Digitaloffensive im Strafrecht! Verbesserte Bekämpfung von Cyberkriminalität durch das IT-Sicherheitsgesetz 2.0?

*von Dr. Anna Oehmichen und Björn Weißenberger**

Abstract
Der Beitrag beschäftigt sich mit den Änderungen, die der Referentenentwurf des IT-Sicherheitsgesetzes 2.0 in den Bereichen des materiellen und prozessualen Strafrechts vorsieht. Besonders eingegangen wird dabei auf das Zugänglichmachen von Leistungen zur Begehung von Straftaten (§ 126a StGB-E; sog. Darknet-Paragraph) und die zwangsweise durchsetzbare Nutzung von Benutzerkonten durch Polizeibeamte (§ 163g StPO-E). Im Ergebnis werden die Vorschläge abgelehnt.

I. Einführung

Cyber- und Informationssicherheit gehören zu den Themen, die in Nachrichten und Politik regelmäßig auf der Tagesordnung stehen.[1] Im gleichen Atemzug wird häufig auch das Phänomen der Internetkriminalität („Cybercrime“) genannt, wenngleich es sich hierbei eigentlich um ein anderes Themengebiet handelt. Dieses erlangt in der Tagespresse regelmäßig dann besondere Beachtung, wenn im Bereich des sog. Darknet[2] operiert wird,[3] wie beispielsweise beim Verkauf der Tatwaffe, die zur Begehung der Münchener Attentate am Olympia Einkaufszentrum am 22.7.2016 gebraucht wurde,[4] und/oder wenn kinderpornographische Netzwerke ausgehoben werden.[5] Das Bundesministerium des Innern, für Bau und Heimat (BMI) sieht hier Regelungsbedarf und hat deshalb 2018 das (inoffizielle) Gesetzgebungsverfahren zu einem sog. IT-Sicherheitsgesetz 2.0 angestoßen.[6] Der entsprechende Referentenentwurf (RefE) wurde am 3.4.2019[7] von netzpolitik.org veröffentlicht und ist zurzeit Gegenstand der Ressortabstimmung innerhalb der Bundesregierung.[8] Da der RefE noch nicht auf den Seiten des BMI veröffentlicht wurde, ist der im Internetangebot der Kriminalpolitischen Zeitung verlinkte Entwurf vom 27.3.2019[9] Grundlage dieses Beitrags.

Am 25.7.2015 trat das (erste) Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)[10] in Kraft. Das Gesetz schuf durch Änderun-

* *Dr. Anna Oehmichen* ist Partnerin bei Knierim & Kollegen in Mainz und Lehrbeauftragte an der Justus-Liebig-Universität Gießen. *Björn Weißenberger* ist Student der Rechtswissenschaften an der Johannes-Gutenberg Universität Mainz und studentischer Mitarbeiter bei Knierim & Kollegen.

1 Vgl. bspw. die Berichterstattung zu mehreren Hackerangriffen auf den Deutschen Bundestag ab dem Jahr 2015, zu denen sogar eine Wikipedia-Seite existiert (https://de.wikipedia.org/wiki/Hackerangriffe_auf_den_Deutschen_Bundestag, zuletzt abgerufen am 4.5.2019). Nur exemplarisch: „Hackerangriff auf Bundestag: „Hier herrscht völlige Ratlosigkeit““ auf handelsblatt.com vom 4.1.2019, https://www.handelsblatt.com/politik/deutschland/datenklau-cyberangriff-auf-politiker-hier-herrscht-voellige-ratlosigkeit/23828688.html (zuletzt abgerufen am 4.5.2019).

2 Entgegen einer landläufigen Meinung gibt es nicht entsprechend zu „dem“ über Standard-Browser zugänglichen Internet (= sog. Surface-Web) „das eine“ Darknet. Ein Darknet ist vielmehr ein abgeschirmter Bereich des Internets (= Teil des sog. Deep Web, das nicht von Suchmaschinen indexiert ist), wobei jedes Darknet nur durch eine speziell auf dieses Darknet zugeschnittene Software betreten werden kann. Die bekannteste (aber keineswegs einzige) entsprechende Software ist der sog. Tor-Browser. Ein wesentliches Merkmal eines jeden Darknets ist die Möglichkeit zur anonymen und nur mit erheblichem Aufwand nachverfolgbaren Kommunikation. Vgl. zur Begriffsdefinition ausführlich *Ihwas,* WiJ 2018, 138 (138 ff.).

3 Vgl. bspw. erst kürzlich die Zerschlagung des „weltweit zweitgrößten Markplatz[es] im Darknet“ „Wallstreet Market“; „BKA und FBI heben Darknet-Marktplatz aus“, Meldung auf tagesschau.de vom 3.5.2019: https://www.tagesschau.de/investigativ/swr/darknet-wall-street-market-101.html (zuletzt abgerufen am 4.5.2019).

4 Vgl. *BGH*, Beschl. v. 8.1.2019 – 1 StR 356/18 – juris. Das *LG München I* hat den Angeklagten wegen mehrerer Waffendelikte, in einem Fall in Tateinheit mit fahrlässiger Tötung in neun Fällen und mit fahrlässiger Körperverletzung in fünf Fällen, zu einer Gesamtfreiheitsstrafe von sieben Jahren verurteilt. Der *BGH* hat sowohl das Rechtsmittel des Angeklagten als auch die der Nebenkläger als unbegründet verworfen, da die Verurteilung, insbesondere die Begründung der Fahrlässigkeitsstrafbarkeit und die Ablehnung eines bedingten Beilhilfevorsatzes rechtsfehlerfrei erfolgt seien. Das Verfahren ist damit rechtskräftig abgeschlossen.

5 Vgl. bspw. die Berichterstattung zum Prozess vor dem *LG Limburg* (Az.: 1 Kls – 3 Js 7309/18) zur kinderpornographischen Plattform „Elysium“. Exemplarisch: „Urteil im Elysium-Prozess“, Videobeitrag des ZDF für „heute - in Deutschland“ vom 7.3.2019: https://www.zdf.de/nachrichten/heute-in-deutschland/urteil-im-elysium-prozess-100.html (zuletzt abgerufen am 13.5.2019).

6 Vgl. MMR-Aktuell 2018, 411330 (Meldung vom 16.10.2018).

7 Vgl. die Meldung „IT-Sicherheitsgesetz 2.0: Wir veröffentlichen den Entwurf, der das BSI zur Hackerbehörde machen soll“ vom 3.4.2019 auf netpolitik.org: https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/ (zuletzt abgerufen am 4.5.2019). Vgl. auch *Kipker,* MMR-Aktuell 2019, 415455.

8 Bundesjustizministerin *Barley* steht dem RefE dabei durchaus skeptisch gegenüber, vgl. die Meldung „Barley bremst Seehofer“ vom 29.4.2019 auf sueddeutsche.de: https://www.sueddeutsche.de/politik/sicherheitsgesetze-barley-bremst-seehofer-1.4426205 (zuletzt abgerufen am 4.5.2019)).

9 Siehe https://kripoz.de/2019/04/04/referentenentwurf-eines-zweiten-gesetzes-zur-erhoehung-der-sicherheit-informationstechnischer-systeme-it-sicherheitsgesetz-2-0-it-sig-2-0/ (zuletzt abgerufen am 4.5.2019).

10 BGBl. I 2015, S. 1324.

gen des BSI-Gesetzes (BSIG) insbesondere IT-Mindeststandards und Meldepflichten für die Betreiber sogenannter Kritischer Infrastrukturen.[11]

Nur knapp zweieinhalb Jahre später kündigten die Regierungsparteien der aktuellen 19. Legislaturperiode in ihrem Koalitionsvertrag vom 12.3.2018 an, das IT-Sicherheitsgesetz weiterentwickeln zu wollen.[12] Auch in der Digitalen Agenda des BMI, die am 20.3.2019 veröffentlicht wurde, findet sich das sog. IT-Sicherheitsgesetz 2.0 an erster Stelle. Es soll eine Reaktion auf immer „dynamischer, variantenreicher und professioneller" werdende Cyberangriffe darstellen.[13]

Insofern erscheint es konsequent, dass der RefE im Wesentlichen Änderungen des BSIG vorsieht bzw. die Kompetenzen des BSI erweitern will (Art. 1 RefE). Im Unterschied zum (ersten) IT-Sicherheitsgesetz sieht der RefE darüber hinaus aber auch Änderungen im StGB und in der StPO vor (Art. 4 und 5 RefE).

