

**Strafrechtliche Abhandlungen**

---

Neue Folge · Band 276

**Die Grundrechtsrelevanz  
„virtueller Streifenfahrten“ –  
dargestellt am Beispiel ausgewählter  
Kommunikationsdienste des Internets**

Von

**Florian Eisenmenger**



**Duncker & Humblot · Berlin**

FLORIAN EISENMENGER

Die Grundrechtsrelevanz „virtueller Streifenfahrten“

# 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 276**

Die Grundrechtsrelevanz  
„virtueller Streifenfahrten“ –  
dargestellt am Beispiel ausgewählter  
Kommunikationsdienste des Internets

Von

Florian Eisenmenger



Duncker & Humblot · Berlin

Zur Aufnahme in die Reihe empfohlen von  
Professor Dr. Hans Kudlich, Erlangen

Die Rechtswissenschaftliche Fakultät  
der Friedrich-Alexander-Universität Erlangen-Nürnberg 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  
© 2017 Duncker & Humblot GmbH, Berlin  
Satz: L101 Mediengestaltung, Fürstenwalde  
Druck: buchbücher.de gmbh, Birkach  
Printed in Germany

ISSN 0720-7271  
ISBN 978-3-428-15171-4 (Print)  
ISBN 978-3-428-55171-2 (E-Book)  
ISBN 978-3-428-85171-3 (Print & E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier  
entsprechend ISO 9706 ☼

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

*Meiner Großmutter*



## Vorwort

Die vorliegende Abhandlung wurde im Wintersemester 2016/17 von der Rechtswissenschaftlichen Fakultät der Friedrich-Alexander-Universität Erlangen-Nürnberg als Dissertation angenommen. Literatur und Rechtsprechung konnten bis ca. Juli 2016 berücksichtigt werden.

Ein langer Weg hat damit seinen erfolgreichen Abschluss gefunden. Die zahlreichen Helfer und Weggefährten sowie Familienmitglieder und Freunde, die mich auf vielfältige Weise unterstützt haben, hier vollständig zu nennen, würde den Rahmen dieses Vorworts sprengen. Ihr Beistand, die vielen aufmunternden Worte und wertvollen Anregungen waren mir stets eine große Hilfe. Ihnen allen sei an dieser Stelle gleichermaßen aufrichtig gedankt. Herzlicher Dank gilt daneben meinem Doktorvater Prof. Dr. Hans Kudlich für seine Unterstützung, auch und gerade bei der Aufnahme in diese Reihe, sowie Herrn Prof. Dr. Christoph Safferling für die außergewöhnlich zügige Erstellung des Zweitgutachtens.

Ganz besonders dankbar bin ich meiner Lebensgefährtin Nina Busemann. Sie stand mir vom ersten Moment an geduldig zur Seite und hat mir auch in schweren Zeiten stets den Rücken gestärkt. Größter Dank gebührt schließlich meiner Großmutter Marie-Luise Eisenmenger, die ihr Vertrauen in mich nie verloren hat und mich immer wieder an ihrer reichhaltigen Lebenserfahrung teilhaben ließ. Die Fertigstellung dieser Arbeit hat sie nicht mehr erlebt. Ihr ist diese Arbeit gewidmet.

München, im März 2017

*Florian Eisenmenger*



# Inhaltsübersicht

<b>§ 1 Einführung</b> .....	19
A. Einleitung .....	19
B. Gegenstand der Untersuchung .....	20
C. Konzeption und Gang der Untersuchung .....	34
<b>§ 2 Grundlegung</b> .....	36
A. Freiheit und Sicherheit – zum Verhältnis von Strafverfahrens- und Verfassungsrecht .....	37
B. Rahmenbedingungen sozialer Entfaltung im virtuellen Raum .....	59
C. Erscheinungsformen kriminellen Verhaltens in Usenet, Internetforen und sozialen Netzwerken .....	114
D. Grundlegendes zur anlassunabhängigen Aufklärung des Internets .....	130
E. Zusammenfassung .....	174
<b>§ 3 Die Grundrechtsrelevanz der anlasslosen Aufklärung des Internets am Beispiel der hier untersuchten Dienste</b> .....	176
A. Grundrechtsrelevanz des <i>Social Webs</i> (Schutzbereich) .....	176
B. Der Eingriffscharakter der anlassunabhängigen Aufklärung des Internets .....	215
C. Rechtfertigung (Schranken) .....	239
D. Konsequenzen für den weiteren Verfahrensgang .....	290
E. Zusammenfassung .....	313
<b>§ 4 Zusammenfassende Gesamtbetrachtung</b> .....	315
A. Schlussfolgerungen .....	315
B. Zusammenfassung .....	323
C. Fazit .....	326
<b>§ 5 Zentrale Thesen</b> .....	328
<b>Literaturverzeichnis</b> .....	330
A. Schriftenverzeichnis .....	330
B. Internetquellen .....	362
<b>Sachregister</b> .....	376



