KriPoZ Kriminalpolitische Zeitschrift JuP

„Junges Publizieren“

Seminararbeit von

Isabel Ruiz de Vargas Staudacher

Die Übernahme digitaler Accounts durch Strafverfolgungsbehörden

Betreuer/ Korrektor: Prof. Dr. Mark A. Zöller
Universität/ Fachbereich: Ludwig-Maximilians-Universität München/Cybercrime
Abgabedatum: 18. April 2023 – Bearbeitungsstand: 16. Oktober 2023

Inhaltsverzeichnis

I. Verdeckte Identitätsübernahme als Ermittlungsmethode

Im Jahr 2016 konnte das Zollkriminalamt den Waffenhändler festnehmen, der als „Rico" im Darknet dem Amokläufer des Attentats 2016 in München im OEZ die tödliche Waffe verkauft hatte.[1] Zuvor hatten sich die Beamten Zugriff auf den Darknet-Account eines anderweitig verfolgten Käufers illegaler Waffen verschafft und traten getarnt mit „Rico" in Kontakt, um ein fingiertes Waffengeschäft abzuwickeln, das letztlich mit der Festnahme endete.[2] Eine ausdrückliche Ermächtigungsgrundlage für diese Übernahme digitaler Accounts durch Strafverfolgungsbehörden kennt das geltende Recht nicht. Deshalb macht es sich diese Arbeit zur Aufgabe, die Grenzen der Zulässigkeit dieser Ermittlungsmethode aufzuzeigen und die Notwendigkeit einer eigenständigen Ermächtigungsgrundlage zu diskutieren. Dabei soll zunächst die Bedeutung, die diese Ermittlungsmethode für die Strafverfolgung hat, dargestellt werden. Im Anschluss hieran werden mit Blick auf die StPO sowie auf die Grundrechte die Möglichkeiten und Grenzen eines staatlichen Zugriffs auf den Account sowie seine Weiterführung aufgezeigt. Sodann erfolgt eine kritische Würdigung des 2019 veröffentlichten, ersten Referentenentwurfs zum IT-Sicherheitsgesetz 2.0, der eine eigenständige Ermächtigungsgrundlage vorsah.

II. Bedeutung der Ermittlungsmethode für die Strafverfolgung

1. Empirische Relevanz

Wie häufig Beamte der deutschen Strafverfolgungsbehörden digitale Accounts übernehmen (sog. verdeckte Identitätsübernahme[3]) und für die verdeckte Strafverfolgung nutzen, ist nicht bekannt. Die Bundesregierung teilte im Jahr 2017 mit, dass die Zollfahndungsämter keine Statistik über die Verwendung fremder digitaler Accounts für Ermittlungszwecke führen.[4] Das Bundeskriminalamt teilte für die Jahre 2014 bis 2017 eine Nutzung von vier übernommenen Accounts mit und die Bundespolizei gab an, in den Jahren 2016 und 2017 insgesamt 36 Accounts übernommen zu haben.[5] Unerwähnt blieb dabei, welche Deliktsbereiche betroffen waren sowie welche Internetdienste genutzt wurden.[6] In Betracht kommt somit sowohl eine Übernahme von Accounts im Clearnet, dem offen zugänglichen Bereich des Internets, als auch im Darknet, das nur durch Anonymisierungsnetzwerke (z.B. das TOR-Netzwerk) erreichbar ist.[7]

2. Ermittlungstechnische Relevanz

Auf personale Ermittlungsmethoden wie die verdeckte Identitätsübernahme wird im Internet bspw. dann zurückgegriffen, wenn klassische technische Ermittlungsmaßnahmen wie etwa die Datenerhebung (z.B. Abfragen von Verkehrs- und Bestandsdaten, §§ 100g, 100j StPO), die Überwachung (z.B. Telekommunikationsüberwachung,

---

1 *Förster*, Der Händler des Todes, Frankfurter Rundschau (25.8.2019), online abrufbar unter: https://www.fr.de/panorama/haendler-todes-11023265.html (zuletzt abgerufen am 21.3.2023).
2 *LG München I*, BeckRS 2018, 5795 Rn. 543 ff.
3 *Sieber*, Straftaten und Strafverfolgung im Internet: Gutachten C zum 69. Deutschen Juristentag, 2012, S. C 126.
4 BT-Drs. 19/116, S. 3.
5 Vgl. BT-Drs. 19/116, S. 3.
6 *Wittmer*, Straftaten und Strafverfolgung im Darknet, in: Zöller, Deutsches und Europäisches Strafprozessrecht und Polizeirecht, Bd. 17, 2023, S. 146.
7 Vgl. *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl. (2018), Rn. 1641; BSI, Darknet und Deep Web – wir bringen Licht ins Dunkle, online abrufbar unter: https://www.bsi.bund.de/dok/13462614 (zuletzt abgerufen am 21.3.2023).

§ 100a StPO) oder eine Beschlagnahme der genutzten Server (§ 94 StPO) nicht denselben Ermittlungserfolg versprechen.[8] Insbesondere im Darknet sind solche technischen Ermittlungsmethoden aufgrund des verschlüsselten Aufbaus, der eine Verschleierung der Identität des Nutzers zur Folge hat, regelmäßig aussichtslos.[9] Deshalb erzielen die Strafverfolgungsbehörden mit verdeckten personalen Ermittlungen im Darknet – die Anonymität ausnutzend[10] – deutlich bessere Ermittlungsergebnisse.[11] Zunächst beobachten und sichern die Ermittler öffentlich zugängliche Daten, bevor sie dann auf den relevanten Plattformen verdeckt in Erscheinung treten und zu anderen registrierten Personen Kontakt aufnehmen.[12] Hierfür erstellen sie sich entweder einen sog. „Fake-Account" oder übernehmen bereits bestehende Accounts Dritter. Letzteres ist im Vergleich in der Regel effektiver, da diesen Accounts von anderen Nutzern ein größeres Vertrauen entgegengebracht wird (sog. „credibility"), da diese etwa schon länger in der Szene aktiv gewesen sind oder bereits kriminell in Erscheinung getreten sind.[13] Zudem gestaltet es sich einfacher für die Ermittler sog. „Scheingeschäfte" mit Verdächtigen in die Wege zu leiten, wenn eine „credibility" besteht.[14] Die Ermittlungsmethode der verdeckten Identitätsübernahme wird vor allem zur Identifizierung krimineller virtueller Identitäten eingesetzt.[15] Sie ist damit regelmäßig „der erste Schritt zur Verlagerung der Ermittlungen in die ‚analoge' Welt."[16] Mit dieser Kombination von digitalen und analogen Ermittlungsmethoden konnten in den Jahren 2015 und 2016 im Darknet rund um die mittlerweile beschlagnahmte Plattform „Deutschland im Deep Web", die auch der Waffenhändler des Münchner Amokläufers nutzte, etwa 30 Waffenhändler überführt werden.[17] Ein weiterer Vorteil dieser Ermittlungsmaßnahme im Darknet ist, dass sog. „Keuschheitsproben" umgangen werden können.[18] Unter „Keuschheitsproben" versteht sich die Begehung einer Straftat, etwa das Hochladen von kinderpornografischem Material, wodurch sich der Nutzer beweisen muss, um in zugangsbeschränkten Foren aufgenommen zu werden.[19] Da die Begehung von Straftaten den Ermittlern untersagt ist,[20] werden strafbewehrte Handlungen vermieden, wenn ein bereits aufgenommener Account übernommen wird.[21]

III. Zugriff auf bestehende digitale Accounts

Für die Übernahme und die spätere Nutzung eines bereits bestehenden Accounts müssen die Strafverfolgungsbehörden sich zunächst Zugriff auf ebendiesen Account verschaffen. In Betracht kommt hierfür eine freiwillige Herausgabe sowie eine Beschlagnahme des Accounts (§ 94 StPO oder §§ 111b ff. StPO). Die Ausführungen gelten sowohl für digitale Accounts im Darknet als auch im Clearnet. Als digitaler Account wird die Zugangsberechtigung einer Person zu einem zugangsbeschränkten IT-System im Internet verstanden, das zur Kommunikation mit anderen Personen verwendet werden kann. Der Account-Zugang besteht regelmäßig aus einem Nutzernamen und einem Passwort (sog. Zugangsdaten).

---

8 Vgl. für das Darknet: *Krause,* NJW 2018, 678 (679); *Zöller,* KriPoZ 2019, 274 (276).
9 Vgl. *Krause,* NJW 2018, 678 (679); *Vogt,* Kripo 2017, 4 (6).
10 *Sieber*, S. C 125.
11 *Fünfsinn/Ungefuk/Krause,* Kriminalistik 2017, 440 (444).
12 Vgl. *Krause,* NJW 2018, 678 (679 f.).
13 *Krause,* NJW 2018, 678 (680).
14 Vgl. *Rath,* DRiZ 2016, 292 (293).
15 Vgl. *Fünfsinn/Ungefuk/Krause,* Kriminalistik 2017, 440 (444).
16 *Grözinger*, in: Müller/Knauer/Schlothauer: Münchener Anwalts Handbuch Strafverteidigung, 3. Aufl. (2022), § 50 Rn. 245.
17 Vgl. *Fittkau*, Die Darknet-Ermittler von Gießen: Interview mit Benjamin Krause von der Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT), Deutschlandfunk Kultur (9.8.2016), online abrufbar unter: https://www.deutschlandfunkkultur.de/kriminalitaet-die-darknet-ermittler-von-giessen.2165.de.html?dram:article_id=362524 (zuletzt abgerufen am 22.3.2023).
18 Vgl. *Krause,* NJW 2018, 678 (680).
19 *Safferling,* DRiZ 2018, 206 (206 f.).
20 Vgl. RiStBV Anl. D Ziff. II Nr. 2.2.
21 Hiergegen wenden sich neuartige Gegenmaßnahmen der Kriminellen, s. *Von Westernhagen,* c't Security 2019, 18 (22 f.).