Der vorliegende Beitrag widmet sich gerade diesen Artikeln 4 und 5 des RefE. Dabei wird der Schwerpunkt auf die für die strafrechtliche Praxis wesentlichsten Punkte gelegt.

Grundsätzlich sind dies der § 126a StGB-E „Zugänglichmachen von Leistungen zur Begehung von Straftaten", der mitunter als Darknet-Paragraph bezeichnet wird (unten II.), der sog. „Digitale Hausfriedensbruch" des § 202e StGB-E („Unbefugte Nutzung informationstechnischer Systeme") und § 163g StPO-E, durch den Ermittlungsbehörden Zugriff auf und Nutzung von virtuellen Identitäten von Tatverdächtigen ermöglicht werden soll (unten III.).

Der vorliegende Beitrag klammert § 202e StGB-E bewusst aus, da es sich bei der Norm um die unveränderte Neuauflage eines Gesetzesentwurfes des Bundesrates aus dem Jahr 2016 handelt.[14] Diese ist bereits mehrfach kommentiert und einhellig abgelehnt worden.[15] Dieser auch vom Bundesjustizministerium geteilten[16] Ansicht ist zuzustimmen, ohne dass es hier einer Wiederholung der Argumente im Einzelnen bedürfte.

Lediglich überblicksartig (unten IV.) werden die Regelungen dargestellt, welche „nur" die Strafrahmen bestehender Vorschriften verschärfen oder Straftatbestände zu Katalogtaten bereits bekannter Ermittlungsmaßnahmen hinzufügen.

II. Der neue § 126a StGB-E – kein (!) Darknet-Paragraph

„Zugänglichmachen von Leistungen zur Begehung von Straftaten

(1) Wer Dritten eine internetbasierte Leistung zugänglich macht, deren Zweck oder Tätigkeit darauf ausgerichtet ist, die Begehung von rechtswidrigen Taten zu ermöglichen, zu fördern oder zu erleichtern, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwerer Strafe bedroht ist.

(2) Die Strafe darf nicht schwerer sein, als die für die Tat im Sinne von Absatz 1 angedrohte Strafe.

(3) Mit Freiheitsstrafe von sechs Monaten bis zu zehn Jahren wird bestraft, wer die Tat gewerbsmäßig oder als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Straftaten im Sinne dieser Vorschrift verbunden hat, begeht.

(4) Absatz 1 gilt nicht für Handlungen,
1. wenn die Begehung von Straftaten nur einen Zweck oder eine Tätigkeit von untergeordneter Bedeutung darstellt, oder
2. die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Dazu gehören insbesondere berufliche Handlungen der in § 53 Abs. 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Personen."

1. Entwicklung und Inhalt der Entwurfsregelung

Bereits im aktuellen Koalitionsvertrag war vorgesehen, dass Strafbarkeitslücken für das „Betreiben eines

---

11 Vgl. *Gitter/Meißner/Spauschus,* ZD 2015, 512 (513 f.). Darüber hinaus beschäftigten sich bspw. auch *Roos,* MMR 2015, 636; *Djeffal,* MMR 2015, 716; *Hornung,* NJW 2015, 3334 und *Spindler*, CR 2016, 297 mit Inhalten und Auswirkungen dieses Gesetzes. Die im Rahmen der Umsetzung der NIS-Richtlinie (Richtlinie [EU] 2016/1148) erfolgten, geringfügigen Anpassungen der nach dem (ersten) IT-Sicherheitsgesetz bestehenden Rechtslage durch das Umsetzungsgesetz vom 23.6.2017 (BGBl. I 2017, S. 1885) bespricht *Kipker*, MMR 2017, 143.

12 So der Koalitionsvertrag zwischen CDU, CSU und SPD „Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für das Land", Zeile 1969; im Ergebnis ähnlich Zeilen 1902 ff., 5868 ff.

13 „Die Digitale Agenda des BMI. Prioritäre digitale Themen des Bundesministeriums des Innern, für Bau und Heimat", S. 2. Sie ist online abrufbar auf der Seite des BMI: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/it-digitalpolitik/digitale-agenda.htm (zuletzt abgerufen am 4.5.2019).

14 Vgl. BR-Drs. 338/16, in den Bundestag mit einer (ablehnenden) Stellungnahme der Bundesregierung eingeführt durch BT-Drs. 18/10182. Der Entwurf wurde in der 18. Legislaturperiode nicht behandelt und unterfiel somit dem Grundsatz der Diskontinuität. Er wurde während der 19. Legislaturperiode mit BR-Drs. 47/18 erneut und unverändert vom Bundesrat verabschiedet. Die Bundesregierung hatte nunmehr keine Vorbehalte gegen das Vorhaben (vgl. BT-Drs. 19/1716, S. 19). Der RefE greift diesen Entwurf im Wesentlichen auf (vgl. RefE, S. 83).

15 *Mavany,* ZRP 2016, 221; *Basar,* jurisPR-StrafR 26/2016, Anm. 1; *Buremeyer/Golla,* K&R 2017, 14; *Tassi,* DuD 2017, 175; *Kahler/Hoffmann-Holland*, KriPoZ 2018, 267; *Brodowski*, ZIS 1/2019, 49; *Kuius,* https://www.kujus-strafverteidigung.de/blog/digitaler-hausfriedensbruch/ (zuletzt abgerufen am 14.5.2019).

16 Vgl. die Stellungnahme gegenüber golem.de in der Meldung „Bund warnt vor Verschärfung der Hackerparagrafen" vom 15.2.2019 unter: https://www.golem.de/news/digitaler-hausfriedensbruch-bund-lehnt-hoehere-strafen-fuer-hacker-weiter-ab-1902-139414.html (zuletzt abgerufen am 14.5.2019).

Darknet-Handelsplatzes für kriminelle Waren und Dienstleistungen“ geschlossen werden sollten.[17] Gesetzgeberische Tätigkeit entfaltete zunächst das Land Nordrhein-Westfalen (NRW), welches am 18.1.2019 einen Gesetzesantrag in den Bundesrat einbrachte, der einen neuen § 126a StGB mit der amtlichen Überschrift „Anbieten von Leistungen zur Ermöglichung von Straftaten“ vorsah.[18] Am 15.2.2019 wurde dieser Antrag zur weiteren Beratung an die Ausschüsse überwiesen[19] und dort offensichtlich kontrovers diskutiert. Jedenfalls fand sich in der Beschlussempfehlung der Ausschüsse (auch) eine Version der Norm, die auf Betreiben Bayerns[20] den Straftatbestand deutlich erweiterte und den Strafrahmen von maximal drei auf maximal fünf Jahren verschärfte.[21] Die bayrische Fassung des § 126a StGB-E lehnte das Plenum des Bundesrats in seiner Sitzung vom 15.3.2019 ab und verabschiedete den restriktiveren[22] Entwurf aus NRW, erweitert um eine Änderung des § 5 StGB zur Anwendbarkeit deutschen Strafrechts bei Auslandstaten.[23]

