

Strafrechtliche Abhandlungen

Neue Folge · Band 281

**Soziale Netzwerke und strafprozessuale
Ermittlungen**

Von

Sebastian Bauer



Duncker & Humblot · Berlin

SEBASTIAN BAUER

Soziale Netzwerke und strafprozessuale Ermittlungen

Strafrechtliche Abhandlungen · Neue Folge

Begründet von Dr. Eberhard Schmidhäuser (†)
em. ord. Prof. der Rechte an der Universität Hamburg

Herausgegeben von

Dr. Dres. h. c. Friedrich-Christian Schroeder
em. ord. Prof. der Rechte an der Universität Regensburg

und

Dr. Andreas Hoyer
ord. Prof. der Rechte an der Universität Kiel

in Zusammenarbeit mit den Strafrechtslehrern der deutschen Universitäten

Band 281

Soziale Netzwerke und strafprozessuale Ermittlungen

Von

Sebastian Bauer



Duncker & Humblot · Berlin

Zur Aufnahme in die Reihe empfohlen von
Professor Dr. Karsten Gaede, Hamburg

Die Bucerius Law School – Hochschule für Rechtswissenschaft Hamburg
hat diese Arbeit im Jahre 2016 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
© 2018 Duncker & Humblot GmbH, Berlin
Satz: L101 Mediengestaltung, Fürstenwalde
Druck: buchbücher.de gmbh, Birkach
Printed in Germany

ISSN 0720-7271
ISBN 978-3-428-15235-3 (Print)
ISBN 978-3-428-55235-1 (E-Book)
ISBN 978-3-428-85235-2 (Print & E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ☺

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

Meinen Eltern

Vorwort

Die vorliegende Arbeit wurde von der Bucerius Law School im Mai 2016 als Dissertation angenommen. Literatur und Rechtsprechung sind auf dem Stand von April 2016. Die mündliche Prüfung fand am 25. Januar 2017 statt.

Mein größter Dank gilt meinem verehrten Doktorvater Prof. Dr. Karsten Gaede für seine hervorragende Betreuung, wertvollen Anregungen und sein mir stets entgegengebrachtes Vertrauen in das Gelingen dieser Promotionsarbeit. Sowohl seine engagierte Begleitung dieses Vorhabens als auch die sehr zügige Begutachtung haben diese Abhandlung bestmöglich gefördert.

Herrn Prof. Dr. Paul Krell danke ich für die zügige Erstellung des Zweitgutachtens.

Für das Korrekturlesen der gesamten Arbeit danke ich herzlich Thomas Huber, Robin Kottenhoff und Maximilian Schröder.

Herzlicher Dank gebührt schließlich meinen Eltern und meinem Bruder, die mich während meiner Promotion unermüdlich begleitet und unterstützt haben.

Berlin, im Juni 2017

Sebastian Bauer

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 fares 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) | Vernehmungsfähnliche 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 Integrität 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) Kenntnisnahme-Theorie | 284 |
| (cc) Entwicklungsoffener Telekommunikationsbegriff | 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 Telekommunikationsdienst i. S. d. § 100b III 1 StPO | 289 |
| (bb) Anwendbares Datenschutzrecht bei sozialen Netzwerken | 292 |
| (e) Überwachung mit eigenen Mitteln der Strafverfolgungsbehörden | 295 |
| (f) Zwischenergebnis | 296 |
| (2) Ermächtigungsgrundlage für Eingriffe in das Fernmeldegeheimnis | 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 |

Abkürzungsverzeichnis

| | |
|---------|-----------------------------------------------------------------------------------------------------------------------------|
| a. A. | anderer Ansicht |
| Abs. | Absatz |
| aF | alte Fassung |
| AfP | Zeitschrift für Medien- und Kommunikationsrecht |
| AG | Amtsgericht |
| AGB | Allgemeine Geschäftsbedingungen |
| AK | Alternativkommentar |
| Anm. | Anmerkung |
| AöR | Archiv des öffentlichen Rechts |
| Art. | Artikel |
| Aufl. | Auflage |
| Az. | Aktenzeichen |
| BayObLG | Bayerisches oberstes Landesgericht |
| BayPAG | Polizeiaufgabengesetz Bayern |
| BB | Betriebs-Berater |
| Bd. | Band |
| BDSG | Bundesdatenschutzgesetz |
| BeckOK | Beck'scher Online-Kommentar |
| Beschl. | Beschluss |
| BGB | Bürgerliches Gesetzbuch |
| BGBI. | Bundesgesetzblatt |
| BGH | Bundesgerichtshof |
| BGHSt | Entscheidungen des Bundesgerichtshofs in Strafsachen |
| BKAG | Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten |
| BNDG | Gesetz über den Bundesnachrichtendienst |
| BR-Drs. | Drucksache des Bundesrats |
| BT-Drs. | Drucksache des Bundestags |
| BtMG | Gesetz über den Verkehr mit Betäubungsmitteln |
| BVerfG | Bundesverfassungsgericht |
| BVerfGE | Entscheidungen des Bundesverfassungsgerichts |

