# II. Kapitel
# Ermittlungen im Internet

## 1. Online-Streife

Von grundlegender Bedeutung für die Bewertung der Grundrechtsrelevanz von Internetermittlungen ist die Entscheidung des *BVerfG* zur Online-Durchsuchung.[1] Das Gericht hat darin dogmatische Aussagen zur allgemeinen Internet-Aufklärung staatlicher Behörden getroffen.[2] Die Kenntnisnahme öffentlich zugänglicher Informationen im Internet ist danach dem Staat grundsätzlich nicht verwehrt. Ein Grundrechtseingriff liegt dann nicht vor, wenn der Staat lediglich im Internet öffentlich zugängliche Kommunikationsinhalte wahrnimmt, etwa wenn die Behörde nicht zugangsgesicherte Webseiten oder Blogs einsieht.

Datenerhebungen aus „allgemein zugänglichen Quellen" sind regelmäßig nicht als Eingriffe in das Grundrecht auf informationelle Selbstbestimmung zu qualifizieren – mangels Schutzwürdigkeit des Betroffenen.[3] Derlei „Datenerhebungen" sind jedermann möglich.[4] Der Begriff der allgemein zugänglichen Quelle entspricht dem in Art. 5 Abs. 1 Satz 2 GG. Danach ist eine Informationsquelle „allgemein zugänglich", wenn sie technisch geeignet und dazu bestimmt ist, der Allgemeinheit, d. h. einem individuell nicht bestimmbaren Personenkreis, Informationen zu verschaffen. Hierzu gehören Telefonbücher, Branchenverzeichnisse, Handelsregister, aber auch Internetsuchmaschinen wie Google. Denn Informationen, die jedermann zu beliebigen Zwecken zugänglich sind, werden auch der Polizei nicht verwehrt, wenn sie diese Daten zur Aufgabenerfüllung benötigt. Daher liegt kein Eingriff in das allgemeine Persönlichkeitsrecht vor, wenn eine staatliche Stelle im Internet verfügbare Kommunikationsinhalte erhebt, die sich an jedermann oder zumindest an einen nicht weiter abgegrenzten Personenkreis richten.

Die Schwelle zu einem Eingriff in das Recht auf informationelle Selbstbestimmung kann jedoch überschritten sein, wenn Informationen, die durch die Sichtung allgemein zugänglicher Inhalte gewonnen wurden, **gezielt zusammengetragen**, gespeichert und ggf. unter Hinzuziehung weiterer

1 BVerfG NJW 2008, 822: Online-Durchsuchung; dazu *Biemann*, S. 68 ff. Grundlegend zu Ermittlungen im Internet und in sozialen Netzwerken *Keller*, S. 206 ff. Zur Analyse der Möglichkeiten und Grenzen in rechtlicher und tatsächlicher Hinsicht *Schön*, S. 81 ff.

2 Zusammenfassend *Keller*, Kriminalistik 2009, 487 (493).

3 *Braun*, PSP 1/2013, 33 ff.

4 Grundlegend zur Internetrecherche *Kleile*, S. 93 ff.

Daten ausgewertet werden und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt.[5]

Eine virtuelle Streife ist regelmäßig nicht als Grundrechtseingriff zu werten, eine spezifische Ermächtigungsgrundlage mithin nicht erforderlich[6]; es muss lediglich der polizeiliche Aufgabenbereich eröffnet sein.[7] Erst wenn Polizeibeamte jenseits der allgemein zugänglichen Datenbestände unter Verwendung falscher Namen recherchieren bzw. agieren, stellt sich die Frage nach der Ermächtigungsgrundlage.[8]

## 2. Ermittlungen in sozialen Netzwerken[9]

Dass gerade in der virtuellen Welt verschiedene kriminelle Phänomene sich etabliert haben, ist keine neue Erkenntnis.[10] Gerade die Veröffentlichung von strafbaren (Propaganda-)Videos[11], urheberrechtliche Verstöße[12] und insbesondere der Besitz und Konsum kinderpornografischer Schriften[13] sind aufgrund der Anonymität im Internet nur schwer verfolgbare Deliktsbereiche.[14] In geschlossenen Foren werden Kreditkartendaten getauscht, in Online-Communities nehmen Pädophile Kontakt zu Minderjährigen auf, usw.[15]

5 BVerfG NJW 2008, 822: Online-Durchsuchung. Zum IT-Strafprozessrecht Albrecht/IuKR-*Seidl*, Rn. 902 ff.

6 *Brenneisen/Staack*, Kriminalistik 2012, 627 (630); a. A. *Rosengarten/Römer*, NJW 2012, 1764, die die Ermittlungsgeneralklausel heranziehen wollen.

