

Schriften zum Öffentlichen Recht

Band 1530

Offene Ermächtigungsgrundlagen im Strafprozessrecht

Verfassungsrechtliche Determinanten für den Einsatz
moderner Kommunikationstechnologie

Von

Hannah Amann



Duncker & Humblot · Berlin

HANNAH AMANN

Offene Ermächtigungsgrundlagen im Strafprozessrecht

Schriften zum Öffentlichen Recht

Band 1530

Offene Ermächtigungsgrundlagen im Strafprozessrecht

Verfassungsrechtliche Determinanten für den Einsatz
moderner Kommunikationstechnologie

Von

Hannah Amann



Duncker & Humblot · Berlin

Die Juristische Fakultät der Julius-Maximilians-Universität Würzburg
hat diese Arbeit im Jahre 2020 als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in
der Deutschen Nationalbibliografie; detaillierte bibliografische Daten
sind im Internet über <http://dnb.d-nb.de> abrufbar.

Alle Rechte vorbehalten
© 2024 Duncker & Humblot GmbH, Berlin
Satz: 3w+p GmbH, Rimpf
Druck: CPI books GmbH, Leck
Printed in Germany

ISSN 0582-0200
ISBN 978-3-428-18284-8 (Print)
ISBN 978-3-428-58284-6 (E-Book)
Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ☺

Internet: <http://www.duncker-humblot.de>

Vorwort

Die vorliegende Arbeit wurde im Sommersemester 2020 von der Juristischen Fakultät der Julius-Maximilians-Universität Würzburg als Dissertationsschrift angenommen. Literatur und Rechtsprechung konnten bis einschließlich Februar 2020 berücksichtigt werden.

Herzlich danken möchte ich meinem Doktorvater, Herrn Professor Dr. Markus Ludwigs. Er ermöglichte mir nicht nur meinem Forschungsinteresse an der Schnittstelle zwischen Verfassungs- und Strafrecht nachzugehen, sondern begleitete das Promotionsvorhaben mit fürsorglichem Engagement und inspirierenden Impulsen. Hervorzuheben ist – neben der hervorragenden fachlichen Betreuung – auch sein Verständnis für Verzögerungen, die der während der Dissertationszeit und Veröffentlichungsvorbereitung aufgetretenen Phasen beruflicher Belastung geschuldet waren.

Für die zügige Erstellung des Zweitgutachtens, das viele wertvolle Hinweise aus der strafrechtlichen Perspektive enthielt, danke ich Herrn Professor Dr. Frank-Peter Schuster, Mag. iur.

Dem Verlag Duncker & Humblot und insbesondere Herrn Dr. Florian R. Simon, LL.M., danke ich für die Aufnahme in die „Schriften zum Öffentlichen Recht“ und seine entgegenkommende Unterstützung im Veröffentlichungsprozess.

Großer Dank gebührt allen, welche die Entstehung dieser Schrift gefördert und mit ihrer Unterstützung erst möglich gemacht haben. Zu nennen sind hier zunächst meine Kolleginnen und Kollegen am Lehrstuhl für Öffentliches Recht und Europarecht der Universität Würzburg. Schließlich danke ich meinen Eltern und Geschwistern herzlich, deren Rückhalt für das Entstehen der Arbeit von unschätzbarem Wert war.