| | |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| BVerfSchG | Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz |
| BVerwG | Bundesverwaltungsgericht |
| BVerwGE | Entscheidungen des Bundesverwaltungsgerichts |
| bzw. | beziehungsweise |
| CCC | Convention on Cybercrime |
| CR | Computer und Recht |
| c't | c't Magazin für Computertechnik |
| ders. | derselbe |
| d. h. | das heißt |
| dies. | dieselbe |
| diff. | differenzierend |
| DJT | Deutscher Juristentag |
| DÖV | Die Öffentliche Verwaltung |
| DRiZ | Deutsche Richterzeitung |
| DuD | Datenschutz und Datensicherheit |
| DVBl | Deutsches Verwaltungsblatt |
| ebd. | ebenda |
| EDV | Elektronische Datenverarbeitung |
| EGMR | Europäische Gerichtshof für Menschenrechte |
| Einl. | Einleitung |
| EL | Ergänzungslieferung |
| EMRK | Europäische Menschenrechtskonvention |
| et al. | et alii/aliae |
| etc. | et cetera |
| eucrim | eucrim – The European Criminal Law Associations' Forum |
| EuGH | Europäischer Gerichtshof |
| EuGRZ | Europäische Grundrechte-Zeitschrift |
| f./ff. | folgende |
| Fn. | Fußnote |
| FS | Festschrift |
| GA | Goltdammer's Archiv für Strafrecht |
| GedS | Gedächtnisschrift |
| gem. | gemäß |
| GG | Grundgesetz |
| ggf. | gegebenenfalls |
| ghM | ganz herrschende Meinung |

| | |
|-----------------------|--------------------------------------------------------------------------|
| GmbH | Gesellschaft mit beschränkter Haftung |
| GRUR | Gewerblicher Rechtsschutz und Urheberrecht |
| HFR | Humboldt Forum Recht |
| HK | Heidelberger Kommentar |
| HRRS | Onlinezeitschrift für Höchststrichterliche Rechtsprechung zum Strafrecht |
| Hrsg. | Herausgeber |
| Hs. | Halbsatz |
| i. E. | im Ergebnis |
| i. R. d. | im Rahmen des/der |
| i. R. v. | im Rahmen von |
| i. S. d. | im Sinne des/der |
| i. V. m. | in Verbindung mit |
| JA | Juristische Arbeitsblätter |
| JR | Juristische Rundschau |
| jurisPK-Internetrecht | Juris PraxisKommentar Internetrecht |
| JuS | Juristische Schulung |
| JZ | Juristen Zeitung |
| K&R | Kommunikation & Recht |
| KG | Kammergericht |
| KK | Karlsruher Kommentar |
| KMR | Kleinknecht Müller Reitberger |
| LG | Landgericht |
| lit. | litera |
| LR | Löwe-Rosenberg |
| LVwG SH | Allgemeines Verwaltungsgesetz für das Land Schleswig-Holstein |
| m. | mit |
| MADG | Gesetz über den militärischen Abschirmdienst |
| MK | Münchener Kommentar |
| MMR | MultiMedia und Recht |
| m. w. N. | mit weiteren Nachweisen |
| NJOZ | Neue Juristische Online-Zeitschrift |
| NJW | Neue Juristische Wochenschrift |
| NJW-RR | Neue Juristische Wochenschrift – Rechtsprechungsreport |
| Nr. | Nummer |
| NSA | National Security Agency |
| NStZ | Neue Zeitschrift für Strafrecht |