7 *Biemann*, S. 174.

8 *Von der Grün*, S. 142.

9 Instruktiv zu Begriff und Bedeutung von Social Media, *Haug*, Rn. 332 ff. Allgemein zur Rolle der Polizei im Zeitalter des Web 2.0 *Fehr*, 2014.

10 Zu den verschiedenen Phänomenen der Internetkriminalität insbesondere *C/A-Hirsch*, S. 622 ff.; *Büchel/Hirsch*, 2014. Zur Täterstruktur im Kontext von Cyber-Crime *Wernert*, S. 32 ff.

11 *Soiné*, NStZ 2003, 225; *Bär*, MMR 1998, 537, Anm. OLG Nürnberg, MMR 1998, 535: Wer über das Internet das religiöse Bekenntnis (hier: durch ein an ein Kreuz genageltes Schwein) beschimpft, macht sich gem. § 166 StGB strafbar.

12 Die Regelungen des Urheberrechts gelten auch bei der Nutzung des Internets, und zwar sowohl beim Bezug des Angebots aus dem Netz als auch bei der Gestaltung von Inhalten, die u. a. wieder im Netz veröffentlicht werden; *Büchel/Hirsch*, S. 107.

13 Der strafbewehrte Besitz kinderpornographischen Materials ist im Übrigen bereits dann gegeben, wenn dieses im Internet gezielt aufgerufen, in den Arbeitsspeicher geladen und am Bildschirm betrachtet wird; *Braun/Keller*, AnwZert ITR 6/2014, Anm. 3; *Braun/Keller*, Kriminalistik 2014, 208 ff. und 293 ff.; *Braun/Keller*, jurisPR-ITR 15/2012, Anm. 3. Wird in einer E-Mail der sexuelle Missbrauch eines Kindes beschrieben, so macht dies die E-Mail nach der Rspr. des BGH noch nicht zu einer kinderpornographischen Schrift; BGH, NJW-Spezial 2013, 472.

14 Mit einer „Checkliste für die Ermittlungspraxis" *Büchel/Hirsch*, S. 125.

15 Spätestens seit der sog. Edathy-Affäre ist die Thematik „Kinderpornografie" in den Fokus einer breiten Öffentlichkeit gerückt; zur Phänomenologie *Büchel/Hirsch*, S. 118 ff. Speziell zur Edathy-Affäre *Braun/Keller*, Kriminalistik 2014, 208 ff. und 283 ff.; *Hoven*, NStZ 2014, 361 ff.; *Krings*, ZRP 2014, 69 ff.; *Frommel*, ZRP 2014, 184 ff.

Die erste Stufe der Ermittlung in sozialen Netzwerken ist der Abruf von Profildaten, die für jedermann, also auch für die Polizei, ohne ein Einloggen in ein soziales Netzwerk frei zugänglich sind. So führt z. B. häufig das „Googeln" des Namens des von der Ermittlungsmaßnahme Betroffenen zu einem Facebook-Profil.[16]

Verdeckte Ermittlungen in sozialen Netzwerken ermöglichen es der Polizei, mit geringem Aufwand umfangreiche, für die Ermittlungsarbeit bedeutsame Informationen zu gewinnen.[17] Soziale Netzwerke gelten als Paradebeispiel für die digitalisierte Aufbereitung von Informationen und digitale Kommunikationsplattformen der heutigen Zeit.[18] So können etwa durch die Einsichtnahme eines Nutzerprofils eine Vielzahl aussagekräftiger personenbezogener Daten über einen Nutzer gewonnen und detaillierte Rückschlüsse über dessen Interessen, Aktivitäten, Aufenthaltsorte und soziale Bindungen gezogen werden.[19]

Im Gegensatz zur realen Welt können Identitäten aber nur eingeschränkt überprüft werden. Gem. § 13 Abs. 6 TMG hat der Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.

