MAKrim XIV 2018/ 2019

Erstgutachter: Prof. Dr. Ken Eckstein

Zweitgutachter: Dr. Holger Plank

Masterarbeit

Verdeckte personale Ermittlungen im Cyberspace

Vorgelegt von:

Kathrin Wecker, LL.M.

Inhaltsverzeichnis

A. Einleitung

> *„Das Internet ist wie eine Welle: Entweder man lernt, auf ihr zu schwimmen, oder man geht unter.“ Bill Gates*

In Zeiten des „Internet of Things“, Web 2.0, Cloud Computing – einer fortschreitenden Vernetzung – spielt der Cyberspace eine immer größere Rolle im Leben der Menschen. Diese Ubiquität führt dazu, dass die Grenzen zwischen dem Leben in der realen Welt und dem in der virtuellen Welt zusehends verschwimmen. In der Literatur wird in diesem Zusammenhang gelegentlich von einer sog. Onlife-Welt[1] gesprochen. Durch diese Verschmelzung entstehen neue Tatgelegenheiten und Tatdynamiken, sodass auch Polizeibehörden ihre Aktivitäten in den Cyberspace verlagern müssen und die Spezifika dieses Raums berücksichtigen müssen. Polizeibehörden können hierbei, wie auch im realen Leben, entweder präventiv oder aber repressiv tätig werden. Die StPO hat den Cyberspace als neuen Einsatzraum partiell erkannt, so z.B. im Rahmen der Online-Durchsuchung gemäß § 100b StPO. Danach darf auch ohne Wissen des Betroffenen mit technischen Mitteln in ein von ihm genutztes informationstechnisches System eingegriffen werden. Darüber hinaus dürfen auch bestimmte Daten daraus erhoben werden, sofern die in der StPO näher bestimmten Voraussetzungen vorliegen. Hierbei handelt es sich um ein technisches Mittel zur Informationsbeschaffung. Daneben existieren jedoch auch personale verdeckte Mittel zur Beschaffung von Informationen. Zu unterscheiden sind verdeckte Ermittler[2], nicht offen ermittelnde Polizeibeamte (noeP), Vertrauenspersonen und Informanten. Einzig die erste Var. – der verdeckte Ermittler – ist gesetzlich, sowohl in der StPO als auch z.B. im PolG NRW, explizit geregelt.

Im Rahmen dieser Arbeit soll, anknüpfend an das o.g. Zitat von *Bill Gates*, untersucht werden, ob die Polizeibehörden im Hinblick auf personale verdeckte Ermittlungsmaßnahmen „auf der Welle schwimmen oder aber untergehen“. Daher werden zunächst einführend diese unterschiedlichen Typen verdeckter personaler Ermittler dargestellt (B). Darauffolgend wird der Cyberspace dogmatisch als Ort der persönlichen und sozialen Entfaltung untersucht

[1] *Hoffmann-Riem,* Rechtliche Rahmenbedingungen für und regulative Herausforderungen durch Big Data, S. 22.

[2] Das in dieser Arbeit verwendete generische Maskulinum bezieht sich immer zugleich auf weibliche, diverse und männliche Personen.

(C), vor allem anlässlich bzw. vor dem Hintergrund der fortschreitenden Digitalisierung und der immer stärker werdenden Offenlegung des Privaten im Cyberspace[3]. Hintergrund dieser Einordnung ist, dass diese als Grundlage für den folgenden Gliederungspunkt, die Beurteilung der Grundrechtsrelevanz, fungiert.

Mithin sollen im Anschluss unterschiedliche Einsatzszenarien, wie z.B. in Chatforen oder sozialen Netzwerken, auf ihre Grundrechtsrelevanz hin untersucht werden (D). Der Fokus liegt hier auf einer Prüfung der Art. 10, Art. 13 und Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Eine besondere Berücksichtigung erfährt in diesem Zusammenhang das Grundsatz-Urteil des BVerfG zur Online-Durchsuchung aus dem Jahr 2008. Im Rahmen dieses Gliederungspunktes soll zudem u.a. die Frage näher beleuchtet werden, ob für die jeweiligen Szenarien im Cyberspace die gleichen Rechtsgrundlagen und Maßstäbe, wie etwa die Abgrenzungskriterien zwischen einem verdeckten Ermittler und einem noeP, Anwendung finden können, wie es in der realen Welt der Fall wäre. Darüber hinaus wird ein weiteres Szenario, das aus einer aktuellen Entwicklung im Bereich der verdeckten personalen Ermittlungen hervorgeht – der Entwurf eines möglichen § 163g StPO – betrachtet, der Teil des Referentenentwurf zum IT-SiG 2.0 ist. Laut diesem soll der Verdächtige einer Straftat in bestimmten Fällen dazu verpflichtet werden, die zur Nutzung der virtuellen Identität erforderlichen Zugangsdaten herauszugeben.[4]

Anknüpfend an eine jüngst durch den BT beschlossene Ergänzung des § 184b Abs. 5 StGB um einen neuen S. 2, soll sich zum Schluss mit einem Sonderproblem im Bereich der personalen verdeckten Ermittlungen – der Keuschheitsprobe – beschäftigt werden, die v.a. im Bereich der Aufklärung von Delikten der Kinderpornographie Relevanz entfaltet (E).

[3] So z.B. *Bernard*, Komplizen der Erkennungsdienstes: Das Selbst in der digitalen Kultur. In diesem Buch beschäftigt er sich mit der Profilbild der Individuen im Cyberspace und somit mit der vermehrten Offenlegung von vormals Privatem.
[4] *BMI*, Referentenentwurf eines IT-SiG 2.0, S. 32.

B. Darstellung der einzelnen Figuren verdeckter personaler Ermittler

Verdeckte personale Ermittler kommen sowohl im realen als auch im virtuellen Raum primär zum Einsatz, wenn das Einsatzszenario ein offenes Handeln der Strafverfolgungsbehörden verbietet. Häufig sind dies Fälle der organisierten Kriminalität.[5] Die Ermittler können in diesem Zusammenhang sowohl präventiv als auch repressiv tätig werden.

Es wird grundsätzlich zwischen drei Arten verdeckter personaler Ermittler unterschieden, die im Folgenden näher dargestellt werden. Auffallend ist an dieser Stelle, dass nur einer dieser Typen – der verdeckte Ermittler – explizit gesetzlich geregelt ist. Zunächst werden die Figuren und die jeweiligen Problemfelder abstrakt dargestellt. Im weiteren Verlauf dieser Arbeit soll sodann darauf aufbauend die Frage beantwortet werden, ob und wie dieses aktuelle partielle Regelungsregime, vor dem Hintergrund der dogmatischen Untersuchung des Cyberspace, auch auf personale Ermittlungsmaßnahmen in dieser Umgebung anwendbar ist.

I. Der verdeckte Ermittler

Der verdeckte Ermittler ist die einzige Figur eines personalen verdeckten Mittels der Informationsbeschaffung, die – sowohl in den Polizeigesetzen des Bundes und der Länder als auch in der StPO – explizit geregelt ist. Da das Gefahrenabwehrrecht und das Strafverfolgungsrecht jeweils unterschiedliche Zwecke erfüllen, sollen diese im weiteren Verlauf der Bearbeitung jedoch nicht miteinander vermengt werden. Der zentrale Fokus wird auf den verdeckten Ermittler mit repressiver Zielsetzung gelegt.[6]

[5] Vgl. *Hegmann*, in: Graf, BeckOK StPO, § 110a StPO Rn. 1.

[6] Gleichwohl sei an dieser Stelle nicht unerwähnt gelassen, dass eine klare zeitgenaue Abgrenzung in einigen Fällen nicht immer möglich ist. In den jeweiligen Polizeigesetzen und auch in § 110c Abs. 3 StPO wird explizit erwähnt, dass sich die Befugnisse des verdeckten Ermittlers auch nach anderen Vorschriften richten können. Damit wird auf die gefahrenabwehrrechtlichen Befugnisse Bezug genommen, die durch die Regelungen in der StPO nicht beschränkt werden (vgl. *Gercke*, in: Gercke u.a., Heidelberger Kommentar, Strafprozessordnung, § 110c StPO Rn. 4; *Graulich*, in: Bäcker/Denninger/Graulich, Handbuch des Polizeirechts, Abschnitt E, Rn. 740). Abgrenzungsprobleme können dann entstehen, wenn eine sog. Gemengelage vorliegt, d.h. der Polizeibeamte ursprünglich präventiv agiert hat, nunmehr jedoch ein Anfangsverdacht für eine Straftat vorliegt. Sodann richtet sich sein weiteres Handeln nach der StPO mit der Folge, dass z.B. die Verfahrensvoraussetzungen nach § 110b StPO einzuhalten sind (vgl. *Bruns*, in: Hannich, Karlsruher Kommentar zur Strafprozessordnung, § 110a StPO Rn. 14).

1. Begriff des verdeckten Ermittlers

Gemäß § 110a Abs. 2 S. 1 StPO sind verdeckte Ermittler Beamte des Polizeidienstes, die unter einer ihnen verliehenen, auf Dauer angelegten, veränderten Identität (Legende) ermitteln. Unter dieser Legende dürfen sie sodann am Rechtsverkehr teilnehmen (vgl. § 110a Abs. 2 S. 2 StPO). Vor diesem Hintergrund erklären sich die detaillierten Verfahrensvorschriften des § 110b StPO[7], da durch den Einsatz eines verdeckten Ermittlers der allgemeine Rechtsverkehr durch eine nicht nur unerhebliche Täuschung des Gegenübers gefährdet werden kann.[8]

Wann also wird aus einem Mitarbeiter der Polizei ein verdeckter Ermittler im Sinne des § 110a Abs. 2 S. 1 StPO? Zunächst muss es sich um einen *Beamten* im Polizeidienst handeln. Die Anforderung des Beamtentums lässt sich darauf zurückführen, dass damit eine disziplinarrechtliche Dienstaufsicht einhergeht, die wiederum die erforderliche engmaschige Führung fördert.[9] Darüber hinaus soll das Beamtentum, über die Berücksichtigung der hergebrachten Grundsätze des Berufsbeamtentums[10] eine rechtliche und wirtschaftliche Unabhängigkeit gewährleisten[11], die vor dem Hintergrund der Involvierung des Polizeibeamten in kriminelle Strukturen auch sachdienlich ist.

Entscheidendes Charakteristikum für das Vorliegen der Rechtsfigur des verdeckten Ermittlers ist das Bestehen einer auf Dauer angelegten Legende; gleichzeitig stellt dieses Merkmal auch das zentrale Abgrenzungskriterium zum noeP dar. Eine Legende, also eine Veränderung der eigenen Identität des Polizeibeamten, betrifft u.a. die folgenden persönlichen Merkmale: Name, Vorname, Anschrift, Nationalität, Beruf und sonstige familiäre und persönliche Umstände.[12] Der Beamte konstruiert sich insofern einen neuen Lebenslauf, den er nach außen hin überzeugend vertreten und vor allem leben kann. Sinn

[7] Der Einsatz eines verdeckten Ermittlers erfordert nach § 110b Abs. 1 S. 1 StPO immer mindestens die Zustimmung der Staatsanwaltschaft. Sofern ein zielgerichteter Einsatz dieses Ermittlungsmittels gegen einen bestimmten Beschuldigten erfolgen soll (§ 110b Abs. 2 S. 1 Nr. 1 StPO) oder aber eine nicht allgemein zugängliche Wohnung betreten wird (§ 110b Abs. 2 S. 1 Nr. 2 StPO), ist darüber hinaus die schriftliche Zustimmung des Gerichts erforderlich.

[8] Vgl. *Hegmann*, in: Graf, BeckOK StPO, § 110a StPO Rn. 2.

[9] Vgl. *Bruns*, in: Hannich, Karlsruher Kommentar zur Strafprozessordnung, § 110a StPO Rn. 5.

[10] Die hergebrachten Grundsätze des Berufsbeamtentums umfassen z.B. das Alimentationsprinzip, das eine lebenslange angemessene Besoldung garantiert (vgl. *Pieroth*, in: Jarass/Pieroth, GG, Art. 33 GG Rn. 63) oder aber die Pflichten des Beamten zur Unbestechlichkeit und Uneigennützigkeit und zum Gehorsam (vgl. *Pieroth*, in: Jarass/Pieroth, GG, Art. 33 GG Rn. 58).

[11] Vgl. *Pieroth*, in: Jarass/Pieroth, GG, Art. 33 GG Rn. 44.

[12] Vgl. *Wolter/Jäger*, in: Wolter, SK StPO, Band II, § 110a StPO Rn. 14.

und Zweck einer solchen Legende ist es, die wahre Identität des verdeckten Ermittlers zu verschleiern, um so die Ermittlungstätigkeit zu fördern oder sie überhaupt erst zu ermöglichen. Gleichzeitig erfüllt sie auch eine Schutzfunktion im Verhältnis zur Zielperson, da nicht auszuschließen ist, dass diese dem agierenden Polizeibeamten – im Falle eines Bekanntwerdens der Ermittlungstätigkeit – nachstellen könnte oder aber andere Repressalien an ihm vollziehen könnte.[13]

Die Legende muss nach dem Wortlaut des § 110a Abs. 2 S. 1 StPO auf Dauer angelegt sein. Der Terminus „auf Dauer angelegt" kann in diesem Zusammenhang auf zwei unterschiedliche Arten ausgelegt werden. Betrachtet man ausschließlich den Wortlaut, beinhaltet dieser zunächst einen zeitlichen Moment. Die Begrifflichkeit impliziert eine gewisse Beständigkeit und Substanz, die durch die Verwendung des Wortes „angelegt" zum Ausdruck kommt. Auf zeitliche Mindestgrenzen kann es daher nicht ankommen[14], vielmehr folgt aus diesem Terminus eine subjektive Absichtskomponente, die sich jedoch auch äußerlich manifestieren muss. Legt man diese Art der Auslegung zugrunde, wären somit das Auftreten des verdeckten Ermittlers nach außen und der Kontakt zur Zielperson von Relevanz.[15] Demnach führt auch der BGH in seiner grundlegenden Entscheidung aus dem Jahr 1995 aus:

> *„Entscheidend ist, ob der Ermittlungs**auftrag** über einzelne wenige, konkret bestimmte Ermittlungshandlungen hinausgeht, ob es erforderlich werden 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 geheimgehalten werden muß. Dabei ist darauf abzustellen, ob der allgemeine Rechtsverkehr oder die Beschuldigtenrechte in künftigen Strafverfahren eine mehr als nur unerhebliche Beeinträchtigung durch den Einsatz des verdeckt operierenden Polizeibeamten erfahren können."*[16]

[13] Vgl. *Bauer*, Soziale Netzwerke und strafprozessuale Ermittlungen, S. 192; *Schneider*, Ausgewählte Rechtsprobleme des Einsatzes verdeckter Ermittler – Eine Zwischenbilanz, NStZ 2004, 359, 362.
[14] Vgl. BGH, Urteil vom 07. März 1995 – 1 StR 685/94 –, juris, Rn. 7.
[15] Vgl. *Günther*, in: Kudlich, Münchener Kommentar zur Strafprozessordnung, Band 1, § 110a StPO Rn. 30.
[16] BGH, Urteil vom 07. März 1995 – 1 StR 685/94 –, juris, Rn. 7.

Auffallend an diesem Zitat ist, dass der BGH hier auf den Ermittlungsauftrag abstellt, also auf den jeweiligen Einsatz und nicht auf die Legende als solche.[17]

Diese Kriterien bestätigte der BGH in einer weiteren Entscheidung aus dem Jahr 2016, in der er noch einmal die Bedeutsamkeit des Auftretens nach außen und den Kontakt zum Beschuldigten herausstellte.[18] Ein gelegentliches und kurzes Auftreten könne daher nicht ausreichen. Erforderlich sei vielmehr eine schwerwiegende Täuschung, die auch eine gewisse Dauer erfordere. Vor diesem Hintergrund sei auch § 110b Abs. 2 S. 4 StPO zu sehen, der bestimmt, dass die Maßnahme zu beenden ist, wenn nicht das Gericht binnen drei Werktagen zustimmt.[19] Eine ähnliche Regelung findet sich auch in § 110b Abs. 1 S. 2 StPO, der ein Zustimmungserfordernis der Staatsanwaltschaft binnen drei Werktagen statuiert. Aus der Erwähnung dieser drei Tage könnte daher nunmehr gefolgert werden, dass derartige Maßnahmen grundsätzlich länger als drei Tage andauern und somit keine Einzelmaßnahmen von § 110a Abs. 2 S. 1 StPO erfasst sind.

Problematisch ist indes, dass diese 3-Tage-Fristenregelung kein Spezifikum des Regelungsregimes des verdeckten Ermittlers darstellt. Vielmehr kann diese z.B. in § 98 Abs. 2 S. 1 StPO (Beschlagnahme) oder aber in § 100e Abs. 1 S. 2 StPO (TKÜ) gefunden werden. Eine Festlegung dahingehend, dass mit dieser Frist auch Aussagen über die Dauer der strafprozessualen Maßnahmen getroffen werden, findet in diesem Zusammenhang jedoch keineswegs statt. Stattdessen erfüllt diese eine „grundrechtssichernde Funktion“[20].

Abweichend von der Rechtsprechung des BGH kann die Begrifflichkeit „auf Dauer angelegt“ auch mit einem anderen Schwerpunkt ausgelegt werden. Wird systematisch die semantische Struktur des § 110a Abs. 2 S. 1 StPO betrachtet, fällt auf, dass von einer „auf Dauer angelegten, veränderten Identität (Legende)“ die Rede ist. Durch die hier auszulegende Begrifflichkeit kann also auch eine qualitative Anforderung an die Legende zum Ausdruck gebracht

[17] So auch vgl. *Hauck*, in: Beck u.a., Löwe-Rosenberg, Die Strafprozessordnung und das Gerichtsverfassungsgesetz, § 110a StPO Rn. 21.
[18] Vgl. BGH, Urteil vom 06. Februar 1996 – 1 StR 544/95 –, juris, Rn. 8.
[19] Vgl. ebd., Rn. 9.
[20] *Günther*, in: Kudlich, Münchener Kommentar zur Strafprozessordnung, Band 1, § 110a StPO Rn. 31.

werden.[21] Sodann müsste eine qualifizierte Legende vorliegen, die sich nicht nur auf die Nutzung von Deckpapieren, wie z.B. einem Personalausweis, erstreckt, sondern vielmehr einen zweiten eigenständigen Lebenslauf erfordert. Dazu gehören dann auch zur Legende passende Eintragungen in entsprechenden Registern, darüber hinaus wären auch eine zweite Wohnung und ein legendiertes soziales Umfeld erforderlich.[22] Kurz gesagt, würde diese Auslegung bedeuten, dass eine von der Klaridentität verschiedene Deckidentität kreiert werden müsste, die über eine gewisse inhaltliche und äußerlich manifestierte Substanz verfügt. Eine derartige Legende wird „Grundlegende" genannt, die jeweils auf den konkreten Ermittlungsanlass angepasst werden kann. Diese Legende wird dann als „anlassbezogene Legende" bezeichnet.[23]

Zusammenfassend lässt sich sagen, dass Teile der Literatur zurecht eine vom BGH abweichende Auslegung wählen. Zuvörderst spricht die Auslegung der Begrifflichkeit „auf Dauer" in ihrem systematischen Satzzusammenhang dafür, hierin eine Anforderung an die Legende und nicht an den Einsatz zu sehen. § 110a Abs. 2 S. 1 StPO erwähnt den Einsatz in diesem Zusammenhang nicht, sodass die Auslegung des BGH an dieser Stelle den Wortlaut der Norm verlässt. Darüber hinaus erfordert auch der Sinn und Zweck einer Legende, also die Vertarnung der Klaridentität, dass diese über einen gewissen Umfang verfügt, denn nur so kann sie ihre Funktion erfüllen.[24] Die Legende wird dem verdeckten Ermittler *verliehen*. Legt man diesen Begriff mithilfe seines Wortlautes aus, erfordert eine Verleihung in der Regel einen gewissen zuvor getätigten Aufwand. So wird – völlig unjuristisch argumentiert – z.B. das deutsche Sportabzeichen verliehen. Um ein solches zu erhalten, mussten zuvor jedoch gewisse substanzielle Anstrengungen unternommen werden. Ähnliches gilt für die Verleihung von Statusämtern, wie z.B. des Beamtenstatus. Auch hier müssen zunächst gewisse Tatsachen geschaffen werden, wie z.B. das Vorliegen der gesundheitlichen und fachlichen Eignung, erst dann kann die Verleihung erfolgen. Auf die hier gegenständliche Legende übertragen, spricht somit auch

[21] Vgl. *Schneider*, Ausgewählte Rechtsprobleme des Einsatzes verdeckter Ermittler – Eine Zwischenbilanz, NStZ 2004, 359, 361.
[22] Vgl. *Günther*, in: Kudlich, Münchener Kommentar zur Strafprozessordnung, Band 1, § 110a StPO Rn. 16.
[23] Vgl. ebd.
[24] Vgl. *Schneider*, Ausgewählte Rechtsprobleme des Einsatzes verdeckter Ermittler – Eine Zwischenbilanz, NStZ 2004, 359, 363.

die Verwendung des Wortes „verliehen“ dafür, dass sich aus der Formulierung „auf Dauer angelegt“ qualitative Anforderungen an die Legende ergeben.[25]

Folgte man der Auffassung des BGH dennoch, hätte dies zur Folge, dass kurzfristige Einsätze von Polizeibeamten unter einer substantiierten und umfassenden Deckidentität nicht unter die strengen Anforderungen der §§ 110a und 110b StPO fielen, obwohl eine umfangreiche Täuschung des Beschuldigten vorläge, die dazu führt, dass dieser nicht mehr freiwillig über die Weitergabe von Informationen, v.a. personenbezogene Daten, entscheiden kann. Ein Eingriff in das aus dem allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG abgeleiteten Recht auf informationelle Selbstbestimmung ist der Ermittlungshandlung der Polizei also immanent; die Kürze der Ermittlungshandlung ist insofern nicht entscheidend, vielmehr kommt es auf die Qualität der Täuschung an, die sich aus der Ausnutzung schützenswerten Vertrauens ergeben kann. Auf den Punkt bringt dieses Paradoxon *Hauck*:

> „[…] nach der Interpretation des Bundesgerichtshofs stünde es der Polizei bei kurzfristigen, punktuellen Ermittlungshandlungen (die keinen „Einsatz“ im Sinne des § 110a darstellen sollen) völlig frei, ob sie den mit einer Legende ausgestatteten Beamten als Verdeckten Ermittler oder als sonstigen „Nicht offen ermittelnden Polizeibeamten“ behandelt.“[26]

Eine solche Interpretation wird jedoch der Schwere des Grundrechtseingriffs nicht gerecht. Diese ergibt sich nicht aus der Dauer der Ermittlungshandlung, sondern aus der konkreten Ausgestaltung ebendieser – nämlich dem Auftreten unter einer substantiierten Legende. Nach der Auffassung des BGH könnte bei kurzfristigen, punktuellen Ermittlungshandlungen stets auf die Generalklausel gemäß §§ 161, 163 StPO zurückgegriffen werden. So könnten u.a. die formellen Anforderungen des § 110b StPO umgangen werden. Diese Sichtweise, die allein auf die Dauer des Einsatzes abstellt, vermag vor diesem Hintergrund daher erst recht nicht zu überzeugen.[27]

---

[25] So auch *Schneider*, Ausgewählte Rechtsprobleme des Einsatzes verdeckter Ermittler – Eine Zwischenbilanz, NStZ 2004, 359, 362.

[26] *Hauck*, in: Beck u.a., Löwe-Rosenberg, Die Strafprozessordnung und das Gerichtsverfassungsgesetz, § 110a StPO Rn. 24.

[27] Gesetzesvergleichend findet sich die Begrifflichkeit „auf Dauer angelegte Legende“ auch in anderen Gesetzen außerhalb der StPO, beispielhaft sei an dieser Stelle § 9a Abs. 1 S. 1 BVerfSchG genannt. Ein Vergleich mit dem BVerfSchG bietet sich deshalb an, da sowohl die Strafverfolgungsbehörden als auch die Nachrichtendienste als Sicherheitsbehörden einzuordnen sind. Zudem werden der verdeckte personale Ermittler sowie auch der verdeckte Mitarbeiter des Bundesamtes für

2. Einsatzvoraussetzungen

Die Einsatzvoraussetzungen eines verdeckten Ermittlers sind in § 110a Abs. 1 StPO geregelt. Dieser unterscheidet zwischen der Aufklärung von Katalogdeliktsgruppen nach S. 1 und der Aufklärung von Verbrechen nach S. 2 und 4. Somit handelt es sich gesetzessystematisch um eine Mischung aus Katalogdelikten und einer Art Generalklausel hinsichtlich der Aufklärung von Verbrechen.[28]

a) Aufklärung von Katalogdeliktsgruppen

Wie bereits oben dargestellt, kommt der verdeckte Ermittler vorrangig im Bereich der organisierten Kriminalität zum Einsatz. Dieses Einsatzszenario greift der Gesetzgeber durch die Aufzählung spezifischer Deliktsgruppen, wie z.B. Straftaten auf dem Gebiet des Staatsschutzes (Nr. 2), auf. Darüber hinaus müssen diese Taten jedoch auch von erheblicher Bedeutung sein. Das alleinige Vorliegen eines Anfangsverdachts der Begehung einer Tat aus dem Deliktskatalog ist mithin nicht ausreichend. Ferner ist es nicht entscheidend, ob es sich bei der Straftat um ein Verbrechen oder Vergehen handelt. Eine solche Regelungssystematik findet sich z.B. auch im Rahmen der Rasterfahndung gemäß § 98 Abs. 1 S. 1 StPO. Eine Straftat ist dann von erheblicher Bedeutung, wenn sie mindestens dem Bereich der mittleren Kriminalität zuzuordnen ist, eine empfindliche Störung des Rechtsfriedens durch sie verursacht wird, und die Tat dazu geeignet ist, eine erhebliche Beeinträchtigung des Empfindens der Rechtssicherheit der Bevölkerung herbeizuführen.[29]

Verfassungsschutz (über den Verweis des § 5 BNDG bzw. § 5 MADG auch der Mitarbeiter des Bundesnachrichtendienstes bzw. des Bundesamtes für den militärischen Abschirmdienst) zur persönlichen Informationsgewinnung eingesetzt, wenn auch der Auftrag jeweils ein anderer ist und sich die Befugnisse unterscheiden.
Gemäß § 9a Abs. 1 S. 1 BVerfSchG darf das Bundesamt für Verfassungsschutz eigene Mitarbeiter unter einer ihnen verliehenen und auf Dauer angelegten Legende zur Aufklärung von Bestrebungen unter den Voraussetzungen des § 9 Abs. 1 BVerfSchG einsetzen. In diesem Zusammenhang stellt sich die gleiche Auslegungsfrage wie im Hinblick auf § 110a Abs. 2 S. 1 StPO. Im dazugehörigen Entwurf eines Gesetzes zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes (BT-Drs. 18/4654) ist auf S. 26 in dem Abschnitt „Zu § 9a Absatz 1“ die Rede von einem „dauerhaften“ Einsatz. Dies ist insofern interessant, als dass der Gesetzgeber in seiner Gesetzesbegründung „dauerhaft“ als Synonym zu „auf Dauer angelegt“ verwendet und damit klar macht, dass es ihm hier tatsächlich auf die Dauer des Einsatzes ankommt. Ob diese Sichtweise vor dem Hintergrund der obigen Darstellungen verfassungsmäßig ist, da auch bei einem Einsatz eines verdeckten Mitarbeiters des Bundesamtes für Verfassungsschutz – unabhängig von dessen Länge – u.U. ein schutzwürdiges Vertrauen auf Seiten der Zielperson entstehen kann, kann an dieser Stelle jedoch dahingestellt bleiben, da das Handeln von Nachrichtendiensten nicht Gegenstand dieser Arbeit ist.

[28] Vgl. *Hauck*, in: Beck u.a., Löwe-Rosenberg, Die Strafprozessordnung und das Gerichtsverfassungsgesetz, § 110a StPO Rn. 32.

[29] Vgl. ebd., Rn. 35.

Darüber hinaus muss der Einsatz des verdeckten Ermittlers der Subsidiaritätsklausel aus S. 3 genügen. Der Einsatz ist danach nur zulässig, soweit die Aufklärung auf andere Weise aussichtslos oder wesentlich erschwert wäre.

b) Aufklärung von Verbrechen

Gemäß § 110a Abs. 1 S. 2 StPO darf ein verdeckter Ermittler zur Aufklärung von Verbrechen auch eingesetzt werden, soweit aufgrund bestimmter Tatsachen die Gefahr der Wiederholung besteht. Durch diese Ergänzung werden die Einsatzmöglichkeiten verdeckter Ermittler erweitert: Erforderlich ist nunmehr keine Tat mehr aus dem Deliktskatalog aus S. 1, auch muss es sich um keine Straftat von erheblicher Bedeutung handeln. Damit wird die Schwelle für den Einsatz des verdeckten Ermittlers deutlich gesenkt. Erforderlich ist nur das Vorliegen einer auf bestimmten Tatsachen gestützten Wiederholungsgefahr eines Verbrechens. Diese muss sich jedoch auf den Einzelfall beziehen und darf nicht auf generelle kriminalistische Erfahrungssätze gestützt werden.[30] Auch hinsichtlich der Aufklärung von Verbrechen greift wieder die Subsidiaritätsklausel aus S. 3.

Ein weiteres Einsatzszenario im Rahmen der Aufklärung von Verbrechen findet sich sodann in S. 4. Laut diesem dürfen verdeckte Ermittler außerdem eingesetzt werden, wenn die besondere Bedeutung der Tat den Einsatz gebietet und andere Maßnahmen aussichtslos wären. Diese Konstellation erfasst also Verbrechen, die nicht unter den Katalog nach S. 1 fallen und für die keine konkrete Wiederholungsgefahr nach S. 2 vorliegt. Im Vergleich zur Subsidiaritätsklausel nach S. 3 fällt auf, dass hier eine wesentliche Erschwerung der Aufklärung der Tat nicht genügt, vielmehr müssen andere Maßnahmen stets aussichtslos sein. Statt wie in S. 1 eine Straftat von erheblicher Bedeutung zu fordern, bezieht sich der Gesetzgeber in S. 4 auf die besondere Bedeutung der Tat. Die Formulierungen verfolgen jedoch die gleiche Intention, da beide Ausprägungen des verfassungsrechtlichen Verhältnismäßigkeitsgrundsatzes sind.[31] Nach diesem Grundsatz muss staatliches Eingriffshandeln grundsätzlich verhältnismäßig sein, d.h. einen legitimen Zweck verfolgen, geeignet, er-

[30] Vgl. *Hauck*, in: Beck u.a., Löwe-Rosenberg, Die Strafprozessordnung und das Gerichtsverfassungsgesetz, § 110a StPO Rn. 39.
[31] Vgl. ebd., Rn. 40.

forderlich und angemessen sein. Entscheidend ist hier das Merkmal der Angemessenheit. Danach muss ein Grundrechtseingriff „in einem angemessenen Verhältnis zu dem Gewicht und der Bedeutung des Grundrechts stehen“[32]. Im Kern findet in diesem Punkt also eine Abwägung zwischen den Grundrechtseingriffen und der Bedeutung des durch die Maßnahme verfolgten Zwecks statt.[33] Diese Gedanken finden auch im Rahmen des S. 4 Anwendung. Liegt keine Tat nach dem Deliktskatalog des S. 1 vor und besteht auch keine Wiederholungsgefahr, muss es sich zumindest um die Aufklärung einer Tat von besonderer Bedeutung handeln, um so die Bedeutung des durch die verdeckte Ermittlung verfolgten Zwecks, den Grundrechtseingriff auf Seiten des Beschuldigten, überwiegen zu lassen. Zur Konkretisierung derartiger Taten kann § 24 Abs. 1 Nr. 3 GVG als Orientierung herangezogen werden, welcher ebenfalls diese Formulierung wählt und die erstinstanzliche Zuständigkeit der Landgerichte in Strafsachen umschreibt.[34] Danach ist eine Straftat dann von besonderer Bedeutung, wenn sie sich „aus der Masse der durchschnittlichen Straftaten nach oben heraushebt“[35]. Dieser Umstand kann sich sowohl aus tatsächlichen als auch aus rechtlichen Aspekten ergeben.[36]

II. Nicht offen ermittelnder Polizeibeamter

Vom verdeckten Ermittler nach § 110a StPO zu unterscheiden ist der noeP. Dieser ist gesetzlich nicht explizit geregelt, sodass auf die Ermittlungsgeneralklausel aus §§ 161, 163 StPO zurückgegriffen wird. Entscheidendes Abgrenzungskriterium zum verdeckten Ermittler ist das Merkmal der auf Dauer angelegten Legende, insofern kann auf die obigen Darstellungen Bezug genommen werden. Je nach Auslegung wäre der Einsatz eines noeP also bei nur gelegentlich unter Legende ermittelnden Polizeibeamten (BGH) oder aber bei einer eher oberflächlichen Legende (Literatur) zu bejahen. Eine derartige Legende ist z.B. dann anzunehmen, wenn einzig der Klarname durch einen Decknamen ersetzt wird.

[32] BVerfG, Beschluss vom 20. Juni 1984 – 1 BvR 1494/78 –, BVerfGE 67, 157-185, juris, Rn. 48.
[33] Vgl. *Schulze-Fielitz*, in: Dreier, Grundgesetz Kommentar, Band II, Art. 20 GG Rn. 184.
[34] Vgl. *Günther*, in: Kudlich, Münchener Kommentar zur Strafprozessordnung, Band 1, § 110a StPO Rn. 14.
[35] BGH, Urteil vom 10. Mai 2001 – 1 StR 504/00 –, BGHSt 47, 16-21, juris, Rn. 13.
[36] Vgl. ebd.