1. Freiwillige Herausgabe

Zunächst besteht die Möglichkeit, dass die Beamten während eines laufenden Strafverfahrens im Wege einer freiwilligen Herausgabe der Zugangsdaten durch den Beschuldigten einen Zugriff auf den Account erlangen.[22] Teil dessen ist auch die Einwilligung zur Abänderung der Zugangsdaten durch die Behörden, um eine anschließende exklusive Nutzung zu gewährleisten. Ein Beweggrund der beschuldigten Account-Inhaber könnte sein, durch die Herausgabe Einsicht und Reue als Nachtatverhalten aufzuweisen, was wiederum bei einer Verurteilung einen positiven Einfluss auf die Strafzumessung haben könnte (vgl. § 46 Abs. 2 StGB).[23] Außerdem kommt auch die Absicht des Beschuldigten in Betracht, durch die Überlassung der Zugangsdaten Hilfe zur Aufklärung oder Verhinderung von schweren Straftaten i.S.d. § 46b StGB zu leisten, um so eine Strafmilderung nach § 49 Abs. 1 StGB zu erreichen.[24] Aufgrund des Verbots des Versprechens eines gesetzlich nicht vorgesehenen Vorteils (§ 136a Abs. 1 S. 3 StPO) ist die Grenze der freiwilligen Herausgabe erreicht, wenn die Ermittler den Beschuldigten durch z.B. bindende Zusagen zum Strafmaß zur „freiwilligen" Herausgabe der Nutzerdaten verleiten.[25]

2. Beschlagnahme eines digitalen Accounts

a) Anwendungsgrundlagen

Der Zugriff auf den Account könnte, wenn keine freiwillige Herausgabe gelingt, im Rahmen einer Beschlagnahme zu Beweiszwecken (§§ 94 Abs. 1, 98 StPO) oder einer Beschlagnahme zur Sicherung der Einziehung (§ 111b Abs. 1 S. 1 Alt. 1 StPO) erfolgen, wobei dies gegenüber dem Account-Inhaber als offene Ermittlungsmaßnahme durchgeführt wird.[26] Ein heimliches Vorgehen würde hierbei keine (vollständige) Übernahme des Accounts darstellen, da der Inhaber diesen weiter nutzen könnte. Auch ermittlungstaktisch erscheint dies wenig sinnvoll, weil der Inhaber fremde Kommunikation bemerken könnte.[27] §§ 94 Abs. 1, 98 StPO ermächtigen die Strafverfolgungsbehörden dazu, Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein könnten, in Verwahrung zu nehmen oder in anderer Weise sicherzustellen. Hierbei sind digitale Accounts als nichtkörperliche Gegenstände auch vom Anwendungsbereich des § 94 Abs. 1 StPO betroffen, da es „nicht auf eine Körperlichkeit des zu beschlagnahmenden Beweismittels an[kommt]"[28], sondern vielmehr auf die Bedeutung seines Beweiswertes für weitere Untersuchungen.[29] Die erforderliche potentielle Beweisbedeutung liegt regelmäßig vor, wenn mit dem Account etwa in der Vergangenheit illegaler Handel betrieben wurde oder Chatverläufe über Verbrechensabreden existieren.[30] Neben der Beschlagnahme zu Beweiszwecken ist gem. § 111b Abs. 1 S. 1 Alt. 1 StPO auch die Beschlagnahme zur Sicherung der Einziehung in Betracht zu ziehen. Sie dient der Beschlagnahme von einziehungsfähigen Gegenständen i.S.d. § 74 Abs. 1 StGB, die im Gegensatz zu § 94 Abs. 1 StPO keine Beweisbedeutung innehaben.[31] Einziehungsfähige Gegenstände i.S.d. § 74 Abs. 1 StGB sind alle (un-)beweglichen Sachen sowie auch Rechte, die zur Begehung oder Vorbereitung einer vorsätzlichen Straftat gebraucht worden oder bestimmt

22 Vgl. *Krause,* NJW 2018, 678 (680).
23 *Wittmer*, S. 147; vgl. *LG München I*, BeckRS 2018, 5795 Rn. 736, 789, 807, 829.
24 *Krause,* NJW 2018, 678 (680).
25 *Schuhr*, in: MüKo-StPO, Bd. 1, 2. Aufl. (2023), § 136a Rn. 61; vgl. *Zöller,* KriPoZ 2019, 274 (276).
26 *Krause,* NJW 2018, 678 (680); vgl. *Greven*, in: KK-StPO, 9. Aufl. (2023), § 94 Rn. 4a.
27 Vgl. *Bauer,* Soziale Netzwerke und strafprozessuale Ermittlungen, in: Hoyer/Schroeder, Strafrechtliche Abhandlungen – Neue Folge, Bd. 281, 2018, S. 157 Fn. 79.
28 *Wittmer*, S. 148.
29 *BVerfG*, NJW 2005, 1917 (1920).
30 Vgl. *Wittmer*, S. 149.
31 Vgl. *Spillecke*, in: KK-StPO, § 111b Rn. 7.

gewesen sind.[32] Das Nutzungsrecht an einem digitalen Account ist auch ein solcher einziehungsfähiger Gegenstand i.S.d. § 74 Abs. 1 StGB.[33] Voraussetzung für die Anordnung nach § 111b Abs. 1 StPO ist zudem, dass ein Anfangsverdacht i.S.d § 152 Abs. 2 StPO vorliegt.[34] Während die Beschlagnahme nach § 94 Abs. 1 StPO nur eine Sicherung für die Zeit bis zum Abschluss eines etwaigen gerichtlichen Verfahrens zulässt, ermöglicht § 111b Abs. 1 StPO eine anschließende dauerhafte Einziehung nach § 74 Abs. 1 StGB.[35] Zwar ist eine Beschlagnahme von digitalen Accounts gem. §§ 94, 98, 111b StPO grundsätzlich möglich, aber ihr konkreter Vollzug ist problematisch: Denn der Vollzug einer Beschlagnahme eines digitalen Accounts erfordert die Abänderung der Zugangsdaten, um so den Account-Inhaber vom weiteren Zugriff sowie der künftigen Nutzung des Accounts auszuschließen, damit nur noch die Ermittlungsbehörden über diesen Account verfügen können.[36] Für die Abänderung der Zugangsdaten benötigen sie aber ebendiese. Mithin stellt sich die Frage, wie die Ermittler die Zugangsdaten erlangen könnten.

b) Erzwungene Herausgabe der Zugangsdaten

Mit Blick auf den Nemo-Tenetur-Grundsatz ist jedenfalls eine erzwungene Herausgabe der Zugangsdaten im Rahmen der Beschlagnahme zu verneinen: Der Nemo-Tenetur-Grundsatz hat Verfassungsrang und ist aus dem Rechtsstaatsprinzip des Art. 20 Abs. 3 GG sowie aus Art. 1 Abs. 1 GG, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG abgeleitet.[37] Er umfasst die Aussagefreiheit des Beschuldigten und das Verbot des Zwangs zur Selbstbelastung.[38] Beschuldigte sowie Zeugen sind danach nicht verpflichtet, aktiv an der Sachaufklärung mitzuwirken, soweit dies zu einer Selbstbelastung führen könnte.[39] Da der Account-Inhaber die Zugangsdaten selbst aktiv nennen müsste und sich auf dem in Rede stehenden Account regelmäßig strafrechtliches sowie ermittlungsrelevantes Material befinden wird, würde eine erzwungene Herausgabe unter Umständen zu einer aktiven Mitwirkung am Straf- bzw. Ermittlungsverfahren des Beschuldigten gegen sich selbst führen bzw. nicht ausschließen.[40] Mithin können die Ermittler die Herausgabe der Zugangsdaten gegen den Willen des Beschuldigten nicht über die Vorschriften zur Beschlagnahme erzwingen.[41]

c) Erlangung durch anderweitige Ermittlungen

Weiter kommt in Betracht, dass über die Zugangsdaten des Accounts – ohne aktive Mitwirkung des Inhabers – durch anderweitige Ermittlungsmaßnahmen Kenntnis erlangt wird, und der Betroffene einen Zugriff gegen seinen Willen zu dulden hat.[42] Die Zugangsdaten könnten z.B. während einer Überwachung mittels der Online-Durchsuchung (§ 100b StPO) mit sog. „Keyloggern“ abgefangen werden.[43] Neuerdings wird ein Zugriff auf die Accounts der Nutzer von Telemediendiensten (elektronische Informations- und Kommunikationsdienste) bei der Verfolgung

32 *Joecks/Meißner*, in: MüKo-StGB, Bd. 2, 4. Aufl. (2020), § 74 Rn. 7.
33 Vgl. *Wittmer*, S. 150.
34 *Spillecke*, in: KK-StPO, § 111b Rn. 9.
35 *Hauschild*, in: MüKo-StPO I, § 94 Rn. 50.
36 *Wittmer*, S. 150 f.
37 *Diemer*, in: KK-StPO, § 136 Rn. 10.
38 *Diemer*, in: KK-StPO, § 136 Rn. 10.
39 *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, 66. Aufl. (2023), Einl. Rn. 29a.
40 Vgl. *Wittmer*, S. 151.
41 So auch *Krause,* NJW 2018, 678 (680); *Wittmer*, S. 151.
42 *Wittmer*, S. 151 f.; vgl. *Kochheim*, S. 759 Rn. 2075 ff.; *Krause,* NJW 2018, 678 (680).
43 *Wittmer*, S. 152.