# Inhaltsverzeichnis

<b>§ 1 Einführung</b> .....	19
A. Einleitung .....	19
B. Gegenstand der Untersuchung .....	20
I. „Virtuelle Streifenfahrten“ .....	21
II. Ausgewählte Kommunikationsdienste als Objekte behördlichen Zugriffs .....	22
1. Usenet .....	23
2. Internetforen .....	25
3. Soziale Netzwerke .....	27
a) Allgemeines .....	27
b) Funktionsweisen sozialer Netzwerke am Beispiel Facebook .....	29
c) Zwischenergebnis .....	30
4. Das soziale Element als verbindendes Merkmal .....	31
III. Ergänzung: Zur Dichotomie von Daten und Information .....	32
IV. Eingrenzung und Abgrenzung der Themenstellung .....	34
C. Konzeption und Gang der Untersuchung .....	34
<b>§ 2 Grundlegung</b> .....	36
A. Freiheit und Sicherheit – zum Verhältnis von Strafverfahrens- und Verfassungsrecht .....	37
I. Staatstheoretische Grundlagen des Strafverfahrensrechts .....	38
1. Freiheit und Sicherheit im historischen Kontext der Staats- werdung .....	38
2. Freiheit und Sicherheit im Grundgesetz .....	41
a) Freiheit .....	41
b) Sicherheit .....	43
c) Der Ausgleich von Freiheit und Sicherheit .....	45
d) Zwischenergebnis .....	47
II. Strafverfahrensrecht im Lichte der Wertordnung des Grund- gesetzes .....	47
1. Grundgesetzliche Vorgaben .....	48
2. Ergänzende Auslegung durch das Bundesverfassungsgericht .....	49
3. Zwischenergebnis .....	52
III. Grundrechtsschutz im Strafverfahren .....	53
1. Staatsrechtliches Eingriffskonzept und strafprozessuale Rechtsgrundlagen .....	53
2. Herausforderung: Informationstechnologie im Strafprozess .....	56

IV.	Fazit . . . . .	57
B.	Rahmenbedingungen sozialer Entfaltung im virtuellen Raum . . . . .	59
I.	„Normalisierung“ und Charakteristika des virtuellen Raums . . . . .	60
1.	Entstehung und Entwicklung eines neuen sozialen Raums . . . . .	61
2.	Normgeltung im virtuellen Raum . . . . .	63
a)	Regulierungsbedürftigkeit und Regulierbarkeit des Virtuellen . . . . .	64
b)	Analoge Regeln für digitale Räume – zum Einfluss der beteiligten Akteure . . . . .	69
aa)	Die Rolle des Nationalstaats . . . . .	70
bb)	Die Rolle der Nutzer . . . . .	72
cc)	Die Rolle der Wirtschaft . . . . .	76
3.	Zwischenergebnis . . . . .	79
II.	Die Kommerzialisierung des Virtuellen . . . . .	81
1.	Die Erhebung von Nutzerdaten als Geschäftsmodell . . . . .	82
2.	Das Geschäftsmodell und seine Konsequenzen . . . . .	86
3.	Zwischenergebnis . . . . .	89
III.	Gewandelte Privatheitsverständnisse? . . . . .	91
1.	Vorüberlegungen zur Dichotomie von Privatheit und Öffentlichkeit im digitalen Kontext . . . . .	92
2.	Verlust des Privaten durch unbeschränkte Öffentlichkeit im digitalen Raum? . . . . .	93
a)	Nutzerpraktiken innerhalb „Dienstöffentlichkeiten“ . . . . .	97
aa)	Identitätsmanagement . . . . .	98
bb)	Beziehungsmanagement . . . . .	100
cc)	Informationsmanagement . . . . .	101
dd)	Die Bedeutung des Publikums . . . . .	102
b)	Personalisierte bzw. persönliche Öffentlichkeiten . . . . .	103
c)	Exkurs: Pegida und die Debatte um sog. Hassbeiträge im deutschsprachigen Internet . . . . .	105
d)	Privatisierte Öffentlichkeiten . . . . .	108
3.	Soziale und technische Entwicklung . . . . .	109
4.	Zwischenergebnis . . . . .	110
IV.	Fazit . . . . .	112
C.	Erscheinungsformen kriminellen Verhaltens in Usenet, Internetforen und sozialen Netzwerken . . . . .	114
I.	Dienstspezifische Kriminalitätsphänomene . . . . .	115
1.	Usenet . . . . .	116
2.	Internetforen . . . . .	119
3.	Soziale Netzwerke . . . . .	121
4.	Exkurs: Die Nutzung sozialer Netzwerke zur Werbung für terroristische und extremistische Gruppen . . . . .	126
5.	Zwischenergebnis . . . . .	127
II.	Abgrenzung zur Computer- und Internetkriminalität . . . . .	128

