Strafprozessuale Ermittlungsmaßnahmen in Sozialen Netzwerken

Lorenz Posch, Bonn*

Ermittlungsbehörden nutzen zunehmend auch die Möglichkeiten sozialer Netzwerke für die eigene Arbeit. Die strafprozessualen Rechtsgrundlagen dafür erscheinen aber noch nicht vollständig auf die neuen Gegebenheiten angepasst zu sein.

A. Einleitung

Die Kombination aus dem Wunsch der Ermittlungsbehörden, Straftaten in sozialen Netzwerken mindestens ebenso effektiv verfolgen zu können wie bei der „analogen" Strafverfolgung und den gewaltigen Datenmengen, weckt große Begehrlichkeiten.[1] Der vorliegende Beitrag soll für zwei exemplarische Maßnahmen die Möglichkeiten und Streitstände im Rahmen der StPO aufzeigen und kritisch beleuchten:

1. Das Ermitteln direkt in sozialen Netzwerken, die sog. „Online-Ermittlung".
2. Die Öffentlichkeitsfahndung in sozialen Netzwerken.

B. Die strafprozessualen Ermittlungsmöglichkeiten im Detail

I. „Online-Ermittler" in sozialen Netzwerken

Die direkteste Ermittlungsmethode ist das unmittelbare Durchsuchen und Auswerten von Daten, die den ermittelnden Beamten bei der Nutzung von sozialen Netzwerken selbst, in der technisch dafür vorgesehenen Art und Weise, offenbart werden.[2] Diese „Online Ermittlung" ähnelt der sog. „Online-Streife", bei der sich Polizeibeamte in ihrer dienstlichen Tätigkeit innerhalb der Netzwerke bewegen.[3] Zunächst ist hier zu klären, inwiefern es bei einem solchen Vorgehen zu Eingriffen in Grundrechte kommt, die spezielle Ermächtigungsgrundlagen notwendig machen würden.[4]

1. Mögliche Grundrechtseingriffe

Eröffnete Schutzbereiche sind insbesondere im Allgemeinen Persönlichkeitsrecht[5] (Art. 2 Abs. 1 GG), dem Recht auf informationelle Selbstbestimmung[6] (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG), der Meinungs- und Informationsfreiheit[7] (Art. 5 Abs. 1 GG) sowie dem Telekommunikationsgeheimnis[8] (Art. 10 Abs. 1 GG) zu erblicken. Daneben sind noch weitere Grundrechte möglicherweise in ihren Schutzbereichen eröffnet, beispielsweise die Religionsfreiheit[9] (Art. 4 Abs. 1 GG), die Kunstfreiheit[10] (Art. 5 Abs. 3 GG), die Versammlungsfreiheit[11] (Art. 8 Abs. 1 GG) oder die Berufsfreiheit[12] (Art. 12 Abs. 1 GG).[13] Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme („IT-Grundrecht", Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) ist hingegen nicht eröffnet, da Soziale Netzwerke gerade nicht die notwendige Er-

* Der Autor studiert Rechtswissenschaft an der Universität Bonn. Der Beitrag basiert auf einer Arbeit, welche im Rahmen eines Seminars zum IT-Strafrecht bei PD Dr. Kay Schumann angefertigt wurde.

1 *Henrichs/Wilhelm,* DP 2010, 6 (6 ff.); *Brenneisen/Staack*, Kriminalistik 2012, 627 (627 ff.); *Henrichs/Wilhelm*, Kriminalistik 2010, 30 (32); *Petri* in: Denniger (Hrsg.), Handbuch des Polizeirechts, 5. Aufl. 2012, Kap. G, Rn. 363; Vgl. auch *Oppong*, Polizei im Web: „Vernetzen und ermitteln", Meedia, http://meedia.de/2012/04/17/polizei-im-web-vernetzen-und-ermitteln/, Abruf v. 06.09.2017; sowie die Studie des Fraunhofer-Instituts: *Denef* et al, Best Practice in Police Social Media Adaptation, http://www.fit.fraunhofer.de/content/dam/fit/de/documents/COMPOSITE-social-media-best-practice.pdf, Abruf v. 06.09.2017; Weiterführend: *Monroy*, Hamburger Polizei und Geheimdienst nutzen bei Ermittlungen immer öfter Soziale Netzwerke – vielleicht bald mit spezieller Software, netzpolitik.org, https://netzpolitik.org/2013/hamburger-polizei-und-geheimdienst-nutzen-bei-ermittlungen-immer-ofter-soziale-netzwerke-vielleicht-bald-mit-spezieller-software/, Abruf v. 06.09.2017.

2 BVerfGE 120, 274 (340); *Schulz/Hoffmann*, CR 2010, 131 (131).

3 *Oermann/Staben*, Der Staat, 630 (630).

4 *Schulz/Hoffmann*, (Fn. 2), 131 (131); *Zöller*, GA 2000, 563 (568); *Singelnstein*, NStZ 2012, 593 (599); *Brenneisen/Staack*, (Fn. 1), 627 (629).

5 *Oermann/Staben*, (Fn. 3), 630 (636).

6 *Oermann/Staben*, (Fn. 3), 630 (635).

7 *Oermann/Staben*, (Fn. 3), 630 (636).

8 Anders bei für jedermann öffentlichen Mitteilungen. Hier fehlt es erkennbar an der Schutzwürdigkeit des Vertrauens in die durch Art. 10 Abs. 1 GG geschützte Vertraulichkeit der Telekommunikation, so auch: *Oermann/Staben*, (Fn. 3), 630 (632 f.).

9 Vgl. *Hufen*, Staatsrecht II, 4. Aufl. 2014, § 22 Rn. 10.

10 Vgl. *Hufen*, (Fn. 9), § 33 Rn. 12.

11 Zwar wird die Möglichkeit einer „Online-Versammlung" überwiegend abgelehnt, vgl. *Pötters/Werkmeister*, ZJS 2011, 222 (226); doch auch die ebenfalls geschützten Vorbereitungshandlungen oder auch Koordinierungsmaßnahmen können über soziale Netzwerke erfolgen, vgl. auch *Hufen*, (Fn. 9), § 30 Rn. 9.