besonders schwerer Straftaten auch durch die neu eingeführte Zugangsdatenabfrage von Telemediendienstanbietern gem. § 100j Abs. 1 S. 3 StPO möglich sein.[44] Des Weiteren könnten sich die erforderlichen Zugangsdaten auf einem sog. „Passwort-Manager" befinden. Dabei handelt es sich um eine Anwendungssoftware, auf der ein Nutzer die Zugangsdaten sämtlicher digitaler Accounts speichern und verwalten kann.[45] Dieser ist regelmäßig selbst verschlüsselt, etwa durch die Verwendung eines allgemeinen Passwortes (Hauptpasswort) oder neuerdings – insbesondere auf Smartphones – mittels biometrischer Verschlüsselungsmöglichkeiten, wie ein Fingerabdruckscan oder eine Gesichtserkennung.[46] Während auch hier die erzwungene Nennung des Hauptpasswortes, wie unter III. 2. b) erläutert, eine aktive Mitwirkungshandlung des Account-Inhabers erfordert und aufgrund eines Verstoßes des Nemo-Tenetur-Grundsatzes regelmäßig unzulässig sein wird, könnte etwas anderes für eine erzwungene Entschlüsselung des biometrisch gesicherten Zugangs zum „Passwort-Manager" und damit zum Account gelten. Diese Entschlüsselung könnte nämlich durchaus mit dem Nemo-Tenetur-Grundsatz vereinbar sein,[47] auch wenn dabei umstritten ist, auf welche konkrete Rechtsgrundlage eine solche Entschlüsselung biometrisch gesicherter Daten gestützt werden kann.[48] Als Beispiel kann hier eine Entsperrung mittels Fingerabdruck angeführt werden, da diese auch ohne eine aktive Mitwirkungshandlung des Beschuldigten möglich ist, indem etwa der Finger von den Ermittlern auf dem Scanner platziert werden kann und der Beschuldigte das zwangsweise Strecken seines Fingers als Ermittlungsmaßnahme passiv zu dulden hat.[49] Ähnliches könnte auch für die Entsperrung mittels Gesichtserkennung gelten, da hier bspw. das Smartphone vor das Gesicht des Beschuldigten gehalten werden kann.[50] Jedoch ist für eine Gesichtserkennung häufig der Blick mit geöffneten Augen erforderlich, was durchaus als eine aktive Mitwirkungshandlung bewertet werden könnte.[51] Im Ergebnis ist mit Blick auf den Nemo-Tenetur-Grundsatz demnach in Bezug auf den „Passwort-Manager" eine erzwungene Entschlüsselung biometrisch gesicherter Daten nicht von vornherein auszuschließen.[52] Neben diesen digitalen Ermittlungsmaßnahmen können anhand „klassischer" Ermittlungsmethoden in der analogen Welt, wie bspw. Durchsuchungsmaßnahmen (§§ 102 ff. StPO), Dokumente gefunden werden, auf denen der Beschuldigte seine Zugangsdaten notiert hat.[53] Soweit die Zugangsdaten durch rechtmäßige Ermittlungsmethoden erforscht wurden,[54] können diese von den Strafverfolgungsbehörden für den Vollzug der Beschlagnahme des Accounts nach §§ 94, 98, 111b StPO im Wege einer gegenüber dem Beschuldigten offenen Maßnahme genutzt werden.[55] Welche Vorschrift der Beschlagnahme einschlägig ist, wird nach einer – zuvor offen durchgeführten – vorläufigen Sicherstellung und Sichtung gem. §§ 94, 102, 110 Abs. 3 StPO bei Bewertung der im Account aufgefundenen Nutzungs- und Kommunikationsdaten entschieden.[56] Den Account-Inhaber trifft eine passive Duldungspflicht der Beschlagnahme,[57] was ebenfalls die Abänderung der Zugangsdaten durch die Ermittlungsbehörde umfasst.

---

44 *Rückert*, in: MüKo-StPO I, § 100j Rn. 19.

45 BSI, Online-Accounts mit dem Passwortmanager schützen – Passwörter sicher im Browser verwalten, online abrufbar unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Projekt-Accountschutz/browser-passwortmanager.html (zuletzt abgerufen am 11.10.2023).

46 Vgl. BSI (Fn. 45).

47 So auch *Rottmeier/Eckel*, NStZ 2020, 193 (199); *Nadeborn/Irscheid*, StraFo 2019, 274 (275).

48 Zur Diskussion und möglichen Rechtsgrundlagen: *Rottmeier/Eckel*, NStZ 2020, 193 (194 ff.); *Grzesiek/Zühlke*, StV Spezial 2021, 117 (118 ff.).

49 *LG Ravensburg*, BeckRS 2023, 3879 Rn. 8; *Rottmeier/Eckel*, NStZ 2020, 193 (199); *Nadeborn/Irscheid*, StraFo 2019, 274 (275); *Bäumerich*, NJW 2017, 2718 (2721).

50 So *Rottmeier/Eckel*, NStZ 2020, 193 (199).

51 So auch *Dornbach*, Ist es der Polizei erlaubt, mein Handy per Face ID zu entsperren? – Fachbeitrag im Strafrecht, online abrufbar unter: https://www.strafverteidigung-dornbach.de/rechtsbeitraege/ist-es-der-polizei-erlaubt-mein-handy-per-face-id-zu-entsperren/ (zuletzt abgerufen am 4.10.2023).

52 Siehe Fn. 47.

53 *Wittmer*, S. 152.

54 Vgl. *Kochheim*, S. 760 Rn. 2078; für § 100j StPO: *Rückert*, in: MüKo-StPO I, § 100j Rn. 20.

55 Vgl. *Krause,* NJW 2018, 678 (680).

56 *Hauschild*, in: MüKo-StPO I, § 110 Rn. 8 f.; *Greven*, in: KK-StPO, § 94 Rn. 4b.

57 Vgl. *Wittmer*, S. 152.

3. Zwischenfazit

Ein Zugriff auf bereits bestehende Accounts ist den Strafverfolgungsbehörden grundsätzlich dann möglich, wenn der Account-Inhaber die Zugangsdaten freiwillig herausgibt oder über die Beschlagnahme gegen seinen Willen, wenn die Zugangsdaten durch anderweitige rechtmäßige Ermittlungsmaßnahmen erforscht wurden und den Account-Inhaber eine passive Duldungspflicht des Zugriffs auf seinen Account trifft. Eine Verpflichtung zur aktiven Herausgabe der Zugangsdaten besteht für den Account-Inhaber bei Achtung des Nemo-Tenetur-Grundsatzes hingegen nicht.

IV. Eingriff in das Fernmeldegeheimnis durch Übernahme des Accounts

Durch die Übernahme eines digitalen Accounts erhalten die Strafverfolgungsbehörden einerseits Kenntnis über Inhalte von bereits geführten Internetkommunikationen und treten andererseits mit neuen Nutzern in Kontakt. Dabei ist die mit einem an das Internet angeschlossenen informationstechnischen System geführte laufende Fernkommunikation von dem Schutzbereich des Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG erfasst.[58] Art. 10 Abs. 1 GG schützt hierbei das Vertrauen eines an der Fernkommunikation Beteiligten darin, dass der Kommunikationsinhalt nicht von Dritten zur Kenntnis genommen wird.[59] Dabei stellt aber allein die verdeckte Kontaktaufnahme einer staatlichen Stelle zu einem Grundrechtsträger noch keinen Eingriff dar, da gerade „die Enttäuschung des personengebundenen Vertrauens in den Kommunikationspartner“[60] nicht vom Schutzbereich erfasst ist. Der Schutzbereich ist somit dann betroffen, wenn eine staatliche Stelle die Kommunikation von außen überwacht und nicht selbst Kommunikationsadressat ist.[61] Ein Eingriff in diesen Schutzbereich ist daran zu messen, ob die staatliche Stelle sich auf dem dafür technisch vorgesehenen Weg unautorisierten oder autorisierten Zugang zu der Kommunikation verschafft hat.[62] Hat nämlich ein Kommunikationsbeteiligter den Ermittlungsbehörden seinen Zugang in das Kommunikationsverhältnis freiwillig zur Verfügung gestellt, sind diese autorisiert, diesen Zugang zu nutzen, ohne dass ein Eingriff in Art. 10 Abs. 1 GG vorliegt.[63] Demgegenüber stellt es einen Eingriff dar, wenn der Kommunikationsbeteiligte seine Zugangsdaten nicht freiwillig herausgegeben hat und die Beamten – etwa die durch anderweitige Ermittlungen erlangten – Zugangsdaten für einen Zugriff auf die Kommunikation gegen oder ohne den Willen des Kommunikationsbeteiligten nutzen.[64] Insbesondere stellt es keinen Eingriff dar, wenn die Ermittlungsbehörde allgemein zugängliche Inhalte aus offenen Diskussionsforen oder nicht zugangsgesicherten Webseiten erhebt.[65] Liegt ein Eingriff in Art. 10 Abs. 1 GG vor, bedarf dieser einer Rechtfertigung. Zur Rechtfertigung eines Eingriffs auf zugangsgeschützte Kommunikationsinhalte in digitalen Accounts können die Vorschriften der Beschlagnahme herangezogen werden,[66] weshalb auf die Ausführungen hierzu verwiesen wird.

58 *BVerfG*, NJW 2008, 822 (835) Rn. 183 f.
59 *BVerfG*, NJW 2008, 822 (835) Rn. 290.
60 *BVerfG*, NJW 2008, 822 (835) Rn. 290.
61 *BVerfG*, NJW 2008, 822 (835) Rn. 290.
62 *BVerfG*, NJW 2008, 822 (835) Rn. 291.
63 *BVerfG*, NJW 2008, 822 (835) Rn. 291, 293.
64 *BVerfG*, NJW 2008, 822 (835) Rn. 292.
65 *BVerfG*, NJW 2008, 822 (835) Rn. 293.
66 Vgl. *BVerfG*, NJW 2009, 2431.

V. Grundrechtseingriffe durch Nutzung des Accounts für verdeckte Ermittlungen

Die zulässige Beschlagnahme des Accounts eröffnet die Möglichkeit, verdeckte Ermittlungen gegenüber bisherigen und künftigen Kommunikationspartnern einzuleiten. Allein aus der zulässigen Beschlagnahme eines digitalen Accounts ergibt sich jedoch nicht die zulässige Nutzung des Accounts durch die Strafverfolgungsbehörden für verdeckte Ermittlungen, da damit neue Kommunikationsdaten geschaffen werden. Soweit die Übernahme und Weiterführung eines digitalen Accounts nicht unter Art. 10 Abs. 1 GG fällt, ist weiter das allgemeine Persönlichkeitsrecht (APR) aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG[67] zu beachten. Das APR schützt den Einzelnen vor staatlichen Eingriffen in seine personale Entfaltung und umfasst dabei die nicht speziell genannten Freiheitsgarantien, die „diesen in ihrer konstituierenden Bedeutung für die Persönlichkeit des Menschen nicht nachstehen."[68] Im Folgenden ist demnach zu prüfen, in welche Ausprägungen des APR in die Rechte des Account-Inhabers einerseits und kontaktierter Dritter andererseits durch die Ermittlungsmethode eingegriffen wird.