Der RefE greift nun gerade die abgelehnte Fassung des Antrags auf und macht sich auch deren Begründung zu eigen.[24] Er sieht demnach als Tatbestandsmerkmal nicht vor, dass „Zugang und Erreichbarkeit [der internetbasierten Leistung] durch besondere technische Vorkehrungen beschränkt“[25] sein müssen. Er stellt das Zugänglichmachen internetbasierter Leistungen unter Strafe, ganz gleich, welche rechtswidrige Tat dadurch ermöglicht, gefördert oder erleichtert werden soll, sofern diese Handlung nicht andernorts mit schwererer Strafe bedroht ist (Abs. 1). Der Bundesratsentwurf (BR-E) enthielt hier noch in einem Satz 2 einen abschließenden Katalog von Straftaten, bei deren Ermöglichung oder Förderung (nicht: Erleichterung) die Strafbarkeit ausschließlich eintreten sollte. Beiden Entwürfen gemein ist die Begrenzung des Strafrahmens auf den Strafrahmen der rechtswidrigen Tat, hinsichtlich derer eine Leistung angeboten (so der BR-E) bzw. zugänglich gemacht (so der RefE) wurde (Abs. 2). Ein besonders schwerer Fall (§ 126a Abs. 3 StGB-E) liegt gemäß dem RefE nicht nur im Fall der Gewerbsmäßigkeit (so noch der BR-E) sondern auch bei einer bandenmäßigen Begehung vor. Eingeschränkt wird die Strafbarkeit im RefE durch den Tatbestandsausschluss des § 126a Abs. 4 StGB-E, der im BR-E nicht vorgesehen war. Danach gilt Abs. 1 nicht in Fällen, in denen das Zugänglichmachen internetbasierter Leistungen zur Begehung von Straftaten nur „einen Zweck oder eine Tätigkeit von untergeordneter Bedeutung darstellt“ (Nr. 1) oder der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dient (Nr. 2). Nicht in den RefE aufgenommen wurde (ohne Begründung) die Änderung des § 5 StGB zur erweiterten Anwendung deutschen Strafrechts in Bezug auf § 126a StGB-E.

2. Erläuterung der Entwurfsregelung

Zwar geht die Regelung in ihrer Begründung auch auf die Besonderheiten des Darknet ein,[26] stellt aber ausdrücklich „jegliche [!] internetbasierte Zugänglichmachung von Leistungen“,[27] die von Abs. 1 erfasst werden, unter Strafe. Die Norm weist somit keinen Darknet-Bezug mehr auf.[28]

Eine Leistung i.S.d. Vorschrift meint dabei jedes Angebot, das sich an einen oder mehrere Nutzer richtet, ohne dass es auf eine Dauer oder wiederholte Nutzung ankäme.[29] Internetbasiert ist sie nach dem RefE, wenn sie mittels eines Dienstes erfolgt, der „auf der Netzwerkschicht des OSI-Referenzmodells über das Internet-Protokoll (IP) vermittelt“[30] wird. Entsprechende Dienste sollen damit nicht nur das Internet nach allgemeinem Sprachgebrauch, sondern auch E-Mail-Anwendungen oder Voice-over-IP-Dienste sein.[31] Zugänglich gemacht werde die internetbasierte Leistung nach den zu § 184 Abs. 1 Nr. 1 StGB entwickelten Maßstäben, „wenn den Nutzern die Möglichkeit der Wahrnehmung der Leistung ermöglicht wird“.[32] Von der Norm erfasst werden sollen demnach auch Handlungsweisen, bei denen eine Person, die an den späteren illegalen Geschäften der Plattform unbeteiligt ist, den Speicherplatz und das Routing hierfür für einen Dritten bereitstellt.[33]

Die zugänglich gemachte internetbasierte Leistung muss schließlich darauf ausgerichtet sein, die Begehung von rechtswidrigen Taten zu ermöglichen, zu fördern oder zu erleichtern. Hierbei handelt es sich nach der Intention des RefE um das zentrale Abgrenzungskriterium zwischen strafwürdigen und straflosen Angeboten, die möglicherweise sogar entgegen ihrer Zielsetzung auch für die Begehung rechtswidriger Taten genutzt werden.[34] Auf die Art der rechtswidrigen Tat komme es hingegen nicht an, sogar Äußerungsdelikte seien grundsätzlich erfasst.[35] Das Abstellen auf die Zielsetzung der zugänglich gemachten internetbasierten Leistung sei dabei in Anlehnung an die

17 Koalitionsvertrag (Fn. 12), Zeilen 6008 f.
18 BR-Drs. 33/19.
19 Vgl. BR-Prot. 974, S. 21.
20 Vgl. dazu die Stellungnahme des bayrischen Staatsministers der Justiz *Eisenreich* in BR-Prot. 975, S. 92.
21 Vgl. BR-Drs. 33/1/19, Ziffer 1 (= S. 1-15).
22 Vgl. dazu die Stellungnahme des nordrhein-westfälischen Justizministers *Biesenbach* in BR-Prot. 975, S. 91 f.
23 Vgl. BR-Prot. 975, S. 93. Die finale Beschlussfassung findet sich in BR-Drs. 33/19(B) und mit einer Stellungnahme der Bundesregierung in BT-Drs. 19/9508.
24 So ausdrücklich RefE, S. 76.
25 So der BR-Antrag (Fn. 23).
26 Vgl. bspw. RefE, S. 76.
27 So wortgleich RefE, S. 79 und 80.
28 So auch *Rückert* in seinem Beitrag „Neues Darknet-Strafrecht im Bundesrat. Überflüssige Strafnorm mit Risiken und Nebenwirkungen“ vom 15.3.2019 auf lto.de zur bayrischen Fassung des BR-E in BR-Drs. 33/1/19, Ziffer 1, die wie geschildert vom RefE 1:1 übernommen wurde: https://www.lto.de/recht/hintergruende/h/bundesrat-strafrecht-fuer-darknet-strafbarkeitsluecke-kriminalisierung/ (zuletzt abgerufen am 13.5.2019).
29 RefE, S. 80 (= BT-Drs. 19/9508, S. 13).
30 RefE, S. 79.
31 So RefE, S. 79.
32 RefE, S. 80.
33 Sog. „bulletproof hosting“, vgl. RefE, S. 80. Das Phänomen beschreibt auch *May* im Interview mit *Suliak* auf lto.de vom 11.1.2019, „Leitender Ermittler nach dem Datenhack. Schwere Hackerangriffe härter bestrafen“, https://www.lto.de/recht/hintergruende/h/hacker-daten-leak-internetkriminalitaet-ermittlungen-ausspaehen-datenhehlerei-staatsanwaltschaft/ (zuletzt abgerufen am 13.5.2019).
34 Vgl. RefE, S. 79 und 80 (ebenso BT-Drs. 19/9508, S. 13)
35 Vgl. RefE, S. 78.

Formulierungen in § 129 StGB[36] bzw. § 202c Abs. 1 Nr. 2 StGB[37] erfolgt. Die Zielsetzung sei in jedem konkreten Einzelfall zu prüfen und ergebe sich indiziell zum Beispiel aus dem tatsächlichen Angebot der Online-Plattform, dem Umgang mit Hinweisen auf Handel mit illegalen Waren und Dienstleistungen und auch Vorgaben in Allgemeinen Geschäftsbedingungen oder Ähnlichem.[38]

3. Begründung der Entwurfsregelung

Als wesentlicher Grund für die Strafbarkeit nach § 126a StGB-E wird im RefE die „besondere Gefährlichkeit des Zugänglichmachens internetbasierter Leistungen […], die sich ohne zeitliche, sachliche und räumliche Grenzen an Personen jeden Alters richten", genannt.[39] Das Betreiben der Plattform alleine solle die Strafbarkeit begründen, ohne dass es auf den Nachweis der Beteiligung an konkreten illegalen Geschäften ankomme.[40] Gerade diese Einbindung könne nämlich hinsichtlich Plattformbetreibern oft nicht nachgewiesen werden, da die einzelnen Transaktionen, Tauschgeschäfte o.Ä. bilateral zwischen Käufer und Verkäufer erfolgten, ohne dass dies öffentlich einsehbar sei. Deshalb und weil auch bei Erstellung eines Forums vom Ersteller oft nicht klar vorgegeben sei, wie sich die (illegalen) Aktivitäten genau entfalten sollten, komme eine Strafbarkeit wegen Beihilfe i.S.d. § 27 StGB häufig nicht in Betracht.[41] Ähnlich bereite es auch bei einem bandenmäßigen Vorgehen regelmäßig Schwierigkeiten, konkrete strafrechtlich relevante Tatbeiträge nachzuweisen, die insbesondere dann *de lege lata* nicht vorlägen, wenn ein einzelner Betreiber einer Plattform sich nur um technische oder organisatorische Belange kümmere und glaubhaft versichern könne, von den illegalen Geschäften keine Kenntnis gehabt zu haben.[42] Schließlich sei auch eine Strafverfolgung nach § 129 StGB nicht stets erfolgsversprechend, da diese nur bei mehreren Betreibern einer Plattform einschlägig sei und selbst solche Zusammenschlüsse nicht immer den Organisationsgrad erreichten, den man für eine kriminelle Vereinigung verlangen müsse.[43] Die deshalb bestehende Strafbarkeitslücke für die Betreiber von auf die Förderung illegaler Zwecke ausgerichteten Plattformen gelte es zu schließen.[44]