III. Vertrauenspersonen und Informanten

Sowohl beim verdeckten Ermittler nach § 110a Abs. 2 S. 1 StPO als auch beim noeP, handelt es sich um Beamte des Polizeidienstes, die innerhalb krimineller Strukturen ermitteln. Verdeckte personale Ermittler können jedoch auch Personen außerhalb der polizeilichen Strukturen sein. Darunter fallen u.a. Vertrauenspersonen und Informanten, die keine Angehörigen einer Strafverfolgungsbehörde sind. Sie unterscheiden sich hinsichtlich des zeitlichen Umfangs ihrer Zusammenarbeit mit den Polizeibehörden. Während eine Vertrauensperson über einen längeren Zeitraum unterstützend im Rahmen der Aufklärung von Straftaten tätig wird, wird auf den Informanten nur im Einzelfall zurückgegriffen.[37] Beide Figuren sind nicht gesetzlich geregelt, was jedoch keine unbeabsichtigte Gesetzeslücke darstellt, sondern vielmehr durch den Gesetzgeber explizit so intendiert ist.[38] Eine analoge Anwendung der Regelungen über den verdeckten Ermittler kommt also mangels einer planwidrigen Regelungslücke nicht in Betracht.[39]

C. Dogmatische Untersuchung des Cyberspace als Ort der persönlichen und sozialen Entfaltung

Bevor die einzelnen Einsatzszenarien des personalen verdeckten Ermittlers im Cyberspace auf ihre Grundrechtsrelevanz hin untersucht werden können, ist es zunächst notwendig, sich grundsätzlich mit dem Cyberspace als Ort der

[37] Vgl. *Bruns*, in: Hannich, Karlsruher Kommentar zur Strafprozessordnung, § 110a StPO Rn. 9.

[38] Vgl. BT-Drs. 12/989 – Entwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG): Auf Seite 41 wird ausdrücklich ausgeführt, dass aus dem Verzicht einer expliziten Regelung der Vertrauenspersonen und Informanten jedoch nicht geschlossen werden dürfe, dass deren Heranziehung nicht zulässig sei. Vielmehr sah der Gesetzgeber kein Regelungsbedürfnis, da beide Personengruppen als Zeugen behandelt werden könnten und somit eine Rechtsgrundlage für ihre Heranziehung vorhanden sei.
Gleichwohl wird aber die Figur der Vertrauensperson z.B. im BVerfSchG in § 9b explizit geregelt. Gemäß § 9b Abs. 1 S. 1 BVerfSchG sind Vertrauensleute Privatpersonen, deren planmäßige, dauerhafte Zusammenarbeit mit dem Bundesamt für Verfassungsschutz Dritten nicht bekannt ist. Im Anschluss werden Anwerbungsverbote und das Verfahren geregelt; über den Verweis auf § 9a BVerfSchG werden die weiteren Rahmenbedingungen näher konkretisiert. Hintergrund dieser expliziten Regelung ist die öffentliche Diskussion anlässlich des NSU-Untersuchungsausschusses, die dem Einsatz von Vertrauensleuten negativ gegenüberstand. Mit der Schaffung einer expliziten gesetzlichen Regelung sollte daher auch die Akzeptanz dieses Mittels der Informationsgewinnung mit menschlichen Quellen gestärkt werden (vgl. *Graulich*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, § 9b BVerfSchG, Rn. 1 und 2). Es bleibt an dieser Stelle abzuwarten, ob sich dieser „Regelungstrend“ auch auf den polizeilichen Bereich übertragen wird.

[39] Vgl. *Bruns*, in: Hannich, Karlsruher Kommentar zur Strafprozessordnung, § 110a StPO Rn. 9.

persönlichen und sozialen Entfaltung zu beschäftigen. Ähnlich einem gerichtlichen Urteil bedarf es zunächst Feststellungen zum Sachverhalt, ehe dieser einer rechtlichen Würdigung unterzogen werden kann.

I. Der Cyberspace

1. Definition und Abgrenzung

Was bedeutet der Begriff Cyberspace? Zuvörderst ist er eine Zusammensetzung aus den Worten „Cyber“ und „Space“, die jeweils für „steuern“ bzw. „navigieren“ und „Raum“ stehen.[40] Damit versteht man unter Cyberspace, kurz gesagt, einen virtuellen Raum, in welchem ein Individuum navigieren kann, sich die einzelnen Akteure aber aufgrund der Virtualität nicht physisch gegenübertreten. Je nach Größe des Raumes können dies einzelne Computernetzwerke (Cyberspace im engeren Sinne) sein, es kann sich allerdings auch um die gesamte virtuelle Realität (Cyberspace im weiten Sinne) handeln. Cyberspace ist nicht gleichbedeutend mit Internet. Vielmehr ist das Internet als Grundlage für die Entwicklung des Cyberspace zu sehen, also als die Menge der technischen Voraussetzungen, die zur Entstehung dieses virtuellen Raumes erforderlich sind.[41]

Neben anderen prägenden Merkmalen, wie der Automatisierbarkeit der dortigen Aktivitäten, der Flüchtigkeit der Daten und der Kopierbarkeit der Artefakte[42], zeichnet sich der Cyberspace sowohl im weiten als auch im engeren Sinne durch die Merkmale der Virtualisierung und Vernetzung aus, die zu dem Phänomen der räumlichen Entgrenzung führen. Von einer Virtualisierung ist die Rede, wenn die Datenverarbeitung nicht mehr an eine körperliche Hardware geknüpft ist.[43] *Brodowski/Freiling* sprechen in diesem Zusammenhang von einer „Entkoppelung von der Ausführungshardware“[44]. Das Merkmal der Vernetzung bezieht sich wiederum auf den geografischen Aufenthaltsort. So

[40] Vgl. *Bühl*, Die virtuelle Gesellschaft: Ökonomie, Politik und Kultur im Zeichen des Cyberspace, S. 23.
[41] Vgl. *Hobe*, Cyberspace – der virtuelle Raum, Rn. 8.
[42] Vgl. *Brodowski/Freiling*, Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, S. 26.
[43] Vgl. ebd., S. 21.
[44] Ebd., S. 23.

sind die Daten im Cyberspace nicht nur von der jeweiligen Ausführungshardware entkoppelt, sondern auch vom geografischen Aufenthaltsort.[45] Virtualisierung und Vernetzung führen also letztlich zu einer räumlichen Entgrenzung des Cyberspace.

Eine dogmatische Untersuchung des Cyberspace im weiten Sinne ist im Rahmen der hier vorliegenden Arbeit nicht möglich und würde bestenfalls in pauschalen Ausführungen münden, daher muss eine Eingrenzung auf einen Cyberspace im engeren Sinne erfolgen.

Diese Eingrenzung soll vor dem Hintergrund des Begriffs „Web 2.0“ erfolgen, der als markantes Schlagwort vor allem die *Rolle des Nutzers* im Cyberspace beschreibt. Der Akteur des Nutzers ist für die vorliegende Arbeit von besonderem Interesse, da das Ermittlungsmittel des personalen verdeckten Ermittlers vorrangig im Rahmen einer Interaktion mit diesem zum Einsatz kommt.

2. Eingrenzung anhand des Terminus „Web 2.0“

Das Sozialverhalten der Menschen im virtuellen Raum wird maßgeblich durch das sog. Web 2.0 geprägt. Eine klare Definition sucht man in der Literatur zwar vergebens[46], dennoch fungiert die Bezeichnung als eine Art Oberbegriff, der im Kern eine Veränderung im Kommunikationsverhalten des Nutzers im Cyberspace [47], also eine neue Form der Anwendung des Internets, beschreibt.[48] Der Nutzer ist nicht mehr allein passiver Konsument der Inhalte des Cyberspace, sondern gestaltet diese aktiv, z.B. durch das Hochladen eigener Fotos auf Instagram, mit. Das Rollenverständnis des Nutzers hat sich dahingehend gewandelt, dass er seiner reinen Rezipienten-Rolle entwachsen ist und nunmehr als aktiver Akteur im Cyberspace agiert. Inhalte in diesem Raum werden also nicht mehr durch vereinzelte Individuen erzeugt[49], sondern von „den Vielen, aus denen eins entsteht: das virtuelle Netzwerk (Netzwerkgesellschaft)

[45] Vgl. *Brodowski/Freiling*, Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, S. 23.
[46] Vgl. *Bauer*, Soziale Netzwerke und strafprozessuale Ermittlungen, S. 26.
[47] Vgl. *Henrichs/Wilhelm*, Polizeiliche Ermittlungen in sozialen Netzwerken, Kriminalistik 2010, 30.
[48] Vgl. *Frank*, in: Harte-Bavendamm/Henning-Bodewig, Gesetz gegen den unlauteren Wettbewerb, Einl. H. Rn. 52.
[49] Durch eine solche Informationsverbreitung zeichnete sich hingegen das Web 1.0 aus. Diese Bezeichnung dient als Schlagwort für die Erstellung von Inhalten, die nur durch Wenige für viele erzeugt werden (vgl. *Schmidt/Pruß*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, § 3 Rn. 123).

der sozial und global Verbundenen“[50]. Kurzum, der Nutzer wird zum sog. „Prosumenten“.[51] Bei diesem Neologismus, der sich auch des Stilmittels des Oxymorons bedient, handelt es sich um eine Kombination aus den beiden Wörtern „Produzent“ und „Konsument“, womit die Doppelrolle des Nutzers des Cyberspace zum Ausdruck gebracht werden soll. Dieser Wandel im Rollenbild ist v.a. auf eine Veränderung der technischen Rahmenbedingungen zurückzuführen. So war es vermutlich noch nie so einfach, eigene Inhalte im Cyberspace zu erzeugen. Wurden anfangs noch vertiefte HTML-Kenntnisse und eine eigene Homepage benötigt, genügt heute ein Account in einem sozialen Online-Netzwerk, der mit nur wenigen Klicks eingerichtet werden kann.[52]

Die Ausprägungen des Web 2.0 lassen sich in unterschiedliche Angebotsformen (Cyberspace im engeren Sinne), wie z.B. Plattformen wie Wikipedia, die es jedem Nutzer ermöglichen, eigenständig Beiträge zu verfassen, oder aber Blogs, die z.B. als eine Art digitales Tagebuch fungieren können, unterteilen.[53] Schwerpunkt der vorliegenden Arbeit ist der personale verdeckte Ermittler, der vorranging – anders als technische Ermittlungsmethoden – dann zum Einsatz kommt, wenn mit der Zielperson in eine Kommunikationsbeziehung getreten werden soll. Daher kann der Cyberspace an dieser Stelle auf die Erscheinungsformen des Web 2.0 eingegrenzt werden, die den Aufbau einer Kommunikationsbeziehung zwischen Personen ermöglichen. Dies sind im Kern Chatforen und soziale Netzwerke, wie z.B. Facebook oder LinkedIn, u.U. aber auch Content-Communities, wie z.B. Instagram.

3. Der Cyberspace als eigene Welt?

„Einst lebten wir auf dem Land, dann in den Städten, und von jetzt an im Netz“[54]. Dieses Zitat aus dem Film „The Social Network“ von *David Fincher* suggeriert, dass das Netz bzw. der Cyberspace einen von realen Lebensorten zu unterscheidenden Lebensraum darstellt. Das Leben hat sich von der realen Stadt in das virtuelle Netz verlagert. Im folgenden Abschnitt soll der Frage nachgegangen werden, ob die reale Welt und der Cyberspace

[50] *Henrichs/Wilhelm*, Polizeiliche Ermittlungen in sozialen Netzwerken, Kriminalistik 2010, 30.
[51] Vgl. *Schmidt/Pruß*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, § 3 Rn. 121; *Gounalakis*, in: Götting/Schertz/Seitz, Handbuch Persönlichkeitsrecht, § 24 Rn. 12.
[52] Vgl. BT-Drs. 16/11570, S. 420.
[53] Vgl. *Henrichs/Wilhelm*, Polizeiliche Ermittlungen in sozialen Netzwerken, Kriminalistik 2010, 30.
[54] Aus dem Film „The Social Network“ von *David Fincher* aus dem Jahr 2010.

tatsächlich zwei voneinander zu unterscheidende Räume mit jeweils unterschiedlichen Dynamiken sind. Diese Einordnung ist notwendig, um im späteren Verlauf der Analyse darüber entscheiden zu können, ob die Rechtsgrundlagen, die sich originär auf Sachverhalte in der realen Welt beziehen, auch auf den Cyberspace angewendet werden können.

Castells, der sich in Band 1 seiner Trilogie zum Informationszeitalter mit dem Aufstieg der Netzwerkgesellschaft beschäftigt, trifft zwar keine Aussage zum Cyberspace als solchem, beschäftigt sich jedoch mit virtuellen Gemeinschaften und vergleicht diese mit solchen im realen Leben. Er stellt fest, dass diese auf einer anderen Wirklichkeitsebene existieren. Sie sind „nicht Imitate anderer Lebensformen, sondern haben ihre eigene Dynamik“[55]. Demnach attestiert er dem Cyberspace indirekt von der realen Welt zu unterscheidende Wirkmechanismen, die ihn letzten Endes zu einem eigenen Raum machen, der über spezifische Eigenarten verfügt. Dahingehend lässt sich auch die Aussage *Langes* interpretieren, der den Cyberspace als „fünfte Dimension“[56] bezeichnet. Neben physischen Dimensionen, wie z.B. der Länge und Breite, tritt also eine neue, was impliziert, dass es sich in diesem Zusammenhang um eine von den bereits existierenden zu unterscheidende Dimension handelt, die über eigene Charakteristika verfügt. Mithin würde es sich um Parallelwelten handeln, die folgerichtig auch spezifischen rechtlichen Regelungen unterworfen werden müssten. Diese Sichtweisen verkennen allerdings, dass der Cyberspace nicht losgelöst von der realen Welt existiert, sondern über Schnittmengen zu ihr verfügt, was sich insbesondere an den Auswirkungen der Kommunikation im Cyberspace zeigt. Wirkungen sind hier nicht im virtuellen Raum, sondern mit dem echten, physisch fassbaren, Ich des Kommunikationspartners im realen Leben intendiert.[57] Damit ist fraglich, ob diese „Zwei-Welten-Sichtweise“ in dieser Absolutheit zutreffend ist oder ob es nicht vielmehr einer differenzierteren Betrachtung einzelner Teile des Cyberspace bedarf. Es stellt sich die Frage, ob nicht stattdessen eine Betrachtung des Cyberspace im engeren Sinne zu einem diversifizierteren – und damit genaueren – Ergebnis kommt. Zweifellos ist

[55] *Castells*, Der Aufstieg der Netzwerkgesellschaft, Teil 1, S. 410.
[56] Vgl. *Lange/Böttcher*, Cyber-Sicherheit, S. 9.
[57] Vgl. *Meier*, Kriminologie und Internet: ein ungeklärtes Verhältnis, S. 96.

der Cyberspace im weiten Sinne durch die folgenden Aspekte geprägt: Automatisierbarkeit der Aktivitäten, Flüchtigkeit der Spuren, räumliche Entgrenzung der programmierten Handlungen, Kopierbarkeit der Artefakte und Angreifbarkeit von IT-Systemen.[58] Diese spezifischen Charakteristika sprechen für das Vorliegen einer eigenen Welt. Betrachtet man jedoch den Cyberspace im engeren Sinne, also die durch den Nutzungszweck abgrenzbaren Räume, drängt sich die Notwendigkeit einer Differenzierung auf. Näher betrachtet werden sollen daher, vor dem Hintergrund dieser Arbeit, soziale Online-Beziehungen. *Von Kardorff* stellt in diesem Zusammenhang fest,

> *„dass soziale Beziehungen im Netz eine neuartige Option für zusätzliche und hoch selektive – individuell spezifiziert adressierte – Kommunikationen darstellen und darüber hinaus viele virtuell geknüpfte und gepflegte Netzbeziehungen in bestehende soziale Netze von Nachbarschaften, Freunden, Vereinsmitgliedern usw. eingebunden sind"[59].*

Damit wird auf die enge Verknüpfung der realen mit der virtuellen Welt im Rahmen sozialer Beziehungen Bezug genommen, die evidenterweise vorliegt. Im Hinblick auf diesen Aspekt greift eine „Zwei-Welten-Theorie" daher nicht. *Brenneisen/Staack* nehmen sogar eine „Spiegelbildlichkeit von realen und virtuellen Kontakten"[60] an und wenden sich damit bezüglich des virtuellen Raumes der sozialen Online-Netzwerke gänzlich von der Annahme zweier Parallelwelten ab.

Die obigen Darstellungen verdeutlichen die Notwendigkeit einer Differenzierung und somit einer Abkehr von einem absoluten Verständnis des Verhältnisses zwischen der realen und der virtuellen Welt. Vielmehr sollten der Cyberspace im engeren Sinne und eine darauf aufbauende Beurteilung Gegenstand der Betrachtung sein. Eine generalisierende Untersuchung des Cyberspace im weiten Sinne, wie sie z.B. *Castells* vornimmt, wird der Diversifizierung dieses Raumes nicht gerecht und verkennt so die Schnittmengen mit der realen Welt, die v.a. durch den Rollenwechsel des Nutzers hin zum „Prosumenten" geprägt sind. Diese Veränderung in der Art und Weise der Nutzung des Cyberspace führt zwangsläufig zu einer Änderung des Verhältnisses zwischen

[58] Vgl. *Brodowski/ Freiling*, Computerkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, S. 26.
[59] *Von Kardorff*, Virtuelle Netzwerke – neue Formen der Kommunikation und Vergesellschaftung, S. 38.
[60] *Brenneisen/Staack*, Die virtuelle Streife in der Welt der Social Media, Kriminalistik 2012, 627, 629.

diesen beiden Räumen, da die Nutzer und deren Kommunikation untereinander, welche vorrangig über soziale Online-Netzwerke stattfindet, eine immer prägendere Rolle spielen. Als „Brücke zwischen den Sphären“ fungiert hier der Sinn und Zweck sozialer Netzwerke, der in der Erweiterung des eigenen Sozialkapitals zu sehen ist.[61] „Soziales Kapital bezeichnet die in soziale Bindungsnetze eingebetteten Ressourcen, die sich für individuelles oder kollektives Handeln nutzen lassen“[62], also den Wert von menschlichen Verbindungen.[63] Damit erfüllen solche Beziehungsgeflechte eine wichtige Funktion im Hinblick auf die Ressourcenausstattung des Individuums. Derartige Ressourcen, die summiert das Sozialkapital darstellen[64], kann das Individuum nicht auf der Grundlage seines eigenen Humankapitals[65] aufbauen, vielmehr benötigt es Beziehungen zu anderen. Im Rahmen der Partizipation an sozialen Online-Netzen wird das Sozialkapital u.a. durch die Teilnahme am Informationsfluss und die Verstärkung gruppenbezogener Identitäten erhöht.[66] Die Auswirkungen einer derartigen Steigerung manifestieren sich jedoch zuvörderst in der realen Welt und führen z.B. zu einer Verbesserung der körperlichen und seelischen Gesundheit oder aber zu einem neuen Arbeitsplatz.[67]

Zusammenfassend ist an dieser Stelle festzuhalten, dass – ausgehend von einer feinmaschigen Betrachtung des Cyberspace – hinsichtlich sozialer Online-Netzwerke von einer Erweiterung der zwischenmenschlichen Beziehungen aus der realen Welt auszugehen ist. Es handelt sich also um keinen Raum mit eigenen Gesetzmäßigkeiten, sondern um einen erweiterten Sozialkontext, in welchem sich der Nutzer grundsätzlich so zeigt, wie er wirklich ist (extended real life- Hypothese[68]).[69] Diese Annahme dürfte umso mehr hinsichtlich beruflicher Netzwerke wie LinkedIn gelten, da der Nutzungszweck hier in der Regel ein beruflicher ist und somit die Anbindung an das reale Leben noch größer ist

[61] Vgl. BT-Drs. 16/11570, S. 420.
[62] *Endruweit/Trommsdorff/Burzan*, Wörterbuch der Soziologie, S. 213.
[63] Vgl. *Kneidinger*, Facebook und Co., S. 25.
[64] Vgl. *Fuchs-Heinritz u.a.*, Lexikon zur Soziologie, S. 332.
[65] Das Humankapital bezieht sich auf die individuellen Fähigkeiten und Fertigkeiten eines Menschen, die er aus sich heraus entwickeln kann (vgl. *Endruweit/Trommsdorff/Burzan*, Wörterbuch der Soziologie, S. 212).
[66] Vgl. *Kneidinger*, Facebook und Co., S. 30; BT-Drs. 16/11570, S. 420.
[67] Vgl. *Kneidinger*, Facebook und Co., S. 32.
[68] Zu unterscheiden ist diese Hypothese von der sog. „idealized vitual identity“-Hypothese, der die Annahme zu Grunde liegt, dass soziale Netzwerke nur wenig über die Persönlichkeit des Nutzers aussagen, da dieser nur ein geschöntes bzw. optimiertes Bild seiner Selbst präsentiert (vgl. *Stopfer/Back/Egloff*, Persönlichkeit 2.0, DuD 2010, 459, 460).
[69] Vgl. *Stopfer/Back/Egloff*, Persönlichkeit 2.0, DuD 2010, 459, 460.

als z.B. bei Facebook, welches primär im Rahmen der Führung von privaten sozialen Kontakten verwendet wird.

II. Soziale Online-Netzwerke als Cyberspace im engeren Sinne

Anknüpfend an die obigen Ausführungen sollen nunmehr soziale Netzwerke als ein virtueller Raum im Cyberspace betrachtet werden, in dem das Individuum und dessen Kommunikation in besonderem Maße im Vordergrund stehen. Dazu soll zunächst der Begriff „soziales Netzwerk“ definiert werden.

1. Definition „soziales Netzwerk“

Der Begriff „Netzwerk“ ist unterschiedlichen Definitionen zugänglich; ein wichtiger Terminus ist er z.B. sowohl in der Soziologie als auch in der Informatik. Ein Netzwerk im Sinne der soziologischen Netzwerkanalyse ist ein Graph, der über eine bestimmte Anzahl von Knoten verfügt, die über Kanten miteinander verbunden sind und so einen Graph bilden.[70] Betrachtet man ein *soziales* Netzwerk, stehen die Knoten für die jeweiligen personalen Akteure und die Kanten für die Beziehungen dieser zueinander.[71] Derartige Netzwerke lassen sich nunmehr auch im Cyberspace finden. Soziale Online-Netzwerke stellen somit einen jeweils eigenen Cyberspace im engeren Sinne dar.

Erstmals gesetzlich definiert wurden soziale Netzwerke in Deutschland im NetzDG. Gemäß § 1 Abs. 1 S. 1 NetzDG sind soziale Netzwerke Telemediendienstanbieter, die mit Gewinnerzielungsabsicht Plattformen im Internet betreiben, die dazu bestimmt sind, dass Nutzer beliebige Inhalte mit anderen Nutzern teilen oder der Öffentlichkeit zugänglich machen. Daraus lässt sich zusammenfassend ableiten, dass solche Online-Netzwerke als Telemediendienstanbieter mit Gewinnerzielungsabsicht fungieren, die eine Plattform für das Entstehen von Verbindungsstellen zwischen einzelnen Nutzern, die sich jeweils mit eigenen Profilen darstellen können, zur Verfügung stellen.[72] Die Nutzer derartiger Netzwerke kennen sich überwiegend auch aus dem realen Raum. Um die Funktionalitäten eines sozialen Online-Netzwerks zu veranschaulichen, soll im Folgenden LinkedIn vorgestellt und auch im weiteren Verlauf dieser Arbeit als Beispiel herangezogen werden.[73]

---

[70] Vgl. *Trappmann/Hummell/Sodeur*, Strukturanalyse sozialer Netzwerke, S. 17.
[71] Vgl. *Fuchs-Heinritz u.a.*, Lexikon zur Soziologie, S. 469.
[72] Vgl. *Uphues*, in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Teil 15.3, A, I, Rn.13.
[73] Die Ausführungen hinsichtlich LinkedIns können jedoch in weiten Teilen auch auf andere soziale Netzwerke, wie z.B. Facebook, übertragen werden.

2. Vorstellung von LinkedIn und dessen Funktionalitäten

LinkedIn[74] ist eine Kommunikationsplattform, die auf die berufliche Vernetzung von Personen spezialisiert ist. Anders als Xing beschränkt sich LinkedIn jedoch nicht auf den nationalen Bereich, sondern wird weltweit genutzt. Damit ist LinkedIn eine Art Facebook für Erwachsene, die soziale Online-Netzwerke auch für ihr berufliches Fortkommen nutzen wollen. So werden z.B. Stellenanzeigen veröffentlicht, die es Nutzern dieser Plattform ermöglichen, sich beruflich zu verändern. Gleichzeitig wird LinkedIn aber auch andersherum durch Headhunter genutzt, die durch eine direkte Ansprache potenzieller Bewerber neue Mitarbeiter für ein Unternehmen rekrutieren. Eine Überprüfung der Identität der Nutzer durch LinkedIn erfolgt grundsätzlich nicht.[75]

Als Hauptzweck LinkedIns fungiert jedoch die Netzwerkbildung. Über die Suchfunktion kann gezielt nach bestimmten Personen gesucht werden. Angemeldete Nutzer können sich anschließend mit diesen, nach deren Einverständnis, vernetzen. Zudem unterbreitet LinkedIn seinen Nutzern auch proaktiv Vorschläge für Personen, zu denen u.U. ein Kennverhältnis bestehen könnte.

a) Erstellung eines eigenen Profils

Die Grundfunktion LinkedIns, die für eine Vernetzung unerlässlich ist, ist zunächst die Profilerstellung. Es müssen ein Vor- und Zuname angegeben werden, wobei beide Namen nicht dem jeweiligen Klarnamen entsprechen müssen. Im Rahmen der Anmeldung genügt die Verwendung einer gültigen E-Mail-Adresse. Eine darüber hinausgehende Verifizierung der Identität des Nutzers findet nicht statt. Eine E-Mail-Adresse kann jedoch vergleichsweise einfach eingerichtet werden. So müssen zwar theoretisch im Rahmen der Anmeldung bei einem E-Mail-Anbieter Daten wie der Klarname und die Adresse an-

[74] Vgl. https://www.linkedin.com/ (abgerufen am: 18.01.2020).

[75] Anders stellt sich die Situation nur dar, wenn der Nutzer nicht mehr in der Lage ist, sein Passwort eigenständig wiederherzustellen oder aber keinen Zugriff mehr auf die bei LinkedIn hinterlegte E-Mail-Adresse hat. In diesen Fällen ist eine Verifizierung der Identität des Nutzers über einen behördlichen Ausweis, wie etwa einen Führerschein, einen Personalausweis oder aber einen Reisepass möglich. Über eine durch LinkedIn genutzte Technik wird ein verschlüsselter Scan des Dokuments erstellt und sodann an LinkedIn übermittelt (vgl. https://www.linkedin.com/help/linkedin/answer/2148, abgerufen am: 18.01.2020). Diese Funktion führt zu einer „Nutzer-Gemengelage“ von einer Mehrzahl von Nutzern, deren Identität nicht verifiziert wurde und einer kleineren Menge, bei denen eine Identitätsprüfung durch LinkedIn vorgenommen wurde. Für die Nutzer von LinkedIn ist eine solch erfolgte Verifizierung ihres Gegenübers jedoch nicht erkennbar.

gegeben werden, in der praktischen Umsetzung bedeutet dies jedoch keineswegs, dass die Angaben wahrheitsgemäß erfolgen müssen. Gleiches gilt für die verpflichtende Angabe einer anderen E-Mail-Adresse oder einer Telefonnummer, die im Falle einer Passwortwiederherstellung herangezogen werden sollen. Auch hier findet keine weitere Nachprüfung seitens des Anbieters statt, sodass eine E-Mail-Adresse auf der ausschließlichen Grundlage von Falschangaben eingerichtet werden kann.

Da es sich bei LinkedIn um ein berufliches Netzwerk handelt, können sodann Angaben über den schulischen bzw. universitären Werdegang und zur Berufserfahrung gemacht werden. Dabei steht es den Nutzern frei, ihre jeweiligen Stationen in einem der Freitextfelder genauer zu beschreiben, um so ihr Profil um weitere Daten anzureichern. Darüber hinaus können Angaben zu spezifischen Kenntnissen gemacht werden, die dann durch das Netzwerk bewertet werden können. Mithilfe dieser Informationen erstellt LinkedIn daraufhin u.a. den personalisierten Newsfeed eines jeden Nutzers.

Die Grundeinstellung eines jeden LinkedIn-Profils weist zunächst die vollständige Öffentlichkeit des Profils auf. Unter dem Menüpunkt „Datenschutz“ kann sodann die Sichtbarkeit weiter eingeschränkt werden (Opt-Out-Verfahren), sodass z.B. einzelne Teile des Profils der Wahrnehmung der gesamten Cyberspace- oder Netzwerköffentlichkeit entzogen werden können. In der Folge sind diese z.B. nur für Mitglieder des eigenen Kontaktnetzwerks sichtbar.

Diese Ausführungen verdeutlichen, dass LinkedIn ein diversifiziertes Konzept hinsichtlich der Gestaltung der Privatsphäre der Nutzer vorsieht. Grundsätzlich kann also unterschieden werden zwischen der **(Cyberspace)Öffentlichkeit**, der **Netzwerköffentlichkeit** und der durch den Nutzer weiter **beschränkten Netzwerköffentlichkeit**.

b) Kommunikation

LinkedIn bietet in der kostenfreien Version die Gelegenheit, Mitglieder des eigenen Netzwerks direkt anzuschreiben. Dies kann über reine Textnachrichten geschehen, es besteht jedoch auch die Möglichkeit, Bilder und Dateien zu übermitteln. Eine weitere Art der Kommunikation bildet die Verwendung von „Like-Buttons“, mithilfe derer das Gefallen bestimmter Inhalte zum Ausdruck gebracht werden kann. Bezieht sich dieses „Liken“ z.B. auf eine Institution als

Ganze, wie z.B. eine bestimmte Universität oder ein Unternehmen, kann dieser gefolgt werden. Sodann erscheint diese unter „Interessen“ im Profil des Nutzers.

Außerdem bietet LinkedIn die Möglichkeit, einen Beitrag auf einer Art eigener virtueller Pinnwand zu erstellen, der dann auf LinkedIn veröffentlicht wird. Die Sichtbarkeit kann auch hier wieder individuell eingestellt werden, sodass der Beitrag z.B. nur von den eigenen Kontakten angesehen werden kann.

c) Suche

Wie beinahe jedes andere soziale Netzwerk auch, bietet LinkedIn die Möglichkeit einer Suche an. Es kann in unterschiedlichen Kategorien, wie z.B. „Personen“ oder „Unternehmen“ gesucht werden. Zudem besteht die Möglichkeit einer Hashtag-Suche (#). Wird nach einer Person gesucht, richtet sich die Reihenfolge der angezeigten Suchergebnisse nach dem Grad der jeweiligen Vernetzung.

III. Chatforen als Cyberspace im engeren Sinne

Ein Einsatz verdeckter personaler Ermittler kommt neben dem in sozialen Online-Netzwerken auch im Kontext von Chatforen in Frage. Festzuhalten ist zunächst, dass sich die Rahmenbedingungen dieser Kommunikationsumgebungen sehr verändert haben. War die Verwendung klassischer Chatrooms über Dienste wie AOL vor ca. 20 Jahren noch eine verbreitete Art und Weise, um weitestgehend anonym in themenspezifischen Foren andere Nutzer kennenzulernen, existieren derartige Chatforen heute nur noch partiell.[76] Stattdessen finden sich Chatforen als Unterfunktionen in sog. „Gaming-Plattformen“ oder aber in der Gestalt sog. „Image- oder Messageboards“[77]. Im Folgenden werden daher zunächst kurz klassische Chatforen und im Anschluss die relevanteren neuen Formen dargestellt.

[76] Als Beispiel sei an dieser Stelle der Chatanbieter Chatcity genannt (https://www.chatcity.de/), der es den Nutzern nach einmaliger Registrierung erlaubt in sog. Channels miteinander in Kontakt zu treten. Zu AOL vgl. *Ratgeber im Web*, AOL Chat – Gibt es ihn noch zum Chatten?.

[77] Diese können mitunter auch über den sog. „Tor-Browser“ aufgerufen werden. Mit diesem ist es möglich ins Darknet zu gelangen. Tor soll über diverse Verschlüsselungsmechanismen ein anonymes Surfen ermöglichen (vgl. *Kant*, Surfen mit dem TOR-Browser: So kommt man ins Darknet). *Zöller* vergleicht den Cyberspace in diesem Zusammenhang mit einem Ozean. An der Wasseroberfläche tummelten sich die frei zugänglichen Webseiten. Darunter folge das sog. „Deep Web“, das u.a. durch Passwörter und Codes vor einem unbefugten Zugriff geschützt sei. Auf dem Grund des Ozeans befinde sich schließlich das Darknet, das nur mithilfe spezieller Software erschlossen werden könne (vgl. *Zöller*, Strafbarkeit und Strafverfolgung des Betreibens internetbasierter Handelsplattformen für illegale Waren und Dienstleistungen, KriPoZ 2019, 274, 275).

1. Klassische Chatforen

Unter einem Chatforum bzw. Chatroom (auf Deutsch in etwa: Gesprächsraum) wird ein Cyberspace im engeren Sinne verstanden, also ein virtueller Raum, in dem die Teilnehmer mittels eines Chat-Clients direkt miteinander kommunizieren können.[78] Die Räume unterliegen in den meisten Fällen thematischen Einschränkungen, sodass die Nutzer ihren Vorlieben entsprechend zwischen unterschiedlichen Räumen wählen können. Ein Chat-Client stellt in diesem Zusammenhang die technische bzw. infrastrukturelle Grundlage für einen Chatroom dar.[79]

Wie der Name schon vermuten lässt, steht in einem Chatroom die wechselseitige Kommunikation im Vordergrund. Im Unterschied zur Nachrichtenfunktion in sozialen Online-Netzwerken wie LinkedIn, erfolgt diese jedoch in der Regel nicht zwischen zwei bekannten Personen, sondern zwischen Chatteilnehmern, bei denen kein gegenseitiges Kennverhältnis im realen Leben vorliegt. Somit besteht die Hauptfunktion von Chatrooms auch darin, völlig unbekannte Personen kennenzulernen. Daher ist die Anbindung derartiger Chatrooms an das reale Leben als wesentlich schwächer zu beurteilen als in sozialen Online-Netzwerken, die in der Regel ein virtuelles Spiegelbild der tatsächlichen Kontakte darstellen.