Eine Möglichkeit, sich auch zu geschützten Bereichen einen Zugang zu verschaffen oder um andere User zur Preisgabe von Informationen zu veranlassen, ist das **legendierte Vorgehen** im Internet. Bei virtuellen Ermittlungen im Cyberspace wird auch von Cyber-VE oder Cyber-NoeP gesprochen.[20] Wird durch Datenerhebung in das Grundrecht auf informationelle Selbstbestimmung eingegriffen, ist eine formell-gesetzliche Ermächtigung auch bei Ermittlungen im Internet erforderlich.

Aus der Perspektive der Grundrechtsträger können dabei bedeutsame prozessuale Positionen betroffen sein. Diese erstrecken sich auf die Freiheit der Selbstbezichtigung (nemo tenetur se ipsum accusare), auf den fair-trial-Grundsatz (Art. 6 EMRK) und das Erheben personenbezogener Daten (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG).

Das Kommunizieren eines polizeilichen Ermittlers unter Verschleierung seiner wahren Identität mit einer Zielperson (z. B. in einem Chat) stellt bei Zugrundelegung des formalen Vernehmungsbegriffs keine Vernehmung dar. Denn darunter ist das offene Auftreten in amtlicher Funktion zu verstehen,

16 *Seidl/Beyvers*, AnwZert-ITR 15/2011, Anm. 3.

17 Die StPO beinhaltet keinen Grundsatz der Offenheit staatlichen Handelns. Aus der Rspr. des BVerfG resultiert, dass „verdecktes bzw. heimliches Handeln der Polizei als solches nicht gegen das im Gebot des fairen Verfahrens verankerte Täuschungsverbot verstößt". (BVerfG NJW 2004, 999).

18 *Fehr*, S. 17.

19 *Braun/Klose*, AnwZert 15/2013, Anm. 2.

20 *Bönisch/Bretschneider*, Die Polizei 2013, 99.

bei der der Vernehmende vom Beschuldigten Auskunft verlangt.[21] Dies hat zur Folge, dass z. B. Eröffnungs- oder Belehrungspflichten (z. B. § 52 Abs. 3, § 55 Abs. 2, § 136 Abs. 1 StPO) nicht zu beachten sind.[22] Jedoch darf die Kommunikation mit Zielpersonen nicht dazu genutzt werden, um bewusst deren Auskunfts-, Zeugnis- oder Aussageverweigerungsrechte auszuhebeln. Daher ist auch ein mittels Zwang, Drohung oder erheblichem Bedrängen untermauertes Befragen eines Beschuldigten bzw. Zeugen, wodurch dessen vorheriges Berufen auf sein Schweigerecht umgangen werden soll, eindeutig unzulässig.[23]

Die Beantwortung der Frage, welche Ermächtigung im Einzelfall in Betracht kommt, ist davon abhängig, wie die Maßnahme zu qualifizieren ist. Dabei reicht die Bandbreite von schlicht-hoheitlichen Maßnahmen, d. h. Maßnahmen ohne Grundrechtsrelevanz, bis zu sog. NoeP und Verdeckten Ermittlern.[24] Zu beachten ist die Intensität der Maßnahmen. Die Persönlichkeit einer Person wird besonders dann betroffen sein, wenn die Datenerhebungen der Bestätigung oder Schaffung eines Anfangsverdachts i.S. des § 152 Abs. 2 StPO dienen und ggf. in einem Ermittlungsverfahren gegen den „Betroffenen" verwandt werden.[25]

Verdeckte Ermittlungen in sozialen Netzwerken erfolgen dabei überwiegend auf Grundlage der strafprozessualen Befugnis- oder Ermittlungsgeneralklauseln.[26]

## 2.1 Datenerhebung aus allgemein zugänglichen Quellen

Der Begriff der „allgemein zugänglichen Quellen" entspricht Art. 5 Abs. 1 Satz 2 GG. Danach ist eine Informationsquelle „allgemein zugänglich", wenn sie technisch geeignet und dazu bestimmt ist, der Allgemeinheit, d. h. einem individuell nicht bestimmbaren Personenkreis, Informationen zu verschaffen.[27] Hierzu gehören Telefonbücher, Branchenverzeichnisse, Handelsregister, aber auch Internetsuchmaschinen wie Google. Denn Informationen, die jedermann zu beliebigen Zwecken zugänglich sind, werden auch der Polizei nicht verwehrt, wenn sie diese Daten zur Aufgabenerfül-

21 *Meyer-Goßner/Schmitt*, § 136a Rn. 4; HK/StPO-*Ahlbrecht*, § 136a Rn. 6.