Würzburg, im März 2024

Hannah Amann

Inhaltsverzeichnis

Einleitung	19
§ 1 Allgemeiner Teil	22
A. Freiheitsrechtliche Grundlagen	22
I. Relevante Grundrechte	22
1. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG	23
a) Das Recht auf informationelle Selbstbestimmung	24
b) Das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	28
aa) Schutzbereich	29
bb) Grundrechtsschranken	32
(1) Anforderungen materieller und verfahrensrechtlicher Art	32
(2) Kernbereichsschutz	33
cc) Verhältnis zu anderen Grundrechten	34
(1) Konkurrenz zum Schutz der informationellen Selbstbestimmung	35
(2) Konkurrenz zum Schutz des Telekommunikationsgeheimnisses	36
(3) Konkurrenz zum Schutz der Unverletzlichkeit der Wohnung	37
dd) Neue Grundrechtsausprägung in der Kritik	38
(1) Kritikpunkte	39
(2) Würdigung	42
(a) Unterschied bzgl. der Anforderungen an das beeinträchtigte Rechtsgut?	43
(b) Unterschied bzgl. der Intensität der Persönlichkeitsrelevanz?	43
(c) Zwischenergebnis	44
ee) Fazit	46
2. Das Telekommunikationsgeheimnis	46
3. Die Unverletzlichkeit der Wohnung	50
4. Entwicklungs offene Grundrechte in der Kritik	55
a) Untersuchung der entwicklungs offenen Grundrechte	55
aa) Kritik am Telekommunikationsgeheimnis	55
bb) Kritik am Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	56
b) Untersuchung der Kritikpunkte	57
aa) Verlust klarer Abgrenzungslinien	57

bb) Verlust der Aussagekraft des Verfassungstextes	57
cc) Vorwurf des Rechtsprechungsaktivismus	58
dd) Große Reichweite der Schutzbereiche	60
ee) Fehlende gesetzliche Legitimation	61
(1) Legitimation verfassungsgerichtlicher Ergänzungen	61
(2) Legitimation gesetzgeberischer Ergänzungen	62
c) Ergebnis der Untersuchung	62
II. Der additive Grundrechtseingriff	63
1. Punktualität eines Eingriffs als Ausgangspunkt	64
2. Terminologie	65
3. Voraussetzungen	66
a) Einfacher additiver Grundrechtseingriff	66
b) Fortgesetzter additiver Grundrechtseingriff	69
4. Abgrenzung	69
a) Abgrenzung der Belastungskumulation von der Grundrechtskonkurrenz	69
aa) Grundrechtskonkurrenz	69
bb) Maßgebliches Abgrenzungskriterium	71
b) Abgrenzung der Belastungskumulation von der Grundrechtskollision	71
c) Abgrenzung der Belastungskumulation von der Schutzbereichskumulation	71
aa) Schutzbereichskumulation	71
bb) Maßgebliches Abgrenzungskriterium	73
5. Rechtsfolge und Prüfungssystematik	74
a) Verbot der übermäßigen Gesamtbelastung des Bürgers	74
b) Verbot der Belastungskumulation als Bestandteil der Wesensgehaltsgarantie	76
6. Lösungsansätze der Rechtsprechung	77
a) Verfahrensrechtliche Sicherungen	78
b) Beobachtungspflichten	78
7. Justiziabilität	79
a) Einfacher additiver Grundrechtseingriff	79
b) Fortgesetzter additiver Grundrechtseingriff	79
8. Zusammenfassende Schlussbetrachtung	80
B. Grenzen für die Technikoffenheit von Ermittlungsbefugnissen	81
I. Interpretation bestehender Ermächtigungsgrundlagen	82
1. Die Analogie im Strafprozessrecht	82
a) Gesetzlichkeitsprinzip	83
b) Analogieverbot	84

c) Analogieverbot im Strafprozessrecht	85
aa) Keine Geltung des Analogieverbots im Strafprozessrecht	86
(1) Gänzliche Verneinung der Geltung	86
(2) Verneinung der Geltung unter Gewährung von Ausnahmen	86
(a) Auslegung des Art. 103 Abs. 2 GG	86
(aa) Wortlaut	87
(bb) Systematik	87
(cc) Historie	87
(dd) Telos	88
(ee) Europarecht	88
(ff) Zwischenergebnis	91
(b) Gewährung von Ausnahmen	91
bb) Geltung des Analogieverbots im Strafprozessrecht	93
cc) Vermittelnde Position	94
dd) Stellungnahme	97
d) Rechtsanwendung des Analogieverbotes	102
e) Fazit	106
2. Die Kombination von Ermächtigungsgrundlagen	109
a) Gegenstand der Untersuchung	110
b) Meinungsstand	111
aa) Unzulässigkeit der Kombination von Ermächtigungsgrundlagen ...	111
bb) Zulässigkeit der Kombination von Ermächtigungsgrundlagen	113
cc) Würdigung	114
3. Die Ableitung einer Ermächtigungsgrundlage aus einer Annexkompetenz	116
a) Grundlagen	117
aa) Begriff	117
bb) Praktische Relevanz	118
b) Zulässigkeit	118
aa) Meinungsstand	119
(1) Rechtsordnung mit Annexkompetenzen	119
(2) Rechtsordnung mit normierten Begleitmaßnahmen	120
(3) Vermittelnde Ansicht	121
(4) Zusammenfassende Stellungnahme	121
bb) Auslegung	122
(1) Abgrenzung zur Rechtsfortbildung	122
(2) Voraussetzungen der Typizität und der Verhältnismäßigkeit ...	123
(a) Kumulatives Vorliegen	123
(b) Alternatives Vorliegen	124
(aa) Kriterium der Typizität	124
(α) Verzicht auf das Kriterium der Typizität	124