Vor der Nutzung eines Chatforums ist eine Registrierung erforderlich. In den meisten Fällen muss in diesem Zusammenhang mindestens die E-Mail-Adresse angegeben werden.[80] Darüber hinaus ist es notwendig, sich einen sog. Nickname zu geben. Dieser zeichnet sich gerade dadurch aus, dass er keinerlei Bezug zur Klaridentität des Nutzers aufweisen muss, also frei erfunden werden kann. Manche Chatforen verlangen darüber hinaus noch weitere Angaben, wie z.B. das Geburtsdatum. Eine Überprüfung der Echtheit der Angaben, die an die Klaridentität des Nutzers anknüpfen, findet nicht statt.

[78] Vgl. *Rüegger/Nägeli*, Chatrooms: Ein Tummelplatz für pädosexuelle Straftäter, Kriminalistik 2006, 404, 405.
[79] Vgl. ebd.
[80] Bezüglich näherer Erläuterungen hinsichtlich der verhältnismäßig einfachen Beschaffung einer E-Mail-Adresse wird auf Abschnitt C, II, 2, a) dieser Arbeit verwiesen.

2. Neue Erscheinungsformen

a) Gaming-Plattformen

Hinter diesem Cyberspace im engeren Sinne verbergen sich Plattformen, die es den Nutzern erlauben, per Live-Stream anderen Spielern zuzuschauen und dabei mit anderen Zuschauern zu chatten. Der einzelne Spieler erhält so die Möglichkeit, Inhalte schnell und kostengünstig einer breiteren Öffentlichkeit zugänglich zu machen – notwendig sind allein ein Mikrofon/ Headset und eine Webcam.[81] Derartige Plattformen gehören nunmehr zu den „relevantesten Medienformen des Internets“[82]. Bekannte Gaming-Plattformen sind z.B. *Twitch*[83] oder *Steam*[84].

Für eine Registrierung sind zumeist einzig ein Nutzername und eine gültige E-Mail-Adresse notwendig, was den Nutzern Anonymität gewährt. Gleichwohl besteht die Möglichkeit der Rückverfolgbarkeit über die verwendete IP-Adresse, es sei denn, der Nutzer verwendet z.B. den Browser Tor.

b) Image- und Messageboards

Unter „Boards“ versteht man durch den Nutzer selbst erstellte Foren. „Image“ und „Message“ umschreiben in diesem Zusammenhang jeweils die vorrangig ausgetauschten Inhalte. Als recht bekanntes Imageboard fungiert der Anbieter 8kun[85]. In seinen FAQ führt 8kun explizit aus, dass zur Erstellung eines eigenen Beitrags in einem bereits bestehenden Image weder ein Name noch eine E-Mail-Adresse erforderlich seien, eigene Imageboards könnten anonym ohne

---

[81] Vgl. *Bodensiek/Walker*, Livestreams von Gaming Video Content als Rundfunk?, MMR 2018,136.

[82] *Ebd.*

[83] https://www.twitch.tv/. Auf dieser Plattform übertrug der Täter des Anschlags in Halle am 09. Oktober 2019 live per Stream seine Taten. Der Stream war noch Stunden nach dem Anschlag auf Twitch abrufbar (vgl. *Köver*, „Wir müssen das als internationalen Terrorismus begreifen“).

[84] https://steamcommunity.com/. Traurige Bekanntheit erlangte Steam u.a. anlässlich des Amoklaufs in München vom 22. Juli 2016. Im Nachgang wurde festgestellt, dass sich der Attentäter intensiv mit William Atchison ausgetauscht hatte, der im Dezember 2017 ein Attentat auf eine Schule in New Mexico verübt hat. Zudem war der Täter Mitglied in einem Forum namens „Anti-Refugee-Club“, das sich auf einer Gaming-Plattform befand. In diesem Forum tauschte er sich mit Gleichgesinnten u.a. über mögliche Amokläufe und Attentate und extremistische Inhalte aus (vgl. *Hartleb*, Neue virtuelle Dimension im Fall des Anschlags von München am 22. Juli 2016, Kriminalistik 2018, 532). Über Steam kam der Täter darüber hinaus mit anderen Gruppen (u.a. Tim Kretschmer Memorial“, „AmokZ“) in Kontakt, die sich mit Amokläufen beschäftigten und in denen die Nutzer ihre Bewunderung für Amokläufer zum Ausdruck brachten (vgl. *Bannenberg*, Die Amoktat des David (Ali) Sonboly, Kriminalistik 2018, 419, 429).

[85] Bis November 2019 firmierte 8kun unter dem Namen 8chan und wurde zeitweise aus dem Cyberspace genommen, nachdem im Unterforum „/pol/“ (Kurzform für „politically incorrect“) allein im Jahr 2019 drei dem Rechtsextremismus zuzuordnende Anschläge angekündigt wurden (vgl. *Laufer*, Das Imageboard hat die falschen Freunde). Darunter fällt u.a. der am 15. März 2019 in Christchurch/Neuseeland durchgeführte Anschlag bei dem 51 Menschen in einer Moschee starben und 49 weitere verletzt wurden. Darüber hinaus liegen auch Hinweise darauf vor, dass der Täter des Anschlags in Halle auf 8kun aktiv war (vgl. *Laufer*, Wie 8chan unter neuem Namen zurückkehren soll).

Namen zu jedem beliebigen Thema erstellt werden.[86] Damit ermöglicht dieser Anbieter eine vollkommen anonyme Kommunikation zwischen den Nutzern ohne eine vorherige Registrierung. Für eine mögliche Rückverfolgbarkeit der User gelten entsprechend die Ausführungen im Abschnitt zuvor.

D. Darstellung unterschiedlicher Einsatzszenarien und ihre Grundrechtsrelevanz

Vor dem Hintergrund der zuvor durchgeführten dogmatischen Untersuchung des Cyberspace wird im Folgenden, zur Prüfung der rechtlichen Anforderungen, das verdeckte personale Handeln der Polizei in sozialen Online-Netzwerken und Chatforen auf seine Grundrechtsrelevanz hin untersucht. Im Rahmen dieses Gliederungspunktes wird zudem u.a. die Frage näher beleuchtet, ob für die jeweiligen Szenarien im Cyberspace die gleichen Rechtsgrundlagen und Maßstäbe wie in der realen Welt, wie z.B. die Abgrenzungskriterien zwischen einem verdeckten Ermittler und einem noeP, Anwendung finden können. In diesem Zusammenhang werden darauffolgend auch die Entwürfe einer speziellen Rechtsgrundlage für verdeckte Ermittler im Cyberspace von *Ihwas*[87] und *Bauer*[88] näher analysiert.

Darüber hinaus wird, als weiteres Szenario einer aktuellen Entwicklung im Bereich der verdeckten personalen Ermittlungen, der Entwurf eines möglichen § 163 g StPO beleuchtet, der aus dem Referentenentwurf zum IT-SiG 2.0 hervorgeht. Laut diesem soll der Verdächtige einer Straftat in bestimmten Fällen dazu verpflichtet werden, die zur Nutzung der virtuellen Identität erforderlichen Zugangsdaten herauszugeben.

I. Grundrechtsbindung der Polizeibehörden im Cyberspace

Bevor eine Bewertung der Grundrechtsrelevanz des jeweiligen polizeilichen Handelns erfolgen kann, ist zunächst grundsätzlich zu begutachten, ob die Polizeibehörden, als staatliche Stellen, der Grundrechtsbindung im Cyberspace unterliegen. Das GG gilt, gemäß S. 3 seiner Präambel, für das gesamte deutsche Volk. Im Hinblick auf die Grundrechte statuiert das GG in Art. 1 Abs. 3

[86] Vgl. https://8kun.top/faq.html (abgerufen am: 18.01.2020).
[87] Vgl. *Ihwas*, Strafverfolgung in sozialen Netzwerken, S. 172.
[88] Vgl. *Bauer*, Soziale Netzwerke und strafprozessuale Ermittlungen, S. 213.

eine Bindung von Gesetzgebung, vollziehender Gewalt und Rechtsprechung an die nachfolgenden Grundrechte. Der Wortlaut der Norm spricht also für eine grundsätzliche Bindung der deutschen Exekutive an die Grundrechte. Damit ließe sich vertreten, dass sich diese Bindung z.B. auch auf polizeiliches Handeln im Ausland bezieht.[89] Somit ist staatliches Handeln im Ausland grundsätzlich nur „unter dem Dach der Grundrechte“[90] möglich.[91] Damit geht einher, dass z.B. auch Ausländer im Ausland als Grundrechtsberechtigte zu sehen sind. Gleichwohl ist aufgrund völkerrechtlicher Erwägungen, wie z.B. dem Souveränitätsprinzip bzw. dem Nichteinmischungsgrundsatz, auch aufgrund praktischer Erwägungen, wie z.B. fehlenden Einwirkungsmöglichkeiten deutscher staatlicher Stellen auf Vorgänge im Ausland, die Intensität des Grundrechtsschutzes im Ausland im Verhältnis zum Grundrechtsschutz in Deutschland abgestuft.[92] Mithin knüpft die Intensität der Bindungswirkung der Grundrechte an die faktischen oder völkerrechtlichen Gestaltungsmöglichkeiten der Bundesrepublik Deutschland.[93]

Der Cyberspace zeichnet sich durch eine räumliche Entgrenzung aus. Damit einhergehend kann das örtliche Wirken der Polizeibeamten bei einem Tätigwerden im virtuellen Raum nicht genau spezifiziert werden. Gleichwohl kann der Cyberspace nicht als staatsfreier Raum gesehen werden.[94] Anknüpfend an die obigen Darstellungen unterliegen die Polizeibehörden – wenn dies schon im Ausland der Fall ist – im Cyberspace erst recht einer Grundrechtsbindung. Die virtuelle Struktur des Cyberspace könnte jedoch eine Abstufung hinsichtlich der Intensität des Grundrechtsschutzes, ähnlich wie bei grenzüberschreitenden Sachverhalten, gebieten. Diese ist allerdings dann zu verneinen, wenn das Geschehen der vollen Kontrolle der deutschen Polizeibehörden unterliegt.[95] In solchen Fällen mangelt es gerade wesensimmanent nicht an der

[89] Vgl. u.a. *Jarass*, in: Jarass/Pieroth, GG, Art. 1 GG Rn. 44; *Sachs*, in: Sachs, Grundgesetz, Vor. Art. 1 GG Rn. 19.
[90] *Herdegen*, in: Herzog u.a., Maunz/Dürig, Grundgesetz, Band I, Art. 1 Abs. 3 GG Rn. 71.
[91] Dieser Aspekt ist auch Kern einer aktuellen Verfassungsbeschwerde von Journalisten und Medienvertretern hinsichtlich der Auslandsfernmeldeaufklärung des Bundesnachrichtendienstes. Diese berufen sich auf das Fernmeldegeheimnis nach Art. 10 Abs. 1 GG und die Pressefreiheit nach Art. 5 Abs. 1 S 2 GG, die ihrer Ansicht nach auch für Ausländer im Ausland gelten würden. Das BVerfG hat über die Verfassungsbeschwerde am 14. und 15. Januar 2020 verhandelt. Eine Entscheidung steht zum Zeitpunkt der Fertigstellung dieser Arbeit noch aus (vgl. u.a. *Legal Tribune*, Journalisten gegen den BND).
[92] Vgl. *Herdegen*, in: Herzog u.a., Maunz/Dürig, Grundgesetz, Band I, Art. 1 Abs. 3 GG Rn. 72.
[93] Vgl. ebd.
[94] Vgl. *Hobe*, Cyberspace – der virtuelle Raum, Rn. 10.
[95] Vgl. *Herdegen*, in: Herzog u.a., Maunz/Dürig, Grundgesetz, Band I, Art. 1 Abs. 3 GG Rn. 73.

Möglichkeit der staatlichen Einflussnahme, sodass eine Verkürzung des Grundrechtsschutzes ausscheiden muss. Demnach sind die Polizeibehörden im Rahmen ihres Tätigwerdens voll an die Grundrechte gebunden. Der Beschuldigte kann sich somit – sofern er vom persönlichen Schutzbereich des jeweiligen Grundrechts erfasst ist – auch auf den Schutz durch diese berufen. Aus diesem Grunde sind nunmehr die unterschiedlichen Ermittlungsszenarien, beginnend mit einem solchen in sozialen Online-Netzwerken, auf ihre Grundrechtsrelevanz hin zu begutachten.

II. Soziale Online-Netzwerke

Im Folgenden wird nun ein verdecktes personales Vorgehen in sozialen Online-Netzwerken auf eine mögliche Grundrechtsbetroffenheit hin untersucht.

1. Grundrechtsrelevanz

a) Fernmeldegeheimnis gemäß Art. 10 Abs. 1 GG

Die aus Art. 10 Abs. 1 GG folgenden Rechte gewährleisten „die freie Entfaltung der Persönlichkeit durch einen privaten, vor den Augen der Öffentlichkeit verborgenen Austausch von Nachrichten, Gedanken und Meinungen (Informationen) und wahr[en] damit die Würde des denkenden und freiheitlich handelnden Menschen“[96]. Somit sind die aus Art. 10 Abs. 1 GG folgenden Gewährleistungen als spezielle Teil- bzw. Bereichsausprägungen des allgemeinen Persönlichkeitsrechts und somit auch als lex specialis zu sehen.[97] Ein möglicher Eingriff in Art. 10 Abs. 1 GG ist daher zuvörderst zu prüfen.

aa) Sachlicher Schutzbereich

Der sachliche Schutzbereich des Fernmeldegeheimnisses erfasst die „unkörperliche Übermittlung von Informationen an individualisierte Empfänger mithilfe des Telekommunikationsverkehrs“[98]. Das Fernmeldegeheimnis greift daher nur während der Übermittlung von Informationen. Als zeitlicher Beginn des Grundrechtsschutzes kann mithin auf Seiten des Absenders das Versenden der Nachricht gesehen werden. Sobald der Übermittlungsvorgang abgeschlossen ist, endet auch der sachliche Schutzbereich des Fernmeldegeheimnisses.[99] Von einem derartigen Abschluss wird dann gesprochen, wenn die

[96] BVerfG, Beschluss vom 20. Juni 1984 – 1 BvR 1494/78 –, BVerfGE 67, 157-185, juris Rn. 43.
[97] Vgl. *Jarass*, in: Jarass/Pieroth, GG, Art. 10 GG Rn. 2; *Ogorek*, in Epping/Hillgruber, BeckOK Grundgesetz, Art. 10 GG Rn 1.
[98] BVerfGE 115, 166.
[99] Vgl. *Ogorek*, in: Epping/Hillgruber, BeckOK Grundgesetz, Art. 10 GG Rn. 45.

Nachricht den alleinigen Herrschaftsbereich eines Teilnehmers an der Kommunikation erreicht hat.[100]

Während des Übermittlungsvorgangs werden sowohl die Inhalte der Kommunikation als auch die Kommunikationsbegleitumstände geschützt.[101] Nicht erfasst vom sachlichen Schutzbereich sind hingegen solche Vorgänge, die sich nicht an bestimmte Kommunikationsteilnehmer, sondern an die Allgemeinheit bzw. Öffentlichkeit richten, sodass nicht mehr von einem schon dem Begriff immanenten Fernmelde*geheimnis* gesprochen werden kann. Als Beispiel für derartige Inhalte fungieren z.B. Inhalte des Cyberspace, sofern der Kommunikationsvorgang nicht durch die Verwendung eines Passworts dem Zugriff der Allgemeinheit entzogen ist.[102]

Ein verdeckter personaler Ermittler kann entweder rein passiv das Auftreten eines Nutzers und die durch ihn verfassten Inhalte mitverfolgen oder aber aktiv in eine Kommunikationsbeziehung mit diesem treten. Beide Konstellationen werden im Folgenden getrennt voneinander betrachtet.

bb) Beiträge eines Nutzers auf dessen virtueller Pinnwand in sozialen Online-Netzwerken

Grundrechtsrelevant sind in diesem Kontext nur solche Informationen, die sich nicht an die gesamte Cyberspace-Öffentlichkeit richten. Damit scheiden z.B. die Daten im sozialen Online-Netzwerk LinkedIn aus, die auch nicht-eingeloggten Nutzern von Suchmaschinen zugänglich sind. In diesen Fällen ist schon der sachliche Schutzbereich des Art. 10 Abs. 1 GG nicht eröffnet, da sich derartige Inhalte nicht an bestimmte Nutzer richten.

Aufgrund der Privatsphäre-Einstellungen kann die Sichtbarkeit von Beiträgen jedoch auch aktiv durch den Nutzer beschränkt werden (Opt-Out). In derartigen Fällen ist zunächst zu untersuchen, ob der Kommunikationsvorgang noch andauert oder bereits abgeschlossen ist. Ist Letzteres der Fall, ist der sachliche Schutzbereich des Fernmeldegeheimnisses schon aus diesem Grunde nicht eröffnet.

[100] Vgl. *Ogorek*, in: Epping/Hillgruber, BeckOK Grundgesetz, Art. 10 GG Rn. 46.
[101] Vgl. ebd., Rn. 39.
[102] Vgl. ebd., Rn. 41.

(1) Übermittlungsvorgang

Mit dem Posten bzw. Veröffentlichen eines Beitrags ist der jeweils festgelegte Adressatenkreis prinzipiell in der Lage, von diesem Posting Kenntnis zu erlangen. Grundsätzlich ist der Kommunikationsvorgang in dem Augenblick abgeschlossen, in dem die Information den alleinigen Herrschaftsbereich eines Kommunikationsteilnehmers erreicht hat,[103] sie muss also, simplifiziert gesagt, „angekommen sein". Bei derartigen Beiträgen an eine größere Anzahl von Teilnehmern kann es ausreichend sein, wenn die Information beim jeweiligen Anbieter des Dienstes gespeichert wurde, also die Möglichkeit der Kenntnisnahme besteht.[104] Folgt man dieser Ansicht, ist der Kommunikationsvorgang bereits mit dem Posten des Beitrags, also dessen Erscheinen, abgeschlossen. Ein durch das Fernmeldegeheimnis geschützter Kommunikationsvorgang ist sodann zu verneinen. Nach *Schenke* hat die Kommunikation mit dem Akt des Postens jedoch noch nicht einmal begonnen, da derartige Beiträge lediglich zum Abruf durch die Nutzer freigegeben würden und somit noch nicht den Herrschaftsbereich des Erstellers verlassen hätten.[105] *Eisenmenger* entgegnet diesen Einwänden, dass eine Kenntnisnahme Dritter mit dem Akt des Postens des Beitrags nur noch vom Zufall abhänge und der Ersteller das weitere Geschehen daher zunächst nicht mehr in der Hand habe. Somit könne die daraus resultierende Gefährdungslage mit einer solchen nach Art. 10 GG verglichen werden.[106]

Diese Argumente stützen jedoch lediglich die Annahme des *Beginns* eines Kommunikationsvorgangs, legen also nahe, dass der Beitrag den Herrschaftsbereich des Erstellers mit der Aktion des Postens verlassen hat. Dies überzeugt grundsätzlich, da diese Schlussfolgerung auch durch die Grundsätze des BGB über die Abgabe von Willenserklärungen gestützt wird. Laut diesen ist eine willentliche Entäußerung in Richtung des Empfängers notwendig, eine solche ist im Rahmen elektronischer Kommunikation mit Betätigung des Sendebefehls anzunehmen.[107] Schuldig bleibt *Eisenmenger* indes einer Antwort

[103] Vgl. *Ogorek*, in: Epping/Hillgruber, BeckOK Grundgesetz, Art. 10 GG Rn. 46.
[104] Vgl. *Levin/Schwarz*, Zum polizeirechtlichen Umgang mit sog. Facebook-Partys – „Ab geht die Party und die Party geht ab!"… oder doch nicht?, DVBl 2012, 10, 12.
[105] Vgl. *Schenke*, in: Stern/Becker, Grundrechte-Kommentar, Art. 10 GG Rn. 43.
[106] Vgl. *Eisenmenger*, Die Grundrechtsrelevanz „virtueller Streifenfahrten", S. 199.
[107] Vgl. *Säcker*, in: Säcker u.a., Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 1, Einleitung Rn. 201.

darauf, ob der Kommunikationsvorgang mit Erscheinen des Beitrags im sozialen Netzwerk beendet ist. Sofern *Levin/Schwarz* die Speicherung beim Dienstanbieter als maßgeblich betrachten, kann dem zunächst nicht zugestimmt werden. Die besondere Schutzbedürftigkeit des Übertragungsvorgangs ergibt sich daraus, dass es sich um eine Kommunikation auf Distanz handelt, im Rahmen derer zwingend ein Dritter eingeschaltet werden muss.[108] Aus diesem Gedanken heraus erklärt sich z.B., dass E-Mails so lange durch das Fernmeldegeheimnis geschützt sind, wie sie noch auf dem Server des Providers gespeichert sind.[109] Der Schutz durch Art. 10 Abs. 1 GG kann also nicht allein durch die Speicherung beim jeweiligen Host-Provider beendet werden. Doch wann ist die Übermittlung dann bei Vorliegen derartiger Sachverhalte abgeschlossen? Vom Schutzzweck des Fernmeldegeheimnisses aus argumentiert, kann dies erst dann der Fall sein, wenn die Informationen keinen Zugriffen durch Dritte mehr ausgesetzt sind. Dritter ist in dieser Konstellation klassischerweise der Host-Provider. Derartige Beiträge auf virtuellen Pinnwänden werden jedoch klassischerweise stets auf den Servern des Providers gespeichert, auch wenn diejenigen Nutzer, die gemäß den Einstellungen des Erstellers Kenntnis erlangen sollen, von diesen erfahren haben. Damit würde die Gefährdungslage jedoch faktisch nie enden und eine Übermittlung könnte in derartigen Fällen höchstens durch Löschen des Postings durch den Ersteller selbst beendet werden.[110] Die klassischerweise auf eine E-Mail-Kommunikation anwendbaren Grundsätze können hier also nicht sachgerecht herangezogen werden.

Wird die Natur derartiger Pinnwand-Beiträge betrachtet, sind diese eher als eine einseitige Kundgabe von Informationen durch den Ersteller zu bewerten, insofern wird dadurch in der Regel keine darauffolgende wechselseitige Konversation intendiert. Vielmehr sind diese Postings mit einseitigen, nicht empfangsbedürftigen Willenserklärungen, wie etwa einem Testament, vergleichbar. Im Rahmen solcher Erklärungen wird für deren Wirksamkeit auf den Zeitpunkt der Abgabe abgestellt. Auf einen Zugang beim Empfänger kommt es

[108] Vgl. *Schwabenbauer*, Kommunikationsschutz durch Art. 10 GG, AöR 2012, 1, 14.
[109] Vgl. BVerfG, Beschluss vom 16. Juni 2009 – 2 BvR 902/06 –, BVerfGE 124, 43-77, juris, Rn. 48.
[110] Selbst im Falle eines Löschens von Inhalten kann jedoch nie in Gänze ausgeschlossen werden, dass ein Beitrag nicht doch noch beim Provider vorhanden ist (vgl. auch: *Englerth/Hermstrüwer*, Die Datenkrake als Nutztier der Strafverfolgung, RW 2013, 326, 341).

insofern nicht an. Werden diese Gedanken auf den hier vorliegenden Sachverhalt übertragen, wäre der Übermittlungsvorgang mit der Entäußerung des Beitrags – also mit dem Klick auf das Feld „Posten“ – beendet. Sodann würden Beginn und Ende des Übermittlungsvorgangs durch ein und dieselbe Handlung realisiert werden. Im Ergebnis ist dann also hinsichtlich dieser Sonderkonstellation, die sich aus der *Natur des Beitrags* ergibt, der Auffassung von *Levin/Schwarz* zuzustimmen, die auf den Zeitpunkt des Erscheinens abstellen. Somit ist in den Fällen, in denen ein personaler verdeckter Ermittler passiv Kenntnis von derartigen geposteten Beiträgen erhält, der Kommunikationsvorgang bereits abgeschlossen, sodass schon aus diesem Grund der sachliche Schutzbereich des Fernmeldegeheimnisses nach Art. 10 Abs. 1 GG nicht eröffnet ist.

(2) Teilnehmer am Kommunikationsvorgang

Zur Vervollständigung der Darlegungen zur Grundrechtsrelevanz, soll im Folgenden ergänzend geprüft werden, ob, sofern doch ein noch andauernder Kommunikationsvorgang angenommen würde, dieser durch das Fernmeldegeheimnis geschützt wäre. Entscheidend ist in diesem Zusammenhang zunächst, ob es sich um einen öffentlichen Kommunikationsvorgang handelt oder sich die geposteten Beiträge an individuelle Empfänger richten.[111] Wird dieses Szenario mit dem klassischen Fall der Kommunikation zwischen zwei Teilnehmern, die durch Art. 10 Abs. 1 GG geschützt ist, verglichen, wird hier nicht ein Empfänger individuell und persönlich adressiert. Vielmehr richten sich die Informationen grundsätzlich an die Netzwerköffentlichkeit, die durch den Nutzer noch weiter eingeschränkt werden kann, sodass Beiträge z.B. nur durch diejenigen Mitglieder von LinkedIn gesehen werden, mit denen der Ersteller vernetzt ist. Der Adressatenkreis wäre in der zuletzt genannten Konstellation zumindest mithilfe der Kontaktliste individualisierbar.

Wird die nicht weiter eingeschränkte Netzwerköffentlichkeit adressiert, kann im Prinzip jeder Nutzer Kenntnis von dem jeweils gegenständlichen Beitrag erlangen; es genügt die bloße Anmeldung bei LinkedIn. In solchen Fällen ist

[111] Vgl. *Gusy*, in: Huber/Voßkuhle, Grundgesetz, Band 1, Art. 10 GG Rn. 59.

der Empfängerkreis nicht individualisierbar, sodass ein schutzwürdiges Vertrauen in die Vertraulichkeit des Beitragsinhalts verneint werden kann[112], also eben nicht mehr von einem Fernmelde*geheimnis* gesprochen werden kann.

Etwas anderes ergibt sich hinsichtlich der durch die Privatsphäre-Einstellungen weiter eingeschränkten Netzwerköffentlichkeit. Derartige Inhalte sind gerade nicht prinzipiell jedem zugänglich, sondern erfordern die Überwindung der jeweils getroffenen technischen Vorkehrung. Bezogen auf LinkedIn würde dies die Vernetzung mit dem entsprechenden Nutzer voraussetzen. In derartigen Fällen ist sodann der sachliche Schutzbereich des Fernmeldegeheimnisses eröffnet.[113] Bezüglich solcher Beiträge in sozialen Netzwerken, die auf einer Art virtueller Pinnwand gepostet werden, sind somit die jeweiligen Privatsphäre-Einstellungen entscheidend. Ist auf dieser Grundlage eine Eingrenzung des Empfängerkreises möglich, ist die jeweilige Kommunikation durch das Fernmeldegeheimnis geschützt. Diese Ausführungen lassen erkennen, dass eine pauschale und generalisierende Betrachtung derartiger Inhalte nicht erfolgen kann, vielmehr müssen die Gesamtumstände des konkreten Einzelfalles herangezogen werden.[114]

Würde der personale verdeckte Ermittler, ohne sich aktiv mit dem Nutzer zu vernetzen, Informationen aus einem durch Privatsphäre-Einstellungen beschränkten Bereich erhalten, z.B. über die Nutzung eines technischen Mittels, könnten die obigen Aussagen so stehen bleiben. Anders verhält es sich hingegen, sofern der Nutzer den Ermittler aktiv zu seinem Netzwerk hinzugefügt hat. In derartigen Fällen erhält sodann gerade der Account-Inhaber Kenntnis

---

[112] Vgl. *Oermann/Staben*, Mittelbare Grundrechtseingriffe durch Abschreckung?, Der Staat 2013, 630, 632.

[113] So auch vgl. *Gusy*, in: Huber/Voßkuhle, Grundgesetz, Band 1, Art. 10 GG Rn. 64; *Englerth/Hermstrüwer*, Die Datenkrake als Nutztier der Strafverfolgung, RW 2013, 326, 350.

[114] Gesetzesvergleichend lässt sich eine Befugnis der mitwirkenden Stellen an einer Sicherheitsüberprüfung zur Einsichtnahme in den öffentlich sichtbaren Teil sozialer Netzwerke in § 12 Abs. 3a SÜG finden. Da sich keine Anhaltspunkte für einen unterschiedlichen Bewertungsmaßstab ergeben, müsste „öffentlich sichtbar" im Sinne der Einheit der Rechtsordnung identisch wie in dem dargestellten Ermittlungsszenario eines personalen verdeckten Ermittlers verstanden werden. Der Gesetzesentwurf zum SÜG (BT-Drs. 18/11281) enthält keine Ausführungen, die zur Auslegung dieses Terminus beitragen können. Ferner ist auch die Kommentarliteratur zum SÜG als eher übersichtlich zu beurteilen. Gleichwohl fällt auf, dass *Däubler* im Rahmen seiner Darlegungen „öffentlich sichtbar" deutlich restriktiver definiert. Danach sind bereits solche Seiten nicht mehr öffentlich zugänglich, die nur durch Mitglieder sozialer Netzwerke eingesehen werden können (vgl. *Däubler*, Sicherheitsüberprüfungsgesetz, § 12 SÜG Rn. 33). Da sich die Rechtsprechung zu dieser Norm und deren Auslegung jedoch noch nicht geäußert hat, ist eine diesbezügliche Entwicklung zu verfolgen. U.U. könnten die Darlegungen sodann auch im Hinblick auf verdeckte personale Ermittler im Cyberspace fruchtbar gemacht werden.

von dem geposteten Beitrag, den der Nutzer auch intendiert hat. Das Vertrauen in die Identität des Kommunikationsteilnehmers wird hingegen nicht durch das Fernmeldegeheimnis geschützt.[115] „Art. 10 schützt das Vertrauen in das Medium, nicht in dessen Benutzer."[116] Derartige Offenlegungspflichten bestehen darüber hinaus auch im realen Leben im Rahmen der persönlichen Kommunikation nicht, sodass der Schutz der Telekommunikation an dieser Stelle nicht weiter greifen kann.[117] Demnach ist also auch die passive Kenntnisnahme von durch den Nutzer adressatenmäßig eingeschränkten Inhalten nicht als Eingriff in das Fernmeldegeheimnis zu bewerten, sofern der verdeckt agierende personale Ermittler aktiv durch den Nutzer als Teil dieser beschränkten Netzwerköffentlichkeit akzeptiert wurde.

(3) Zusammenfassung

Zusammenfassend lässt sich also hinsichtlich der durch den Nutzer erstellten Beiträge auf einer Art virtuellen Pinnwand in sozialen Netzwerken, wie z.B. LinkedIn, festhalten, dass die Kernproblematiken in der Bestimmung der zeitlichen Grenzen des Übermittlungsvorgangs und der Individualkommunikation zu sehen sind. Der vorliegenden Arbeit wird die Rechtsauffassung zugrunde gelegt, dass der Übermittlungsvorgang in Bezug auf diesen Einzelfall mit dem Erscheinen des Beitrags in dem sozialen Online-Netzwerk beendet ist. Folglich ist keine durch das Fernmeldegeheimnis zu schützende Übermittlung anzunehmen.

Das Vorliegen des Merkmals der Individualkommunikation hängt entscheidend von der Inanspruchnahme der Privatsphäre-Einstellungen durch den Nutzer ab. Begrenzt er durch diese den Empfängerkreis, ist letzterer zumindest individualisierbar, was als hinreichend zu bewerten ist.

Hinsichtlich des Einsatzes eines personalen verdeckten Ermittlers, der nur Kenntnis von Beiträgen erlangt, weil zuvor eine Vernetzung mit dem Ersteller stattgefunden hat, ist die Schutzrichtung des Fernmeldegeheimnisses von besonderer Relevanz. Geschützt wird insofern ausschließlich das Vertrauen in das Medium, nicht jedoch in die Wahrhaftigkeit der Empfänger in Gestalt der

[115] Vgl. *Gusy*, in: Huber/Voßkuhle, Grundgesetz, Band 1, Art. 10 GG Rn. 70.
[116] Ebd.
[117] Vgl. ebd., Fn. 16.

Netzwerkmitglieder. Somit scheidet in derartigen Ermittlungskonstellationen ein Eingriff in das Fernmeldegeheimnis aus.

cc) Aktive Kommunikation innerhalb des sozialen Online-Netzwerks mit eigenem Account

Neben einer rein passiven Kenntnisnahme der o.g. Inhalte, kommt auch eine aktive Kommunikation des Ermittlers mit dem Nutzer in Betracht. Eine Offenlegung des Ermittlungskontextes erfolgt in derartigen Fällen nicht. In LinkedIn kann z.B. über die Nutzung der Nachrichtenfunktion miteinander kommuniziert werden. Da sich die Nachricht stets auf dem Server des Anbieters befindet, ist der Übermittlungsvorgang noch nicht abgeschlossen. Zudem ist eine individualisierte Kommunikation zweifelsfrei zu bejahen. Dennoch ist dieses Ermittlungsszenario nicht als Eingriff in das Fernmeldegeheimnis zu bewerten. An dieser Stelle kommen die gleichen Überlegungen zum Tragen wie unter Abschnitt bb), (2). Der verdeckte personale Ermittler greift nicht in den Übermittlungsvorgang ein, vielmehr erreicht die Nachricht die durch den Absender intendierte Person. Art. 10 Abs. 1 GG schützt hingegen gerade nicht das Vertrauen in die Identität des Nutzers, sondern in das Kommunikationsmedium.[118]

dd) Einbeziehung durch einen Kommunikationsteilnehmer

Neben der Nutzung eines eigenen Accounts durch den verdeckten personalen Ermittler, kann dieser auch freiwillig durch einen Privaten in den Kommunikationsvorgang mit der Zielperson einbezogen werden. Auch hier kommt grundsätzlich ein Mitlesen von den durch die Zielperson verfassten Beiträgen auf virtuellen Pinnwänden im sozialen Online-Netzwerk oder aber von an den anderen Kommunikationsteilnehmer gerichteten Nachrichten in Betracht. Bezüglich der ersten Var. kann auf Abschnitt D, II, 1 a), bb) verwiesen werden.

Im Rahmen der zweiten Konstellation erreicht die Nachricht den durch den Absender intendierten Nutzer, es liest jedoch noch jemand anderes mit Wissen des Adressaten mit. Der verdeckte personale Ermittler ist also nicht selbst Kommunikationspartner, sondern fungiert hier als Außenstehender. Der Kommunikationsinhalt gelangt also einer dritten Person zur Kenntnis, was durch den Absender nicht bezweckt wurde und ihm darüber hinaus auch unbekannt

[118] Vgl. *Gusy*, in: Huber/Voßkuhle, Grundgesetz, Band 1, Art. 10 GG Rn. 70.

ist. Der sachliche Schutzbereich des Fernmeldegeheimnisses ist somit eröffnet.

