at/sites/default/files/PStSG-3.pdf>, 35 f.

personenbezogenen Daten nach diesem Bundesgesetz ist ein Eingriff in das von § 157 Abs 1 Z 2 bis 4 StPO geschützte Recht nicht zulässig. § 157 Abs 2 StPO gilt sinngemäß.“

Dies ist insofern zu begrüßen, als dass damit der Schutz der Berufsgeheimnisse quasi in letzter Minute doch noch gewährleistet werden konnte. Dies zeigt jedoch, dass im Rahmen der Gesetzgebung die Rechte der Berufsgeheimnisträger stets von neuem verteidigt werden müssen und immer wieder neu bei jedem Gesetzgebungsverfahren zur Disposition stehen. Folglich ist darüber nachzudenken, wie diese Berufsgeheimnisse nachhaltig geschützt werden, so dass nicht bei jedem Gesetzgebungsverfahren neu um deren Schutz gekämpft werden muss. Da der Berufsgeheimnisträgerschutz nicht nur in der StPO von Bedeutung ist, ist hierbei eine gesonderte gesetzliche Verankerung unter Umständen angezeigt.

Wie der Schutz der Berufsgeheimnisträger dann praktisch abläuft, etwa über eine Whitelist, welche ja angeblich große rechtliche Probleme aufwirft,⁶⁹² wenn eine flächendeckende Überwachung gestützt auf das PStSG durchgeführt wird, darüber schweigen sich sowohl Gesetz als auch die Regierungsvorlage aus, so dass man hierüber nur mutmaßen kann.⁶⁹³ Daher bleibt es mit Spannung zu erwarten wie der VfGH dies bewerten wird.⁶⁹⁴

28.2. „Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden“ – Österreich

Mit der Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, plante der Gesetzgeber, in Anlehnung an bereits bestehende ähnliche Maßnahmen in Deutschland und als eine Art Anlassgesetzgebung als Reaktion auf jüngste Terroranschläge, eine heimliche Überwachung von Computersystemen mittels

⁶⁹² Vgl hierzu 14.3.

⁶⁹³ Dies kritisiert auch der AK-Vorrat in seiner abschließenden Stellungnahme zum PStSG, vgl *Kargl/Tschohl/Czadilek*, <https://akvorrat.at/sites/default/files/PStSG-4.pdf>, 11.

⁶⁹⁴ Grüne und FPÖ haben eine Beschwerde gegen das Gesetz, welches am 1. Juli 2016 in Kraft getreten ist, eingebracht; <http://news.orf.at/#/stories/2346791/>.

Trojaner.⁶⁹⁵ Das BMJ hatte hierfür bereits einen Begutachtungsentwurf erstellt.⁶⁹⁶ Hiermit wollte man unter anderen dem Phänomen begegnen, dass es mit heutigen technischen Methoden leicht möglich ist, Ende-zu-Ende-verschlüsselt zu kommunizieren, was ein „Abfangen“ der Nachricht auf dem Übertragungsweg unmöglich macht.⁶⁹⁷ Der hohen Eingriffsintensität wollte man damit begegnen, dass von der Überwachungsmethode zurückhaltend Gebrauch gemacht wird.⁶⁹⁸

Durch die Einbettung in das System der StPO konnte davon auszugehen sein, dass ein grundsätzlicher Berufsgeheimnisträgerschutz gegeben ist. Dieser musste in diesem Fall, anders als im PStSG, nicht gänzlich erkämpft werden. Jedoch zeigen sich auch hier massive Schwächen, auf die die Rechtsanwaltskammer auch zu Recht hinweist,⁶⁹⁹ da in „besonders schwerwiegenden Fällen“, ein Zugriff auf Berufsgeheimnisträger möglich sein soll, wenn dieser „verhältnismäßig erscheint“. Dies höhlt den Berufsgeheimnisträgerschutz völlig aus, da sich weder aus dem Gesetz noch aus den Erläuterungen ergab, was hierunter verstanden werden sollte, so dass der Schutz der Berufsgeheimnisträger letztlich zur Disposition des Rechtsschutzbeauftragten stand. Aus diesem Grund fordert die Rechtsanwaltskammer auch, dass Berufsgeheimnisträger ohne Ausnahme von der Maßnahme auszunehmen seien. Gleiche Bedenken erhebt auch der Verband Österrei-

⁶⁹⁵ Hierbei ging der Gesetzgeber fälschlicherweise davon aus, die Terroranschläge, welche im Jahr 2015 in Paris verübt wurden, seien auf einer internetfähigen Spielekonsole geplant worden und hätten mittels eines Überwachungstrojaners verhindert werden können. Näher hierzu *Kargl/Tschohl/Czadilek*, https://akvorrat.at/sites/default/files/AKVorrat_Stellungnahme_StPO%20A%CC%88nderung_Bundestrojaner.pdf, 26.

⁶⁹⁶ Bundesgesetz, mit dem die Strafprozessordnung 1975 und das Staatsanwaltschaftsgesetz geändert werden,

⁶⁹⁷ Vgl Erläuterungen zum Gesetzesentwurf 192/ME XXV, 1. Hierbei wird unter anderen der Fehlschluss gezogen, dass sich dies vor allem Kriminelle zunutze machen. Dies ist insofern lebensfern, als dass gerade Berufsgeheimnisträger oft darauf angewiesen sind, verschlüsselt zu kommunizieren um sich nicht dem Vorwurf aussetzen zu müssen, sie hätten die Aufdeckung einer vom Berufsgeheimnis geschützten Tatsache leichtfertig gefördert. Nebenbei lässt der Entwurf völlig außer Acht, dass es nurmehr eine Frage der Zeit ist, bis auch einfache, für die breite Masse der Nutzer zugängliche Software zugänglich ist, die es möglich macht, entsprechende staatliche Spionagesoftware auszuschalten. Erst recht wenn jemand sich dazu entschlossen hat, mittels des Internets Straftaten zu begehen, wird er eine solche Software zum Einsatz bringen und zwar bereits dann, wenn eine solche Software noch nicht für einen großen Nutzerkreis zur Verfügung steht, ohne dass hieran staatliche Stellen etwas ändern können.

⁶⁹⁸ Vgl Erläuterungen zum Gesetzesentwurf 192/ME XXV, 3.

⁶⁹⁹ Vgl Stellungnahme der Österreichischen Rechtsanwaltskammer zum Gesetzesentwurf 192/ME XXV, 6.

chischer Zeitungen, der als Lösungsmöglichkeit vorschlug, bei Überwachungsmaßnahmen einen Abgleich mit einer auf freiwilliger Basis geführten Liste durchzuführen und dies im Rahmen der Maßnahme besonders zu berücksichtigen.⁷⁰⁰

Der Gesetzesentwurf wies darüber hinaus, ebenso wie der Erstentwurf des PStSG, massive Schwächen auf und war insbesondere in Bezug auf die getroffenen Abwägungen, etwa dass eine heimliche Überwachung des Computers weniger eingriffsintensiv ist als eine Wohnraumüberwachung,⁷⁰¹ zurückzuweisen. Insbesondere schien sich der Gesetzgeber der Tatsache nicht bewusst zu sein, dass Durchsuchungen im Gegensatz zur Überwachung von Kommunikation normalerweise keine heimlichen Maßnahmen sind, sondern für den Betroffenen nachvollziehbar und – nach Möglichkeit – in dessen Anwesenheit erfolgen sollen.⁷⁰²

Beim Gesetzgebungsentwurf handelte es sich aus legistischer Sicht wohl um einen besonders schlechten „Schnellschuss“. Dies sah wohl letztlich sogar das BMJ selbst ein und nahm von einer Einführung des Bundestrojaners, zumindest mit dem anvisierten Gesetzesentwurf, Abstand.⁷⁰³

28.3. „Vorratsdatenspeicherung neu“ in Deutschland

Bestrebungen, die Vorratsdatenspeicherung auf europäischer Ebene durch eine Richtlinie wieder einzuführen gibt es – zumindest zurzeit – wohl nicht.⁷⁰⁴ Deutschland hat inzwischen jedoch im Alleingang eine Art „Vorratsdatenspeicherung neu“ einge-

⁷⁰⁰ Vgl. Stellungnahme der Österreichischen Rechtsanwaltskammer zum Gesetzesentwurf 192/ME XXV, 2f.

⁷⁰¹ Hierzu zu recht kritisch Kargl/Tschohl/Czadilek, https://akvorr.at/sites/default/files/AKVorrat_Stellungnahme_StPO%20A%CC%88nderung_Bundestrojaner.pdf, 33.

⁷⁰² So ist etwa gem § 121 Abs 2 S 1 StPO bei der Durchsuchung von Wohnungen, falls der Wohnungsinhaber nicht erreichbar ist und auch kein erwachsener Mitbewohner zur Verfügung steht, wenigstens die Beziehung zweier vertrauenswürdiger Personen erforderlich. Lediglich bei Gefahr im Verzug, kann hiervon abgewichen werden. Ein solcher Fall dürfte allerdings bei einer Online-Durchsuchung denklogisch nie vorliegen. Brauchen die Ermittler nämlich bei Gefahr im Verzug Zugriff auf ein elektronisches Endgerät des Verdächtigen, so bleibt Ihnen für eine Infiltrierung des Systems in der Regel zu wenig Zeit, so dass die Maßnahme letztlich ins Leere lief.

⁷⁰³ <http://derstandard.at/2000038486797/Justizministerium-legt-offenbar-Plaene-fuer-Bundestrojaner-auf-Eis>.

⁷⁰⁴ <http://futurezone.at/netzpolitik/planen-keine-neuregelung-zur-vorratsdatenspeicherung/127.600.036>.

führt, wenn auch die Bezeichnung Vorratsdatenspeicherung euphemistisch vermieden wird.⁷⁰⁵ Unabhängig von der verfassungsrechtlichen Beurteilung dieses Gesetzgebungsvorhabens wird dieses auch aus europarechtlicher Perspektive zu bewerten sein. Ferner ist zu untersuchen, inwiefern das Vorhaben die Belange des Berufsgeheimnisträgerschutzes berücksichtigt. Hierzu haben wie bereits gezeigt wurde, das BVerfG und der EuGH Vorgaben gemacht, die es umzusetzen gilt.

Grundsätzlich verbirgt sich hinter dem *Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten* ein umfangreiches Gesetzgebungspaket, mit dem mehrere bestehende Vorschriften geändert oder ergänzt werden.⁷⁰⁶ Die Speicherpflicht umfasst hierbei grundsätzlich sämtliche Verkehrsdaten, welche nach der vor dem Gesetzeserlass des Bundestages bestehenden Rechtslage grundsätzlich zu löschen waren, sobald diese vom Telekommunikationsunternehmen, bei dem diese anfielen, nicht mehr benötigt wurden. Sie beträgt für Verbindungsdaten zehn Wochen, für Standortdaten vier Wochen.⁷⁰⁷ Hierbei geht der Gesetzgeber davon aus, dass von Standortdaten ein höheres Missbrauchspotenzial als von Verbindungsdaten ausgeht und bringt dieses in zwei unterschiedlichen Speicherfristen zum Ausdruck. Ein weiterer Schwerpunkt des Gesetzgebungsverfahrens, der jedoch von der eigentlichen „Vorratsdatenspeicherung neu“ zu unterscheiden ist, ist die Einführung des Straftatbestandes der „Datenhehlerei“⁷⁰⁸ für die illegale Weitergabe oder Kopie rechtswidrig erlangter Daten.⁷⁰⁹

28.3.1. Zielsetzung der „Vorratsdatenspeicherung neu“

Ziel des Gesetzgebungsvorhabens ist, es eine „zeitlich befristeten Speicherung von Verkehrsdaten zur Strafverfolgungsvorsorge und zur Gefahrenabwehr“ zu ermögli-

⁷⁰⁵ Vgl BT-Drucksache 18/5088.

⁷⁰⁶ Vgl zum Ganzen auch Geuer, Das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten aus Sicht von Berufsgeheimnisträgern, AnwZert ITR 24/2015, Anm 2.

⁷⁰⁷ BT-Drucksache 18/5088, 28.

⁷⁰⁸ Dieser Straftatbestand soll als neuer § 202d dStGB eingeführt werden.

⁷⁰⁹ Hierin wird in Bezug auf Berufsgeheimnisträger für das Redaktionsgeheimnis eine Gefahr erblickt, da es nicht unüblich ist, dass sich etwa ein Informant mit rechtswidrig erlangten Informationen an einen Journalisten wendet, die dieser sich dann kopiert oder weitergibt. Durch diese Handlung wäre jedoch ebenfalls der Tatbestand der Datenhehlerei erfüllt. Es bleibt abzuwarten, ob hier nicht eine verfassungskonforme Auslegung entsprechende Einschränkungen gebietet. Näheres zu diesem neuen Straftatbestand vgl Esser in Hornung/Müller-Terpitz, Rechtshandbuch Social Media, 277 ff.

chen.⁷¹⁰ Dies sei auch verfassungsrechtlich geboten. Hierzu hält der Gesetzesentwurf in seiner Begründung folgendes fest:⁷¹¹

Das Bundesverfassungsgericht hat wiederholt das verfassungsrechtliche Gebot einer effektiven Strafverfolgung hervorgehoben, das Interesse an einer möglichst vollständigen Wahrheitsermittlung im Strafverfahren betont und die wirksame Aufklärung gerade schwerer Straftaten als einen wesentlichen Auftrag eines rechtsstaatlichen Gemeinwesens bezeichnet. [...] Der Gesetzesentwurf behebt die beschriebenen Unzulänglichkeiten in der Strafverfolgungsvorsorge und der Gefahrenabwehr. Durch die Speicherung der Verkehrsdaten für eine begrenzte Zeit werden zusätzliche Aufklärungsmöglichkeiten geschaffen, die der zunehmenden Bedeutung der Telekommunikation für die Vorbereitung und Begehung von Straftaten Rechnung tragen.

Der Gesetzgeber beklagt hierbei, dass es seit der Abschaffung der Vorratsdatenspeicherung, dem Zufall überlassen sei, ob die angefragten Daten beim Telekommunikationsanbieter noch vorhanden seien und dies einer effektiven Strafverfolgung entgegen stehe; der Zufallseffekt käme gleichsam dadurch zustande, dass manche Telekommunikationsanbieter Daten länger vorhielten als andere.⁷¹² Um dem entgegenzuwirken sei es notwendig, die (einheitliche) Speicherung einzuführen.

28.3.2. Datenerhebung im Bereich der Telekommunikation

In den Erläuterungen zur „Vorratsdatenspeicherung neu“ ist der Gesetzgeber sehr darum bemüht zu betonen, wie stark sich das Gesetzgebungsverfahren von der vom EuGH wegen Verstoß gegen die Charta der Grundrechte der Europäischen Union aufgehobene Richtlinie unterscheidet.

In der Tat unterscheidet sich das Gesetzgebungsvorhaben von dem, was in der Richtlinie gefordert wurde. Der Gesetzgeber hat gleichsam die Vorratsdatenspeicherung ausgehöhlt und eine abgeschwächte Version dieser geschaffen. Dies äußert sich in der

⁷¹⁰ BT-Drucksache 18/5088, 2.

⁷¹¹ BT-Drucksache 18/5088, 21 f mit Verweis auf BVerfGE 129, 208, 260.

⁷¹² BT-Drucksache 18/5088, 1 f.

geringeren Speicherdauer. Damit bleiben grundsätzliche grundrechtliche Problematiken bestehen.