(αα) Entbehrlichkeit bei einem geringfügigen Eingriff	125
(ββ) Entbehrlichkeit aus Gründen der Sachgerechtigkeit und Praktikabilität	127
(γγ) Leerlaufen strafprozessualer Eingriffsgrundlagen	128
(δδ) Würdigung	129
(β) Einschränkung des Kriteriums der Typizität	131
(γ) Zwischenergebnis	132
(bb) Verzicht auf das Kriterium der Verhältnismäßigkeit	132
(c) Zwischenfazit	133
cc) Fazit	133
4. Zusammenfassende Schlussbetrachtung	134
II. Schaffung neuer Ermächtigungsgrundlagen	135
1. Die Gesetzgebung auf Vorrat	135
a) Problemaufriss	135
aa) Beispiel des § 51 Abs. 2 BKAG	136
bb) Schwierigkeit	136
b) Offene Formulierungen im Gesetz	139
aa) Prognosen	140
(1) Begriff und Funktion	140
(2) Zulässigkeit	141
bb) Rezeption technischer Regelungen	143
(1) Begriffserläuterungen	143
(2) Funktionen	145
(a) Entlastungsfunktion	145
(b) Anpassungs- und Dynamisierungsfunktion	145
(c) Kooperationsfunktion	146
(3) Erreichung der Funktionen im Sicherheitsrecht?	148
(a) Entlastungsfunktion	149
(b) Anpassungs- und Dynamisierungsfunktion	149
(c) Kooperationsfunktion	150
(4) Zulässigkeit	150
c) Vergleich	154
aa) Prognose	154
(1) Parallelen	154
(2) Unterschied	155
bb) Technikklauseln	155
(1) Parallelen	155

(2) Unterschiede	156
(a) Ausrichtung	156
(b) Funktionen	157
(aa) Entlastungsfunktion	157
(bb) Anpassungs- und Dynamisierungsfunktion	158
(cc) Kooperationsfunktion	159
cc) Ergebnis des Vergleichs	159
d) Zulässigkeit der Gesetzgebung auf Vorrat	159
aa) Verfassungskonformität	159
(1) Verstoß gegen den Verhältnismäßigkeitsgrundsatz	160
(a) Keine technische Realisierbarkeit	161
(b) Zeitlich ungewisse technische Realisierbarkeit	161
(aa) Einschüchterungseffekte	162
(bb) Gefahr der falschen Auslegung bzw. des Missbrauchs	162
(cc) Zwischenfazit	163
(2) Verstoß gegen den Bestimmtheitsgrundsatz	164
(a) Bestimmtheit	164
(b) Unbestimmtheit	164
bb) Rechtsfolgen	167
(1) Regelung über die spätere Billigung	167
(2) Kompletter Verzicht einer Normierung	169
cc) Zwischenergebnis	170
2. Fazit	170
§ 2 Besonderer Teil	171
C. Die Quellen-Telekommunikationsüberwachung	171
I. Allgemeine Grundlagen	171
1. Begriffserläuterung und Inhalt	172
2. Abgrenzung	173
3. Praktische Notwendigkeit	174
II. Technische Grundlagen	176
1. Primärmaßnahme	176
2. Sekundärmaßnahme	177
III. Verfassungsrechtliche Grundlagen	180
1. Eingriffscharakter der Quellen-TKÜ	180
2. Art. 13 GG	181
a) Meinungsstand in Literatur und Rechtsprechung	181
b) Würdigung	182