Die Regelung solle im Kernstrafrecht getroffen werden, um eine einheitliche Rechtsanwendung zu gewährleisten.[45] Ebenso sei ein Straftatenkatalog nicht sachgerecht, da dieser unvollständig zu bleiben drohe. Außerdem würden die oben dargestellten Gründe für die Strafwürdigkeit der Norm unabhängig von der (mindestens) erleichterten rechtswidrigen Tat gelten, sodass es nicht darauf ankomme, ob es sich dabei um Äußerungsdelikte oder andere Straftaten handele. Die Verhältnismäßigkeit werde dabei durch die Begrenzung des Strafrahmens nach § 126a Abs. 2 StGB-E gewahrt.[46]

4. Würdigung der Entwurfsregelung

Wenngleich das Bestreben des Gesetzgebers, die Förderung krimineller Handlungen im Internet durch Strafgesetze zu unterbinden, praktischen Bedürfnissen Rechnung tragen mag, ist doch zweifelhaft, inwieweit der aktuelle Entwurf diesem Ziel auch gerecht wird. Die Weite des Tatbestands führt dazu, dass auch neutrales, alltägliches Verhalten wie etwa das Erbringen einer IT-Dienstleistung kriminalisiert werden kann. Entgegen der Auffassung des Gesetzgebers handelt es sich in solchen Fällen nicht um eine „Nachweisschwierigkeit", sondern eher um eine Frage der Strafwürdigkeit.

Die Schwierigkeit, neutrales Verhalten strafrechtlich zu erfassen, ist bereits seit dem Problem der „neutralen Beihilfe" bekannt.[47] Entgegen den Überlegungen des Gesetzgebers erschöpft sich das Problem aber nicht in dem Umstand, dass es an einer gesetzlichen Regelung fehlt, sondern besteht vielmehr im Kern darin, dass erhebliche Zweifel an der Strafwürdigkeit solcher Verhaltensweisen und damit der wichtigsten Legitimation des Strafrechts fehlen. Es wird dabei nicht verkannt, dass die Entscheidung über die Strafwürdigkeit einer Handlung in erster Linie dem Gesetzgeber zusteht.[48] Dieser ist dabei jedoch angehalten, für eine einheitliche Rechtsordnung zu sorgen, die frei von widersprüchlichen Normen ist.[49] Nach den §§ 7 ff. TMG sind Betreiber von Internetseiten grundsätzlich nicht für fremde Inhalte verantwortlich und müssen diese nicht aktiv nach illegalen Inhalten durchsuchen, sondern nur bei Kenntniserlangung löschen. Indem nunmehr auch der Umgang des Betreibers mit illegalen Inhalten auf seiner Seite als Kriterium für eine Strafbarkeit nach § 126a StGB-E dienen soll,[50] wird dieses Prinzip unterlaufen und der Betreiber doch zu einer Kontrolle aller Inhalte gezwungen.[51] Spätestens der parlamentarische Gesetzgeber sollte diesen Wertungswiderspruch thematisieren und idealerweise auflösen.

---

36 So RefE, S. 79 (und BT-Drs. 19/9508, S 9).
37 So RefE, S. 80.
38 So übereinstimmend RefE, S. 79 und 80 (= BT-Drs. 19/9508, S 13). Durch die Ergänzung des Wortlautes um das „zu erleichtern" im RefE im Unterschied zum BR-E soll wohl klargestellt werden, dass eine verwerfliche Zielrichtung der internetbasierten zugänglich gemachten Leistung nicht nur dann vorliegt, wenn das Maß einer Beihilfe i.S.d. § 27 StGB erreicht ist. So jedenfalls die Begründung zur bayrischen Fassung des BR-E in BR-Drs. 33/1/19, S. 13.
39 RefE, S. 80. Ähnlich auch S. 78.
40 RefE, S. 78 (= BT-Drs. 19/9508, S. 11).
41 RefE, S. 77 (= BT-Drs. 19/9508, S. 9 f.).
42 RefE, S. 77 f. (= BT-Drs. 19/9508, S. 10).
43 RefE, S. 78 (= BT-Drs. 19/9508, S. 10).
44 RefE, S. 78 (= BT-Drs. 19/9508, S. 11).
45 RefE, S. 78 (= BT-Drs. 19/9508, S. 11).
46 RefE, S. 78 f., 81 (= BT-Drs. 19/9508, S. 11, 14)
47 Vgl. hierzu ausführlich insb. zuletzt *LG Karlsruhe*, BeckRS 2018, 40013, Rn. 292 ff. m.w.N.
48 Vgl. *Hassemer/Neumann,* in: NK-StGB, 5. Aufl. (2017), Vor § 1 Rn. 85 ff. auch mit zutreffendem Verweis auf *BVerfG*, NJW 1994, 1577 (1579).
49 Zwar wird durchaus diskutiert, inwiefern das Prinzip der Widerspruchsfreiheit der Rechtsordnung tatsächlich Verfassungsrang besitzt (eher bejahend: *Andorfer/Rimpf,* NZWiSt 2019, 54 [56 f.], eher verneinend: *Brüning,* NVwZ 2002, 33). Die Bundesregierung misst dem Prinzip jedoch im Bereich der Rechtsetzung durchaus Bedeutung zu, vgl. § 46 Abs. 1 GGO und Anlage 6, Nr. 3, lit. b zu § 45 Abs. 1 GGO.
50 Vgl. oben bei Fn. 38.
51 So auch *Rückert,* Fn. 28. *Kubiciel/Mennemann,* jurisPR-StrafR 08/2019, Anm. 1 meinen sogar, die Implementierung „eine[r] Art Dauerüberwachungspflicht" sei der vermutlich mit Schaffung der Norm verfolgte Zweck.

Zweifel bestehen auch hinsichtlich der Verhältnismäßigkeit der Vorschrift. Durch den Verzicht auf einen Straftatenkatalog wird nämlich auch das Zugänglichmachen von internetbasierten Leistungen zur Begehung von Bagatellkriminalität pönalisiert, wobei erschwerend hinzukommt, dass die Norm in den Katalog des § 100a StPO aufgenommen werden soll und damit verdeckte Überwachungsmaßnahmen von erheblicher Eingriffsintensität wie TKÜ ermöglicht werden (vgl. unten IV.). Insoweit wird man §§ 100a ff. StPO jedenfalls verfassungskonform restriktiv auslegen und auf Straftaten von einiger Erheblichkeit beschränken müssen.

