Sachstand

Nutzung von Tarnidentitäten in sozialen Netzwerken durch die Polizei und die Strafverfolgungsorgane

Nutzung von Tarnidentitäten in sozialen Netzwerken durch die Polizei und die Strafverfolgungsorgane

Aktenzeichen:	WD 3 - 3000 - 280/18, WD 7 – 300 – 181/18
Abschluss der Arbeit:	30. August 2018
Fachbereich:	WD3: Verfassung und Verwaltung (Gliederungspunkt 2) WD 7: Zivil-, Straf- und Verfahrensrecht, Umweltschutzrecht, Bau und Stadtentwicklung (Gliederungspunkte 1 und 3)

Inhaltsverzeichnis

1. Einleitung

Soziale Netzwerke haben sich zu wertvollen Erkenntnisquellen für die Strafverfolgungsbehörden entwickelt. Die staatlichen Stellen bedienen sich daher, gerade im Umgang mit sozialen Netzwerken, „virtueller Ermittler[1]“.[2] Im Folgenden wird dargestellt, ob hierfür eine Ermächtigungsgrundlage erforderlich ist und ob sich die für das präventive Handeln der Polizei in der realen Welt bestehenden Ermächtigungsgrundlagen in die „virtuelle Welt“ übertragen lassen. Im Anschluss beschäftigt sich der Sachstand mit den Arten repressiver Ermittlungsformen und deren Abgrenzung. Nach der Erörterung der Frage, ob die hierfür geltenden Ermächtigungsgrundlagen auf das verdeckte Ermitteln in sozialen Netzwerken übertragbar sind, wird abschließend erläutert, wie sich ein möglicher Verstoß gegen die Nutzungsbedingungen sozialer Netzwerke auswirken kann.

2. Präventive Nutzung von Tarnidentitäten in sozialen Netzwerken durch die Polizei

Das Kommunizieren von Polizeibeamten in sozialen Netzwerken mittels einer Tarnidentität zum Zweck der Gefahrenabwehr bedarf eine Ermächtigungsgrundlage, wenn dadurch in Grundrechte eingegriffen wird.[3] Ein staatlicher Eingriff ohne Ermächtigungsgrundlage würde einen Verstoß gegen den Vorbehalt des Gesetzes aus Art. 20 Abs. 3 Grundgesetz (GG)[4] darstellen. Es stellt sich daher die Frage, welche Grundrechte durch derartige Maßnahmen der Polizei betroffen sein könnten.

Der Schutzbereich des Fernmeldegeheimnisses aus Art. 10 GG ist allein durch die Nutzung von Tarnidentitäten nicht eröffnet. Art. 10 GG schützt nur das Vertrauen des Einzelnen, dass seine Kommunikation nicht von Dritten zur Kenntnis genommen wird, nicht dagegen das Vertrauen in die Identität des Kommunikationspartners.[5] Denkbar ist jedoch ein Eingriff in das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Das Recht auf informationelle Selbstbestimmung ist Teil des allgemeinen Persönlichkeitsrechts und schützt die Befugnis

---

1 Zur besseren Lesbarkeit werden in diesem Sachstand personenbezogene Bezeichnungen, die sich zugleich auf Frauen und Männer beziehen, generell nur in der im Deutschen üblichen männlichen Form angeführt. Dies soll jedoch keinesfalls eine Geschlechterdiskriminierung oder eine Verletzung des Gleichheitsgrundsatzes zum Ausdruck bringen.

2 Antwort der Bundesregierung vom 14. Juli 2011 auf Anfrage der Abgeordneten Ulla Jelpke, Jan Korte, Dr. Petra Sitte, weiterer Abgeordneter und der Fraktion DIE LINKE – Nutzung sozialer Netzwerke zu Fahndungszwecken – BT-Drs. 17/6587.

3 Zum Erfordernis einer Ermächtigungsgrundlage siehe Grzeszick, in: Maunz/Dürig, Grundgesetz-Kommentar, 82. Ergänzungslieferung (2018), Art. 20 GG Rn. 111 ff.