3. Art. 10 GG	183
a) Abgrenzung zu Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG	184
aa) Rechtsprechung des BVerfG	184
bb) Würdigung	184
b) Sachgemäße Gleichsetzung mit klassischer Telefonie?	185
aa) Rechtsprechung des BVerfG	185
bb) Gegenmeinung aus der Literatur	185
cc) Würdigung	186
c) Gesamtwürdigung der technikoffenen Rechtsprechung des BVerfG	188
d) Fazit	189
IV. Analyse der Verfassungsmäßigkeit	190
1. Primärmaßnahme	190
a) Uneinigkeit vor Gesetzeserlass	191
aa) §§ 100a, 100b StPO a.F. in direkter Anwendung	192
(1) Geltung des Verbots einer Vorratsgesetzgebung?	192
(a) Annahme des Verbots der Vorratsgesetzgebung	193
(b) Ablehnen einer absoluten Grenze	193
(c) Zwischenergebnis	194
(2) Technikoffene Auslegung	195
(a) §§ 100a, 100b StPO a.F. als Rechtsgrundlage	195
(b) Verfassungsrechtliche Defizite	196
(aa) Argumentativer Fehlschluss	196
(α) Meinungsstand	196
(β) Würdigung	197
(bb) Mangelnde Umsetzung der Anforderungen des BVerfG	198
(α) Defizitäre Ausführung technischer Vorkehrungen	198
(β) Defizitäre Realisierung rechtlicher Vorgaben	199
(γ) Defizitäre Beachtung systematischer Konsequenzen	200
(δ) Würdigung	200
(c) Zwischenergebnis	201
bb) §§ 100a, 100b StPO a.F. in analoger Anwendung	202
cc) Annexkompetenz zu § 100a StPO a.F.	204
dd) Strafprozessuale Ermittlungsgeneralklausel	205
ee) Kombination von Ermächtigungsgrundlagen	207
ff) Fazit	208
b) Klarstellung durch Gesetzeserlass?	209
aa) Rechtsgrundlage des § 100a Abs. 1 S. 2, 3 StPO	210
(1) Regelung des § 100a Abs. 1 S. 2 StPO	211
(2) Regelung des § 100a Abs. 1 S. 3 StPO	212

- (3) Einschränkung der Überwachung 213
 - (a) Regelungskomplex des § 100a Abs 5 S. 1 Nr. 1 StPO 214
 - (b) Regelungskomplex der § 100a Abs. 5 S. 1 Nr. 2–3, S. 2 und S. 3 StPO 215
- bb) Neue Norm in der Kritik 215
 - (1) Gesetzgebungsprozess 215
 - (a) Zweifelhafter Änderungsantrag nach § 82 Abs. 1 GO BT .. 216
 - (b) Vorwurf der Verschleierung 217
 - (aa) Verhinderung einer Auseinandersetzung 217
 - (bb) Keine Eilbedürftigkeit 218
 - (c) Verhinderung einer Beratung 219
 - (d) Stellungnahme 219
 - (2) Verfassungskonformität 220
 - (a) § 100a Abs. 1 S. 2 StPO 220
 - (b) § 100a Abs. 1 S. 3 StPO 221
 - (aa) Ermittlung des Prüfungsmaßstabs 221
 - (α) Anforderungen des Art. 10 GG 222
 - (β) Anforderungen des Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG 223
 - (γ) Würdigung 225
 - (bb) Erfüllung der Anforderungen von Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG? 227
 - (α) Vorgaben des BVerfG 227
 - (β) Bestimmtheit 228
 - (αα) Verstoß gegen das Verbot der Gesetzgebung auf Vorrat? 229
 - (ββ) Durchführbarkeit der gesetzlichen Vorgaben? 229
 - (γγ) Verstoß gegen das Gebot des Grundrechtsschutzes durch Verfahrensgestaltung und den Wesentlichkeitsgrundsatz? 234
 - (γ) Angemessenheit 236
 - (αα) Schrankentransfer von präventiven zu repressiven Eingriffen 236
 - (ββ) Eingriffsanlass des § 100a Abs. 1 S. 3 StPO 238
 - (δ) Verfahrensrechtliche Sicherungen 241
 - (αα) Protokollierungsvorschriften 242
 - (ββ) Anordnungsvorschriften 243
 - (γγ) Kernbereichsvorschriften 245
 - (cc) Zwischenergebnis 247
- cc) Fazit 247