1. Recht auf Selbstdarstellung des Account-Inhabers

Eine Ausprägung der unbenannten Freiheitsgarantien aus dem APR ist der Schutz der Selbstdarstellung gegenüber anderen Personen, wobei es insbesondere das Selbstbestimmungsrecht über die „Darstellung des persönlichen Lebens- und Charakterbildes [schützt]."[69]

a) Eingriff

Indem Ermittler einen übernommenen digitalen Account gegen den Willen des Account-Inhabers weiterführen und für Ermittlungszwecke nutzen, könnte in dieses Recht eingegriffen werden.[70] Mangels „Zwangs- und Eingriffscharakter"[71] liegt eben keine Verletzung des APR vor, wenn der Account-Inhaber in die Nutzung seines Accounts für Ermittlungszwecke mithin in den Grundrechtseingriff wirksam – also freiwillig – einwilligt.[72] Ein Eingriff in das Recht auf Selbstdarstellung kann daraus hergeleitet werden, dass der Account-Inhaber mit der Erstellung eines digitalen Accounts eine virtuelle Identität geschaffen hat, über die er „einem Teil seiner Persönlichkeit Ausdruck verleiht"[73] und mit der er sich nach außen durch einen Nutzernamen von anderen Profilen unterscheidet.[74] Dabei können sämtliche persönliche Beiträge und Äußerungen nur genau diesem Nutzernamen zugeordnet werden.[75] Nutzen Ermittler diesen Account und treten unter dieser virtuellen Identität verdeckt gegenüber anderen Nutzern in Erscheinung, stellt dies einen Eingriff in das Recht auf Selbstdarstellung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG des Account-Inhabers dar.[76] Diese Verknüpfung von virtueller Identität mit einem geschützten Ausdruck der Persönlichkeit ist jedoch bei einem anonymen Account nicht zwingend, weil das Grundrecht die reale Person und nicht eine virtuelle Person als solche umfasst. Bei Erstellung eines anonymen Accounts,

67 *Di Fabio*, in: Dürig/Herzog/Scholz, GG, Bd. 1, 99. EL (Sept. 2022), Art. 2 Abs. 1 Rn. 127.
68 *BVerfG*, NJW 2022, 139 (142) Rn. 113.
69 *Di Fabio*, in: Dürig/Herzog/Scholz, GG, Art. 2 Abs. 1 Rn. 166.
70 *Wittmer*, S. 155.
71 *El-Ghazi,* ZIS 2019, 110 (111).
72 *Di Fabio*, in: Dürig/Herzog/Scholz, GG, Art. 2 Abs. 1 Rn. 228; vgl. *Wittmer*, S. 157.
73 *Meyer*, Identität und virtuelle Identität natürlicher Personen im Internet, in: Borges, Internet und Recht, Bd. 7, 2011, S. 140.
74 Vgl. *Wittmer*, S. 155.
75 Vgl. *Wittmer*, S. 155; *Meyer*, S. 140.
76 So auch *Wittmer*, S. 155 f.

insbesondere im Darknet, will der Account-Inhaber eben nicht mit seiner analogen Identität in Verbindung gebracht werden. Gegen diese hier erarbeitete Differenzierung zwischen einer anonymen virtuellen Identität und der dahinterstehenden realen Person könnte die in der Literatur vorzufindende Ansicht angeführt werden, die sich gegen das Absprechen jeglicher Schutzwürdigkeit einer anonymen Kommunikation wendet, da sich z.B. im Darknet nicht ausschließlich über strafrechtlich relevante Themen, sondern in Diskussionsforen auch etwa über Politik und Wirtschaft ausgetauscht wird.[77] Allerdings bleibt unbegründet, warum eine anonyme virtuelle Identität als solche eigenständig schutzwürdig sein sollte, wenn keinerlei Bezug zu einer realen Person erkennbar ist. Die Kommunikation, die der Anbahnung und Abwicklung von Straftaten dient, wird aber auch bei dieser Ansicht richtigerweise für nicht schutzwürdig erachtet.[78] Festzuhalten ist somit, dass grundsätzlich die Nutzung eines digitalen Accounts in das Recht auf Selbstdarstellung des Account-Inhabers eingreifen kann, soweit es sich nicht lediglich um einen anonymen Account handelt, da dann nicht ersichtlich ist, wie eine anonymisierte virtuelle Identität als Teil des Ausdruckes der Persönlichkeit der dahinterstehenden Person angesehen werden kann.

b) Rechtfertigung

Willigt der Account-Inhaber nicht ein, ist für den Grundrechtseingriff eine rechtfertigende Ermächtigungsgrundlage erforderlich. Da die StPO für diese Ermittlungsmethode bislang keine eigenständige Ermächtigungsgrundlage kennt, bleibt allein der Rückgriff auf die Ermittlungsgeneralklausel aus §§ 161, 163 StPO.[79] Diese ermächtigt die Staatsanwaltschaft zu „Ermittlungen jeder Art“, wobei die konkreten Ermittlungsmaßnahmen nur einen geringfügigen Grundrechtseingriff darstellen und es deshalb keiner Spezialbefugnis bedarf.[80] Aus dem allgemeinen Verhältnismäßigkeitsgrundsatz ergibt sich, dass der Rechtfertigungsbedarf der Ermittlungsmaßnahme steigt, je tiefer durch sie in den engeren persönlichen Bereich des Betroffenen eingegriffen wird.[81] Dabei bleibt beim APR insbesondere der absolut geschützte Kernbereich der Persönlichkeit, der sich durch Art. 1 Abs. 1, 19 Abs. 2 GG bestimmt, unantastbar.[82] Auch hier ist danach zu differenzieren, ob der Account einen unmittelbaren sowie offen erkennbaren Persönlichkeitsbezug aufweist oder ob es sich um einen anonymen Account ohne erkennbaren Bezug zu einer bestimmten analogen Person handelt.[83] Bei einem unmittelbaren Persönlichkeitsbezug soll nach einer Ansicht kein geringfügiger Grundrechtseingriff vorliegen, während bei anonymen Accounts die Ermittlungsgeneralklausel als ausreichend erachtet wird.[84] Demgegenüber begründet eine andere Ansicht für die Übernahme von anonymen Darknet-Accounts dennoch eine hohe Eingriffsintensität mit dem Einwand, dass der Identitätsschutz des APR auch „das soziale Ansehen bzw. das Prestige einer Person“[85] umfasst und gerade im Darknet insbesondere die Accounts übernommen werden, die bereits durch ihre langjährige Aktivität auf den Plattformen und Foren über eine entsprechende „credibility“ in der Szene verfügen.[86] Dies soll also durchaus dazu führen, dass ein Grundrechtseingriff nicht mehr bloß geringfügig wäre und nicht von der Ermittlungsgeneralklausel gerechtfertigt werden

77 Vgl. *Wittmer*, S. 57, 155.
78 *Wittmer*, S. 155; vgl. *Kochheim*, S. 761 Rn. 2081.
79 Vgl. *Wittmer*, S. 156.
80 *Kölbel*, in: MüKo-StPO, Bd. 2, 1. Aufl. (2016), § 161 Rn. 6 f.
81 *Di Fabio*, in: Dürig/Herzog/Scholz, GG, Art. 2 Abs. 1 Rn. 130.
82 *Di Fabio*, in: Dürig/Herzog/Scholz, GG, Art. 2 Abs. 1 Rn. 130.
83 *Grözinger*, in: Müller/Knauer/Schlothauer, § 50 Rn. 246.
84 Vgl. *Grözinger*, in: Müller/Knauer/Schlothauer, § 50 Rn. 246.
85 *Kunig/Kämmerer*, in: Münch/Kunig, GG, Bd. 1, 7. Aufl. (2021), Art. 2 Rn. 70.
86 *Wittmer*, S. 157.

könnte.[87] Die Folge dessen wäre, dass mangels Ermächtigungsgrundlage eine Nutzung des Accounts für Ermittlungszwecke gegen den Willen des Account-Inhabers nicht zulässig wäre.[88] Diese Auffassung stellt jedoch darauf ab, dass selbst eine anonyme virtuelle Identität und nicht die reale Person unmittelbar mit dem Ansehen bzw. Prestige dieser Person verknüpft ist. Für diese Gleichstellung des Ansehens bzw. Prestige einer anonymisierten virtuellen Identität mit jenem einer realen Person werden jedoch weder die sachlichen noch die rechtlichen Grundlagen genannt. Sachlich kann – aufgrund der Anonymisierung – ein Dritter keine Verknüpfung zur dahinterstehenden Person herstellen.[89] Und grundrechtlich vom APR geschützt ist nur eine „lebende natürliche Person“[90], während die anonyme virtuelle Identität, die nicht auf die dahinterstehende Person durchschlägt, als solche nicht eigenständig schutzwürdig ist.

c) Zwischenfazit

Die Übernahme eines bereits bestehenden Accounts für verdeckte Ermittlungen gegen den Willen des Inhabers stellt demnach keinen Eingriff in das Recht auf Selbstdarstellung dar, soweit es sich um eine rein anonyme virtuelle Identität handelt. Ansonsten wird die Ermittlungsmethode regelmäßig nur dann zulässig sein, wenn der Account-Inhaber in die Nutzung seines Accounts einwilligt.