22 *Artkämper/Schilling*, Rn. 116 ff.

23 Zu den „verbotenen Mitteln und Methoden" insbesondere SSW/StPO-*Eschelbach*, § 136a Rn. 16 ff.

24 *Bönisch/Bretschneider*, Die Polizei 2013, 99.

25 *Biemann*, S. 175; *Rosengarten/Römer*, NJW 2012, 1764 (1765); *Henrichs*, Kriminalistik 2011, 622.

26 *Soiné*, NStZ 2014, 248 (251). Allerdings kommen die Ermächtigungen nicht zur Anwendung bei Maßnahmen ohne Eingriffscharakter. Bei nicht grundrechtsrelevanten Ermittlungshandlungen im Internet stellt sich die Frage nach einer speziellen Rechtsgrundlage nicht, *Rosengarten/Römer*, NJW 2012, 1764 (1766); so auch H/M-T-*Esser*, 7. Kap., Rn. 335.

27 BVerfGE 27, 71 (83).

lung benötigt. Daher liegt kein Eingriff in das allgemeine Persönlichkeitsrecht vor, wenn eine staatliche Stelle im Internet verfügbare Kommunikationsinhalte erhebt, die sich an alle oder zumindest an einen nicht weiter abgegrenzten Personenkreis richten.

Die Schwelle zu einem Eingriff in das Recht auf informationelle Selbstbestimmung kann jedoch überschritten sein, wenn Informationen, die durch die Sichtung allgemein zugänglicher Inhalte gewonnen wurden, gezielt zusammengetragen, gespeichert und ggf. unter Hinzuziehung weiterer Daten ausgewertet werden und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt.

Die Erhebung und Verarbeitung **anonymer Daten** und **pseudonymisierten Daten** im Internet hat nur Eingriffscharakter, wenn es sich um personenbezogene Daten handelt. Der Definition des personenbezogenen Datums kommt eine zentrale Rolle zu, denn sie eröffnet den Anwendungsbereich des datenschutzrechtlichen Regimes.[28] Die erforderliche Personenbezogenheit des Datums besteht zunächst, wenn es eine Information über eine identifizierte, d. h. konkret benannte Person enthält. Ist die Person, auf die sich die Daten beziehen, nicht benannt, bleibt die Personenbezogenheit der Information bestehen, wenn die betroffene Person identifizierbar ist, d. h. ermittelt werden kann.[29]

In der DS-GVO wird der **Begriff Anonymisierung** nicht definiert. Anonymisieren ist das Verändern personenbezogener Daten derart, dass die hinter den Einzelangaben über persönliche oder sachliche Verhältnisse stehende betroffene Person nicht bzw. nicht mehr identifiziert werden kann. Dies ist ein Mehr gegenüber der Pseudonymisierung, bei der die Hinzuziehung zusätzlicher, aber getrennt aufbewahrter Informationen zur Identifikation genügt. Die Grundsätze des Datenschutzrechtes sind auf anonyme Daten nicht anwendbar.[30] **Anonyme Daten** sind mithin keine personenbezogenen Daten. In der sog. JI-Richtlinie des Europäischen Parlaments zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (RL 2016/680/EU) vom 27.04.2016 wird festgelegt, dass die Grundsätze des Datenschutzes nur dann nicht für anonyme Informationen gelten sollen, wenn eine Anonymisierung dergestalt stattgefunden hat, dass eine Identifizierung der betroffenen Person nicht mehr möglich ist (Erwägungsgrund 21 RL 2016/680/EU).[31]

Dagegen wird in der DS-GVO **Pseudonymisierung** definiert als die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezoge-

28 *Krügel*, ZD 2017, 455 ff.; *Schmitz*, ZD 2018, 5 ff.