Auch wird sich die Strafbarkeit des jeweiligen Beitrages dem Plattforminhaber nicht in jedem Falle unmittelbar erschließen, so dass auch die Vereinbarkeit mit dem Bestimmtheits-Grundsatz angesichts der Weite des Tatbestandmerkmales „rechtswidrige Taten“ zweifelhaft ist. Damit werden auch Fahrlässigkeitstaten erfasst. Zu diesen ist aber keine Beihilfe oder Anstiftung möglich, weshalb Wertungswidersprüche vorprogrammiert sind. Was, wenn Schuldausschließungs- oder Entschuldigungsgründe für den Täter dieser rechtswidrigen Tat greifen? Gerade die im RefE explizit in Bezug genommenen Äußerungsdelikte[52] oder bspw. auch Verstöße gegen das Urheberrecht, die in §§ 106 ff. UrhG strafbewehrt sind, können zudem nur bei einer Begutachtung jedes einzelnen Beitrages (in einer Chat-, Pinnwand- oder Kommentarfunktion, in Gestalt eines Fotos oder Videos etc.) erkannt werden und bedürfen zur Beurteilung ihrer Strafbarkeit im Hinblick auf Art. 5 GG mindestens fortgeschrittener Kenntnisse des Verfassungsrechts.

Das Tatbestandsmerkmal der Zweckrichtung der zugänglich gemachten internetbasierten Leistung stellt dabei aufgrund seiner Unbestimmtheit keine hilfreiche Einschränkung dar. Dabei ist schon unklar, ob wie bei § 129 StGB eher auf die innere Geisteshaltung[53] bei Erstellung der internetbasierten Leistung oder in Anlehnung an § 202c StGB eher auf deren objektiven Zweck[54] abgestellt werden soll. Die vom RefE genannten Indizien helfen auch nicht weiter. Nach welchem Maßstab soll sich das „tatsächliche Angebot“ einer Plattform bestimmen? Beleidigungsdelikte und Urheberrechtsverstöße finden sich auf jeder größeren (Video-)Plattform (mit Kommentarfunktion) zuhauf. Der Umgang mit Hinweisen auf Handel mit illegalen Waren mag bspw. bei angezeigten Verstößen gegen das WaffG einen Rückschluss auf die Redlichkeit des Webseitenbetreibers geben. Etwaige Hinweise auf Verstöße gegen § 259 StGB (Hehlerei) dürften für einen Betreiber jedoch kaum aufzuklären sein. Vorgaben in den AGB wird man nach der Intention des RefE wohl nur dann als Kriterium heranziehen können, wenn diese AGB nicht nur auf dem Papier bestehen, sondern auch aktiv durchgesetzt werden. Es stellt sich dann die Frage, welche Vorgaben sich der Gesetzgeber hier vorstellt, die im Ergebnis nicht doch wieder auf eine allgemeine Kontrollpflicht entgegen §§ 7 ff. TMG hinauslaufen. Schließlich verhält sich der RefE auch nicht zu der Frage, welche Indizien bei internetbasierten Chat-Diensten gelten sollen, bei denen die Betreiber überhaupt keinen Einblick in die Kommunikation, mithin die tatsächliche Nutzung der zugänglich gemachten Leistung haben.

Eine nennenswerte Beschränkung dieser Unsicherheiten ist auch durch den Tatbestandsausschluss nach Abs. 4 Nr. 1 nicht zu erwarten. Denn wenn bei einer zugänglich gemachten internetbasierten Dienstleistung die Begehung von Straftaten nur von untergeordneter Bedeutung ist, dann kann es ohnehin nicht Zweck dieser Dienstleistung sein, die Begehung von Straftaten (mindestens) zu erleichtern. Der Regelungsgehalt von Abs. 4 Nr. 1 beschränkt sich somit darauf, festzustellen, dass Abs. 1 nicht für Handlungen gilt, die schon gar nicht vom Tatbestand des Abs. 1 erfasst sind.

Selbst wenn der Gesetzgeber im weiteren Verfahren wieder einen Straftatenkatalog einführen sollte, würde dies zwar zur Verhältnismäßigkeit und Bestimmtheit der Norm beitragen, könnte aber dennoch die aufgezeigten Probleme nicht lösen. Diese dürften im Endeffekt nicht geringer sein als die Probleme, die den Behörden bei der Frage, ob eine Beihilfe nach § 27 StGB vorliegt, begegnen.[55] Auch an den rein praktischen Schwierigkeiten, der (anonym agierenden) Betreiber nicht habhaft werden zu können, dürfte sich durch die Vorschrift jedenfalls bei verfassungskonformer Anwendung der verdeckten Ermittlungsmaßnahmen nichts ändern.[56]

III. Staatlicher Zugriff auf Benutzerkonten durch § 163g StPO-E[57]

> *„[1] Begründen bestimmte Tatsachen den Verdacht, dass jemand Täter oder Teilnehmer einer Straftat im Sinne von § 100g Abs. 1 StPO ist, so dürfen die Staatsanwaltschaft sowie die Behörden und Beamten des Polizeidienstes auch gegen den Willen des Inhabers auf Nutzerkonten oder Funktionen, die ein Anbieter eines Telekommunikations- oder Telemediendienstes dem Verdächtigen zur Verfügung stellt und mittels derer der Verdächtigte im Rahmen der Nutzung des Tele-*

52 Vgl. oben Fn. 35.

53 Vgl. *Heintschel-Heinegg,* in: BeckOK-StGB, 41. Edition (Stand: 1.2.2019), § 129 Rn. 6 f.

54 Vgl. *Widemann,* in: BeckOK-StGB, 41. Edition (Stand: 1.2.2019), § 202c Rn. 7.

55 Vgl. hierzu auch *Rückert* (Fn. 28), der zutreffend in Frage stellt, dass *de lege lata* überhaupt Strafbarkeitslücken bestehen. Ebenso *Kubiciel/Mennemann* (Fn. 51). Ähnlich *Buermeyer* im Zitat gegenüber netzpolitik.org in der Meldung vom 12.3.2019 „Bundesrat: Gesetzentwurf gegen „Darknet-Märkte“ könnte Anonymisierungs-Dienste gefährden“, https://netzpolitik.org/2019/bundesrat-gesetzentwurf-gegen-darknet-maerkte-koennte-anonymisierungs-dienste-gefaehrden/ (zuletzt abgerufen am 14.5.2019).

56 In diese Richtung zielend kann man auch das Zitat von *Bäcker* gegenüber netzpolitik.org (gleiche Meldung wie in Fn. 55) verstehen, dass der neue Straftatbestand wohl kaum je zu Verurteilungen führen werde, die sonst nicht möglich wären, seine Bedeutung aber in der Ermöglichung der Durchführung von Überwachungsmaßnahmen liegen werde (vgl. dazu unten IV.)

57 Die Einfügung von Satzzahlen in der nachstehend abgedruckten Norm des RefE erfolgte zur besseren Übersicht durch die *Verfasser*.

kommunikations- oder Telemediendienstes eine dauerhafte virtuelle Identität unterhält, zugreifen. [2] Sie dürfen unter dieser virtuellen Identität mit Dritten in Kontakt treten. [3] Der Verdächtige ist verpflichtet, die zur Nutzung der virtuellen Identität erforderlichen Zugangsdaten herauszugeben. [4] § 95 Abs. 2 gilt entsprechend mit der Maßgabe, dass die Zugangsdaten auch herauszugeben sind, wenn sie geeignet sind, eine Verfolgung wegen einer Straftat oder einer Ordnungswidrigkeit herbeizuführen. [5] Jedoch dürfen die durch Nutzung der Zugangsdaten gewonnenen Erkenntnisse in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Verdächtigen oder einen in § 52 Abs. 1 der Strafprozessordnung bezeichneten Angehörigen des Verdächtigen nur mit Zustimmung des Verdächtigen verwendet werden."

1. Entwicklung und Inhalt der Entwurfsregelung

Die Regelung des § 163g StPO-E geht nicht auf einen BR-E zurück und war – soweit ersichtlich – weder von den Strafverfolgungsbehörden[58] noch der Justizministerkonferenz ausdrücklich gefordert worden.