2. Eingriff in das RiS von kontaktierten Personen

Gegenüber einer durch den übernommenen Account kontaktierten Person kommt ein Eingriff in das Recht auf informationelle Selbstbestimmung (RiS) als weiterer Ausfluss des APR in Betracht. Hierbei kann es keinen Unterschied machen, ob der Account gegen den Willen oder freiwillig übernommen wurde, da dies für den Dritten nicht erkennbar ist und zudem eine Einwilligung des Account-Inhabers keine Grundrechtseingriffe gegenüber Dritten rechtfertigen kann.[91]

a) Schutzbereich und Eingriff nach Auffassung des BVerfG

Nach dem RiS darf jeder Grundrechtsträger grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen.[92] Ein Eingriff in das RiS liegt nach Auffassung des *BVerfG* nur dann vor, wenn „eine staatliche Stelle sich unter einer Legende in eine Kommunikationsbeziehung zu einem Grundrechtsträger begibt […und] 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 […].“[93] Dabei ermöglichen Kommunikationsdienste des Internets zwar in weitem Umfang den Aufbau von Kommunikationsbeziehungen, jedoch ist hier das Vertrauen in die Identität und Wahrhaftigkeit der Kommunikationspartner nicht schutzwürdig, wenn dafür keinerlei Überprüfungsmechanismen existieren.[94] Dies gelte selbst dann, wenn bestimmte Personen über einen längeren Zeitraum kommunizieren und sich eine Art „elektronische Gemeinschaft“

87 So *Wittmer*, S. 157.
88 Vgl. *Wittmer*, S. 157; a.A. *Krause,* NJW 2018, 678 (680); *Grözinger*, in: Müller/Knauer/Schlothauer, § 50 Rn. 246.
89 Vgl. *Meyer*, S. 54.
90 *Di Fabio*, in: Dürig/Herzog/Scholz, GG, Art. 2 Abs. 1 Rn. 223.
91 Vgl. *Wittmer*, S. 158.
92 BVerfGE 65, 1 (43).
93 *BVerfG*, NJW 2008, 822 (836) Rn. 310; vgl. *BVerwG*, NJW 1997, 2534.
94 *BVerfG*, NJW 2008, 822 (836) Rn. 311.

bildet.[95] Damit legt das *BVerfG* 2008 in seiner Entscheidung zur Online-Durchsuchung den Schutzbereich des RiS restriktiv aus.[96] Wann genau ein „schutzwürdiges Vertrauen" besteht, bleibt dabei offen, denn Kriterien für eine Bestimmung nennt das *BVerfG* nicht. Aufgabe sei es nun zu untersuchen, wann ein schutzwürdiges Vertrauen nach restriktivem Schutzbereichsverständnis vorliegen könnte.

aa) Eingriff in bestehende Kommunikationsbeziehungen mit realem Bezug

Das *BVerfG* zieht für seine Ausführungen das Beispiel des Diskussionsforums heran.[97] In solchen Gruppen kennen sich die Nutzer meist zunächst nicht, das Vertrauen knüpft also nur an den Avatar des Nutzers an,[98] also an einer anonymen virtuellen Identität. Hier könnte durch länger andauernde Kommunikation ein Vertrauen erzeugt werden, das aber mehr die durch bestimmte Verhaltensweisen entstandenen individuellen Eigenschaften des Avatars betrifft als die Identität des dahinterstehenden Nutzers als solche.[99] Insoweit verkörpern Diskussionsforen wohl treffend eine „elektronische Gemeinschaft" und keine analogen Beziehungen.[100] Nach dem *BVerfG* reicht ein solches auf länger andauernder Kommunikation basierendes Vertrauen noch nicht für die Schutzwürdigkeit aus, woraus sich schließen lässt, dass wohl mehr als eine zeitliche Komponente hinzukommen muss.[101] In Betracht kommen dafür Kommunikationsbeziehungen, die in „Wechselwirkung mit der realen Welt [stehen]"[102], die Nutzer sich also bereits aus der analogen Welt kannten oder eben auf das virtuelle Kennenlernen ein reales Treffen folgte.[103] Videotelefonate oder Ähnliches können ebenfalls die Anonymität durchbrechen und einen realen Bezug begründen.[104] Dies wird wohl häufig in sozialen Netzwerken der Fall sein,[105] aber auch im Darknet ist dies aufgrund der verschiedensten Nutzungsarten nicht auszuschließen.[106] Die Kommunikationsbeziehung bildet hierbei keine „elektronische Gemeinschaft", da das Vertrauen nicht bloße virtuelle, sondern reale Beziehungen umfasst. Das somit geschaffene Vertrauen ist einem allein in der realen Welt geschaffenen Vertrauen gleichzustellen und dürfte demnach vom restriktiven Schutzbereichsverständnis des *BVerfG* gedeckt sein. Bei der verdeckten Identitätsübernahme im Darknet wird ein Eingriff in das RiS dennoch von einigen Stimmen abgelehnt mit dem Einwand des vom *BVerfG* angeführten Kriteriums der fehlenden Überprüfungsmechanismen im Internet.[107] Auf mangelnde Überprüfungsmechanismen im Internet kann es aber bei dem Eindringen in bereits bestehende Kommunikationsverhältnisse, die einen realen Bezug haben, nicht mehr ankommen, da die Vertrauensbeziehung in der Vergangenheit bestand und ebendieser reale Bezug bereits einen Überprüfungsmechanismus darstellt.[108] Bei diesem realen Bezug muss es auf die Erkennbarkeit dessen für die Ermittlungsbehörden ankommen. Ergeben sich im Rahmen der Ermittlungen oder bei Sichtung des Accounts nach § 110 StPO Anhaltspunkte für einen realen Bezug, ist dies von den Ermittlungsbehörden zu beachten. Ein Eindringen in bereits bestehende, ausschließlich inkriminierte Kommunikationsbeziehungen führt hingegen – unabhängig von einem realen Bezug – zu keinem Eingriff in das RiS.[109] Denn die Abrede und Durchführung von Straftaten genießt keinesfalls Grundrechtsschutz,[110] weshalb die

95 *BVerfG*, NJW 2008, 822 (836) Rn. 311.
96 Vgl. *Bauer*, S. 155; *Eifert,* NVwZ 2008, 521 (522).
97 *BVerfG*, NJW 2008, 822 (836) Rn. 311.
98 *Bauer*, S. 156.
99 Vgl. *Rosengarten/Römer,* NJW 2012, 1764 (1767); *Bauer*, S. 156.
100 Vgl. *Bauer*, S. 156.
101 *BVerfG*, NJW 2008, 822 (836) Rn. 311; vgl. *Ihwas,* WiJ 2018, 138 (144 Fn. 46); *Singelnstein,* NStZ 2012, 593 (600).
102 *Bauer*, S. 156.
103 Vgl. *Ihwas,* WiJ 2018, 138 (146).
104 Vgl. *Oehmichen/Weißenberger,* KriPoZ 2019, 174 (181).
105 Vgl. *Bauer*, S. 156.
106 *Ihwas,* WiJ 2018, 138 (143 f.).
107 Vgl. *Krause,* NJW 2018, 678 (680); *Grözinger*, in: Müller/Knauer/Schlothauer, § 50 Rn. 246.
108 Vgl. *Bauer*, S. 158.
109 Vgl. *Wittmer*, S. 163.
110 Vgl. *Kochheim*, S. 761 Rn. 2081.

Kommunikationspartner hierbei nicht schutzwürdig darauf vertrauen können, dass sie nicht mit einer staatlichen Stelle kommunizieren.[111]

bb) Eingriff in Kommunikationsverhältnisse ohne realen Bezug

Ein Eingriff könnte jedoch auch dann vorliegen, wenn kein realer Bezug vorliegt, aber eine Überprüfung des Vertrauensverhältnisses auf andere Weise gegeben ist, was im Einzelfall zu beurteilen ist.[112] Dies kann sowohl bei bereits bestehenden Kommunikationsverhältnissen als auch beim Initiieren neuer Kommunikationsbeziehungen der Fall sein. Hierbei bietet sich ein Vergleich der unterschiedlichen Überprüfungsmechanismen von sozialen Netzwerken und Darknet an.

(1) Überprüfungsmechanismen bei sozialen Netzwerken

In Betracht kommen Überprüfungsmechanismen, bei denen einerseits die Kontrolle durch den Betreiber und andererseits die Kontrolle durch die Nutzer getätigt werden.[113] Eine Ansicht lehnt ein schutzwürdiges Vertrauen ab, solange die Betreiber sozialer Netzwerke die Nutzung von Nicknames statt Klarnamen zulasse, obwohl sie in ihren AGB auf eine Klarnamenpflicht bestehen, aber keine eigene Überprüfung dessen vornehmen.[114] Denn bei Verwendung von Nicknames haben diese Nutzer eben kein Interesse an der Verknüpfung des Accounts mit ihrer echten Identität, weshalb das Vertrauen in die virtuelle Identität nicht schutzwürdig sein soll.[115] Demgegenüber kommt es nach einer anderen Ansicht nicht auf die Kontrolle durch die Betreiber an, denn einerseits verzichten die Betreiber auf die strenge Durchsetzung der Klarnamenpflicht, um ein schnelles, müheloses Vernetzen zu gewährleisten und andererseits wäre ihnen dies gar nicht möglich, denn Telemedien müssen nach § 19 Abs. 2 TTDSG eine Nutzung unter einem Pseudonym ermöglichen.[116] Wieder andere stellen auf die Kontrolle durch den Nutzer ab und verneinen ein schutzwürdiges Vertrauen, wenn dieser jegliche Freundschaftsanfragen ohne Überprüfung annimmt.[117] Hier könnte z.B. die Ausgestaltung eines Nutzerprofils aufgrund bestimmter Merkmale auf „Echtheit" geprüft werden,[118] wobei sich diese Merkmale i.d.R. schwer kategorisieren lassen und regelmäßig wenig über die tatsächliche Echtheit aussagen werden.[119] Eine Kontrolle durch den Nutzer könnte auch aufgrund „personenbezogenen Zusatzwissens" durchgeführt werden, wenn etwa Nutzer wissen, wer sich hinter bestimmter Pseudonyme verbirgt,[120] jedoch sind diese inneren Umstände für eine Beurteilung eines schutzwürdigen Vertrauens nach außen hin weder feststellbar noch objektivierbar.[121] Letztlich wird es eine Einzelfallentscheidung bleiben, ob aufgrund genannter Überprüfungsmechanismen ein schutzwürdiges Vertrauen in sozialen Netzwerken angenommen werden kann.

