Strafbarkeit und Strafverfolgung des Betreibens internetbasierter Handelsplattformen für illegale Waren und Dienstleistungen

*von Prof. Dr. Mark A. Zöller**

Abstract
Vor dem Hintergrund spektakulärer Strafverfahren gegen die Betreiber von Foren und Handelsplattformen für illegale Waren und Dienstleistungen im Darknet ist aktuell eine intensive rechtspolitische Debatte über die Notwendigkeit entbrannt, das Anbieten bzw. Zugänglichmachen von internetbasierten Leistungen zur Begehung von Straftaten eigenständig mit Strafe zu bedrohen. Der vorliegende Beitrag stellt zunächst die besonderen Rahmenbedingungen von Ermittlungen im Darknet dar und wirft vor diesem Hintergrund einen kritischen Blick auf die aktuellen Vorschläge des Bundesrates sowie des Bundesministeriums des Innern, für Bau und Heimat zur Einführung eines neuen § 126a StGB. Er gelangt zu dem Ergebnis, dass die damit vorgelegten Regelungskonzepte mit zahlreichen Widersprüchlichkeiten behaftet sind und ihnen der Nachweis tatsächlich bestehender Strafbarkeitslücken bislang nicht überzeugend gelungen ist.

Against the background of numerous spectacular criminal proceedings against operators of forums and trading platforms for illegal goods and services on the internet a lively debate has flared up on the necessity for imposing criminal sanctions for offering or making available internet-based services for committing criminal offenses. The article at hand starts by presenting the special conditions for criminal investigations within the so-called darknet. It takes a critical look at the current legislative proposals by the German Federal Assembly and the Federal Ministry of the Interior for the introduction of a new paragraph 126a to the German Criminal Code. As a result, the regulation concepts presented so far seem to include several contradictions and their protagonists have been unable to present proof for the existence of actual loopholes in criminal liability.

I. Die aktuelle Situation

In den Medien überschlagen sich derzeit die Berichte darüber, was man im sog. Darknet alles anonym ordern kann:[1] *Waren* wie Betäubungsmittel,[2] Waffen und Munition, Hacker-Programme, gefälschte Dokumente wie Reisepässe, Personalausweise oder Führerscheine und kinderpornografisches Material, aber auch illegale *Dienstleistungen* wie die Anmeldung von Wohnsitzen, Fahrzeugen, Bankkonten, die Entwicklung und Verbreitung von Schadsoftware, die Vermietung von Bot-Netzen und sogar die Ausführung von Auftragsmorden sind für alle, die ernsthaft danach suchen, nur wenige Mausklicks entfernt. Andererseits häufen sich aber auch Berichte über entsprechende Ermittlungserfolge der Strafverfolgungsbehörden. Dazu nur drei Beispiele:[3]

Beispiel 1: Am 22. Juli 2016, erschoss beim sog. Amoklauf von München[4] der zur Tatzeit 18-jährige *David S.* im Olympia-Einkaufszentrum im Stadtteil Moosach neun Menschen und tötete sich anschließend selbst. Bei der Tatwaffe handelte es sich um eine wieder schussfähig gemachte Dekowaffe vom Typ „Glock 17“. Sie war von *David S.* unter dem Pseudonym „Maurächer“ von einem 33-jährigen Marburger Waffenhändler mit rechtsextremistischem Hintergrund und dem Pseudonym „rico“ erworben worden. Der Kontakt zwischen Käufer und Verkäufer war zuvor über das Darknet-Forum „Deutschland im Deep Web“ hergestellt worden.[5]

Beispiel 2: Am 23. und 24. April 2019, haben Kräfte des Bundeskriminalamts drei mutmaßliche Betreiber des Darknet-Marktplatzes „Wall Street Market“ vorläufig festgenommen. Hierbei handelte es sich nach Angaben der Ermittler um die „weltweit zweitgrößte Handelsplattform im Darknet“.[6] Zuletzt waren dort 63.000 Verkaufsangebote, insbesondere für Betäubungsmittel, gestohlene Daten, gefälschte Ausweise und Kreditkarten, gelistet. Die Plattform hatte etwa 5.400 Verkäufer und 1.150.000 Kundenkonten. Bezahlt wurde mit Kryptowährungen wie Bitcoin[7] oder Monero. Das Umsatzvolumen soll bei 40 Mio. Euro gelegen haben. Von den Transaktionen haben die mutmaßlichen Betreiber der Plattform

* Der Verfasser ist Inhaber des Lehrstuhls für Deutsches, Europäisches und Internationales Strafrecht und Strafprozessrecht sowie Wirtschaftsstrafrecht und Direktor des Instituts für Deutsches und Europäisches Strafprozessrecht und Polizeirecht (ISP) an der Universität Trier.