29 *Gola-Piltz*, Art. 4 DSGVO, Rn. 4 f.

30 P/P-*Ernst*, Art. 4 DSGVO, Rn. 48.

31 Dazu *Johannes/Weinhold*, Rn. 309.

nen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Ein Pseudonym ist der erfundene, die wahre Identität einer Person verdeckende Name. Dieser Name wird z. B. in Form einer Ordnungsziffer oder sonstigen Kennzeichen der betroffenen Person von dem für die Verarbeitung der Daten Verantwortlichen zugewiesen, wobei die Möglichkeit der Feststellung der wahren Identität nicht verloren gehen soll. Bei **pseudonymisierten Daten** handelt es sich weiterhin um personenbezogene Daten mit der Folge, dass die Vorgaben der DS-GVO umfassend zu beachten sind.[32]

## 2.2 Staatlich gelenkte Kommunikationsbeziehungen

Nach der Rechtsprechung des *BVerfG* zur Online-Durchsuchung[33] ist das Vertrauen in die Identität und Wahrhaftigkeit der Kommunikationsteilnehmer im Internet wegen fehlender Überprüfungsmechanismen nicht schutzwürdig. Dies soll auch dann gelten, wenn bestimmte Personen – etwa in Diskussionsforen – über einen längeren Zeitraum an der Kommunikation teilnehmen und sich auf diese Weise eine Art „elektronische Gemeinschaft" gebildet habe. Jedem Teilnehmer sei bewusst, dass er die Identität seiner Partner nicht kenne bzw. deren selbstbezogenen Angaben nicht überprüfen könne. Deshalb sei sein Vertrauen darauf, dass er nicht mit einer staatlichen Stelle kommuniziere, nicht schutzwürdig.[34] Nach Auffassung des *BVerfG* ist bei staatlich gelenkten Kommunikationsbeziehungen zu Grundrechtsträgern im Internet im Grunde nicht von einem Eingriff auszugehen.[35]

In der Literatur wird vor diesem Hintergrund angenommen, dass ein Grundrechtseingriff der Beteiligten eines überwachten geschlossenen Chats nicht vorliegt, wenn die Strafverfolgungsbehörden den von einem Teilnehmer freiwillig zur Verfügung gestellten Zugangscode nutzen.[36] Nicht schutzwürdig seien daher auch unvertraute, auf Täuschung angelegte Kontakte verdeckt ermittelnder Polizeibeamter mit Zielpersonen.[37] Auf die Kommunikationsform, etwa mit persönlich-bildlicher Wahrnehmungsmöglichkeit (Voice-over-IP einschließlich Bildübertragung, z. B. Skype oder Facetime), könne es ebenso wenig ankommen wie auf deren Häufigkeit.[38]

32 *Scheurer*, AnwZert ITR 24/2017, Anm. 2; differenzierend *Roßnagel*, ZD 2018, 243 ff. Eine einfache Einordnung aller pseudonymen Daten als personenbezogen wird der Vielfalt und den unterschiedlichen Funktionsweisen pseudonymer Daten nicht gerecht. Vielmehr ist zwischen einer anonymisierenden und einer risikomindernden Pseudonymisierung zu unterscheiden.

33 BVerfG NJW 2008, 822.

34 BVerfG NJW 2008, 822 (836).

35 *Soiné*, NStZ 2014, 248 (249).

36 *Müller*, Kriminalistik 2012, 295, 296.

37 *Soiné*, NStZ 2014, 248 (249).

38 *Seidl/Beycers*, AnwZert ITR 15/2011 Anm. 3; *Henrichs*, Kriminalistik 2012, 632 (633 ff.).

Diese Auffassung ist gleichwohl strittig. Verbleibt ein Beamter nämlich längere Zeit unter aktiver Teilnahme im Chat und musste er zur Anmeldung seine Existenz durch eine aufwändige Legende, die auch Probegeschäfte und Leumundszeugen beinhalten kann, belegen (im Extremfall mittels Kreditkarte oder gar Post-Ident-Verfahren), so wird er auch als Verdeckter Ermittler (§§ 110a ff. StPO) eingestuft, auch wenn sich die Ermittlungen noch nicht gegen einen bestimmten Beschuldigten richten. Dies beruht maßgeblich auf der Überlegung, dass zum einen das Vertrauen in die Identität der Teilnehmer nunmehr schutzwürdig wäre, und zum anderen, dass eine dauerhafte und aktive Täuschung eines unbestimmten Personenkreises erfolgt.[39]