Die Vorschrift ermächtigt Ermittlungsbehörden, auf Benutzerkonten von Tatverdächtigen einer Straftat i.S.d. § 100g Abs. 1 StPO zuzugreifen und die mit dem Account verbundenen Funktionen zu nutzen (Satz 1). Einzige weitere Einschränkung ist dabei, dass der Account und seine Funktionen von einem Anbieter eines Telekommunikations- oder Telemediendienstes zur Verfügung gestellt werden und zur Unterhaltung einer dauerhaften virtuellen Identität dienen. Die Befugnis nach Satz 1 schließt dabei insbesondere die Nutzung von Chat-Funktionen ein (klarstellend Satz 2). Die Zugangsdaten muss der Tatverdächtige auch gegen seinen Willen herausgeben (Satz 3) und kann hierzu mittels Ordnungsgeld und Beugehaft angehalten werden (Satz 4). Erkenntnisse, die gem. § 163g StPO-E gewonnen werden, dürfen nur mit Einverständnis des Tatverdächtigen, auf dessen Nutzerkonto sie zurückzuführen sind, verwendet werden (Satz 5).

2. Erläuterung der Entwurfsregelung

Die Ausführungen des RefE zu § 163g StPO-E[59] beschäftigen sich hauptsächlich mit der angeblichen grundsätzlichen Notwendigkeit und Zulässigkeit einer solchen Ermächtigungsgrundlage, ohne auf die Eingriffsvoraussetzungen im Einzelnen einzugehen.

So kann lediglich vermutet werden, dass mit dem Begriff des „Anbieter[s] eines Telekommunikations- oder Telemediendienstes" (Satz 1) die Definitionen des § 3 Nr. 6 TKG und § 2 Nr. 1 TMG in Bezug genommen werden sollen. Auch die „dauerhafte virtuelle Identität" (ebenfalls Satz 1), die mittels des Nutzerkontos und seiner Funktionen unterhalten werden soll, wird nicht näher definiert. Dabei ist der Begriff der StPO und – soweit ersichtlich – auch dem übrigen Gesetzeskanon bisher fremd. Im weiteren Gesetzgebungsverfahren wäre eine Klarstellung über die Zielrichtung der Formulierung wünschenswert.

Zur Regelung des Satzes 5 erklärt der RefE, dass hierfür § 97 Abs. 1 InsO als Vorbild diente.[60] Nach dieser Norm ist ein Schuldner zur umfassenden Auskunftserteilung verpflichtet (§ 97 Abs. 1 Satz 1 InsO), auch wenn er sich selbst belasten muss (§ 97 Abs. 1 Satz 2 InsO), kommt in einem solchen Fall allerdings in den Genuss eines Verwendungsverbotes (§ 97 Abs. 1 Satz 3 InsO). Hierzu ist es hM, dass das Verwendungsverbot nicht nur ein Verwertungsverbot bzgl. mitgeteilter Tatsachen darstellt, sondern solche Informationen nicht einmal der Anlass weiterer Ermittlungen sein dürfen.[61] Bei § 163g StPO-E müsste dies entsprechend sowohl für alle Tatsachen gelten, die aufgrund der mitgeteilten Nutzungsdaten im Account vorgefunden werden, als auch für solche Tatsachen, die den Ermittlungsbehörden erst durch die Nutzung des Accounts bekannt werden. Eine entsprechende Klarstellung des Gesetzgebers, ob das sog. Fernwirkungsverbot des § 97 Abs. 1 Satz 3 InsO ebenso umfassend für § 163g StPO-E gelten soll, wäre wünschenswert.

3. Begründung der Entwurfsregelung[62]

Die grundsätzliche Notwendigkeit, § 163g StPO-E zu schaffen, wird damit begründet, dass für die Übernahme digitaler Identitäten zurzeit keine Rechtsgrundlage bestünde. Die Zugangsdaten an sich seien keiner Beschlagnahme oder vorläufigen Sicherstellung nach §§ 94 bzw. 111b ff. StPO zugänglich. Eine freiwillige Herausgabe der Daten erfolge nur äußerst selten, insbesondere weil für den Tatverdächtigen trotz der für ihn positiven Folgen des § 46b StGB regelmäßig ein erhebliches Risiko der Selbstbelastung bestünde. Trotzdem seien Zugriff auf und Nutzung von Benutzerkonten in den Bereichen des illegalen Handels im Darknet und der Kinderpornographie äußerst wichtige Ermittlungsmethoden. Den bereits bestehenden Nutzeraccounts würde im Unterschied zu neu angelegten Konten ein erhöhtes Maß an Vertrauen entgegengebracht,

---

58 Vgl. bspw. den Vortrag „Kernpunkte einer Digitalen Agenda für das Straf- und Strafprozessrecht" von *Franosch* auf der BKA-Herbsttagung im November 2018, online abrufbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Herbsttagungen/2018/herbsttagung2018FranoschLangfassung.html (zuletzt abgerufen am 12.5.2019), der trotz zahlreicher im RefE aufgegriffener Vorschläge keine Regelung, wie sie § 163g StPO-E darstellt, forderte. Vgl. auch *Krause,* NJW 2018, 678 (680), der trotz seiner Tätigkeit als Staatsanwalt bei der Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) der Generalstaatsanwaltschaft Frankfurt a.M. keinen Reformbedarf bzgl. der *de lege lata* bestehenden Möglichkeit der (freiwilligen) Übernahme von digitalen Identitäten anmeldete.

59 RefE, S. 86 a.E. bis 88.

60 RefE, S. 88.

61 Sog. Fernwirkungsverbot, vgl. *Werner,* in: BeckOK-InsO, 13. Edition (Stand: 26.10.2018), § 97 InsO Rn. 17; *Jungmann,* in: Schmidt, Insolvenzordnung, 19. Aufl. (2016), § 97 Rn. 12;

62 Zum gesamten Nachfolgenden vgl. RefE, S. 86 f.

sodass strafrechtlich relevantes Verhalten schneller/deutlicher zutage trete bzw. ermittelt werden könne. Anders könne die pseudonymisierte und anonymisierte Kommunikation innerhalb dieser Netzwerke kaum erfasst werden.

Ausschließlich die Übernahme der digitalen Identität, nicht aber deren anschließende Nutzung, bedürfe einer ausdrücklichen Ermächtigungsgrundlage. Letztere stelle keinen grundrechtlich relevanten Eingriff (gegenüber dem Kommunikationspartner) dar. Das Fernmeldegeheimnis (Art. 10 GG) schütze nur das Vertrauen des Einzelnen darin, dass seine Fernkommunikation nicht von Dritten zur Kenntnis genommen werde, nicht aber, dass der Kommunikationspartner tatsächlich (nur) der sei, den man erwarte. Ein personengebundenes Vertrauen in den Kommunikationspartner werde demnach nicht geschützt. Auch das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) sei nicht betroffen, da ein Eingriff nur bei einer staatlich veranlassten Verletzung des Vertrauens in den Kommunikationspartner vorliege. Bei einer anonymisierten Kommunikation könne es jedoch kein grundrechtlich geschütztes Vertrauen geben, da man über die Identität des Kommunikationspartners ohnehin nie Gewissheit habe. Ein allgemeines Vertrauen darauf, jedenfalls nicht mit einer staatlichen Stelle zu kommunizieren, sei nicht schutzwürdig. Dies gelte auch dann, wenn die staatliche Stelle sich wie ein Straftäter gebärde und gerade dieses Vertrauen ausgenutzt werde.