Fraglich ist, ob auch ein Eingriff in dieses Grundrecht zu bejahen ist. An dieser Stelle ist zu erörtern, ob ein Kommunikationsteilnehmer auf den Grundrechtsschutz verzichten kann. Dies hätte zur Folge, dass ein Eingriff in das Fernmeldegeheimnis entfällt. Grundsätzlich ist ein derartiger Verzicht möglich; bei Art. 10 Abs. 1 GG handelt es sich also nicht um ein dispositionsloses Grundrecht.[119] Im vorliegenden Fall verzichtet jedoch nur der Empfänger der Nachricht auf seinen Grundrechtsschutz. Entscheidend ist daher, ob ein derartiger Verzicht auch nur durch einen Teilnehmer wirksam erklärt werden kann oder ob vielmehr beide Kommunikationsteilnehmer den Verzicht erklären müssen.

In der älteren Rechtsprechung wurde die Auffassung vertreten, dass die Zustimmung nur eines Teilnehmers ausreichend sei. Begründet wurde dies damit, dass das Fernmeldegeheimnis keine Geltung zwischen den beiden Kommunikationspartnern entfalte.[120] So könne eben auch jeder von ihnen im Anschluss Dritte über den Inhalt der Unterhaltung unterrichten, sodass daraus folge, dass auch ein Verzicht einseitig erklärt werden könne.[121]

Anders entschied das BVerfG in seiner Fangschaltungsentscheidung[122]. Explizit spricht es sich gegen die oben gezogene Schlussfolgerung aus. So folge daraus, dass jeder der Kommunikationsteilnehmer einen Dritten im Anschluss über die Inhalte unterrichten könne, nicht, dass dies auch eine einseitige Möglichkeit eines Grundrechtsverzichts mit Wirkung für den anderen Teilnehmer impliziere.[123] Das Gericht stellt sodann auf den Schutzzweck des Art. 10 Abs. 1 GG ab, der ein Abwehrrecht gegen den Staat sei und somit vor jeder staatlichen Einflussnahme schütze, sofern diese nicht zuvor durch beide Kommunikationsteilnehmer autorisiert wurde.[124] Somit wäre eine Einbeziehung einer

[119] Vgl. *Jarass*, in Jarass/Pieroth, GG, Art. 10 GG Rn. 13.
[120] Vgl. VG Bremen, NJW 1978, 66, 67; *Löwer*, in: Münch von/Kunig, Grundgesetz, Band 1, Art. 10 GG Rn. 7.
[121] Vgl. *Durner*, in: Herzog u.a., Maunz/Dürig, Grundgesetz, Band II, Art. 10 GG Rn. 127.
[122] BVerfG, Beschluss vom 25. März 1992 – 1 BvR 1430/88 –, BVerfGE 85, 386-405, juris.
[123] Vgl. BVerfG, Beschluss vom 25. März 1992 – 1 BvR 1430/88 –, BVerfGE 85, 386-405, juris, Rn. 55.
[124] Vgl. ebd.

staatlichen Stelle stets als Grundrechtseingriff zu beurteilen, sofern diese Einbeziehung nicht mit dem kumulativen Einverständnis aller an der Kommunikation beteiligten Personen erfolgt.[125]

Neue Aspekte zu dieser Problematik ergeben sich hingegen aus der Entscheidung des BVerfG zur Online-Durchsuchung.[126] Das Gericht stellt explizit auf den Schutzzweck des Art. 10 Abs. 1 GG ab und zieht daraus Schlussfolgerungen für die Zuweisung der Befugnis zur Erteilung eines wirksamen Einverständnisses. Einmal mehr betont es, dass das Fernmeldegeheimnis eben nicht das Vertrauen in die Teilnehmer an der Kommunikation schütze, sodass in denjenigen Fällen, in denen die Enttäuschung des Vertrauens in die Person des Gegenübers im Vordergrund stehe und nicht ein unautorisierter Zugriff auf den Kommunikationsvorgang, kein Eingriff in Art. 10 Abs. 1 GG vorliege.[127] Das BVerfG stellt nunmehr auf den Schwerpunkt der staatlichen Maßnahme, also die Gefährdungslage, ab.[128] Ist diese **kommunikationsbezogen**[129], liegt ein Grundrechtseingriff vor und ein Verzicht kann nur durch **alle Teilnehmer kumulativ** wirksam erklärt werden. Ergibt sich die Gefährdungslage hingegen aus einem enttäuschten **Vertrauen in die Integrität des Kommunikationsteilnehmers**, knüpft die Gefährdung nicht an den Kommunikationsvorgang als solchen an. Daher ist ein Grundrechtseingriff in diesen Fällen nur anzunehmen, wenn die staatliche Stelle nicht durch mindestens **einen Teilnehmer** autorisiert wurde.[130] Zurecht weist *Durner* jedoch darauf hin, dass einer Unterscheidung anhand der Gefährdungslage eine gewisse Unschärfe innewohne.[131] So ist das Endergebnis – eine staatliche Stelle erhält Informationen aus einem Kommunikationsvorgang – letztlich sowohl im Rahmen der Nutzung einer Fangschaltung als auch durch ein Mitlesen einer staatlichen Stelle das Gleiche, einzig der Weg ist ein anderer. So kommt eine Fangschaltung während des Übertragungsvorgangs zum Einsatz, wohingegen das Mitlesen am Ende des Vorgangs im Verantwortungsbereich des Empfängers erfolgt. Die

[125] Vgl. *Durner*, in: Herzog u.a., Maunz/Dürig, Grundgesetz, Band II, Art. 10 GG Rn. 127.
[126] BVerfG, NJW 2008, 822.
[127] Vgl. ebd., 835.
[128] Vgl. *Durner*, in: Herzog u.a., Maunz/Dürig, Grundgesetz, Band II, Art. 10 GG Rn. 129.
[129] Eine solche Kommunikationsbezogenheit wird z.B. angenommen, wenn ein staatlicher Akteur einen gegen die Kenntnisnahme Dritter geschützten Kommunikationsvorgang mithilfe eines Zugangsschlüssels überwacht, der ihm nicht durch die Kommunikationsteilnehmer überlassen wurde (vgl. BVerfG, NJW 2008, 822).
[130] Vgl. BVerfG, NJW 2008, 822, 835.
[131] Vgl. *Durner*, in: Herzog u.a., Maunz/Dürig, Grundgesetz, Band II, Art. 10 GG Rn. 129.

Gefahr für die Vertraulichkeit der Information geht daher von der **Person des Empfängers** aus, während eine Fangschaltung nur funktioniert, weil sie eine **Schwachstelle des Kommunikationsvorgangs** ausnutzt. Vor diesem Hintergrund können die Ausführungen des BVerfG überzeugen. Schlussendlich soll der Teilnehmer an einer Fernkommunikation auch nicht besser stehen als im Rahmen einer Kommunikation unter Anwesenden, vielmehr soll er nur vor „den spezifischen Gefahren, denen der Kommunikationsvorgang ausgesetzt ist“[132], geschützt werden. Die o.g. Konstellation verdeutlicht auch das Verhältnis zwischen dem Fernmeldegeheimnis gemäß Art. 10 Abs. 1 GG und dem allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Ersteres fungiert als lex specialis zum letztgenannten Recht, sodass enttäuschtes Vertrauen in die Integrität einer Person tatsächlich kein kommunikationsspezifisches Risiko darstellt und sodann eher im Rahmen einer Prüfung einer möglichen Verletzung des allgemeinen Persönlichkeitsrechts von Relevanz ist.[133]

Darüber hinaus liegt auch kein Widerspruch zwischen der Fangschaltungsentscheidung des BVerfG und derjenigen zur Online-Durchsuchung vor.[134] Würde das BVerfG heute unter Zugrundelegung der Überlegungen zur Gefährdungslage über den erstgenannten Sachverhalt entscheiden, käme es zu dem gleichen Ergebnis und würde erneut einen Eingriff in das Fernmeldegeheimnis bejahen.

Außerdem kann auch der Einwand *Hermes*‘ nicht überzeugen, der insbesondere qualitative Unterschiede zwischen einem direkten Mitlesen bzw. Mithören einer staatlichen Stelle und einer anschließenden Preisgabe des Inhalts durch einen der Kommunikationsteilnehmer im Rahmen einer mittelbaren Informationsweitergabe sieht.[135] Aufgrund des „Stille-Post-Phänomens“ und der subjektiven Wahrnehmung des Gesprächsteilnehmers gingen stets Informationen verloren, sodass ein Qualitätsunterschied vorliege. Somit sei die zweifelsohne nicht in Art. 10 Abs. 1 GG eingreifende Mitteilung des Inhalts im Anschluss an

[132] *Durner*, in: Herzog u.a., Maunz/Dürig, Grundgesetz, Band II, Art. 10 GG Rn. 43.
[133] Vgl. so auch *Durner*, in: Herzog u.a., Maunz/Dürig, Grundgesetz, Band II, Art. 10 GG Rn. 130.
[134] So auch vgl. *Bauer*, Soziale Netzwerke und strafprozessuale Ermittlungen, S. 151.
[135] Vgl. *Hermes*, in: Dreier, Grundgesetz. Band 1, Art. 10 GG Rn. 58.

die Konversation an einen Dritten nicht mit einem direkten Mitlesen bzw. Mithören vergleichbar. Es handle sich schlussendlich daher wohl doch um ein kommunikationsbezogenes Risiko, das sich in derartigen Konstellationen verwirkliche. Diese Interpretation des Sachverhalts ändert jedoch letzten Endes nichts daran, dass durch ein Mitlesen bzw. Mithören eben kein Risiko, das diesem Kommunikationsvorgang innewohnt, ausgenutzt wird. Vielmehr ist das Verhalten des Gesprächsteilnehmers eine conditio sine qua non für einen Informationsgewinn auf Seiten des staatlichen Akteurs. Ebenso verhält es sich bei einer Weitergabe von Kommunikationsinhalten an diesen im Anschluss an die Konversation. Daher können beide Szenarien sehr wohl miteinander verglichen werden, da die Gefährdungslage in beiden Fällen identisch ist und aus dem Verantwortungsbereich des Gesprächspartners resultiert. Letztlich geht es an dieser Stelle im Kern um eine Abgrenzung zwischen dem Fernmeldegeheimnis und dem allgemeinen Persönlichkeitsrecht. Der Umfang des Informationsgewinns einer Ermittlungsmaßnahme ist jedoch kein taugliches Abgrenzungskriterium.[136]

Abschließend lässt sich also festhalten, dass die aktive oder passive Teilhabe des personalen verdeckten Ermittlers an der Nachrichtenfunktion eines sozialen Online-Netzwerkes dann keinen Eingriff in das Fernmeldegeheimnis darstellt, wenn dies mit Einverständnis eines Kommunikationsteilnehmers geschieht. Die Willenserklärung nur eines Teilnehmers ist hinreichend, da in derartigen Fällen keine fernmeldespezifische Gefahr verwirklicht wird.

b) Schutz der Wohnung gemäß Art. 13 GG (virtuelle Wohnung)

Die Inhalte sozialer Online-Netzwerke sind die in vielen Fällen darauf ausgerichtet, die Identität bzw. Persönlichkeit der Nutzer v.a. durch ihre Profilfunktion abzubilden. Daher wird im Folgenden untersucht, ob soziale Online-Netzwerke eine Wohnung für die virtuelle Identität eines Individuums darstellen können und somit durch das Wohnungsgrundrecht nach Art. 13 GG geschützt sind.

Ähnlich wie das Fernmeldegeheimnis nach Art. 10 Abs. 1 GG, stellt auch das Wohnungsgrundrecht aus Art. 13 GG eine spezielle Bereichsausprägung des allgemeinen Persönlichkeitsrechts dar. Der Grundrechtsberechtigte soll einen Rückzugsort erhalten, an dem er seine Persönlichkeit frei entfalten kann, kurz

[136] Vgl. so auch *Bauer*, Soziale Netzwerke und strafprozessuale Ermittlungen, S. 151.

gesagt, einen Ort der räumlichen Privatsphäre[137], der als „Stätte privaten Lebens und Wirkens“[138] fungiert.

Unter einer Wohnung wird „ein […] Raum [verstanden], den der Mensch der allgemeinen Zugänglichkeit entzieht, um sich darin aufzuhalten“[139]. Dies bedeutet, dass Maßnahmen getroffen werden müssen, um das Betreten dieses Raumes durch andere Personen zu verhindern. In der Regel fallen darunter körperliche Begrenzungen, wie etwa Zäune, Mauern oder Türen.[140] Klassischerweise sind also u.a. Häuser, Mietwohnungen, Hotelzimmer oder aber Wohnschiffe bzw. Hausboote als Wohnungen im Sinne des Art. 13 GG zu qualifizieren.[141]

Vor dem Hintergrund der obigen Ausführungen, wird v.a. die Betonung auf die physische Räumlichkeit der Wohnung deutlich. Es handelt sich um Räumlichkeiten in der realen Welt, die durch körperliche und fassbare Vorrichtungen von der Öffentlichkeit abgegrenzt sind. Diese Kriterien erfüllt der virtuelle Raum zweifellos nicht, vielmehr sind Datenverarbeitungen im virtuellen Raum durch eine Virtualisierung geprägt.

Die entscheidende Frage muss mithin sein, ob diese Eigenschaften zwingend sind oder aber der Wohnungsbegriff auch in einem weiteren Sinne verstanden werden kann. Wie in Abschnitt C geschildert, sind soziale Online-Netzwerke, als eine Ausprägung des Web 2.0 und als Sinnbild der Veränderung des Nutzers hin zum „Prosumenten“, nicht als eine von der realen Welt losgelöste eigenständige Welt zu sehen, sondern als erweiterter Sozialkontext, der mithin dem weiteren Ausbau zwischenmenschlicher Beziehungen dient und daher keinen eigenen Gesetzmäßigkeiten unterliegt. Wird diese Verschmelzung der realen Welt mit sozialen Online-Netzwerken zugrunde gelegt, kann ein Schutz durch das Wohnungsgrundrecht nach Art. 13 GG nicht von vornherein mit Ver-

[137] Vgl. *Gornig*, in: Huber/Voßkuhle, Grundgesetz, Band 1, Art. 13 GG Rn. 1; *Stern*, in: Stern/Becker, Grundrechte-Kommentar, Art. 13 GG Rn. 22.
[138] *Jarass*, in: Jarass/Pieroth, GG, Art. 13 GG Rn. 4.
[139] *Gornig*, in: Huber/Voßkuhle, Grundgesetz, Band 1, Art. 13 GG Rn. 13.
[140] Vgl. ebd., Rn. 15.
[141] Vgl. *Papier*, in: Herzog u.a., Maunz/Dürig, Grundgesetz, Band II, Art. 13 GG Rn. 10.

weis auf ein Charakteristikum der realen Welt – der Körperlichkeit – ausgeschlossen werden.[142] Vielmehr muss eine übergreifende Gesamtbetrachtung anhand des Schutzzwecks des Art. 13 GG durchgeführt werden.

Art. 13 GG soll die freie Entfaltung der Persönlichkeit im räumlichen Bereich gewährleisten. Im Kern geht es also nicht zwingend nur um Wohnraum im engeren Sinne, sodass der Wohnungsbegriff nach der hM weit auszulegen ist. *Papier* schlägt als Alternativformulierung des Art. 13 Abs. 1 GG daher folgende Formulierung vor: „Die Freiheit der räumlichen Privatsphäre wird gewährleistet."[143] Diese Fassung triff die Schnittmenge der gegenwärtigen Auslegung des sachlichen Schutzbereichs des Art. 13 GG recht gut, stellt sie doch nicht mehr allein auf das Merkmal der Wohnung im klassischen Sinne ab, sondern auf das dahinterstehende Schutzgut – die räumliche Privatsphäre. Der entscheidende Punkt ist daher, wie das Adjektiv „räumlich" in diesem Zusammenhang zu definieren ist. Das BVerfG beschäftigt sich in seiner Entscheidung zur Online-Durchsuchung mit einem staatlichen Zugriff auf informationstechnische Systeme. Im Rahmen dessen verlangt das Gericht in seinen Ausführungen zu Art. 13 GG stets einen räumlichen Wohnungsbezug. Ein solcher liegt z.B. vor, wenn ein staatlicher Akteur die Wohnung betritt, um das System zu manipulieren oder aber, wenn er das informationstechnische System so bearbeitet, dass mit dessen Hilfe Aktivitäten innerhalb der Wohnung überwacht werden können.[144] Diesen Darlegungen immanent ist ein Bezug zu einer Wohnung im räumlich-gegenständlichen Bereich. *Eisenmenger* schließt sich dieser Auslegung an und betont, dass Art. 13 GG gerade dem Schutz der Körperlichkeit dienen solle und der virtuelle Raum daher nicht erfasst werde.[145]

Diesen Erwägungen ist im Ergebnis zuzustimmen. Eine Subsumtion des virtuellen sozialen Online-Netzwerks unter den Wohnungsbegriff führt zunächst zu definitorischen Unschärfen. Vor dem Hintergrund der Entwicklung des Web 2.0 erfüllen zwar einzelne virtuelle Räume (Cyberspace im engeren Sinne)

---

[142] So aber z.B. *Luch/Schulz*, die darauf abstellen, dass die Inhaber des Wohnungsgrundrechts nach Art. 13 GG auf die gegenständliche Unversehrtheit vertrauen dürfen. Da der virtuelle Raum jedoch gerade nicht gegenständlich bzw. körperlich sei, könne dieser auch nicht unter den Wohnungsbegriff fallen und sei daher nicht durch Art. 13 GG geschützt (vgl. *Luch/Schulz*, Die digitale Dimension der Grundrechte, Die Bedeutung der speziellen Grundrechte im Internet, MMR 2013, 88, 91.)

[143] *Papier*, in: Herzog u.a., Maunz/Dürig, Grundgesetz, Band II, Art. 13 GG Rn. 4.

[144] Vgl. BVerfG, NJW 2008, 822, 826.

[145] Vgl. *Eisenmenger*, Die Grundrechtsrelevanz „virtueller Streifenfahrten", S. 183.

durchaus eine persönlichkeitsentfaltende Funktion, das Erfordernis eines grundgesetzlichen Schutzes derartiger Entfaltungsbereiche ergibt sich jedoch nur, sofern diese gegenüber der Öffentlichkeit nach außen hin abgegrenzt sind. Nur so können sie u.U. der räumlichen Privatsphäre, in Abgrenzung zur Sozialsphäre, zugeordnet werden. Dies trifft auf soziale Online-Netzwerke partiell zu. Entscheidend ist insofern die Umsetzung von Privatsphäre-Einstellungen, die eine Eingrenzung des Nutzerkreises ermöglichen. Auch dies wirft jedoch Schwierigkeiten im Hinblick darauf auf, dass das Nutzerverhalten diesbezüglich keiner generalisierenden Bewertung unterzogen werden kann. So mag es eine Vielzahl von Nutzern geben, die tatsächlich nur ihnen bekannte Personen „adden" bzw. ihrem Netzwerk hinzufügen. Auf der anderen Seite gibt es jedoch auch solche, die ihre Kontaktliste gleichsam inflationär mit auch ihnen unbekannten Personen erweitern, sodann entfalten auch die Privatsphäre-Einstellungen keine hinreichende Abgrenzung zum öffentlichen Teil des Netzwerks. Gleichzeitig implizieren diese Netzwerke zunächst stets eine Preisgabe privater Daten, um im Anschluss eine virtuelle Privatsphäre entstehen lassen zu können. Die Grenzen zwischen Privat- und Sozialsphäre verschwimmen mithin zwangsläufig.[146] Diese Darlegungen machen deutlich, dass eine Subsumtion unter den sachlichen Schutzbereich des Art. 13 GG nur einzelfallbezogen möglich wäre und stets sehr vom Verhalten des jeweiligen Nutzers abhängig wäre. Eine wirkliche Rechtssicherheit wäre so nur schwerlich zu erreichen.[147]

Diese Erwägungen sind exemplarisch für das Web 2.0, dem eine Nutzerzentrierung und somit auch Nutzerabhängigkeit immanent sind, die letztlich dazu führen, dass eine generalisierende Betrachtung seiner Erscheinungsformen nicht erfolgen kann. Eine Verwässerung des Schutzbereichs und definitorische Unschärfen sind daher unvermeidbar und dem Web 2.0 folglich wesensimmanent. Diese Unschärfen im Bereich der Definition des sachlichen Schutzbereichs und der damit verbundene Mangel an Unterscheidungskraft führen jedoch zu einer Disqualifizierung im Sinne eines verfassungsrechtlichen Schutzbereichs.[148]

---

[146] Vgl. *Hauck*, Heimliche Strafverfolgung und Schutz der Privatheit, S. 426.
[147] Vgl. so auch *Eisenmenger*, Die Grundrechtsrelevanz „virtueller Streifenfahrten", S. 183.
[148] Vgl. *Hauck*, Heimliche Strafverfolgung und Schutz der Privatheit, S. 425.

Die räumliche Privatheit wird zudem geschützt, um dem Grundrechtsberechtigten einen Ort der privaten Entfaltung zu gewähren, somit fungiert sie als Ausgangspunkt für ebendiese. Würden soziale Online-Netzwerke unter Art. 13 GG subsumiert, würde genau die entgegengesetzte Herangehensweise gewählt werden. Der Cyberspace im engeren Sinne würde erst durch die Zuordnung persönlicher Daten zu einer Wohnung im Sinne des Art. 13 GG. Laut dem klassischen Schutzbereichsverständnis ist die körperliche Wohnung also gerade deshalb schutzwürdig, weil sie die notwendige Grundbedingung für die „Entfaltung informationeller und dezisionaler Privatheit“[149] darstellt, letztere also auf der Wohnung aufbaut. Im Hinblick auf soziale Online-Netzwerke ist dieser Zusammenhang jedoch andersherum zu denken. Erst die Auslebung der informationellen Privatheit führt zu einer Qualifizierung dieses virtuellen Raumes als „Stätte des privaten Lebens und Wirkens“[150].[151] Somit scheidet eine Vergleichbarkeit der Interessenlage auch wegen konzeptueller Differenzen aus.

Aufgrund der Erscheinungsformen des Web 2.0 und der partiellen Verlagerung des privaten Lebens in den virtuellen Raum kann heutzutage außerdem nahezu alles auch durch informationelle Erwägungen begründet werden. *Hauck* sieht daher auch die Gefahr, dass eine Subsumtion der unterschiedlichen Erscheinungsformen im Cyberspace unter Spezialgrundrechte zu einer Verwässerung der jeweiligen Schutzbereiche führe und diese Grundrechte somit Gefahr liefen ihre Eigenständigkeit zu verlieren.[152] Aus den Spezialgrundrechten würden mithin persönlichkeitsrechtlich aufgeladene „Supergrundrechte“ werden.[153]

Derartige Grundrechte sollten indes nur in Kauf genommen werden, wenn tatsächlich eine Schutzlücke für virtuelle Räume bestünde. Für den Bereich der informationellen Selbstbestimmung – und um diese geht es hier im Kern – ist jedoch ein Schutz über das allgemeine Persönlichkeitsrecht gewährleistet, sodass in diesem Fall Art. 13 GG nicht anzuwenden ist.

[149] *Hauck*, Heimliche Strafverfolgung und Schutz der Privatheit, S. 426.
[150] *Jarass*, in: Jarass/Pieroth, GG, Art. 13 GG Rn. 4.
[151] Vgl. *Hauck*, Heimliche Strafverfolgung und Schutz der Privatheit, S. 426.
[152] Vgl. ebd.
[153] Vgl. *Heckmann*, Der virtuelle Raum als Wohnung?, S. 629.

Darüber hinaus ist ein Spezifikum des Cyberspace, dass die Daten auf unterschiedlichen Servern auf der ganzen Welt gespeichert werden. Diese räumliche Entgrenzung – und somit das Wesen des virtuellen Raumes – sprechen ebenso gegen die Anwendung von Grundrechten, die ipso iure feste Lokalitäten schützen sollen.[154] Bestünde die Absicht, diese Gegensätzlichkeit überbrücken zu wollen, führt dies zwangsläufig zu den o.g. Problematiken.

c) Allgemeines Persönlichkeitsrecht gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Ein verdeckter personaler Ermittler könnte ferner in das allgemeine Persönlichkeitsrecht nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG eingreifen. Ausprägungen dieses Rechts sind das Recht auf informationelle Selbstbestimmung und das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, die im Folgenden näher betrachtet werden sollen.

aa) Recht auf informationelle Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung gewährleistet „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“[155]. Damit wird das Recht des Individuums geschützt, generell selbst darüber zu entscheiden, wann es welchen persönlichen Lebenssachverhalt wem offenbart.[156] Es ist dabei unerheblich, welcher Sphäre des Persönlichkeitsschutzes das Datum zuzuordnen ist[157], da im Rahmen moderner Informationstechnologien eine Zusammenführung von Daten möglich ist, auf deren Grundlage ein umfassendes Persönlichkeitsbild erstellt werden kann[158], sodass es „unter den Bedingungen der automatischen Datenverarbeitung kein „belangloses“ Datum mehr“[159] gibt.

Diese Ausweitung des Persönlichkeitsschutzes wird jedoch in Bezug auf Kommunikationsbeziehungen im virtuellen Raum durch das BVerfG in seiner Grundsatzentscheidung zur Online-Durchsuchung aus dem Jahr 2008 wiederum eingeschränkt, indem ergänzend das Vorliegen eines schutzwürdigen Vertrauens gefordert wird.

---

[154] Vgl. Grözinger, Die Überwachung von Cloud-Storage, S. 66.
[155] BVerfG, Urteil vom 15. Dezember 1983 – 1 BvR 209/83 –, BVerfGE 65, 1-71, juris, Rn. 149; BVerfG, Beschluss vom 07. Dezember 2011 – 2 BvR 2500/09 –, BVerfGE 130, 1-51, juris, Rn. 37.
[156] Vgl. *Jarass*, in: Jarass/Pieroth, GG, Art. 2 GG Rn. 42.
[157] Vgl. *Horn*, in: Stern/Becker, Grundrechte-Kommentar, Art. 2 GG Rn. 50.
[158] Vgl. *Di Fabio*, in: Herzog u.a., Maunz/Dürig, Grundgesetz, Band I, Art. 2 GG Rn. 174.
[159] BVerfG, Urteil vom 15. Dezember 1983 – 1 BvR 209/83 –, BVerfGE 65, 1-71, juris, Rn. 152.

> *„Ein Eingriff in das Recht auf informationelle Selbstbestimmung liegt nicht schon dann vor, wenn eine staatliche Stelle sich unter Legende in eine Kommunikationsbeziehung zu einem Grundrechtsträger begibt, wohl aber, wenn sie dabei ein schutzwürdiges Vertrauen des Betroffenen in die* ***Identität und die Motivation*** *seines Kommunikationspartners ausnutzt, um persönliche Daten zu erheben, die sie ansonsten nicht erhalten würde."*[160]

Damit stellt das BVerfG maßgeblich auf die Ausnutzung eines schutzwürdigen Vertrauens ab, das dann nicht vorliegt, wenn das Kommunikationsmedium keine Mechanismen zur Überprüfung der Identität und Wahrhaftigkeit der Teilnehmer an der Kommunikation zur Verfügung stellt.[161] Auf dieser Grundlage schließt das Gericht einen Grundrechtseingriff u.a. bei Diskussionsforen aus, im Rahmen dessen sich zwar eine Art virtuelle Gemeinschaft bilden kann, es aber jedem Teilnehmer an der Kommunikation bewusst ist, dass eine Prüfung der jeweiligen Identität nicht valide erfolgen kann.[162] Soziale Online-Netzwerke unterscheiden sich jedoch hinsichtlich ihrer Konstruktion von Diskussionsforen. Derartige Netzwerke fungieren als erweiterter Sozialkontext und übertragen reale Beziehungen in den virtuellen Raum. Im Unterschied zu Diskussionsforen, sind die Kommunikationsbeziehungen hier gerade nicht durch Anonymität geprägt, sodass an dieser Stelle auch nicht per se auf eine vermeintlich „geringe […] Verbindlichkeit im Internet"[163] abgestellt werden kann.[164]

Nach dem BVerfG ist für die Ermittlung der Grundrechtsrelevanz des jeweiligen Einsatzszenarios des verdeckten personalen Ermittlers nunmehr entscheidend, ob zuverlässige Überprüfmechanismen vorliegen.

(1) Passive Kenntnisnahme von Inhalten als Teil der (Netzwerk-)Öffentlichkeit

Sofern der Ermittler ausschließlich passiv Kenntnis von öffentlich sichtbaren Profilinhalten nimmt, also solchen, die z.B. im Rahmen von LinkedIn allen Nutzern einer externen Suchmaschine zugänglich sind, ist ein schutzwürdiges Vertrauen in die Identität und Motivation des Rezipienten zu verneinen. Gleiches gilt für solche Inhalte, die zwar nicht der gesamten Cyberspace-

[160] BVerfG, NJW 2008, 822, 836.
[161] Vgl. ebd.
[162] Vgl. ebd.
[163] *Soiné*, Personale verdeckte Ermittlungen in sozialen Netzwerken zur Strafverfolgung, NStZ 2014, 248, 249.
[164] So auch *Hornung*, Ein neues Grundrecht, CR 2008, 299, 305.

Öffentlichkeit offenstehen, wohl aber der Netzwerköffentlichkeit, da zum einen der Kreis der Rezipienten für den Nutzer nicht individualisierbar ist und zum anderen eine Überprüfung der Nutzeridentität, wie oben dargestellt, nur in Einzelfällen stattfindet, etwa, wenn das Nutzerkonto vorübergehend gesperrt wurde. In allen anderen Fällen genügt für die Anmeldung in sozialen Online-Netzwerken eine gültige E-Mail-Adresse, die wiederum ohne eine Verifizierung der Klaridentität erstellt werden kann. Die Kenntnisnahme solcher Daten in sozialen Online-Netzwerken stellt daher grundsätzlich keinen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Etwas anderes gilt nur dann, wenn diese öffentlich zugänglichen Daten gezielt zusammengetragen werden und u.U. unter Zuhilfenahme darüberhinausgehender Daten ausgewertet werden und daraus eine „besondere Gefahrenlage für die Persönlichkeit“[165] des Nutzers resultiert.[166]

(2) Der verdeckte personale Ermittler mit eigenem Account als Mitglied des Netzwerks eines Nutzers

Neben einer passiven Kenntnisnahme der Inhalte sozialer Netzwerke, ohne aktiv gegenüber einem Nutzer in Erscheinung zu treten, kann der Ermittler auch Teil des Netzwerks des Nutzers werden. In diesen Fällen muss der Nutzer die Anfrage des verdeckten personalen Ermittlers aktiv annehmen und ihn so seinem Netzwerk hinzufügen. Da der Nutzer also hier die Profilinhaber, die Kenntnis von seinen Inhalten erhalten, individualisieren kann, trifft dies grundsätzlich auch auf das für einen Eingriff in das Recht auf informationelle Selbstbestimmung erforderliche Vertrauen zu. Fraglich ist jedoch, wann ein solches in sozialen Netzwerken entsteht. An dieser Stelle ist zwischen der Nutzung einer fiktiven Identität und der Übernahme einer real existierenden zu unterscheiden.

(a) Verwendung einer fiktiven Identität

Der verdeckte personale Ermittler kann unter Verwendung einer fiktiven Identität Teil des Kontaktnetzwerks des Nutzers werden. Sofern nicht offensichtlich ein Nickname bzw. Fantasiename verwendet wird, entsteht auf Seiten des

[165] BVerfG, NJW 2008, 822, 836.

[166] So z.B. auch *Warg* (in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, § 12 SÜG Rn. 21d), der hinsichtlich der Einsichtnahme in den öffentlich sichtbaren Teil sozialer Netzwerke durch die an der Sicherheitsüberprüfung mitwirkende Stelle die Notwendigkeit einer Rechtsgrundlage für ein derartiges Handeln bezweifelt und einen Grundrechtseingriff nur bejaht, wenn ein solch gezieltes Zusammentragen und Auswerten von öffentlich zugänglichen Informationen zu bejahen ist.

Nutzers zunächst die Vorstellung, dass derjenige, der Teil seines Netzwerkes werden möchte, tatsächlich den Namen trägt unter dem er in dem sozialen Online-Netzwerk aktiv ist. Werden die Grundsätze aus der oben dargestellten Rechtsprechung des BVerfG zur Online-Durchsuchung angewendet, genügt ein bloßes Vertrauen in die Identität des Anfragenden jedoch nicht. Vielmehr ist dieses nur dann schutzwürdig, wenn **Überprüfungsmechanismen** in Bezug auf die Identität und Motivation des Nutzers vorliegen.

