

Soziale Netzwerke und strafprozessuale Ermittlungen

Von

Sebastian Bauer



Duncker & Humblot · Berlin

Inhaltsverzeichnis

Einleitung	21
Ziel und Gang der Untersuchung	22
A. Grundlagen zu Ermittlungen in sozialen Netzwerken	26
I. Soziale Netzwerke – Begriffsklärung und Grundfunktionen	26
1. Begriffsklärung: Web 2.0, soziale Medien und soziale Netzwerke ..	26
a) Web 2.0 und soziale Medien	26
b) Soziale Netzwerke	28
2. Grundfunktionen	31
a) Profilerstellung	31
b) Kommunikationsfunktionen	32
c) Veranstaltungsmanagement	34
d) Suchfunktionen	34
e) Konsequenzen der Grundfunktionen für den Untersuchungsge- genstand	35
3. Entwicklung sozialer Netzwerke	36
4. Zahlen und Fakten zur Nutzung sozialer Netzwerke	37
5. Zwischenergebnis	39
II. Technische Grundlagen zu sozialen Netzwerken	39
1. Akteure	40
2. Datenübertragung im Internet	41
3. Adressierung im Internet	42
4. Soziale Netzwerke	43
a) Architektur	43
b) Datenübertragung	44
c) Verschlüsselung	46
III. Soziale Netzwerke als Informationsquellen für die Strafverfolgungsbe- hörden	47
1. Ermittlungsauftrag	47
2. Nutzung sozialer Netzwerke zu Ermittlungen und aktuelle For- schungsprojekte	47
a) Kleine Anfrage an den Bundestag zur Nutzung sozialer Netzwer- ke zu Fahndungszwecken	49
b) Kleine Anfrage an den Hamburger Senat zur Nutzung sozialer Netzwerke zu Fahndungszwecken	49
c) Erkenntnisse aus der NSA-Affäre für Ermittlungen in sozialen Netzwerken	50

d) Aktuelle Forschungsprojekte	52
3. Besonderheiten bei Ermittlungen in sozialen Netzwerken	54
a) Daten mit Wissen des Nutzers	54
b) Daten ohne Wissen des Nutzers	55
aa) Daten aus netzwerkinternem Verhalten	55
bb) Daten aus netzwerkexternem Verhalten	57
c) Zwischenergebnis	58
4. Beweiseinführung und Beweiswert	58
5. Internationale Durchsetzung	61
6. Zwischenergebnis	64
IV. Folgerungen für den Umfang der Untersuchung	64
B. Verfassungsrechtliche Anforderungen an strafprozessuale Ermächti-	
gungsgrundlagen	65
I. Vorbehalt des Gesetzes und grundrechtliche Gesetzesvorbehalte	66
1. Grundrechtliche Gesetzesvorbehalte	66
2. Allgemeiner Vorbehalt des Gesetzes	67
II. Gebot der Normenklarheit und -bestimmtheit	69
1. Herleitung und Funktionen	70
2. Bestimmtheitsanforderungen	72
a) Heimliche Ermittlungsmaßnahmen	73
b) Einsatz technischer Mittel	75
c) Generalklauseln	77
III. Analogieverbot für strafprozessuale Ermittlungsmaßnahmen	78
1. Rechtsprechung und Literatur	79
2. Ableitung eines Analogieverbotes aus dem Vorbehalt des Gesetzes bzw. den grundrechtlichen Gesetzesvorbehalten	81
3. Folgerungen für ein Analogieverbot im Strafprozessrecht	84
4. Abgrenzung von Auslegung und Analogie	85
IV. Verhältnismäßigkeitsgrundsatz	87
1. Verhältnismäßigkeitsgrundsatz und Gesetzgebung	87
a) Legitimes Ziel und Geeignetheit	89
b) Erforderlichkeit	90
c) Angemessenheit	91
2. Verhältnismäßigkeit der Einzelfallmaßnahme	94
C. Zugriff auf öffentlich zugängliche Daten	98
I. Grundrechtlicher Schutz	99
1. Fernmeldegeheimnis	99
a) Abgrenzung von Massen- und Individualkommunikation	101
aa) Zugangssicherungen	101
bb) Autorisierung	102
b) Schutz der Netzwerköffentlichkeit in sozialen Netzwerken	104
2. Recht auf informationelle Selbstbestimmung	105

3. Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	108
II. Eingriff	109
1. Öffentlichkeitsbezug als Eingriffsausschluss	110
2. Bagatellvorbehalt	113
3. Grundrechtsverzicht	114
a) Verzichtserklärung	115
b) Freiwilligkeit	117
c) Reichweite	119
4. Zwischenergebnis	121
III. Ermächtigungsgrundlage	121
1. Anwendungsbereich der Generalermittlungsklausel	121
2. Eingriffsintensität der Online-Streife	124
a) Persönlichkeitsrelevanz der betroffenen Daten	124
aa) Abgrenzung zwischen öffentlichen und privaten Bereichen	125
(1) Inhaltliche Bestimmung der allgemeinen Zugänglichkeit	126
(2) Übertragung auf soziale Netzwerke	129
(3) Zwischenergebnis	131
bb) Schutz der Privatheit in der Netzwerköffentlichkeit	131
(1) Ausforschungspotential	133
(2) Berechtigte Privatheitserwartung	134
(3) Zwischenergebnis	139
b) Heimlichkeit	140
c) Einsatz technischer Mittel	144
IV. Zwischenergebnis	146
D. Verdeckte Ermittlungen	147
I. Grundrechtlicher Schutz	148
1. Fernmeldegeheimnis	148
2. Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	154
3. Recht auf informationelle Selbstbestimmung	155
a) Restriktives Schutzbereichsverständnis	155
aa) Verdeckte Identitätsübernahme	157
bb) Nutzung fiktiver Identitäten	159
(1) Identitätskontrolle durch den Betreiber	160
(2) Identitätskontrolle durch den Nutzer	161
(a) Äußere Umstände	162
(b) Innere Umstände	163
b) Weites Schutzbereichsverständnis	164
c) Zwischenergebnis	167
II. Ermächtigungsgrundlagen	167
1. Verdeckte Ermittlungen und Selbstbelastungsfreiheit	168

a)	Anknüpfungspunkt Selbstbelastungsfreiheit bzw. Recht auf ein faïres Verfahren	169
aa)	Rechtsprechung des EGMR	169
bb)	Rechtsprechung des BGH	171
b)	Direkte bzw. entsprechende Anwendung des § 136 I 2 StPO bzw. des § 136a I StPO	173
aa)	Täuschung als Umgehung des Schweigerechts	174
bb)	Täuschung als verbotene Vernehmungsmethode	176
c)	Der gebotene Täuschungsschutz der Selbstbelastungsfreiheit	178
aa)	„Zwangsgleichheit“ von Täuschungen	179
bb)	Täuschungen als Zurechnungsproblem	182
d)	Folgen für verdeckte Ermittlungen in sozialen Netzwerken	186
2.	§§ 110a ff. StPO	188
a)	Abgrenzung zum NoeP	188
b)	Virtueller verdeckter Ermittler in sozialen Netzwerken	190
aa)	Legende	192
(1)	Aufbau einer fiktiven virtuellen Identität	192
(2)	Verdeckte Identitätsübernahme	195
bb)	Befugnisse	196
c)	Zwischenergebnis	198
3.	§§ 161 I 1, 163 I 2 StPO	198
a)	Vernehmungähnliche Befragungen	199
b)	Verdeckte Kommunikation	200
c)	Verdeckte Freundschaftsanfrage	204
aa)	Eingriffsintensität	204
bb)	Strafbarkeit nach § 202a StGB	205
d)	Verdeckte Identitätsübernahme	208
III.	Zwischenergebnis	209
IV.	Gesetzgebungsvorschlag	209
1.	Maßstäbe	209
2.	Gesetzentwurf	212
E.	Zugriff auf nichtöffentlich zugängliche Daten	214
I.	Inhaltsdaten	215
1.	E-Mail	218
a)	Grundrechtlicher Schutz	219
aa)	Fernmeldegeheimnis	220
(1)	Online-Entwurfsphase	222
(2)	Endspeicherung beim Provider	224
(3)	Zwischenergebnis	228
bb)	Grundrecht auf Gewährleistung der Vertraulichkeit und Inte- grität informationstechnischer Systeme	228
cc)	Konkurrenzen	232