| | |
|------------|-------------------------------------------------------------------------------------------------------------------|
| NStZ-RR | Neue Zeitschrift für Strafrecht – Rechtsprechungsreport |
| NVwZ | Neue Zeitschrift für Verwaltungsrecht |
| NZA | Neue Zeitschrift für Arbeitsrecht |
| OLG | Oberlandesgericht |
| PNAS | Proceedings of the National Academy of Sciences |
| POG RhLPfl | Polizei- und Ordnungsbehördengesetz Rheinland-Pfalz |
| RDV | Recht der Datenverarbeitung |
| Rn. | Randnummer |
| RW | Zeitschrift für rechtswissenschaftliche Forschung |
| S. | Seite |
| Sch/Sch | Schönke/Schröder |
| SK | Systematischer Kommentar |
| SMS | Short Message Service |
| sog. | sogenannt/e |
| SSW | Satzger Schluckebier Widmaier |
| st. Rspr. | ständige Rechtsprechung |
| StGB | Strafgesetzbuch |
| StPO | Strafprozessordnung |
| StraFo | Strafverteidiger Forum |
| StV | Strafverteidiger |
| TDDSG | Teledienstdatenschutzgesetz |
| TKG | Telekommunikationsgesetz |
| TKÜV | Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation |
| TMG | Telemediengesetz |
| UrhG | Urhebergesetz |
| Urt. | Urteil |
| UWG | Gesetz gegen unlauteren Wettbewerb |
| v. | vom |
| VG | Verwaltungsgericht |
| VGH | Verwaltungsgerichtshof |
| vgl. | vergleiche |
| Vol. | Volume |
| vs. | versus |
| VSG NRW | Gesetz über den Verfassungsschutz in Nordrhein-Westfalen |
| VuR | Verbraucher und Recht |

| | |
|---------|---------------------------------------------------------------------|
| VVDStRL | Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer |
| Wistra | Zeitschrift für Wirtschafts- und Steuerstrafrecht |
| z. B. | zum Beispiel |
| ZD | Zeitschrift für Datenschutz |
| ZIS | Zeitschrift für Internationale Strafrechtsdogmatik |
| ZRP | Zeitschrift für Rechtspolitik |
| ZStW | Zeitschrift für die gesamte Strafrechtswissenschaft |

Einleitung

„So the question isn't what do we want to know about people, it's what do people want to tell about themselves. Right?“¹ – diese Interviewaussage des Facebook-Gründers Mark Zuckerberg ist symptomatisch für die zunehmende Bereitschaft zur Preisgabe und Veröffentlichung persönlicher Daten in den Kommunikationsdiensten des Internets, allen voran den Angeboten des Web 2.0. Zu diesen zählen auch soziale Netzwerke², die als onlinebasierte Kommunikationsform längst fester Bestandteil unseres Alltags sind und neben E-Mails und Internet-Telefonie zu den meistgenutzten Kommunikationsanwendungen zählen.³ Soziale Netzwerke bieten ihren Nutzern eine Plattform für onlinebasiertes Identitäts- und Beziehungsmanagement.⁴ Nach der Errichtung eines persönlichen Profils können sich die Nutzer im Netzwerk selbst darstellen, Beziehungen zu anderen Menschen pflegen oder aufbauen sowie sich zu ihren Interessen und Hobbies informieren. Soziale Netzwerke sind aufgrund ihrer Popularität und hoher Nutzerzahlen aber auch in den Fokus der Strafverfolgungsbehörden gerückt. Einerseits liegt dies an den riesigen Mengen an persönlichen Daten, die Nutzer in sozialen Netzwerken auf ihren Profilen preisgeben oder vom Betreiber des sozialen Netzwerks ohne deren Wissen erzeugt werden. Für Ermittlungsbehörden sind sie Informationsquel-

¹ Frei übersetzt: Die Frage lautet nicht „Was wollen wir über die Leute wissen“, sie lautet „Was wollen die Leute über sich erzählen“, oder?, abrufbar unter: <https://techcrunch.com/2011/11/07/zuckerberg-talks-to-charlie-rose-about-war-ipos-and-googles-little-version-of-facebook/>.