12 Vgl. *Hufen*, (Fn. 9), § 35 Rn. 6.

13 *Oermann/Staben*, (Fn. 3), 630 (631 f.).

wartungshaltung in die Vertraulichkeit der gespeicherten Informationen und ihrer Integrität erwecken.[14]
Mithin ist der Schutzbereich vieler verschiedener Grundrechte bei der Nutzung von sozialen Netzwerken eröffnet. Aus praktischer Sicht ist problematisch, dass die tatsächlich betroffenen Grundrechte bei jeder Einzelperson je nach Nutzung stark variieren können.

a) Unmittelbar Unmittelbar-finale Eingriffe in die eröffneten Schutzbereiche

aa) Eingriff in das Recht auf informationelle Selbstbestimmung
Ein unmittelbar-finaler Grundrechtseingriff durch Online-Ermittlungen wird sowohl in der Rechtsprechung[15] als auch Literatur[16] sehr überwiegend abgelehnt. Fraglich ist dies jedoch hinsichtlich des Rechts des Grundrechtsträgers, im Rahmen des Rechts auf informationelle Selbstbestimmung über die *Preisgabe* sowie die *Verwendung* seiner personenbezogenen Daten zu bestimmen. Ein solcher Eingriff findet jedenfalls hinsichtlich der Preisgabe zunächst wohl unbestritten statt.[17]
Bezüglich der Verwendung der personenbezogenen Informationen kann nach Meinung des BVerfG ein Eingriff jedoch nur dann angenommen werden, wenn „*Informationen, die durch die Sichtung allgemein zugänglicher Inhalte gewonnen wurden, gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt*“.[18]

Mag bei einer präventiven Maßnahme („Online-Streife“) davon regelmäßig nicht auszugehen sein, so ist es im Rahmen einer Ermittlungstätigkeit, die gerade das Zusammentragen von ermittlungsrelevanten Informationen zum Gegenstand hat, deutlich wahrscheinlicher.[19] Insofern wäre auch bezüglich der Verwendung ein Eingriff zunächst anzunehmen.
Beides könnte durch eine Einwilligung der Nutzer jedoch unbeachtlich sein. Ob eine konkludente Einwilligung über die Preisgabe und Verwendung der Daten auch gegenüber und durch (Ermittlungs-) Behörden vorliegt, ist problematisch.

(1) Einwilligung der Grundrechtsträger
Fraglich ist, ob allein aus der Öffentlichkeit der online zugänglich gemachten Daten[20] eine grundrechtseingriffsausschließende Einwilligung geschlussfolgert werden kann.[21]

(a) Allgemeine Zulässigkeit des Verzichts
Zunächst müsste ein Verzicht auf grundrechtlichen Schutz bezüglich des betroffenen Grundrechts grundsätzlich möglich sein.[22] Schon aus dem Gedanken der Freiheit der Entfaltung der eigenen Persönlichkeit des Grundrechtsträgers wird dessen Verzicht auf den Schutz des Rechts der informationellen Selbstbestimmung grundsätzlich möglich sein müssen.[23]
Dies muss jedoch auch im konkreten Fall gelten. Zweifelhaft erscheint dies aufgrund der unkalkulierbar langen Dauer[24] und der durch Synergieeffekte erhöhten Eingriffsintensität.[25] Doch auch diese Gesichtspunkte können eine grundsätzliche Unmöglichkeit des Verzichts nicht begründen.
Ein Grundrechtsverzicht kann jedoch nicht grenzenlos angenommen werden, da ansonsten eine allzu leichtfertige Umgehung des grundrechtlichen Schutzes möglich würde. Zu prüfen ist folglich, ob wesentliche Anhaltspunkte gegen die Annahme einer (konkludenten) Einwilligung in den Grundrechtsverzicht bei der Nutzung von sozialen Netzwerken vorliegen. Hierfür sind insbesondere folgenden Punkte relevant:

14 *Oermann/Staben*, (Fn. 3), 630 (633); *Hoffmann-Riem*, JZ 2008, 1009 (1012); *Hufen*, (Fn. 9), § 12 Rn. 5; *Petri*, (Fn. 1), Kap. G, Rn. 10; *Roßnagel/Schnabel*, NJW 2008, 3534 (3534).

15 BVerfGE 120, 274 (344), die technische Öffnung der Webserver (für beliebige Dritte) und die fehlende Schutzwürdigkeit des Vertrauens in die unterbleibende Kenntnisnahme durch staatliche Stellen sind insoweit wohl als Einwilligungstheorie zu verstehen. Ebenso in der Bewertung: *Schulz/Hoffmann*, (Fn. 2), 131 (135); *Schulz/Hoffmann*, DuD 2012, 7 (10); *Luch/Schulz*, Das Recht auf Internet als Grundlage der Online-Grundrechte, 1. Aufl. 2013, S. 86.

16 Ebenfalls im Sinne einer Einwilligungslösung: *Bär*, ZIS 2012, 53 (58), *Bär,* in: Wabnitz/Janovsky (Hrsg.), Handbuch des Wirtschafts- und Steuerstrafrechts, 4. Aufl. 2014, Kap. 27 Rn. 123; *Bär*, MMR 1998, 463 (464); *Zöller*, (Fn. 4), 563 (569). Ohne nähere Begründung einen Eingriff ablehnend: *Soiné*, Kriminalistik 2013, 507 (511); *Roxin/Schünemann,* Strafverfahrensrecht, § 32 Rn. 2. Einen Eingriff annehmend nur: *Schulz/Hoffmann*, (Fn. 2), 131 (135); *Schulz/Hoffmann*, (Fn. 15), 7 (10); *Luch/Schulz*, (Fn. 15), S. 86.

17 *Oermann/Staben*, (Fn. 3), 630 (638 f.)

