

Inhaltsverzeichnis

1. Einleitung.....	25
2. Grundsätzliches zu technischen staatlichen Überwachungsmaßnahmen	27
2.1. Rechtfertigung und Auswirkungen technischer staatlicher Überwachungsmaßnahmen	27
2.2. Effizienz und Rechtswirklichkeit technischer staatlicher Überwachungsmaßnahmen	32
2.3. Grundrechtliche Schranken der Anwendung technischer staatlicher Überwachungsmaßnahmen.....	35
2.3.1. Grundrechtseingriffe und Verhältnismäßigkeit.....	35
2.3.1.1. Allgemeines.....	35
2.3.1.2. Legitimität	36
2.3.1.3. Eignung	36
2.3.1.4. Erforderlichkeit.....	37
2.3.1.5. Verhältnismäßigkeit im engeren Sinne	39
2.3.2. Grundrechtliches Determinierungsgebot.....	39
2.3.3. Verfassungsrechtliche Beweisverbote	40
3. Die SPG-Novelle 2007	43
3.1. Zur Entstehungsgeschichte des § 53 Abs 3a und 3b SPG nF.....	43
3.2. Die Befugnisse des § 53 Abs 3a SPG	44
3.2.1. Allgemeines	44
3.2.2. Die Befugnisse des § 53 Abs 3a Z 1 und § 53 Abs 3a Satz 2 SPG	47
3.2.3. Die Befugnis des § 53 Abs 3a Z 2 SPG	50
3.2.3.1. Allgemeines.....	50
3.2.3.2. Der Nachrichtenbegriff des § 53 Abs 3a Z 2 SPG	52
3.2.3.3. Zur Bestimmtheit der Nachricht	58
3.2.3.4. Zu übermittelnde Daten	62
3.2.3.5. Eingriff in das Fernmeldegeheimnis	65
3.2.3.6. Eingriff in das Grundrecht auf Achtung der Privatsphäre.....	69
3.2.3.7. Eingriff in das Grundrecht auf Datenschutz.....	75
3.2.3.8. Der Gleichheitssatz.....	76
3.2.3.9. Zur Unbestimmtheit des § 53 Abs 3a Z 2 SPG.....	79
3.2.4. Die Befugnis des § 53 Abs 3a Z 3 SPG	81
3.2.4.1. Kreis der auskunftspflichtigen Provider	81
3.2.4.2. Exkurs: Statische und dynamische IP-Adressen	83
3.2.4.3. Das Verhältnis zwischen Auskunftspflicht und Löschungspflicht	85
3.2.4.4. Eingriff in das Fernmeldegeheimnis.....	87
3.2.4.5. Eingriff in das Grundrecht auf Achtung der Privatsphäre.....	87
3.2.4.6. Eingriff in das Grundrecht auf Datenschutz.....	89
3.2.4.7. Der Gleichheitssatz.....	89

3.3. Die Befugnisse des § 53 Abs 3b SPG	91
3.3.1. Voraussetzungen.....	91
3.3.1.1. Gefahrensituation.....	91
3.3.1.2. Die sicherheitspolizeilichen Aufgaben im Anwendungsbereich des § 53 Abs 3b SPG.....	93
3.3.2. Auskunft über Standortdaten und IMSI	94
3.3.2.1. Exkurs: Auskunft über Standortdaten im Falle von Notrufen: § 98 TKG 2003.....	95
3.3.3. Dokumentation des Auskunftsbegehrens	97
3.3.3.1. Standortdaten aus der Vergangenheit und der Gegenwart	98
3.3.4. Die Ortung von Personen aus verfassungsrechtlicher Sicht.....	99
3.3.4.1. Standortdaten im Lichte des Fernmeldegeheimnisses.....	99
3.3.4.2. Standortdaten aus Sicht des Art 8 EMRK bzw § 1 DSGVO	100
3.3.5. Technische Mittel zur Lokalisierung	102
3.3.5.1. Die IMSI.....	102
3.3.5.2. Der IMSI-Catcher	103
3.4. Rechtsnatur von Anfragen gem § 53 Abs 3a und 3b SPG.....	105
3.4.1. Verfassungsrechtliche Bindung des Gesetzgebers	105
3.4.2. Gesetzliche Vorgaben für die Sicherheitsbehörden	105
3.4.3. Die Rechtsqualität des Formulars	107
3.5. Rechtsschutz.....	110
3.5.1. Zur mangelnden Kenntnis des Betroffenen von der Maßnahme	110
3.5.2. Grundsätzliches zum Rechtsschutzbeauftragten	113
3.5.2.1. Weisungsfreistellung des Rechtsschutzbeauftragten.....	115
3.5.2.2. Bestellung, Rechte und Pflichten des Rechtsschutzbeauftragten	116
3.5.3. Rechtsschutz durch den Rechtsschutzbeauftragten	117
3.5.4. Form des Rechtsschutzes	118
3.5.4.1. Zuständigkeit der UVS und der DSK	118
3.5.4.2. Auskunftsanspruch gemäß § 26 DSGVO	119
3.5.5. Beschwerde an die UVS bzw die DSK.....	121
3.5.5.1. Der Betroffene	121
3.5.5.2. Der Provider	121
3.5.5.3. Parteistellung des Betroffenen in Verfahren des Providers.....	122
3.5.6. Individualantrag gem Art 140 B-VG	123
3.6. Zusammenfassung.....	124
4. Die Vorratsdatenspeicherung von Verkehrs- und Standortdaten	126
4.1. Die Vorratsdatenspeicherungs-RL	126
4.1.1. Der Kreis der speicherungspflichtigen Provider.....	127
4.1.2. Art und Umfang der zu speichernden Daten.....	129
4.1.2.1. Allgemeines.....	129