² Teils wird auch von Online-Network-Diensten (OND), Online Social Networks (OSN) oder Social Network Sites (SNS) gesprochen, vgl. *Henrichs/Wilhelm* Kriminalistik 2010, 30 ff.; vgl. *Ebersbach/Glaser/Heigl*, Social Web, S. 96; siehe auch *Bieber et al.*, in: Bieber et al. (Hrsg.), Soziale Netzwerke in der digitalen Welt, S. 12. Diese Begriffe sind insoweit genauer, da sie den Online-Bezug widerspiegeln und eine klare Abgrenzung zu „sozialen Netzwerken“ in der Soziologie, der Betriebswirtschaft oder der Systemtheorie gewährleisten. Im allgemeinen Sprachgebrauch hat sich aber der Begriff „soziale Netzwerke“ für online-basierte soziale Netzwerke durchgesetzt. Terminologisch wie hier bzw. nicht erörternd *Singelstein*, NStZ 2012, 593, 599 f.; *Kudlich*, StV 2012, 560, 566; *Rosengarten/Römer*, NJW 2012, 1764 ff.; *Schulz/Hoffmann*, DuD 2012, 7 ff.; BeckOK StPO/*Graf*, § 100a, Rn. 32c ff.; *Meyer-Göbner/Schmitt*, § 100a, Rn. 7.

³ Vgl. BT-Drs. 16/11920, S. 1, die erwähnte Bedeutung von Instant Messaging wie Windows Live Messenger ist stark zurückgegangen, da solche Kommunikationsanwendungen heute integriert von sozialen Netzwerken angeboten werden.

⁴ BT-Drs. 16/11570, S. 420.

len bei der Aufklärung von Straftaten; für Kriminelle sind sie Informationsquellen beim Ausspähen potentieller Opfer. Andererseits können soziale Netzwerke aber auch – vergleichbar mit der E-Mail-Kommunikation – zur Verständigung zwischen Straftätern genutzt werden oder als Mittel zur Begehung von Straftaten wie Betrug, Beleidigung oder Volksverhetzung.⁵

Ziel und Gang der Untersuchung

Angesichts dieser Bestandsaufnahme macht es sich diese Arbeit zur Aufgabe, die Zulässigkeit der Strafverfolgung in sozialen Netzwerken herauszuarbeiten.⁶ Trotz der enormen Relevanz dieses noch relativ jungen Ermittlungsumfelds in der Praxis sind die dazu erfolgten Abhandlungen vielmals beschränkt auf einzelne Ermittlungsmaßnahmen oder liefern mit Gesamtüberblicken eine oftmals zu holzschnittartige Gleichsetzung von sozialen Netzwerken und anderen Kommunikationsdiensten des Internets. Die Komplexität des Themas ergibt sich nicht zuletzt daraus, dass Ermittlungen in sozialen Netzwerken sowohl Strafprozessrecht als auch IT-Recht und öffentliches Recht betreffen.

Ziel dieser Abhandlung ist es, die spezifischen Herausforderungen bei Ermittlungen in sozialen Netzwerken im Unterschied zu den mittlerweile klassischen Ermittlungen in den Kommunikationsdiensten des Internet herauszuarbeiten. Ein Hauptaugenmerk liegt auf den relevanten Grundrechten bei Ermittlungen in sozialen Netzwerken. Hierzu zählen das Allgemeine Persönlichkeitsrecht (APR), insbesondere in seinen Ausprägungen des Rechts auf informationelle Selbstbestimmung und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht)⁷, sowie das Fernmeldegeheimnis⁸. Die erheblichen Abgren-

⁵ Im Zuge steigender Flüchtlingszahlen ist ein bedauerlicher „Trend“ zu rassistischen und menschenverachtenden öffentlichen Äußerungen auf Facebook zu verzeichnen, <http://www.welt.de/politik/deutschland/article144566722/7500-Euro-Strafe-gegen-Facebook-Hetze-gegen-Auslaender.html>.

⁶ Die Fahndung über soziale Netzwerke, bei der über offizielle Seiten der Polizei in sozialen Netzwerken öffentlich nach Verdächtigen gefahndet wird, ist nicht Teil dieser Abhandlung. Hierzu eingehend: *Kolmey* DRiZ 2013, 242 ff.; *Ihwas*, Strafverfolgung in Sozialen Netzwerken, S. 266 ff.; *Gerhold*, ZIS 2015, 156 ff.; *Caspar*, ZD 2015, 12, 15 f. m. w. N.