(2) Überprüfungsmechanismen im Darknet

Im Darknet kommt es den Nutzern, anders als in sozialen Netzwerken, insbesondere darauf an, völlig anonym zu

111 *Wittmer*, S. 163.
112 *BVerfG*, NJW 2008, 822 (836) Rn. 311; vgl. *Ihwas,* WiJ 2018, 138 (144).
113 Vgl. *Bauer*, S. 160.
114 *Henrichs,* Kriminalistik 2012, 632 (633 f.).
115 *Henrichs,* Kriminalistik 2012, 632 (634).
116 Vgl. *Bauer*, S. 160 f.
117 *Ihwas*, Strafverfolgung in Sozialen Netzwerken: Facebook & Co. als moderne Ermittlungswerkzeuge, in: Zöller, Deutsches und Europäisches Strafprozessrecht und Polizeirecht, Bd. 1, 1. Aufl. (2014), S. 151.
118 Vgl. *Ihwas*, S. 152 ff.
119 *Bauer*, S. 163.
120 Vgl. *Soiné,* NStZ 2014, 248 (249).
121 *Bauer*, S. 163 f.

bleiben.[122] Eine Kontrolle der echten Identität durch den Betreiber soll gerade nicht vorgenommen werden. Auch eine Kontrolle äußerer Umstände wie eine Überprüfung von Nutzerprofilen auf ihre Echtheit wird an der Anonymisierung und der Nichtpreisgabe von Angaben der echten Identität regelmäßig scheitern. Ein Abstellen auf „personenbezogenes Zusatzwissen“[123] ist zwar dahingehend denkbar, wenn etwa ein Account „credibility“ besitzt und die Zielperson bislang keinen Kontakt zu diesem Account hatte, aber ihn etwa aus der Szene kennt und somit ein Vertrauen in den „Ruf“ des Accounts entstehen könnte. Jedoch sind solche inneren Umstände nach außen nicht erkennbar. Ermittler können nicht wissen, ob die Zielperson dieses Zusatzwissen hat oder nicht.[124] Zudem stellt das *BVerfG* in seiner Entscheidung bei der Bestimmung des schutzwürdigen Vertrauens maßgeblich auf die anonyme Kommunikation ab.[125] Im Darknet ist demzufolge ein schutzwürdiges Vertrauen in die Identität und Wahrhaftigkeit bei anonymen Kommunikationspartnern, bei denen kein realer Bezug besteht, grundsätzlich nicht anzunehmen.[126]

b) Weites Schutzbereichsverständnis in der Literatur

Es gibt Stimmen in der Literatur, die immer eine verfassungsrechtliche Rechtfertigung verlangen, wenn staatliche Stellen verdeckt an Kommunikationen im Internet teilnehmen.[127] Danach steht die „täuschungsbedingte Preisgabe von persönlichen Daten […] im direkten Widerspruch zum [RiS]“[128], da bei verdeckten Ermittlungsmethoden der Grundrechtsträger aufgrund der Täuschung eben nicht mehr erkennen und kontrollieren kann, wer seine Daten empfängt, weshalb dies grundsätzlich immer das RiS berührt.[129] Bemängelt wird an der restriktiven Auslegung des *BVerfG*, dass lediglich an die faktische Möglichkeit der Identitätstäuschung im Internet anknüpft wird, wobei es einen erheblichen Unterschied ausmacht, ob die Täuschung von privaten Personen oder staatlichen Stellen vorgenommen wird, da bei staatlichem Handeln „die Erwartung der Bürger wegen der Kompetenzgebundenheit des Staates ja gerade durch die Rechtslage geprägt“[130] ist. Wann ein schutzwürdiges Vertrauen angenommen wird und den Ermittlern eine Täuschung erlaubt wird, ist nicht anhand von „(Überprüfungs-)Möglichkeiten“ zu messen, sondern ist „stark normgeprägt.“[131] Anders als vom *BVerfG* bewertet, soll nach dieser Auffassung der Nutzer aufgrund der erleichterten Täuschungsmöglichkeit im Internet erst recht grundrechtlich zu schützen sein.[132] Diese Auffassung verkennt, dass die erleichterten Täuschungsmöglichkeiten im Internet aus den fehlenden Überprüfungsmechanismen hervorgehen, die die restriktive Auslegung des *BVerfG* gerade begründet. Eine Kommunikation mit einem anonymisierten Account, bei der die dahinterstehende reale Identität nicht vom Kommunikationspartner überprüft werden kann, lässt Täuschungen eben nicht ausschließen.

122 Vgl. *Ihwas,* WiJ 2018, 138 (143 f.); *Sinn*, Ermittlungen im Darknet, in: Gesk/Sinn, Schriften des Zentrums für Europäische und Internationale Strafrechtsstudien 10, Organisierte Kriminalität und Terrorismus im Rechtsvergleich, Deutsch-Chinesischer Rechtsdialog, Bd. 1, 2019, S. 145 (152 f.).
123 *Soiné,* NStZ 2014, 248 (249).
124 Vgl. *Bauer*, S. 164.
125 *BVerfG*, NJW 2008, 822 (836) Rn. 311; vgl. *Ihwas,* WiJ 2018, 138 (143 f.).
126 So auch *Krause,* NJW 2018, 678 (680) der aber nicht zum realen Bezug abgrenzt.
127 Vgl. *Eifert,* NVwZ 2008, 521 (522); *Singelnstein,* NStZ 2012, 593 (600) *Bauer*, S. 164.
128 *Bauer*, S. 165.
129 Vgl. *Bauer*, S. 164 f.; *Eifert,* NVwZ 2008, 521 (522).
130 *Eifert,* NVwZ 2008, 521 (522).
131 *Eifert,* NVwZ 2008, 521 (522).
132 *Bauer*, S. 166.

c) Beweisverwertungsgrenzen der kriminalistischen List

Bei der staatlichen verdeckten Kommunikation mit einem Grundrechtsträger sind eine Vielzahl anderer strafprozessrechtlicher Rahmenbedingungen zu beachten, um später Beschuldigten ein faires Verfahren garantieren zu können. Auf die hier am relevantesten erachteten Rahmenbedingungen ist einzugehen: Tritt ein verdeckter Ermittler mit einem Verdächtigen in Kontakt und versucht ihn etwa mittels eines Scheinkaufes zu überführen, muss er mit Blick auf die Mindestgarantie des fairen Verfahrens aus Art. 2 Abs. 1 i.V.m. Art. 20 Abs. 3 GG und Art. 6 Abs. 1 EMRK die Grenzen der rechtsstaatswidrigen Tatprovokation beachten.[133] Diese liegt vor, wenn der verdeckte Ermittler „auf das Wecken der Tatbereitschaft oder eine Intensivierung der Tatplanung mit einiger Erheblichkeit stimulierend auf den Täter einwirkt."[134] Außerdem muss bei der Datenverarbeitung stets darauf geachtet werden, dass der Schutz des absoluten Kernbereichs der privaten Lebensgestaltung gewahrt ist und Daten, die diesem angehören, zu löschen sind.[135] Insbesondere aber ist eine täuschungsbedingte Selbstbelastung, die gegen den Nemo-Tenetur-Grundsatz verstößt, unzulässig und kann zu einem Beweisverwertungsverbot führen.[136] Ein Verstoß liegt etwa vor, wenn der Zielperson unter Ausnutzung eines Vertrauensverhältnisses durch beharrliches Drängen zur Aussage oder vernehmungsähnlicher Befragung selbstbelastende Informationen zu begangenen Straftaten entlockt werden sollen.[137] Demgegenüber ist die Erhebung von Informationen zulässig, die der Beschuldigte aufgrund des geschaffenen Vertrauensverhältnisses freiwillig und von sich aus offenbart hat, da hier nichts anderes gilt, als wenn der Beschuldigte gegenüber einer Vertrauensperson, wie bspw. Einem Freund, eine belastende Aussage tätigt und irrig annimmt, dass dieser die Informationen nicht an die Strafverfolgungsbehörden weitergibt.[138] Vereinbar mit dem Nemo-Tenetur-Grundsatz ist folglich die Kontaktaufnahme zu Beschuldigten zum Zwecke der Erhebung von Informationen, wie etwa Beruf, Alter, Wohnort oder Freizeitaktivitäten, die eine Identifizierung oder das Herauslocken gesuchter Tatverdächtiger aus der anonymen virtuellen Welt in die analoge Welt ermöglichen.[139] Dabei ist es auch zulässig, im Rahmen eines Scheinkaufes durch fingierte Verhandlungsgespräche den Beschuldigten dazu zu bewegen, auf nicht-anonymen Plattformen weiter zu kommunizieren oder ihn von einem Treffen in der realen Welt zu überzeugen.[140]

d) Mögliche Ermächtigungsgrundlagen als Rechtfertigung

Soweit ein Eingriff in das RiS des Kommunikationspartners angenommen wird, gilt es sich seiner Rechtfertigung zuzuwenden. Wenn staatliche Ermittler verdeckt handeln, kommt die spezielle Ermächtigungsgrundlage des verdeckten Ermittlers (VE) nach den §§ 110a ff. StPO und die sich aus der Ermittlungsgeneralklausel ergebende Regelung des nicht offen ermittelnden Polizeibeamten (NoeP) in Betracht.[141] Ein NoeP ist ein Beamter, der nicht dauerhaft unter einer Legende ermittelt, sondern nur gelegentlich – ohne vorherige Schaffung einer Legende – und hierbei seine Funktion nicht offenlegt.[142] Demgegenüber ist ein VE nach § 110a Abs. 2 StPO ein Beamter des Polizeidienstes, der unter einer ihm verliehenen, auf Dauer angelegten, veränderten Identität (Legende) ermittelt,