1 Hierzu etwa *Rath*, DRiZ 2016, 292 (293); *Fünfsinn/Ungefuk/Krause*, Kriminalistik 2017, 440 (442 f.); *Fünfsinn/Krause*, FS Eisenberg, 2019, S. 641 (643); *Greco*, ZIS 2019, 435 (437 f.).

2 Diese machen den weit überwiegenden Teil der im Darknet gehandelten Güter aus; vgl. *Fünfsinn/Ungefuk/Krause*, Kriminalistik 2017, 440 (442).

3 Zu weiteren Beispielen, insbesondere den Vorläufern „Silk Road“ und „Alpha-Bay“, s. *Tzanetakis*, APuZ 2017, 41 (43 ff.).

4 Hierzu *Hartleb*, Kriminalistik 2018, 532 ff.

5 Bei „Deutschland im Deep Web“ handelte es sich ursprünglich um ein Forum zur Diskussion und zum Meinungsaustausch. Später wurde u.a. auch eine Unterkategorie „Waffen“ hinzugefügt, die – neben der Veröffentlichung von Diskussionsbeiträgen – dazu genutzt wurde, unerlaubt mit Waffen zu handeln; vgl. *LG Karlsruhe*, StV 2019, 400 (401).

6 Vgl. dazu die Pressemitteilung der Generalstaatsanwaltschaft Frankfurt am Main und des Bundeskriminalamts v. 3.5.2019, abrufbar unter: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2019/Presse2019/190503_WallStreetMarket.html (zuletzt abgerufen am 10.9.2019).

7 Zum Phänomen Bitcoin *Brenneis*, APuZ 2017, 29 ff.

Provisionen zwischen 2 und 6 Prozent des Verkaufspreises erhalten.

Beispiel 3: Am 28. Juni 2019 schließlich teilte das BKA mit, man habe nach monatelangen Ermittlungen den größten Online-Drogenshop Deutschlands mit der Bezeichnung „Chemical Revolution" abgeschaltet.[8] Elf Tatverdächtige seien wegen des dringenden Tatverdachts des bandenmäßigen Handeltreibens mit Betäubungsmitteln in nicht geringer Menge festgenommen worden. Als Hauptverdächtiger gilt ein aus dem Landkreis München stammender, 26 Jahre alter Mann, der diese Plattform im September 2017 aufgebaut und anschließend mit weiteren Tatverdächtigen gemeinsam betrieben haben soll. Auf der Internetseite des Onlineshops waren Betäubungsmittel und vor allem *synthetische Drogen* wie Ecstasy und Amphetamin zum Verkauf und weltweiten Versand angeboten worden. Auch hier haben die Käufer mit der Kryptowährung Bitcoin bezahlt.

II. Strafrechtliche Ermittlungen im Darknet

Allen drei Beispielen ist gemeinsam, dass es um das Betreiben internetbasierter Plattformen für illegale Waren im sog. Darknet ging. Schon der Begriff dieses Phänomens ist häufig mit Fehlvorstellungen behaftet, die für eine Betrachtung aus juristischer Sicht naturgemäß nicht förderlich sind. Die Bezeichnung als „Darknet", d.h. als „dunkles Netz" suggeriert einen Zusammenhang mit negativen bzw. illegalen Geschehnissen, die besser im Verborgenen bleiben.[9]