28.3.3. Umsetzung des Berufsgeheimnisträgerschutzes bei der „Vorratsdatenspeicherung neu“

Wie bereits im Urteil des BVerfG und des EuGH festgehalten, stellt der Schutz der Berufsgeheimnisträger eine Voraussetzung für die Zulässigkeit der Speicherung dar. Dies heißt in letzter Konsequenz: Eine Überwachungsmaßnahme, die dies nicht gewährleisten kann, die also technisch nicht zwischen Berufsgeheimnisträgern und dem Rest der Bevölkerung unterscheiden kann, kann keine taugliche Überwachungsmaßnahme im rechtsstaatlichen Sinne sein. Ihre gesetzliche Umsetzung würde stets den verfassungsrechtlichen Vorgaben zuwiderlaufen.

Bei einer oberflächlichen Betrachtung mögen Zweifel an der Berücksichtigung grundrechtlicher Belange zunächst zerstreut werden. Zunächst erweckt der Gesetzgeber den Anschein, als sei ihm der Schutz der Berufsgeheimnisträger ein großes Anliegen. Nicht müde wird er in seinem Entwurf zu betonen, dass er diesem Rechnung getragen habe.

In § 100g dStPO regelt der Gesetzgeber die Erhebung von Daten bei Berufsgeheimnisträgern und führt ein entsprechendes Erhebungsverbot ein. Losgelöst vom Gesetzeswortlaut lässt dies vermuten, dass die Daten, die bei der Telekommunikation von Berufsgeheimnisträgern anfallen, gar nicht in die Hände von Ermittlern gelangen können, findet doch ihre „Erhebung“ gar nicht statt. Dies bedeutet jedoch in der Terminologie des Gesetzes nichts anderes als dass diese zunächst gespeichert werden, da sich die Erhebung von Daten nach der Terminologie des Gesetzes lediglich auf den nachträglichen Zugriff der Ermittler auf bereits beim Telekommunikationsanbieter gespeicherte Daten bezieht, mithin die Daten bereits angefallen sind und vom Anbieter für den vom Gesetz vorgesehenen Zeitraum vorgehalten werden.

Zurückhaltend war der Gesetzgeber, was Ausnahmen von der Speicherpflicht angeht: Von der Speicherung, welche in § 113b dTKG geregelt ist, sind nur die Daten nach § 113b Abs 6 dTKG ausgenommen. Dies sind jene, die nach § 99 Abs 2 dTKG in keinem Einzelverbindungsanweis aufscheinen dürfen, also nur jene Anschlüsse von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen. Diese

Daten werden in vielen Fällen Berufsgeheimnisträger betreffen, jedoch nur bestimmte wie etwa Seelsorger oder Psychologen. Im Ergebnis wird hier zwischen einzelnen Berufsgeheimnisträgern unterschieden, was problematisch ist.⁷¹³

Wenig überraschend begegnen Berufsverbände dieser Vorgehensweise mit Kritik: Zutreffend weist die Bundesrechtsanwaltskammer darauf hin, dass bereits die Speicherung und nicht erst die „Erhebung“, also eine Analyse der Daten durch Ermittlungspersonen, ein verfassungsrechtliches Problem darstelle.⁷¹⁴ Dem werde auch nicht dadurch abgeholfen, dass sich ein späteres Verwertungsverbot ergebe. Schließlich seien Verwertungsverbote dazu geschaffen, um illegales staatliches Handeln im Nachhinein zu unterbinden und gewissermaßen zu pönalisieren.⁷¹⁵ Mögen diese Daten auch nicht offiziell in die Ermittlungen mit einbezogen werden, so beeinflussen sie mit großer Wahrscheinlichkeit das Handeln der Ermittler. Dieser verfassungsrechtliche Aspekt sei offenkundig und werde vom Gesetzgeber in seinen Erläuterungen nicht weiter kommentiert. Der Bundesrechtsanwaltskammer ist zuzustimmen, dass dieser Aspekt gänzlich unberücksichtigt blieb und sich hierdurch ein verfassungsrechtliches Problem ergibt.

Ein wirksamer Berufsgeheimnisträgerschutz könne letztlich nur dann erfolgen, wenn Metadaten aus der Telekommunikation von Berufsgeheimnisträgern von der Speicherung ausgenommen seien. Dass dies nur schwer möglich sei, ist zurückzuweisen.⁷¹⁶ Auch bei einer generellen Speicherpflicht wäre es technisch implementierbar, Daten von Berufsgeheimnisträgern auszunehmen oder sogleich zu löschen. Ist dies technisch so nicht implementierbar, bedeute dies eben nicht, dass ein Verwertungsverbot die Lösung des Problems darstellt, sondern vielmehr, dass dann eine Vorratsdatenspeicherung sich rechtmäßig nicht umsetzen lässt.⁷¹⁷ Dass BVerfG und EuGH eine – wie auch immer geartete – Vorratsdatenspeicherung nicht für schlechthin grundrechtlich

⁷¹³ Vgl hierzu oben unter 15.2.2.

⁷¹⁴ Stellungnahme der Bundesrechtsanwaltskammer, 11.; so auch *Nachbaur*, Vorratsdatenspeicherung "light" - Rechtswidrig und allenfalls bedingt von Nutzen, ZRP 2015, 215, 216 mit Verweis auf BVerfG NJW 2014, 2169 2172

⁷¹⁵ Stellungnahme der Bundesrechtsanwaltskammer, 13.

⁷¹⁶ Stellungnahme der Bundesrechtsanwaltskammer, 16.

⁷¹⁷ *Nachbaur*, Vorratsdatenspeicherung "light" - Rechtswidrig und allenfalls bedingt von Nutzen, ZRP 2015, 215, 216.

unmöglich halten, bedeutet nicht, dass der Gesetzgeber sich nicht auch für bislang nicht beschrittene technische Lösungsmöglichkeiten öffnen muss. Gelingt dies aus technischen Gründen nicht, dann ist eine grundrechtskonforme Umsetzung der Vorratsdatenspeicherung aus technischen – nicht rechtlichen – Gründen unmöglich. Das Recht muss den Rahmen für die Technik vorgeben, nicht die Technik den Rahmen für das Recht.

28.3.4. Bewertung nach der Entscheidung des EuGH

In seiner jüngsten Entscheidung zur Überwachung von Telekommunikation in Schweden und im Vereinigten Königreich hat der EuGH dortige Vorratsdatenspeicherungsregelungen für mit der Charta der Grundrechte unvereinbar erklärt.⁷¹⁸ Der Gerichtshof hält damit seine bereits bekannte Kritik an der Vorratsdaten nicht nur aufrecht, sondern bezieht klar Stellung, dass er – anders als etwa das Bundesverfassungsgericht in Deutschland⁷¹⁹ – eine flächendeckende, verdachtsunabhängige Telekommunikationsüberwachung mit höherrangigem Recht für unvereinbar ansieht.

Der EuGH legt hierzu Regelungen der RL 2002/58, dort vor allem Art. 15 und die Erwägungsgründe, im Lichte von Art 7, 8 und auch 11 GRC aus und hebt hervor, dass „eine derartige Maßnahme [Anm.: wie die Vorratsdatenspeicherung] in einem „strikt“ angemessenen Verhältnis zum intendierten Zweck stehen muss.“⁷²⁰ Hierbei reicht eine allgemeine Bedrohung durch schwere Kriminalität, etwa organisierte Kriminalität und Terrorismus, nicht aus.⁷²¹ Eine allgemeine und unterschiedslose Speicherung von Verkehrs- oder Standortdaten ist damit aus Sicht der Grundrechtecharta ausgeschlossen; sie ist in der Form immer unverhältnismäßig.⁷²²

Damit sollte auch aus deutscher Sicht klar sein, dass das Bundesverfassungsgericht nicht umhin kommt, die Vorschriften zur Vorratsdatenspeicherung neu für nichtig zu erklären. Allerdings wäre der Gesetzgeber im Sinne einer Selbstkontrolle gut bera-

⁷¹⁸ EuGH C-203/15, C-698/15.

⁷¹⁹ Das BVerfG hatte etwa eine Vereinbarkeit von Vorratsdatenspeicherung und GG nicht schlechthin ausgeschlossen, vgl hierzu

⁷²⁰ EuGH C-203/15, C-698/15, Rz 95.

⁷²¹ EuGH C-203/15, C-698/15, Rz 108.

⁷²² EuGH C-203/15, C-698/15, Rz 112.

ten, die beschlossenen Regelungen außer Kraft zu setzen, um einer gerichtlichen Entscheidung zuvor zu kommen.

Derweil liegt dem EuGH bereits ein Vorabentscheidungsersuchen des Protodikeio Rethymnis, eines griechischen Gerichts, vor, welches sich mit der dortigen Vorratsdatenspeicherung beschäftigt, da es die Vereinbarkeit eines Zugriffs auf Daten bei Verdacht auf eine Straftat durch die Polizei mit Art 7 und 8 GRC bezweifelt.⁷²³ Auch bei der Beantwortung dieser Frage dürfte der EuGH zu dem Schluss kommen, dass eine Vereinbarkeit nicht gegeben ist.

28.3.5. Erste gerichtliche Entscheidung

Nach zutreffender Auffassung des OVG Münster verstößt die Vorratsdatenspeicherung neu gegen europarechtliche Vorschriften.⁷²⁴ Auf den Eilantrag eines Providers⁷²⁵ kam das OVG Münster zu dem Ergebnis, das nach Auslegung von Art. 15 Abs. 1 der Datenschutzrichtlinie im Lichte der Rechtsprechung des EuGH zur Vorratsdatenspeicherungsrichtlinie die Vorratsdatenspeicherung neu, zumindest in der vom Gesetzgeber in Deutschland gewählten Form, voraussichtlich nicht mit der Datenschutzrichtlinie vereinbar ist; zumindest ist es dem Provider unzumutbar, bis zur Entscheidung in der Hauptsache abzuwarten. Der Provider sei damit – bis zur Entscheidung des Verfahrens – nicht an diese Regelung gebunden. Hierbei hielt das OVG Münster insbesondere fest:⁷²⁶

In der Auslegung, die Art. 15 Abs. 1 der Richtlinie 2002/58/EG durch den Gerichtshof der Europäischen Union gefunden hat, steht die Vorschrift einer nationalen Regelung zur Vorratsdatenspeicherung wie der hier zu beurteilenden deutschen Regelung jedenfalls dann entgegen, wenn die Speicherpflicht - unabhängig von einer nur auf die Verfolgung schwerer Straftaten bzw. die Abwehr schwerwiegender Gefahren für die öffentliche Sicherheit beschränkten und unter

⁷²³ EuGH, C-475/16.

⁷²⁴ OVG Münster v 22.06.2017, Az. 13 B 238/17.

⁷²⁵ Vgl. auch die Pressemitteilung des Providers bzw. des Branchenverbandes eco unter <https://www.eco.de/2017/pressemitteilungen/erste-bremse-fuer-die-vorratsdatenspeicherung-von-eco-unterstuetzte-klage-erzielt-etappensieg-im-einstweiligen-rechtsschutz.html>.

⁷²⁶ OVG Münster v 22.06.2017, Az. 13 B 238/17.

einem strikten Richtervorbehalt stehenden Zugriffsmöglichkeit der Sicherheitsbehörden auf die gespeicherten Daten sowie ausreichender Vorkehrungen zur Datensicherheit- keinerlei Zusammenhang zwischen den auf Vorrat zu speichernden Daten und dem durch das Gesetz verfolgten Zweck der Bekämpfung schwerer Straftaten bzw. der Abwehr schwerwiegender Gefahren für die öffentliche Sicherheit verlangt, sondern unterschiedslos ohne jede personelle, zeitliche oder geographische Begrenzung sämtliche Nutzer der von § 113b TKG erfassten Telekommunikationsmittel erfasst:

Im Einzelnen hat der Gerichtshof diese Anforderungen einer an den Grundrechten aus Art. 7, 8 und 11 sowie Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union orientierten Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58/EG entnommen. Das Erfordernis einer grundrechtsorientierten Auslegung ergibt sich bereits unmittelbar aus der Regelung in Art. 15 Abs. 1 Satz 3 der Richtlinie 2002/58/EG, die ausdrücklich bestimmt, dass alle nach dieser Vorschrift ergriffenen Maßnahmen den allgemeinen Grundsätzen des Gemeinschaftsrechts, einschließlich den in Art. 6 Abs. 1 und 2 des Vertrages über die Europäische Union niedergelegten Grundsätzen entsprechen müssen, zu denen neben den sog. allgemeinen Grundsätzen des Unionsrechts auch die Grundrechte gehören, die nunmehr durch die Charta der Grundrechte der Europäischen Union gewährleistet werden. Aus dem 2. Erwägungsgrund der Richtlinie folgt dabei, dass der Unionsgesetzgeber mit der Richtlinie insbesondere den Schutz des durch Art. 7 der Charta garantierten Rechts jeder Person auf Achtung ihres Privatlebens und des durch Art. 8 der Charta garantierten Rechts jeder Person auf Schutz der sie betreffenden personenbezogenen Daten achten will, so dass die Auslegung des Art. 15 Abs. 1 der Richtlinie in erster Linie anhand dieser Grundrechte zu erfolgen hat. Zu berücksichtigen ist zudem das durch Art. 11 der Charta garantierte Recht auf freie Meinungsäußerung, das eine der wesentlichen Grundlagen einer demokratischen und pluralistischen Gesellschaft darstellt, die zu den Werten gehört, auf die sich die Europäische Union nach Art. 2 des Vertrages über die Europäische Union gründet. Eine Einschränkung der genannten Grundrechte muss nach Art. 52 Abs. 1 der Charta gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen der Ausübung dieser Rechte und Frei-

heiten nur vorgenommen werden, wenn sie erforderlich und von der Europäischen Union anerkannten, dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen. Dieser letzte Gesichtspunkt wird dabei durch Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58/EG insoweit aufgegriffen, als dass die Mitgliedstaaten eine Vorschrift erlassen können, die von dem Grundsatz der Vertraulichkeit von Kommunikation und der damit verbundenen Verkehrsdaten abweicht, sofern dies in Anbetracht der dort genannten Ziele „in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig“ ist.

Es ist davon auszugehen, dass auch weitere Provider nun im Eilverfahren auf dem Verwaltungsrechtsweg gegen die Vorratsdatenspeicherung vorgehen. Die Entscheidung hat auch durchaus eine starke Präjudizwirkung auf die Hauptsache, da ansonsten eine Anordnung wie diese im Eilverfahren gar nicht ergehen dürfte. Da ein Vorgehen weiterer Provider auf dem gleichen Rechtsweg am Sitz der Bundesnetzagentur in Bonn – hier ist das VG Köln und in weiterer Instanz das OVG Münster zuständig – wahrscheinlich ist, dürfte die Vorratsdatenspeicherung damit in Deutschland gekippt sein, zumal die zuständige Bundesnetzagentur, welche die Aufsicht über die Provider ausübt, angekündigt hat, die Vorratsdatenspeicherung als Reaktion auf die Entscheidung mit sofortiger Wirkung auszusetzen.⁷²⁷ Provider können die Kosten, die ihnen durch die Vorratsdatenspeicherung entstanden sind, bei der Bundesnetzagentur geltend machen.

Die Ankündigung der Bundesnetzagentur verpflichtet Provider zwar nicht zur Aussetzung der Vorratsdatenspeicherung, allerdings kündigten die führenden Provider umgehend an, ab sofort keine Speicherung von Vorratsdaten mehr vorzunehmen.⁷²⁸

⁷²⁷

https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS.html

⁷²⁸ <https://www.heise.de/newsticker/meldung/Bundesnetzagentur-setzt-Vorratsdatenspeicherung-aus-3757527.html>.