III.	Ermittlungsansätze	128
IV.	Fazit	129
D.	Grundlegendes zur anlassunabhängigen Aufklärung des Internets	130
I.	Begriffsdefinition und Wesensmerkmale	130
1.	Begriffsbestimmung	131
2.	Zugriffsobjekt	132
3.	Befasste Behörden	134
4.	Erkennbarkeit der Maßnahme	135
5.	Zweck der Maßnahme	138
6.	Konsequenzen für die vorläufige Einordnung „virtueller Streifenfahrten“	140
II.	Positionen in Lehre und Rechtsprechung – zur Genese der h. M.	141
1.	Die rechtspolitische Ausgangslage	142
2.	Von Einzelstimmen zur herrschenden Meinung	143
3.	Vom Bundesverfassungsgericht zum status quo	144
4.	Zwischenergebnis	145
III.	Dogmatische Herleitung und Rückübertragung	146
1.	Zentrale Argumentationslinien und warum sie nicht überzeugen	146
a)	Testkäufer – Fälle	146
b)	Unbeachtlichkeit eines Zugriffsvorbehalts	148
c)	„Handeln wie Private“	149
d)	Einwilligung der Betroffenen	150
aa)	Einheit von Betreiber und Autor	150
bb)	Einverständnis mit unbeschränktem Zugriff	150
cc)	Auseinanderfallen von Betreiber und Autor	151
(1)	Übertragung der Dispositionsbefugnis	151
(2)	Kenntnis von der Reichweite der Erklärung	152
(3)	Sonderfall: Minderjährige	154
dd)	Zwischenergebnis	155
e)	Fehlen schutzwürdigen Vertrauens	155
2.	Zwischenergebnis: Argumentation mittels Analogiebildung	160
3.	Übertragung der Analogien in die „Realität“	161
a)	Rechtliche Bewertung und Charakteristika der polizeilichen Streifenfahrt	162
b)	Folgen für die weitere Betrachtung	163
aa)	Fehlende Wahrnehmbarkeit polizeilicher Präsenz	163
bb)	Erweiterung des räumlichen und zeitlichen Wahrneh- mungsrahmens	164
cc)	Überwindung sozialer Grenzen	165
dd)	Die nur bedingte Vergleichbarkeit „analoger“ und „virtueller“ persönlicher bzw. personalisierter Öffent- lichkeiten	167
c)	Zwischenergebnis	171