1. Das Phänomen „Darknet"

Für viele ist das Darknet daher ein Synonym für die Unterwelt des Internet mit all seinen Schattenseiten.[10] Bei nüchterner Betrachtung stellt es sich zunächst einmal nur als digitaler Raum dar, der mit technologischen Instrumenten abgeschirmt ist und seinen Nutzern ein hohes Maß an Anonymität gewährleistet.[11] Die meisten Dinge, die Menschen jeden Tag im Netz erledigen – Kommunizieren, Musik und Videos abrufen, Einkaufen, Restaurants suchen oder Tickets buchen – finden aber üblicherweise nur im *sichtbaren Teil des Internets* statt, der häufig auch als „Visible Web", „Surface Web" oder „Clearnet" bezeichnet wird. Mit Standardbrowsern wie Firefox, Safari oder Google Chrome erreichen wir nur *frei zugängliche* Webseiten. Auch Suchmaschinen wie Google präsentieren uns in Wirklichkeit gar nicht *alle* vorhandenen Daten zu unserer jeweiligen Suchanfrage, sondern indizieren nicht einmal das Visible Web vollständig. Das Internet gleicht insoweit einem Ozean.[12] In diesem Ozean an Informationen liegen die frei zugänglichen Webseiten unmittelbar an der Wasseroberfläche. Unterhalb dieser sichtbaren Oberfläche folgt sodann das sog. „Deep Web", also der Bereich, der durch Passwörter und Codes geschützt ist. Hierzu zählen z.B. Datenbanken und Archive. Erst auf dem Grund des Ozeans liegt schließlich das Darknet.[13]

Als „Darknet" wird jener Teil des Internets bezeichnet, der durch sog. Peer-to-Peer-Verbindungen (P2P) zwischen Nutzern geschaffen wird und nur unter Zuhilfenahme spezieller Software zugänglich ist.[14] Benötigt werden eine Verschlüsselungsplattform und die genaue Zieladresse der gewünschten Internetseite. Hierfür ist in der Praxis häufig eine vorherige Einladung durch einen bereits als vertrauenswürdig eingestuften Nutzer und eine Bestätigung durch einen Administrator erforderlich. Allerdings existieren auch im frei zugänglichen Teil des Internets Listen mit direkten Links im TOR-Netzwerk.[15] Zudem hält auch das Darknet Suchmaschinen wie Grams, Torch oder Ahmia bereit, die aber im Hinblick auf Schnelligkeit und Nutzerfreundlichkeit nicht mit den aus dem Visible Web bekannten Produkten wie Google vergleichbar sind. Natürlich besitzt die so erreichte Anonymität in besonderem Maße Anziehungskraft für potenzielle Straftäter. Aber weder sind das Darknet selbst noch seine Nutzung per se illegal. Beides ist zunächst nur Ausdruck des Wunsches vieler Internetnutzer, sich im digitalen Raum frei von staatlicher wie privater Kontrolle bewegen zu können. Hierauf sind etwa Dissidenten und Oppositionelle in autokratischen Staaten,[16] Whistleblower oder Journalisten zwingend angewiesen.[17] Es ist auch kein Zufall, dass speziell die Entwicklung des TOR-Browser vor allem durch das US Naval Research Laboratory maßgeblich unterstützt wurde. Schließlich besteht ein nachvollziehbares praktisches Bedürfnis nicht nur US-amerikanischer Streitkräfte und Nachrichtendienste dafür, dass ihre Soldaten und Agenten auch von fremdem Territorium aus unüberwacht mit der eigenen Nachrichtendienstzentrale in der Heimat kommunizieren können.[18] Andererseits zeigt eine im Jahr 2016 veröffentlichte Studie des International Institute for Strategic Studies, dass immerhin 57 Prozent von insgesamt 5205 untersuchten aktiven Seiten im Darknet als illegal einzustufen waren.[19] Nach Angaben des BKA weisen dort rund 50 kriminelle Foren und Plattformen einen Deutschlandbezug auf.[20]

Der größte und bekannteste Teil des Darknets ist das „TOR-Netzwerk".[21] Für den Zugang hierzu ist ein sog.

---

8 Presseeinladung der Generalstaatsanwaltschaft Frankfurt am Main und des Bundeskriminalamts vom 28.6.2019, abrufbar unter: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2019/Presse2019/190628_PMChemicalRevolution.html (zuletzt abgerufen am 10.9.2019).