28.4. BKA-Gesetz - Deutschland

Deutschland hat, neben den Befugnissen in den Polizeigesetzen der Länder und des Bundes und den strafprozessualen Befugnissen noch spezielle Eingriffsnormen für Ermittler des Bundeskriminalamts geschaffen.⁷²⁹ Dort ist etwa auch die Online-Durchsuchung mittels Trojaner als spezielle Norm vorgesehen, weiters finden sich dort viele Befugnisse zur Telekommunikationsüberwachung, die denen in den Landespolizeigesetzen und der dStPO zumindest ähnlich sind. Das BVerfG hat dieses Gesetz im April 2016 teilweise für verfassungswidrig erklärt.⁷³⁰ Die Entscheidung des BVerfG es enthält einige interessante Aspekte, die zeigen, dass das Gericht der Ansicht ist, den „Kernbereich“ neu zu bestimmen und ihm eine modernere, weniger statische Form zu geben. Außerdem lassen sich aus einigen Aussagen im Bereich des Berufsgeheimnisträgerschutzes wertvolle Erkenntnisse ziehen.

28.4.1. Vergleichbarkeit von Kernbereichsschutz und Berufsgeheimnisträgerschutz

Bereits in einem der Leitsätze, hebt das Gericht hervor, wie wichtig der Schutz des Kernbereichs der privaten Lebensgestaltung und der Berufsgeheimnisträger ist und nennt dabei beide in einem Atemzug:⁷³¹

Befugnisse, die tief in das Privatleben hineinreichen, müssen auf den Schutz oder die Bewehrung hinreichend gewichtiger Rechtsgüter begrenzt sein, setzen voraus, dass eine Gefährdung dieser Rechtsgüter hinreichend konkret absehbar ist, dürfen sich nur unter eingeschränkten Bedingungen auf nichtverantwortliche Dritte aus dem Umfeld der Zielperson erstrecken, verlangen überwiegend besondere Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung sowie einen Schutz von Berufsgeheimnisträgern, unterliegen Anforderungen an Trans-

⁷²⁹ Vgl hierzu auch die Tabelle unter 7.4. Früher waren Beamte des Bundeskriminalamtes ausschließlich in der Strafverfolgung tätig. Im Jahr 2009 erweiterte der Gesetzgeber den Aufgabenbereich des Bundeskriminalamts auf Tätigkeiten im Rahmen der Gefahrenabwehr, wobei die Beamten im Regelfall nur in seltenen Fällen tätig werden, wenn länderübergreifende Gefahren vorliegen.

⁷³⁰ BVerfG v 20.04.2016, 1 BvR 966/09, 1 BvR 1140/09; vgl auch eine erste Analyse hierzu *van Ljinden*, Mit Korrekturen zurück, LTO v. 20.4.2016.

⁷³¹ BVerfG v 20.04.2016, 1 BvR 966/09, 1 BvR 1140/09, dort Leitsatz 1b).

parenz, individuellen Rechtsschutz und aufsichtliche Kontrolle und müssen mit Löschungspflichten bezüglich der erhobenen Daten flankiert sein.

Das BVerfG stellt damit zunächst die Grundaussage des Urteils voran, nämlich dass der Gesetzgeber bei so weitreichenden Maßnahmen Transparenz, individuellen Rechtsschutz, Aufsichts-Kontrolle und Löschungspflichten bezüglich der erhobenen Daten zu bedenken hat. Hier gibt das Gericht dem Gesetzgeber eine Art Maßnahmenkatalog an die Hand. Zudem zeigt sich, dass beides, Berufsgeheimnisträgerschutz auf der einen und Schutz des Kernbereichs privater Lebensgestaltung auf der anderen Seite auf gleicher Stufe stehen und zu deren Schutz gleichartige Maßnahmen herangezogen werden müssen. Es dürfte entschieden sein, dass zwischen Berufsgeheimnisträgerschutz und dem Schutz des Kernbereichs privater Lebensgestaltung Parallelen bestehen und sich vieles aus dem Schutz des Kernbereichs privater Lebensgestaltung auf den Schutz der Berufsgeheimnisträger übertragen lässt.

28.4.2. Die Bedeutung einer „unabhängigen Vorabkontrolle“

Besonders hervorzuheben ist die Tatsache, dass das Gericht eine unabhängige Vorabkontrolle fordert, sofern in den Kernbereich eingegriffen wurde. Das Gericht bezieht hierbei zunächst Stellung zum unbeabsichtigten Eindringen in den Kernbereich, der nach zutreffender Ansicht nie ganz verhindert werden könne.⁷³² Der Gesetzgeber habe aber, was im BKAG nicht in ausreichender Form der Fall sei, Maßnahmen zu treffen, dass solche Eingriffe nicht geschehen. Hierbei geht das Gericht sogar soweit, dass eine Prüfung stattzufinden habe, bevor bestimmtes Material in die Hände von Ermittlern gelangt. Dies ist in dieser Deutlichkeit ein Novum und führt zu einer zusätzlichen Prüfung durch eine Kontrollinstanz bei bestimmten Eingriffen, um einen Eingriff in den Kernbereich auszuschließen. Hier zu führt das BVerfG aus:⁷³³

Auf der Ebene der Datenerhebung ist bei verletzungsgeneigten Maßnahmen durch eine vorgelagerte Prüfung sicherzustellen, dass die Erfassung von kernbereichsrelevanten Situationen oder Gesprächen jedenfalls insoweit ausgeschlossen

⁷³² BVerfG v 20.04.2016, 1 BvR 966/09, 1 BvR 1140/09, Rz 124, mit Verweis auf BVerfGE 120, 274, 337 f.

⁷³³ BVerfG v 20.04.2016, 1 BvR 966/09, 1 BvR 1140/09, Rz 128 f.

ist, als sich diese mit praktisch zu bewältigendem Aufwand im Vorfeld vermeiden lässt. Für Gespräche mit Personen höchstpersönlichen Vertrauens kann unter Umständen, die typischerweise auf eine vertrauliche Situation hinweisen, die Vermutung geboten sein, dass sie dem Kernbereichsschutz unterfallen und nicht überwacht werden dürfen. [...] Auf der Ebene der Auswertung und Verwertung hat der Gesetzgeber für den Fall, dass die Erfassung von kernbereichsrelevanten Informationen nicht vermieden werden konnte, in der Regel die Sichtung der erfassten Daten durch eine unabhängige Stelle vorzusehen, die die kernbereichsrelevanten Informationen vor deren Verwendung durch die Sicherheitsbehörden herausfiltert. [...] Die Erforderlichkeit einer solchen Sichtung hängt von der Art sowie gegebenenfalls auch der Ausgestaltung der jeweiligen Befugnis ab. Dabei kann auf die Sichtung durch eine unabhängige Stelle umso eher verzichtet werden, je verlässlicher schon auf der ersten Stufe die Erfassung kernbereichsrelevanter Sachverhalte vermieden wird und umgekehrt. [...] In jedem Fall hat der Gesetzgeber die sofortige Löschung von gegebenenfalls erfassten höchstpersönlichen Daten vorzusehen und jegliche Verwendung auszuschließen. Die Löschung ist in einer Weise zu protokollieren, die eine spätere Kontrolle ermöglicht.

Damit ist sich das Gericht der Tatsache bewusst, dass es immer vorkommen kann, dass eine Ermittlungsmaßnahme heimlicher Natur in den Kernbereich eingreift, obwohl dies von den Ermittlern nicht einmal beabsichtigt war. Es nimmt diese Tatsache aber nicht einfach als gegeben hin, sondern zeigt Auswege aus diesem grundrechtlichen Dilemma, auch wenn es dabei sehr vage bleibt. Die Sichtung durch eine unabhängige Stelle, welche im Übrigen in den Sondervoten zur Entscheidung als wenig praxisnah kritisiert wird,⁷³⁴ stellt aus grundrechtlicher Sicht sicher eine gute Lösung dar. Auf diese Weise kann zwar nicht in jedem Fall die Aufzeichnung kernbereichsrelevanter Sachverhalte vermieden werden, aber eine Kenntnisnahme durch die mit dem Fall befassten

⁷³⁴ So sieht etwa das Sondervotum von *Schluckebier* die „unabhängige Stelle“ als für die Gefahrenabwehr komplett ungeeignet an, weil Eilbedürftigkeit, im Gegensatz zu strafprozessualen Ermittlungen, eher die Regel als die Ausnahme sein wird; vgl BVerfG v 20.04.2016, 1 BvR 966/09, 1 BvR 1140/09, abweichende Meinung 2, Rz 15 ff.

Ermittler wird hierdurch verhindert. Diese können das Beweismaterial sichten, ohne von kernbereichsrelevanten Informationen eventuell beeinflusst zu werden.⁷³⁵

28.4.3. Kernbereichsrelevante Eingriffe außerhalb des Wohnraums

Ferner hält das BVerfG fest, dass Eingriffe in den Kernbereich auch außerhalb von Wohnungen stattfinden können.⁷³⁶ Der Gesetzgeber hat also auch bei Überwachungen außerhalb von Wohnungen dafür Sorge zu tragen, dass gesetzliche Vorschriften den Kernbereich entsprechend absichern.⁷³⁷

Es lassen sich also zum einen die Parallelen des Kernbereichs- und des Berufsgeheimnisträgerschutzes nicht von der Hand weisen und zum anderen ist die Tatsache anerkannt worden, dass allein dann, wenn sich eine Person außerhalb einer Wohnung befindet, dies noch nichts über den Kernbereich aussagt, dieser also sehr wohl bei Maßnahmen außerhalb von Wohnungen bedacht werden muss. Außerdem wird der Tatsache Rechnung getragen, dass auch im Rahmen von Beweisverwertungsverbieten die Ermittler, von den Beweisen beeinflusst werden können, welche sie letztlich nicht verwenden dürfen.

28.5. Arbeitsprogramm der Bundesregierung 2017/2018 – Österreich

Die Bundesregierung hat im Jänner 2017 für die Zeit bis zur nächsten Nationalratswahl, welche planmäßig im Herbst 2018 stattfinden sollte, das Arbeitsprogramm „Für Österreich“ beschlossen,⁷³⁸ welches auch Details zur Telekommunikationsüberwachung und zum Richtervorbehalt enthält. Die legislative Umsetzung der einzelnen

⁷³⁵ Näher hierzu BVerfG v 20.04.2016, 1 BvR 966/09, 1 BvR 1140/09, Rz 224. Letztlich hat der Gesetzgeber einen großen Gestaltungsspielraum bei der Ausgestaltung der „unabhängigen Stelle“. Hierbei kann es sich auch um eine besondere behördeninterne Abteilung handeln, die besonderen Vertraulichkeitsvereinbarungen unterliegt. Entscheidend ist nach Sicht des Gerichts, dass die unmittelbar mit der Ermittlung befassten Personen, die kernbereichsrelevanten Informationen nach Möglichkeit nicht zu Gesicht bekommen. Hierbei ist sich das Bundesverfassungsgericht der Tatsache bewusst, dass bei bestimmten Fallkonstellationen, etwa bei Eilbedürftigkeit wegen Gefahr im Verzug, hiervon u.U. auch abgewichen werden muss.

⁷³⁶ BVerfG v 20.04.2016, 1 BvR 966/09, 1 BvR 1140/09, Rz 175 f.

⁷³⁷ BVerfG v 20.04.2016, 1 BvR 966/09, 1 BvR 1140/09, Rz 176.

⁷³⁸ Abrufbar unter <http://archiv.bundestkanzleramt.at/DocView.axd?CobId=65201>, im Folgenden referenziert als Arbeitsprogramm.

Gesetze sollte zur Gänze noch heuer erfolgen. Nachdem sich die Koalitionspartner allerdings auf eine Neuwahl im Oktober 2017 geeignet hatten, dürften die meisten Vorschläge in der Form vorerst nicht zur Umsetzung kommen. Letztlich zeigt sich aber durch das Programm gleichsam, in welche Richtung die Gesetzgebung im Bereich Überwachung gehen könnte, zumal davon auszugehen ist, dass wenigstens eine der bisherigen Koalitionsparteien auch an der nächsten Bundesregierung beteiligt sein wird.

Im Kapitel „Sicherheit und Integration“ des Arbeitsprogramms⁷³⁹ finden sich unter „Strafrechtspaket zwei Maßnahmen, die Telekommunikationsüberwachung betreffen:⁷⁴⁰ zum einen das „Quick-Freeze“-Verfahren und zum anderen die „Ermöglichung der Überwachung internetbasierter Kommunikation“.

Während das Quick-Freeze-Verfahren ein Verfahren ist, das als Alternative zu einer anlasslosen Datenspeicherung in jedem Fall gegen die GRC verstößt, bietet sich das „Quick-Freeze“-Verfahren, bei dem Daten bei einem Anfangsverdacht gespeichert werden und bei Erhärtung des Verdachts nach richterlicher Freigabe herausgegeben werden, als grundrechtskonforme Alternative an. Insofern ist zu begrüßen, dass man, im Gegensatz zu anderen Ländern, hier nicht auf eine Massenüberwachung setzen möchte. Inwiefern es hier zu Ausnahmen für Berufsgeheimnisträger kommt, bleibt abzuwarten.

28.5.1. „Quick-Freeze“-Verfahren

Nach dem Ministerialentwurf⁷⁴¹ soll beim „Quick-Freeze“-Verfahren die Löschverpflichtung auf Anordnung der Staatsanwaltschaft für den Zeitraum von 12 Monaten aufgehoben werden (§ 99 Abs 1a TKG-E), was dazu führt, dass Verbindungsdaten eines bestimmten Anschlusses zunächst weiter gespeichert werden. Eine solche Anordnung soll in den Fällen des § 135 Abs 2 Z 2 bis 4 StPO zulässig sein. Eine Einsichtnahme in die Daten soll auf richterliche Anordnung erfolgen, ebenfalls nach den Voraussetzungen

⁷³⁹ Arbeitsprogramm, 23 ff.

⁷⁴⁰ Arbeitsprogramm, 24.

⁷⁴¹ 326/ME XXV. GP.

des § 135 Abs 2 Z 2 bis 4 StPO (§ 99 Abs 1b TKG-E). Nach den Erläuterungen zum Ministerialentwurf will man damit der Staatsanwaltschaft die Möglichkeit an die Hand geben, bei einem Anfangsverdacht Daten sichern zu lassen und bei Erhärtung des Verdachts mit richterlicher Anordnung darauf zuzugreifen. Warum diese Vorstellung nicht in den Gesetzestext eingeflossen ist, sondern der Gesetzgeber auf die exakt gleichen Voraussetzungen Bezug nimmt, wird nicht weiter ausgeführt. Damit wird die Tatsache übersehen, dass der Grundrechtseingriff nicht bereits bei Einsichtnahme in die gespeicherten Daten erfolgt, sondern bereits bei deren Speicherung. Alle Probleme, die sich bereits für Berufsgeheimnisträger bei anderen Überwachungen nach der StPO stellen, stellen sich bei dieser Art der Überwachung ebenfalls.

28.5.2. Überwachung verschlüsselter Kommunikation und IMSI-Catcher in der StPO

Weiters wurde ein Ministerialentwurf⁷⁴² zur Überwachung verschlüsselter Kommunikation eingebracht. Ein Beschluss des Nationalrates scheint nach Uneinigkeit in der aktuellen Regierungskoalition fraglich.⁷⁴³ Kern des sog Sicherheitspakets ist die Einführung des IMSI-Catchers⁷⁴⁴ in der StPO (§ 134 Z 2a StPO-E) und die Überwachung verschlüsselter Nachrichten (§ 135a StPO-E).

Die Überwachung mittels IMSI-Catcher war bislang eine Maßnahme, die lediglich im SPG geregelt war. Diese Maßnahme soll nunmehr in die StPO übernommen werden. Diese Maßnahme lässt insbesondere vermissen, wie das Mithören oder Mitlesen von Inhalten von Telekommunikation wirksam verhindert werden soll, zumal der IMSI-Catcher ja eine normale Funkzelle simuliert.

Bei der Überwachung verschlüsselter Nachrichten will man dem Phänomen Rechnung tragen, dass ein Großteil der Kommunikation (etwa über VoIP-Telefonie aber auch Textnachrichten über Messaging-Apps) heutzutage automatisch Ende-zu-Ende-

⁷⁴² 325/ME XXV. GP.