18 BVerfGE 120, 274 (344).

19 *Oermann/Staben*, (Fn. 3), 630 (639, Fn. 41); „Das gezielte Zusammentragen und Auswerten mit anderen Daten dürfte vielmehr den Regelfall bilden“, *Kutscha/Thomé*, Grundrechtsschutz im Internet, 1. Aufl. 2013, S. 31 f.

20 Zum Begriff der allgemein zugänglichen Daten siehe auch: *Klas*, Grenzen der Erhebung und Speicherung allgemein zugänglicher Daten, 1. Aufl. 2012, S. 42; BVerfGE 120, 274 (340).

21 *Petri*, (Fn. 1), Kap. G, Rn. 24.

22 Zur Problematik des Grundrechtsverzichts: *Hufen*, (Fn. 9), § 6 Rn. 42f.; *Pieroth* u.a. (Hrsg.), Grundrechte, 30 Aufl. 2014, § 5 Rn. 146 ff.; *Michael/Morlok*, Grundrechte, 4. Aufl. 2014, Rn. 534 ff.

23 *Pieroth* u.a. (Fn. 22), § 5, Rn. 152.

24 Vgl. zum sogenannten „Recht auf Vergessen“ das Urteil des EuGH, 13.05.2014, Rs. C-131/12 – Google Spain und Google.

25 *Petri*, (Fn. 1), Kap. G, Rn. 21.

(b) Individualisierung des Angebotes
Mit der notwendigen Registrierung in sozialen Netzwerken[26] geht der Wunsch der Betreiber einher, den Nutzern die eindeutige Zuordnung ihrer Kommunikationspartner und ihre Motivlage zu ermöglichen.[27] Nach Ansicht des BVerfG wird wegen der faktischen Möglichkeit der Verwendung eines Pseudonyms auch durch eine Individualisierung im Internet aber kein schutzwürdiges Vertrauen in die Identität oder Motivation der anderen Nutzer begründet.[28] Dies wäre lediglich unter besonderen Voraussetzungen möglich, wozu auch eine längere Zeit andauernde Kommunikationsbeziehung allein nicht ausreicht.[29]
Diese Differenzierung zwischen virtueller und realer Beziehungspflege kann nicht überzeugen.[30] Zwar ist ein umfassendes Vertrauen in die jeweilige Identität des Kommunikationspartners in sozialen Netzwerken durchaus nicht annehmbar,[31] doch zumindest „[d]as Vertrauen darauf, mit einer aus „privatem" Interesse handelnden Person zu kommunizieren statt mit einem „verdeckt ermittelnden" Beamten einer Sicherheitsbehörde, sollte in einem Rechtsstaat durchaus schutzwürdig sein"[32].

(c) Gesonderter Zugang zu sozialen Netzwerken für Behörden
Im Zuge der Registrierung wird der Nutzer durch Nutzungsbedingungen und Datenschutzregelungen darauf aufmerksam gemacht, dass der Zugriff für Behörden nur über gesonderte Verfahren bewilligt wird, ebenso wie die Umstände, unter welchen Daten an Dritte übermittelt werden. So ist beispielsweise die Möglichkeit der Datenerhebung durch Behörden mit Zustimmung des Nutzers bei *Facebook* gesondert geregelt. Hierbei wird auch für (netzwerk-) öffentliche Daten wie z.B. „Chronikeinträge" oder „Fotos" explizit auf die Mitwirkung des Nutzers verwiesen, der die Daten aktiv den Behörden übermitteln soll.[33] Insofern kann gerade nicht davon ausgegangen werden, dass die Nutzer, die sich bei der Registrierung mit diesen Vereinbarungen einverstanden erklären müssen, mit einem allgemeinen Zugriff durch Behörden rechnen oder in diesen auch unter deutlich geringeren Voraussetzungen eingewilligt hätten.

(d) Unvernünftiger Umgang ≠ Einwilligung
Auch ein, aus objektiver Sicht, unvernünftiger Umgang mit personenbezogenen Daten stellt lediglich den Gebrauch grundrechtlicher Freiheitsrechte dar, der gerade Ausdruck der Möglichkeit der freien Entfaltung der Persönlichkeit ist.[34] Folglich muss auch dies grundrechtlichen Schutz erfahren können und darf nicht pauschal als vom grundrechtlichen Schutz ausgeklammert betrachtet werden.[35] Die Tatsache, dass Nutzer eine Grundrechtsausübung auch vornehmen, wenn (aus ihrer Sicht) möglicherweise ungerechtfertigt in diese eingegriffen wird, bedeutet nicht, sie würden damit zugleich in eine Verletzung des Grundrechts einwilligen. Eine unfreie Grundrechtsausübung allein begründet keine wirksame Einwilligung.[36]

(e) Aufhebung der Einwilligung
Bei konsequenter Anwendung einer Einwilligungslösung müsste den Grundrechtsträgern jederzeit die Möglichkeit zustehen, durch eine Erklärung diese (fiktive) Einwilligung aufzuheben. An diese dürften dabei zugleich keine erhöhten Anforderungen gestellt werden. Insbesondere darf nicht angenommen werden, dass eine solche Erklärung nur dann ausreicht, wenn die Daten dem öffentlichen Zugriff entweder durch technische Schutzmaßnahmen oder durch alternative Methoden, z.B. Löschen, dauerhaft entzogen werden. Vielmehr muss bereits der klar geäußerte Wille des Betroffenen ausreichend sein.[37]

(2) Zwischenfazit: Keine Einwilligung
Die Annahme einer (fiktiven) Einwilligung ist deshalb abzulehnen. Auch andere Versuche, das Fehlen eines Grundrechtseingriffs dogmatisch zu begründen, überzeugen nicht.[38] Es liegt bereits ein unmittelbar-finaler Eingriff in das Recht auf informationelle Selbstbestimmung vor.[39]

bb) Eingriffe in die weiteren eröffneten Schutzbereiche
Ein unmittelbar-finaler Eingriff in die weiteren eröffneten Schutzbereiche ist abzulehnen, da die freie Grundrechtsausübung insoweit weder direkt verhindert noch erschwert wird.[40]

b) Mittelbar-faktische Eingriffe durch Abschreckung

aa) Dogmatische Herleitung
Der mittelbar-faktische Grundrechtseingriff (durch Abschreckung) stellt eine Kombination aus mittelbarem[41]

26 *Petri,* (Fn. 1), Kap. G, Rn. 363; vgl. insofern z.B. die Nutzungsbedingungen von Facebook, Punkt 4 (abrufbar unter: https://de-de.facebook.com/legal/terms?locale=de_DE) oder *Google+* (abrufbar unter https://www.google.com/intl/de_ALL/+/policy/content.html).