Im Unterschied zur realen Welt treten sich die Nutzer sozialer Online-Netzwerke nicht körperlich gegenüber, sodass das Vertrauen in die Identität des jeweils anderen aus anderen Umständen als den unmittelbar physisch Wahrnehmbaren resultieren muss. Grundsätzlich besteht die Möglichkeit, sich unter einem fiktiven Namen in sozialen Online-Netzwerken anzumelden oder aber einen einzelnen Account durch verschiedene Personen zu nutzen.[167] Eine Überprüfung der Identität des Account-Inhabers durch den Host-Provider der Plattform findet, wie oben dargestellt, grundsätzlich nicht statt. Demnach können die Registrierungsmodalitäten mangels Überprüfungsmechanismus kein schutzwürdiges Vertrauen in die Identität vermitteln.[168]

Der Anfragende selbst könnte jedoch ein schutzwürdiges Vertrauen in seine Identität erzeugen. *Ihwas* stellt u.a. auf die äußere Ausgestaltung des Profils ab, die die Schutzwürdigkeit vermitteln könne. Er unterscheidet zwischen primären Eigenschaften (z.B. Name, Kontaktliste oder Profilbild) und sekundären Merkmalen (z.B. Geburtsdatum oder Arbeitsplatz) eines Profils in sozialen Online-Netzwerken.[169] Besonders hervor hebt er in diesem Zusammenhang die Kontaktliste. Sei diese umfangreich, spreche dies für eine bereits länger andauernde Nutzung des Kontos und dafür, dass auch schon andere Nutzer Vertrauen in die Identität des Profilinhabers gefasst hätten.[170] Klingt dieses Kriterium auf den ersten Blick überzeugend, korrespondiert es jedoch nicht mit den aktuellen Gegebenheiten. So können Kontakte in derartigen Netzwerken

[167] Vgl. *Henrichs*, Verdeckte personale Ermittlungen im Internet, Kriminalistik 2012, 632, 633.
[168] Vgl. *Hertel*, Virtuelle verdeckte personale Ermittlungen, Kriminalistik 2019, 162, 163.
[169] Vgl. *Ihwas*, Strafverfolgung in sozialen Netzwerken, S. 152.
[170] Vgl. ebd., S. 153.

heute z.B. käuflich erworben werden.[171] Auch dem Profilbild kommt nach seiner Ansicht eine große Bedeutung zu.[172] Zeige dies eine Person[173] anstatt z.B. eine Landschaft etc., könne auch dieser Umstand das Vertrauen in die Identität erhöhen. Problematisch ist indes, wie *Bauer* zu Recht betont, dass diese Auffassung letztlich für den staatlich ermittelnden Akteur als Anreiz fungieren kann, ein möglichst datensparsames Profil zu verwenden und auf die Leichtgläubigkeit des Nutzers zu vertrauen.[174] Somit könnte der verdeckte personale Ermittler gegenüber diesem Personenkreis auf der Grundlage der Ermittlungsgeneralklausel der §§ 161, 163 StPO agieren, eine bestimmtere Rechtsgrundlage wäre sodann nicht erforderlich.

Darüber hinaus nennt *Ihwas* als weiteren möglichen Anknüpfungspunkt die Ausgestaltung der Kontaktanfrage. Enthalte diese weitergehende Informationen, wie etwa Details zum jeweiligen Kennverhältnis oder aber den Grund für die Kontaktaufnahme, könnten dies Indizien sein, die für ein schutzwürdiges Vertrauen in die Identität des Gegenübers sprechen würden.[175] In Bezug auf das soziale Online-Netzwerk LinkedIn genügt für die Übersendung einer Vernetzungseinladung ein einziger Klick. Fakultativ kann im Anschluss noch eine persönliche Nachricht hinzugefügt werden, zwingend notwendig ist dies jedoch nicht. Dies führt im Ergebnis ebenfalls dazu, dass ein Anreiz für staatliche Stellen geschaffen wird, die Kontaktanfrage nicht mit einer zusätzlichen Nachricht anzureichern. Letztlich würde auch hier der leichtgläubige Nutzer benachteiligt werden und gerade dieser – vermutlich am meisten schützenswerte – Nutzertypus eines grundrechtlichen Schutzes beraubt werden. Dies würde bedeuten, dass der staatliche Akteur selbst eine Grundrechtsbetroffenheit durch die Art und den Umfang derjenigen Informationen, die er bereitstellt, beeinflussen könnte und somit auch die Anforderungen einer dem Bestimmtheitsgrundsatz genügenden Rechtsgrundlage, wie §§ 110a StPO ff., aktiv umgehen könnte. Damit trüge jedoch der private Nutzer des sozialen Online-Netzwerkes allein die Risiken, die sich aus einer erschwerten Nachprüfbarkeit der Identität

[171] Vgl. *Bauer*, Soziale Netzwerke und strafprozessuale Ermittlungen, S. 163.
[172] Vgl. *Ihwas*, Strafverfolgung in sozialen Netzwerken, S. 154.
[173] Hierbei ist zu berücksichtigen, dass der verdeckte Ermittler nur solche Fotos verwenden darf, für die er auch entsprechende Nutzungsrechte besitzt. Die Verwendung eines realen Fotos wäre darüber hinaus auch aus ermittlungstaktischen und sicherheitlichen Gründen nicht sinnvoll. Daher ist ein manipuliertes Foto zu verwenden (vgl. *Ihwas*, Strafverfolgung in sozialen Netzwerken, S. 154).
[174] Vgl. *Bauer*, Soziale Netzwerke und strafprozessuale Ermittlungen, S. 163.
[175] Vgl. *Ihwas*, Strafverfolgung in sozialen Netzwerken, S. 150.

des jeweils anderen Nutzers ergeben. Letztlich würde ein Grundrechtsschutz von weiteren Auskünften des anderen abhängig gemacht werden.

Eine solche Argumentationsweise, die einzig auf Überprüfmechanismen der Identität abstellt, lässt jedoch sowohl die Qualität der Daten, die soziale Online-Netzwerke enthalten, als auch das Wesen dieser Netzwerke völlig außer Acht. Wie oben dargestellt, fungieren diese als erweiterter Sozialkontext und sind dadurch geprägt, dass die virtuellen Kontakte in der Regel den realen entsprechen. Es kann hier also von einer Spiegelbildlichkeit gesprochen werden.[176] Darüber hinaus greift hinsichtlich der Darstellung der Nutzer die extended-real-life-Hypothese, sodass die Profile durchaus Rückschlüsse auf die Persönlichkeit des Inhabers erlauben. Die direkte Übertragung der Rechtsprechung des BVerfG zur Online-Durchsuchung auf soziale Online-Netzwerke wird daher der Konstruktion des Cyberspace im weiten Sinne nicht gerecht, da dieser jeweils aus „Unterräumen" (Cyberspace im engeren Sinne) besteht, die separat betrachtet werden müssen. So können für ein Diskussionsforum als ein Cyberspace im engeren Sinne nicht pauschal die gleichen Grundsätze gelten wie für ein soziales Online-Netzwerk, dessen Wesen es gerade ist, die eigene Persönlichkeit virtuell zu präsentieren. Eine solche Wertung widerspricht auch nicht der Entscheidung zur Online-Durchsuchung. So bezieht sich das Gericht auf Diskussionsforen und stellt darauf ab, dass sich in diesem Zusammenhang jeder Kommunikationsteilnehmer darüber im Klaren sei, dass er die Identität des jeweils anderen nicht kenne und dessen Angaben auch letztlich nicht überprüfen könne. Daraus schließt das Gericht, dass „sein Vertrauen darauf, dass er nicht mit einer staatlichen Stelle kommuniziert, […] **in der Folge** nicht schutzwürdig"[177] sei. Wichtig ist hier die Verwendung der Formulierung „in der Folge", die eine Kausalität indiziert. Wesen sozialer Online-Netzwerke ist es jedoch gerade nicht, dass die Nutzer die jeweils anderen Identitäten nicht kennen, sondern dieser Cyberspace im engeren Sinne gerade durch wesensimmanente Schnittstellen zum realen Leben gekennzeichnet ist, sodass sich daraus die Erwartung ergibt, dass die nach außen hin suggerierte Identität der tatsächlichen entspricht.

[176] Vgl. *Brenneisen/Staack*, Die virtuelle Streife in der Welt der Social Media, Kriminalistik 2012, 627, 629.
[177] BVerfG, NJW 2008, 822, 836.

Das BVerfG fordert für ein grundrechtsschutz-auslösendes, schützenswertes Vertrauen in die Identität des Kommunikationspartners das Vorliegen von Überprüfmechanismen. Sinn und Zweck ebendieser Mechanismen ist es, eine Art Brücke in die reale Welt zu konstruieren. Dies kann entweder auf Seiten des Host-Providers z.B. durch die Übersendung einer Ausweiskopie erfolgen oder durch den anfragenden Kommunikationspartner, der sich z.B. im Rahmen seiner Kontaktanfrage auf reale Kennverhältnisse bezieht. Entscheidend für die Entstehung eines schützenswerten Vertrauens ist mithin stets eine Verknüpfung der virtuellen mit der realen Welt, die vertrauensbildenden Faktoren sind demnach der realen Welt zuzuordnen. Diese Annahme geht jedoch letztlich davon aus, dass es sich jeweils um unterschiedliche Welten handelt, die über diese Art „Brücken“ miteinander partiell verbunden werden. Wie oben dargestellt, trifft dies jedoch hinsichtlich des sozialen Online-Netzwerks als Cyberspace im engeren Sinne nicht zu. Vielmehr handelt es sich gerade nicht um einen Raum mit eigenen Gesetzmäßigkeiten, sondern um eine Erweiterung der zwischenmenschlichen Beziehungen aus der realen Welt. Demnach kann sich ein schützenswertes Vertrauen auch aus dem Wesen dieses Raumes an sich ergeben, der die reale Welt erweitert. So darf der Nutzer, ebenso wie im realen Leben, auf die Identität seines Gegenübers vertrauen, also darauf, dass er, bildlich gesprochen, nur mit der Person, die tatsächlich vor ihm steht, kommuniziert und ihr personenbezogene Daten mitteilt. Die Schutzwürdigkeit dieses Vertrauens ergibt sich aus den Spezifika dieses Raumes als Erweiterung des realen Lebens, sodass es keiner zusätzlichen Verknüpfungen als Überprüfmechanismen mehr bedarf.

Daher ist die hinsichtlich des Schutzbereichs entwickelte Restriktion des BVerfG auf soziale Online-Netzwerke nicht anwendbar, sodass auf eine weite Auslegung des Schutzbereichs des Rechts auf informationelle Selbstbestimmung zurückgegriffen werden kann. Laut diesem hat grundsätzlich jeder selbst das Recht, freiwillig über die Artikulation und Weitergabe seiner persönlichen Daten zu entscheiden.[178]

[178] Vgl. BVerfG, Urteil vom 15. Dezember 1983 – 1 BvR 209/83 –, BVerfGE 65, 1-71, juris, Rn. 149; BVerfG, Beschluss vom 07. Dezember 2011 – 2 BvR 2500/09 –, BVerfGE 130, 1-51, juris, Rn. 37.

Nutzt also ein verdeckter personaler Ermittler eine fiktive Identität, um Teil des Kontaktnetzwerks einer privaten Person zu werden, und erlangt auf diesem Wege Kenntnis von persönlichen Daten dieses Nutzers, liegt ein Eingriff in das Recht auf informationelle Selbstbestimmung vor. In diesem Zusammenhang spielt auch für das reine Vorliegen eines Grundrechtseingriffs die Unterscheidung zwischen einer passiven Aufnahme dieser Daten oder einer tatsächlichen Interaktion mit der Zielperson keine Rolle.[179] Entscheidend ist einzig, dass der Ermittler täuschungsbedingt Kenntnis von persönlichen Daten erlangt.

(b) Verdeckte Übernahme einer bereits existierenden Identität
Schlussendlich besteht auch die Möglichkeit, dass der Ermittler einen bereits existierenden Account übernimmt, der schon Teil des Netzwerks der Zielperson ist. In diesem Fall penetriert der staatliche Akteur ein bereits bestehendes Vertrauensverhältnis zwischen den beiden Nutzern der Profile und nutzt dieses aus, um an Informationen zu gelangen. Es liegt eine Täuschung über die Identität des Account-Inhabers vor, sodass die Weitergabe persönlicher Daten durch den privaten Nutzer nicht freiwillig erfolgt, da er nicht vollumfänglich über die Rahmenbedingungen seiner Datenkundgabe informiert ist. Ein Eingriff in das Recht auf informationelle Selbstbestimmung ist mithin zu bejahen.

bb) Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme
Als weitere Ausprägung des allgemeinen Persönlichkeitsrechts gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hat das BVerfG in seiner Entscheidung zur Online-Durchsuchung das Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme (im Folgenden „IT-Grundrecht“[180]) entwickelt. Dieses soll vor einem staatlichen Zugriff auf das informationstechnische System als Ganzes und nicht nur vor einem Zugriff auf konkretisierte Kommunikationsvorgänge schützen. Nach Auffassung des Gerichts bedarf das Individuum zur Entfaltung seiner Persönlichkeit informationstechnische Systeme und stellt diesen explizit persönliche Daten zur Verfügung oder aber liefert diese bewusst oder unbewusst durch die

[179] Gleichwohl ist diese Unterscheidung im Rahmen der Bestimmung der Eingriffsintensität von Relevanz.
[180] Vgl. *Albrecht*, in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Teil 28, B, I, Rn. 33.

Nutzung derartiger Systeme.[181] Unter diesen Umständen ist es einem auf dieses System zugreifenden Dritten möglich, „sich einen potenziell äußerst großen und aussagekräftigen Datenbestand zu verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein“[182]. Im Unterschied zum Recht auf informationelle Selbstbestimmung schützt das IT-Grundrecht also nicht nur vor einzelnen Datenerhebungen. Die Abgrenzung zwischen diesen beiden Ausprägungen des allgemeinen Persönlichkeitsrechts erfolgt daher nach Auffassung des Gerichts anhand quantitativer Aspekte.[183]

Der sachliche Schutzbereich des IT-Grundrechts ist daher dann betroffen, wenn ein informationstechnisches System durch einen staatlichen Akteur als Ganzes infiltriert wird.[184] Wird der personale verdeckte Ermittler in sozialen Online-Netzwerken tätig, beschränken sich seine Datenerhebungen auf die Informationen, die die Zielperson teilt, sodass nicht das soziale Online-Netzwerk als solches infiltriert wird, sondern nur vereinzelt Daten erhoben werden.[185]

Der verdeckte personale Ermittler greift somit durch ein Tätigwerden in sozialen Online-Netzwerken nicht in das IT-Grundrecht ein.

---

[181] Vgl. BVerfG, NJW 2008, 822, 827.

[182] Ebd.

[183] Ob die Schaffung dieser neuen Ausprägung des allgemeinen Persönlichkeitsrechts tatsächlich notwendig war, ist eine in der Literatur viel diskutierte Frage, die hier jedoch nicht weiter vertieft werden soll. Streitig ist in diesem Zusammenhang insbesondere die Frage, ob dem IT-Grundrecht ein eigenständiger Schutzgehalt zukommt oder aber ein Schutz nicht ebenso über das Recht auf informationelle Selbstbestimmung zu erreichen wäre. *Kube* schlägt z.B. vor, den Umfang der Daten, auf die im Rahmen der Infiltration informationstechnischer Systeme Zugriff genommen werden kann, im Rahmen der Prüfung der Verhältnismäßigkeit eines Eingriffs in das Recht auf informationelle Selbstbestimmung zu berücksichtigen (vgl. *Kube*, Persönlichkeitsrecht, Rn. 70).

[184] Vgl. *Hoffmann-Riem*, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008,1009, 1019.

[185] An dieser Stelle kann daher die Frage dahinstehen, ob ein soziales Netzwerk überhaupt ein derartiges unter das IT-Grundrecht fallendes informationstechnisches System darstellt. Eine genaue Definition dieses Begriffs bleibt das BVerfG in seiner Entscheidung schuldig. Es begründet die Notwendigkeit eines neuen Grundrechts vorrangig mit quantitativen Gesichtspunkten, aufgrund derer ein umfassender Einblick in die Persönlichkeit des Profilinhabers erlangt werden kann. Wird auf die Natur dieser Art von Online-Netzwerken, die schlussendlich als erweiterter Sozialkontext die Auslebung der eigenen Persönlichkeit erlauben, abgestellt, ließe sich auf dieser Grundlage das Vorliegen eines derartigen informationstechnischen Systems bejahen. *Eisenmenger* schlägt hingegen eine „hardwareäquivalente Auslegung“ vor und stellt maßgeblich darauf ab, ob das System eine „gerätegleiche Ersatzfunktion“ entfalte. Da die vorrangige Dienstleistung sozialer Online-Netzwerke eben nicht – wie beim heimischen PC – eine Archivierung von Inhalten sei, scheide eine Qualifizierung als informationstechnisches System im Sinne des IT-Grundrechts aus (*Eisenmenger*, Die Grundrechtsrelevanz „virtueller Streifenfahrten, S. 204).

2. Rechtsgrundlagen für einen Eingriff in das allgemeine Persönlichkeitsrecht

Zusammenfassend lässt sich sagen, dass der verdeckte personale Ermittler in sozialen Online-Netzwerken einzig und auch nur dann in das allgemeine Persönlichkeitsrecht in der Ausformung des Rechts auf informationelle Selbstbestimmung eingreift, wenn er in den Bereich des Netzwerkes vordringt, auf den der Zugriff durch die Zielperson eingeschränkt wurde oder aber aktiv mit letzterer unter einem eigenen Account (oder dem eines Dritten) kommuniziert.[186] Im Folgenden werden daher zunächst die sich aus der Verfassung abzuleitenden Anforderungen für einen solchen Grundrechtseingriff dargelegt. Im Anschluss wird der Frage nachgegangen, ob die auf den realen Raum anwendbaren Rechtsgrundlagen (§§ 161, 163 StPO und § 110a StPO) herangezogen werden können.

a) Verfassungsrechtliche Anforderungen

Ein Eingriff in das allgemeine Persönlichkeitsrecht ist gemäß Art. 2 Abs. 1 GG auf der Grundlage des sog. **Schrankentrias** möglich.[187] Am relevantesten ist in diesem Zusammenhang die sog. verfassungsmäßige Ordnung, die jede formell und materiell verfassungsmäßige Rechtsnorm erfasst. Darunter fallen insbesondere formelle Bundes- und Landesgesetze, aber auch Rechtsverordnungen, Satzungen oder das Richterrecht.[188] *Kunig* spricht aus diesem Grunde von einem Rechtsvorbehalt[189], in Abgrenzung zum Gesetzesvorbehalt.

Darüber hinaus ergibt sich aus dem allgemeinen **Grundsatz vom Vorbehalt des Gesetzes**, der aus Art. 20 Abs. 3 i.V.m. Abs. 2 GG abgeleitet wird[190], dass dem Gesetzgeber die Entscheidung über alle für das Gemeinwesen wesentlichen Belange obliegt.[191] Dieser auch als Wesentlichkeitsprinzip bezeichnete Grundsatz besagt, dass Eingriffe in Grundrechte stets als wesentliche Fragen zu qualifizieren sind, für die es einer gesetzlichen Eingriffsgrundlage bedarf.

---

[186] Folgte man der Rechtsauffassung des BVerfG, das sich für ein restriktives Verständnis des Schutzbereichs des Rechts auf informationelle Selbstbestimmung ausspricht, würde ein Eingriff in dieses Grundrecht nur vorliegen, wenn ein schutzwürdiges Vertrauen der Zielperson in die Identität und Motivation des Ermittlers zu bejahen wäre. Ein solches entsteht jedoch erst, sofern das soziale Netzwerk entsprechende Überprüfungsmechanismen beinhaltet. Dies ist, wie oben bereits dargestellt, regelmäßig nicht der Fall. In der Konsequenz kann sich die Strafverfolgungsbehörde auf §§ 161, 163 StPO stützen (vgl. *Bär*, in: Heintschel-Heinegg von/Bockemühl, KMR- StPO, § 100a StPO Rn. 62).

[187] Vgl. *Horn*, in: Stern/Becker, Grundrechte-Kommentar, Art. 2 GG Rn. 95.

[188] Vgl. ebd., Rn. 97.

[189] Vgl. *Kunig*, in: Münch von/Kunig, Grundgesetz Kommentar, Art. 2 GG Rn. 23.

[190] Vgl. *Sommermann*, in: Huber/Voßkuhle, Grundgesetz, Band 2, Art. 20 GG Rn. 278.

[191] Vgl. ebd., Rn. 273.

Die Voraussetzungen für einen solchen Eingriff müssen sodann in der Rechtsgrundlage klar und bestimmt festgelegt werden.[192] Der sog. **Bestimmtheitsgrundsatz**, der dem Grundsatz vom Vorbehalt des Gesetzes wesensimmanent ist, besagt, dass für den jeweiligen Normadressaten die Norm so klar sein muss, dass er sein Verhalten danach ausrichten kann (Normenklarheit und Normenwiderspruchsfreiheit).[193] Daraus folgt hingegen nicht, dass der Gesetzgeber jeden Einzelfall bis ins kleinste Detail regeln muss, insofern ist es ihm grundsätzlich gestattet, z.B. im Rahmen eines als gering einzustufenden Grundrechtseingriffs, auslegungsbedürftige Rechtsbegriffe oder aber Generalklauseln zu verwenden.[194] Das jeweils notwendige Maß an Bestimmtheit kann daher nicht pauschal ermittelt werden, sondern ist mithilfe unterschiedlicher Faktoren zu eruieren[195], wobei die Intensität des Grundrechtseingriffs[196] das entscheidende Kriterium ist. Je schwerwiegender bzw. intensiver der Grundrechtseingriff ist, umso höher sind die Anforderungen an die Bestimmtheit der Norm auf deren Grundlage der Eingriff vorgenommen wird.[197]

b) Anwendbarkeit der Rechtsgrundlagen für den realen Raum

Die BReg hat sich zu diesem Aspekt in der Antwort auf eine Kleine Anfrage am 14.07.2011 dahingehend geäußert, dass sie keine Notwendigkeit zur Schaffung spezieller gesetzlicher Befugnisse im Hinblick auf offene und verdeckte Ermittlungen in sozialen Netzwerken sehe, vielmehr reichten die bereits existierenden Normen (§§ 110a, 161, 163 StPO).[198] Zu dem gleichen Ergebnis kommt der Wissenschaftliche Dienst des Deutschen BT in seiner Sachstandszusammenfassung zur Nutzung von Tarnidentitäten in sozialen Netzwerken durch die Polizei und die Strafverfolgungsorgane. Laut diesen kann ein noeP auf der Grundlage der Ermittlungsgeneralklausel nach §§ 161, 163 StPO ermitteln und ein verdeckter Ermittler gemäß § 110a StPO.[199] Diesen

[192] Vgl. *Sommermann*, in: Huber/Voßkuhle, Grundgesetz, Band 2, Art. 20 GG Rn. 278.
[193] Vgl. ebd., Rn. 289.
[194] Vgl. *Sommermann*, in: Huber/Voßkuhle, Grundgesetz, Band 2, Art. 20 GG Rn. 289; *Grzeszick*, in: Herzog u.a., Maunz/Dürig, Grundgesetz Kommentar, Band III, Art. 20 GG VII Rn. 62; *Jarass*, in: Jarass/Pieroth, GG, Art. 20 GG Rn. 83.
[195] Vgl. *Grzeszick*, in: Herzog u.a., Maunz/Dürig, Grundgesetz Kommentar, Band III, Art. 20 GG VII Rn. 59.
[196] Vgl. ebd., Rn. 60.
[197] Vgl. *Jarass*, in: Jarass/Pieroth, GG, Art. 20 GG Rn. 84.
[198] Vgl. BT-Drs. 17/6587, S. 3+4.
[199] Vgl. *Wissenschaftlicher Dienst des Deutschen BT*, Nutzung von Tarnidentitäten in sozialen Netzwerken durch die Polizei und die Strafverfolgungsorgane, S. 8.

Darlegungen folgt auch die überwiegende Literatur.[200] Anhand der jeweiligen Eingriffsintensität soll im Folgenden untersucht werden, ob dieser Rechtsauffassung gefolgt werden kann.

aa) Intensität des Grundrechtseingriffs

Möchte der verdeckte personale Ermittler rein passiv Kenntnis von denjenigen Profilinhalten der Zielperson nehmen, die gemäß der durch sie vorgenommenen Privatsphäre-Einstellungen nur Mitgliedern ihres Netzwerkes offenstehen oder aber mit ihr über die Nachrichtenfunktion kommunizieren, ist es erforderlich, dass der Ermittler über ein Profil verfügt unter dem er die Anfrage stellen kann. Die Zielperson wird somit zum einen darüber getäuscht, dass es sich um einen fiktiven Account handelt und zum anderen darüber, dass der Inhaber dieses Accounts ein Mitarbeiter einer Strafverfolgungsbehörde ist. Als erster Anknüpfungspunkt zur Bestimmung der Eingriffsintensität kann daher der **Grad der Täuschung** herangezogen werden. Liest der Ermittler nur die Profilinhalte der Zielperson und durch ebendiese erstellte Beiträge mit, handelt es sich um Inhalte, die der entsprechende Nutzer grundsätzlich nicht nur einer Person, sondern mindestens allen Mitgliedern seines Netzes zur Verfügung stellen möchte. Daraus lässt sich also schließen, dass er grundsätzlich keine umfassende Vertraulichkeitserwartung hinsichtlich dieser Inhalte hegt. Gleichwohl täuscht der Ermittler die Zielperson über seine Identität. Diese ist umso größer, je umfangreicher das fiktive Profil ist. Diese Darlegungen sind bereits vom Beginn der vorliegenden Arbeit bekannt und entsprechen dem entscheidenden Abgrenzungskriterium zwischen einem verdeckten Ermittler und einem noeP – der „auf Dauer angelegten Legende“. Das Merkmal „auf Dauer angelegt“ umschreibt Anforderungen an die Qualität bzw. Substanz der Legende. Je umfangreicher diese ist, umso größer ist die Täuschung gegenüber der Zielperson und umso intensiver ist der daraus folgende Grundrechtseingriff. Schlussendlich münden diese Überlegungen in der Prüfung des – im Rahmen dieser Arbeit bereits umfassend thematisierten – Vorliegens eines schutzwürdigen Vertrauens des Betroffenen in die Identität und Motivation des

[200] Vgl. z.B. *Bruns*, in: Hannich, Karlsruher Kommentar zur Strafprozessordnung, § 110a StPO Rn. 7; *Soiné*, Personale verdeckte Ermittlungen in sozialen Netzwerken zur Strafverfolgung, NStZ 2014, 248, 249; *Singelnstein*, Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co, NStZ 2012, 593, 600; *Rosengarten/Römer*, Der „virtuelle verdeckte Ermittler“ in sozialen Netzwerken und Internetboards, NJW 2012, 1764, 1767.

Kommunikationspartners. Im Unterschied zur Entscheidung des BVerfG zur Online-Durchsuchung wird an dessen Vorliegen jedoch nicht das grundsätzliche Bestehen eines Eingriffs in das Recht auf informationelle Selbstbestimmung geknüpft, sondern vielmehr, diesem Schritt nachgelagert, die Intensität des Eingriffs bestimmt. Ein derartiges Vertrauen ist, kurz gesagt, also nicht für das „Ob“ eines Eingriffs in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG im Bereich des sozialen Online-Netzwerks von Relevanz, wohl aber für die Bestimmung des Umfangs bzw. der Intensität des Grundrechtseingriffs. Dieses Vertrauen könnte sich nach der Ausgestaltung des Profils der staatlichen Stelle richten. Gleichwohl treffen hier die gleichen Erwägungen zu, wie sie bereits in Abschnitt D, II, 1, c), aa), (2), (a) dargestellt wurden, insbesondere kann der staatliche Akteur durch die Ausgestaltung selbst beeinflussen, ob er nunmehr auf der Grundlage der Ermittlungsgeneralklausel tätig wird oder restriktivere Vorgaben gemäß einer spezielleren gesetzlichen Grundlage einzuhalten sind. Eine auf Seiten der Zielperson bestehende Leichtgläubigkeit würde dieser schlussendlich zum „Nachteil“ gereichen, da ein Eingriff in das Recht auf informationelle Selbstbestimmung an geringere gesetzliche Anforderungen geknüpft wäre. Vor dem Hintergrund der Qualität der Daten, die ein solches soziales Netzwerk enthält, die einen Rückschluss auf die Persönlichkeit des Betroffenen zulassen, ist ein Abstellen auf ein schutzwürdiges Vertrauen, das sich aus einer umfassenden virtuellen Legende des Ermittlers ergibt, jedoch nicht interessengerecht. Den Besonderheiten des sozialen Online-Netzwerks als Cyberspace im engeren Sinne würde sodann nicht ausreichend Rechnung getragen werden. Vor dem Hintergrund der Spezifika der sozialen Online-Netzwerke als erweiterter Sozialkontext dürfen also keine hohen Anforderungen an die virtuelle Legende gestellt werden, vielmehr kann für die Bewertung der Intensität des Eingriffs auf die Qualität der in dem Netzwerk enthaltenen Informationen abgestellt werden.

Aus den vorgenannten Ausführungen folgt, dass bei Vordringen des verdeckten personalen Ermittlers in den durch die Zielperson gegenüber dem Zugriff durch die (Netzwerk-)Öffentlichkeit geschützten Bereich des sozialen Online-Netzwerks stets ein intensiver Eingriff in das aus dem allgemeinen Persönlichkeitsrecht abgeleitete Recht auf informationelle Selbstbestimmung des Betroffenen vorliegt. Mithin kann dieser ausgehend vom verfassungsrechtlichen

Bestimmtheitsgrundsatzes nicht auf der Grundlage der Ermittlungsgeneralklausel gemäß §§ 161, 163 StPO erfolgen.[201]

Kann schon das passive Mitlesen zugriffseingeschränkter Inhalte in sozialen Online-Netzwerken nicht auf die Generalklausel gestützt werden, muss dies erst recht für die aktive Kommunikation mit der Zielperson gelten.

bb) Anwendbarkeit des § 110a StPO

Da die Ermittlungsgeneralklausel den Bestimmtheitsanforderungen nicht genügt, wird nunmehr untersucht, ob § 110a StPO als Rechtsgrundlage fungieren kann.

§ 110a StPO ist auf die organisierte Kriminalität zugeschnitten, sodass das vorrangige Ziel eines verdeckten Ermittlers in der realen Welt das Vordringen in das Innere einer dieser Organisationen ist.[202] Auf den virtuellen verdeckten Ermittler trifft dieses jedoch nur partiell zu. Aufgrund der Ausgestaltung der sozialen Online-Netzwerke soll dieser zum einen Informationen zur Zielperson generieren und zum anderen – im Falle eines direkten Kommunikationskontakts – eine Vertrauensbeziehung zu dieser aufbauen, um darauf aufbauend wiederum Erkenntnisse zu sammeln. Das Ermittlungsinstrument des virtuellen verdeckten Ermittlers eignet sich daher insbesondere für Konstellationen, die sich auf einen deutlich kleineren Personenkreis als organisierte Kriminalitätsstrukturen beziehen, nämlich v.a. dann, wenn sich die Ermittlungen gegen eine konkrete Person richten. Somit konvenieren die in § 110a Abs. 1 S. 1 StPO genannten Fallgruppen nicht mit dem Sinn und Zweck des Einsatzes eines virtuellen Ermittlers in sozialen Online-Netzwerken.

Die gleichen Erwägungen treffen auf die in der Vorschrift weiterhin genannten Einsatzmöglichkeiten zu, die sich auf Verbrechen beschränken. Gemäß § 12 Abs. 1 StGB sind dies Taten, die im Mindestmaß mit einer Freiheitsstrafe von einem Jahr oder darüber hinaus bedroht sind. Damit würden z.B. klassische Anlasstaten aus dem Bereich der Kinderpornographie, wie § 184b StGB, der die Verbreitung, den Erwerb und den Besitz kinderpornographischer Schriften

[201] So auch vgl. *Bauer*, Soziale Netzwerke und strafprozessuale Ermittlungen, S. 205; *Zöller*, in: Gercke u.a., Heidelberger Kommentar, Strafprozessordnung, § 163 StPO Rn. 12. AA wohl: *Henrichs*, Ermittlungen im Internet, Kriminalistik 2011, 622, 626.

[202] Vgl. *Gercke*, in: Gercke u.a., Heidelberger Kommentar, Strafprozessordnung, § 110a StPO Rn. 1.

unter eine Freiheitsstrafe von drei Monaten bis zu fünf Jahren stellt, nicht erfasst, da es sich hier um ein Vergehen gemäß § 12 Abs. 2 StGB handelt. *Soiné* merkt zur scheinbaren Lösung dieser Regelungslücke an, dass solchen Taten in einer Vielzahl von Fällen z.B. ein sexueller Missbrauch oder aber eine sexuelle Nötigung zugrunde liege.[203] Beides ist als Verbrechen zu qualifizieren, womit der verdeckte personale Ermittler in diesen Fällen die Voraussetzungen des § 110a Abs. 1 StPO erfüllen würde. Die Krux dieser Sichtweise besteht jedoch darin, dass ein solches Grunddelikt eben nicht stets vorliegen wird, sodass ein virtueller verdeckter personaler Ermittler in diesen Konstellationen nicht in einem sozialen Online-Netzwerk tätig werden dürfte. Darüber hinaus wären auch, wie *Bauer* zutreffend feststellt, typische Delikte der Computerkriminalität nicht erfasst, wie z.B. §§ 185 ff., 263a oder aber 303b StGB.[204] Eine Beschränkung des Einsatzes eines virtuellen personalen verdeckten Ermittlers auf die Aufklärung von Verbrechen würde somit die Einsatzszenarien dieses Ermittlungsinstruments – und letztlich dessen Relevanz – stark einschränken.

Dennoch müssen die Anwendungsfälle des virtuellen verdeckten Ermittlers aufgrund der Intensität des Grundrechtseingriffs Einschränkungen unterliegen. *Ihwas* nimmt in seinem Gesetzgebungsvorschlag, der sich einzig auf Ermittlungen in sozialen Netzwerken bezieht, auf Straftaten von erheblicher Bedeutung Bezug und zählt dazu insbesondere solche nach § 100a Abs. 2 StPO aF. Darüber hinaus lässt er es jedoch auch ausreichen, wenn eine Straftat mittels Kommunikation begangen wurde.[205] Darunter fallen sodann sämtliche Straftaten, die der Computerkriminalität im weiten Sinne zuzuordnen sind, da sich die zuvor genannte Erheblichkeitsschwelle nicht auf diese Fallgruppe erstreckt. Eine derart weite Regelung entspricht jedoch aufgrund der Tiefe des Grundrechtseingriffs nicht dem verfassungsrechtlichen Bestimmtheitsgrundsatz.

[203] Vgl. *Soiné*, Verdeckte Ermittler als Instrument zur Bekämpfung von Kinderpornographie im Internet, NStZ 2003, 225, 227.
[204] Vgl. *Bauer*, Soziale Netzwerke und strafprozessuale Ermittlungen, S. 210.
[205] Vgl. *Ihwas*, Strafverfolgung in sozialen Netzwerken, Facebook und Co. als moderne Ermittlungswerkzeuge, S. 172.