4 Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliedernummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 13. Juli 2017 (BGBI. I S. 2347) geändert worden ist, abrufbar unter: https://www.gesetze-im-internet.de/gg/BJNR000010949.html [zuletzt abgerufen am [20. August 2018].

5 Bundesverfassungsgericht (BVerfG), Urteil vom 27. Februar 2008 - 1 BvR 370/7 -, BVerfGE 120, 274, 340.

des Einzelnen, über die Preisgabe und Verwendung seiner persönlichen Daten selbst zu bestimmen.[6]

Ein Eingriff in dieses Recht liegt grundsätzlich nicht vor, wenn die Polizei lediglich im Internet offen verfügbare oder für einen nicht weiter abgegrenzten Personenkreis bestimmte Kommunikationsbeziehungen abruft.[7] Dies gilt auch dann, wenn auf diese Weise im Einzelfall personenbezogene Informationen erhoben werden können. Mangels Grundrechtsrelevanz benötigt die Polizei für diese Ermittlungstätigkeiten keine spezielle Ermächtigungsgrundlage. Ausreichend sind daher die jeweiligen Aufgabenzuweisungen der landesrechtlichen Polizeigesetze. Solche Onlineermittlungen können aber im Einzelfall in das Recht auf informationelle Selbstbestimmung eingreifen, wenn die Polizei die allgemein zugänglichen Informationen gezielt zusammenträgt und auswertet und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt.[8] In diesen Fällen ist eine Ermächtigungsgrundlage erforderlich.

Ein Eingriff in das Recht auf informationelle Selbstbestimmung liegt auch dann vor, wenn die Polizei das schutzwürdige Vertrauen eines Betroffenen in die Identität und Motivation seines Kommunikationspartners ausnutzt.[9] Die Schutzwürdigkeit des Vertrauens des Betroffenen beurteilt sich maßgeblich danach, ob die Identität der Nutzer bei der Anmeldung in einem sozialen Netzwerk tatsächlich überprüft wird, was regelmäßig nicht der Fall ist.[10] Daher kann auch die Tatsache, dass die Betreiber von sozialen Netzwerken in ihren Nutzungsbedingungen die Verwendung eines Pseudonyms ausschließen, kein schutzwürdiges Vertrauen in die Identität des Kommunikationspartners begründen.[11] Jedem Teilnehmer einer solchen Kommunikation muss bewusst sein, dass er die Identität seines Kommunikationspartners nicht überprüfen kann.[12] Er kann daher auch nicht schutzwürdig darauf vertrauen, nicht mit einer staatlichen Stelle zu kommunizieren.[13] Bei einem Einsatz in einem sozialen Netzwerk, das die Identität der Teilnehmer überprüft, etwa mittels Post-Ident-Verfahren, läge hingegen ein Ausnutzen des schutzwürdigen Vertrauens des Betroffenen vor.[14] Für solche Ermittlungsmaßnahmen ist somit eine Ermächtigungsgrundlage erforderlich.

Als Ermächtigungsgrundlage für die präventivrechtliche Nutzung von Tarnidentitäten in sozialen Netzwerken kommen einerseits die polizeirechtlichen Generalklauseln der Landespolizeigesetze

---

6 Lang, in: Beck'scher Online-Kommentar Grundgesetz (BeckOK GG), hrsg. von Epping/Hillgruber, 37. Edition, Stand: 15. Mai 2015, Art. 2 Rn. 45.

7 BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/7 -, BVerfGE 120, 274, 344 f.

8 BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/7 -, BVerfGE 120, 274, 345.

9 BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/7 -, BVerfGE 120, 274, 345.

10 Kamp, in: Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen (BeckOK PolG NRW), hrsg. von Möstl/Kugelmann, 10. Edition (2018), § 20 Rn. 47.1.