⁷⁴³ Zunächst signalisierte die SPÖ am 20. Juli 2017 ihre Zustimmung zum Sicherheitspaket (<http://derstandard.at/2000061570381/Sicherheitspaket-SPOe-steht-hinter-Whatsapp-Ueberwachung>), widerrief diese dann aber wieder (<http://orf.at/stories/2400872/2400880/>). Zumindest dürfte die Uneinigkeit so groß sein, dass ein Beschluss mit absoluter Mehrheit nach jetzigem Stand ausgeschlossen scheint.

⁷⁴⁴ Vgl unter 7.1.2.

verschlüsselt ist und es für außenstehende während des Kommunikationsvorgangs nicht, oder nur mit stark erhöhtem Aufwand, möglich ist, diese Kommunikation überwachen. Demgemäß möchte man am Endgerät mittels Trojaner und Quellen-Telekommunikationsüberwachung ansetzen, um die Nachrichten bereits vor dem Telekommunikationsvorgang abzufangen. Der Gesetzesentwurf geht unter anderem davon aus, dass ein Zugriff auf verschlüsselte Nachrichten unter gleichen Voraussetzungen möglich sein soll, wie ein Zugriff auf Nachrichten während des Telekommunikationsvorgangs, was daran erkennbar wird, dass beide Vorschriften gleich aufgebaut sein. Hierbei wird in der Erläuterung zum Ministerialentwurf⁷⁴⁵ unter anderem verkannt, dass die Eingriffsintensität ungleich stärker ist, wenn zunächst in den häuslichen Bereich des Überwachten eingedrungen werden muss, sei es physisch oder mittels rein technischen Methoden, um ein bestimmtes Endgerät zu infiltrieren. Völlig offen bleibt zudem die Frage, wie die entsprechende Ermittlungssoftware sich rein auf Nachrichten beschränkt und wie diese verhindert, dass die Überwachung zu einer Online-Durchsuchung⁷⁴⁶ wird, da diese nur Transportverschlüsselungen decodieren darf, nicht aber die Verschlüsselung von Dokumenten, die lediglich am Endgerät verfügbar sind und nicht für den Versand mittels Telekommunikation bestimmt sind. Wie bei allen Arten der Überwachung nach der StPO stellen sich auch hier dieselben berufsgeheimnisträgerspezifischen Probleme.

28.6. Überwachungspaket neu - Deutschland

In einem wohl nicht mehr zu überbietenden legislativen Dilettantismus hat der Bundestag am 22.06.2017 unter dem Schlagwort „Fahrverbot als Nebenstrafe“ ein umfangreiches Überwachungspaket beschlossen, in welches in letzter Minute ein umfassender Einsatz eines Staatstrojaners beschlossen wurde.⁷⁴⁷ Anscheinend fehlte

⁷⁴⁵ Erläuterungen zu 325/ME XXV. GP, 6.

⁷⁴⁶ Vgl hierzu unter 7.1.7.

⁷⁴⁷ BT-Drs 18/11272; in der Pressemitteilung zunächst unter dem Titel „Fahrverbot als Nebenstrafe“ aufgeführt (https://www.bundestag.de/presse/hib/2017_03/-/499646) und erst später als „Spionagesoftware für Ermittler“ bezeichnet (https://www.bundestag.de/presse/hib/2017_06/-/511304). Die entscheidende Änderung von § 100a dStPO und weiterer strafprozessualer Vorschriften erfolgte erst über einen Änderungsantrag der Regierungsfractionen zum eigentlichen Gesetzesentwurf und in einer Formulierungshilfe (Dokument abrufbar unter https://cdn.netzpolitik.org/wp-upload/2017/06/2017-06-19_Rechtsausschuss_18-6-361_Aenderungsantrag_GroKo_StPO-Reform.pdf).

dem Gesetzgeber der Mut, das Thema der staatlichen Überwachung offen anzusprechen.⁷⁴⁸ Im Übrigen bleibt auch das Reizwort Trojaner in der Gesetzesbegründung unerwähnt.

Hierbei setzt sich der Gesetzgeber klar über die vom Bundesverfassungsgericht festgelegten Leitlinien zum Einsatz von Trojanern durch das Bundeskriminalamt hinweg. Das Gericht hielt nämlich in seiner Grundsatzentscheidung folgendes fest:⁷⁴⁹

Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.

Die Änderungen der dStPO sehen nunmehr allerdings eine Quellen-Telekommunikationsüberwachung (neuer § 100a dStPO) und Online-Durchsuchung (neuer § 100b dStPO) auf breiter Basis vor, nicht nur in wenigen Einzelfällen. Der Gesetzgeber sieht hierbei die zunehmende Verschlüsselung im Rahmen der Telekommunikation als Problem, dem er mit dem Zugriff direkt am Endgerät begegnen möchte.

Aus Sicht der Berufsgeheimnisträger hält das Überwachungspaket einige Punkte bereit, die zurecht für Kritik sorgen. Neben der allgemeinen Kritik an der Überwachung, die in der Form schon wegen mangelnder Verhältnismäßigkeit als verfassungswidrig anzusehen ist, kritisiert der Deutsche Anwaltsverein etwa die Unterscheidung zwischen Berufshelfern und dem Berufsgeheimnisträger selbst. So soll ein Mail im Mailpostfach des Strafverteidigers nicht im Rahmen eines heimlichen Zugriffs ausgespäht werden

⁷⁴⁸ Vgl etwa die Kritik des Deutschen Anwaltsvereins zum „heimlichen Gesetzgebungsverfahren“ (https://anwaltverein.de/de/newsroom/sn-44-17-einfuehrung-der-online-durchsuchung-und-quellen-tkue?file=files/anwaltverein.de/downloads/newsroom/stellungnahmen/2017/DAV-SN_44-17_%C3%84nderungsantrag.pdf).

⁷⁴⁹ BVerfG v 27.08.2008, 1 BvR 370/07, 1 BvR 595/07.

dürfen, im Postfach seines Sekretariats aber soll dies möglich sein.⁷⁵⁰ Aus Sicht der Berufsgeheimnisträger kommt also, neben der allgemeinen Unverhältnismäßigkeit, noch ein mangelnder Schutz der Kommunikation hinzu, sofern sie sich Hilfspersonen bedienen.

29. Ergebnisse

Bei neueren Gesetzesvorhaben im Bereich der Telekommunikationsüberwachung sind die Rechte von Berufsgeheimnisträgern stets bedroht. Gerade der Gesetzgebungsprozess zum PStSG zeigt, dass erst in quasi letzter Minute der Schutz der Berufsgeheimnisträger auf massiven Druck hin in das Gesetz aufgenommen wurde. Hier scheint die Situation in Deutschland insofern besser, als dass etwa ein Erhebungsverbot für Verkehrs- und Inhaltsdaten der Telekommunikation nach § 160a dStPO besteht, sofern Berufsgeheimnisträger betroffen sind. Dies hilft allerdings auch in den Fällen nur bedingt weiter, in denen eine verdachtsunabhängige Speicherung von Kommunikationsvorgängen erfolgt.

Ferner muss sich der Gesetzgeber, gerade bei Maßnahmen wie etwa der Online-Durchsuchung, bewusst sein, dass der Kernbereichsschutz besonders gewahrt werden muss. Ist es nicht möglich, einen Eingriff in diesen mit an Sicherheit grenzender Wahrscheinlichkeit auszuschließen, dann muss er eine Kenntnisnahme des Materials durch die unmittelbar an der Ermittlung beteiligten Personen dergestalt verhindern, dass zunächst andere Personen das Material sichten. Das BVerfG hat erkannt, dass es durchaus ein Problem darstellt, wenn Ermittler Material zu Gesicht bekommen, welches sie eigentlich nicht zu Gesicht bekommen dürften. Allein die Tatsache, dass dieses Material nicht verwendet werden darf, führt nicht unbedingt dazu, dass sich Ermittler von den gewonnenen Erkenntnissen nicht beeinflussen lassen. Dieser für den Kernbereich angedachte Schutz ist auch – gerade wegen der Vergleichbarkeit – für den Berufsgeheimnisträgerschutz anzudenken.

⁷⁵⁰ Stellungnahme des Deutschen Anwaltsvereins, abrufbar unter https://anwaltverein.de/de/newsroom/sn-44-17-einfuehrung-der-online-durchsuchung-und-quellen-tkue?file=files/anwaltverein.de/downloads/newsroom/stellungnahmen/2017/DAV-SN_44-17_%C3%84nderungsantrag.pdf, 21 f.

Unabhängig davon sollte der Gesetzgeber nur Überwachungsmaßnahmen einführen, die technisch ausgereift sind und einen wirklichen Nutzen zur Bekämpfung der einschlägigen Straftaten darstellen, die der Gesetzgeber damit zu bekämpfen gedenkt. Beides ist bei der Online-Durchsuchung nicht der Fall.

Kapitel VII – Zusammenfassung und Schlussbetrachtung

Abschließend seien die wichtigsten Ergebnisse zusammengefasst und einige Lösungsvorschläge zusammengetragen, mit denen sich ein verfassungskonformer und moderner Schutz der Telekommunikation von Berufsgeheimnisträgern gewährleisten lässt.

30. Zusammenfassung der wichtigsten Ergebnisse

Die Erkenntnisse dieser Arbeit betreffen verschiedene Bereiche des Verfassungsrechts und strahlen auch auf das Strafprozessrecht und Sicherheitspolizeirecht aus. Einigkeit mag in der Rechtswissenschaft darin bestehen, dass Berufsgeheimnisträger einen gewissen Schutz benötigen. Darüber hinaus gehen über die konkrete Ausgestaltung dieses Schutzes die Meinungen auseinander. Im Rechtsvergleich zu Deutschland herrscht in beiden Ländern über die Frage, wer Berufsgeheimnisträger ist, weitgehend Einigkeit. Unterschiede beschränken sich auf eher unwichtige Nuancen.

Die Telekommunikationsüberwachung ist zurzeit in Deutschland wesentlich breiter aufgestellt. Ermittler setzen mehr oder minder die gesamte Bandbreite von Überwachungsmethoden ein, die technisch zur Verfügung stehen.⁷⁵¹ Dies ist nicht unbedingt vorbildhaft für Österreich. Die Rechtsprechung des BVerfG zeigt, dass hier immer wieder der Gesetzgeber vom Gericht in die Schranken gewiesen werden muss. Kaum ein neues Gesetzespaket im Bereich der Telekommunikationsüberwachung wurde ohne jede Änderung in Karlsruhe bestätigt. Während auf verfassungsrechtlicher Ebene die richterliche Kontrolle effektiv zu funktionieren scheint, dürfte diese gerade in der ordentlichen Gerichtsbarkeit versagen. Wenn es um die Anordnungen bestimmter Überwachungsmaßnahmen geht, findet eine effektive richterliche Kontrolle – zumindest in Deutschland – offenbar nicht statt. Den Beweis, dass durch den umfangreichen Einsatz der Überwachungsmethoden in Deutschland die Verbrechensbekämpfung effektiver wäre, ist man bislang schuldig geblieben. Zudem besteht das Problem, dass

⁷⁵¹ Einschränkungen gibt es hier im Prinzip nur auf Behördenebene, so dass nicht alle Behörden auch alle Überwachungsmaßnahmen einsetzen (dürfen).

bei zunehmender Überwachung das Ungleichgewicht zwischen den Überwachungsmaßnahmen der Behörden einerseits und dem Schutz der Grundrechte andererseits immer größer wird.

Es zeigt sich, dass Österreich im Vergleich zu Deutschland eine andere Grundrechtssystematik hat, was den grundrechtlichen Schutz der Telekommunikation und aller Geschehnisse im Vorfeld und im Nachhinein angeht, die strenggenommen noch nicht oder nicht mehr unter den Begriff der Telekommunikation fallen, also etwa eine Nachricht kurz vor ihrem Absenden oder nach ihrem Empfang am Endgerät. Hier war der Rechtsvergleich insofern hilfreich, als dieser ermöglichte, bekannte Argumentationsmuster zu verlassen und Grundrechte, wie Art 10a StGG, neu zu durchdenken. Das Fernmeldegeheimnis bedarf einer technikoffenen, zeitgemäßen Interpretation. Da mittlerweile Verkehrsdaten enorm an Bedeutung gewonnen haben, lässt sich auf Dauer nicht am eingeschränkten Fernmeldegeheimnisbegriff festhalten, der den Schutzbereich auf den Inhalt der Kommunikation beschränkt. Vielmehr zeigt auch der Verfassungsvergleich zwischen Art 10a StGG und Art 10 GG, dass es gute Gründe gibt, Verkehrsdaten – zumindest dann, wenn es sich nicht um ein einziges Datum handelt, sondern um eine Vielzahl an Daten, aus denen sich ein persönliches Profil erstellen lässt – mit in den Schutzbereich einzubeziehen, ebenso, wie sich umgekehrt für Deutschland ein Richtervorbehalt bei Art 10 GG als zielführend erweisen würde.

Österreichisches und deutsches Verfassungsrecht unterscheiden sich von ihrem Aufbau und ihrer Systematik her teilweise. Der wohl größte Unterschied ist die Rolle der Menschenwürde im GG, die dort den zentralen Platz unter den Grundrechten einnimmt, wohingegen diese im österreichischen Verfassungsrecht ursprünglich nicht als eigenes Grundrecht geschützt war, nun aber durch die GRC auch in den nationalen Grundrechtekanon Eingang gefunden haben könnte. Zudem ist zu beobachten, dass es, auch bedingt durch die GRC, zu Annäherungen zwischen deutschem und österreichischem Verfassungsrecht kommt, die dazu führen, dass bestimmte Rechtsgedanken aus Deutschland auf Österreich übertragen werden können. Was die Menschenwürde und ihren Einfluss auf das österreichische Verfassungsrecht angeht, können argumentativ neue Wege beschritten werden. Dies führt letztlich dazu, dass sich der Grundrechtsschutz und das Grundrechtsverständnis in Österreich dem von Deutschland in einigen Punkten annähern. Das heißt nicht, dass man sich in Österreich auf einmal mit völlig neuen Grundrechten, wie etwa dem Grundrecht auf informationelle Selbstbestimmung,

konfrontiert sieht, die plötzlich das gesamte österreichische Verfassungsrecht auf den Kopf stellen. Vielmehr treten diese Grundrechte zu den bisher bekannten, wie etwa § 1 DSG 2000 hinzu und lassen diese in neuem Lichte erscheinen.

Gerade durch den Einfluss von Art 1 Abs 1 GG auf die Rechtsprechung des BVerfG hat sich zur Notwendigkeit von überwachungsfreien (Wohn-)Räumen mittlerweile eine ausführliche Rechtsprechung etabliert. Allerdings wirkt eine reine Bezogenheit auf Wohnraum heutzutage aus der Zeit gefallen zu sein. Dem wird die verfassungsgerichtliche Rechtsprechung in Deutschland auch gerecht: In seiner jüngsten Entscheidung zum BKA-Gesetz hat das BVerfG zum einen anerkannt, dass auch außerhalb vom klassischen Wohnraum eine solche Schutzbedürftigkeit unter Umständen vorliegen kann und zum anderen – ohne die Vergleichbarkeit der Situation explizit zu nennen – festgehalten, dass das Kontaktieren von Berufsgeheimnisträgern ebenfalls den gleichen strikten Regeln unterliegt wie der Kernbereich der privaten Lebensführung.