b) Ermächtigungsgrundlagen	235
aa) Rechtsprechung	235
bb) Schrifttum	238
2. Soziale Netzwerke	239
a) Grundrechtlicher Schutz	239
aa) Fernmeldegeheimnis	239
(1) Nachrichten und Chatinhalte	239
(2) Weitere Kommunikationsinhalte	241
(a) Massen- oder Individualkommunikation?	241
(b) Fehlender Kommunikationsvorgang?	243
(3) Zwischenergebnis	244
bb) Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	245
b) Ermächtigungsgrundlagen	246
aa) §§ 94 ff. StPO	246
(1) Anwendungsbereich	246
(a) Gegenstand	246
(aa) Wortlaut	247
(bb) Historie	247
(cc) Systematik	248
(dd) Telos	250
(ee) Zwischenergebnis	251
(b) Sicherstellung	251
(aa) Unkörperliche Sicherstellung und körperliches Gegenstandsverständnis	251
(bb) Unkörperliche Sicherstellung und unkörperliches Gegenstandsverständnis	253
(c) Zwischenergebnis	256
(2) Ermächtigungsgrundlage für Eingriffe in das Fernmeldegeheimnis	256
(a) Eingriffsintensität	256
(aa) Offenheit der Maßnahme	256
(bb) Einmaliger und punktueller Zugriff	258
(cc) Selbstschutzmöglichkeiten	259
(dd) Zwischenergebnis	261
(b) Normenklarheit und -bestimmtheit	261
(aa) Anlass und Zweck	261
(bb) Umfang und Grenzen	264
(c) Verhältnismäßigkeit	267
(aa) Eingriffsschwellen	268
(bb) Verfahrensregeln	270
(3) Zwischenergebnis	273
bb) §§ 99 ff. StPO	274

(1) Direkte Anwendung	274
(2) Analoge Anwendung	277
(3) Zwischenergebnis	281
cc) §§ 100a ff. StPO	281
(1) Anwendungsbereich	281
(a) Telekommunikation	281
(aa) Technisch-dynamisches Begriffsverständnis... ..	282
(bb) Kenntnisaufnahme-Theorie	284
(cc) Entwicklungsoffener Telekommunikationsbe- griff	285
(b) Überwachung und Aufzeichnung	286
(c) Soziale Netzwerke als Anordnungsgegner i. S. d. § 100a III StPO	288
(d) Soziale Netzwerke als Adressat des § 100b III 1 StPO	289
(aa) Soziale Netzwerke als Telekommunikations- dienst i. S. d. § 100b III 1 StPO	289
(bb) Anwendbares Datenschutzrecht bei sozialen Netzwerken	292
(e) Überwachung mit eigenen Mitteln der Strafverfol- gungsbehörden	295
(f) Zwischenergebnis	296
(2) Ermächtigungsgrundlage für Eingriffe in das Fernmelde- geheimnis	297
(a) Anordnungsvoraussetzungen	298
(b) Grenzen	299
(c) Verfahrenssicherungen	301
(d) Kernbereichsschutz	303
(3) Ermächtigungsgrundlage für Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	307
(a) Anlasstaten	308
(aa) Heimlicher Zugriff mit Infiltration	308
(bb) Heimlicher Zugriff ohne Infiltration	311
(b) Verfahrenssicherungen	313
(c) Kernbereichsschutz	314
(4) Zwischenergebnis	316
(5) Gesetzgebungsvorschlag	316
(a) Maßstäbe	317
(b) Gesetzentwurf	321
dd) § 110 III StPO	325
(1) Accounts sozialer Netzwerke als Speichermedien i. S. d. § 110 III StPO	327

(2) Gefahr des Beweismittelverlustes	331
(3) Offenheit der Maßnahme	332
(4) Zwischenergebnis	334
3. Zwischenergebnis zum Zugriff auf Inhaltsdaten	334
II. Bestandsdaten	335
1. Zugriff auf Bestandsdaten	336
a) § 100j StPO	337
b) §§ 161 I 1, 163 I 2 StPO	338
c) §§ 94 ff. StPO	342
2. Gesetzgebungsvorschlag	342
a) Maßstäbe	343
b) Gesetzentwurf	343
III. Verkehrsdaten	344
1. § 100g StPO	345
2. §§ 100a ff. StPO	349
3. Zwischenergebnis	349
IV. Nutzungsdaten	349
1. Grundrechtlicher Schutz	352
a) Fernmeldegeheimnis	352
b) Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	355
2. Ermächtigungsgrundlagen	357
a) §§ 161 I 1, 163 I 2 StPO	358
b) §§ 94 ff. StPO	360
c) § 100g StPO und § 100j StPO	361
d) §§ 100a ff. StPO	362
3. Gesetzgebungsvorschlag	365
a) Maßstäbe	366
b) Gesetzentwurf	369
F. Gesamtergebnis und Schlussbemerkung	371
I. Gesamtergebnis	372
II. Schlussbemerkung	375
Literaturverzeichnis	377
Internet-Adressen	403
Stichwortverzeichnis	404