⁷ Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme wird aufgrund seiner wenig eingängigen Formulierung auch als IT-Grundrecht oder Computergrundrecht abgekürzt, kritisch hierzu BeckOK InfoMedienR/*Gersdorf*, Art. 2 GG, Rn. 22 m. w. N. Im Rahmen dieser Arbeit wird es als IT-Grundrecht abgekürzt, so auch *Albers*, DVBl 2010, 1061, 1068; *Gurlit*, NJW 2010, 1035, 1036; *Bäcker*, in: Uerpmann-Witzack (Hrsg.), Das neue Computergrundrecht, S. 1; *Hauser*, Das IT-Grundrecht, S. 16.

zungsprobleme der Grundrechte zueinander bei herkömmlichen Internetdiensten finden ihren Höhepunkt bei sozialen Netzwerken. Dies ist auf die mannigfaltige Bandbreite an Kommunikationsformen zurückzuführen, welche private Nachrichten, öffentliche Posts und diverse Zwischenformen umfassen. Die Abgrenzung zwischen Massen- und Individualkommunikation bzw. zwischen öffentlichen und nichtöffentlichen Daten, gerät im Zuge des Trends zur vermehrten, öffentlichen Preisgabe privater Daten an seine Grenzen. Entsprechendes gilt für das IT-Grundrecht, das auch acht Jahre nach seinem Entstehen einen trennscharfen Anwendungsbereich vermissen lässt und gerade bei repressiven Ermittlungen in informationstechnischen Systemen wie sozialen Netzwerken bisher kaum zum Tragen kommt.⁹ Neben den einschlägigen Grundrechten wird zu klären sein, welche Ermächtigungsgrundlagen der StPO anwendbar sind. Angesichts des rasanten Fortschritts im Bereich der technischen Überwachungsmaßnahmen, deren „Potential“ nicht zuletzt durch die NSA-Affäre aufgedeckt wurde, muss vor allem untersucht werden, ob das technisch Mögliche auch rechtlich zulässig ist. Das Spektrum an in Betracht kommenden Befugnisnormen umfasst beispielsweise die §§ 94 ff., 100a ff., 110a StPO sowie die §§ 161, 163 StPO.

Der Zugriff auf öffentliche Daten greift in das Recht auf informationelle Selbstbestimmung ein. Ob die Generalermittlungsklausel für diesen, von vielen als geringfügig erachteten Eingriff herangezogen werden kann, wird zu untersuchen sein. Daneben ist auch auf die Regelungen über verdeckte Ermittlungen näher einzugehen. Die §§ 110a ff. StPO gehen von einem legendierten Ermittler aus, der sich physisch in einem Milieu organisierter Kriminalität und nicht in einem virtuellen Umfeld zu behaupten hat. Beim Zugriff auf zugangsgeschützte Daten ergibt sich ein ähnliches Bild. Die Vorschriften zur Beschlagnahme stammen aus einer Zeit, in welcher der Gesetzgeber eine onlinebasierte Kommunikationsform wie soziale Netzwerke nicht antizipieren konnte.¹⁰ Ob der Zugriff auf providergespeicherte Kommunikationsinhalte auf die §§ 94 ff. StPO gestützt werden kann, bleibt auch nach der Entscheidung des BVerfG zur E-Mail-Beschlagnahme umstritten. Für die Beschlagnahme eines gesamten Accounts in sozialen Netzwerken, der das

⁸ Das Fernmeldegeheimnis wird mittlerweile auch als Telekommunikationsgeheimnis bezeichnet, BVerfGE 125, 260, 309. Im Rahmen dieser Arbeit wird der im Grundgesetz stehende Begriff Fernmeldegeheimnis verwendet.

⁹ Ähnlich auch *Hauser*, S. 16. Symptomatisch sind die knappen Ausführungen zum IT-Grundrecht bei *Ihwas*, der zwar die spezifische Gefährdungslage bei Ermittlungen in sozialen Netzwerken anspricht (S. 90 ff.), im Rahmen der Ermächtigungsgrundlagen aber die Anwendbarkeit der §§ 100a ff. StPO beim Zugriff auf unterschiedliche Datenbestände mit zwei Sätzen bejaht, *ders.*, S. 254.

¹⁰ Die Beschlagnahmenvorschriften stammen noch aus dem Jahr des Inkrafttretens der Reichstraßprozessordnung 1879, *Bär*, MMR 1998, 577, 577.