11 Kamp, in: BeckOK PolG NRW, § 20 Rn. 47.1 f.

12 BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/7 -, BVerfGE 120, 274, 345.

13 BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/7 -, BVerfGE 120, 274, 345.

14 Kamp, in: BeckOK PolG NRW, § 20 Rn. 47.1 f.

in Betracht. Die Generalklauseln sind außerhalb der „virtuellen Welt“ für den kurzfristigen Einsatz von sog. nicht offen ermittelnden Polizeibeamten (noeP) ausreichend.[15] Andererseits könnten auch die jeweiligen polizeirechtlichen Vorschriften für verdeckte Ermittler einschlägig sein. Nach wohl überwiegender Auffassung in der Literatur richtet sich die Frage, welche Ermächtigungsgrundlage anzuwenden ist, hinsichtlich der „virtuellen Welt“ nach den gleichen Kriterien wie in der „realen Welt“, nämlich nach der Dauer des Einsatzes und der Intensität des Grundrechtseingriffs.[16]

3. Repressive Nutzung von Tarnidentitäten in sozialen Netzwerken durch die Strafverfolgungsorgane

3.1. Arten repressiver verdeckter Ermittlungsformen

Auch im Zuge der Verbrechensaufklärung bedienen sich die Beamten der verdeckten Ermittlung in sozialen Netzwerken. Beim repressiven Einsatz von „virtuellen Ermittlern“ in sozialen Netzwerken kommen ausschließlich Maßnahmen in Betracht, die auf der Strafprozessordnung (StPO)[17] beruhen. Den staatlichen Stellen bieten sich bei der verdeckten personalen Ermittlung zur Aufklärung begangener Straftaten im Wesentlichen zwei Möglichkeiten.

Zum einen kann, wie bei präventiven Maßnahmen, ein noeP eingesetzt werden. Für diese Variante existiert bislang keine gesonderte gesetzliche Regelung. Das Handeln der Ermittler stützt sich auf die allgemeinen Ermittlungsklauseln aus den §§ 161, 163 StPO. Die genauen Betätigungsfelder eines noeP sind nicht im Einzelnen geregelt. Die Beamten ermitteln nicht dauerhaft unter einer festen verdeckten Identität, sondern werden nur gelegentlich aktiv, ohne ihre Rolle als Ermittler offen zu legen. Sie erhalten daher in der Regel auch keine komplexe Legende. Bei dieser Form der Ermittlungsarbeit ist wie auch im präventiven Bereich nicht von einem schutzwürdigen Vertrauen in die Identität des Kommunikationspartners auszugehen, da die Angaben aufgrund der Anonymität im Netz nicht überprüfbar sind.[18]

Zum anderen kann, sofern bereits ein Anfangsverdacht besteht, ein verdeckter Ermittler im Sinne der §§ 110a ff. StPO eingesetzt werden. In diesem Fall wird für den entsprechenden Beamten eine Legende gebildet. Gemäß § 110a Abs. 2 und 3 StPO ist eine Legende eine auf Dauer angelegte, veränderte Identität, die am Rechtsverkehr teilnehmen darf und der Durchführung des Ein-

---

15 Vgl. für entsprechende repressive Maßnahmen Soiné, Personale verdeckte Ermittlungen in sozialen Netzwerken zur Strafverfolgung, Neue Zeitschrift für Strafrecht (NStZ) 2014, 248 (249 f.).

16 Die Diskussion wird weitestgehend auf der Grundlage der entsprechenden Vorschriften der StPO geführt, vgl. etwa Rosengarten/Römer, Der „virtuelle verdeckte Ermittler“ in sozialen Netzwerken und Internetboards, Neue Juristische Wochenschrift (NJW) 2012, 1764; Singelnstein, Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co, NStZ 2012, 593 (600).

17 Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Gesetz vom 30. Dezember 2017 (BGBl. I S. 3618) m.W.v. 09. November 2017 geändert worden ist, abrufbar unter: https://www.gesetze-im-internet.de/stpo/ [zuletzt abgerufen am 20. August 2018].