4. Würdigung der Entwurfsregelung

Insbesondere im BtM-Bereich wird das im Entwurf vorgesehene Ermittlungshandeln unter Einsatz verdeckter Ermittler im Darknet bereits heute praktiziert. Unter dem Versprechen einer Strafmilderung (mit oder ohne § 46b StGB) werden Beschuldigte zur "freiwilligen" Weitergabe ihrer Zugangsdaten zu Darknet-Foren verleitet, ohne dass es hierfür eine gesetzliche Grundlage gäbe. Vor diesem Hintergrund muss man dankbar sein, dass überhaupt das Erfordernis einer gesetzlichen Grundlage gesehen wird. Problematisch ist aber deren konkrete Ausgestaltung. Die Regelung in ihrer jetzigen Form ist abzulehnen. Denn sie steht in diametralem Gegensatz zum Nemo Tenetur-Grundsatz. Die Selbstbelastungsfreiheit wird vollständig unterlaufen, wenn der Verdächtige zur Herausgabe seiner Zugangsdaten *verpflichtet* wird. Erschreckend ist, dass der Gesetzgeber, der offenbar nur von schuldigen Verdächtigen ausgeht, dies sehenden Auges hingenommen hat, wenn ausgeführt wird, die "freiwillige" Herausgabe mittels Kronzeugenregelung sei nicht ausreichend, weil trotz der "für ihn positiven Folgen" ein erhebliches Risiko der Selbstbelastung bestünde. Dass es ein großes praktisches Bedürfnis der Ermittlungsbehörden darstellt, kriminelle Strukturen auch im Internet zu infiltrieren, ist angesichts der Omnipräsenz und Möglichkeiten der digitalen Welt zwar eine Selbstverständlichkeit. Der RefE begeht aber den fatalen Fehler, den Gesetzeswortlaut nicht auf diese Zweckrichtung zu beschränken, wodurch die Regelung trotz ihres intendierten, engen Anwendungsbereichs[63] zu einer Generalklausel verkommt.

So ist es nach der aktuellen Gesetzesfassung nicht einmal notwendig, dass ein Tatverdacht bezüglich einer Straftat in der digitalen Welt im Raum steht, um den Ermittlungsbehörden den Zugriff auf virtuelle Identitäten zu gestatten. Erforderlich ist lediglich ein Tatverdacht einer Straftat i.S.d. § 100g Abs. 1 StPO, d.h. einer „mittels Telekommunikation begangenen“ Straftat oder einer „Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere“ (aber nicht ausschließlich) einer Katalogtat i.S.d. § 100a Abs. 2 StPO. Eine Beziehung zwischen diesem Tatverdacht und der virtuellen Identität, die übernommen werden soll, ist nach dem Wortlaut des RefE nicht erforderlich. Der Zugriff wird auf jede virtuelle Identität gestattet, die von einem TKG- oder TMG-Anbieter zur Verfügung gestellt wird und der Unterhaltung einer dauerhaften virtuellen Identität dient. Dies bedeutet auch, dass selbst beim Verdacht einer mittels einer virtuellen Identität begangenen Tat i.S.d. § 100g Abs. 1 StPO nicht nur gerade diese Identität, sondern auch jedes beliebige andere existierende Nutzerkonto übernommen werden kann. Da Straftaten i.S.d. 100g Abs. 1 StPO auch jegliche mittels Telekommunikation begangene Straftaten sind (§ 100g Abs. 1 Nr. 2 StPO), genügt grundsätzlich schon jedes simple Beleidigungsdelikt in einem sozialen Netzwerk oder Chat, um den Ermittlungsbehörden umfassenden Zugriff bspw. auf E-Mail-Konten zu gewähren.

An diesem Beispiel wird deutlich, dass bei § 163g StPO-E die sonst bei den §§ 100a ff., §§ 163d ff. StPO üblichen (und verfassungsrechtlich gebotenen[64]) Einschränkungen fehlen. So enthält die Norm keinerlei Einschränkungen zur Gewährung ihrer Verhältnismäßigkeit und knüpft die Ausübung der Befugnis nicht an die Vorgabe, dass die Ermittlungen andernfalls wesentlich erschwert oder gar aussichtslos wären. Angesichts der Eingriffsintensität – der Zugriff bedeutet in den meisten Fällen einen Eingriff in den Kernbereich privater Lebensführung – ist auch nicht nachvollziehbar, weshalb die Norm keinen Richtervorbehalt und keinen Kernbereichsschutz vergleichbar den §§ 100d, 100e StPO n.F. vorsieht. Der Zugriff auf Benutzerkonten ist hinsichtlich der Eingriffsintensität durchaus vergleichbar mit den Eingriffen auf Telekommunikationsdaten iSd §§ 100a, 100b StPO.

Etwas anderes könnte allenfalls bei der Nutzung eines einmal übernommenen Accounts gelten. Hierzu muss dem RefE zwar vorgehalten werden, dass es verfassungsrechtlich unzulässig[65] wäre, wenn man – wie es der aktuelle Wortlaut (Satz 2) nahelegt – ohne Weiteres die Kommunikation zu jedem beliebigen Dritten erlauben würde, ganz gleich ob auch nur irgendein Bezug zu einer Straftat besteht.[66] Man muss dem RefE jedoch zugestehen, dass

63 Schließlich spricht auch der RefE „nur“ von Darknet-Handelsplattformen und Plattformen zur Verbreitung von Kinderpornografie (S. 86).

64 Vgl. die für sämtliche Ermittlungsmethoden der Strafprozessordnung geltenden Aussagen in *BVerfG*, BeckRS 2005, 27151 Rn. 102 ff.

65 Vgl. oben *BVerfG* (Fn. 64).

66 Vgl. zur sonst in der StPO üblichen Praxis bspw. die einschränkenden bzw. explizit klarstellenden Regelungen bei § 163f Abs. 1 S. 3, Abs. 2 oder §§ 100a Abs. 3, 100b Abs. 3 StPO.

zahlreiche Stimmen für die Nutzung eines einmal übernommenen Accounts keine spezielle Ermächtigungsgrundlage verlangen, sondern dies als den Einsatz eines nicht öffentlich ermittelnden Polizeibeamten ansehen, der von der Generalklausel des § 163 StPO umfasst ist.[67] Paradox ist freilich, dass der RefE mit den vorstehenden Regelungen ja gerade eine spezielle Ermächtigungsgrundlage schafft, obwohl er davon auszugehen scheint, dass nicht einmal ein Rückgriff auf die Generalklausel notwendig sei, da überhaupt kein Grundrechtseingriff vorliege.[68]

Auch verfassungsrechtlich ist die Rechtslage aber keineswegs so eindeutig, wie im RefE geschildert. Zutreffend ist zwar, dass nach der Rechtsprechung des *BVerfG* Art. 10 GG hauptsächlich die (technische) Integrität des Übertragungsmediums schützt und nicht betroffen ist, wenn einer der Beteiligten die Inhalte der Kommunikation auch staatlichen Stellen zur Kenntnis bringt.[69] Dies gilt jedoch nur, solange der Zugriff auf die Kommunikationsinhalte von dem Beteiligten, der ihn ermöglicht, *freiwillig* eingeräumt wird.[70] Von einer Freiwilligkeit kann angesichts der Regelungen des § 163g StPO-E allerdings keine Rede mehr sein. Darüber hinaus erscheint es auch vorschnell, einer Unterhaltung im Darknet pauschal jegliches schutzwürdige Vertrauen im Hinblick auf das Recht auf informationelle Selbstbestimmung abzusprechen. Zwar existiert zweifelsohne das vielseits zitierte Diktum des *BVerfG*, dass nur das Ausnutzen eines schutzwürdigen Vertrauens des Betroffenen in die Identität und Motivation seines Kommunikationspartners einen Grundrechtseingriff darstellt und ein solches Ausnutzen aufgrund der Anonymität im Internet bzw. der damit verbundenen generellen Ungewissheit über die Identität des Gegenüber regelmäßig nicht vorliegt.[71] Dass diese Regelvermutung aber auch für den Fall gilt, in dem eine staatliche Stelle eine bereits laufende Kommunikation übernimmt (und nicht erst selbst in Gang bringt), innerhalb derer möglicherweise bereits zahlreiche private Details ausgetauscht wurden, sodass sich beim Kommunikationspartner ein gefestigtes Bild seines Gegenübers gebildet hat, ist zumindest nicht selbstverständlich.[72] Jedenfalls würde diese Regel nicht greifen, wenn in Einzelfällen die Anonymität bspw. durch Videotelefonate oder reale Treffen aufgegeben wurde.[73]

Eine spezielle Eingriffsgrundlage (auch) für die Account-Nutzung ist demnach zwar vorzugswürdig, sollte sich dabei aber nicht auf einen (Neben-)Satz beschränken. Dabei sind die Rechtsprechung zur rechtstaatswidrigen Tatprovokation,[74] der Schutz des Kernbereichs privater Lebensgestaltung des Kommunikationspartners[75] und die Tatsache zu beachten, dass die Nutzung des Benutzerkontos nur dann tatsächlich erfolgsversprechend sein wird, wenn sie zeitgleich mit einem Nutzungsverbot für den eigentlichen Inhaber (und Dritte mit Kenntnis der Zugangsdaten) einhergeht, was wiederum die Eingriffsintensität der Maßnahme erhöht.