IV.	Fazit	173
E.	Zusammenfassung	174
<b>§ 3</b>	<b>Die Grundrechtsrelevanz der anlasslosen Aufklärung des Internets am Beispiel der hier untersuchten Dienste</b>	<b>176</b>
A.	Grundrechtsrelevanz des <i>Social Webs</i> (Schutzbereich)	176
I.	Art. 8 GG	177
	1. Schutzbereichseröffnung	177
	2. Zwischenergebnis	181
II.	Art. 13 GG	181
	1. Schutzbereichseröffnung bezüglich der Nutzer	181
	a) Der individuelle Account als „Wohnung“ der virtuellen Identität?	182
	b) Schutzbereichseröffnung durch externen Datenzugriff	183
	2. Schutzbereichseröffnung bezüglich der Betreiber	184
	3. Zwischenergebnis	185
III.	Art. 14 GG	185
	1. Schutzbereichseröffnung	185
	2. Zwischenergebnis	187
IV.	Art. 12 GG	187
	1. Schutzbereichseröffnung bezüglich der Nutzer	187
	2. Schutzbereichseröffnung bezüglich der Anbieter	189
	3. Zwischenergebnis	189
V.	Art. 4 GG	190
	1. Schutzbereichseröffnung bezüglich der Nutzer	190
	2. Schutzbereichseröffnung bezüglich der Anbieter	191
	3. Zwischenergebnis	191
VI.	Art. 5 GG	191
	1. Abgrenzung der umfassten Grundrechte	192
	2. Schutzbereichseröffnung	193
	a) Kommunikationsgrundrechte, Art. 5 I 1 GG	193
	b) Kunstfreiheit, Art. 5 III GG	195
	3. Zwischenergebnis	196
VII.	Art. 10 GG	196
	1. Schutzbereichseröffnung	196
	a) Kommunikation in sozialen Netzwerken	197
	b) Kommunikation in Foren	200
	c) Kommunikation in Newsgroups	200
	2. Zwischenergebnis	201
VIII.	Art. 2 I GG	201
	1. Schutzbereichseröffnung – Allgemeines Persönlichkeitsrecht	201
	a) Das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	203
	aa) Sachlicher Schutzbereich	203

	bb) Persönlicher Schutzbereich der Nutzer . . . . .	205
	cc) Persönlicher Schutzbereich der Anbieter . . . . .	205
	dd) Zwischenergebnis . . . . .	206
	b) Das Recht auf informationelle Selbstbestimmung . . . . .	206
	aa) Sachlicher Schutzbereich . . . . .	206
	bb) Eröffnung des persönlichen Schutzbereichs der Nutzer und Anbieter . . . . .	207
	cc) Grundrechtsausübung . . . . .	208
	2. Schutzbereichseröffnung – Allgemeine Handlungsfreiheit . . . . .	208
	3. Zwischenergebnis . . . . .	209
IX.	Annex: Art. 1 I GG als Grundlage des allgemeinen Persönlich- keitsrechts . . . . .	209
	1. Zur Sphärentheorie . . . . .	210
	2. Kernbereich persönlicher Lebensgestaltung . . . . .	211
	3. Zwischenergebnis . . . . .	214
X.	Zusammenfassung . . . . .	214
B.	Der Eingriffscharakter der anlassunabhängigen Aufklärung des Inter- nets . . . . .	215
I.	Eingriffsbegriff und -voraussetzungen . . . . .	216
	1. Klassischer Eingriffsbegriff . . . . .	216
	2. Moderner bzw. erweiterter Eingriffsbegriff . . . . .	216
	3. Zwischenergebnis . . . . .	217
II.	Art. 8 GG . . . . .	217
	1. Eingriff . . . . .	218
	2. Zwischenergebnis . . . . .	219
III.	Art. 12 GG . . . . .	219
	1. Eingriff . . . . .	219
	2. Zwischenergebnis . . . . .	220
IV.	Art. 4 GG . . . . .	220
	1. Eingriff . . . . .	220
	2. Zwischenergebnis . . . . .	221
V.	Art. 5 GG . . . . .	221
	1. Eingriff in Art. 5 I 1 GG . . . . .	221
	2. Eingriff in Art. 5 III GG . . . . .	223
	3. Zwischenergebnis . . . . .	223
VI.	Art. 10 GG . . . . .	223
	1. Eingriff . . . . .	223
	2. Zwischenergebnis . . . . .	224
VII.	Art. 2 I GG . . . . .	224
	1. Eingriff in die allgemeine Handlungsfreiheit . . . . .	225
	2. Eingriff in das allgemeine Persönlichkeitsrecht . . . . .	225
	a) Zugriff auf einschränkbare, aber nicht eingeschränkte Informationen . . . . .	226