18 BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/7 -, BVerfGE 120, 274, 345.

satzes dienen soll. Voraussetzung für den Einsatz eines verdeckten Ermittlers ist zudem, dass zureichende tatsächliche Anhaltspunkte für eine Straftat von erheblicher Bedeutung auf dem Gebiet des unerlaubten Betäubungsmittel- oder Waffenverkehrs, der Geld- oder Wertzeichenfälschung, auf dem Gebiet des Staatschutzes (§§ 74a, 120 des Gerichtsverfassungsgesetzes)[19], gewerbs- oder gewohnheitsmäßig oder von einem Bandenmitglied oder in einer anderer Weise organsiert begangen worden sind, § 110a Abs. 1 S.1 StPO. Zudem sind die §§ 110a bis 110c StPO anwendbar, wenn es sich bei der Tat um ein Verbrechen, also eine Straftat mit einer Mindeststrafe von einem Jahr, handelt, wenn Wiederholungsgefahr besteht oder die Tat von besonderer Bedeutung war und der Einsatz andere Maßnahmen aussichtlos wäre. Der Einsatz eines verdeckten Ermittlers ist dabei von der Anordnung der Staatsanwaltschaft abhängig, § 110b Abs. 1 S.1 StPO. Soll zudem gegen eine bestimmte Person ermittelt werden, wovon in der zu Grunde liegenden Situation auszugehen ist, bedarf der Einsatz der richterlichen Zustimmung, § 110b Absatz 2 Nr. 1 StPO.

3.2. Abgrenzung der Ermittlungsformen

Die Rechtsprechung hat eine Reihe von Kriterien herausgearbeitet, anhand derer die Ermittlungsformen des verdeckten Ermittlers und des noeP in der realen Welt zu unterscheiden sind.[20] So kommt es im Zuge einer Gesamtbewertung hauptsächlich auf das Merkmal der Legende und die Intensität des Grundrechtseingriffs an.[21] Entscheidend ist, „ob der Ermittlungsauftrag über einzelne wenige, konkret bestimmte Ermittlungshandlungen hinausgeht, ob es erforderlich sein wird, eine unbestimmte Vielzahl von Personen über die wahre Identität des verdeckt operierenden Polizeibeamten zu täuschen, und ob wegen der Art und des Umfanges des Auftrages von vornherein abzusehen ist, dass die Identität des Beamten in künftigen Strafverfahren auf Dauer geheim gehalten werden muss“.[22]

3.3. Übertragbarkeit der Ermächtigungsgrundlagen in die „virtuelle Welt“

Ob die §§ 110a ff. StPO und die Generalklauseln der §§ 161, 163 StPO als Ermächtigungsgrundlage auf den Einsatz „virtueller Ermittler“ in sozialen Netzwerken übertragbar sind, wird nicht einheitlich beantwortet.[23] Die Gerichte mussten sich mit dieser Frage bislang nicht befassen. In einer Antwort auf eine Kleine Anfrage aus dem Jahr 2011 hat die Bundesregierung die Auffassung vertreten, dass für die verdeckte Ermittlungstätigkeit in sozialen Netzwerken dieselben

---

19 Gerichtsverfassungsgesetz in der Fassung der Bekanntmachung vom 9. Mai 1975 (BGBl. I S. 1077), das zuletzt durch Artikel 1 des Gesetzes vom 12. Juli 2018 (BGBI. I S. 1151) geändert worden ist, abrufbar unter: https://www.gesetze-im-internet.de/gvg [zuletzt abgerufen am 20. August 2018].

20 Bundesgerichtshof (BGH), Urteil vom 7. März 1995 - 1 StR 685/94 -, NJW 1995, 2237 f.; BGH, Urteil vom 6. Februar 1996 - 1 StR 544/95 -, NStZ 1996, 450.