[133] *EGMR*, NJW 2015, 3631; vgl. *LG München I*, BeckRS 2018, 5795 Rn. 711 ff.
[134] *BGH*, NStZ 2018, 355 (356 f.).
[135] BT-Drs. 19/116, S. 3.
[136] *BGH*, NJW 2007, 3138.
[137] *BGH*, NJW 2007, 3138.
[138] *BGH*, NJW 2007, 3138 Rn. 14.
[139] Vgl. *Wittmer*, S. 159 f.
[140] Vgl. *Wittmer*, S. 160.
[141] *Rosengarten/Römer,* NJW 2012, 1764 (1765); BT-Drs. 19/116, S. 2, 4.
[142] BVerfGE 129, 208 (257); *Henrichs/Weingast*, in: KK-StPO, § 110a Rn. 6.

unter dieser auch am Rechtsverkehr teilnehmen darf und zum Aufbau oder Aufrechterhaltung der Legende nach § 110a Abs. 3 StPO auch entsprechende Urkunden herstellen, verändern und gebrauchen darf. Die Abgrenzung beider Vorschriften ist strittig und ist nach Auffassung des *BGH* anhand einer Gesamtwürdigung aller Umstände vorzunehmen,[143] wobei sich zunächst der grundsätzlichen Anwendbarkeit der Spezialermächtigungsklausel des § 110a StPO gewidmet werden muss.

aa) Anwendbarkeit der §§ 110a ff. StPO

Ob die §§ 110a ff. StPO bei der verdeckten Identitätsübernahme anwendbar sind, ist umstritten. Wird ein schutzwürdiges Vertrauensverhältnis bei bestehenden Kommunikationsverhältnissen ausgenutzt, werden die §§ 110a ff. StPO regelmäßig für nicht anwendbar erklärt,[144] da eine systematische Auslegung dagegen spricht: Dem VE ist es gem. § 100c StPO gestattet, die Wohnung einer Zielperson zu betreten, soweit diese ihr Einverständnis erteilt hat und dieses Einverständnis nicht über ein die Nutzung der Legende hinausgehendes Vortäuschen eines Zutrittsrechts herbeigeführt wurde. Letzteres ist etwa der Fall, wenn der VE sich als Angehöriger der Hausverwaltung ausgibt und vortäuscht, er müsse als solcher die Wohnung betreten.[145] Könnte ein VE in der realen Welt nun vortäuschen, er wäre eine Person aus dem Bekanntenkreis des Betroffenen, um so ein Einverständnis zu erschleichen, „müsste die gesetzgeberische Wertung des § 110c S. 2 StPO erst recht gelten, da der Betroffene davon ausging, einer Person aus seinem persönlichen Nähefeld Zutritt zu gewähren."[146] Hierbei wird nämlich über die Nutzung der falschen Identität hinaus zusätzlich eine Vertrauensbeziehung vorgetäuscht und ausgenutzt.[147] Insbesondere dort, wo zwei Nutzer bereits digital und real vernetzt sind und die Zielperson etwa durch Annehmen einer „Freundschaftsanfrage" ihr Einverständnis gar nicht mehr erteilen kann, da die „Freundschaft" bereits besteht, dürfte sich der Konflikt mit § 110c S. 2 StPO verstärken.[148] Nach der systematischen Auslegung lässt sich die Ermittlungshandlung nicht auf die §§ 110a ff. StPO stützen, wenn Ermittler einen übernommenen Account nutzen, um Dritte darüber zu täuschen, eine bekannte Person aus deren Umfeld zu sein. [149] Aufgrund der hohen Intensität eines Eingriffs in eine bereits bestehende Vertrauensbeziehung wird daher teilweise im Schrifttum eine strengere Ermächtigungsgrundlage als § 110a StPO gefordert.[150] Besteht hingegen kein realer Bezug, kann ein über die Nutzung der Legende hinausgehendes bestehendes Vertrauensverhältnis nicht ausgenutzt werden. Deshalb nehmen Stimmen im Schrifttum an, dass sich bei nicht bestehenden Vertrauensbeziehungen – etwa bei Initiieren neuer Kommunikationsbeziehungen – die Zulässigkeit einer Kommunikation nach den Bestimmungen beurteilen lässt, die für eine Nutzung von durch die Strafverfolgungsbehörden eigenständig erstellten „Fake-Accounts" gelten.[151] Bei der Zulässigkeit von verdeckten Ermittlungen mittels „Fake-Accounts" stellt sich die grundsätzliche Frage, ob die Vorschriften des VE auch für einen virtuell agierenden Ermittler gelten, wobei hier im Schrifttum Uneinigkeit besteht.[152] Die Streitfrage könnte hier jedoch dahinstehen, denn selbst wenn man eine Anwendbarkeit der §§ 110a ff. StPO für virtuell verdeckte Ermittler annimmt, müsste erst recht die grundsätzliche Voraussetzung des § 110a StPO gelten, dass eine neue Legende aufgebaut und genutzt wird. Legt man nämlich § 110a Abs. 2 und Abs. 3 StPO nach dem Wortlaut aus, betrifft die Norm den Aufbau einer Legende mit fiktiven Angaben und nicht

143 *BGH*, NStZ 1995, 516.
144 Vgl. *Sinn*, in: Gesk/Sinn, S. 156; *Wittmer*, S. 164 f.; *Bauer*, S. 195 f.; *Sieber/Brodowski* in: Hoeren/Holznagel/Sieber, Handbuch Multimedia-Recht Rechtsfragen des elektronischen Geschäftsverkehrs, 58. EL (2022), Teil 19.3 Rn. 47.
145 *Henrichs/Weingast*, in: KK-StPO, § 110c Rn. 2.
146 *Bauer*, S. 196.
147 Vgl. *Bauer*, S. 196.
148 *Bauer*, S. 196.
149 So auch *Wittmer*, S. 164 f.; *Bauer*, S. 195 f.
150 *Sieber*, C 126.
151 *Wittmer*, S. 162.
152 Vgl. *Rosengarten/Römer,* NJW 2012, 1764 (1766).

die Übernahme einer fremden, bestehenden realen privaten Identität.[153] Die Vorschriften, die für die Nutzung selbst erstellter „Fake-Accounts" gelten, sind nicht ohne weiteres auf die verdeckte Identitätsübernahme übertragbar.[154] Die Vorschriften des VE sind somit nicht als rechtfertigende Ermächtigungsgrundlage für die verdeckte Identitätsübernahme anwendbar.[155]

bb) Rückgriff auf die Ermittlungsgeneralklausel (NoeP)

Soweit keine spezielle Ermächtigungsgrundlage greift, ist der Rückgriff auf die Ermittlungsgeneralklausel eröffnet. Mithin bleibt zu beurteilen, ob ein lediglich geringfügiger Grundrechtseingriff vorliegt. Die Frage um das schutzwürdige Vertrauen tritt auch hier auf,[156] weshalb auf Abschnitt V. 2. a) und b) zu verweisen ist. Der *BGH* hatte im Jahr 2010 über eine verdeckte Identitätsübernahme zu entscheiden, bei der die Ermittlungsbehörde von dem E-Mail-Account eines Beschuldigten eine E-Mail eines Dritten beantworten und nach Reaktion hierauf mit dem Dritten weiter per E-Mail kommunizieren wollte, wobei die Ermittlungsdauer auf drei Monate angesetzt werden sollte. Nach Auffassung des *BGH* handelte der Ermittler als NoeP, folglich wurde der Einsatz auf die Ermächtigungsgeneralklausel gestützt, womit die Annahme eines bloß geringfügigen Eingriffs in das RiS einhergeht.[157] Jedoch findet sich im Beschluss weder eine nähere Auseinandersetzung mit dem Urteil des *BVerfG* zur Online-Durchsuchung und der damit verbundenen Diskussion um ein schutzwürdiges Vertrauen, noch geht aus dem Beschluss hervor, ob das Kommunikationsverhältnis einen realen Bezug hat, weshalb ein Heranziehen dieser Entscheidung zur Bewertung der Eingriffsintensität einer verdeckten Identitätsübernahme fraglich erscheint. Ein Eingriff in bereits bestehende Kommunikationsverhältnisse, bei denen ein schutzwürdiges Vertrauen der Zielperson vorliegt, könnte dabei mehr als ein bloß geringfügiger Grundrechtseingriff sein, wenn ein realer Bezug zwischen den Kommunikationspartnern bestand. Dies ist nach dem restriktiven Schutzbereichsverständnis des *BVerfG* der Fall, denn beim Ausnutzen eines schutzwürdigen Vertrauens verlangt es eine spezielle Ermächtigungsgrundlage.[158] Liegt hingegen kein realer Bezug vor, kommt die Annahme eines geringfügigen Grundrechtseingriffs durchaus in Betracht. Wird nämlich ein schutzwürdiges Vertrauen mangels Überprüfungsmechanismen abgelehnt, so sieht das *BVerfG* richtigerweise keinen Eingriff in das RiS, mithin es keiner speziellen Ermächtigungsgrundlage bedarf und die Ermittlungshandlung im Rahmen des Einsatzes eines NoeP für zulässig erachtet werden kann.[159] Führen jedoch im Einzelfall bestehende Überprüfungsmechanismen dennoch zur Annahme eines schutzwürdigen Vertrauens, bedarf es einer Ermächtigungsgrundlage und die Ermächtigungsgeneralklausel könnte hierfür nicht mehr ausreichen.[160]

e) Zwischenfazit

Die Nutzung eines übernommenen Accounts für verdeckte Ermittlungen durch die Strafverfolgungsbehörden kann bei bestehendem realen Bezug zwischen den Kommunikationspartnern bzw. aufgrund anderer Überprüfungsmechanismen, die ein Vertrauensverhältnis begründen, durchaus mehr als geringfügig in das APR der Betroffenen

153 vgl. *Zöller,* GA 2000, 563 (571 f.); Böckenförde, Die Ermittlung im Netz. Möglichkeiten und Grenzen neuer Erscheinungsformen strafprozessualer Ermittlungstätigkeit, 1. Aufl. (2003), S. 234; *Jofer*, Strafverfolgung im Internet. Phänomenologie und Bekämpfung krimineller Verhaltens in internationalen Computernetzen, in: Europäische Hochschulschriften: Reihe 2, Rechtswissenschaft, Bd. 2555 (1999), S. 200; *Bauer*, S. 195; wohl a.A. *Jäger/Wolter*, in: SK-StPO, Bd. 2, 6. Aufl. (2023), § 110a Rn. 14.
154 So aber *Wittmer*, S. 162.
155 So auch *Bauer*, S. 195; a.A. *Wittmer*, S. 162.
156 Vgl. *Bauer*, S. 199.
157 *BGH*, BeckRS 2010, 143592.
158 *BVerfG*, NJW 2008, 822 (836) Rn. 310.
159 *BVerfG*, NJW 2008, 822 (836) Rn. 311; So auch *Krause,* NJW 2018, 678 (680).
160 *BVerfG*, NJW 2008, 822 (836) Rn. 310.

eingreifen. Ist dies der Fall, fehlt es an einer dem Grundrechtseingriff rechtfertigenden Ermächtigungsgrundlage. Bei ausschließlich anonymisiert geführten Kommunikationsverhältnissen ist dies nicht anzunehmen.