b) Zugriff auf nicht einschränkbare Informationen . . . . .	230
c) Zwischenergebnis . . . . .	231
3. Eingriff in das Recht auf informationelle Selbstbestimmung . . . . .	232
a) Soziale Netzwerke . . . . .	234
b) Internetforen und Newsgroups . . . . .	235
c) Zur Erforderlichkeit der Einschränkung des Eingriffs- begriffs . . . . .	236
4. Zwischenergebnis . . . . .	237
VIII. Zusammenfassung . . . . .	237
C. Rechtfertigung (Schranken) . . . . .	239
I. Einwilligung bzw. Grundrechtsverzicht . . . . .	239
1. Zur Unmöglichkeit eines verallgemeinernden Ansatzes . . . . .	240
2. Einwilligungserklärung . . . . .	240
3. Einsichts- bzw. Einwilligungsfähigkeit der Nutzer . . . . .	244
4. Freiwilligkeit der Einwilligung . . . . .	245
5. Exkurs: „Freundschaft“ als Einwilligung? . . . . .	247
6. Zwischenergebnis . . . . .	248
II. Allgemeine Anforderungen an eine mögliche Rechtsgrundlage . . . . .	248
1. Notwendigkeit einer Rechtsgrundlage . . . . .	249
2. Allgemeine Anforderungen an eine Beschränkung des Rechts auf informationelle Selbstbestimmung . . . . .	249
III. Strafprozessuale Ermächtigungsgrundlagen . . . . .	250
1. Begriff und Zulässigkeit von Vorermittlungen . . . . .	251
a) Natur der anlassunabhängigen Aufklärung . . . . .	252
b) Rechtfertigungswirkung strafprozessualer Vorermittlungen . . . . .	254
c) Zwischenergebnis . . . . .	255
2. Strafverfolgungsvorsorge . . . . .	255
3. § 163 I 2 StPO . . . . .	256
a) Das für § 163 I 2 StPO mindestens zu fordernde Maß an Verdacht . . . . .	257
b) Die von § 163 I 2 StPO erlaubte Eingriffstiefe . . . . .	259
c) Zwischenergebnis . . . . .	261
4. Die anlassunabhängige Aufklärung als operative Maßnahme des Vorfelds? . . . . .	261
a) Das Konzept der vorbeugenden Verbrechensbekämpfung . . . . .	262
b) Das Vorfeld im weiteren Sinne . . . . .	263
c) Konsequenzen für die Einordnung der anlassunabhängigen Aufklärung . . . . .	265
d) Zwischenergebnis . . . . .	267
5. Vorläufiges Fazit . . . . .	267
IV. Annex: Verhältnismäßigkeit . . . . .	268
1. Legitimer Zweck . . . . .	268
2. Geeignetheit . . . . .	269

3. Erforderlichkeit . . . . .	270
a) Soziale Netzwerke . . . . .	270
b) Internetforen . . . . .	273
c) Usenet . . . . .	274
d) Zwischenergebnis . . . . .	275
4. Angemessenheit bzw. Verhältnismäßigkeit im engeren Sinne . . . . .	275
a) Charakteristika der anlassunabhängigen Aufklärung . . . . .	276
aa) Heimlichkeit . . . . .	276
bb) Verdachtsgrad bzw. Anlasslosigkeit . . . . .	276
cc) Streubreite . . . . .	277
dd) Unterschiedsloser Zugriff – fehlender Kernbereichs-	
schutz . . . . .	278
ee) Zwischenergebnis . . . . .	279
b) Charakteristika der betrachteten Dienste . . . . .	279
aa) Soziale Netzwerke . . . . .	279
bb) Internetforen . . . . .	281
cc) Usenet . . . . .	282
dd) Zwischenergebnis . . . . .	282
c) Durch die Maßnahme drohende Nachteile und mittelbare	
Konsequenzen . . . . .	283
d) Entgegenstehende Belange . . . . .	284
aa) Funktionstüchtigkeit der Strafrechtspflege . . . . .	284
bb) Rechtsgüter Dritter . . . . .	286
cc) Stärkung des Sicherheitsgefühls . . . . .	287
dd) Zwischenergebnis . . . . .	288
e) Abwägungsergebnis . . . . .	288
V. Zusammenfassung . . . . .	289
D. Konsequenzen für den weiteren Verfahrensgang . . . . .	290
I. Beweisverbote . . . . .	291
1. Beweiserhebungsverbote . . . . .	292
a) Beweismethodenverbote . . . . .	292
b) Beweisthemenverbote . . . . .	293
c) Beweismittelverbote . . . . .	294
d) Zwischenergebnis . . . . .	295
2. Beweisverwertungsverbote . . . . .	295
a) Kernbereichsverletzung . . . . .	296
b) Verletzungen des außerhalb des Kernbereichs liegenden	
Bereichs (Privatsphärenverletzung) . . . . .	298
aa) Fallbeispiel 1 . . . . .	299
bb) Fallbeispiel 2 . . . . .	300
cc) Zwischen- und Abwägungsergebnis . . . . .	301
c) Planmäßiges Außerachtlassen von Verfahrensvorschriften . . . . .	301
d) Recht auf ein faires Verfahren . . . . .	303