2. Sekundärmaßnahme	247
a) Wahrung des Gesetzesvorbehalts	248
aa) Grundrechtsrelevanz	248
(1) „Ob“ der Grundrechtsrelevanz	248
(2) „Wie“ der Grundrechtsrelevanz	249
(a) Relevante Grundrechte	249
(aa) Art. 10 GG in Abgrenzung zu Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG	249
(bb) Art. 13 Abs. 1 GG	251
(b) Grundrechtsrelevanz der alten Rechtslage	251
(c) Grundrechtsrelevanz der neuen Rechtslage	252
bb) Vorliegen einer Ermächtigungsgrundlage?	254
(1) Alte Rechtslage	254
(2) Neue Rechtslage	255
(a) Regelung zum „Ob“ des Begleiteingriffs	256
(b) Regelung zum „Wie“ des Begleiteingriffs	257
cc) Zwischenergebnis	259
b) Weitere Determinanten des Verfassungsrechts	259
aa) Angemessenheit	259
bb) Grundsatz der Offenheit	263
cc) Zwischenergebnis	267
c) Fazit	267
V. Zusammenfassende Schlussbetrachtung	267
D. Die stille SMS	268
I. Allgemeine Grundlagen	268
1. Begriffserläuterung und Inhalt	269
2. Abgrenzung	270
a) IMSI-Catcher	270
b) Erhebung von Verkehrsdaten	271
3. Praktische Notwendigkeit	272
II. Technische Grundlagen	275
III. Verfassungsrechtliche Grundlagen	278
1. Art. 10 GG	278
a) Begriff der Telekommunikation	279
b) Wandel der höchstrichterlichen Rechtsprechung	279
aa) Alte Rechtsprechung des BGH	280
bb) Kritik	280
cc) Rechtsprechung des BVerfG	281
dd) Neue Rechtsprechung des BGH	282
c) Fazit	282

- 2. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG 283
 - a) Erhebung der Standortdaten 284
 - b) Erzeugung der Standortdaten 284
 - aa) Keine Grundrechtsrelevanz der Datenerzeugung 285
 - bb) Grundrechtsrelevanz der Datenerzeugung 285
 - (1) Datenerzeugung als Maßnahmekern 286
 - (2) Datenerzeugung als Maßnahmenunterstützung 287
 - cc) Rechtsprechung des BGH 287
 - dd) Würdigung 288
 - c) Fazit 291
- IV. Analyse der Verfassungsmäßigkeit 291
 - 1. § 100a StPO 292
 - a) Datenerzeugung als Überwachung der Telekommunikation 292
 - b) Datenerhebung als Überwachung der Telekommunikation 293
 - c) Fazit 295
 - 2. § 100g StPO 296
 - a) Rechtslage vor der TKÜ-Novelle 2008 296
 - b) Rechtslage nach der TKÜ-Novelle 2008 296
 - aa) Bedarf für die Maßnahme der stillen SMS? 297
 - bb) Rechtsgrundlage für die Maßnahme der stillen SMS? 298
 - cc) Fazit 299
 - 3. §§ 163 Abs. 1, 161 Abs. 1 StPO i. V. m. § 100a bzw. § 100g StPO 299
 - a) Grundrechtsintensität des Versandes der stillen SMS 300
 - b) Kombination verschiedener Rechtsgrundlagen 301
 - aa) Untersuchungsgegenstand „Stille SMS“ 302
 - bb) Unzulässigkeit einer Kombination 303
 - c) Fazit 304
 - 4. § 100h StPO 304
 - a) Tatbestand des § 100h Abs. 1 S. 1 Nr. 2 StPO 304
 - aa) „Sonstiges besonderes für Observationszwecke bestimmtes technisches Mittel“ 304
 - bb) „Außerhalb von Wohnungen“ 306
 - b) § 100h Abs. 1 S. 1 Nr. 2 StPO als Rechtsgrundlage für die stille SMS 307
 - c) Fazit 308
 - 5. § 100i StPO 308
 - a) Auslegung von § 100i Abs. 1 Nr. 2 StPO 309
 - aa) Wortlaut 309
 - bb) Historie 310
 - cc) Systematik 312
 - dd) Telos 313