Folglich bedarf es bei der Konstellation im BKA-Gesetz, bei der ja im Vorfeld keine richterliche Kontrolle möglich ist, einer behördlichen Vorabkontrolle vor der Sichtung des Materials durch die Ermittler, die mit der Aufklärung des Falls betraut sind. Dies zeigt auch, dass in der verfassungsgerichtlichen Rechtsprechung der Tatsache, dass unverwertbares Material trotz allem in der Lage ist Ermittler zu beeinflussen, Rechnung getragen wird. Letztlich ist bei der Kommunikation von Berufsgeheimnisträgern ein Beweiserhebungsverbot zu fordern, das entweder in der Weise durchgesetzt werden sollte, dass Berufsgeheimnisträger nach Möglichkeit nicht in den Fokus der Ermittlungen geraten oder – falls dies nicht umgesetzt werden kann – dass das Material, das möglicherweise Daten von Berufsgeheimnisträgern enthält, einer Vorabsichtung durch eine unabhängige Stelle zugeführt wird, die das Material entsprechend prüft und freigibt. Hiervon sollte nur in den Fällen abgewichen werden, in denen aufgrund besonderer Eilbedürftigkeit, um Verletzungen von absolut geschützten Rechtsgütern zu verhindern, eine Vorabkontrolle nicht möglich ist. Ähnliches gibt es in Österreich bereits, sofern bei Berufsgeheimnisträgern Gegenstände oder Datenträger beschlagnahmt werden, welche bei Widerspruch des Berufsgeheimnisträgers bis zu einer Entscheidung über diesen Widerspruch nicht zum Akt zu nehmen sind.

Letztlich ist es dem Gesetzgeber nicht empfohlen, Grundfesten der strafprozessualen Ermittlungen umzukehren. Nach dem von Metternich im 19. Jahrhundert in Öster-

reich installierten Spitzelstaat wandte man sich radikal von der Praxis des Ermitteln im Geheimen ab und entschied sich in der StPO bewusst für Ermittlungen, die grundsätzlich offen zu erfolgen haben.⁷⁵² Dies gerät zunehmend zum Problem, da Überwachung von Telekommunikation ihrem Wesen nach stets heimlich erfolgt, außer in den Fällen, in denen Endgeräte bei einem Verdächtigen beschlagnahmt werden und die Ermittler nachträglich von der Kommunikation Kenntnis nehmen. Dieser Fall ist aber kein Hauptanwendungsfall. Der Schwerpunkt von Ermittlungen liegt in der heimlichen Telekommunikationsüberwachung.

31. Lösungsvorschläge und Ausblick

Alle Gesetzesentwürfe mit dem Schwerpunkt Telekommunikationsüberwachung in der letzten Zeit weisen sowohl in Österreich als auch in Deutschland verfassungsrechtliche Probleme auf. Hierbei erweist sich für Österreich als nachteilig, dass ein klares und umfassendes Beweiserhebungsverbot, wie es in Deutschland durch § 160a dStPO geschaffen wurde, nicht existiert. Allerdings hat man hiermit auch nur eine Norm für den Strafprozess geschaffen. Die Grundidee hierfür ist sicher richtig, löst das Problem aber nur partiell, da bei anderen Gesetzen – etwa dem BKAG – wieder neue Regelungen für Berufsheimnisträger geschaffen werden müssen. Am Ende stellt sich damit die gleiche Problematik, die sich in Österreich beim PStSG gezeigt hat, nämlich, dass die Regelungen zum Schutz von Berufsheimnisträgern bei jedem Gesetz aufs Neue festgeschrieben werden müssen.

Letztlich scheint damit der Berufsheimnisträgerschutz falsch verortet. Möchte man ihn nicht gleich auf verfassungsrechtlicher Ebene regeln, was zumindest bedenkenswert wäre, dann sollte er vielmehr auf TKG-Ebene geregelt werden. Auf dieses verweisen Gesetz sowohl das Strafprozessrecht als auch das Sicherheitspolizeirecht und darüber hinaus auch weitere Gesetze, die Überwachung jetzt und in Zukunft regeln werden. Schließlich wird auch im TKG geregelt, welche Daten bei Telekommunikati-

⁷⁵² *Rose*, Verdeckter Ermittler, 94; *Fuchs*, Verdeckte Ermittler - anonyme Zeugen, ÖJZ 2001, 495.

onsanbietern überhaupt vorliegen sollen und wie lange dies der Fall ist.⁷⁵³ Hiermit könnte eine Möglichkeit geschaffen werden, den Berufsgeheimnisträgerschutz legislativ bei der Wurzel zu packen und bei der Datenerhebung anzusetzen.

Hierbei sollte im TKG auch darüber nachgedacht werden, Berufsgeheimnisträger grundsätzlich von der Datenspeicherung durch Anbieter auszunehmen. Hier kann insbesondere die gesetzgeberische Ansicht, die bei der Vorratsdatenspeicherung in Österreich vertreten wurde, nicht überzeugen, die eine „Whitelist“ für Berufsgeheimnisträger „aus Datenschutzgründen“ generell ablehnt. Schließlich ist die Tatsache, dass eine bestimmte Person Berufsgeheimnisträger ist, für sich genommen kein sonderlich sensibles Datum. Es mag dem Berufsgeheimnisträger darauf ankommen, seinem Beruf von staatlicher Überwachung ungestört nachgehen zu können, jedoch wird es ihm nicht darauf ankommen, seinen Beruf im Geheimen auszuüben, zumal er dann auch für Ratsuchende nicht auffindbar ist. Eine solche Liste birgt daher nur ein stark eingeschränktes bis nicht vorhandenes Missbrauchspotenzial, da entsprechende Listen zum Teil ohnehin öffentlich zugänglich sind und dies zu Informationszwecken der Ratsuchenden auch sein müssen.⁷⁵⁴

Weiters muss eine solche Liste nicht notwendigerweise zentral – beispielsweise in Österreich auf Ebene der Durchlaufstelle – geführt werden. Denkbar ist etwa auch, dass der Berufsgeheimnisträger gegenüber seinem Telekommunikationsanbieter seine Zugehörigkeit zu einer bestimmten Berufsgruppe nachweist. Dadurch würde das Entstehen einer zentralen „Berufsgeheimnisträgerliste“ verhindert, da entsprechende Meldungen auf viele einzelne Provider aufgeteilt wären, und ein Missbrauchspotenzial auf ein Minimum reduziert wäre. Insofern mag es eher am gesetzgeberischen Unwillen gelegen haben, dass entsprechende Regelungen nicht umgesetzt worden sind.

Die Frage, welche Berufsgeheimnisträger von diesem Schutz umfasst sein müssen, lässt sich, wie der Rechtsvergleich mit Deutschland zeigt, nicht ohne weiteres

⁷⁵³ Aus diesem Grund ist die Vorratsdatenspeicherung neu in Deutschland auch in § 113 Abs 5 TKG geregelt. Hierbei wird einfach die Speicherdauer von Verbindungsdaten erhöht.

⁷⁵⁴ In diesem Zusammenhang kann beispielhaft die Liste aller Rechtsanwälte erwähnt werden, welche unter <http://www.rechtsanwaelte.at/buergerservice/servicecorner/rechtsanwalt-finden/> für jeden abrufbar ist.

beantworten. In jedem Fall müssen Seelsorger, Strafverteidiger, Rechtsanwälte und ähnliche Berufe, sofern sich diese auf eine Strafverteidigung beziehen, bereits einem absoluten Beweiserhebungsverbot unterliegen.⁷⁵⁵ Der Gesetzgeber muss diese absoluten Beweiserhebungsverbote aus verfassungsrechtlichen Gründen zwingend schaffen.

Dabei muss er sich bewusst sein, dass, wenn er weiteren Gruppen diesen Schutz zubilligt, was grundsätzlich aus Grundrechtsschutzgedanken zu begrüßen ist, er unter Umständen aus Gründen des Gleichheitssatzes (Art 7 B-VG, Art 2 StGG) diesen absoluten Schutz auch auf andere Berufsgeheimnisträger ausweiten muss. Dies stellt natürlich den Gesetzgeber, sofern er dies aus Sicht der Strafverfolgung betrachtet, vor gewisse Herausforderungen.

Da Kommunikation seit einiger Zeit verstärkt verschlüsselt abläuft bzw es auch für technische Laien einfacher und praktikabler geworden ist, sich Verschlüsselungstechniken, vor allem solcher, die Ende-zu-Ende-Verschlüsselungen⁷⁵⁶ einsetzen, zu bedienen, gibt es auch staatlicherseits in Österreich und Deutschland Bestrebungen, anstatt bei der Telekommunikation und damit beim Anbieter im Bereich des TKG, beim Nutzer und dessen Endgeräten mittels Spionagesoftware anzusetzen. Verabschieden sollte man sich von dem Gedanken, stärkerer Digitalisierung mit einer stärkeren Überwachung dieses Bereiches zu begegnen, insofern diese die Maße der Überwachung der Offline-Welt deutlich übersteigt. Weiters ist es auch nicht zielführend, stärkerer Verschlüsselung damit zu begegnen, in Systeme einzudringen und diese vor Verschlüsselung zu durchsuchen oder auf verstärkte Entschlüsselung zu setzen. Zwar mag es auf den ersten Blick folgerichtig erscheinen, einfach für weniger Verschlüsselung einzutreten, da diese Ermittlern die Arbeit erschwert, jedoch bleiben hierbei viele Aspekte außer

⁷⁵⁵ Hierbei ist auch § 58 Abs 1 StPO von Bedeutung.

⁷⁵⁶ Hierbei handelt es sich keinesfalls um eine Erfindung der letzten Jahre. Schon in den 1980er Jahren wurde in Fachkreisen über Ende-zu-Ende-Verschlüsselung publiziert: *Hunter*, Encrypting from end-to-end, Network World v 29.02.1988, 47; *Longley/Shain*, Data And Computer Security: A Dictionary Of Terms And Concepts, 230.

Betracht. Treffend formuliert es *Schallbruch*, ehemaliger IT-Leiter im deutschen Bundesinnenministerium:⁷⁵⁷

[W]er Verschlüsselung einschränkt, berührt die Grundlagen digitalen Lebens. Abgeschwächte Verschlüsselung hilft nicht nur der Polizei, sie macht es Terroristen leicht, in industrielle Steuerungsanlagen einzudringen. Hintertüren werden nicht nur für rechtsstaatlich abgesicherte Ermittlungen genutzt, sondern auch von ausländischen Nachrichtendiensten.

Verschlüsselung gehört mittlerweile zur normalen Kommunikation, da es immer einfacher wird, diese einzusetzen. Sie ist Teil des technologischen Fortschritts. Es kann also nicht staatlicherseits Ziel sein, Verschlüsselung zu bekämpfen. Gerade für Berufsgeheimnisträger ist Verschlüsselung nicht nur sinnvoll, sondern auch notwendig, wollen sie sich nicht dem Vorwurf aussetzen, mit Geheimnissen leichtfertig umzugehen, was unter Umständen auch einen Bruch ihrer berufsrechtlichen Verpflichtungen zur Folge haben kann.

Letztlich ist als Ausgleich für staatliche Überwachung auch eine verstärkte staatliche Überprüfung von angeordneten Überwachungen zu überdenken, die zu erfolgen hat, bevor die mit dem Fall befassten Ermittler das gewonnene Material auswerten. Hierbei ist Material, das die Kommunikation von Berufsgeheimnisträgern und den Personen, die sich an diese im Wege der Telekommunikation gewandt haben, zu entfernen, sofern ein vorheriges Herausfiltern bei der Erhebung aus technischen Gründen nicht möglich ist.

Bezüglich einer verdachtsunabhängigen und flächendeckenden Überwachung gilt jedoch, dass diese allgemein nicht mit der Grundrechtecharta vereinbar ist. Hierbei bedarf es also keiner Whitelist oder ähnlicher Instrumente, um diese Art der Überwachung für Berufsgeheimnisträger zu unterbinden, da eine solche Art der Überwachung, wie bei der Vorratsdatenspeicherung, für die gesamte Bevölkerung als unzulässig anzusehen ist. Lediglich dürfen bestimmte Verkehrs- und Standortdaten aufgrund eines Verdachts für einen bestimmten Zeitraum aufgezeichnet werden.

⁷⁵⁷ <http://www.faz.net/aktuell/feuilleton/debatten/ueberwachung/wie-man-kryptologie-und-verbrechensbekämpfung-balanciert-14319234.html>.

Nicht nur für Berufsgeheimnisträger, sondern für die gesamte Bevölkerung muss aber gelten, dass vor jeder neuen Überwachungsmaßnahme zum einen Ausnahmeregelungen geschaffen werden und darüber hinaus auch die Frage gestellt werden sollte, ob eine grundrechtskonforme, verhältnismäßige Lösung möglich ist. Schon im Jahr 1890 wurden von *Warren und Brandeis* in der *Harvard Law Review* entsprechende Überlegungen getroffen, indem diese das Recht „allein gelassen zu werden“ als Recht auf Privatheit entsprechend definierten.⁷⁵⁸ Dieses Recht ist letztlich Ausdruck dafür, von niemandem – auch nicht von staatlichen Institutionen – besessen zu werden oder in deren Eigentum zu stehen. Dies sollte gerade in der heutigen Zeit auch der Grundpfeiler des staatlichen Handelns gegenüber allen Menschen sein, die sich auf ihrem Staatsgebiet aufhalten. Der Staat darf diese nicht als Eigentum oder Besitz betrachten und auch mit ihren Daten nicht so verfahren, zumal eine vollständige Überwachung der Bevölkerung und eine Überantwortung aller möglichen persönlichen Daten in die Hände staatlicher Stellen von geringem Nutzen ist. Hierfür sei an das Zitat von Benjamin Franklin erinnert:

*“They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety.”*⁷⁵⁹

⁷⁵⁸ Die Autoren gelten als diejenigen, die erstmals ein „Right to Privacy“ definierten und als Komponente dessen auch ein „right to be let alone“ ansahen. Hierzu führen die Autoren aus: *These considerations lead to the conclusion that the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone. It is like the right not be assaulted or beaten, the right not be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed. In each of these rights, as indeed in all other rights recognized by the law, there inheres the quality of being owned or possessed -- and (as that is the distinguishing attribute of property) there may some propriety in speaking of those rights as property.* Zitiert nach http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

⁷⁵⁹ Franklin/Franklin, *Memoirs of the Life and Writings of Benjamin Franklin*, 270; Übersetzung: Wer wesentliche Freiheit aufgeben kann um eine geringfügige bloß jeweilige Sicherheit zu bewirken, verdient weder Freiheit, noch Sicherheit.

Literaturverzeichnis

Monographien

Albers, Marion (2004), Informationelle Selbstbestimmung

Albrecht, Peter-Alexis, Die vergessene Freiheit. Strafrechtsprinzipien in der europäischen Sicherheitsdebatte

Auer, Maximilian (2011), Das Grundrecht auf Datenschutz im Unternehmen.

Bauer, Lukas / Reimer, Sebastian (2009), Handbuch Datenschutzrecht

Berka, Walter (2012), Verfassungsrecht, Grundzüge des österreichischen Verfassungsrechts für das juristische Studium, 4. Auflage

Berka/Grabenwarter/Holoubek Hrsg (2012), Persönlichkeitsschutz in elektronischen Massenmedien, Bd 9 der Schriftenreihe Recht der elektronischen Massenmedien REM

Deutsche Bischofskonferenz, Katechismus der katholischen Kirche, Kompendium

Ennöckl, Daniel, (2014) Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung

Franklin, Benjamin / Franklin, William Temple, Memoirs of the Life and Writings of Benjamin Franklin

Geuer, Ermano (2008), Digitale Identität 2.0, Möglichkeiten und Grenzen der Identifizierung von Nutzern im www.

Giese, Karim (2004), Sicherheitspolizeirecht in Bachmann ua (Hrsg), Besonderes Verwaltungsrecht, 5. Aufl., überarbeitete und ergänzte Fassung, 1 – 31

Grabenwarter, Christoph / Pabel, Katharina (2012), Europäische Menschenrechtskonvention (EMRK), 5. Auflage.