e) Grenzüberschreitende Ermittlungstätigkeit . . . . .	305
f) Zwischenergebnis . . . . .	305
3. Fern-/Vorauswirkung . . . . .	306
4. Zwischenergebnis . . . . .	308
II. Verwendungsverbote . . . . .	308
1. § 477 II 2 StPO . . . . .	309
2. § 161 II 1 StPO . . . . .	309
a) Hypothetischer Ersatzeingriff . . . . .	309
b) Zweckbindung . . . . .	310
c) Rechtmäßige Erhebung . . . . .	311
3. Zwischenergebnis . . . . .	312
III. Ergebnis . . . . .	312
E. Zusammenfassung . . . . .	313
<b>§ 4 Zusammenfassende Gesamtbetrachtung . . . . .</b>	<b>315</b>
A. Schlussfolgerungen . . . . .	315
I. Gänzlicher Verzicht auf anlassunabhängige Aufklärung . . . . .	315
II. Einschränkung: Teilverzicht . . . . .	316
III. Verrechtlichung . . . . .	316
IV. Vorschlag einer Rechtsgrundlage de lege ferenda . . . . .	318
V. Ergänzende Anmerkungen hierzu . . . . .	319
1. Verdachtsgrad . . . . .	319
2. Einschränkung des Anwendungsbereichs durch Straftaten-	
katalog . . . . .	319
3. Sonderregelung für soziale Netzwerke . . . . .	320
4. Kennungen . . . . .	320
5. Richtervorbehalt . . . . .	321
6. Kernbereichsschutz . . . . .	321
7. Berichtspflichten . . . . .	321
VI. Zwischenergebnis . . . . .	322
B. Zusammenfassung . . . . .	323
C. Fazit . . . . .	326
<b>§ 5 Zentrale Thesen . . . . .</b>	<b>328</b>
<b>Literaturverzeichnis . . . . .</b>	<b>330</b>
A. Schriftenverzeichnis . . . . .	330
B. Internetquellen . . . . .	362
I. Journalistische Inhalte und Quellen . . . . .	363
II. Sonstige Quellen . . . . .	370
<b>Sachregister . . . . .</b>	<b>376</b>

# § 1 Einführung

## A. Einleitung

Als Bundeskanzlerin Merkel am 19.06.2013 auf einer Pressekonferenz<sup>1</sup> mit dem US-Präsidenten Obama anlässlich der kurz zuvor bekannt gewordenen Geheimdienstprogramme zur flächendeckenden Überwachung des Internets das selbige zum „Neuland“ erklärte, ließen die Reaktionen nicht lange auf sich warten. Insbesondere die sog. Netzöffentlichkeit griff die Floskel dankbar auf – innerhalb kurzer Zeit entwickelte sich unter dem *hashtag* #neuland eine lebhaft, oft spöttische Diskussion zur Internetkompetenz der Politik im Allgemeinen und der Bundeskanzlerin im Besonderen, die auch von den etablierten Medien schnell begleitet wurde.<sup>2</sup> Nur gut zwanzig Jahre vorher wäre eine solche Dynamik kaum vorstellbar gewesen – das Medium Internet war gesamtgesellschaftlich genauso wenig relevant wie Thema der täglichen Berichterstattung.