VI. Kritische Würdigung des § 163g StPO-E

Im März 2019 wurde im ersten Referentenentwurf (RefE) des IT-Sicherheitsgesetzes 2.0 (IT-SiG 2.0) in der Fassung vom 27.3.2019 erstmals die Schaffung einer eigenständigen Ermächtigungsgrundlage in der StPO für die Übernahme von digitalen Identitäten angeregt.[161] Der RefE stieß auf heftige Kritik im Schrifttum.[162] Die Ermächtigungsgrundlage fand sich im neu einzufügenden § 163g StPO-E[163] und sollte Ermittlungsbehörden dazu ermächtigen, auf Nutzerkonten von Tatverdächtigen auch gegen deren Willen zuzugreifen, wobei sie anschließend unter dieser virtuellen Identität auch mit Dritten in Kontakt hätten treten dürfen. Des Weiteren sah die Entwurfsregelung eine Verpflichtung des Account-Inhabers zur Herausgabe der erforderlichen Zugangsdaten und eine Sanktionierung mit Ordnungsgeld oder Beugehaft bei Weigerung vor. Um den Account-Inhaber vor einer erzwungenen Selbstbelastung zu schützen, sollte ein Verwendungsverbot der durch die Nutzung der Zugangsdaten gewonnenen Erkenntnisse bei einem Verfahren gegen ihn gelten. Die Regelung steht in „diametralem Gegensatz“[164] zum Nemo-Tenetur-Grundsatz. Wie bereits dargelegt, stellt die Verpflichtung zur aktiven Herausgabe der Zugangsdaten eine Verletzung des Nemo-Tenetur-Grundsatzes dar.[165] Auch der Versuch, den Kontoinhaber vor einer erzwungenen Selbstbelastung mit einem Verwendungsverbot zu schützen, führt nicht zu demselben Schutz wie die Möglichkeit, eine Herausgabe der Zugangsdaten schlichtweg zu verweigern, wenn etwa Zufallsfunde – was bei dem RefE unklar bleibt – verwertet werden können.[166] Neben weiteren fehlenden verfassungsrechtlich gebotenen Einschränkungen wie ein Richtervorbehalt oder ein Kernbereichsschutz[167] ist aber vor allem die anschließende Nutzung des übernommenen Accounts unzureichend geregelt. Laut Gesetzesbegründung ist eine ausdrückliche Ermächtigungsgrundlage für die Nutzung nicht erforderlich, da diese gegenüber kontaktierten Dritten keinen Eingriffscharakter haben soll, insbesondere weder in Art. 10 Abs. 1 GG noch in das RiS aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG eingreife.[168] Mit der Rechtsprechung des *BVerfG* argumentierend verkennt die Gesetzesbegründung, dass das *BVerfG* in seiner Entscheidung einen Eingriff in Art. 10 Abs. 1 GG nur bei *freiwilliger* Einwilligung in diesen durch einen Kommunikationsbeteiligten ausschließt.[169] Wo sich diese Freiwilligkeit bei einer erzwungenen Herausgabe finden lässt, ist nicht ersichtlich.[170] Wie sich gezeigt hat, kann man auch einen Eingriff in das RiS nicht undifferenziert mit dem Argument des aufgrund mangelnder Überprüfungsmechanismen nicht schutzwürdigen Vertrauens in anonymen Kommunikationen ablehnen, denn unabhängig von der Anonymisierung kann schutzwürdiges Vertrauen bestehen, wenn das Kommunikationsverhältnis Bspw. einen realen Bezug hat. Hier wird aber auch nur in der Gesetzesbegründung von einer anonymen Internetkommunikation gesprochen und eine Zweckbegrenzung im Entwurfswortlaut lässt sich nicht finden.[171] Zu Recht wird die Notwendigkeit gesehen in der

[161] 1. Referentenentwurf des IT-Sicherheitsgesetz 2.0 in der Fassung vom 27.3.2019 unveröffentlicht abrufbar unter: http://intrapol.org/wp-content/uploads/2019/04/IT-Sicherheitsgesetz-2.0-_-IT-SiG-2.0.pdf (zuletzt abgerufen am 28.3.2023), S. 32, 86 ff.
[162] Vgl. *Oehmichen/Weißenberger,* KriPoZ 2019, 174 (179 ff.); *Greier/Hartmann,* jurisPR-StrafR 13/2019 Anm. 1 B. 4; *Laudon,* StRR 2019, 10 f.; *Stadler*, Das geplante IT-Sicherheitsgesetz 2.0, Internet-Law Onlinerecht und Bürgerrechte 2.0 (7.4.2019), online abrufbar unter: https://www.internet-law.de/2019/04/das-geplante-it-sicherheitsgesetz-2-0.html (zuletzt abgerufen am 29.3.2023).
[163] Zum Nachfolgenden vgl. 1. RefE (Fn. 161), S. 32 f.
[164] *Oehmichen/Weißenberger,* KriPoZ 2019, 174 (180).
[165] So auch: *Oehmichen/Weißenberger,* KriPoZ 2019, 174 (180); *Greier/Hartmann,* jurisPR-StrafR 13/2019 Anm. 1 B. 4; *Laudon,* StRR 2019, 10 f.; *Wittmer*, S. 166.
[166] *Stadler* (Fn. 162).
[167] Vgl. *Oehmichen/Weißenberger,* KriPoZ 2019, 174 (180).
[168] 1. RefE (Fn. 161), S. 87.
[169] *BVerfG*, NJW 2008, 822 (835) Rn. 293.
[170] Vgl. *Oehmichen/Weißenberger,* KriPoZ 2019, 174 (181).
[171] Vgl. *Oehmichen/Weißenberger,* KriPoZ 2019, 174 (180).

StPO eine spezialgesetzliche Vorschrift für die verdeckte Identitätsübernahme zu schaffen, da diese nach geltendem Recht unzureichend geregelt ist.[172] Der RefE verpasst jedoch die Chance, eine erforderliche Regelung insbesondere für die Nutzung einer übernommenen virtuellen Identität für verdeckte Ermittlungen zu entwickeln. Alles in allem wies der § 163g StPO-E „ganz erhebliche handwerkliche Mängel"[173] auf und war „verfassungsrechtlich höchst problematisch."[174] Weshalb diese Vorschrift aber bereits im zweiten Entwurf des IT-SiG 2.0 ersatzlos gestrichen wurde[175] und nicht weiter versucht wurde, eine geeignete verfassungskonforme Regelung zu erarbeiten, ist nicht ersichtlich. Denn Handlungsbedarf bezüglich der Ausgestaltung spezialgesetzlicher Vorschriften für verdeckte Ermittlungen im Internet besteht weiterhin.[176]

VII. Fazit

Die Übernahme digitaler Identitäten ist eine erfolgversprechende Ermittlungsmethode für die Strafverfolgungsbehörden, wenn es um Ermittlungen im Internet, insbesondere im Darknet, geht. Dennoch kennt das geltende Recht der StPO hierfür keine ausdrückliche Ermächtigungsgrundlage. Das führt einerseits zu großer Uneinigkeit im Schrifttum bei der Bewertung der Schutzwürdigkeit einer virtuellen Identität in den verschiedensten Netzwerken (Darknet, soziale Netzwerke etc.) und andererseits zu einer erheblichen Unsicherheit und Verunsicherung auf Ebene der Strafverfolgungsbehörden. Bei der hier herausgearbeiteten, differenzierten Betrachtung finden sich die Grenzen der Zulässigkeit der verdeckten Identitätsübernahme regelmäßig dort, wo die betroffene virtuelle Identität einen nach außen erkennbaren Bezug zur Persönlichkeit der dahinterstehenden Person zulässt oder andere Überprüfungsmechanismen bestehen, die ein schutzwürdiges Vertrauensverhältnis schaffen können. Die komplexe Bewertung der Zulässigkeit stellt die Strafverfolgungsbehörden regelmäßig vor die Aufgabe, mangels unzureichend geregelter Standardmaßnahmen selbst beurteilen zu müssen, wie bestehende – teilweise für analoge Ermittlungsmethoden gedachte – Ermächtigungsgrundlagen auf Ermittlungen in der virtuellen Welt mit Achtung der Grundrechte der Betroffenen anwendbar sind. Die Eingriffsbefugnisse der StPO hinken der technischen Entwicklung hinterher, wobei es Aufgabe des Staates ist, solche zu entwickeln und dabei den staatlichen Strafanspruch und die den Einzelnen schützenden Grundrechte ins Gleichgewicht zu bringen.

172 1. RefE (Fn. 161), S. 86 f.
173 *Gercke,* ZUM 2020, 948 (954).
174 *Stadler* (Fn. 162).
175 Vgl. 2. Referentenentwurf des IT-Sicherheitsgesetz 2.0 in der Fassung vom 7.5.2020 unveröffentlicht abrufbar unter: https://ag.kritis.info/wp-content/uploads/2020/12/20200507-IT-Sicherheitsgesetz-2.0.pdf (zuletzt abgerufen am 12.4.2023).
176 Vgl. *Zöller,* KriPoZ 2019, 274 (281); *Bauer*, S. 212 der einen Gesetzgebungsvorschlag formuliert.