27 BT-Drucks. 17/13000, S. 75.

28 BVerfGE 120, 274 (345).

29 BVerfGE 120, 274 (345); ebenso: *Brenneisen/Staack*, (Fn. 1), 627 (629); *Soiné*, (Fn. 16), 507 (513).

30 *Hornung*, CR 2008, 299 (305); *Rosengarten/Römer,* NJW 2012, 1764 (1766 f.); *Singelnstein*, (Fn. 4), 593 (600); *Brenneisen/Staack*, (Fn. 1), 627 (629); *Oermann/Staben*, (Fn. 3), 630 (649).

31 Ebenso unter gewöhnlichen Umständen jedoch auch in der „realen Welt".

32 *Kutscha/Thomé*, (Fn. 19), S. 32 m.w.N.

33 Siehe unter dem Punkt „Zustimmung des Nutzers/der Nutzerin", abrufbar unter: https://de-de.facebook.com/safety/groups/law/guidelines/, Abruf v. 06.09.2017.

34 *Schulz*, DuD 2009, 601 (604).

35 *Schulz/Hoffmann*, (Fn. 2), 131 (135).

36 *Oermann/Staben*, (Fn. 3), 630 (649).

37 *Schulz/Hoffmann*, (Fn. 2), 131 (136); *Schulz/Hoffmann*, (Fn. 15), 7 (10).

38 Zu diesen: *Schulz/Hoffmann*, (Fn. 2), 131 (136); *Schulz/Hoffmann*, (Fn. 15), 7 (10); *Luch/Schulz*, (Fn. 15), S. 84 ff.

39 Im Ergebnis ebenso: *Kutscha/Thomé*, (Fn. 19), S. 30 ff., 41; *Petri*, (Fn. 1) Kap. G, Rn. 191.

40 *Oermann/Staben*, (Fn. 3), 630 (639 f.).

41 *Hufen*, (Fn. 9), § 8, Rn. 9.

und faktischem Eingriff[42] dar. Die tatsächliche (faktische) Handlung des Staates entfaltet eine Abschreckungswirkung, in deren Folge beliebige Dritte mittelbar in ihrer Grundrechtsverwirklichung beeinträchtigt werden.[43] Problematisch ist insofern, dass die faktische Verkürzung der grundrechtlichen Entfaltungsmöglichkeiten erst aufgrund einer Reaktion der Grundrechtsträger selbst entsteht.[44] Das Bundesverfassungsgericht hat bereits in einer Vielzahl von Entscheidungen ausgeführt, dass auch abschreckende Effekte als „eingriffsgleiche Maßnahme[n]"[45] verstanden werden können und insofern jedenfalls zu vermeiden sind.[46] Betroffen ist durch die sogenannten „chilling effects"[47] insbesondere die sog. Willensentschließungsfreiheit (*forum internum*) der Grundrechtsträger, die der grundrechtlichen Handlungsfreiheit vorgelagert ist.[48] Es besteht die Gefahr, dass sich Personen durch staatliche Handlungen in ihrer Willensentschließungsfreiheit beschränkt fühlen und folglich grundrechtsbeeinträchtigend wirken.[49]
Heimliche Maßnahmen wie die Online-Ermittlung können ihren Abschreckungseffekt logischerweise nicht aus dem Wissen des Betroffenen ziehen, dass er von dieser Maßnahme betroffen ist. Vielmehr reicht allein das Wissen um die Existenz solcher heimlichen Maßnahmen aus, um Personen zu einer Verhaltensanpassung zu bewegen. Sie befürchten, dass sie jederzeit Ziel einer solchen Maßnahme sein könnten. Dieser sog. panoptische Effekt[50] führt aber nicht „nur" zu einer Anpassung des Verhaltens an die objektive Rechtsordnung. Vielmehr wird das Verhalten durch die Betroffenen an ihre eigene Vorstellung der Rechtsordnung angepasst, kann also sowohl über- als auch unterschießende Tendenzen aufweisen.[51] Dabei gilt es zu bedenken, dass Betroffene gerade auch in Zweifelsfragen in ihrer Willensentschließungsfreiheit eingeschränkt sind, da sie ein (nach ihrem Verständnis) rechtskonformes Verhalten anstreben, im Zweifel also eine ansonsten gewünschte (und nach der objektiven Rechtsordnung womöglich auch gestattete) Handlung unterlassen.

bb) Subsumtion
Als Regelfall und zugleich einfachste und erfolgversprechendste Lösung erscheint es, wenn Ermittlungsbehörden fiktive Profile nutzen und sich mit diesen nach Möglichkeit weiteren Zugriff zu geschlossenen Bereichen verschaffen.[52] Die Beamten gehen insofern eine „digitale Beziehung" zu der Zielperson ein, z.B. indem sie eine „Freundschaftsanfrage" an diese versenden oder sich in geschlossene Gruppen aufnehmen lassen. Hierdurch erlangen sie auch Zugang zu Daten, die speziell ausgewählten Nutzerkreisen vorbehalten sind.
Die Besonderheit sozialer Netzwerke und zugleich wesentlicher Unterschied zu „Offline-Ermittlungen" ist, dass soziale Netzwerke nicht nur eine Momentaufnahme des Lebens der Zielperson abbilden. Vielmehr zeichnen sich soziale Netzwerke durch die Persistenz einer großen Menge von durchsuchbaren Daten aus.[53] Diese können Ermittler nicht nur suchen und auswerten, sondern auch beliebig oft kopieren und ohne Verzögerung nachverfolgen. Dabei können auch Informationen über zunächst Nicht-Verdächtige erhoben und ausgewertet werden.[54] Für Nutzer geht aufgrund der heimlichen Durchführung und der hohen Gefahr, auch unverschuldet und unverdächtigt Ziel zu werden, ein unkalkulierbares Risiko einer Grundrechtsbeeinträchtigung von solchen Maßnahmen aus. Verhaltensanpassungen aufgrund einer befürchteten Beobachtung (auch) durch den Staat sind die Folge.[55]