Himberger, Simon, Fernmeldegeheimnis und Überwachung, Schutzbereiche & Eingriffe – Durchführung & Kosten

Höflich, Ann-Kathrin (2011), Die ärztliche Schweigepflicht, Unter besonderer Beachtung der postmortalen ärztlichen Schweigepflicht.

Hornung, Gerrit / Müller-Terpitz, Ralf (2015), Rechtshandbuch Social Media

Jahnel, Dietmar / Mader, Peter / Staudegger, Elisabeth (2012), IT-Recht, 3. Auflage

Kammeiner, Heinz / Michalke Regina (2004), Streben nach Gerechtigkeit, Festschrift für Prof Dr Günter Tondorf zum 70. Geburtstag

Klaushofer, Reinhard, Strukturfragen der Rechtsschutzbeauftragten

Knyrim, Rainer (2012), Datenschutzrecht, Praxishandbuch für richtiges Registrieren Verarbeiten Übermitteln Zustimmung Outsourcen Werben uvm, 2.Auflage.

Korinek, Karl, Grundrechte und Verfassungsgerichtsbarkeit

Krause, Gerhard / Müller, Gerhard (1980), Theologische Realenzyklopädie (TRE).

Leitner, Richard (2004), Vernehmungsverbote im österreichischen Strafprozessrecht, Beichtgeheimnis und Amtsgeheimnis versus Wahrheitsfindung.

Lienbacher, Georg Hrsg (2011), Verfassungsinterpretation in Europa, Heinz Schäffer Gedächtnissymposium.

Marent, Sabine, Das Fernmeldegeheimnis und die Telefonüberwachungsregelungen der StPO

Marschner, Ernst / Stefaner, Marcus C. (2015), Steuerreform 2015/2016

Menzel, Matthias / Pierlings, Tobias / Hoffmann, Jeannine (Hrsg) (2005), Völkerrechtsprechung, Ausgewählte Entscheidungen zum Völkerrecht aus der Retrospektive

Öhlinger, Theo (2009), Verfassungsrecht, 8. Auflage.

Park, Tido (2015), Durchsuchung und Beschlagnahme, 3. Auflage.

Raschauer, Nicolas Hrsg (2011), Datenschutzrecht 2010.

Regenfelder, Wolfgang, Ermittlungsmaßnahmen bei neuen Informationstechnologien im Spannungsverhältnis zum Grundrechtsschutz

Roxin, Claus / Schünemann Bernd (2012), Strafverfahrensrecht, 27. Auflage.

Schlaich, Klaus / Koriath, Stefan (2015), Das BVerfG , 5. Auflage.

Schubert, Charlotte (2005), Der hippokratische Eid, Medizin und Ethik von der Antike bis heute.

Szuba, Dorothee (2011), Vorratsdatenspeicherung, Der europäische und deutsche

Gesetzgeber im Spannungsfeld zwischen Sicherheit und Freiheit.

Talós, Emmerich, Das austrofaschistische Herrschaftssystem, Österreich 1933-1938, 2. Auflage

Tamblé, Philipp, Der Anwendungsbereich der EU-GRC (GRC) gemäß Art 51 I 1 GRC – Grundlagen und aktuelle Entwicklungen in Beiträge zum Europa- und Völkerrecht (Heft 9, März 2014) [=Der Anwendungsbereich der GRC]

Vogl, Mathias, Der Rechtsschutzbeauftragte in Österreich

Wild, Maximiliane-Stephanie (2008), Die anwaltliche Verschwiegenheitspflicht in Deutschland und Frankreich.

Witte, John / Alexander, Frank S. Hrsg (2008), Christianity and Law, An Introduction.

Zerbes, Ingeborg (2010), Spitzeln, Spähen, Spionieren – Sprengung strafprozessualer Grenzen durch geheime Zugriffe auf Kommunikation

Kommentare

Aigner, Gerhard / Kletečka, Andreas / Kletečka-Pulker, Maria / Memmer, Michael Hrsg (2012), Handbuch Medizinrecht für die Praxis, 18. EL.

Berka, Walter / Heindl, Lucie / Höhne, Thomas / Noll, Alfred (2012), Mediengesetz Praxiskommentar, 3. Auflage

Berner, Georg / Köhler, Gerd Michael / Käß, Robert (2010), Polizeiaufgabengesetz (PAG), 20. Auflage.

Bertel, Christian / Venier, Andreas (2012), Kommentar zur StPO.

Calliess, Christian / Ruffert, Matthias Hrsg (2011), EUV/AEUV, 4. Auflage.

Dohr, Walter / Pollirer, Hans-Jürgen / Weiss, Ernst M. / Knyrim, Rainer Hrsg (2015), Datenschutzgesetz, 19. Ergänzungslieferung.

Dreier, Horst Hrsg (2004), Grundgesetz (GG), Kommentar, 2. Auflage.

Epping, Volker / Hillgruber, Christian Hrsg (2012), Beck'scher Online-Kommentar Grundgesetz (BeckOK, GG), Stand 1.7.2012.

Fabrizy, Ernst Eugen Hrsg (2010), StGB und ausgewählte Nebengesetze, Kurz-

kommentar, 10. Auflage.

Fasching, Hans / Konecny, Werner Hrsg (2013), Zivilprozessgesetze, 3. Auflage.

Fuchs, Helmut / Ratz, Eckart Hrsg (2014), Wiener Kommentar zur Strafprozessordnung (WK-StPO), (Stand 1.9.2014, rdb.at).

Geppert, Martin / Schütz, Raimund, Beck'scher TKG-Kommentar, 4. Auflage

Graf, Peter Hrsg (2012), Beck'scher Online Kommentar zur Strafprozessordnung (BeckOK StPO), Stand: 1.6.2012.

Hannich, Rolf Hrsg (2008), Karlsruher Kommentar zur Strafprozessordnung, 6. Auflage.

Hauer, Andreas / Keplinger, Rudolf (2011), Sicherheitspolizeigesetz, 4. Auflage.

Hengstschläger, Johannes / Leeb, David (2009), Allgemeines Verwaltungsverfahrensgesetz, Kommentar.

Holoubek, Michael / Lienbacher, Georg Hrsg (2014), GRC Kommentar, Charta der Grundrechte der Europäischen Union

Höpfel, Franz / Ratz, Eckart Hrsg (2005), Wiener Kommentar zum Strafgesetzbuch [=WK-StGB], 2. Auflage, (Stand: 1.12.2005, rdb.at)

Jarass, Hans D. Hrsg (2013), Charta der Grundrechte der EU, 2. Auflage.

Jöcks, Wolfgang / Miebach, Klaus Hrsg (2013), Münchener Kommentar zum StGB (MüKo-StGB), 2. Auflage 2013.

Kahl, Wolfgang / Waldhoff, Christian / Walter, Christian Hrsg (2012), Bonner Kommentar zum Grundgesetz (Bonner Kommentar GG), 159. Aktualisierung.

Karpenstein, Ulrich / Mayerr Franz Hrsg (2012), EMRK.

Kilian, Wolfgang / Heussen, Benno Hrsg (2012), Computerrechtshandbuch, Informationstechnologie in der Rechts- und Wirtschaftspraxis, 31. Ergänzungslieferung.

Kindhäuser, Urs / Neumann, Ulfrid / Paeffgen, Hans-Ulrich Hrsg (2013), Kommentar StGB, 4. Auflage.

Kletečka, Andreas / Schauer, Martin Hrsg (2015), ABGB-ON, (Stand 01.03.2015, rdb.at).

Korinek, Karl / Holoubek, Michael (2011), Österreichisches Bundesverfassungsrecht, Textsammlung und Kommentar, 10. Lieferung

- Laurer, René / Borns, Rainer / Strobl, Johann / Schütz, Melitta / Schütz, Oliver* (2007), Kommentar zum Bankwesengesetz, 3. Auflage
- Litzka, Gerhard / Strebing, Iris* (2005), Mediengesetz Kurzkomentar, 5. Auflage.
- Longley, Dennis / Shain, Michael*, Data And Computer Security: A Dictionary Of Terms And Concepts
- Maunz, Theodor / Dürig, Günter Hrsg* (2014), Grundgesetz-Kommentar (GG), Stand Dezember 2014, 73. Ergänzungslieferung
- Meyer, Jürgen* (2014), Charta der Grundrechte der Europäischen Union, 4. Auflage
- Meyer-Ladewig, Jens* (2011), Europäische Menschenrechtskonvention, Handkommentar (EMRK), 3. Auflage
- Pfeiffer, Gerd* (2004), Strafprozessordnung Kommentar, 5. Auflage
- Roggan, Frederik Hrsg* (2012), G 10 Gesetz, Kommentar.
- Röggla, Werner / Wittmann, Heinz / Zöchbauer, Peter* (2012), Mediengesetz, Praxiskommentar.
- Rose, Gregor*, Verdeckter Ermittler, V-Person und Informant unter besonderer Berücksichtigung des Scheingeschäfts im deutsch-österreichischen Rechtsvergleich
- Rüpke, Giselher*, (1975) Der verfassungsrechtliche Schutz der Privatheit
- Rummel, Peter Hrsg* (2014) ABGB, (Stand: 1.11.2014, rdb.at)
- Sachs, Michael Hrsg* (2011), Grundgesetz (GG), Kommentar, 6. Auflage.
- Sodann, Helge Hrsg* (2011), Grundgesetz (GG), 2. Auflage.
- Spickhoff, Andreas Hrsg* (2011), Medizinrecht.
- Wolff, Heinrich Amadeus / Brink, Stefan Hrsg* (2012), Beck'scher Online-Kommentar Datenschutzrecht (BeckOK, BDSG), Stand 1.11.2012

Aufsätze

- Albrecht, Florian / Dienst, Sebastian*, Der verdeckte hoheitliche Zugriff auf informationstechnische Systeme - Rechtsfragen von Online-Durchsuchung und Quellen-TKÜ, JurPC Web-Dok. 5/2012

- Albrecht, Florian*, Rechtswidrige Online-Durchsuchung durch das Bayerische Landeskriminalamt, Anmerkung zu LG Landshut, Beschl. v. 20.01.2011 - 4 Qs 346/10, JurPC Web-Dok. 59/2011
- Albrecht, Florian*, ZITiS: Kommunikationsüberwachung durch den Staat: Neue Behörde soll Licht ins Dunkel bringen, LTO v 18.07.2016, http://www.lto.de/persistent/a_id/20038/
- Asbrock, Bernd*, Der Richtervorbehalt – prozedurale Grundrechtssicherung oder rechtsstaatliches Trostpflaster, ZRP 1998, 17
- Bär, Wolfgang*, Anmerkung, LG Landshut: Überwachung verschlüsselter Skype-Kommunikation, MMR 2011, 691
- Becherer, Herbert*, Zum Seminar B: Der Schutz des Berufsgeheimnisses bei Steuerberatern in Deutschland, IStR 2010, 555
- Bertheau, Camilla*, § 160a StPO neuer Fassung – doch offene Fragen bleiben, StV 2012, 303
- Brandstetter, Wolfgang*, Die Fernmeldeüberwachung öffentlicher Telefonzellen, JBl 1984, 457
- Braum, Stefan*, „Parallelwertungen in der Laiensphäre“: Der EuGH und die Vorratsdatenspeicherung, ZRP 2009, 174
- Braun, Frank / Roggenkamp, Jan Dirk*, 0Zapftis – (Un)Zulässigkeit von „Staatstrojanern“, K&R 2011, 681
- Braun, Frank*, Der so genannte „Lauschangriff“ im präventivpolizeilichen Bereich, Die Neuregelung in Art IV-VI GG, NVwZ 2000, 375
- Britz, Gabriele*, Vertraulichkeit und Integrität informationstechnischer Systeme, DÖV 2008, 411
- Brüning, Janique*, Der Richtervorbehalt – ein zahnloser Tiger? Über die verfassungsrechtliche Notwendigkeit des Richtervorbehalts und seine Ineffizienz in der Praxis, ZIS 2006, 29
- Burgstaller, Manfred*, Sicherheitspolizeiliche Ermittlungshandlungen unter Kontrolle des Rechtsschutzbeauftragten beim BMI, Informationen zur Praxis 2010 und 2009, ÖJZ 2011, 644
- Busch, Ralf*, Vorschlag zur Neuordnung der Anordnungskompetenz für die Entnahme von Blutproben, ZRP 2012, 79
- Danda, Clemens*, Die Anwendung der Charta der Grundrechte der Europäischen Union im österreichischen Grundrechtsschutz, migralex 2013, 14

- Deusch, Florian / Eggendorfer, Tobias*, Das Fernmeldegeheimnis im Spannungsfeld aktueller Kommunikationstechnologien, K&R 2017, 93
- Dörr, Dieter*, Freier Verkehr zwischen Untersuchungshäftling und seinem Verteidiger, JuS 1993, 508
- Eckhardt, Jens*, Wie weit reicht der Schutz des Fernmeldegeheimnisses (Art 10 GG), DuD 2006, 365
- Ende, Claudia*, Verstärkter Schutz von Berufsgeheimnisträgern – auch für Steuerberater!, DStR 2009, 2556
- Fischedick, Walter*, Das Beicht- und Seelsorgegeheimnis, Zur Legitimation und Reichweite der Zeugnisverweigerungsrechte für Geistliche, DÖV 2008, 584
- Forgó, Nikolaus / Krügel, Tina*, Der Personenbezug von Geodaten, Cui bono, wenn alles bestimmbar ist?, MMR 2010, 17
- Fuchs, Helmut*, Verdeckte Ermittler - anonyme Zeugen, ÖJZ, 2001, 495
- Gercke, Björn*, Rechtliche Probleme durch den Einsatz des IMSI-Catchers, MMR 2003, 453
- Geuer, Ermanno*, Das Fernmeldegeheimnis als gesetzliches Verbot. Rechtsprobleme bei der Forderungsabtretung aus TK-Verträgen, ZD 2012, 515
- Geuer, Ermanno*, Das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten aus Sicht von Berufsgeheimnisträgern, AnwZert ITR 24/2015, Anm 2
- Geuer, Ermanno*, Vorratsdatenspeicherung in Österreich, Stärken und Schwächen der Richtlinienumsetzung, ZD 2012, 421
- Geuer, Ermanno*, Zur Bedeutung des Kriteriums „in völliger Unabhängigkeit“ bei Datenschutzkontrollstellen, ZIR 2013, 8
- Goez, Christoph*, Keine Gleichheit von Steuerberatern mit Rechtsanwälten als Verteidiger, SteuK 2012, 107
- Grabenwarter, Christoph*, Das Recht auf informationelle Selbstbestimmung im Europarecht und im Verfassungsrecht, Österreichisches Anwaltsblatt 2015, 405
- Gusy, Christoph*, Überwachung der Telekommunikation unter Richtervorbehalt, Effektiver Grundrechtsschutz oder Alibi?, ZRP 2003, 275
- Haas, Günter*, Zeugnisverweigerungsrecht des Geistlichen, NJW 1990, 3253
- Harbich, Herbert*, Einige Fragen der anwaltlichen Verschwiegenheit, AnwBl 1983,