## 2.3 Kriminalistische List[40]

Zur Kriminaltaktik zählt auch die Anwendung (zulässiger) kriminalistischer List.[41] Erfolgt ein einmaliger Zugriff auf einen geschützten Bereich nach vorheriger unpersönlicher Kontaktaufnahme über eine hierfür vorgesehene Funktion (z. B. „Freundschaftsanfrage“ in Facebook) und wird durch dieses Vorgehen der „Zielperson“ lediglich signalisiert, dass ein anderer Accountinhaber einen Kontaktwunsch hat, ohne dass der Anfragende eine persönliche Nachricht formuliert, so fällt dieses Vorgehen als „unterste Schwelle“ polizeilichen Eingriffshandelns unter die kriminalistische List.[42] Dieses Vorgehen findet seine Rechtfertigung auf strafprozessualer Ebene in der Ermittlungsgeneralklausel (§§ 161, 163 StPO).[43]

Nutzt eine im Internet unter Legende ermittelnde Person schutzwürdiges Vertrauen eines Grundrechtsträgers in die Identität und Motivation seines Kommunikationspartners aus, um persönliche Daten zu erheben, die sie ansonsten nicht erhalten würde, liegt nach Auffassung des *BVerfG* ein Eingriff in das Recht auf informationelle Selbstbestimmung des Betroffenen vor.[44] Damit stellt das Gericht maßgeblich darauf ab, ob der Grundrechtsträger darauf vertrauen darf, dass seine Vorstellung von der Identität und Moti-

39 *Rosengarten/Römer*, NJW 2012, 1764 (1767).

40 Grundlegend zur kriminalistischen List im Ermittlungsverfahren *Soiné*, Kriminalistik 2010, 596 ff.: Obwohl erst seit dem späten 19. Jahrhundert von einer wissenschaftlich fundierten Kriminalistik gesprochen werden kann, ist der Begriff der List schon wesentlich länger ein fester Bestandteil der deutschen Sprache. Er wurde im ursprünglichen Sinne – moralisch neutral – als Klugheit, Schlauheit, Kenntnis, Wissen oder Geschicklichkeit verstanden. Nach einer neueren Ansicht soll die List – negativ – das Vermögen sein, sich zur Erlangung des eigenen Vorteils einer Täuschung zu bedienen; das charakteristische, listkonstituierende Element sei die Irreführung des Gegenübers. Das moralische Negativbild der List wird nicht zuletzt auf die Heimlichkeit zurückgeführt.

41 *Soiné*, S. 19.

42 *Bönisch/Bretschneider*, Die Polizei 2013, 99 (102).

43 *Müller*, Kriminalistik 2012, 295 ff.; *Henrichs/Wilhelm*, Kriminalistik 2010, 30 ff.

44 BVerfG NJW 2008, 822.

vation der verdeckt ermittelnden Person mit der Wirklichkeit übereinstimmt.[45]

**Beispiel:**
Ein Polizeibeamter gibt sich als Bruder einer per Haftbefehl zur Fahndung ausgeschrieben Zielperson aus und lokalisiert diese mittels zahlreicher Kommunikationskontakte. Hier täuscht die Polizei und enttäuscht Vertrauen, das als schutzwürdig einzustufen ist.

Die Begründung der grundrechtlichen Schutzwürdigkeit hängt gleichwohl dann ab, ob durch das Anmeldeverfahren auf der Plattform eine individuelle Bestimmtheit des zugangsberechtigten Personenkreises erreicht werden kann. Dabei gilt, dass die Kenntnisnahme eines der Öffentlichkeit innerhalb eines anmeldepflichtigen Dienstes zur Verfügung gestellten Inhalts jedenfalls dann nicht grundrechtsrelevant ist, wenn die Anmeldung anonym oder unter einem Pseudonym jederzeit möglich ist.[46] Denn die Ermittlungsbehörde nutzt in diesen Fällen kein schutzwürdiges Vertrauen des Betroffenen in die Identität und die Motivation seines Kommunikationspartners aus, um persönliche Daten zu erheben, die sie sonst nicht erhalten würde. Ein Grundrechtseingriff könnte allenfalls dann angenommen werden, wenn sich alle Teilnehmer, und damit auch der Polizeibeamte, unter Angabe echter Personaldaten bei der Plattform registrieren müssen, der vollständige Name im Userprofil erscheint und seitens des Anbieters eine Überprüfung der Anmeldedaten stattfindet.[47]