Innerhalb sozialer Netzwerke können eine Vielzahl von grundrechtlich geschützten Freiheiten ausgeübt werden. Die Abschreckungseffekte sind, gerade unter Bezugnahme auf bekannte Wirkungen von Chilling Effects, auch erheblich.[56] Insbesondere der zentrale grundrechtliche Schutz von Minderheiten wird durch abschreckende Hoheitsmaßnahmen besonders stark beeinträchtigt.[57]

42 *Hufen*, (Fn. 9), § 8 Rn. 10.; *Brenneisen/Staack*, (Fn. 1), 627 (627 f.).
43 *Oermann/Staben*, (Fn. 3), 630 (640).
44 *Oermann/Staben*, (Fn. 3), 630 (641).
45 BVerfGE 120, 378 (405 f.).
46 Z.B. BVerfGE 65, 1 (40, 43); 93, 181 (188); 99, 185 (197); 100, 313 (359); 107, 299 (313); 113, 63 (78); 117, 244 (259); 120, 378 (405 f.); 124, 161 (195); 125, 260 (331); 133, 277; 134, 141. Zu der uneinheitlichen sprachlichen Umschreibung dieser Abschreckungswirkung vgl. *Assion,* Überwachung und Chilling Effects in: Telemedicus e.V. (Hrsg.), Überwachung und Recht. Tagungsband zur Telemedicus Sommerkonferenz 2014, 31 (39 ff.) m.w.N. und Verweisen auch zu Urteilen des EGMR; *Englerth/Hermstrüwer*, RV 2013, 326 (344).
47 Ausführlich zu „chilling effects" allgemein: *Assion*, (Fn. 46), 31 (32 ff.).
48 *Oermann/Staben*, (Fn. 3), 630 (641) m.w.N.
49 *Oermann/Staben*, (Fn. 3), 630 (643); *Kutscha/Thomé*, (Fn. 19), S. 33.
50 *Oermann/Staben*, (Fn. 3), 630 (644) mit Erläuterung über die Entwicklung der panoptischen Verhaltensbeeinflussung.
51 *Oermann/Staben*, (Fn. 3), 630 (647).
52 *Soiné*, NStZ 2014, 248 (251); *Henrichs/Wilhelm*, (Fn. 1), 30 (35); *Schulz/Hoffmann*, (Fn. 15), 7 (12).
53 *Oermann/Staben*, (Fn. 3), 630 (648).
54 *Oermann/Staben*, (Fn. 3), 630 (648 f.).
55 Vgl. *Schenk* u.a. (Hrsg.), Digitale Privatsphäre: Heranwachsende und Datenschutz auf Sozialen Netzwerkplattformen, in: Schriftenreihe Medienforschung der Landesanstalt für Medien Nordrhein-Westfalen, Band 71, 1. Aufl. 2012, S. 235 ff.; *Sidhu*, The Chilling Effect of Government Surveillance Programs on the Use of the Internet By Muslim-Americans, in: University of Maryland Law Journal of Race, Religion, Gender and Class, 2007 S. 375 ff., online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1002145, Abruf v. 06.09.2017, S. 17 (gem. Online-Version); *Marthews/Tucker*, Government Surveillance and Internet Search Behavior, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564, Abruf v. 06.09.2017, S. 10 ff.; *Assion*, (Fn. 46), 31 (71 f.).
56 Ebenso *Oermann/Staben*, (Fn. 3), 630 (648 f.) bzgl. APR, Meinungs- und Informationsfreiheit; *Assion*, (Fn. 46), 31 (80), der insofern auch unmittelbare Eingriffe durch Chilling Effects für möglich hält.
57 *Assion*, (Fn. 46), 31 (65 ff.).

2. Mögliche Ermächtigungsgrundlagen der StPO
Aufgrund der aufgezeigten Intensität grundrechtsrelevanter Eingriffe durch Online-Ermittlungen bedürfen diese einer gesetzlichen Ermächtigungsgrundlage (Art. 20 Abs. 3 GG).[58] Fraglich ist, ob dazu bereits bestehende Ermächtigungsgrundlagen der StPO herangezogen werden können.

a) Anforderungen an die Ermächtigungsgrundlagen
Aus dem grundrechtlichen Bestimmtheitsgebot ergibt sich zunächst das Erfordernis einer förmlichen Ermächtigungsgrundlage, in der Anlass sowie Umfang der Online-Ermittlung hinreichend konkret beschrieben und eingegrenzt werden.[59]
Des Weiteren bedarf es besonderer Verfahrensanordnungen, da diese als heimliche Maßnahme zum einen eine besondere Gefahrenlage für die einzelnen Grundrechtsträger begründen, zum anderen eine gerichtliche Überprüfbarkeit mangels Kenntnis über die konkrete Betroffenheit in der Praxis häufig ausgeschlossen ist.[60].[61] Außerdem ist aufgrund der erheblichen Gefahrenlage der Erstellung umfassender Persönlichkeitsprofile und dem Einblick in Bereiche der Intimsphäre ein Konzept zum Kernbereichsschutz notwendig.[62]