Bauer hingegen schlägt an diesen Gesetzgebungsvorschlag anknüpfend vor, einen virtuellen verdeckten Ermittler „zur Aufklärung einer Straftat von erheblicher Bedeutung, die mittels Kommunikation begangen worden ist“[206], zum Einsatz kommen zu lassen, „wenn die besondere Bedeutung der Tat den Einsatz gebietet“.[207] Im Gegensatz zu *Ihwas* beinhaltet sein Vorschlag die oben monierte Erheblichkeitsschwelle und beschränkt sich nicht auf soziale Netzwerke, er inkludiert jedoch nicht zwangsläufig die Katalogtaten nach § 100a Abs. 2 StPO. Auslegungsschwierigkeiten wirft zudem die gleichzeitige Verwendung der Begrifflichkeiten „Straftat von erheblicher Bedeutung“ und „besondere Bedeutung der Tat“ auf. Zutreffend stellt *Köhler* fest, dass sich diese Formulierungen in keinem sachlichen Antagonismus befinden würden und ihnen mithin kein über die jeweils andere Begrifflichkeit hinausgehender Bedeutungsgehalt zukomme.[208] Die gleichzeitige Verwendung beider Termini stiftet daher Rechtsunsicherheit.[209]

§ 110a Abs. 2 S. 1 StPO enthält eine Legaldefinition des verdeckten Ermittlers. Laut dieser ist letzterer ein Beamter des Polizeidienstes, der unter einer ihm verliehenen, auf Dauer angelegten, veränderten Identität (Legende) ermittelt. Diese Definition kann jedoch nicht analog auf den verdeckten Ermittler in sozialen Netzwerken angewendet werden, da es für die Grundrechtsbetroffenheit nicht auf das Kriterium „auf Dauer angelegt“, in der Interpretation als qualitative Anforderung an die Legende, ankommt. Wie dargestellt, liegt stets ein intensiver Eingriff in das Recht auf informationelle Selbstbestimmung vor, wenn sich der staatliche Akteur über eine Vernetzungsanfrage Zugang zum nicht-netzwerköffentlichen Teil des Profils der Zielperson verschafft. Auf die Qualität bzw. Substanz der virtuellen Legende kommt es dabei nicht an. Entscheidend ist vielmehr, dass die Zielperson täuschungsbedingt persönliche Daten an den Ermittler weitergibt. Mithin ist die bestehende Legaldefinition zu eng, es bedarf daher einer separaten Begriffsbestimmung für diese spezielle

[206] *Bauer*, Soziale Netzwerke und strafprozessuale Ermittlungen, S. 213.
[207] Ebd.
[208] Vgl. *Köhler*, in: Meyer-Goßner/Schmitt, Strafprozessordnung, § 110a StPO Rn. 13, aA *Bruns*, in: Hannich, Karlsruher Kommentar zur Strafprozessordnung, § 110a StPO Rn. 21, der ausführt, dass beide Begrifflichkeiten nicht zwangsläufig bedeutungsidentisch sein müssten.
[209] Wird gesetzesvergleichend z.B. § 9a BVerfSchG betrachtet, fällt auf, dass dieser die Formulierung „Bestrebungen von erheblicher Bedeutung“ wählt. Eine weitere Einschränkung der Befugnisnorm durch die Begrifflichkeit „besondere Bedeutung“ findet indes nicht statt.

Art von Ermittler. In diesem Zusammenhang ist also sowohl *Ihwas*[210] als auch *Bauer*[211] zuzustimmen, die beide einen eigenen Vorschlag in ihren Darlegungen unterbreiten. Im Gegensatz zu *Bauer* erwähnt *Ihwas* explizit im Rahmen der Definition den Grund, aus dem sich der Bedarf einer solchen Legende ergibt – nämlich die „Wahrnehmung nicht öffentlich zugänglicher Daten in sozialen Netzwerken“[212]. Diese Ergänzung ist vor dem Hintergrund wichtig, als dass sich die Notwendigkeit einer derart bestimmten Rechtsgrundlage nur auf den Einsatz in nicht öffentlichen Bereichen sozialer Netzwerke bezieht. *Bauer* führt dies hingegen erst im Rahmen der Darlegung der Befugnisse des verdeckten virtuellen Ermittlers in Abs. 3 S. 1 seines Gesetzesentwurfs auf. Aus Klarstellungsgründen, v.a. auch um den diversifizierten Privatsphäre-Einstellungen in sozialen Online-Netzwerken gerecht zu werden, wäre jedoch darüber hinaus eine Legaldefinition des Begriffs „nicht öffentlich“ (*Ihwas*) oder aber „nicht allgemein zugänglich“ (*Bauer*) im Kontext dieser Netzwerke zielführend.[213]

Letztlich lassen sich die Unterschiede hinsichtlich der Definitionen v.a. auf die Weite des Regelungsgegenstandes zurückführen. *Bauer* wählt einen breiteren Regelungsgegenstand, indem er den Einsatz virtueller verdeckter Ermittler in den Kommunikationsdiensten des Cyberspace regeln möchte, soziale Online-Netzwerke sind sodann nur ein Unterszenario seines umfassenderen Entwurfs.

III. Chatforen

Als weiteres Einsatzszenario soll nun der Einsatz eines personalen verdeckten Ermittlers in Chatforen auf seine Grundrechtsrelevanz hin untersucht werden. Bezüglich der theoretischen Ausführungen zu den einzelnen Grundrechten kann auf das bisher Gesagte verwiesen werden.

---

[210] Vgl. *Ihwas*, Strafverfolgung in sozialen Netzwerken, Facebook und Co. als moderne Ermittlungswerkzeuge, S. 172.
[211] *Bauer*, Soziale Netzwerke und strafprozessuale Ermittlungen, S. 213.
[212] *Ihwas*, Strafverfolgung in sozialen Netzwerken, Facebook und Co. als moderne Ermittlungswerkzeuge, S. 172.
[213] Vgl. Fn. 114 zu § 12 Abs. 3a SÜG, der sich auch auf den Zugriff nicht-öffentlich sichtbarer Teile sozialer Netzwerke bezieht und ebenfalls einer Definition schuldig bleibt. Auch hier wäre eine Klarstellung des Gesetzgebers wünschenswert.

1. Grundrechtsrelevanz

a) Fernmeldegeheimnis gemäß Art. 10 Abs. 1 GG

Ein Eingriff in das Fernmeldegeheimnis nach Art. 10 Abs. 1 GG ist zu verneinen. Im Falle der Nutzung einer fiktiven Identität durch den staatlichen Akteur wird nicht das Vertrauen in das Kommunikationsmedium als solches tangiert, sondern in die Wahrhaftigkeit des Chatpartners. Eben dieses Vertrauen wird jedoch nicht durch Art. 10 Abs. 1 GG geschützt, sodass eine Verletzung dieses Grundrechts in dieser Konstellation ausscheidet.

Im Falle der Übernahme eines bereits existierenden Accounts mit Einverständnis des Inhabers scheidet ein Eingriff in Art. 10 Abs. 1 GG ebenfalls aus, da der Ermittler mit Einverständnis des Account-Inhabers in den Kommunikationsvorgang einbezogen wurde. Da die Gefährdungslage in dieser Konstellation keine kommunikationsbezogene ist, genügt das Einverständnis nur eines Teilnehmers an der Kommunikation, um den Grundrechtseingriff auszuschließen.

b) Wohnungsgrundrecht gemäß Art. 13 GG (virtuelle Wohnung)

Im Gegensatz zu sozialen Online-Netzwerken zeichnen sich Chatforen gerade durch eine signifikant geringere Anbindung an das reale Leben aus. In der Regel werden Pseudonyme verwendet, deren Zweck es ist, eine Distanz zwischen der Klaridentität und der virtuellen Realität zu erzeugen, die eine Identifizierung des Account-Inhabers verhindert. Wie in Abschnitt C, III, 2, b) dargestellt, ist z.B. für das Verfassen von Beiträgen auf einem Imageboard auf der Plattform 8kun noch nicht einmal ein Nickname erforderlich. Beiträge können ohne eine irgendwie geartete namentliche Zuordnung veröffentlicht werden. Primärer Sinn und Zweck dieser Foren ist es, mit unbekannten Personen in Kontakt zu treten und zu diesen eine Kommunikationsbeziehung aufzubauen. Damit ist eine Spiegelbildlichkeit der Kontakte, wie es für soziale Online-Netzwerke typisch ist, in der Regel zu verneinen. Chatforen fungieren nicht als erweiterter Sozialkontext. Vielmehr besteht die Möglichkeit, in Gänze anonym Kommunikationsvorgänge anzustoßen und auszuleben, die von der realen Existenz abgekoppelt sind. Eine Verschmelzung der realen und virtuellen Welt, wie es für soziale Online-Netzwerke charakteristisch ist, findet mithin nicht statt. Daher scheidet unter diesen Rahmenbedingungen erst recht das

Vorliegen einer virtuellen Wohnung aus, sodass der verdeckte personale Ermittler ebenfalls durch sein Handeln nicht in das Wohnungsgrundrecht aus Art. 13 GG eingreift.

c) Allgemeines Persönlichkeitsrecht gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

aa) Recht auf informationelle Selbstbestimmung

Auf der Grundlage des Rechts auf informationelle Selbstbestimmung hat jeder das Recht, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu entscheiden. Bezüglich Chatforen greift jedoch, aufgrund der fehlenden Verknüpfung zwischen diesen und der realen Welt, die Einschränkung des Schutzbereichs, die das BVerfG in seiner Entscheidung zur Online-Durchsuchung statuiert hat. Laut diesem ist ein Eingriff in das Recht auf informationelle Selbstbestimmung in den Fällen, in denen eine staatliche Stelle unter Legende in eine Kommunikationsbeziehung zu einem Grundrechtsberechtigten tritt, nur dann anzunehmen, wenn der staatliche Akteur ein schutzwürdiges Vertrauen des Partners in seine Identität und Motivation ausnutzt.[214] Solch eine Schutzwürdigkeit ist nach Auffassung des BVerfG an das Vorliegen von Prüfmechanismen hinsichtlich der genannten Parameter geknüpft.[215] Wie auch in sozialen Online-Netzwerken findet eine Überprüfung der Klaridentität grundsätzlich nicht statt. In vielen Fällen ist – wenn überhaupt – einzig eine gültige E-Mail-Adresse erforderlich. Sofern es sich um Foren im Darknet handelt, würde eine derartige Überprüfung auch gerade dem Sinn und Zweck des Darknets widersprechen, in welchem möglichst anonym gesurft werden soll. Somit besteht auf Seiten des Host-Providers kein Überprüfmechanismus.

Da die Teilnehmer an einem Chatforum in der Regel auch nicht über ihren Account ergänzende Profile verfügen, die persönliche Daten enthalten, kann auch aus diesen Umständen bzw. Indizien kein schutzwürdiges Vertrauen in die Identität des Kommunikationspartners resultieren. Somit besteht auf Seiten der Chatforen-Teilnehmer kein Überprüfmechanismus, der ein schutzwürdiges Vertrauen in die Identität und Motivation begründen könnte. Mithin liegt für den Fall, dass der Ermittler einen fiktiven Account verwendet oder aber die

[214] Vgl. BVerfG, NJW 2008, 822, 836.
[215] Vgl. ebd.

Zugangsdaten eines Dritten verwendet, kein Eingriff in das Recht auf informationelle Selbstbestimmung vor.

An dieser Stelle könnte jedoch eine einzelfallbezogene Betrachtung gefordert werden. In den Fällen, in denen bereits eine längere Kommunikationsbeziehung zwischen den Teilnehmern des Chatforums bestand, könnte dadurch ein Vertrauensverhältnis zwischen den Chatpartnern entstanden sein. Gleichwohl bezieht sich dieses sodann grundsätzlich nicht auf die Identität des Chatpartners, da Wesen eines Chatforums gerade die Anonymität der Kommunikanten ist. Mithin scheidet auch in diesem Ermittlungsszenario ein Eingriff in das Recht auf informationelle Selbstbestimmung aus.

Ein derartiger Eingriff ist jedoch dann zu bejahen, wenn sich die Chatpartner auch aus dem realen Leben kennen, sodass sowohl eine reale als auch eine virtuelle Kommunikation vorliegt. Eine solche Verknüpfung zwischen der realen Welt und dem hier zu untersuchenden Cyberspace im engeren Sinne, kann sich z.B. aus zusätzlichen Videotelefonaten ergeben. In diesen Fällen vertrauen die Kommunikationspartner auf die Identität des jeweils anderen, sodass ein Eingriff in das Recht auf informationelle Selbstbestimmung zu bejahen wäre.[216] Diese Überlegungen machen deutlich, dass an dieser Stelle also keine pauschale Betrachtung erfolgen kann, sondern jeweils der Einzelfall begutachtet werden muss.

bb) Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme

Schlussendlich ist auch ein Eingriff in das IT-Grundrecht abzulehnen. Eine Infiltration eines informationstechnischen Systems liegt nicht vor, da lediglich partiell Daten erhoben werden. Dies geschieht auch nur dann, wenn der Chatpartner diese Inhalte willentlich mit den Teilnehmern des Chatforums teilt. Diesbezüglich greifen die gleichen Erwägungen wie im Rahmen sozialer Online-Netzwerke.

[216] In derartigen Fällen ließe sich aufgrund der Erwägungen in Abschnitt D, II, 1, c), aa), (2), (a) auch vertreten, eine solche Schutzbereichseinschränkung erst gar nicht zu fordern, da eine Verbindung zwischen dem virtuellen Chatforum und der realen Welt vorliegt, sodass auf das Vorliegen von externen Überprüfungsmechanismen verzichtet werden kann.

2. Anwendbarkeit der Rechtsgrundlagen für den realen Raum

Ein verdeckter personaler Ermittler greift somit, sofern er in einem Chatforum ermittelt, in den meisten Fällen nicht in Grundrechte der betroffenen Zielperson ein. Derartige Maßnahmen können daher grundsätzlich auf der Grundlage der Aufgabenzuweisung an die Polizei erfolgen, in diesem Zusammenhang genügt daher § 163 Abs.1 S. 1 StPO als Rechtsgrundlage. Ist ein Grundrechtseingriff hingegen aus den oben dargestellten Erwägungen zu bejahen, könnte dieser nur dann auf die Ermittlungsgeneralklausel gemäß §§ 161, 163 StPO gestützt werden, wenn die Intensität des Eingriffs als gering zu beurteilen wäre. Erstreckt sich die Kommunikation nicht nur auf den virtuellen Bereich, sondern finden z.B. auch Videotelefonate statt, die die Identität des Gegenübers offenbaren, entsteht beim nicht-staatlichen Akteur des Chatforums zunächst ein Vertrauen in die Identität des Chatpartners, das durch letzteren schlussendlich enttäuscht wird. Aufgrund der Tatsache, dass die Kommunikation über ein Chatforum in diesen Fällen nur als Ermittlungsannex gesehen werden kann und sich auch das Erfordernis einer Rechtsgrundlage nur aus der Verknüpfung dieses Annexes mit einer Ermittlungsmaßnahme im realen Raum ergibt, kann für eine Abgrenzung zwischen der Ermittlungsgeneralklausel und § 110a StPO zur Bestimmung der Eingriffsintensität auf die Qualität der Legende abgestellt werden. Gleichwohl muss eine vollständige Anwendung des § 110a StPO, aufgrund der fehlenden Konvergenz mit den praktisch relevanten Einsatzszenarien des personalen verdeckten Ermittlers im Cyberspace, ausscheiden.

Zusammenfassend ist somit im Hinblick auf die Durchführung personaler verdeckter Ermittlungsmaßnahmen in Chatforen nur in wenigen Fällen eine Rechtsgrundlage in Form einer Befugnisnorm erforderlich. Eine direkte Anwendung des § 110a StPO muss jedoch aus den oben dargestellten Erwägungen ausscheiden, sodass es einer eigenständigen Rechtsgrundlage bedarf. In diesem Sinne ist also *Bauer* zuzustimmen, der seinen Entwurf einer Rechtsgrundlage nicht nur auf soziale Online-Netzwerke beschränkt. [217]

[217] Vgl. *Bauer*, Soziale Netzwerke und strafprozessuale Ermittlungen, S. 213.

V. IT-SiG 2.0: Verpflichtende Herausgabe von Zugangsdaten auf der Grundlage eines neuen § 163g StPO

1. Regelungsgegenstand und Hintergründe

Aus dem Referentenentwurf des BMI eines IT-SiG 2.0 vom 27.03.2019 ergibt sich ein weiteres Szenario des Einsatzes eines verdeckten personalen Ermittlers im Cyberspace. Nach dem Gesetzesentwurf soll ein neuer § 163g in die StPO eingefügt werden, der wie folgt formuliert wird:

> *„Begründen bestimmte Tatsachen den Verdacht, dass jemand Täter oder Teilnehmer einer Straftat im Sinne von § 100g Absatz 1 StPO ist, so dürfen die Staatsanwaltschaft sowie die Behörden und Beamten des Polizeidienstes auch gegen den Willen des Inhabers auf Nutzerkonten oder Funktionen, die ein Anbieter eines Telekommunikations- oder Telemediendienstes dem Verdächtigen zur Verfügung stellt und mittels derer der Verdächtige im Rahmen der Nutzung des Telekommunikations- oder Telemediendienstes eine dauerhafte virtuelle Identität unterhält, zugreifen. Sie dürfen unter dieser virtuellen Identität mit Dritten in Kontakt treten. Der Verdächtige ist verpflichtet, die zur Nutzung der virtuellen Identität erforderlichen Zugangsdaten herauszugeben. § 95 Absatz 2 gilt entsprechend mit der Maßgabe, dass die Zugangsdaten auch herauszugeben sind, wenn sie geeignet sind, eine Verfolgung wegen einer Straftat oder einer Ordnungswidrigkeit herbeizuführen. Jedoch dürfen die durch Nutzung der Zugangsdaten gewonnenen Erkenntnisse in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Verdächtigen oder einen in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen des Verdächtigen nur mit Zustimmung des Verdächtigen verwendet werden.“*[218]

Das BMI bezieht sich in seiner Gesetzesbegründung explizit auf Handelsplattformen im Darknet und solche zur Verbreitung von Kinderpornographie. In diesen Umgebungen sei das Vertrauen in einen bestimmten Kommunikationspartner der entscheidende Faktor, sodass es für ein erfolgsversprechendes Ermittlungshandeln unerlässlich sei, auf bereits bestehende Accounts zurückzugreifen.[219] Gerade neuen Accounts werde zunächst einmal Misstrauen entgegengebracht, während solchen, die schon über Jahre hinweg aktiv seien ein umso größeres Vertrauen entgegengebracht werde.[220] Daraus folgt der Entwurf, dass der Zugriff auf die virtuelle Identität des Beschuldigten „eine der wichtigsten Ermittlungsmethoden“[221] sei. Da dieses Szenario derzeit nicht explizit gesetzlich geregelt sei, sieht das BMI hier einen Regelungsbedarf, den es mit einem neuen § 163g StPO heilen möchte.[222]

Fraglich ist jedoch zunächst, was unter Telekommunikations- und Telemediendiensten zu verstehen ist. Eine genaue Definition oder aber einen Verweis

---

[218] *BMI*, Referentenentwurf eines IT-SiG 2.0, S. 32.
[219] Vgl. ebd., S. 86.
[220] Vgl. ebd., S. 87.
[221] Ebd., S. 87.
[222] Vgl. ebd., S. 87.

in andere Gesetze zur Konkretisierung bleiben der Wortlaut der Norm und auch die Gesetzesbegründung schuldig. *Oehmichen/Weißenberger* vermuten an dieser Stelle – aufgrund fehlender entgegenstehender gesetzlicher Anhaltspunkte wohl zu Recht –, dass die Definitionen aus § 3 Nr. 6 TKG und § 2 Nr. 1 TMG heranzuziehen seien.[223] Telemediendienste im Sinne des § 163g StPO sind daher wohl u.a. soziale Online-Netzwerke, wie z.B. LinkedIn oder Facebook oder aber Chatforen.[224] Wenngleich sich die Gesetzesbegründung nur auf das Darknet bezieht, lässt sich eine derartige Beschränkung auf diesen Teil des Cyberspace dem Wortlaut des Gesetzes nicht entnehmen, sodass erst einmal davon ausgegangen werden muss, dass auch Telemediendienste des offenen Teils des Cyberspace erfasst werden sollen.

2. Grundrechtsrelevanz

a) Auf Seiten des Beschuldigten

aa) Selbstbelastungsfreiheit gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Nach S. 3 des Regelungsentwurfs soll der Beschuldigte dazu verpflichtet werden, die Zugangsdaten zur Nutzung seiner virtuellen Identität an die Strafverfolgungsbehörden herauszugeben. Aus dem allgemeinen Persönlichkeitsrecht gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG[225] wird für das Strafverfahren der Grundsatz abgeleitet, dass niemand gezwungen werden darf sich selbst zu belasten („nemo tenetur se ipsum accusare“). Die Selbstbelastungsfreiheit ist als eines der Grundprinzipien eines rechtsstaatlichen Verfahrens im Strafrecht einzuordnen.[226] Darüber hinaus ist diese ein Bestandteil des in Art. 6 Abs. 1 S. 1 EMRK[227] geregelten Grundsatzes auf Gewährleistung eines fairen Verfahrens (fair trial). Im Kern geht es um die Achtung des durch den Beschuldigten artikulierten Willens, zu schweigen.[228]

---

[223] Vgl. *Oehmichen/Weißenberger*, Digitaloffensive im Strafrecht, Verbesserte Bekämpfung von Cyberkriminalität durch das IT-Sicherheitsgesetz 2.0?, KriPoZ 2019, 174, 179.

[224] Vgl. *Spindler*, in: Spindler/Schmitz/Liesching, Telemediengesetz, § 1 TMG Rn. 78.

[225] Mitunter wird als Grundlage des Grundsatzes der Selbstbelastungsfreiheit neben dem allgemeinen Persönlichkeitsrecht auch das Rechtsstaatsprinzip gemäß Art. 20 Abs. 3 GG genannt (z.B. *Jarass*, in: Jarass/Pieroth, GG, Art. 2 GG Rn. 68a).

[226] Vgl. BGH, Urteil vom 27. Juni 2013 – 3 StR 435/12 –, BGHSt 58, 301-309, juris, Rn. 8.

[227] Die EMRK ist ein völkerrechtlicher Vertrag zwischen allen 47 Mitgliedstaaten des Europarates. Formell hat sie den Rang eines einfachen Bundesgesetzes, wird jedoch, aufgrund des Grundsatzes der Völkerrechtsfreundlichkeit des GG, im Rahmen der Auslegung von Grundrechten und anderen Gesetzen herangezogen (vgl. *Schmitt*, in: Meyer-Goßner/Schmitt, Strafprozessordnung, Anhang 4, Vorbemerkungen Rn. 1+ 4).

[228] Vgl. EGMR, NJW 2010, 213, 215.

Im Hinblick darauf, dass § 163g S. 3 StPO die Verpflichtung des Beschuldigten zur Herausgabe der Zugangsdaten zu seiner virtuellen Identität regelt, ist hierin ein Verstoß gegen den Grundsatz der Selbstbelastungsfreiheit zu sehen. Schlussendlich können die Ermittler durch die verpflichtende Herausgabe der Zugangsdaten zum einen auf die Inhalte des bestehenden Accounts zugreifen und zum anderen unter Nutzung der virtuellen Identität des Beschuldigten mit Dritten in Kontakt treten. Dadurch können sie wesensimmanent an Informationen gelangen, die den Beschuldigten belasten. Der Gesetzgeber versucht diesen Verstoß durch Einfügung des S. 5 zu heilen, indem er festlegt, dass eine Verwendung der so generierten Erkenntnisse in einem gegen den Verdächtigen geführten Strafverfahren nur mit dessen Zustimmung erfolgen dürfe. Aus der Gesetzesbegründung ergibt sich, dass hier eine Parallelregelung zu § 97 Abs. 1 S. 3 InsO geschaffen werden sollte, der den Schuldner vor einer strafrechtlichen Verfolgung von Taten, die nur aufgrund seiner Mitwirkung aufgedeckt werden, schützen soll.[229] Im Rahmen des § 97 Abs. 1 InsO ist weitestgehend anerkannt, dass durch die Nutzung des Wortes „verwenden“ ein umfassendes Verwendungsverbot geregelt werden soll, das neben einem Verwertungsverbot auch eventuelle Fernwirkungen mit einschließt. Dies bedeutet, dass die Auskünfte auch nicht als Basis für die Durchführung von Ermittlungen zur Auffindung von anderweitigen selbstständigen Beweismitteln verwendet werden dürfen.[230] Vor diesem Hintergrund wirft jedoch die Gesetzesbegründung Schwierigkeiten auf. Während es im Insolvenzrecht unstreitig ist, dass sich das Verwendungsverbot auch auf die Tat bezieht, die Anlass für die Ermittlungen gegeben hat, lässt der Referentenentwurf zum IT-SiG 2.0 anderes vermuten. Dieser spricht davon, dass der Nutzer der virtuellen Identität davor geschützt werden soll, „aufgrund von durch den Mitwirkungsakt ggf. aufgedeckter weiterer Straftaten verfolgt zu werden“[231]. Diese Formulierung ist missverständlich, lässt sie doch vermuten, dass sich das Verwendungsverbot eben nicht auf die Anlasstat, sondern ausschließlich auf weitere Straftaten bezieht. Gleichzeitig nennt der Gesetzesentwurf jedoch auch § 97 Abs. 1 InsO als Beispiel für die im IT-SiG 2.0 getroffene Regelung. Diese missverständlichen und

[229] Vgl. *BMI*, Referentenentwurf eines IT-SiG 2.0, S. 88.
[230] Vgl. *Werner*, in: Fridgen/Geiwitz/Göpfert, BeckOK InsO, § 97 InsO Rn. 17; *Stephan*, in: Stürner/Eidenmüller/Schoppmeyer, Münchener Kommentar zur Insolvenzordnung, Band 2, § 97 InsO Rn. 18.
[231] *BMI*, Referentenentwurf eines IT-SiG 2.0, S. 88.

sich widersprechenden Darlegungen führen dazu, dass der Wille des Gesetzgebers nicht zweifelsfrei ermittelt werden kann. Betrachtet man ergänzend den vorgeschlagenen Wortlaut des § 163g S. 5 StPO, der weiter gefasst von einem „Strafverfahren gegen den Verdächtigen“ spricht, lässt dies eher auf einen tatsächlich gewollten Gleichlauf zu § 97 Abs. 1 S. 3 InsO schließen.

Festzuhalten bleibt daher, hinsichtlich der Grundrechtsrelevanz der verpflichtenden Herausgabe der Zugangsdaten für sich betrachtet, dass zweifellos ein Eingriff in die Selbstbelastungsfreiheit gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und den Grundsatz des fairen Verfahrens gemäß Art. 6 Abs. 1 S. 1 EMRK vorliegt. Gleichwohl kann dieser durch einen in seiner Klarheit nachzufassenden S. 5 geheilt werden.

bb) Recht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Durch die verpflichtende Herausgabe der Zugangsdaten – und dem darauf aufbauenden Zugriff auf die virtuelle Identität des Beschuldigten – könnte in das Recht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts eingegriffen werden. Gemäß § 163g S. 1 StPO soll den Strafverfolgungsbehörden erlaubt werden, auf Nutzerkonten oder Funktionen zuzugreifen, die durch einen Anbieter eines Telekommunikations- oder Telemediendienstes zur Verfügung gestellt werden. Wie bereits in Abschnitt C, I, 3 dargestellt, stellen die sozialen Online-Netzwerke einen erweiterten Sozialkontext dar und vermitteln ein umfassendes Bild von der Persönlichkeit des Account-Inhabers, sodass ein Grundrechtseingriff zu bejahen ist.

Ergänzend sei an dieser Stelle angemerkt, dass der Gesetzeswortlaut in S. 1 von einem Unterhalten einer virtuellen Identität spricht. Die Verwendung dieser Formulierung suggeriert eine gewisse Selbstständigkeit im Sinne einer Abgrenzbarkeit dieser Identität von der realen. Genau das ist aber nicht stets der Fall, v.a. nicht in Bezug auf soziale Online-Netzwerke. Damit konveniert der Begriff in seiner hier recht pauschalen Verwendung nicht mit den tatsächlichen Rahmenbedingungen des Cyberspace. Der Gesetzesentwurf nebst seiner Begründung bleibt zudem einer Definition dieses Begriffs schuldig; andere nationale Gesetze enthalten eine solche Formulierung nicht, sodass auch diese nicht im Rahmen der Auslegung herangezogen werden können.

Im Hinblick auf die Nutzung eines Chat-Accounts in solchen Chatforen, die im Rahmen dieser Arbeit begutachtet wurden, läge wohl kein Eingriff in das Recht auf informationelle Selbstbestimmung des Beschuldigten vor, da diese in der Regel keine persönlichen Daten enthalten. Es wird jedoch zumindest in das Auffanggrundrecht der allgemeinen Handlungsfreiheit nach Art. 2 Abs. 1 GG eingegriffen.

b) Auf Seiten der weiteren Kommunikationsteilnehmer

Da die Strafverfolgungsbehörden gemäß § 163g S. 2 StPO unter der virtuellen Identität des Beschuldigten mit Dritten in Kontakt treten dürfen, ist auch im Hinblick auf diesen Personenkreis die Grundrechtsrelevanz zu beurteilen. Die Gesetzesbegründung lehnt einen Eingriffscharakter einer solchen Nutzung gegenüber dem Kommunikationspartner ab. Es liege kein Eingriff in das Fernmeldegeheimnis nach Art. 10 Abs. 1 GG vor, da dieser nicht das personengebundene Vertrauen im Hinblick auf den Kommunikationspartner schütze. Ein Eingriff in das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG wird mit Hinweis auf die fehlenden Überprüfungsmechanismen, die für die Entstehung eines schutzwürdigen Vertrauens in die Identität und Motivation des Partners erforderlich seien, ebenfalls abgelehnt.[232] Im Folgenden werden diese rechtlichen Erwägungen gewürdigt.

aa) Fernmeldegeheimnis gemäß Art. 10 Abs. 1 GG

Werden die in Abschnitt D, II, 1, a), dd) dargestellten Erwägungen zugrunde gelegt, stellt die Einbeziehung eines Dritten in den Kommunikationsvorgang ohne Kenntnis des Kommunikationspartners einen Eingriff in das Fernmeldegeheimnis gemäß Art. 10 Abs. 1 GG dar. Ein solcher kann jedoch entfallen, wenn wirksam auf den Schutz durch dieses Grundrecht verzichtet wurde (Grundrechtsverzicht). Es kann an dieser Stelle dahinstehen, ob ein solcher Verzicht im Rahmen des Art. 10 Abs.1 GG wirksam durch nur einen Kommunikationspartner erklärt werden kann oder ob beide Teilnehmer auf den Grundrechtsschutz verzichten müssen, da weder der Kommunikationspartner noch der Beschuldigte wirksam einen derartigen Verzicht erklärt haben. Der Kommunikationspartner weiß nicht, dass jemand Drittes den Account des anderen übernommen hat, daher kann ersterer mangels Kenntnis nicht wirksam auf

[232] Vgl. *BMI*, Referentenentwurf eines IT-SiG 2.0, S. 87.

sein Grundrecht verzichten. In Betracht kommt daher einzig ein Verzicht durch den Beschuldigten selbst. Ein solcher muss jedoch freiwillig erfolgen.[233] Nach § 163g StPO soll der Beschuldigte jedoch gesetzlich dazu verpflichtet werden, seine Zugangsdaten zur Nutzung seiner virtuellen Identität herauszugeben – von einer freiwilligen Entscheidung zur Einbeziehung des staatlichen Akteurs in den Kommunikationsvorgang kann also gerade nicht die Rede sein. Vor dem Hintergrund dieser Überlegungen kann der Gesetzesbegründung an dieser Stelle nicht gefolgt werden, da diese einen Eingriff in Art. 10 Abs. 1 GG durch die Nutzung eines übernommenen Accounts gegenüber dem Kommunikationsteilnehmer grundsätzlich verneint.[234]

bb) Recht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Im Hinblick auf einen Eingriff in das Recht auf informationelle Selbstbestimmung kann der pauschalen Festlegung des Gesetzesentwurfs so nicht zugestimmt werden. In seiner Undifferenziertheit verkennt er, dass es Szenarien geben kann, in denen ein schützenswertes Vertrauen sehr wohl zu bejahen ist. Dies betrifft v.a. Konstellationen, in denen bereits bestehende reale Kommunikationen in den virtuellen Raum übertragen werden oder aber beide Sphären, z.B. durch ergänzende Videotelefonate, miteinander vermischt werden[235], es also an einer klaren lokalen Abgrenzbarkeit der Kommunikation mangelt.

Bezüglich sozialer Online-Netzwerke ist darüber hinaus das oben Gesagte zu berücksichtigen. Das restriktive Schutzbereichsverständnis des Rechts auf informationelle Selbstbestimmung, das ein derartiges schutzwürdiges Vertrauen fordert, findet auf diesen Cyberspace im engeren Sinne keine Anwendung, sodass im Rahmen der Nutzung eines bestehenden Accounts in sozialen Netzwerken zur Kommunikation mit einem Dritten stets ein Eingriff in dieses Grundrecht anzunehmen ist.

---

[233] Vgl. *Jarass*, in: Jarass/Pieroth, GG, Vorb. Rn. 36.

[234] Vgl. *Oehmichen/Weißenberger*, Digitaloffensive im Strafrecht, Verbesserte Bekämpfung von Cyberkriminalität durch das IT-Sicherheitsgesetz 2.0?, KriPoZ 2019, 174, 181.

[235] Vgl. *Ihwas*, „Die digitale Unterwelt“ – Strafprozessuale Ermittlungsmöglichkeiten im Darknet, WiJ 2018, 138, 144.

Vor dem Hintergrund dieser Ausführungen – und des Eingriffs in das Fernmeldegeheimnis auf Seiten des Kommunikationspartners des Beschuldigten – bedarf es also durchaus einer speziellen gesetzlichen Grundlage für die Nutzung eines bereits bestehenden Accounts durch die Strafverfolgungsbehörden.

3. Zusammenfassende Betrachtung

Es kann zusammengefasst werden, dass sowohl der reine Regelungsentwurf als auch die Gesetzesbegründung noch einige Unschärfen aufweisen, die es im weiteren Verlauf des Gesetzgebungsverfahrens, insbesondere im Rahmen der Ressortabstimmungen, zu bereinigen gilt.