21 BGH, Urteil vom 7. März 1995. - 1 StR 685/94 -, NJW 1995, 2237 f.

22 BGH, Urteil vom 7. März 1995. - 1 StR 685/94 -. Njw 1995, 2238.

23 Bauer, Soziale Netzwerke und strafprozessuale Ermittlungen, 2018, Berlin, S. 198 m.w.N.

Rechtsgrundlagen maßgeblich sind wie für die Ermittlungstätigkeit in der realen Welt.[24] Dieser Auffassung begegnen in der Literatur erhebliche Bedenken.[25] Nach Meinung einiger Autoren stehe einer Anwendung der Ermächtigungsgrundlagen für den verdeckten Ermittler in der sogenannten „virtuellen Welt“ entgegen, dass die §§ 110a ff. StPO für Ermittler geschaffen wurden, die in realen Kontakt mit der Zielperson treten. Es werde in diesem Zusammenhang zwischen den Beamten, welche in der „realen“ und „virtuellen“ Welt ermitteln, unterschieden. Die „virtuellen verdeckten Ermittler“ nähmen, anders als die in der „realen Welt“, nicht am Rechtsverkehr teil und bedürften, entgegen des Normzwecks der §§ 100a ff. StPO auch keines Schutzes, da eine Konfrontation mit der Zielperson nahezu ausgeschlossen werden könne. Zudem wird daraufhin gewiesen, dass der „virtuelle verdeckte Ermittler“ bei der Einführung des § 110a am im Jahr 1992 nicht bedacht worden sei. Auch in der umfangreichen Änderung der StPO von Dezember 2012 zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen[26] wurde der „virtuelle verdeckte Ermittler“, obwohl er zu diesem Zeitpunkt bereits ermittlungstaktische Relevanz erlangt hatte, nicht explizit bedacht. An diesem Umstand scheitere auch eine analoge Anwendung des § 110a StPO, da es sich gerade nicht um eine planwidrige Regelungslücke handele. Auch der Rückgriff auf Generalermittlungsklauseln wird abgelehnt. Die §§ 161, 163 StPO würden nur geringfügige Grundrechtseingriffe abdecken. Die gezielte Kommunikation mit einer Zielperson durch einen „virtuellen Ermittler“ könne schon auf Grund ihrer Eingriffstiefe damit nicht gemeint sein.[27]

Zusammenfassend lässt sich festhalten, dass für den Einsatz „virtueller Ermittler“ in sozialen Netzwerken zwei verschiedene Ermächtigungsgrundlagen in Betracht kommen. Je nachdem Grad des schützenswerten Interesses der Zielperson ist zwischen noeP und verdeckten Ermittlern zu unterscheiden. Die Anforderungen an den Einsatz eines verdeckten Ermittlers (formell und materiell) sind dabei wesentlich höher, als die für den nur Generalklausel artig abgedeckten, nicht offen ermittelnden Polizeibeamten. Ob ein schützenwertes Vertrauen gegeben ist und welche der beiden Ermittlungsformen konkret vorliegt, ist der Rechtsprechung zu Folge stets anhand einer Gesamtwürdigung im Einzelfall festzustellen.

3.4. Verstoß verdeckter Ermittler gegen Nutzungsbestimmungen sozialer Netzwerke bei repressiven Ermittlungstätigkeiten

Um verdeckt in sozialen Netzwerken ermitteln zu können, erstellt die Polizei Accounts unter falschen Namen. Diese Praxis widerspricht in der Regel den Nutzungsbestimmungen der sozialen

---

24 Antwort der Bundesregierung vom 14. Juli 2011 auf Anfrage der Abgeordneten Ulla Jelpke, Jan Korte, Dr. Petra Sitte, weiterer Abgeordneter und der Fraktion DIE LINKE – Nutzung sozialer Netzwerke zu Fahndungszwecken – BT-Drs. 17/6587, vgl. die Erörterungen zu Frage 3, S. 3.
Ebenso: Rosengarten/Römer, NJW 2012, 1764; Singelnstein, NStZ 2012, 593, 600.