4.1.2.2.	Die Bestimmung des Art 5 Abs 1 Vorratsdaten- speicherungs-RL.....	130
4.1.2.3.	Telefonfestnetz und Mobilfunk.....	134
4.1.2.4.	Internetzugang	137
4.1.2.5.	Internet-E-Mail	140
4.1.2.6.	Internet-Telefonie	143
4.1.2.7.	Eine tabellarische Darstellung der Speicherpflichten	145
4.1.3.	Die zweifelhafte Rechtsgrundlage der Vorratsdatenspeicherungs- RL.....	147
4.1.4.	Eingriff in das Grundrecht auf Achtung der Privatsphäre.....	152
4.2.	Der österreichische Umsetzungsentwurf.....	163
4.2.1.	Materielle Unterschiede.....	163
4.2.2.	Der Eingriff in Art 8 EMRK und § 1 DSGVO 2000	164
4.2.3.	Der Gleichheitssatz.....	165
4.3.	Zusammenfassung.....	168
5.	Die Online-Durchsuchung	171
5.1.	Begriffsbestimmung.....	171
5.2.	Technische Aspekte der Online-Durchsuchung.....	173
5.2.1.	Formen der Zugangsverschaffung zu einem Computersystem	173
5.2.1.1.	Social Engineering.....	173
5.2.1.2.	Ausnutzung technischer Sicherheitslücken.....	175
5.2.1.3.	Physische Angriffe	176
5.2.1.4.	Backdoors.....	176
5.2.2.	Formen der Ausnutzung des Zugangs.....	177
5.2.3.	Technische Gegenmaßnahmen und Möglichkeiten ihrer Über- windung	178
5.2.3.1.	Präventive Sicherheitsmaßnahmen	178
5.2.3.2.	Detektive Sicherheitsmaßnahmen.....	181
5.2.3.3.	Korrektive Sicherheitsmaßnahmen	181
5.2.4.	Das Erfordernis der kontinuierlichen Weiterentwicklung der Angriffsmethoden	182
5.2.5.	Technische Alternativen zur Online-Durchsuchung	182
5.2.5.1.	Hardware Keylogger.....	183
5.2.5.2.	Das Auffangen elektromagnetischer Abstrahlung	183
5.3.	Allgemeines zum Beschuldigten und zu dessen Rechten nach der StPO	184
5.4.	Notwendigkeit einer gesetzlichen Grundlage.....	186
5.5.	Zulässigkeit der Online-Durchsuchung nach den Bestimmungen der StPO	187
5.5.1.	Die Auskunft über Daten einer Nachrichtenübermittlung.....	188
5.5.1.1.	Exkurs: Auskunft über Stammdaten	189
5.5.1.2.	Voraussetzungen der Auskunft über Daten einer Nachrichtenübermittlung	192
5.5.2.	Überwachung von Nachrichten.....	193
5.5.2.1.	Voraussetzungen der Nachrichtenüberwachung	195
5.5.3.	Optische und akustische Überwachung von Personen	196

5.5.3.1.	Screenshots	197
5.5.3.2.	Keylogger	199
5.5.3.3.	Durchsuchen von Datenspeichern.....	199
5.5.3.4.	Optische und akustische Überwachung des Computer-Arbeitsplatzes	199
5.5.3.5.	Voraussetzungen der optischen und akustischen Überwachung.....	200
5.5.4.	Hacking zur Durchführung bestehender Befugnisse?	202
5.5.5.	Verfahren	204
5.5.6.	Analoge Anwendung der Regeln über die Durchsuehung von Orten und Gegenständen.....	207
5.6.	Zulässigkeit der Online-Durchsuehung nach den Bestimmungen des MBG und SPG	209
5.7.	Grundrechtliche Beurteilung der Online-Durchsuehung.....	211
5.7.1.	Recht auf Achtung der Privatsphäre (Art 8 EMRK)	211
5.7.1.1.	Schutzbereich	211
5.7.1.2.	Gesetzliche Ermächtigung	212
5.7.1.3.	Ziel und Notwendigkeit in einer demokratischen Gesellschaft	213
5.7.2.	Grundrecht auf Datenschutz (§ 1 DSG 2000)	215
5.7.3.	Recht auf eine wirksame Beschwerde (Art 13 EMRK)	216
5.7.4.	Fernmeldegeheimnis	218
5.7.4.1.	Schutzumfang	218
5.7.5.	Das Hausrecht	220
5.7.5.1.	Maßnahmen, die zur Gänze online erfolgen	222
5.7.5.2.	Maßnahmen, bei denen vom Hausrecht geschützte Räume betreten werden	223
5.8.	Zusammenfassung.....	224
6.	Resümee	227
Anhang 1:	Das für Auskunftsverlangen gem § 53 Abs 3a und 3b SPG zu verwendende Formular.....	231