ee) Zwischenergebnis	313
b) § 100i Abs. 1 Nr. 2 StPO als Rechtsgrundlage für die stille SMS	314
aa) Retrograde Abfrage von erzeugten Daten	314
bb) Kombination von Rechtsgrundlagen	315
c) Fazit	315
6. Zusammenfassung	316
V. Gesamtergebnis	316
E. Der virtuelle verdeckte Ermittler	318
I. Allgemeine Grundlagen	318
1. Begriff und Inhalt	318
2. Abgrenzung	318
a) Unterscheidung der Ermittler	319
aa) Analoger verdeckter Ermittler	319
bb) Virtueller noeP	320
(1) Differenzierung von verdecktem Ermittler und noeP	320
(2) Übertragbarkeit auf soziale Netzwerke	322
b) Unterscheidung der Ermittlungsmaßnahmen	323
aa) Abrufen öffentlich zugänglicher Daten	323
bb) Zugriff auf Zugangsgeschützte Informationen	324
cc) Onlinefahndung	325
c) Zwischenergebnis	325
3. Praktische Notwendigkeit	325
II. Technische Grundlagen	326
1. Eigenart und Bedeutung sozialer Netzwerke	326
2. Funktionsweise sozialer Netzwerke	327
III. Verfassungsrechtliche Grundlagen	329
1. „Ob“ der Grundrechtsrelevanz	329
2. „Wie“ der Grundrechtsrelevanz	332
a) Art. 10 GG	332
b) Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG	333
aa) Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme	333
bb) Recht auf informationelle Selbstbestimmung	334
(1) Vorgaben des BVerfG	334
(2) Übertragung auf soziale Netzwerke	335
(a) Anwendung der BVerfG-Vorgaben	335
(b) Inhalt der BVerfG-Vorgaben	336
(c) Schutzwürdiges Vertrauen in sozialen Netzwerken	338
(d) Zwischenergebnis	341
3. Fazit	341

IV. Analyse der Verfassungsmäßigkeit	341
1. §§ 161, 163 StPO	342
a) Eingriffsstärke des virtuellen verdeckten Ermittlers	342
b) Abgrenzung zum virtuellen noeP	344
c) Zwischenergebnis	347
2. § 110a StPO	347
3. § 110a StPO analog	350
a) Zulässigkeit einer Analogie	350
b) Vorliegen der Voraussetzungen einer Analogie	351
aa) Planwidrige Regelungslücke	351
bb) Vergleichbare Interessenlage	352
c) Zwischenergebnis	353
4. Fazit	353
V. Zusammenfassung und dogmatischer Ausblick	353
§ 3 Schluss	355
Literaturverzeichnis	358
Stichwortverzeichnis	379

Einleitung

Die Funktion des Rechts lässt sich knapp damit umschreiben, dass es ein Instrument sozialer Steuerung darstellt. Ausschlaggebend für die Gestaltung des Rechts als Steuerungsinstrument muss demnach auch das Objekt der Steuerung sein. Bei Änderung der tatsächlichen, etwa gesellschaftlichen oder technischen, Verhältnisse kann das Gesetz auf drei unterschiedliche Arten reagieren: durch die Anwendung bestehender Normen auf die neuen Gegebenheiten, Gesetzesänderungen oder Untätigkeit. Diese verschiedenen Reaktionsmöglichkeiten bergen dabei jeweils unterschiedliche Gefahren: Die erste Alternative einen Konflikt mit dem Bestimmtheitsgrundsatz, die zweite eine Hypertrophie der Rechtsordnung und die dritte das Entstehen von Regelungslücken.¹