IV. Weitere geplante Änderungen

1. Qualifikationstatbestände für die Geheimnisschutzdelikte der §§ 202a bis e StGB(-E)

Im Bereich der weiteren Änderungen ist insbesondere die Einführung umfangreicher Qualifikationstatbestände durch einen geplanten neuen § 202f StGB-E[76] hervorzuheben, der dann auch den weiteren geplanten „digitalen Hausfriedensbruch" (§ 202e StGB-E) umfassen soll. Mit der Norm sollen konzentriert an einer Stelle Qualifikationstatbestände für Geheimnisschutzdelikte im IT-Bereich (§§ 202a bis e StGB(-E)) geschaffen werden, für die der Strafrahmen sechs Monate bis zehn Jahre beträgt (§ 202f Abs. 1 StGB-E).[77] Ein Strafmaß nicht unter einem Jahr soll bei schweren Fällen i.S.d. § 202f Abs. 2 und 3 StGB-E gelten, sofern diese nicht „minder schwer" (§ 202f Abs. 4 StGB-E) sind.

Zusätzlich sollen mit § 202f Abs. 5 StGB-E besonders schwere Fälle (anhand von vier Regelbeispielen) begründet werden, bei deren Verwirklichung der Strafrahmen zwischen einem und zehn Jahren beträgt.

2. Strafrahmenverschärfungen

Nach Art. 4 Nr. 3 RefE sollen die Strafrahmen der §§ 202a bis d und 303 b Abs. 1 StGB einheitlich von bis zu zwei bzw. drei Jahren auf bis zu fünf Jahren angehoben werden. Für § 303b Abs. 2 StGB soll das Strafmaß von Geldstrafe bis zu fünf Jahren auf sechs Monate bis fünf Jahre angehoben werden.

3. Erweiterung von Straftatenkatalogen im Rahmen der §§ 100a ff. StPO

Schließlich sieht der RefE vor, die Kataloge der §§ 100a, b und g StPO zu erweitern (Art. 5 Nr. 1 bis 3 RefE). In

---

67 So *Krause,* NJW 2018, 678 (680) mit Verweis (auch) auf *BGH*, BeckRS 2010, 143592. *Soiné,* NStZ 2014, 248 und *Rosengarten/Römer,* NJW 2012, 1764 positionieren sich zwar nicht ganz so eindeutig, neigen jedoch auch deutlich dieser Ansicht zu.

68 RefE, S. 87 ist hier zugegebenermaßen etwas uneindeutig. Einerseits wird konstatiert, dass die Nutzung übernommener Accounts „keinen Eingriffscharakter habe". Andererseits wird hieraus (nur) die Schlussfolgerung gezogen, dass es „keine[r] spezielle[n] Ermächtigungsgrundlage" bedürfe.

69 Vgl. *BVerfG*, NJW 2008, 822 (835 Rn. 290).

70 *BVerfG* (Fn. 69), Rn. 291 ff.

71 Vgl. *BVerfG* (Fn. 69), Rn. 310, 311.

72 Kritisch auch *Laudon* in seinem Beitrag „Passwort oder Beugehaft: Das Ende des Schweigens" vom 10.4.2019 auf strafakte.de: https://www.strafakte.de/gesetzgebung/passwort-beugehaft/ (zuletzt abgerufen am 13.5.2019).

73 Vgl. dazu auch *Ihwas,* WiJ 2018, 138 (143 f., 146).

74 Zuletzt *BGH*, NStZ 2018, 355 m. Anm *Esser* auch zu den Divergenzen zwischen deutscher und europäischer Rechtsprechung.

75 Vgl. hierzu bspw. § 100d StPO.

76 Vgl. RefE S. 30 f.

77 Im Einzelnen sind Qualifikationstatbestände vorgesehen für
- §§ 202a bis e StGB(-E) bei Handeln für eine fremde Macht, Gewerbsmäßigkeit oder bandenmäßiger Begehung (§ 202f Abs. 1 Nr. 1 StGB-E);
- §202e StGB-E, soweit eine große Anzahl an informationstechnischen Systemen unbefugt genutzt werden (§ 202f Abs. 1 Nr. 2 StGB-E);
- §§ 202a bis d StGB, soweit die Tathandlung in der Absicht erfolgt, eine Gefahr für die öffentliche Sicherheit, die Begehung einer gemeingefährlichen Straftat oder einer besonders schweren Umweltstraftat (§ 330 StGB) herbeizuführen oder zu ermöglichen (§ 202f Abs. 1 Nr. 3 StGB-E).

den Katalog der (Quellen-)TKÜ (§ 100a StPO) sollen die §§ 126a, 202a bis e, 202f Abs. 2 und 3 und §§ 303 a und b StGB(-E) aufgenommen werden. Eine Online-Durchsuchung (§ 100b StPO) und die Erhebung gespeicherter Verkehrsdaten (§ 100g Abs. 2 StPO) sollen bei Tatverdacht bzgl. Qualifikationstatbeständen der §§ 126a Abs. 3 und 202 Abs. 2 und 3 StGB-E möglich sein. Die Begründung hierzu stellt in den wenigen Worten, die sie zu den Änderungen verliert, ausschließlich auf das durch den RefE erhöhte Strafmaß ab, was nicht den Vorgaben des *BVerfG* genügt.[78] Die Änderungen sind (mit dieser Begründung) abzulehnen. Der RefE widerspricht sich sogar selbst, da er zu § 126a Abs. 1 StGB-E noch ausführte, dass dieser für sich genommen kein Anlass für eine TKÜ nach § 100a StPO sein könne, sondern allenfalls die Qualifikationstatbestände.[79]

VI. Fazit und Ausblick

Dem RefE muss zugutegehalten werden, dass er zahlreiche Vorhaben des Bundesrates aufgreift, bündelt und in letzter Konsequenz möglicherweise eine Entscheidung des parlamentarischen Gesetzgebers über sie herbeiführt. Allerdings überzeugen die vorgeschlagenen Regelungen inhaltlich nicht. Soweit das materielle Strafrecht betroffen ist, handelt es sich um symbolische Gesetzgebung, die zum einen keinen Mehrwert für die Praxis bringt und zum anderen Gesetzeslücken annimmt, um neutrale Verhaltensweisen zu kriminalisieren, deren Strafwürdigkeit sich nicht ohne Weiteres erschließt. Es scheint, dass die neu geplanten Qualifikationstatbestände sowie die Strafschärfungen im Bereich der (digitalen) Geheimschutzdelikte insbesondere mit dem Ziel eingeführt wurden, verdeckte Ermittlungsmaßnahmen in diesem Bereich zu ermöglichen und so frühzeitig „Hacker“, aber auch politisch missliebige Whistleblower wie *Snowden* oder *Assange*, zu einem frühen Zeitpunkt aufzuspüren. Hinsichtlich der strafprozessualen Änderungsvorschläge gelingt es dem RefE nicht, (angebliche) Strafverfolgungsbedürfnisse und (verfassungsrechtlich garantierten) Grundrechtsschutz in einen angemessenen Ausgleich zu bringen. In der Ressortabstimmung wird der RefE sicherlich einige Änderungen erfahren[80] und es wird sich lohnen, die weitere Entwicklung im Blick zu behalten.

---

78 Vgl. *BVerfG,* NJW 2012, 833 (836, Rn. 204 ff), wo eine „Gesamtschau“ gefordert wird.

79 RefE, S. 80.

80 Vgl. in diese Richtung oben Fn. 8 und 16.