Es bleibt festzuhalten, dass im Hinblick auf den Verdächtigen grundsätzlich Eingriffe in das Recht auf Selbstbelastungsfreiheit nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, den Grundsatz des fairen Verfahrens aus Art. 6 Abs. 1 S. 1 EMRK und, je nach Bezugsmedium, in das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG vorliegen. Diese sind auch nicht als gering zu bewerten, sodass ein Rückgriff auf die Ermittlungsgeneralklausel gemäß §§ 161, 163 StPO nicht erfolgen kann. Somit bedarf es einer Rechtsgrundlage, die bezüglich ihrer Bestimmtheit dieser durchaus als erheblich zu bewertenden Intensität des Grundrechtseingriffs Rechnung trägt. Diese Anforderungen erfüllt § 163g S. 1 StPO indes nicht.

Es bedarf einer Klarstellung der durch das Gesetz angesprochenen Telekommunikations- und Telemediendienste. Darüber hinaus ist eine Legaldefinition des Begriffs „dauerhafte virtuelle Identität“ erforderlich.[236] Wann ist eine solche als dauerhaft zu bezeichnen? Aus welchen Umständen ergibt sich eine virtuelle Identität? Welche Anforderungen an die Substanz ebendieser werden durch den Gesetzgeber gestellt? In welcher Umgebung des Cyberspace muss sich diese befinden? Ist tatsächlich, wie die Gesetzesbegründung vermuten lässt, nur das Darknet als ein Teil des Cyberspace gemeint? An diesen Stellen müsste der Gesetzesentwurf also deutlich präziser ausgestaltet sein, um den Anforderungen des Bestimmtheitsgrundsatzes zu genügen.

Als Konkretisierung der Anlasstat wird auf eine Straftat im Sinne von § 100g Abs.1 StPO verwiesen. Problematisch ist indes, dass § 100g Abs. 1 Nr. 2 StPO

[236] Vgl. *Oehmichen/Weißenberger*, Digitaloffensive im Strafrecht, Verbesserte Bekämpfung von Cyberkriminalität durch das IT-Sicherheitsgesetz 2.0?, KriPoZ 2019, 174, 179.

durch die Formulierung „Straftat mittels Telekommunikation“ sehr weit gefasst ist. Im Rahmen des § 163g StPO müssten dies wohl – im Hinblick auf die im Gesetz genannte Herkunft der virtuellen Identitäten – Straftaten mittels Telekommunikation und Telemedien sein. Diese Schlussfolgerung ergibt sich indes nur durch eine systematische Auslegung der Norm, sodass auch hier eine bestimmtere Formulierung gewählt werden müsste. Ungeachtet dessen führt der hier gewählte Verweis jedoch auch zu weiteren Bestimmtheitsproblemen, da letztlich der Kreis der Delikte, die eine solche Anlasstat darstellen könnten, sehr weit gefasst wäre, z.B. würde eine Beleidigung in einem Chatforum gemäß § 185 StGB bereits ausreichen.[237] Eine solch weite Statuierung der Anlasstaten entspricht jedoch aufgrund der Tiefe des Grundrechtseingriffs nicht dem verfassungsrechtlichen Bestimmtheitsgrundsatz.

Darüber hinaus wirft die ebenfalls sehr weit gefasste Formulierung in S. 3 „mit Dritten“ Bestimmtheitsprobleme auf. Wie dargestellt, wird durch das in S. 3 geregelte Einsatzszenario nicht unerheblich in Art. 10 Abs.1 GG und in bestimmten Fällen ebenso in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG eingegriffen. Die durch den Gesetzgeber gewählte Formulierung eines Dritten lässt offen, welcher Personenkreis unter diesen Terminus fallen soll. Ist dies jeder x-beliebige Dritte?[238]

Im Hinblick auf S. 5 des § 163g StPO müsste die Gesetzesbegründung angepasst werden. Das Verwendungsverbot muss sich auch auf die Anlasstat beziehen.

Schlussendlich fehlen im Rahmen des § 163g StPO auch Formulierungen, die deutlich machen, dass vor den Ermittlungshandlungen nach dieser Norm zunächst mildere Mittel anzuwenden sind. Diese Forderung ergibt sich aus dem verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz. Es könnte z.B. eine der Regelung des § 110a Abs. 1 S. 3 StPO vergleichbare Formulierung gewählt werden.[239] Vor dem Hintergrund der Schwere der Grundrechtseingriffe lässt der Gesetzesvorschlag außerdem eine Formulierung zum Schutz des

[237] Vgl. *Oehmichen/Weißenberger*, Digitaloffensive im Strafrecht, Verbesserte Bekämpfung von Cyberkriminalität durch das IT-Sicherheitsgesetz 2.0?, KriPoZ 2019, 174, 180.
[238] Vgl. ebd.
[239] Vgl. ebd.

Kernbereichs privater Lebensführung und verfahrensrechtliche Absicherungen, wie z.B. einen Richtervorbehalt, vermissen.[240]

E. Sonderproblem der verdeckten personalen Ermittlungen im Cyberspace: Die Keuschheitsprobe

I. Einleitung

Die sog. Keuschheitsprobe wird derzeit v.a. im Zusammenhang mit der Aufklärung von Delikten aus dem Bereich der Kinderpornographie auf Darknet-Plattformen diskutiert. Eine Verbreitung von Kinderpornographie findet hier zumeist in geschlossenen Gruppen statt, die für eine Aufnahme das Bestehen einer sog. Keuschheitsprobe in Form des eigenständigen Uploads von entsprechenden Bild- oder Videodateien fordern.[241] Der verdeckte personale Ermittler steht in diesen Situationen also vor der Entscheidung, ob er selbst kinderpornographisches Bildmaterial hochladen möchte oder aber die Ermittlungen in dieser Gruppe einstellt. Letzteres soll durch die Keuschheitsprobe gerade bezweckt werden. Sie dient also auf Seiten der Betreiber derartiger Gruppen gerade auch dazu, verdeckte Ermittler gleichsam auszusperren. Nicht als Keuschheitsprobe können hingegen solche Verhaltensweisen des ermittelnden Polizeibeamten qualifiziert werden, die noch unter den Begriff der kriminalistischen List subsumierbar sind. Darunter fällt z.B. die Artikulierung von Fantasien in derartigen geschlossenen Gruppen.[242]

II. Gesetzliche Vorstöße zur Regelung der Keuschheitsprobe

Im Rahmen der 89. Justizministerkonferenz 2018 wurde die Keuschheitsprobe in einer der getroffenen Beschlüsse[243] thematisiert. Dieser Beschluss nimmt Bezug auf Erfahrungen aus der Praxis, aus denen sich ergebe, dass der Upload kinderpornographischer Schriften in ein einschlägiges Forum häufig die einzige Möglichkeit sei, um Zugang zu diesem zu erhalten. Daher sei es für

[240] Vgl. *Oehmichen/Weißenberger*, Digitaloffensive im Strafrecht, Verbesserte Bekämpfung von Cyberkriminalität durch das IT-Sicherheitsgesetz 2.0?, KriPoZ 2019, 174, 180.
[241] Vgl. *Wittmer/Steinebach*, Computergenerierte Kinderpornografie zu Ermittlungszwecken im Darknet, MMR 2019, 650, 651.
[242] Vgl. *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, Rn. 2081.
[243] Vgl. *Justizministerinnen und Justizminister*, Beschluss, TOP II.9.

eine effektive Strafverfolgung notwendig, dass die ermittelnden Polizeibeamten ihrerseits computergeneriertes kinderpornographisches Material hochladen dürften.[244] Der Beschluss endet mithin mit einer Bitte an die Bundesministerin der Justiz und für Verbraucherschutz ihrerseits eine Prüfung durchzuführen, „ob – und wenn ja, in welchem Umfang – im Rahmen eines strafrechtlichen Ermittlungsverfahrens verdeckten Ermittlern die Begehung bestimmter milieubedingter Straftaten […] gestattet werden soll“[245].

Anknüpfend an den Gesetzesentwurf der BReg zur Einführung einer Versuchsstrafbarkeit im Rahmen des Cybergroomings[246] stellten die Bundesländer Bayern und Hessen am 04. September 2019 einen Änderungsantrag im Rechtsausschuss des BR, der auf die Umsetzung des o.g. Beschlusses hinwies und forderten, es verdeckten Ermittlern unter engen Voraussetzungen zu erlauben straflos Keuschheitsproben abzugeben.[247]

Im Rahmen der Plenarsitzung des BR vom 20. September 2019 trug der Bayerische Staatsminister Georg Eisenreich sein o.g. Anliegen anlässlich der Behandlung des Entwurfs eines Gesetzes zur Änderung des Strafgesetzbuchs – Versuchsstrafbarkeit des Cybergroomings – vor.[248] Daraufhin beschloss der BR sodann in dieser Sitzung diesen Aspekt in seine Stellungnahme zum Gesetzentwurf gemäß Art. 76 Abs. 2 GG aufzunehmen und forderte die Aufnahme eines neuen S. 2 in den § 184b Abs. 5 StGB.[249]

In dem ergänzten Gesetzesentwurf vom 09. Oktober 2019 kündigte die BReg nunmehr an, diesen Vorschlag zu prüfen.[250] In der 141. Sitzung des BT vom 17. Januar 2020 wurde der Gesetzesentwurf in der Fassung, die sich aus der Beschlussempfehlung und dem Bericht des Ausschusses für Recht und Verbraucherschutz[251] ergibt, sodann angenommen. Abweichend von der Wortwahl des vorgeschlagenen Entwurfs des BR, wird § 184b Abs. 5 StGB wie folgt lauten:

---

[244] Vgl. *Justizministerinnen und Justizminister*, Beschluss, TOP II.9, S. 2.
[245] Ebd.
[246] Vgl. aktuelle Version: BT-Drs. 19/13836.
[247] Vgl. *Redaktion beck-aktuell*, Bayerns Justizminister fordert gesetzliche Zulassung von „Keuschheitsproben“.
[248] Vgl. *BR*, Plenarprotokoll 980, Top 43, S. 386-387.
[249] Vgl. BR-Drs. 365/19, S. 2+3.
[250] Vgl. BT-Drs. 19/13836, S. 17.
[251] BT-Drs. 19/16543.

> *„Absatz 1 Nummer1 und 4 gilt nicht für dienstliche Handlungen im Rahmen von strafrechtlichen Ermittlungsverfahren, wenn*
>
> *1. die Handlung sich auf eine kinderpornographische Schrift bezieht, die **kein tatsächliches Geschehen wiedergibt** und auch nicht unter Verwendung einer Bildaufnahme eines Kindes oder Jugendlichen hergestellt worden ist, und*
>
> *2. die Aufklärung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre.“*[252]

Darüber hinaus wird ein neuer § 110d in die StPO eingefügt, der besondere Verfahrensvoraussetzungen für die Durchführung der Keuschheitsprobe, insbesondere einen Richtervorbehalt, regelt.[253]

Im Folgenden wird daher zunächst die Notwendigkeit der Schaffung der o.g. Ergänzungen zu § 184b Abs. 5 StGB in der Fassung der Beschlussempfehlung untersucht. Im Anschluss erfolgt eine Würdigung der neuen Vorschriften im StGB und in der StPO.

III. Derzeitige rechtliche Rahmenbedingungen

Grundsätzlich ist es verdeckten personalen Ermittlern nicht gestattet, zur Aufklärung von Straftaten ihrerseits Straftaten zu begehen. Dies folgt zum einen aus dem Legalitätsprinzip und zum anderen daraus, dass im Falle einer Zulassung derartiger Handlungen das Vertrauen der Menschen in die Integrität der Strafverfolgungsbehörden erschüttert werden könnte. Eine Ausnahme von diesem Grundsatz kommt nur bei Vorliegen der engen Voraussetzung der §§ 34, 35 StGB in Betracht.[254] Anders gestaltet sich die Rechtslage in den Niederlanden, wo es den Polizeibeamten unter bestimmten Umständen gestattet ist, Straftaten zu begehen.[255] Im Folgenden soll nun eine mögliche Strafbarkeit des Polizeibeamten geprüft werden, indem dieser selbst kinderpornographisches Material hochlädt. Vor dem Hintergrund des § 184b Abs. 5 Nr. 1 StGB, der einen Strafbarkeitsausschluss im Hinblick auf Delikte, die nach § 184b Abs. 1 Nr. 2 und Abs. 3 StGB strafbar wären, in denjenigen Fällen statuiert, in denen die Handlungen ausschließlich der rechtmäßigen Erfüllung staatlicher Aufgaben dienen, ist die genaue Prüfung einer möglichen Strafbarkeit eines ermittelnden Polizeibeamten entscheidend, da u.U. auch schon nach der derzeitigen Rechtslage die Strafbarkeit entfallen kann.

---

[252] BT-Drs. 19/16543, S. 5.
[253] Vgl. ebd.
[254] Vgl. *Safferling*, Keuschheitsproben und Verdeckte Ermittler im Darknet, DRiZ 2018, 206, 207.
[255] Vgl. ebd.

Es ist grundsätzlich zu differenzieren zwischen einem Upload in eine geschlossene Gruppe und einem direkten Versand an den Moderator dieser Gruppe. Das in dem Gesetzesentwurf ebenfalls genannte Herstellen kinderpornographischer Schriften gemäß § 184b Abs. 1 Nr. 4 StGB wird vor dem Hintergrund, dass dieses in der Regel keine Handlung des verdeckten personalen Ermittlers darstellt, im Rahmen dieser Arbeit nicht näher beleuchtet.

1. Upload in eine geschlossene Gruppe

a) Strafbarkeit nach § 184b Abs. 1 Nr. 1, 1. Var. StGB

Der Upload eines kinderpornographischen Bildnisses in eine geschlossene Gruppe könnte als Verbreiten im Sinne des § 184b Abs. 1 Nr. 1, 1. Var. StGB zu qualifizieren sein. Ein Verbreiten wird dann angenommen, wenn die Schrift einem größeren Personenkreis in körperlicher Form zugänglich gemacht wird.[256] Da es sich hier um einen Upload in den Cyberspace handelt, der gerade durch seine Flüchtigkeit und fehlende Körperlichkeit geprägt ist, müsste man ein Verbreiten im Sinne des § 184b Abs. 1 Nr. 1, 1. Var. StGB in diesen Fällen stets ablehnen. Der BGH hat daher einen internetspezifischen Verbreitungsbegriff[257] entwickelt.

Danach sei es ausreichend, wenn sich die entsprechende Datei auf dem Rechner des Nutzers befinde. Es genüge der flüchtige Arbeitsspeicher, auf eine Speicherung auf einem dauerhaften Speichermedium komme es insofern nicht an, genauso wenig darauf, ob der Empfänger die Möglichkeit des Zugriffs in Anspruch genommen habe.[258] Es ist jedoch zu berücksichtigen, dass derartige Sachverhalte seit dem 49. StrÄndG vom 21.01.2015 durch den § 184d StGB, der sich explizit mit einem Zugänglichmachen in Telemedien beschäftigt, erfasst werden sollen, sodass für eine internetspezifische Auslegung des Begriffs „Verbreiten“ keine Notwendigkeit mehr besteht.[259] § 184d Abs. 1 S. 1 StGB ist insofern im Verhältnis zu § 184b S. 1 Nr. 1, 1. Var. StGB als das

[256] Vgl. *Heger*, in: Kühl/Heger, Strafgesetzbuch, § 74d StGB Rn. 5.

[257] Auf der Grundlage der im Rahmen dieser Arbeit verwendeten Terminologie, müsste es sich um einen sog. „cyberspacespezifischen Verbreitungsbegriff“ handeln.

[258] Vgl. BGH, Urteil vom 27. Juni 2001 – 1 StR 66/01 –, BGHSt 47, 55-62, juris, Rn. 32-34; *Heger*, in: Kühl/Heger, Strafgesetzbuch, § 184 StGB Rn. 5; *Laue*, in: Dölling u.a., Gesamtes Strafrecht, § 184b StGB Rn. 3; *Ziegler*, in: Heintschel-Heinegg von, Strafgesetzbuch, § 184b StGB Rn. 10; *Fischer*, Strafgesetzbuch, § 184b StGB Rn. 16.

[259] Vgl. *Hörnle*, in: Miebach, Münchener Kommentar zum Strafgesetzbuch, Band 3, § 184b StGB Rn. 22; *Greco*, Verbreitung pornographischer Schriften, Rn. 105; *Gercke*, in: Spindler/Schuster, Recht der elektronischen Medien, Neunter Teil, § 184b StGB Rn. 21; im Ergebnis auch *Eisele*, in: Schönke/Schröder, Strafgesetzbuch, § 184b StGB Rn. 21 i.V.m. § 184d StGB Rn. 2.

speziellere Delikt zu beurteilen.[260] Vor diesem Hintergrund ist mithin an der für ein Verbreiten erforderlichen Körperlichkeit festzuhalten, die im vorliegenden Fall zu verneinen ist.[261]

b) Strafbarkeit nach § 184b Abs. 1 Nr. 1, 2. Var. StGB

Es könnte indes eine Zugänglichmachung an die Öffentlichkeit vorliegen. Ein Zugänglichmachen in Form der Schaffung einer Möglichkeit zur Wahrnehmung[262] ist unstreitig gegeben. Fraglich ist indes, ob die Mitglieder einer geschlossenen Gruppe bzw. eines Forums unter den Begriff der Öffentlichkeit zu subsumieren sind. Dies ist dann der Fall, „wenn für eine unbestimmte Vielzahl von Personen die Möglichkeit geschaffen wird, dass sie vom Inhalt der Schrift Kenntnis erlangen können“[263]. Mithin ist die konkrete Ausgestaltung der Gruppe entscheidend. Handelt es sich um eine solche, die für jedermann zugänglich ist, oder aber zu denen ein jederzeitiger Beitritt durch jeden Nutzer des Cyberspace möglich ist, kann das Merkmal der Öffentlichkeit bejaht werden.[264] Liegt jedoch eine Gruppe vor, der nur nach Bestehen einer Keuschheitsprobe beigetreten werden kann, spricht dies gegen die Qualifizierung der Gruppe als öffentlich, da der Zugang an ein ernsthaftes Hindernis geknüpft ist.[265] Diese Abstufungen entsprechen denjenigen, die im Hinblick auf soziale Online-Netzwerke im Rahmen dieser Arbeit vorgenommen wurden. Diesen zufolge konnten Inhalte dann nicht mehr als öffentlich qualifiziert werden, wenn sie nur nach vorheriger Vernetzung mit dem jeweiligen Profilinhaber sichtbar sind, also eine „Hürde“ in Form einer qualifizierten „Zulassung“ durch den Angefragten genommen wurde. Wird dieser Aspekt auf Foren übertragen, sind auch diese nicht mehr der Öffentlichkeit zuzurechnen, wenn zuvor eine

[260] Vgl. *Hörnle*, in: Miebach, Münchener Kommentar zum Strafgesetzbuch, Band 3, § 184d StGB Rn. 44.
[261] AA mit Verweis auf die in Fn. 258 genannte Rechtsprechung: *Wittmer/Steinebach*, Computergenerierte Kinderpornografie zur Ermittlungszwecken im Darknet, MMR 2019, 650, 651.
[262] Vgl. *Heger*, in: Kühl/Heger, Strafgesetzbuch, § 184d StGB Rn. 4.
[263] *Gercke*, in: Spindler/Schuster, Recht der elektronischen Medien, Neunter Teil, § 184b StGB Rn. 21.
[264] Vgl. *Gercke*, Brauchen Ermittlungsbehörden zur Bekämpfung von Kinderpornographie im sog. „Darknet“ weitergehende Befugnisse, CR 2018, 480, 482.
[265] Vgl. *Gercke*, Brauchen Ermittlungsbehörden zur Bekämpfung von Kinderpornographie im sog. „Darknet“ weitergehende Befugnisse, CR 2018, 480, 483; *Eisele*, in: Schönke/Schröder, Strafgesetzbuch, § 184b StGB Rn. 25.

„Hürde“ in Form einer Keuschheitsprobe genommen werden muss. Mithin machen sich die ermittelnden Polizeibeamten auch nicht gemäß § 184b Abs. 1 Nr. 1, 2. Var. StGB strafbar.[266]

c) Strafbarkeit nach § 184b Abs. 1 Nr. 2 StGB

Eine Strafbarkeit nach § 184b Abs. 1 Nr. 2 StGB richtet sich danach, wie die Begrifflichkeit „Besitzverschaffung“ zu definieren ist. Darunter versteht man „jede Vermittlungshandlung, die den Inhalt weiterleitet und zur vollen Verfügungsgewalt seitens des Empfängers führt“[267]. Fraglich ist mithin, ob das Posten in einer geschlossenen Gruppe als Besitzverschaffung qualifiziert werden kann. Nach der wohl hM liegt eine solche bereits beim reinen Sichtbarwerden auf dem Bildschirm vor.[268] Nach aA genügt dies für eine tatsächliche Verfügungsgewalt noch nicht.[269] Vor dem Hintergrund, dass die Strafbarkeit jedenfalls gemäß § 184b Abs. 5 StGB entfällt, kann eine Streitentscheidung in diesem Fall dahinstehen.

d) Strafbarkeit nach § 184d Abs. 1 S. 1 StGB

Nach § 184d Abs. 1 S. 1 StGB macht sich strafbar, wer einen pornografischen Inhalt mittels Telemedien einer anderen Person oder der Öffentlichkeit zugänglich macht. Im Unterschied zu § 184b Abs. 1 Nr. 1, 2. Var. StGB ist hier auch ein Zugänglichmachen an eine nur eingeschränkte Anzahl von Personen oder sogar an nur eine einzige Person strafbegründend. Mit Einstellen kinderpornographischen Bildmaterials in eine geschlossene Gruppe macht sich der ermittelnde Polizeibeamte also unstreitig wegen der Zugänglichmachung pornografischer Inhalte mittels Telemedien strafbar. Die Strafbarkeit entfällt jedoch gemäß § 184d Abs. 1 S. 3 StGB i.V.m. 184b Abs. 5 StGB.

2. Versand an den Moderator

Im Folgenden soll sodann kurz auf die Strafbarkeit des direkten Versands des kinderpornographischen Materials an den Moderator der Gruppe eingegangen werden. Eine solche nach § 184b Abs. 1 Nr. 1 StGB scheidet aus den o.g.

---

[266] Im Ergebnis hätte aufgrund der spezielleren Norm des §184d Abs. 1 S. 1 StGB eine Prüfung unterbleiben können. Da diese Auffassung jedoch nicht unstreitig ist (so untersuchen z.B. *Wittmer/Steinebach* eine mögliche Strafbarkeit), wurde eine Prüfung an dieser Stelle im Sinne einer umfassenden Betrachtung der Strafbarkeit durchgeführt.

[267] *Hörnle*, in: Miebach, Münchener Kommentar zum Strafgesetzbuch, Band 3, § 184b StGB Rn. 27.

[268] Vgl. Hanseatisches OLG Hamburg, Urteil vom 15. Februar 2010 – 2 - 27/09 (REV) –, juris, Rn. 44+45; *Eckstein*, Ist das „Surfen“ im Internet strafbar, NStZ 2011, 18, 19; *Keye*, Befugnisse der Ermittlungsbehörden zur Bekämpfung von Kinderpornographie im Darknet**,** ITRB 2018, 194, 195.

[269] Vgl. *Hörnle*, in: Miebach, Münchener Kommentar zum Strafgesetzbuch, Band 3, § 184b StGB Rn. 38.

Gründen aus. Ferner kann auch, hinsichtlich der Prüfung der Straftatbestände aus § 184b Abs. 1 Nr. 2 und § 184d Abs. 1 S. 1 StGB, nach oben verwiesen werden. In beiden Fällen entfällt die Strafbarkeit aufgrund des Tatbestandsausschlusses nach § 184b Abs. 5 StGB (i.V.m. § 184d Abs. 1 S. 3 StGB).

IV. Würdigung des Gesetzesvorschlags

Entscheidend für die Beurteilung der Notwendigkeit des o.g. Gesetzesvorschlags ist, ob sich der ermittelnde Polizeibeamte nach § 184b Abs. 1 Nr. 1 StGB strafbar macht und somit der Tatbestandsausschluss nach § 184b Abs. 5 StGB nicht greift. Wie oben gezeigt, ist dies im Rahmen des Uploads einer kinderpornographischen Schrift in eine geschlossene Gruppe nicht der Fall. Eine Strafbarkeit liegt vielmehr nur hinsichtlich solcher Delikte vor, die durch § 184b Abs. 5 StGB bereits erfasst sind. Gleichwohl gibt es beträchtliche Stimmen in der Literatur, die eine Strafbarkeit nach § 184b Abs. 1 Nr. 1, 1. Var. StGB annehmen.[270] Die Gretchenfrage dieser Diskussion ist, ob der internetspezifische Verbreitungsbegriff, der durch den BGH im Jahre 2001 entwickelt wurde, noch anwendbar ist oder aber mittlerweile durch die Schaffung des § 184d StGB in seiner jetzigen Form überholt und somit redundant ist. Wie dargestellt, wurde im Jahr 2015 das 49. StrÄndG erlassen, wodurch der § 184d StGB seine heutige Fassung erhalten hat. Nach 2015 hat sich der BGH nicht mehr mit der Frage auseinandergesetzt, ob der internetspezifische Verbreitungsbegriff vor dem Hintergrund dieser neuen Regelung noch weiter aufrechterhalten werden soll. Im Sinne der Rechtssicherheit wäre eine solche Entscheidung sehr zu begrüßen. Die Gesetzesbegründung führt zu den beabsichtigten Änderungen des § 184d StGB mit Verweis auf den internetspezifischen Verbreitungsbegriff aus, dass auch „einfachere und klarere Regelungen“[271] möglich seien und sieht daher vor, die strafbegründenden Handlungen nach § 184b Abs. 1 Nr. 1 StGB (Verbreiten und der Öffentlichkeit zugänglich machen) für den Bereich der Telemedien durch eine solche nach § 184d Abs. 1 S. 1 StGB (einer Person oder Öffentlichkeit zugänglich machen) zu ersetzen.[272] Bei Betrachtung dieser gesetzgeberischen Intention muss dies zwangsläufig zu einer Abkehr vom internetspezifischen Verbreitungsbegriff

[270] Vgl. Fn. 258.
[271] BT-Drs. 18/2601, S. 16.
[272] Vgl. ebd.

führen. Somit scheidet eine Strafbarkeit nach § 184b Abs. 1 Nr. 1, 1. Var. StGB für den ermittelnden Polizeibeamten grundsätzlich aus. Vor dem Hintergrund, dass die gegenteilige Auffassung aber mit einigem Gewicht im Schrifttum vertreten wird, besteht zweifellos eine Klärungsbedürftigkeit dieser Rechtsfrage. Es ist jedoch anzuzweifeln, dass der Gesetzesentwurf des BT eine solche herbeiführen kann. Problematisch ist, dass dieser suggeriert, dass eine Strafbarkeit nach § 184b Abs. 1 Nr. 1, 1. Var. StGB grundsätzlich vorliegen kann, was nur der Fall sein kann, wenn der internetspezifische Verbreitungsbegriff zugrunde gelegt wird. Eine Aussage, wie sodann das Verhältnis zwischen § 184b Abs. 1 Nr. 1 StGB und § 184d Abs. 1 S. 1 StGB ist, bleibt der Vorschlag inklusive seiner Begründung indes schuldig.

Ferner bezieht sich der Gesetzesvorschlag nur auf § 184b Abs. 1 Nr. 1 und 4 StGB und statuiert einen Strafbarkeitsausschluss für Schriften, die kein tatsächliches Geschehen wiedergeben und auch nicht unter Verwendung einer Bildaufnahme eines Kindes oder Jugendlichen hergestellt worden sind. Im Hinblick auf eine Tat nach § 184b Abs. 1 Nr. 2 StGB, der bereits durch § 184b Abs. 5 S. 1 StGB erfasst ist, bliebe jedoch auch die Verschaffung des Besitzes an einer kinderpornographischen Schrift, die ein tatsächliches Geschehen wiedergibt, straffrei. Diese Differenzierung vermag indes nicht zu überzeugen, da kein sachlicher Grund für eine derartige Andersbehandlung ersichtlich ist. Vielmehr ist eine grundsätzliche Beschränkung auf fiktive Geschehnisse begrüßenswert. Würde z.B. das Bildnis eines realen Kindes, das in der Vergangenheit Opfer eines Missbrauchs geworden ist, erneut in ein derartiges Forum hochgeladen werden, würde es ein weiteres Mal viktimisiert werden.[273] Es gibt heute bereits einige forensische Methoden, die die Erstellung derartiger wirklichkeitsnaher Bildnisse mit vertretbarem technischen Aufwand ermöglichen und täuschend echt wirken[274], sodass diese als milderes Mittel zu beurteilen sind und ausschließlich im Rahmen der Keuschheitsprobe verwendet werden sollten. Eine mögliche Anwendung des § 184d Abs. 1 S. 1 StGB wirft sodann

[273] Vgl. *Gercke*, Brauchen Ermittlungsbehörden zur Bekämpfung von Kinderpornographie im sog. „Darknet“ weitergehende Befugnisse, CR 2018, 480, 484.

[274] Vgl. *Wittmer/Steinebach*, Computergenerierte Kinderpornografie zu Ermittlungszwecken im Darknet, MMR 2019, 650, 651 ff. Als Möglichkeiten einer technischen Umsetzung werden Vektorgrafiken und der Austausch von Gesichtern vorgestellt.

die gleichen Probleme auf. Auch in diesem Zusammenhang wäre das Zugänglichmachen von realen pornografischen Inhalten, und nicht nur von fiktiven, gemäß § 184d Abs. 1 S. 3 StGB i.V.m. § 184b Abs. 5 S. 1 StGB straffrei.

Mithin würde eine Ergänzung des § 184b Abs. 5 StGB um den durch den BT beschlossenen S. 2 zu sachlich nicht gerechtfertigten – und wahrscheinlich auch nicht intendierten – Differenzierungen führen. Die Beschränkung des Tatbestandsausschlusses auf die Wiedergabe eines nicht-tatsächlichen Geschehens, das nicht unter Verwendung einer Bildaufnahme eines Kindes oder Jugendlichen hergestellt worden ist, ist indes aufgrund der obigen Erwägungen ausdrücklich zu befürworten.

Im Vergleich zum Gesetzesentwurf des BR enthält die durch den BT beschlossene Ergänzung des Abs. 5 nunmehr in Ziff. 2 eine Subsidiaritätsklausel. Im Hinblick auf den Grundsatz der Verhältnismäßigkeit, der im Rahmen jeglichen staatlichen Handelns zu berücksichtigen ist, und den Regelungsgegenstand, der die Polizeibeamten zu einer im Grundsatz strafrechtlich relevanten Handlung autorisiert, ist dies auch zwingend notwendig. Darüber hinaus ist aus diesen Gründen auch der Richtervorbehalt sehr zu begrüßen, der als verfahrensrechtliches Pendant, sicherstellt, dass die durch den Strafbarkeitsausschluss erfassten Handlungen nur im begründeten Einzelfall vorgenommen werden und nicht standardmäßig zur Anwendung kommen.

Gesetzessystematisch ist der Richtervorbehalt in § 110d StPO geregelt, sodass sich aus der systematischen Auslegung ergibt, dass der Gesetzgeber davon ausgeht, dass der handelnde Polizeibeamte als verdeckter Ermittler im Sinne des § 110a StPO agiert. Wie die vorliegende Arbeit jedoch gezeigt hat, liegt im Bereich von Ermittlungen in Chatforen nicht stets ein in § 110a StPO genanntes Einsatzszenario vor, sodass ein Rückgriff auf § 110d StPO u.U. ausscheidet. Darüber hinaus bestehen Bedenken hinsichtlich der Erfüllung der qualitativen Anforderungen an die durch § 110a Abs. 2 StPO geforderte Legende.[275]

[275] Aus dem Plenarprotokoll 19/141 des BT zur 141. Sitzung ergibt sich jedoch, dass die Auswirkungen der Einordnung des § 110d StPO in den Regelungszusammenhang des verdeckten Ermittlers keineswegs klar und unumstritten sind. *Thorsten Frei* führt dazu auf S. 17617 im Abschnitt D aus: *„Ich bin froh, dass wir es bei den Polizeibeamten nicht auf verdeckte Ermittler begrenzt haben, weil wir dann ganz praktische Probleme bekommen hätten, etwa bei den Landespolizeibehörden, in denen wenige verdeckte Ermittler in diesem Bereich eingesetzt werden. Wir haben uns auf den Einsatz*

Praktisch problematisch ist indes der neue § 110d S. 2 StPO. Laut diesem muss im Antrag an das Gericht dargelegt werden, dass die handelnden Polizeibeamten auf den Einsatz umfassend vorbereitet wurden. Die Begründung der Beschlussempfehlung konkretisiert dies dahingehend, dass der handelnde Polizeibeamte somit „besonders qualifiziert“[276] sein müsse, da u.a. die Verbreitung mit „besonderen Risiken“[277] verbunden sei. Als ein besonderes Risiko dürfte sicherlich die im Anschluss zu behandelnde Möglichkeit der Tatprovokation zu qualifizieren sein. Es ist nicht auszuschließen, dass durch derartige hochgeladene Bildnisse ein Teilnehmer des Chatforums erst zur Begehung von Sexualstraftaten motiviert wird. Darüber hinaus ist unklar, wann ein Beamter über eine derartige besondere Qualifikation verfügt. Wie gestaltet sich die Erlangung solcher Qualifikationen im Polizeialltag? Welche Inhalte müssen Teil der erforderlichen umfassenden Vorbereitung sein? Ist die Teilnahme an speziellen, v.a. ethischen, Fortbildungen erforderlich? Spielen auch charakterliche Eigenschaften oder der Dienstgrad des handelnden Polizeibeamten eine Rolle? Klar ist insoweit nur, dass er sich aufgrund seiner Kenntnisse und Fähigkeiten aus der Masse der Polizeibeamten hervorheben muss. Da das Vorliegen dieser besonderen Qualifizierung jedoch richterlich geprüft wird, muss es an dieser Stelle bestimmte Standards geben, die der Gesetzgeber zumindest rudimentär festlegen muss. Die Verwendung von unbestimmten Rechtsbegriffen genügt hingegen nicht.