Eine fundamentale Änderung der Lebensumstände erfolgte durch die zunehmende Verbreitung elektronischer Datenverarbeitung und die damit einhergehende, wachsende Abhängigkeit von Informationen und Informationsverarbeitungssystemen. Die Entwicklung einer Informationsgesellschaft hat zu einer zunehmenden Vernetzung von Informationssystemen und der fortschreitenden Konvergenz von klassischen Medien und Kommunikationsformen geführt. Die Ausbreitung des Internets und die schnelle Entwicklung der dazugehörigen Technik werden als größte Veränderung in Kultur und Wirtschaft seit dem Buchdruck klassifiziert.²

Bei Wandel der technischen Möglichkeiten ist jeweils klärungsbedürftig, ob bzw. inwiefern Normen an den geänderten Regelungsgegenstand anzupassen sind oder ob durch eine sinnvolle Anwendung dieser Normen auch die neu auftretenden Sachverhalte einer angemessenen Lösung zuführbar sind. Diese Frage stellt sich insbesondere bei strafprozessualen Ermittlungsmaßnahmen wegen der scharfen Form staatlicher Eingriffstätigkeit. Das Strafverfahrensrecht liefert gesetzliche Legitimationen, die für Zwecke der Strafverfolgung Eingriffe in die (Grund-)Rechte der Bürger gestatten. Umgekehrt finden diese Eingriffsbefugnisse ihre Begrenzung in der wertsetzenden Bedeutung der Grundrechte.³ Zu prüfen ist im Falle neuer technischer Möglichkeiten, ob eine beabsichtigte Ermittlungstätigkeit auf eine bereits bestehende Befugnis gestützt werden kann oder ob der Gesetzgeber tätig werden muss, um den verfassungsgerichtlichen Maßgaben zu entsprechen.

Werden die Möglichkeiten der strafprozessualen Ermittlungstätigkeit durch die Praxis der Behörden, mit der Entwicklung der Technik einhergehend, erweitert, kann

¹ Kudlich, JuS 2001, 1165 (1165).

² Kudlich, Jura 2001, 305 (305).

³ Fischer, in: Karlsruher Kommentar StPO, Einleitung Rn. 4.

dies zeitgleich den Gesetzgeber zum Tätigwerden veranlassen. Denn dem Staat kommt von Verfassungen wegen die Aufgabe zu, eine funktionstüchtige Strafrechtspflege zu gewährleisten, da ohne eine solche der Gerechtigkeit nicht zum Durchbruch verholfen werden kann. Dazu gehört es, die Vorschriften des Strafprozessrechts „laufend auf ihre Tauglichkeit, Zeitgemäßheit und Effektivität hin zu überprüfen und das bestehende Regelungsgefüge (...) an die sich ändernden Rahmenbedingungen anzupassen“.⁴ Es scheint daraus gleichsam eine Art Automatismus der Schaffung von Rechtsgrundlagen zu entstehen, dessen Tempo im Wesentlichen von der Exekutive bestimmt wird. Aus diesem folgen immer weitergehende Möglichkeiten der Überwachung. Verstärkt wird die Entwicklung dadurch, dass der technische Fortschritt ständig neue, effektivere und einfachere Überwachungsmethoden ermöglicht. Die zunehmenden Maßnahmen erleichtern zum einen die Ermittlungstätigkeit, zum anderen gehen damit aber weitere und teilweise auch intensivere Grundrechtseingriffe einher.⁵