Die Ursachen hierfür sind vielfältig, doch unter anderem in einem seit einigen Jahren zu beobachtenden Wandel des Mediums selbst zu suchen. In vorher nicht gekanntem Ausmaß hat sich das Internet vom futuristisch angehauchten *Cyberspace* der 1990er Jahre zu einem das tägliche Leben bestimmenden Massenkommunikationsmittel entwickelt und dabei gleichzeitig eine neue Art gesellschaftlicher und medialer Öffentlichkeit hervorgebracht. Ermöglicht hat dies eine kaum zu überblickende Menge auf den ersten Blick kostenloser Dienste, die es ihren Nutzern erlauben, sich miteinander zu vernetzen und auszutauschen, Inhalte aller Art auf Knopfdruck zu veröffentlichen und sich schließlich auch auf jede erdenkliche Weise selbst zu

---

<sup>1</sup> Eine Aufzeichnung dieser Pressekonferenz ist abrufbar unter: [https://www.youtube.com/watch?v=2n\\_-lA8GB4](https://www.youtube.com/watch?v=2n_-lA8GB4). Die angesprochene Aussage findet sich bei 2:33 und lautet im Volltext: „Das Internet ist für uns alle Neuland, und es ermöglicht auch Feinden und Gegnern unserer demokratischen Grundordnung, mit völlig neuen Möglichkeiten und völlig neuen Herangehensweisen unsere Art zu leben in Gefahr zu bringen.“

<sup>2</sup> Exemplarisch: <http://www.spiegel.de/netzwelt/netzpolitik/kanzlerin-merkel-nennt-bei-obama-besuch-das-internet-neuland-a-906673.html>; <http://www.zeit.de/digital/internet/2013-06/merkel-das-internet-ist-fuer-uns-alle-neuland>; <http://www.sueddeutsche.de/politik/kritik-an-merkels-internet-aeusserung-neuland-aufschrei-im-spiessernetz-1.1700710>. Erkenntnisse zum Nutzerverhalten stellt in diesem Zusammenhang *Busemann*, Media Perspektiven 2013, 391 dar.

inszenieren. Bei genauerem Hinsehen werden die meisten dieser Dienste allerdings von der umfassenden Vermarktung und Verwertung der Daten ihrer Nutzer getragen – das soziale Netzwerk Facebook steht zwar einerseits geradezu paradigmatisch für diese Entwicklung, markiert andererseits aber nur den Höhepunkt der Nutzung der Netzwerktechnologie zum Zwecke der sozialen Interaktion.

Damit einher gehen bislang unbekannte Chancen und Gefahren für alle Beteiligten. Dem einzelnen Nutzer bietet die neue Datenökonomie des Netzes vor allem „mehr“ – mehr Information, mehr Komfort, mehr Unterhaltung. In Kauf nehmen muss er dagegen andererseits mehr Abhängigkeit von informationstechnologischen Systemen, mehr Kontrollverlust und schließlich auch: mehr Überwachung. Jede Nutzung von Telekommunikationsdiensten, jeder Zugriff auf digitale Inhalte hinterlässt wertvolle Spuren im weltweiten Netz. Das Interesse der Sicherheitsbehörden an diesen Daten ist hinlänglich bekannt. Staatliche Bemühungen, möglichst viele davon zu erlangen – Verkehrsdatenauskunft, Vorratsdatenspeicherung, strategische Fernmeldeüberwachung, um nur einige Beispiele zu nennen –, stehen jüngst wieder im Mittelpunkt intensiver Diskussionen.

So aufschlussreich diese Daten für die Sicherheitsbehörden indes sein mögen, so stellen sie doch nur eine von mehreren Möglichkeiten der Informationsgewinnung dar. Schon lange bedienen sie sich zur Erfüllung ihrer Aufgaben auch aller im Internet öffentlich zugänglichen Daten, ohne dabei besonderes Aufsehen zu erregen. Doch wenn dort immer mehr Nutzer immer mehr von sich preisgeben und es wirklich „kein „belangloses“ Datum mehr“<sup>3</sup> gibt, dann stellt sich die Frage, ob der anlasslose Zugriff auf all diese Informationen nicht vielleicht doch auch einer Rechtsgrundlage bedarf, mithin also mit einem Grundrechtseingriff verbunden ist.