V. Tatprovokation

Problematisch könnte darüber hinaus sein, dass der ermittelnde Polizeibeamte durch das Hochladen der o.g. Inhalte die sonstigen Gruppenmitglieder zur Begehung einer Straftat nach § 184d Abs. 2 S. 1 StGB provoziert, indem diese die bereitgestellten Inhalte abrufen. Eine Tatprovokation ist jedoch nur dann zulässig, wenn bezüglich der betroffenen Person ein Anfangsverdacht entweder im Hinblick auf eine bereits begangene Straftat oder aber dahingehend vorliegt, dass die jeweilige Person in der Zukunft zu einer solchen Tat

besonders geschulter Polizeibeamter verständigt und damit, glaube ich, eine sachgerechte Lösung entwickelt.“ Würden diese Darlegungen zugrunde gelegt, spräche dies für einen neuen – von dem verdeckten Ermittler nach § 110a Abs. 2 S. 1 StPO zu unterscheidenden – Ermittlertypus: Den besonders geschulten Polizeibeamten. Dies vermag aber vor dem Hintergrund der eindeutigen systematischen Stellung nicht zu überzeugen. Vielmehr müsste es sich in diesem Kontext um einen besonders geschulten verdeckten Ermittler handeln.

[276] BT-Drs. 19/16543, S. 12.

[277] Ebd.

bereit sein wird.[278] Dies ist im Rahmen der Absolvierung der Keuschheitsprobe, um Zugang zu der geschlossenen Gruppe zu erhalten, sehr fraglich. Der ermittelnde Polizeibeamte hat noch keinerlei Kenntnis davon, wer Teil dieser Gruppe ist, sodass der Anfangsverdacht nicht hinlänglich konkretisierbar ist. Daher würde die Absolvierung einer Keuschheitsprobe stets zu einer unzulässigen Tatprovokation führen, mit dem Ergebnis, dass dieser Umstand entweder zu einem Verfahrenshindernis auf Seiten des Betroffenen führt (2. Strafsenat des BGH)[279] oder aber strafmildernd im Rahmen der Strafzumessung zu berücksichtigen ist (1. Strafsenat des BGH)[280]. Daher genügt die Einfügung eines Tatbestandsausschlusses für den ermittelnden Polizeibeamten nicht. Es bedarf ferner einer Regelung, wie dies auf Seiten des sodann Beschuldigten zu berücksichtigen ist. Im Hinblick auf diesen Aspekt wird dem Koalitionsvertrag der aktuellen BReg zugestimmt, der einen Auftrag zur Prüfung eines gesetzgeberischen Handlungsbedarfs hinsichtlich der Schaffung einer Rechtsgrundlage für die Tatprovokation enthält.[281] Dies wäre auch vor dem Hintergrund wünschenswert, als dass ein Dissens zwischen dem ersten und zweiten Strafsenat des BGH existiert, sodass eine gesetzliche Regelung auch diesbezüglich Rechtsklarheit schaffen könnte. Der nunmehr beschlossene § 184b Abs. 5 S. 2 StGB und dessen Begründung beschäftigen sich jedoch nicht mit diesem Aspekt, sodass unklar bleibt, wie strafrechtlich mit den Teilnehmern der Chatforen umzugehen ist.

[278] Vgl. *Bruns*, in: Hannich, Karlsruher Kommentar zur Strafprozessordnung, § 110c StPO Rn. 10.
[279] Vgl. BGH NJW 2016, 91, 97.
[280] Vgl. BGH, NStZ 2013, 99, 100.
[281] Koalitionsvertrag CDU/CSU/SPD für die 19. Legislaturperiode, S. 123, Zeilen 5780+5781.

F. Schlussbetrachtung

Zu Beginn dieser Arbeit wurde, anknüpfend an ein Zitat von *Bill Gates*, die Frage aufgeworfen, ob die Polizeibehörden im Hinblick auf personale verdeckte Ermittlungsmaßnahmen „auf der Welle schwimmen oder aber untergehen“. Auf diese Frage muss derweil wohl folgendermaßen geantwortet werden: Sie halten ihren Kopf über Wasser, von einem Schwimmen auf der Welle kann indes noch nicht die Rede sein.

Die vorliegende Arbeit hat gezeigt, dass eine globale Betrachtung des Cyberspace im weiten Sinne die Besonderheiten dieses Raumes verkennt. Dieser lässt sich in ganz unterschiedliche virtuelle Räume teilen (Cyberspace im engeren Sinne), die jeweils für sich genommen dogmatisch untersucht werden müssen. So zeigte sich insbesondere an den Darlegungen zu sozialen Online-Netzwerken und Chatforen, dass diesen unterschiedliche Rahmenbedingungen zugrunde liegen. Während erstere eine starke Bindung an das reale Leben aufweisen und letztlich eine Erweiterung der Darstellung der eigenen Persönlichkeit ermöglichen, sind letztere durch Anonymität geprägt. Daraus ergeben sich Auswirkungen für die Prüfung der Grundrechtsrelevanz. Insbesondere kann eine Einschränkung des Schutzbereichs des Rechts auf informationelle Selbstbestimmung, wie sie das BVerfG vornimmt, nicht stets auf Kommunikationsvorgänge im Cyberspace übertragen werden, vielmehr ist die Anwendbarkeit für jeden Cyberspace im engeren Sinne separat zu prüfen. Dabei ist auf den Sinn und Zweck der Forderung von Überprüfmechanismen abzustellen – der Schaffung einer Art Brücke zwischen virtueller und realer Welt. Dass dies jedoch dann nicht notwendig ist, wenn der Cyberspace im engeren Sinne als erweiterter Sozialkontext dient und die – metaphorisch gesprochen – geforderte Brücke bereits besteht, gilt es bei der Anwendung der Entscheidung des BVerfG zu berücksichtigen. Daraus ergibt sich jedoch auch, dass es für den Einsatz verdeckter personaler Ermittler in sozialen Online-Netzwerken stets einer hinreichend bestimmten Rechtsgrundlage in Form eines Parlamentsgesetzes bedarf. Ein Rückgriff auf die Ermittlungsgeneralklausel scheidet mithin indes stets aus. Gleichwohl hat die vorliegende Arbeit auch gezeigt, dass auch § 110a StPO nicht anwendbar ist, da dieser den speziellen Rahmen- und Einsatzbedingungen dieses Raumes nicht gerecht wird, vielmehr

bedarf es einer eigenen Rechtsgrundlage. Wird für die Bestimmung der Eingriffsintensität auf die Qualität der in sozialen Online-Netzwerken enthaltenen Informationen abgestellt, bedarf es einer Rechtsgrundlage für jegliches Handeln von Polizeibeamten in dem der Netzwerköffentlichkeit entzogenen Teil des sozialen Online-Netzwerks. Für ein Tätigwerden in Chatforen gilt dies nur dann, wenn eine „Brücke“ zwischen der realen Welt und dem Chatforum besteht, etwa weil sich die Kommunikationspartner auch privat kennen. Erforderlich ist auch hier stets eine einzelfallbezogene Betrachtung.

Gesetzgeberisch wurde grundsätzlich die Bedeutung sozialer Online-Netzwerke wie auch Chatforen für die Begehung von Straftaten erkannt. So ist die hinter § 163g StPO stehende Intention durchaus zu begrüßen, dennoch sind zwingend Anpassungen sowohl des Wortlauts der Norm als auch der Gesetzesbegründung erforderlich. Die Nutzung eines bestehenden Accounts wird in Zukunft eine immer größere Bedeutung erfahren, da z.B. Facebook vermehrt gegen Fake-Accounts vorgeht und diese sperrt.[282] Damit wird es immer schwieriger werden, virtuelle Fake-Profile aufzubauen, die nicht durch eine Sperrung gefährdet sind. Somit wird die Zukunft wohl tatsächlich in der Nutzung eines bereits bestehenden Accounts liegen. Gleichwohl können die Zugangsdaten nur unter engen gesetzlichen Voraussetzungen vom Berechtigten herausverlangt werden, insbesondere ist der Grundsatz der Verhältnismäßigkeit zu beachten.

Kommuniziert der verdeckte personale Ermittler aktiv mit der Zielperson, ist durch den Polizeibeamten stets darauf zu achten, dass keine Vernehmung im Sinne des § 136 StPO vorliegt, die vorherige Belehrungspflichten auslöst, die den Beschuldigten wiederum vor einer Selbstbelastung schützen sollen.

Die Darlegungen zur Keuschheitsprobe haben gezeigt, dass für eine derartige Regelung, wie sie der BT beschlossen hat, im Grunde kein gesetzgeberisches Bedürfnis besteht, da der Polizeibeamte auch heute schon kinderpornographische Bildnisse straffrei in derartige Foren hochladen kann. Dennoch wird die gegenteilige Auffassung von zahlreichen Vertretern der Literatur vertreten,

[282] Vgl. Tagessschau, Facebook sperrt Milliarden Fake-Accounts.

was jedoch im Kern einzig auf die unklare Problematik der weiteren Heranziehung des internetspezifischen Verbreitungsbegriffs im Rahmen des § 184b Abs. 1 Nr. 1 StGB zurückzuführen ist. Somit würde dem Regelungsbedürfnis des BR und des BT durch eine gesetzliche Regelung, die das Verhältnis von § 184b StGB und § 184d StGB statuiert, einfacher und – mit für andere Sachverhalte rechtsklarstellender Wirkung – Rechnung getragen. Ausdrücklich zu begrüßen ist indes die Beschränkung der Straffreiheit auf den Upload von computergenerierten Geschehnissen. Diese stellen ein im Verhältnis zur Verwendung von realen Geschehen milderes Mittel dar und beugen einer sekundären Viktimisierung des Opfers vor. Gleichwohl müsste diese Beschränkung konsequenterweise für alle Tätigkeiten des ermittelnden Polizeibeamten in derartigen Foren gelten. Die Zukunft wird jedoch zeigen, ob die nunmehr gesetzlich geregelte Keuschheitsprobe tatsächlich die Ermittlungsarbeit der handelnden Polizeibeamten effektiver gestaltet. Aus Sicht der Betreiber dieser Foren fungieren solche Bildnisse als eine Art Eintrittskarte und werden bewusst verwendet, um Polizeibeamte auszusperren. Da dieses Interesse der Betreiber jedoch auch weiterhin besteht, ist davon auszugehen, dass diese ihre Zugangsmodalitäten entsprechend anpassen werden. Der Gesetzgeber reagiert also hier nur auf derzeit bestehende Gegebenheiten, im Hinblick auf zukünftige Zugangsmechanismen findet er jedoch keine Regelung. Zynisch könnte man sagen, der Gesetzgeber rennt der Entwicklung an dieser Stelle hinterher und stellt aller Wahrscheinlichkeit nach nur temporär eine Art Waffengleichheit her.

Die derzeitigen Gesetzesvorstöße zeigen anschaulich, dass die Bedeutung des Cyberspace, sei es im weiten oder aber im engeren Sinne, erkannt wird und auch das Bedürfnis nach personalen Ermittlungsmaßnahmen steigt. Gleichwohl wirken die Vorstöße an manchen Stellen eher aktionistisch: Sie verfolgen ein legitimes Ziel, das tatsächlich einer Regelung bedarf, enthalten dann jedoch sprachliche und systematische Unschärfen, sodass diese Art der Gesetzgebung durchaus eher als symbolhaft bezeichnet werden kann. Aktuell wird dies auch am Referentenentwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität des BMJV deutlich.[283] Dieser

[283] Vgl. BMJV, Referentenentwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität.

sieht die Einfügung eines neuen § 15a in das TMG vor, der unter bestimmten Voraussetzungen einen Auskunftsanspruch der Strafverfolgungsbehörden gegenüber dem Telemediendienstanbieter hinsichtlich der durch den Nutzer verwendeten Passwörter statuiert. Grundsätzlich ist auch hier eine ausdrückliche gesetzliche Regelung zu begrüßen und auch notwendig, liegt doch – gerade im Hinblick auf den Zugriff auf soziale Netzwerke – ein schwerwiegender Grundrechtseingriff vor, der einer ausdrücklichen Rechtsgrundlage bedarf. Im Unterschied zum Nutzer selbst, der die Klardaten seines Passworts kennt, speichert der Telemediendienstanbieter das Passwort jedoch aufgrund datenschutzrechtlicher Vorgaben nur in „gehashter" Form, sodass dieses für die Polizeibehörden erst nach einer zeitlich nicht zu unterschätzenden Entschlüsselung nutzbar wäre.[284] Fraglich ist daher, ob diese gesetzliche Regelung tatsächlich praktisch sinnvoll wäre, so wirkt dieser Vorschlag wieder wie eine gut gemeinte Absicht, die jedoch noch einer weiteren Überarbeitung bedarf. Dennoch zeigen die jüngsten Entwicklungen, dass gesetzgeberischer Handlungsbedarf gesehen wird und somit auch die im Rahmen dieser Arbeit aufgeworfenen Aspekte und Bewertungen zukünftig eine Rolle spielen werden. Im Hinblick auf § 163g StPO sind die Ergebnisse der weiteren Ressortabstimmungen abzuwarten, bezüglich der Schaffung einer gesetzlichen Regelung der Keuschheitsprobe ist der Gesetzgeber jüngst aktiv geworden. Der Gesetzgeber hat sich jedoch viel zu lange nicht vertieft genug mit sozialen Online-Netzwerken und Chatforen und was diese virtuellen Räume für das personale Ermittlungshandeln der Polizeibeamten bedeuten, beschäftigt, sodass es zuvörderst überhaupt erst einmal einer Rechtsgrundlage für deren Tätigwerden im Rahmen des in dieser Arbeit dargestellten Umfanges bedarf. Die Rechtsprechung des BVerfG zur Online-Durchsuchung aus dem Jahr 2008 kann nicht auf jeden virtuellen Raum angewendet werden und muss dahingehend weiterentwickelt werden, dass u.U. sehr wohl eine über die Ermittlungsgeneralklausel hinausgehende Rechtsgrundlage nötig ist. Erst dann können Einzelfragen des Handelns und die Befugnisse der Polizeibeamten geregelt werden. Derzeit handelt es sich eher um gutgemeinte Einzelvorstöße, die jedoch eine grundlegende Regelung vermissen lassen. Solche gesetzgeberischen Puzzleteile fügen sich jedoch nicht zusammen, wenn kein Überblick über das große

[284] Vgl. *Rähm*, Anti-Terror-Gesetzentwurf bedroht Bürgerrechte.

Ganze besteht und der Rahmen fehlt. Daher ist für die Zukunft dringend eine gesetzgeberische Grundregelung hinsichtlich virtueller Räume erforderlich.

Bezugnehmend auf das zu Beginn dieser Arbeit verwendete Zitat von *Bill Gates* lässt sich also sagen, dass der deutsche Gesetzgeber zwar seine ersten Schwimmversuche absolviert hat, es jedoch noch der Schaffung weiterer Grundlagen braucht, um tatsächlich auf der Welle des Internets surfen zu können ohne immer mal wieder partiell unterzugehen und sich „digitale Inkompetenz“[285] vorwerfen lassen zu müssen.

[285] Vgl. *Wieduwilt*, Angriff auf die digitale Privatsphäre.

Literaturverzeichnis

Auer-Reinsdorff, Astrid/Conrad, Isabell	Handbuch zum IT- und Datenschutzrecht, 3. Auflage, München 2019
Bäcker, Matthias/Denninger, Erhard/Graulich, Kurt	Handbuch des Polizeirechts, 6. Auflage, München 2018
Bannenberg, Britta	Die Amoktat des David (Ali) Sonboly, in: Kriminalistik 2018, S. 419-433
Bauer, Sebastian	Soziale Netzwerke und strafprozessuale Ermittlungen, Berlin 2018
Becker, Jörg-Peter u.a.	Löwe-Rosenberg, Die Strafprozessordnung und das Gerichtsverfassungsgesetz, Dritter Band, Teilband 1, §§ 94-111a, 27. Auflage, Berlin/Boston 2019
Bernard, Andreas	Komplizen des Erkennungsdienstes: Das Selbst in der digitalen Kultur, Frankfurt 2017
Bodensiek, Kai/Walker, Matthias	Livestreams von Gaming Video Content als Rundfunk?, in: MMR 2018,S. 136-141
Brenneisen, Hartmut/Staack, Dirk	Die virtuelle Streife in der Welt der Social Media, in: Kriminalistik 2012, S. 627-631
Brodowski, Dominik/ Freiling, Felix C.	Computerkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, Forschungsforum Öffentliche Sicherheit, Schriftenreihe Sicherheit Nr. 4, Berlin 2011
Bühl, Achim	Die virtuelle Gesellschaft: Ökonomie, Politik und Kultur im Zeichen des Cyberspace, Wiesbaden 2013
Bundesministerium des Innern, für Bau und Heimat	Referentenentwurf eines IT-SiG 2.0 (http://intrapol.org/wp-content/uploads/2019/04/IT-Sicherheitsgesetz-2.0-_-IT-SiG-2.0.pdf, abgerufen am: 18.01.2020)
Bundesministerium für Justiz und für Verbraucherschutz	Referentenentwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_BekaempfungHatespeech.pdf;jsessionid=7BD8035FD7AB13C9E6A5AD9486A6A983.1_cid297?__blob=publicationFile&v=1, abgerufen am: 18.01.2020)

Bundesrat	Plenarprotokoll 980 vom 20. September 2019 (https://www.bundesrat.de/SharedDocs/downloads/DE/plenarprotokolle/2019/Plenarprotokoll-980.pdf?__blob=publicationFile&v=2, abgerufen am: 18.01.2020)
Bundestag	Plenarprotokoll 19/141 vom 17. Januar 2020 (http://dip21.bundestag.de/dip21/btp/19/19141.pdf, abgerufen am: 26.01.2020)
Castells, Manuel	Der Aufstieg der Netzwerkgesellschaft, Teil 1 der Trilogie „Das Informationszeitalter“, Opladen 2001
CDU, CSU, SPD	Koalitionsvertrag für die 19. Legislaturperiode (https://www.bundesregierung.de/resource/blob/975226/847984/5b8bc23590d4cb2892b31c987ad672b7/2018-03-14-koalitionsvertrag-data.pdf?download=1, abgerufen am: 18.01.2020)
Däubler, Wolfgang	Sicherheitsüberprüfungsgesetz, München 2019
Dölling, Dieter u.a.	Gesamtes Strafrecht, 4. Auflage, Baden-Baden 2017
Dreier, Horst	Grundgesetz Kommentar, Band II Artikel 20-82, 3. Auflage, Tübingen 2015
Eckstein, Ken	Ist das „Surfen“ im Internet strafbar, in: NStZ 2011, S. 18-22
Eisenmenger, Florian	Die Grundrechtsrelevanz „virtueller Streifenfahrten“ – dargestellt am Beispiel ausgewählter Kommunikationsdienstes des Internets, Berlin 2017
Endruweit, Günter/Trommsdorf, Gisela/Burzan, Nicole	Wörterbuch der Soziologie, 3. Auflage, Konstanz/München 2014
Englerth, Markus/Hermstrüwer, Yoan	Die Datenkrake als Nutztier der Strafverfolgung, Zum strafprozessualen Zugriff auf Facebook-Profile, in: RW 2013, S. 326-359
Epping,Volker/Hillgruber, Christian	BeckOK Grundgesetz, 41. Edition, München 2019
Fischer, Thomas	Strafgesetzbuch, 66. Auflage, München 2019
Fridgen, Alexander/Geiwitz, Arndt, Göpfert, Burkhard	BeckOK InsO, 16. Edition, München 2019
Fuchs-Heinritz, Werner u.a.	Lexikon zur Soziologie, 5. Auflage, Wiesbaden 2011

Gercke, Björn u.a. Heidelberger Kommentar, Strafprozessordnung, 6. Auflage, München 2019

Gercke, Marco Brauchen Ermittlungsbehörden zur Bekämpfung von Kinderpornographie im sog. „Darknet“ weitergehende Befugnisse, in: CR 2018, S. 480-484

Götting, Horst-Peter/Schertz, Christian/Seitz, Walter Handbuch Persönlichkeitsrecht, Presse- und Medienrecht, 2. Auflage, München 2019

Graf, Jürgen-Peter BeckOK StPO, 35. Edition, München 2019

Greco, Luis Verbreitung pornographischer Schriften, S. 519-565, in: Hilgendorf, Eric/Kudlich, Hans/Valerius, Brian, Handbuch des Strafrechts, Band 4, Heidelberg 2019

Hannich, Rolf Karlsruher Kommentar zur Strafprozessordnung mit GVG, EGGVG und EMRK, 8. Auflage, München 2019

Harte-Bavendamm, Henning/Henning-Bodewig, Frauke Gesetz gegen den unlauteren Wettbewerb, 4. Auflage, München 2016

Hartleb, Florian Neue virtuelle Dimension im Fall des Anschlags von München am 22. Juli 2016, in: Kriminalistik 2018, S. 532-536

Hauck, Pierre Heimliche Strafverfolgung und Schutz der Privatheit, Tübingen 2014

Heintschel-Heinegg von, Bernd Strafgesetzbuch, 3. Auflage, München 2018

Heintschel-Heinegg von, Bernd/Bockemühl, Jan KMR – Kommentar zur Strafprozessordnung, Band 2, 94. Ergänzungslieferung, Köln 2019

Henrichs, Axel/ Wilhelm, Jörg Polizeiliche Ermittlungen in sozialen Netzwerken, in: Kriminalistik 2010, S. 30-37

Henrichs, Axel Ermittlungen im Internet, Zugriff auf öffentlich zugängliche oder nicht öffentlich zugängliche Informationen?, in: Kriminalistik 2011, S. 622-627

Henrichs, Axel Verdeckte personale Ermittlungen im Internet, in: Kriminalistik 2012, S. 632-636

Hertel, Florian Virtuelle verdeckte personale Ermittlungen, in: Kriminalistik 2019, S. 162-168

Herzog, Roman u.a. Maunz/Dürig, Grundgesetz Kommentar, Band I, Art. 1-5, 86. EL, München 2019

Herzog, Roman u.a. Maunz/Dürig, Grundgesetz Kommentar, Band II, Art. 6-16a, 86. EL, München 2019

Herzog, Roman u.a. Maunz/Dürig, Grundgesetz Kommentar, Band III, Art. 17-28, 86. EL, München 2019

Hobe, Stephan Cyberspace – der virtuelle Raum, S. 249-273, in: Isensee, Josef/Kirchhof, Paul, Handbuch des Staatsrechts, Band XI, 3. Auflage, Heidelberg 2013

Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd Multimedia-Recht, 49. EL, München 2019

Hoffmann-Riem, Wolfgang Rechtliche Rahmenbedingungen für und regulative Herausforderungen durch Big Data, S. 11-78 in: Hoffmann-Riem, Wolfgang, Regulative Herausforderungen, Baden-Baden 2018

Hornung, Gerrit Ein neues Grundrecht, in: CR 2008, S. 299-306

Huber, Peter M./Voßkuhle, Andreas Grundgesetz Band 1, Präambel, Artikel 1-19, 7. Auflage, München 2018

Huber, Peter M./Voßkuhle, Andreas Grundgesetz Band 2, Artikel 20-82, 7. Auflage, München 2018

Ihwas, Saleh Ramadan Strafverfolgung in sozialen Netzwerken, Facebook und Co. als moderne Ermittlungswerkzeuge, Baden-Baden 2014

Ihwas, Saleh Ramadan „Die digitale Unterwelt“ – Strafprozessuale Ermittlungsmöglichkeiten im Darknet, in: WiJ 2018, S. 138-147

Jarass, Hans D./ Pieroth, Bodo Grundgesetz für die Bundesrepublik Deutschland, Kommentar, 15. Auflage, München 2018

Justizministerinnen und Justizminister Beschluss, TOP II.9, Effektive Verfolgung und Verhinderung von Kinderpornographie und Kindesmissbrauch im Darknet durch die ausnahmsweise Zulassung von sog. Keuschheitsproben für Verdeckte Ermittler (https://www.justiz.nrw.de/JM/jumiko/beschluesse/2018/Fruehjahrskonferenz_2018/II-9-BY---Effektive-Verfolgung-und-Verhinderung-von-Kinderpornografie-und-Kindesmissbrauch-im-Darknet.pdf, abgerufen am: 18.01.2020)

Kant, Alexander Surfen mit dem TOR-Browser: So kommt man ins Darknet, in: Netzwelt vom 19.09.2019 **(**https://www.netzwelt.de/news/163498-surfen-tor-browser-so-kommt-ins-darknet.html, abgerufen am: 18.01.2020)

Kardorff von, Ernst Virtuelle Netzwerke – neue Formen der Kommunikation und Vergesellschaftung, S. 23-55, in: Willems, Herbert, Weltweite Welten, Internet-Figurationen aus wissenssoziologischer Perspektive, Wiesbaden 2008

Keye, Julia Befugnisse der Ermittlungsbehörden zur Bekämpfung von Kinderpornographie im Darknet**,** in: ITRB 2018, 194-195

Kneidinger, Bernadette Facebook und Co., Eine soziologische Analyse von Interaktionsformen in Online Social Networks, Wiesbaden 2001

Kochheim, Dieter Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Auflage, München 2018

Köver, Chris „Wir müssen das als internationalen Terrorismus begreifen“, in: Netzpolitik.org vom 15.10.2019 (https://netzpolitik.org/2019/interview-zu-online-extremismus-wir-muessen-das-als-internationalen-terrorismus-begreifen/#spendenleiste, abgerufen am: 18.01.2020)

Kube, Hanno Persönlichkeitsrecht, S. 79-145, in: Isensee, Josef/Kirchhof, Paul, Handbuch des Staatsrechts der Bundesrepublik Deutschland, Band VII, 3. Auflage, Heidelberg 2009

Kudlich, Hans Münchener Kommentar zur Strafprozessordnung, Band 1, §§ 1 – 159, 1. Auflage, München 2014

Kühl, Kristian/Heger, Martin Strafgesetzbuch, 29. Auflage, München 2018

Laufer, Daniel Wie 8chan unter neuem Namen zurückkehren soll, in: Netzpolitik.org vom 01.11.2019 (https://netzpolitik.org/2019/wie-8chan-unter-neuem-namen-zurueckkehren-soll/#spendenleiste, abgerufen am: 18.01.2020)

Laufer, Daniel Das Imageboard hat die falschen Freunde, in: Netzpolitik.org vom 08.11.2019 (https://netzpolitik.org/2019/8chan-8kun-das-imageboard-hat-die-falschen-freunde/#spendenleiste, abgerufen am: 18.01.2020)

Legal Tribune Journalisten gegen den BND vom 30.12.2019 (https://www.lto.de/recht/nachrichten/n/bverfg-bnd-gesetz-aufklaerung-klage-journalisten-medien-ueberwachung-weltweit/, abgerufen am: 18.01.2020)

Levin, Ilya/Schwarz, Michael — Zum polizeirechtlichen Umgang mit sog. Facebook-Partys – „Ab geht die Party und die Party geht ab!"… oder doch nicht?, in: DVBl 2012, S. 10-17

Luch, Anika D./Schulz, Sören E. Meier, Bernd-Dieter — Die digitale Dimension der Grundrechte, Die Bedeutung der speziellen Grundrechte im Internet, in: MMR 2013, S. 88-93
Kriminologie und Internet: ein ungeklärtes Verhältnis, S. 93-118, in: Beck, Susanne/Meier, Bernd-Dieter/Momsen, Carsten, Cybercrime und Cyberinvestigations, Baden-Baden 2015

Meyer-Goßner, Lutz/Schmitt, Bertram — Strafprozessordnung, 62. Auflage, München 2019

Miebach, Klaus — Münchener Kommentar zum Strafgesetzbuch, Band 3, 3. Auflage, München 2017

Münch von, Ingo/Kunig, Philip — Grundgesetz Kommentar, Band 1, Präambel – Art. 69, 6. Auflage, München 2012

Oehmichen, Anna/Weißenberger, Björn — Digitaloffensive im Strafrecht, Verbesserte Bekämpfung von Cyberkriminalität durch das IT-Sicherheitsgesetz 2.0?, in: KriPoZ 2019, S. 174-182

Oermann, Markus/Staben, Julian — Mittelbare Grundrechtseingriffe durch Abschreckung?, in: Der Staat 2013, S. 630-661

Rähm, Jan — Anti-Terror-Gesetzentwurf bedroht Bürgerrechte, in: Deutschlandfunk vom 21.12.2019 (https://www.deutschlandfunk.de/streit-um-verfassungsmaessigkeit-anti-terror-gesetzentwurf.684.de.html?dram:article_id=466516, abgerufen am: 18.01.2020)

Ratgeber im Web — AOL Chat – Gibt es ihn noch zum Chatten? vom 13.12.2017 (https://ratgeber-im-web.de/aol-chat-gibt-es-ihn-noch-zum-chatten/, abgerufen am: 18.01.2020)

Redaktion beck-aktuell — Bayerns Justizminister fordert gesetzliche Zulassung von „Keuschheitsproben vom 05. September 2019, becklink 2014054

Rosengarten, Carsten/Römer, Sebastian — Der „virtuelle verdeckte Ermittler" in sozialen Netzwerken und Internetboards, in: NJW 2012, S. 1764-1767

Rüegger, Peter/Nägeli, Rolf — Chatrooms: Ein Tummelplatz für pädosexuelle Straftäter, in: Kriminalistik 2006, S. 404-414

Sachs, Michael — Grundgesetz, 8. Auflage, München 2018

Säcker, Franz Jürgen u.a. — Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 1, 8. Auflage, München 2018

Safferling, Christoph — Keuschheitsproben und Verdeckte Ermittler im Darknet, in: DRiZ 2018, S. 206-207

Schenke, Wolf-Rüdiger/ Graulich, Kurt/ Ruthig, Josef — Sicherheitsrecht des Bundes, 2. Auflage, München 2019

Schneider, Hartmut — Ausgewählte Rechtsprobleme des Einsatzes verdeckter Ermittler – Eine Zwischenbilanz, in: NStZ 2004, S. 359-367

Schönke, Adolf/Schröder, Horst — Strafgesetzbuch, 30. Auflage, München 2019

Schwabenbauer, Thomas — Kommunikationsschutz durch Art. 10 GG, in: AöR 2012, S. 1-41

Singelnstein, Tobias — Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co, in: NStZ 2012, S. 593-606

Soiné, Michael — Verdeckte Ermittler als Instrument zur Bekämpfung von Kinderpornographie im Internet, in: NStZ 2003, S. 225-230

Soiné, Michael — Personale verdeckte Ermittlungen in sozialen Netzwerken zur Strafverfolgung, in: NStZ 2014, S. 248-251

Spindler, Gerald/Schuster, Fabian — Recht der elektronischen Medien, 4. Auflage, München 2019

Spindler, Gerald/Schmitz, Peter/Liesching, Marc — Telemediengesetz, 2. Auflage, München 2018

Stern, Klaus/Becker, Florian — Grundrechte-Kommentar, 3. Auflage, Köln 2019

Stopfer, Juliane M./Back, Mitja D./ Egloff, Boris — Persönlichkeit 2.0 Genauigkeit von Persönlichkeitsurteilen anhand von online Social Network-Profilen, in: DuD 2010, S. 459-462

Stüner, Rolf/Eidenmüller, Horst/Schoppmeyer, Heinrich — Münchner Kommentar zur Insolvenzordnung, Band 2, 4. Auflage, München 2019

Tagesschau — Facebook sperrt Milliarden Fake-Accounts vom 14.11.2019 (https://www.tagesschau.de/wirtschaft/facebook-sperrungen-101.html, abgerufen am: 18.01.2020)

Trappmann, Mark/Hummell, Hans J./Sodeur, Wolfgang — Strukturanalyse sozialer Netzwerke, Konzepte, Modelle, Methoden, 2. Auflage, Wiesbaden 2011

Wieduwilt, Hendrik — Angriff auf die digitale Privatsphäre, in: FAZ vom 14.12.2019 (https://www.faz.net/aktuell/wirtschaft/digitec/ohne-buerger-rechtsgewissen-16535825.html, abgerufen am 18.01.2020)

Wissenschaftlicher Dienst des Deutschen Bundestages — Nutzung von Tarnidentitäten in sozialen Netzwerken durch die Polizei und die Strafverfolgungsorgane, Az. WD 3 – 3000 – 280/18, WD 7 – 300 – 181/18, 30. August 2018

Wittmer, Sandra/Steinebach, Martin — Computergenerierte Kinderpornografie zu Ermittlungszwecken im Darknet, in: MMR 2019, S. 650-653

Wolter, Jürgen — Systematischer Kommentar zur Strafprozessordnung mit GVG und EMRK, Band II, 5. Auflage, Köln 2016

Zöller, Mark A. — Strafbarkeit und Strafverfolgung des Betreibens internetbasierter Handelsplattformen für illegale Waren und Dienstleistungen, in: KriPoZ 2019, S. 274-281

Abkürzungsverzeichnis

aA	andere Ansicht
Abs.	Absatz
aF	alte Fassung
Art.	Artikel
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BMI	Bundesministerium des Innern, für Bau und Heimat
BMJV	Bundesministerium der Justiz und für Verbraucherschutz
BNDG	Gesetz über den Bundesnachrichtendienst
BR	Bundesrat
BR-Drs.	Bundesrats-Drucksache
BReg	Bundesregierung
BT	Bundestag
BT-Drs.	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
BVerfSchG	Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz
bzw.	beziehungsweise
ca.	circa
ff.	die Folgenden
Fn.	Fußnote
GG	Grundgesetz
ggf.	gegebenenfalls
hM	herrschende Meinung

InsO	Insolvenzordnung
IT-SiG	Entwurf eines zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)
i.V.m.	in Verbindung mit
MADG	Gesetz über den militärischen Abschirmdienst
NetzDG	Netzwerkdurchsetzungsgesetz
noeP	nicht offen ermittelnder Polizeibeamter
Nr.	Nummer
o.g.	oben genannt
OLG	Oberlandesgericht
PolG	Polizeigesetz
Rn.	Randnummer
S.	Seite
sog.	sogenannt
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StrÄndG	Gesetz zur Änderung des Strafgesetzbuches
SÜG	Sicherheitsüberprüfungsgesetz
TKÜ	Telekommunikationsüberwachung
TMG	Telemediengesetz
u.a.	unter anderem
usw.	und so weiter
u.U.	unter Umständen
Var.	Variante
vgl.	vergleiche
z.B.	zum Beispiel
Ziff.	Ziffer

Eigenständigkeitserklärung

Hiermit versichere ich, dass ich die vorliegende Masterarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe, alle Ausführungen, die anderen Schriften wörtlich oder sinngemäß entnommen wurden, kenntlich gemacht sind und die Masterarbeit in gleicher oder ähnlicher Fassung noch nicht Bestandteil einer Studien- oder Prüfungsleistung war.

XX, den_____