b) Ermittlungsgeneralklausel §§ 161, 163 StPO
Überwiegend wird die Ermittlungsgeneralklausel als ausreichende Ermächtigungsgrundlage angesehen.[63] Insofern wird davon ausgegangen, dass es sich bei den dabei tätigen Beamten um sogenannte „nicht offen ermittelnde Polizeibeamte“ („noeP“) handelt, die vom Verdeckten Ermittler („VE“) zu unterscheiden sind.[64] Die Ermächtigungsgrundlage für den Einsatz von noep sollen nach „bröckelnde[r] h.M.“[65] die Ermittlungsgeneralklauseln darstellen.[66]
Diese Ansicht kann bereits aufgrund des aufgezeigten schwerwiegenden Eingriffs in die unterschiedlichsten Grundrechte nicht überzeugen. Die Generalermittlungsklauseln sind für ein Tätigwerden von Beamten zu Zwecken der Online-Ermittlung als untauglich anzusehen, da es sich nicht um eine intensitätsarme Maßnahme handelt.[67] Auch wird sie den dargestellten notwendigen Anforderungen nicht gerecht.[68]

c) Verdeckte Ermittler, §§ 110a-c StPO
Die Möglichkeit eines Einsatzes von VE im Internet wird bereits seit längerem unter verschiedenen Gesichtspunkten diskutiert.[69] Folglich wird die Ermächtigungsgrundlage zum Einsatz verdeckter Ermittler in der Literatur ebenfalls als Grundlage für Online-Ermittlungen herangezogen.[70]
Dagegen spricht zum einen, dass Online-Ermittler auch dann, wenn das Nutzerkonto als dienstliches Konto bekannt wird, ihre Anonymität nicht verlieren[71] und damit die wesentliche Gefahr für Verdeckte Ermittler bei Online-Ermittlungen gerade fehlt. Zum anderen mangelt es auch an den notwendigen besonderen Verfahrensanforderungen.[72]

58 *Henrichs/Wilhelm,* (Fn. 1), 30 (33); *Oermann/Staben*, (Fn. 3), 630 (656).

59 *Oermann/Staben*, (Fn. 3), 630 (657 f.); *Kudlich*, GA 2011, 193 (195); *Petri*, (Fn. 1), Kap. G, Rn. 35 ff.; BT-Drucks. 17/5200, S. 86.

60 *Kutscha/Thomé*, (Fn. 19), S. 35; *Oermann/Staben*, (Fn. 3), 630 (658); *Petri*, (Fn. 1), Kap. G, Rn. 57 ff.

61 *Oermann/Staben*, (Fn. 3), 630 (658).

62 *Kudlich*, (Fn. 66), 193 (197 f.); *Meinicke*, StV 2012, 463 (464); *Petri*, (Fn. 1), Kap. G, Rn. 28 f.

63 *Bär,* in: von Heintschel-Heinegg/Stöckel (Hrsg.), KMR-StPO, 73. Erg., Nov. 2014, § 100a Rn. 33a; *Bär*, (Fn. 16), 53 (58); *Bär,* (Fn. 16), Kap. 27 Rn. 130*; Brenneisen/Staack*, (Fn. 1), 627 (630); *Henrichs/Wilhelm*, (Fn. 1) 30 (36); *Soiné*, (Fn. 16), 507 (511); *Soiné*, (Fn. 58) 248 (249); *Klesczewski*, ZStW 2011, 737 (739)*; Hauck*, in: Erb (Hrsg.) Löwe-Rosenberg StPO, Band 3: §§ 94 – 111p, 26. Aufl. 2014, § 110a, Rn. 26; *Schulz/Hofmann*, (Fn. 15), 7 (13); so wohl nur bei offenen Inhalten, die nicht nur bestimmten Personenkreisen vorbehalten sind: *Englerth/Hermstrüwer*, (Fn. 46), 326 (358); *Brunst*, DuD 2011, 618 (623); *Kudlich*, (Fn. 66), 193 (198 f.); *Wiedemann*, Kriminalistik 2000, 229 (238); *Bruns,* in: Hannich (Hrsg.) Karlsruher Kommentar zur StPO, 7. Aufl. 2013, § 100a, Rn. 22, 110a Rn. 7; *Graf,* in: Graf (Hrsg.), Beck'scher Online-Kommentar StPO, § 100a, Rn. 32i; sofern keine dauerhafte verdeckte Tätigkeit vorliegt: *Spatscheck/Alvermann*, wistra 1999, 333 (336); *Wernert*, Internetkriminalität, 2. Aufl. 2014, S. 46 ff.; *Satzger*, in: Satzger u.a. (Hrsg.), StPO, 1. Aufl. 2014, § 110a, Rn. 9; Vgl. *Bode*, Verdeckte strafprozessuale Ermittlungsmaßnahmen, 1. Aufl. 2012, S. 453 f., der die Ermittlungsgeneralklausel insgesamt für verfassungswidrig hält.

64 *Gercke,* in: Gercke u.a. (Hrsg.), Strafprozessordnung, 5. Aufl. 2012, § 110a, Rn. 4, 11; *Frister*, in: Denniger (Hrsg.), Handbuch des Polizeirechts, 5. Aufl. 2012, Kap. F, Rn. 320; Satzger, (Fn. 70), § 110a, Rn. 10.

65 *Hauck*, (Fn. 70), § 110a, Rn. 14 m.w.N.

66 *Soiné*, Strafprozessordnung, 108. Erg., Dez. 2014, §§ 110a, Rn. 7, 163, Rn. 21; *Soiné*, (Fn. 58), 248 (249); Meyer-Goßner u.a. (Hrsg.) Strafprozessordnung, 57. Auflage 2014, § 110a, Rn. 4; *Deckers* in: Widmaier (Hrsg.), Münchener Anwaltshandbuch, 2. Aufl. 2014, § 19, Rn. 3; *Bruns* (Fn. 70), § 110a, Rn 6; *Frister*, (Fn. 71), Kap. F, Rn. 320; BT-Drucks. 12/989, S. 42; a.A. *Wolter* in: Wolter (Hrsg.), SK-StPO, Band II. §§ 94 – 136a, 4. Aufl. 2010, §110a, Rn. 13 und *Bockemühl* in: von Heintschel-Heinegg/Stöckel (Hrsg.), KMR-StPO, 73. Erg., Nov. 2014, § 110a, Rn. 9.

67 *Oermann/Staben*, (Fn. 3), 630 (660).