## **B. Gegenstand der Untersuchung**

Die vorliegende Untersuchung befasst sich daher mit der verfassungsrechtlichen Zulässigkeit strafprozessual motivierter und anlassunabhängig erfolgender Ermittlungen in ausgewählten Teilen des Internets. Dazu wird zunächst ein Überblick über die praktische Relevanz dieser Maßnahme gegeben (I.), bevor im Anschluss daran die einzelnen Dienste vorgestellt werden, auf die sich der Blick im Folgenden richten wird (II.). Es folgt eine knappe Erläuterung zum Verhältnis von Daten und Informationen (III.), bevor schließlich die Themenstellung konkretisiert wird (IV.).

---

<sup>3</sup> BVerfGE 65, 1, 45.

## I. „Virtuelle Streifenfahrten“

Das Internet hat sich in den letzten 20 Jahren von einem Nischendienst zu einer Kommunikationsinfrastruktur von essentieller Wichtigkeit für die moderne Gesellschaft entwickelt. Aus einem lediglich technischen Instrument wurde ein sozialer Raum. Wie überall aber, wo sich Menschen – und sei es eben nur virtuell – begegnen, kommt es früher oder später zu sozial unerwünschtem oder gar strafrechtlich relevantem Verhalten. Das Internet ist hier keine Ausnahme; auf vielfältige Weise kann es Tatort unterschiedlichster Delikte sein.

Aus den verschiedensten Gründen erlangen die Strafverfolgungsbehörden nicht immer auch Kenntnis von diesen Taten – um dem entgegenzuwirken, bedarf es also mitunter eines Einschreitens schon dann, wenn noch kein konkreter Verdacht besteht, dass eine Straftat begangen wurde. Seit gut 20 Jahren gehört eine solche anlasslose Recherche zur polizeilichen Praxis.<sup>4</sup> Wie andere Nutzer auch surfen die Beamten dabei durch das Web und sichten die öffentlich zugänglichen Informationen innerhalb verschiedener Dienste. Im Zuge einer solchen Aufklärung des Internets können dann bereits begangene Taten entdeckt, und vielleicht sogar anderweitige Ermittlungsansätze gewonnen werden – nicht ausgeschlossen ist schließlich, dass der bislang unbekannte Täter mit seinen Taten prahlt und die Beamten so erst auf die richtige Spur führt. Im Idealfall lassen sich potentielle Täter sogar von der zukünftigen Tatbegehung abschrecken, weil sie von der polizeilichen Präsenz im Netz erfahren haben. Denkbar sind darüber hinaus auch Einblicke in „szene-interne“ Entwicklungen. Ein Grundrechtseingriff soll mit dieser Maßnahme insbesondere nach Auffassung des Bundesverfassungsgerichts gleichwohl nicht einhergehen.<sup>5</sup>

Die technischen und sozialen Entwicklungen der jüngeren Vergangenheit lassen „virtuelle Streifenfahrten“ besonders erfolgversprechend erscheinen. Insbesondere soziale Netzwerke scheinen geeignet, sowohl die Gefahrenabwehr, als auch die Strafverfolgung mit den Mitteln der Informationstechnologie einer neuen Qualität zuzuführen. Bekanntheit erlangte beispielweise die Einrichtung eines eigenen Facebook-Accounts für bestimmte Polizeidienststellen („Polizei Hannover“<sup>6</sup> u. a.), oder aber auch die Nutzung des Dienstes zur

---

<sup>4</sup> Seit 1998 existiert bei dem Bundeskriminalamt die Zentralstelle für anlassunabhängige Recherchen in Datennetzen (ZaRD), [http://www.bka.de/nn\\_206376/DE/DasBKA/Aufgaben/Zentralstellen/ZaRD/zard\\_\\_node.html?\\_\\_nnn=true](http://www.bka.de/nn_206376/DE/DasBKA/Aufgaben/Zentralstellen/ZaRD/zard__node.html?__nnn=true).

<sup>5</sup> BVerfGE 120, 274, 344 f.

<sup>6</sup> <https://www.facebook.com/PolizeiHannover>; <https://www.facebook.com/PolizeiKrefeld>; <https://www.facebook.com/PolizeiHessen>; <https://www.facebook.com/PolizeiMV>.