Grundsätzlich liegt bei Ermittlungen von Polizeibeamten in sozialen Netzwerken unter einer Legende bei einer Datenerhebung durch Ausnutzung des Vertrauens des Kommunikationspartners in die Identität seines Gegenübers ein Eingriff in das Recht auf informationelle Selbstbestimmung vor. Obwohl die Kommunikation im Internet gerade darauf angelegt ist, die eigene Identität nicht zwangsläufig preisgeben zu müssen, ist jedenfalls der Versuch von Polizeibeamten, sich unter Ausnutzung eines Irrtums oder gar einer Täuschung über ihre Identität Zugang zu diesen geschlossenen Foren zu verschaffen, grundrechtsrelevant. In den Fällen, in denen „schutzwürdiges Vertrauen des Betroffenen in die Identität und Motivation seines Kommunikationspartners schutzwürdig ist und dies (durch die Polizei) ausgenutzt wird, um persönliche Daten zu erheben, die sie ansonsten nicht erhalten würde," ist jedenfalls von einem Eingriff in das Recht auf informationelle Selbstbestimmung auszugehen.[48] Der Anbieter hat durch sein Vorgehen

45 *Bönisch/Bretschneider*, Die Polizei 2013, 99 (100).
46 *Seidl/Beyvers*, AnwZert ITR 15/2011, Anm. 3.
47 *Seidl/Beyvers*, AnwZert ITR 15/2011, Anm. 3.; *Braun*, PSP 1/2013, 33 (35).
48 BVerfG NJW 2008, 822, Anm. *Bär, MMR 2008, 315*: Online-Durchsuchung.

deutlich gemacht, dass die Daten gerade nicht frei zugänglich sein sollen.[49] Der Eingriff bedarf dann zu seiner Rechtfertigung einer dem Grundsatz der Tatbestandsbestimmtheit und Normenklarheit entsprechenden Eingriffsnorm. Allerdings wird angenommen, dass die Ermittlungsgeneralklausel („Ermittlungen jeder Art") zu unbestimmt ist, „um diesen schwerwiegenden, nur auf der Grundlage einer Täuschung des Grundrechtsträgers ermöglichten Eingriff rechtfertigen zu können".[50] Dieser Ansicht folgend ist dann auf §§ 110a ff. StPO abzustellen.[51]

## 2.4 Abgrenzung: Nicht offen ermittelnder Polizeibeamter vs. Verdeckter Ermittler

Die StPO kennt neben verdeckten Ermittlern auch sonstige nicht offen ermittelnde Polizeibeamte. NoeP sind deutsche Polizeibeamte, die einzelfallbezogen (nur gelegentlich) verdeckt tätig werden und nicht weiter in die konkreten polizeilichen Ermittlungen eingebunden sind.[52] Diese treten vor allem im Bereich der Drogendelinquenz als Scheinaufkäufer in Erscheinung. Hierbei kaschieren sie ihre staatliche Anbindung. In aller Regel benutzen sie während ihres Einsatzes Tarnnamen; zuweilen verfremden sie ihre Identität in umfassender Weise, sodass Unterschiede zur Legende eines verdeckten Ermittlers zuweilen kaum noch erkennbar sind (sog. qualifizierte Scheinaufkäufer).[53]

Als Rechtsgrundlage kommen in Betracht im repressiven Bereich die Ermittlungsgeneralklausel, wenn der sich den Zutritt verschaffende Beamte zum sozialen Netzwerk als bloßer „virtuell nicht offen ermittelnder Polizeibeamter (VNoeP)" zu beurteilen ist, oder §§ 110a ff. StPO, wenn dieser als verdeckter Ermittler zu qualifizieren ist.[54]