- Hattenberger, Doris / Klingbacher, Kerstin*, Bemerkenswertes zur Entscheidung des VfGH zur Vorratsdatenspeicherung, Jahrbuch Öffentliches Recht 2015, 179
- Helmken, Dierk*, Reform des Richtervorbehalts: Vom Palliativum zum effektiven Grundrechtsschutz, StV 2003, 193
- Hennsler, Martin*, Das anwaltliche Berufsgeheimnis, NJW 1994, 1817
- Hoeren, Thomas*, Was ist das „Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme“?, MMR 2008, 365
- Hornung, Gerrit*, Zwei runde Geburtstage: Das Recht auf informationelle Selbstbestimmung und das WWW, MMR 2004, 3
- Hunter, John J.*, Encrypting from end-to-end, Network World v. 29.02.1988, 47
- Jarass, Hans D.*, Das allgemeine Persönlichkeitsrecht im Grundgesetz, NJW 1989, 587
- Klein, Oliver*, Offen und (deshalb) einfach – Zur Sicherstellung und Beschlagnahme von E-Mails beim Provider, NJW 2009, 2996
- Kretschmer, Joachim*, § 160a StPO – gelungene oder misslungene Gesetzgebung?, HRRS 2010, 521
- Krumm, Carsten*, Richtervorbehalt bei der Blutprobe: Weg damit!, ZRP 2009, 71
- Kunert, Karl H.*, Erweitertes Zeugnisverweigerungsrecht der Medienmitarbeiter Gesetz zur Änderung der Strafprozessordnung vom 15. 2. 2002, NStZ 2002, 169
- Kutscha, Martin*, Mehr Schutz von Computerdaten durch ein neues Grundrecht?, NJW 2008, 1042
- Kutzner, Lars*, Die Beschlagnahme von Daten bei Berufsgeheimnisträgern, NJW 2005, 2652
- Lachmayer, Konrad*, Transnationales Polizeihandeln – Demokratische und rechtsstaatliche Herausforderungen der europäischen Polizeikooperation, JBl. 2011, 409
- Langheinrich, Gertraude / Ryda, Wolfgang*, Beweismittel im Verfahren vor den (Abgaben-)Behörden und den Verwaltungsgerichten (Teil II), FJ 2016, 3
- Leipold, Klaus*, Der „große Lauschangriff“, NJW-Spezial 2005, 135

- Leipold, Klaus*, Der Richtervorbehalt in der Praxis, NJW-Spezial 2010, 504
- Leisner, Walter*, Das neue „Kommunikationsgrundrecht“ – Nicht Alibi für mehr, sondern Mahnung zu weniger staatlicher Überwachung, NJW 2008, 2902
- Metzler, Matthäus*, Verkehrsdaten nicht vom Fernmeldegeheimnis erfasst (Anmerkung zu VfGH 29. 6. 2012, B 1031/11), ZTR 2012, 170
- Meyerdierks, Per*, Sind IP-Adressen personenbezogene Daten?, MMR 2009, 8
- Miklau, Robert / Pilnacek, Christian*, Optische und akustische Überwachungsmaßnahmen und organisierte Kriminalität („Lauschangriff“) – Paradigmenwechsel im Verfahrensrecht, JRP 1997, 286
- Morscher, Siegbert / Waitz, Waltraud*, Zum Schutz des Briefgeheimnisses, JBl. 2008, 424
- Möstl, Markus*, Datenverfügbarkeit als Voraussetzung für innere Sicherheit, Ein Bericht aus Deutschland, SIAK-Journal SIAK-Journal 2010 H 2, 61
- Müller, Eckhart*, Durchsuchung einer Rechtsanwaltskanzlei - Verhaltenshinweise, Mitteilung der Rechtsanwaltskammer München 03/2013, 4
- Müller-Jacobsen, Anke*, Schutz von Vertrauensverhältnissen zu Rechtsanwälten im Strafprozess, Ein erster Schritt zum Abschied vom „Zwei-Klassen-Recht“, NJW 2011, 257
- Muzak, Gerhard*, Wer darf die GRC prüfen: EuGH oder VfGH?, ecolex 2014, 1113
- Nachbauer, Andreas*, Standortfeststellung und Art 10 GG - Der Kammerbeschluss des BVerfG zum Einsatz des „IMSI-Catchers“, NJW 2007, 335
- Neuhoff, Heiko*, Die Dynamik der Medienfreiheit am Beispiel von Presse und Rundfunk, ZUM 2012, 371
- Otto, Gerald / Seitlinger, Michael*, Zur Umsetzung der Data Retention-Richtlinie in Österreich, Der Begutachtungsentwurf des Ludwig Boltzmann Instituts für Menschenrechte im Lichte der Entscheidung des BVerfG s vom 2. 3. 2010, MR 2010, 59
- Peter Krömer*, Zur Problematik unterschiedlicher Rechtsvorschriften für Religionsgemeinschaften, öarr 2010, 198
- Pilnacek, Christian / Pscheidl, Andreas*, Das Strafverfahren und seine Grundsätze (Teil I), Alte Hüte im neuen Gewand oder Fundgrube für die Auslegung?, ÖJZ 2008, 629
- Pühringer, Lisa*, Vorratsdatenspeicherung, Zugriffsmöglichkeiten durch Sicherheits- und Strafverfolgungsbehörden, JAP 2012/2013/10

- Rami, Michael*, Österreichische Medienprivilegien unter den Messern des EuGH und des EGMR, ÖJZ 2015, 533.
- Ratz, Eckhart*, Beweisverbote und deren Garantie durch die Rechtsprechung des OGH, RZ 2005, 74
- Rogalski, Maciej*, Verpflichtung zur Vorratsspeicherung und Bereitstellung von Telekommunikationsdaten in Polen, Nach dem Urteil des Europäischen Gerichtshofs vom 8. April 2014, WiRO 2015, 50
- Rogalski, Maciej*, Verpflichtung zur Vorratsspeicherung und Bereitstellung von Telekommunikationsdaten in Polen, Nach dem Urteil des Europäischen Gerichtshofs vom 8. April 2014, WiRO 2015, 50
- Roßnagel, Alexander / Schnabel, Christoph*, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, NJW 2008, 3534
- Roßnagel, Alexander / Scholz, Philip*, Datenschutz durch Anonymität und Pseudonymität, Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, 721
- Sachs, Michael*, Grundrechte: Fernmeldegeheimnis und Unverletzlichkeit der Wohnung, Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen im Strafprozess, JuS 2012, 374
- Satenig, Maral Charodian*, Stille Nacht, heimliche Nacht – Zur SPG-Novelle 2007 und der Erweiterung sicherheitspolizeilicher Befugnisse, juridikum 2008, 130
- Schaefer, Hans Christoph*, Kommentar: Richtervorbehalt, NJW 2005, 1332
- Schmoller, Kurt*, Zur Reichweite der Verschwiegenheitspflicht von Ärzten, Psychologen und Psychotherapeuten, RdM 1996, 131
- Schmölzer, Gabriele*, Rückwirkende Überprüfung von Vermittlungsdaten im Fernmeldeverkehr, Anmerkungen zu OGH 6. 12. 1995, 13 Os 161/95, JBl 1997, 211
- Simitis, Spiros*, Der EuGH und die Vorratsdatenspeicherung oder die verfehlte Kehrtwende bei der Kompetenzregelung, NJW 2009, 1782
- Simitis, Spiros*, Die informationelle Selbstbestimmung - Grundbedingung einer verfassungskonformen Informationsordnung, NJW 1984, 394
- Smith, Stephan*, Kurzer Zwischenstand zu Recht und Praxis der „stillen SMS“, VR 2012, 334
- Spielmann, Dean*, Das anwaltliche Berufsgeheimnis in der Rechtsprechung des EGMR, AnwBl 2010, 346

- Stadler, Thomas*, Der Richtervorbehalt – ein stumpfes Schwert oder ein rechtsstaatlich gebotenes Instrument?, ZRP 2013, 179
- Steiner, Udo*, Der Richter als Ersatzgesetzgeber, Richterliche Normenkontrolle - Erfahrungen und Erkenntnisse, NJW 2011, 2919
- Stolzlechner, Harald*, Überlegungen zur ärztlichen Verschwiegenheits-, Anzeige- und Meldepflicht, RdM 2000, 67
- Stricker, Martin*, Schutz von Berufsgeheimnissen, Zum Widerspruch nach § 112 StPO, ÖJZ 2016, 539
- Strömer, Rainer*, Verwertung tagebuchartiger Aufzeichnungen, NStZ 1990, 397
- Stuefer, Alexia*, Durchsuchung und Beschlagnahme im Strafverfahren, JSt 2011, 134
- Terhechte, Jörg Philipp*, Rechtsangleichung zwischen Gemeinschafts- und Unionsrecht – die Richtlinie über die Vorratsdatenspeicherung vor dem EuGH, EuZW 2009, 199
- Tiedemann, Jens*, Die „stille SMS“ – Überwachung im Mobilfunk, K&R 2004, 63
- Tinnefeld, Maria-Theres*, Vom archimedischen Punkt in einer Zivilgesellschaft, MMR 2004, 797
- Tretter, Hannes / Nowak, Manfred*, Vorschläge zur Errichtung einer nationalen Menschenrechtsinstitution in Österreich, JRP 2007, 1
- van Lijnden, Constantin Baron*, Mit Korrekturen zurück, BVerfG erklärt BKA-Gesetz größtenteils für verfassungswidrig, LTO v. 20.04.2016, <http://www.lto.de/recht/hintergruende/h/bverfg-urteil-1-bvr-966-09-1-bvr-1140-09-bka-gesetz-teilweise-verfassungswidrig/>
- Vcelouch, Peter*, Auswirkungen der österreichischen Unionsmitgliedschaft auf den Rechtsschutz vor dem VfGH und dem VfStGH, ÖJZ 1997, 721
- Vinken, Horst*, Ausdehnung des § 160a StPO auf Steuerberater zum Schutz der Mandanten, DStR-KR 2011, 13
- Vinken, Horst*, Praxistauglichkeit verbessern – mehr Rechtssicherheit im Steuerrecht schaffen, Beihefter zu DStR 22 2012, 81
- Wegner, Kilian*, Die "Fransson"-Entscheidung des EuGH - Eine Erschütterung im System der europäischen Grundrechte?, Anmerkung zum Urteil des Europäischen Gerichtshofs vom 26. Februar 2013 (EuGH C-617/10 - Fransson), HRRS 2013, 126
- Werwigg, Ulrich*, Zur Geltung des Richtervorbehalts bei der Durchsuchung von

besetzten Häusern, NJW 1983, 2366

Wessely, Wolfgang, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht?, ÖJZ 1999, 491

Zenz, Daniela, "Staatlich anerkannte Pflicht zur Verschwiegenheit" bestimmter Berufsgruppen im Verhältnis zur Zeugnisablegung im Verwaltungs-, Zivil- und Strafverfahren, JRP 2005, 230

Zerbes, Ingeborg, Anwaltsverschwiegenheit: überkommenes Privileg oder rechtsstaatliches Erfordernis?, Österreichisches Anwaltsblatt, 565

Zerbes, Ingeborg, Das Urteil des deutschen BVerfG s zur Online-Durchsuchung und Online-Überwachung Grundrechtlicher Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme - auch in Österreich, ÖJZ 2008, 834

Binder, Bruno, Der materielle Gesetzesvorbehalt der Erwerbsfreiheit (Art 6 StGG) - Überlegungen zur neuen Judikatur des VfGH, ÖZW 1988, 1.

Veröffentlichungen im Internet

Abgeordnetenhaus Berlin

Drucksache 17/2401

<http://pardok.parlament-berlin.de/starweb/adis/citat/VT/17/DruckSachen/d17-2401.pdf>

AK-Vorrat (Stellungnahmen)

https://www.verfassungsklage.at/files/120615_IA_VDS_Konsolidierte_Fassung.pdf

Kargl, Rolf Dieter / Tschohl, Christof,
http://akvorrat.at/sites/default/files/AKVorrat_PStSG_Stellungnahme_RV.pdf

Kargl, Rolf Dieter / Tschohl, Christof, / Czadilek, Alexander,
<https://akvorrat.at/sites/default/files/PStSG-3.pdf>

Kargl, Rolf Dieter / Tschohl, Christof, / Czadilek, Alexander,
<https://akvorrat.at/sites/default/files/PStSG-4.pdf>

Kargl, Rolf Dieter / Tschohl, Christof, / Czadilek, Alexander,
https://akvorrat.at/sites/default/files/AKVorrat_Stellungnahme_StPO%20A%CC%88nderung_Bundestrojaner.pdf

Bundesrechtsanwaltskammer (Deutschland)

Stellungnahme zum Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

<http://www.brak.de/zur-rechtspolitik/stellungnahmen-pdf/stellungnahmen-deutschland/2015/september/stellungnahme-der-brak-2015-32.pdf>

Bundesnetzagentur

https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS.html;jsessionid=D4F71FC38673C1A16E69195D6334AA05

Datenschutzbeauftragter des Freistaates Sachsen

http://www.saechdsb.de/images/stories/sdb_inhalt/behoerde/oea/bericht-funkzellenabfragen.pdf

Datenschutzbeauftragter des Landes Berlin

http://www.datenschutz-berlin.de/attachments/896/Pr__fbericht.pdf?1346753690

Der Standard

<http://derstandard.at/2000012472104/Stille-SMS-Ein-Perfektes-Tool-fuer-Ueberwachung>

<http://derstandard.at/2000009821924/31c3-App-snoopSnitch-spaecht-Handyueberwachung-aus>

<http://derstandard.at/2000026665430/Neuer-Rechtsschutz-Senat-kommt-etwas-spaeter>

<http://derstandard.at/2000061570381/Sicherheitspaket-SPOe-steht-hinter-Whatsapp-ueberwachung>

<http://derstandard.at/2000054819239/IBM-schafft-Home-Office-wieder-ab>

Deutscher Bundestag

BT-Drucksache 14/5166

<http://dip21.bundestag.de/dip21/btd/14/051/1405166.pdf>

BT-Drucksache 16/5846

<http://dip21.bundestag.de/dip21/btd/16/058/1605846.pdf>

BT-Drucksache 17/2637

<http://dip21.bundestag.de/dip21/btd/17/026/1702637.pdf>

BT-Drucksache 18/5088

<http://dip21.bundestag.de/dip21/btd/18/050/1805088.pdf>

Die Presse

[http://diepresse.com/home/wirtschaft/alpbach2010/1445831/Experten-empoert Faellt-mit-Amts-auch-Redaktionsgeheimnis](http://diepresse.com/home/wirtschaft/alpbach2010/1445831/Experten-empoert_Faellt-mit-Amts-auch-Redaktionsgeheimnis)

Faz.net

<http://www.faz.net/aktuell/feuilleton/debatten/ueberwachung/wie-man-kryptologie-und-verbrechensbekaempfung-balanciert-14319234.html>

Futurezone.at

<http://futurezone.at/netzpolitik/planen-keine-neuregelung-zur-vorratsdatenspeicherung/127.600.036>

Heise

<http://www.heise.de/tp/blogs/8/150615>

<https://www.heise.de/newsticker/meldung/Bundesnetzagentur-setzt-Vorratsdatenspeicherung-aus-3757527.html>

Internet-law.de (Thomas Stadtler)

<http://www.internet-law.de/2010/11/redaktionsgeheimnis-und-quellenschutz-auch-fur-blogger.html>

Intratext - Virtual Library

http://www.intratext.com/IXT/ENG0431/_PL.HTM#2D

news.orf.at

<http://news.orf.at/#/stories/2346791/>
<http://orf.at/stories/2400872/2400880/>

Österreichischer Nationalrat

http://www.parlament.gv.at/PAKT/VHG/XXV/ME/ME_00110/
https://www.parlament.gv.at/PAKT/PR/JAHR_2015/PK1364/index.shtml
https://www.parlament.gv.at/PAKT/VHG/XXV/AB/AB_02109/imfname_364266.pdf
https://www.parlament.gv.at/PAKT/VHG/XXV/AB/AB_03910/imfname_409316.pdf
https://www.parlament.gv.at/PAKT/VHG/XXIV/AB/AB_14397/fname_315133.pdf

Österreichischer Presserat

http://www.presserat.at/rte/upload/pdfs/grundsaeetze_fuer_die_publizistische_arbeit_ehrenkodex_fuer_die_oesterreichische_presse_idf_vom_14.11.2012.pdf

Posteo.de

Transparenzbericht 2014

https://posteo.de/site/transparenzbericht_2014

Profil

<http://www.profil.at/articles/1142/560/310153/bundestrojaner-trojanische-sitten>

SnoopSnitch-Wiki

<https://opensource.srlabs.de/projects/snoopsnitch/wiki/Wiki>

www.webinformation.at/

http://www.webinformation.at/material/AG_Online-Durchsuchung_Endbericht.pdf

Liste verwendeter Judikatur

Österreich

Verfassungsgerichtshof

VfSlg 18.146/2007

VfSlg 15.753/2000, 15.810/2000

VfSlg 1486/1933

VfSlg 5182/1965

VfSlg 9525/1982

VfSlg 10.897/1986

VfGH v 14.03.2012, U 466/11

VfGH v 29. 6. 2012, B 1031/11

VfGH v 29. 6. 2012, B 1031/11

VfGH v 28.11.2012, G47/12-11, 59/12-10

VfGH v 27.06.2014, G 47/2012-49

Ordentliche Gerichte

OGH v 6.12.1995, 13 Os 161/95

OGH v 17.6.1998, 13 Os 68/98.