68 BT-Drucks. 17/5200, S. 86; *Oermann/Staben*, (Fn. 3), 630 (660).

69 *Zöller*, (Fn. 4), 563 (571 f.); *Rosengarten/Römer*, (Fn. 30), 1764 (1764).

70 *Kutscha/Thomé*, (Fn. 19), S. 41; *Bode*, (Fn. 70), S. 424, der § 110a im Weiteren jedoch für insgesamt verfassungswidrig hält; *Spatscheck/Alvermann*, (Fn. 70), 333 (336); *Rosengarten/Römer*, (Fn. 30), 1764 (1767), sofern es sich um eine dauerhafte verdeckte Tätigkeit handelt, ansonsten §§ 161, 163 StPO.

71 *Spatscheck/Alvermann*, (Fn. 70), 333 (336).

72 *Oermann/Staben*, (Fn. 3), 630 (660).

d) Telekommunikationsüberwachung §§ 100a, b, g StPO

Abschließend käme auch eine Ermächtigung durch verschiedene Normen zur Telekommunikationsüberwachung (TKÜ) in Betracht.[73] Diese kennen zwar einen Kernbereichsschutz (100a Abs. 4 StPO)[74] und auch Anlass und Umfang der Maßnahme werden eingrenzend bestimmt. Jedoch fehlt es an besonderen Verfahrensanforderungen.[75] Auch erscheint die TKÜ aufgrund ihres Charakters als „Live-Überwachungsmaßnahme" nicht geeignet, auch eine Ausforschung bereits vergangener Kommunikation, die sich in sozialen Netzwerken in erheblichem Umfang findet, sowie von nicht-kommunikativen Inhalten,[76] umfassend zu legitimieren.[77]

3. Fazit

Die herrschende Ansicht, nach der Online-Ermittlungen in sozialen Netzwerken bereits *de lege lata* rechtmäßig möglich sein sollen, stellt sich bei genauerer Betrachtung als unzutreffend heraus.[78] Eine Anpassung und Neuschaffung strafprozessualer Ermächtigungsgrundlagen ist insofern nicht mehr nur als ratsam anzusehen,[79] sondern als längst überfällig und dringend notwendig.[80]

II. Öffentlichkeitsfahndung in „sozialen Netzwerken"

Auf den ersten Blick vergleichsweise problemlos gestaltet sich dem gegenüber die Möglichkeit von Öffentlichkeitsfahndungen im Internet, §§ 131-131c StPO. Diese sind nach überwiegender Ansicht ebenfalls grundsätzlich möglich.[81] Das gilt auch für Zeugenausschreibungen nach § 131b Abs. 3 StPO.[82] Inwiefern dies jedoch eine Öffentlichkeitsfahndung auch direkt auf Dienstleistungsplattformen Dritter wie z.B. sozialen Netzwerken umfasst, ist nicht eindeutig geklärt. Dies wird auch aus den Normen an sich nicht deutlich.

In Anlage B zur RiStBV Nr. 3.2 Satz 2 heißt es diesbezüglich ergänzend: „*Private Internetanbieter sollen grundsätzlich nicht eingeschaltet werden*". Ungeklärt ist jedoch, ab wann von einem Einschalten privater Internetanbieter auszugehen ist und unter welchen Voraussetzungen von diesem Grundsatz Ausnahmen möglich bleiben sollen.

1. „Einschalten" von privaten Internetanbietern

Wegen der erheblich gesteigerten Gefahr, die insbesondere durch die Nutzung von sozialen Netzwerken zur Öffentlichkeitsfahndung ausgeht, ist in jeglicher Zugänglichmachung auf Internetseiten von privaten Dritten ein „Einschalten" im Sinne der RiStBV zu sehen. Auch das „Teilen" von Links ist folglich als „Einschalten" i.S.d. RiStBV zu werten. Damit wäre auch das Verbreiten von Links auf die – nach herrschender Ansicht rechtmäßigen – Seiten von Behörden, mit dort entsprechend publizierten Fahndungen, grundsätzlich untersagt. Dies ist auch in den Fällen zu bejahen, in denen die Funktionen des sozialen Netzwerkes durch die Behörden in der dafür vorgesehenen Art und Weise als selbstständiger Benutzer vorgenommen werden.

2. Besondere Voraussetzungen für mögliche Ausnahmen

Ebenfalls nicht näher bestimmt sind sowohl die Möglichkeiten für Ausnahmen vom Grundsatz der Nichteinschaltung von privaten Drittanbietern als auch die dabei zu beachtenden besonderen Voraussetzungen.

Durch Öffentlichkeitsfahndungen entstehen auf Dauer Verbindungen innerhalb der sozialen Netzwerke, die auch nach dem Löschen der Informationen auf der Behördenseite verbleiben. Dies kann gerade auch wegen der intensiven Prangerwirkung einer solchen Maßnahme sowie der Gefahr der Verselbstständigung von Informationen innerhalb der sozialen Netzwerke nicht einfach als „Kollateralschaden" hingenommen werden.[83] Dies ist deshalb bei der Eingrenzung möglicher Ausnahmen und ihrer Voraussetzungen zu berücksichtigen.

Dem Verfasser erscheinen dabei die folgenden Erwägungen als folgerichtig:

- Das Einschalten von Drittanbietern muss als *ultima ratio* der Öffentlichkeitsfahndung begriffen werden.[84]
- Das Einschalten Dritter darf ausschließlich aufgrund einer expliziten richterlichen Anordnung erfolgen. Die Möglichkeiten der Anordnung auch durch die Staatsanwaltschaft oder Ermittlungspersonen der Staatsanwaltschaft[85] kann nicht als ausreichend angesehen werden.

73 *Bär,* (Fn. 70), § 100a, Rn. 33; Sofern ein unautorisierter Zutritt zu geschlossenen Foren (oder wohl auch ähnlichen Bereichen innerhalb sozialer Netzwerke) vorliegt: *Klesczewski*, (Fn. 70), 737 (753 f.); *Henrichs/Wilhelm*, (Fn. 1) 30 (36).

74 Hierzu vertiefend*: Bär,* (Fn.70), § 100a, Rn. 41 ff.

75 *Oermann/Staben*, (Fn. 3), 630 (660).