Der *BGH* hat die maßgeblichen Aspekte genannt, die einen VE-Einsatz ausmachen, und insofern eine Abgrenzung zum Einsatz des NoeP vorgenommen.[55] Ein nicht offen eingesetzter Polizeibeamter wird als verdeckter Ermittler im Sinne des § 110a Abs. 2 StPO tätig, wenn er über einen längeren Zeitraum unter Benutzung seiner Legende mit einer oder mehreren Per-

49 *Soiné*, NStZ 2003, 225: Selbst wenn im Internet personenbezogene Daten über Staatengrenzen hinweg transportiert und kommuniziert werden, berühren entsprechende Ermittlungen deutscher Polizeibeamter solange nicht die territoriale Souveränität ausländischer Staaten, als staatliche Hoheitsakte nicht auf fremdem Staatsgebiet ohne Erlaubnis des ausländischen Staates vorgenommen oder durchgesetzt werden; vgl. *Soiné*, NStZ 1997, 166 (in Bezug auf Internet-Fahndungen).

50 *Kutscha/Thome*, S. 41.

51 *Rosengarten/Römer*, NJW 2012, 1764 (1767).

52 BGH NStZ 1996, 450; BGH, NStZ 1997, 294.

53 Zur Abgrenzung: *Schneider*, NStZ 2004, 359 ff.

54 H/M-T-*Esser*, 7. Kap., Rn. 342 ff.

55 BGH NStZ 1005, 2237. v. 07.03.1995 – 1 StR 685/94.

sonen (hier: über den Erwerb von Betäubungsmitteln) verhandelt, mag auch der Kontakt zu einzelnen Verhandlungspartnern nur kurz sein. „Ob der Einsatz eines verdeckt ermittelnden Polizeibeamten auf Dauer angelegt ist und deshalb den strengen Auflagen der §§ 110a ff. StPO unterliegt, ist durch eine Gesamtwürdigung aller Umstände festzustellen. Dabei kann es auf zeitliche Mindestgrenzen nicht ankommen (…).[56] Entscheidend ist, ob der Ermittlungsauftrag 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 geheim gehalten 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."[57]

Die Abgrenzung von NoeP und verdecktem Ermittler bereitet gleichwohl Schwierigkeiten, wenn man die vom *BGH* zum „Scheinkauf von Drogen" entwickelten Abgrenzungskriterien[58] heranziehen will. Denn diese sind bis auf wenige Kriterien, wie etwa Art und Umfang der Legende und die Dauer des verdeckten Einsatzes, nicht auf die Besonderheiten von Ermittlungshandlungen im Internet übertragbar.[59]

Gleichwohl führt es zu weit, wenn aufgrund dieser „fehlenden Vergleichbarkeit" mit herkömmlichen Einsätzen verdeckter Ermittler nach §§ 110a ff. StPO die Schlussfolgerung gezogen wird, dass alle verdeckten Maßnahmen in sozialen Netzwerken bei Vorliegen der (niedrigschwelligen) Voraussetzungen der Ermittlungsgeneralklausel gerechtfertigt wären.[60]

Erforderlich sind (neue) Abgrenzungskriterien, die an Sinn und Zweck der Unterscheidung zwischen („bloßem") „NoeP" und „verdecktem Ermittler" anknüpfen.

Erste Abgrenzungskriterien hierfür werden von *Rosengarten* und *Römer* angeführt[61]: Nachdem der Zugriff auf personenbezogene Daten in sozialen Netzwerken durch den jeweiligen Nutzer oder Gruppenmoderator kontrolliert wird, ist jeweils im Einzelfall die „Intensität der Zugangskontrolle" zu einem geschlossenen Bereich zu berücksichtigen, die anhand einer Legende überwunden werden muss.[62] Weiterhin ist von entscheidender Bedeutung,

56 A. A. *Kraushaar*, Kriminalistik 1994, 481 (482), Mindestdauer 6 Monate.
57 BGH NJW 1995, 2237.
58 BGH NJW 1996, 2108.
59 *Rosengarten/Römer*, NJW 2012, 1764 (1765).
60 So aber *Henrichs*, Kriminalistik 2012, 632 (633).
61 *Rosengarten/Römer*, NJW 2012, 1764 (1765).
62 *Rosengarten/Römer*, NJW 2012, 1764 (1767).