OGH v 26.7.2005, 11 Os 57/05Z

OGH v 18.01.2011, 12 Os152/00.

Verwaltungsgerichtshof

VwGH 2015/04/0002

Deutschland

Bundesverfassungsgericht

BVerfG BeckRS 2004, 21087

BVerfG MMR 2004, 302

BVerfG MMR 2006, 217

BVerfG MMR 2008, 308

BVerfG MMR 2008, 315

BVerfG MMR 2009, 673
BVerfG NJW 1969, 1707
BVerfG NJW 1975, 588
BVerfG NJW 1984, 1741
BVerfG NJW 1990, 563
BVerfG NJW 1997, 386
BVerfG NJW 2002, 3458
BVerfG NJW 2003, 1787
BVerfG NJW 2004, 999
BVerfG NJW 2005, 1637
BVerfG NJW 2007, 117
BVerfG NJW 2007, 1865
BVerfG NJW 2007, 351
BVerfG NJW 2010, 833
BVerfG v. 20.4.2016, 1 BvR 966/09, 1 BvR 1140/09
BVerfG v. 24.4.2013, 1 BvR 1215/07
BVerfG ZUM-RD 2001, 142
BVerfG, NJW 879, 880.
BVerfGE 100, 313
BVerfGE 106, 28
BVerfGE 109, 279
BVerfGE 113, 348
BVerfGE 120, 274
BVerfGE 129, 208
BVerfGE 27, 1
BVerfGE 6, 32
BVerfGE 65, 1
BVerfGE 90, 255

Landesverfassungsgerichte

BayVerfGHE 1, 29
BayVerfGHE 2, 85

Ordentliche Gerichte

BGH DNotZ 1975, 420
BGH NJW 1968, 1773
BGH NJW 1981, 1089
BGH NStZ 2010, 646
LG Hamburg StV 2011, 148
LG Köln ZUM-RD 2012, 613
LG Landshut MMR 2011, 690
LG Mannheim wistra 2012, 400
OLG Braunschweig BeckRS 2009, 87886
OLG München AnwBl 1975, 159, 161
RG JW 1928, 2142

Verwaltungsgerichte

OVG Berlin-Brandenburg, BeckRS 2015, 47831, Rz 16
VG Düsseldorf, BeckRS 2014, 51325
VGH Kassel, WM 2009, 2004
OVG NRW v 22.06.2017, Az. 13 B 238/17

Europäischer Gerichtshof

EuGH 1.12.1998, Rs. C-326/96
EuGH Slg. 2001, I-7149, 7168.
EuGH Slg.1989, 2859.
EuGH v 16.10.2012, C-614/10.
EuGH v 5.5.2013, C-617/10 - Fransson
EuGH v 8. April C-293/12, C-594/12.
EuGH v 9.3.2010, C-518/07.
EuGH, NJW 2003, 35.

Europäischer Gerichtshof für Menschenrechte

EGMR EuGRZ 1992, 298, 300 – Lüdi ./.. Schweiz
EGMR JuS 2007, 369 – Buck ./.. Deutschland
EGMR NJW 1993, 718 – Niemitz ./.. Deutschland

EGMR NJW 2008, 3409 – Wieser u. Bicos Beteiligungen-GmbH ./ Österreich

EGMR ÖJZ 1992, 343 S./ Schweiz

EGMR ÖJZ 2000, 728 – W.R. ./ Österreich.

EGMR v 27/04/2017, 73607/13 – Sommer ./ Deutschland

Abkürzungsverzeichnis

Abs	Absatz
AVG	Allgemeines Verwaltungsverfahrensgesetz
BayVBl.	Bayerische Verwaltungsblätter
BeckOK	Beck'scher Onlinekommentar
BGBI	Bundesgesetzblatt
BGH	Bundesgerichtshof
BT	Bundestag
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des BVerfG (amtl. Sammlung)
dBGBI	Bundesgesetzblatt (Deutschland)
DÖV	Die öffentliche Verwaltung
dRGBI	Reichsgesetzblatt (Deutschland)
dStGB	Strafgesetzbuch (Deutschland)
dStPO	Strafprozessordnung (Deutschland)
dTKG	Telekommunikationsgesetz (Deutschland=
DStR	Deutsches Steuerrecht
ECG	E-Commerce-Gesetz
Fn	Fußnote
G 10 G	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldeheimnisses (Deutschland)
GG	Grundgesetz
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
JB1	Juristische Blätter
JRP	Journal für Rechtspolitik
JuS	Juristische Schulung
JW	Juristische Wochenschrift
K&R	Kommunikation und Recht
MMR	Multimedia und Recht
NJW	Neue Juristische Wochenschrift
NStZ	Neue Zeitschrift für Strafrecht
NStZ	Neue Zeitschrift für Strafrecht
NVwZ	Neue Zeitschrift für Verwaltungsrecht
öarr	Österreichisches Archiv für recht & religion
PAG	Polizeiaufgabengesetz (Bayern)
RAO	Rechtsanwaltsordnung
RG	Reichsgericht
RGBI	Reichsgesetzblatt
S	Satz
StGB	Strafgesetzbuch
StGBI	Staatsgesetzblatt
StGG	Staatsgrundgesetz
StPO	Strafprozessordnung
TRE	Theologische Realenzyklopädie
VfGH	Verfassungsgerichtshof
VGH	Verwaltungsgerichtshof
vgl	vergleiche
VR	Verwaltungsrundschau

WK	Wiener Kommentar
WRV	Weimarer Reichsverfassung
WRV	Weimarer Reichsverfassung
Z	Ziffer
z B	zum Beispiel
ZD	Zeitschrift für Datenschutz
ZIR	Zeitschrift für Informationsrecht
ZTR	Zeitschrift für Energie- und Technikrecht

Zusammenfassung

In den letzten Jahren haben sich die technischen Möglichkeiten stark verändert. Die Arten miteinander zu kommunizieren haben sich dabei in Alltag und Beruf vervielfacht. Dies wirkt sich auf die Kommunikation von Personen untereinander in allen Bereichen aus; auch auf das Kommunikationsverhalten zwischen Personen und Berufsgeheimnisträgern. Ebenso vielfältig wie die Möglichkeiten zu kommunizieren, sind die technischen Möglichkeiten diese zu überwachen. An der Schnittstelle zwischen Berufsgeheimnisträgerschutz und Telekommunikationsüberwachung setzt diese Arbeit an. Die Überwachung auf Telekommunikation stellt für sich genommen eine der größten Herausforderungen für den Grundrechtsschutz dar. Bei jedem Terrorakt sind die Rufe nach möglichst flächendeckender Überwachung der Telekommunikation da. Die Grundrechte, welche die Telekommunikation schützen müssen hierbei stets auf neue erstritten werden. Der Schutz der Telekommunikation ist umfassend und geht über den eigentlichen Begriff der Telekommunikation vom Beginn bis zum Ende der Verbindung hinaus. Das Verfassungsrecht schützt auch den Entstehungsprozess und die gespeicherte Kommunikation auf dem Endgerät. Der Vergleich mit Deutschland zeigt hierbei, dass der Grundrechtsschutz dort ähnlich ist, jedoch von der Systematik anders was zu teilweise strengeren, teilweise zu weniger strengen Anforderungen führt. Interessant erweist sich hierbei der Vergleich des Fernmeldegeheimnisses in beiden Verfassungen (Art 10a StGG u. Art 10 GG), die beide ähnliche Inhalte haben, deren Interpretation aber unterschiedlich ist. Durch die Europäische GRC erfährt der Grundrechtsschutz europaweit zwar keine Vereinheitlichung, aber es besteht nunmehr die Möglichkeit, dass sich neue Grundrechtsperspektiven auftun. So ist zum Beispiel der Schutz der Menschenwürde, wie er in Art 1 Abs 1 GG in Deutschland eine wichtige Grundlage des Verfassungsrechtes ist, in der Verfassungsrechtsordnung in Österreich bislang unbekannt. Die Europäische GRC, deren Art 1 GRC Art 1 GG nachempfunden ist, kann hier zu einer neuen Grundrechtsinterpretation und somit zu weiterem Schutz verhelfen. Der Schutz der Berufsgeheimnisträger stammt teilweise noch aus einer Zeit, in welcher nicht jedes Jahr neue Überwachungsmaßnahmen im Nationalrat diskutiert wurden. Hier sind Reformen nötig, die den Berufsgeheimnisträgerschutz auf eine solide Basis stellen, so dass er auch bei neuen Gesetzgebungsverfahren nicht jedes Mal explizit erwähnt werden muss, um Schutz zu erfahren. Ferner erweisen sich Kontrollelemente wie der Rechtsschutzbeauftragte und der in der Verfassung bei manchen Grundrechten ange-

ordnete richterliche Befehl als reformbedürftig, da sie insgesamt keinen ausreichenden Schutz vor Überwachung mehr bieten.

Abstract

In the recent years technological progress has emerged. The ways people communicate with each other have multiplied in both private and business context. This technical evolution influences the way people communicate with each other. This applies to the communication between people and bearers of professional secrecy. But not only have the possibilities to communicate multiplied but the ways to surveil telecommunication. This thesis starts at the interface between the protection of professional secrets and the surveillance of telecommunication. Surveillance of telecommunication may be the greatest challenge in the field of human rights of this century. After every terrorist attack politics call for a more extensive surveillance of communication. The protection of telecommunication through Human Rights is comprehensive and protects more than the communication between two individuals. Constitutional Law protects communication before sending and after receiving the message. Comparing Austria to Germany shows that the protection of communication through Constitutional Law is similar but with some systematic differences that may lead to a stricter or less strict requirements for the surveillance of communication. The protection of the secrecy of telecommunication in both constitutions (Art 10a StGG and Art 10 GG) is of high interest for this research because both Human Rights do have a similar wording but a rather different interpretation. There is no standardization of Human Rights throughout Europe through the influence of the European Charter of Fundamental Rights but the introduction of this charter may lead to new perspective for the interpretations of Human Rights. One major example is the protection of Human Dignity as a key foundation of the German Constitution which is unknown as a Human Right to the Austrian Constitution. As the European Charter of Human Rights protects in its Art 1 Human Dignity as its key foundation, which is actually based on the influence of German Constitutional Law, this influences Austrian Constitutional Law and may lead to a better protection of Human Rights. The protection of professional secrecy is dated back to a time where new methods of surveillance of communication weren't a topic arising every year in the Austrian Parliament (*Nationalrat*). So there is a need for reform to put the protection of professional secrecy on a foundation that strengthens its legal basis so that there is no need to take care of this topic in proposed legislation. Furthermore, elements of control like the Legal Protection Commissioner (*Rechtsschutzbeauftragter*) and the constitu-

tional requirement of a court decision prior to certain surveillances needs to be reformed in order to guarantee a sufficient protection of Fundamental Rights.

Lebenslauf

Ermano Geuer

geboren am 22.08.1984 in Offenbach / Main, Deutschland

Studium:

Oktober 2004 – September 2009	Universität Passau, Studium Rechtswissenschaften, Abschluss im Juli 2009 mit dem Ersten Juristischen Staatsexamen (Dipl.-Jur.)
seit August 2012	Universität Wien, Doktoratsstudium Rechtswissenschaften

Berufstätigkeit:

Dezember 2005 – Dezember 2008	Universität Passau, Lehrstuhl Prof. Dr. Braun (studentische Hilfskraft)
September 2009 – März 2011	Universität Passau, Lehrstuhl Prof. Dr. Braun (nebenberufl. wiss. Hilfskraft)
Oktober 2009 – Oktober 2011	Oberlandesgericht München, Rechtsreferendar Abschluss im Oktober 2011 mit dem Zweiten Staatsexamen (Ass. iur.)
August 2011 – August 2013	Universität Passau, Lehrstuhl Prof. Dr. Heckmann, (wissenschaftlicher Mitarbeiter)
September 2013 – Oktober 2014	Media Saturn Holding GmbH, Legal Counsel
seit November 2014	s IT Solutions AT Spardat GmbH, Legal Counsel

Lehre:

Wintersemester 2009/10, Sommersemester 2010, Wintersemester 2010/11: Große Übung im Öffentlichen Recht; Universität Passau

Wintersemester 2010/11: Grundkurs im Bürgerlichen Recht; Universität Passau

Sommersemester 2011: Grundkurs im Öffentlichen Recht (Grundrechte); Universität Passau

gelegentliche Vorlesungsvertretung: Internetrecht, Verwaltungsrecht; Universität Passau

Wissenschaftliche Publikationen (Auswahl):

1. Die Kruzifixentscheidung des EGMR - Auferstehung einer alten Rechtslage?, VR 2011, 259
2. Verstößt die Möglichkeit der Nutzungsbeschränkung bei öffentlichen Einrichtungen auf Gemeindeangehörige nach Art 21 Abs 1 GO gegen die Grundfreiheiten der Europäischen Union, BayVBl. 2011, 752
3. Vorratsdatenspeicherung in Österreich, ZD 2012, 421
4. Der praktische Fall: "Nun danket alle Gott", VR 2012, 310
5. Einwilligung in Cookieempfang durch Browsereinstellungen?, Schlussfolgerungen aus einer Auslegung der gesetzlichen Regelung in Österreich, ITRB 2012, 20
6. Die Haushaltsabgabe für den öffentlich-rechtlichen Rundfunk in Deutschland - Modell für Österreich?, MR 2012, 219
7. Das Fernmeldegeheimnis als gesetzliches Verbot, ZD 2012, 515
8. Zur Verfassungswidrigkeit der "Haushaltsabgabe" für den öffentlich-rechtlichen Rundfunk, VR 2012, 378
9. Zur Bedeutung des Kriteriums "in völliger Unabhängigkeit" bei Datenschutzkontrollstellen, ZIR 2013, 8
10. Der neue Rundfunkbeitrag aus europarechtlicher Sicht, CR 2013, 156.
11. Der neue Rundfunkbeitrag aus kommunaler Sicht, Hessische Städte- und Gemeindezeitung 2013, 115
12. Die Niederlassung im datenschutzrechtlichen Sinne, ZIR 2013, 151
13. Vorratsdatenspeicherung – Nach der Entscheidung des EuGH vom 08.04.2014 - C-293/12, C-594/12, juris AnwZert ITR 10/2014, Anm. 3
14. Zur Rechtsprechung der Landesverfassungsgerichte und Verwaltungsgerichte zum Rundfunkbeitrag, juris AnwZert ITR 22/2014, Anm. 3
15. Der praktische Fall: Rock mi‘, VR 2015, 422
16. Zielgerichtete Werbung für Kunden in sozialen Netzwerken, Dako 2017, 34