76 Z.B. verschiedene Profilinformationen (Geburtsdatum, Wohnort, Beruf, Hobbys etc.), Freundeslisten oder Fotogalerien.

77 So wohl auch: *Bruns,* in: (Fn. 73), § 100a, Rn. 7 f.

78 *Oermann/Staben*, (Fn. 3), 630 (660); *Zöller,* (Fn. 4), 563 (575).

79 *Petri*, (Fn. 1), Kap. G, Rn. 363; *Kutscha/Thomé*, (Fn. 19), S. 41.

80 *Singelnstein*, (Fn. 4), 593 (597); *Zöller*, (Fn. 4), 563 (575); BT-Drucks. 17/5200, S. 86.

81 *Soiné* (Fn. 73)*,* Vorbm. §§ 131-131c, Rn. 18; *Satzger,* (Fn. 70), §131, Rn. 17; *Pfeiffer*, StPO, 5. Aufl. 2005, § 131, Rn. 4; *Wernert*, (Fn. 70), S. 53; *Paeffgen*, in: Wolter (Hrsg.), SK-StPO, Band II. §§ 94 – 136a, 4. Aufl. 2010, §§ 131a, Rn. 7, 131c, Rn. 5; *Schultheis,* in: Hannich (Hrsg.), Karlsruher Kommentar zur StPO, 7. Aufl. 2013, § 131, Rn. 15; *Graf* (Fn. 70), §131, Rn. 5; *Wernert*, (Fn. 70), S. 53; BT-Drucks. 17/13000, S. 100; siehe auch Anlage B zur RiStBV Nr. 3.2. Satz 1. Anders wohl nur: *Kühne*, Strafprozessrecht, 8. Aufl. 2010, § 31, Rn. 551.

82 *Satzger,* (Fn. 70), §131b, Rn. 10, *Pfeiffer*, (Fn. 88), § 131a, Rn. 4; *Schultheis,* (Fn. 88), § 131a, Rn. 4; wohl grundsätzlich ablehnend *Paeffgen,* (Fn. 88), § 131a, Rn. 8.

83 BT-Drucks. 17/13000, S. 100.

84 So auch BT-Drucks. 17/13000, S. 100.

85 So allgemein zulässig, vgl. §§ 131 Abs. 3 Satz 2, 131c Abs. 1 StPO.

- Der Kontrollverlust soll, auch aus datenschutzrechtlichen Gründen,[86] durch die ausschließliche Nutzung von an sich informationsarmen Links auf Behördenseiten vermieden werden. Die Behörde soll „Herrin des Verfahrens“ bleiben.[87]
- Die Anordnung ist zwingend auf eine Dauer von wenigen Tagen bis Wochen zu befristen.

3. Ergebnis

Die Möglichkeit der Öffentlichkeitsfahndung auch in sozialen Netzwerken für Ermittlungsbehörden ist bereits jetzt gegeben. Die notwendigen Voraussetzungen werden den besonderen Ansprüchen, die sich durch das Einschalten eines privaten Drittanbieters mit der Funktionsfülle und -nutzung von heutigen sozialen Netzwerken ergeben, jedoch nicht umfassend gerecht. Eine restriktive Auslegung bestehender Vorschriften mag bereits zu praktikablen Ergebnissen führen, wünschenswert wäre jedoch eine legislative Umsetzung und Klarstellung, die sich an den oben aufgestellten Grundsätzen orientieren sollte.

C. Fazit

Durch die zunehmende Einhegung digitaler Dienstleistungsangebote in unseren Alltag entstehen nicht nur neue Möglichkeiten für jeden Einzelnen und neue Gefahren durch Kriminelle, die diese ebenfalls für sich zu nutzen wissen. Zugleich wird auch staatliches Handeln einem Transformationsprozess unterworfen, mit dem die Gesetzgebung häufig nicht Schritt halten kann. So ist die aktuelle Gesetzeslage nur sehr unzureichend auf die strafprozessualen Ermittlungsformen in sozialen Netzwerken vorbereitet und in weiten Teilen bestehen keine ausreichenden Ermächtigungsgrundlagen.

Dennoch nehmen Grundrechtseingriffe durch Online-Ermittlungen und Öffentlichkeitsfahndungen in Sozialen Netzwerken immer weiter zu. Insofern ist erkennbar, dass staatliche Maßnahmen immer häufiger verdeckter Natur sind und sich damit vom Ideal des offen agierenden Staates entfernen. Heimliche Maßnahmen sollten jedoch auch weiterhin – auch weil ein effektiver Rechtsschutz für die Betroffenen in der Praxis häufig verwehrt bleibt[88] – die Ausnahme strafprozessualer Ermittlungstätigkeit darstellen. Das alles stellt verschiedenste Akteure vor neue Herausforderungen.

Notwendig ist folglich zum einen die Schaffung neuer strafprozessualer Ermittlungsgrundlagen. Diese müssen in einer immer weiter digitalisierten und vernetzten Welt einen Ausgleich zwischen Strafverfolgungsinteressen und individuellem Grundrechtsschutz schaffen. Dabei muss nicht alles, was technisch machbar wäre, auch umgesetzt werden. Beschränkungen und der damit einhergehende Mehraufwand für Strafverfolgungsbehörden sind, zum Schutz der Bürger vor dem Staat, im Gegenteil notwendig.[89]

Zum anderen wird die Weiterentwicklung der rechtswissenschaftlichen Eingriffsdogmatik, hier insbesondere der mittelbar-faktischen Eingriffe durch Abschreckung, notwendig sein, um den individuellen Grundrechtsschutz auch weiterhin effektiv gewährleisten zu können.

86 Siehe dazu bspw. die Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder: online abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/87_DSKMenschenrechteElektrische-Kommunikation.html, Abruf v. 06.09.2017.

87 BT-Drucks. 17/13000, S. 100.

88 *Petri*, (Fn. 1), Kap. G, Rn. 345.

89 *Singelnstein*, (Fn. 4), 593 (606).