Bei neu geschaffenen Gesetzesgrundlagen eröffnen sich Fragen, inwieweit noch neuere Entwicklungen, die nach Gesetzeserlass entstehen, unter die Norm subsumiert werden können. Häufig wird gezielt eine weite Fassung gewählt, die gegenüber technischen Entwicklungen offen ist. So hat der Gesetzgeber seinerzeit mit den §§ 100a, 100b StPO auf neue Möglichkeiten der Kommunikation reagiert, um dem verfassungsrechtlichen Fernmeldegeheimnis ausreichend Schutz zu gewährleisten. Gegenstand war bei Erlass der Norm im Jahr 1968 die Sprachtelefonie.⁶ Im Jahr 1997 wurde mit der neuen Wendung der „Überwachung und Aufzeichnung der Telekommunikation“ anstelle des Begriffs des Fernmeldeverkehrs⁷ eine technisch offene Formulierung gewählt. Mit weiterer technischer Entwicklung, wie beispielsweise der verschlüsselten Kommunikation oder auch noch nicht bekannter Techniken der Nachrichtenübertragung, wird der Gesetzesanwender wiederum erneut vor die Frage gestellt, ob diese unter den weiten Begriff der Telekommunikation subsumierbar sind. Denn trotz der weit gewählten Fassung ist es im Einzelfall schwierig zu beantworten, ob bestimmte Informationen noch unter „Telekommunikation“ zu fassen sind bzw. sich bestimmte technische Kontrollmöglichkeiten als Überwachung der Telekommunikation darstellen.⁸

Ziel der Bearbeitung ist es, neue technische Möglichkeiten für die Ermittlungstätigkeit der Strafverfolgungsbehörden an den aus dem Verfassungsrecht folgenden Vorgaben zu messen. Die Arbeit wurde dazu in zwei große Blöcke aufgeteilt. In einem *Allgemeinen Teil* werden zunächst verfassungsrechtliche Determinanten

⁴ Bundesregierung, Entwurf eines Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens, BT-Drs. 18/11277, S. 1.

⁵ Kritisch dazu *Eisenberg/Singelstein*, NSTZ 2005, 62 (67).

⁶ § 100a und § 100b StPO wurden mit dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses BGBl. 1986 I, S. 949 (951 f.) eingeführt.

⁷ BegleitG zum TelekommunikationsG, BGBl. 1997 I, S. 3108 (3113).

⁸ Siehe dazu auch *Bär*, TK-Überwachung, § 100a StPO Rn. 9; *Kudlich*, JuS 2001, 1165 (1166).

aufgestellt, die innerhalb des Strafprozessrechts zu berücksichtigen sind. Eine wesentliche Rolle kommt dabei zum einen den Grundrechten zu (A.). Zum anderen können aus der Verfassung weitere Sätze hergeleitet werden, die technikoffenen Ermittlungsbefugnissen Grenzen setzen (B.). Die „Technikoffenheit“ ist in der Straf- bzw. Strafprozessrechtswissenschaft bisher kein feststehender, allgemein anerkannter Topos.⁹ Gemeint sind mit technik- bzw. entwicklungs-offenen Ermächtigungsgrundlagen Befugnisse, wie das angeführte Beispiel des § 100a StPO, die für technische Entwicklungen „offen“ gehalten werden.

In einem *Besonderen Teil* werden sodann drei strafprozessuale Ermittlungsmaßnahmen im Konkreten an den im Allgemeinen Teil abstrakt gewonnenen Determinanten gemessen: Die Quellen-Telekommunikationsüberwachung (Quellen-TKÜ), die stille SMS und der virtuelle verdeckte Ermittler (C.–E.). Die Maßnahmen verbindet, dass mit ihnen jeweils auf Veränderungen innerhalb der Kommunikationstechnologie reagiert wurde. Die *Quellen-TKÜ* trägt dem Umstand Rechnung, dass die klassische Telekommunikation überwiegend durch verschlüsselte Kommunikationsmöglichkeiten ersetzt wird. Die *stille SMS* übermittelt – trotz ihrer Bezeichnung – keine Kurzmitteilung, sondern dient der Ortung von Zielpersonen. Dabei nutzt sie zum einen die Gegebenheit, dass in Zeiten moderner Kommunikation nahezu jeder ein Mobiltelefon mit sich führt. Zum anderen greift die stille SMS im Gegensatz zu vergleichbaren Ermittlungsmaßnahmen auch dann, wenn das Handy nicht über den klassischen Kommunikationsweg genutzt wird. Zuletzt findet mit dem Instrument des *virtuellen verdeckten Ermittlers* die zunehmend über soziale Netzwerke erfolgende Kommunikation Berücksichtigung.

⁹ So auch Roggan, NJW 2015, 1995 (1995).