25 Bauer, Soziale Netzwerke und strafprozessuale Ermittlungen, S. 209; Ihwas, Strafverfolgung in sozialen Netzwerken, 1. Auflage, 2014, Baden-Baden, S. 172.

26 Gesetzentwurf der Bundesregierung zur Neuregelung der Telekommunikationsüberwachung und andere verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 27. Juni – BT-Drs. 16/5846.

27 Bauer, Soziale Netzwerke und strafprozessuale Ermittlungen, S. 204.

Netzwerke.[28] Es stellt sich die Frage, welche Folgen sich daraus ergeben. Nach einer im Schrifttum vertretenen Auffassung sollen die Nutzungsbedingungen der sozialen Netzwerke für die Strafverfolgungsbehörden nicht wirksam sein. Da der Staat den Dienst nicht als solchen zur Kommunikation in Anspruch nehme, sondern sich zum Zwecke der Strafverfolgung in dem Netzwerk vorhandener Informationen bediene, komme zwischen ihm und dem Betreiber des sozialen Netzwerks kein zivilrechtlicher Vertrag zustande.[29] Denn der Staat nehme mit der Ermittlungstätigkeit eine hoheitliche Aufgabe wahr. In diesem Verhältnis des Staates zu dem Bürger entfalten zivilrechtliche Vereinbarungen keine Wirkung, sodass bei Vorliegen einer ausreichenden Ermächtigungsgrundlage die Nutzungsbedingungen auf die Rechtmäßigkeit des Handelns der Behörden keinen Einfluss haben können.[30]

Aber selbst wenn man davon ausgehe, dass zwischen den Strafverfolgungsbehörden und dem Betreiber ein zivilrechtlicher Vertrag zustande komme, habe dies nur zur Folge, dass im Falle eines Verstoßes gegen die Nutzungsbedingungen durch die Strafverfolgungsbehörden dem Betreiber bestimmte Rechte zustünden. Da sich die Rechtswirkung eines Schuldverhältnisses grundsätzlich auf die an ihm Beteiligten beschränke,[31] könnten andere Nutzer grundsätzlich keine Rechte aus solch einem Verstoß der Strafverfolgungsbehörden herleiten.

Weiter ist zu überlegen, ob ein Verstoß gegen die Nutzungsbedingungen Auswirkungen dahingehend hat, dass hierdurch ein schutzwürdiges Vertrauen des Nutzers in die Identität des Kommunikationspartners begründet wird. Nach Auffassung des Bundesverfassungsgerichts ist aber für die Begründung eines solch schutzwürdigen Vertrauens allein maßgeblich, ob Mechanismen bereitstehen, die die Identität der Nutzer überprüfen.[32] Denn jedem Nutzer sei bewusst, dass er die Identität seines Kommunikationspartners nicht kenne, beziehungsweise diese nicht überprüfen könne.[33] Daraus schließt eine in der Literatur vertretene Meinung, dann sei auch unerheblich, ob die Verwendung einer Tarnidentität gegen die Nutzungsbestimmungen verstieße oder nicht.[34]

* * *

28 Vgl. https://de-de.facebook.com/legal/terms [zuletzt abgerufen am 20. August 2018].

29 Ihwas, Strafverfolgung in sozialen Netzwerken, S. 165.

30 Ihwas, Strafverfolgung in sozialen Netzwerken, S. 165.

31 Mansel, in: Jauernig Bürgerliches Gesetzbuch: BGB, 17. Auflage (2018), § 241 Rn. 4; Bachmann in Münchener Kommentar zum BGB, 7. Auflage (2016), § 241 Rn. 11.

32 BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/7 -, BVerfGE 120, 274, 340 f.

33 BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/7 -, BVerfGE 120, 274, 340 f.

34 Kamp, in: BeckOK PolG NRW, § 20 Rn. 47.1 f.