9 Zur Historie und Definition des Begriffs *Ihwas*, WiJ 2018, 138 (140 f.) m.w.N.

10 *Göppner*, Kriminalistik 2018, 623 (624).

11 Vgl. *Mey*, Darknet: Waffen, Drogen, Whistleblower, 2017, S. 11; *ders.*, APuZ 2017, 4; *Ihwas*, WiJ 2018, 138.

12 Instruktiv hierzu *Göppner*, Kriminalistik 2018, 623 (624).

13 Für eine Einstufung des Darknets als Teil des Deep Webs *Ihwas*, WiJ 2018, 138.

14 *Rath*, DRiZ 2016, 292; *Tzanetakis*, APuZ 2017, 41 (42); *Krause*, NJW 2018, 678; *Fiebig,* DRiZ 2019, 50.

15 *Rath*, DRiZ 2016, 292; *Ihwas*, WiJ 2018, 138 (141); *Greco*, ZIS 2019, 435 (436 f.).

16 Vgl. *Moßbrucker*, APuZ 2017, 16 ff.

17 Vgl. *Fiebig*, DRiZ 2019, 50.

18 Zur Abhängigkeit des Tor-Projekts von US-amerikanischen Regierungszuwendungen *May*, APuZ 2017, 4 (8).

19 Vgl. *Moore/Rid*, Cryptopolitik and the Darknet, 2016.

20 BT-Drs. 18/9487, S. 2; *Vogt,* Die Kriminalpolizei 2/2017, 4 (5); *Krause*, NJW 2018, 678 (679).

21 Allg. hierzu *Fünfsinn/Ungefuk/Krause*, Kriminalistik 2017, 440 f.; *May*, APuZ 2017, 4 ff.; *Göppner*, Kriminalistik 2018, 623 (624); *Ihwas*, WiJ 2018, 138 (139); *Greco*, ZIS 2019, 435 (436).

TOR-Browser erforderlich. Er steht auf zahlreichen frei zugänglichen Webseiten kostenlos zum Download bereit. Die Abkürzung „TOR" steht für „The Onion Router". Der Name erklärt sich aus der Tatsache, dass ihm ein stufenweises Verschlüsselungsschema zugrunde liegt, das an die Form einer Zwiebel mit ihren Schalen erinnert. Der TOR-Browser kaschiert die IP-Adresse des Ausgangsrechners, indem eine lange Reihe an Verbindungen zu verborgenen Servern ermöglicht wird. Diese Server werden als „Knoten" bezeichnet. Da jeder Knoten das gesendete Datenpaket erneut verschlüsselt, ist es bereits nach dem Passieren von drei Knotenpunkten technisch unmöglich, die Ursprungsadresse nachzuvollziehen. Erst am Ausgangsknoten erfolgt dann eine Entschlüsselung des Datenpaketes, so dass der *Empfänger* dieses ohne Probleme verarbeiten kann.

2. Besonderheiten für strafprozessuale Ermittlungen

Diese technischen Besonderheiten des Darknets haben natürlich auch praktische Folgen für die Ermittlungsarbeit der Strafverfolgungsbehörden.

a) Wirkungslosigkeit technikgestützter Überwachungsmaßnahmen

Wichtig ist zunächst die Erkenntnis, dass die ganz überwiegende Zahl der technikgestützten Zwangsmaßnahmen nach der Strafprozessordnung angesichts der Nutzung von Anonymisierungs- und Verschlüsselungssoftware im Darknet von vornherein aussichtslos ist.[22] Dies gilt insbesondere für „klassische" Telekommunikationsüberwachungsmaßnahmen (§ 100a Abs. 1 S. 1 StPO), Auskünfte über Verkehrs- und Bestandsdaten (§§ 100g, 100j StPO) oder die Beschlagnahme von Servern (§§ 94 ff. StPO). Wenn man nicht weiß, wo sich etwas befindet oder stattfindet, kann man es weder überwachen noch beschlagnahmen. Auch sofern individuelle Benutzerkennungen von Tatverdächtigen bei Darknet-Handelsplattformen oder -Foren öffentlich einsehbar sind, kommen Abfragen von Bestands- oder Nutzungsdaten nach den §§ 14 und 15 des Telemediengesetzes (TMG) bei den entsprechenden Plattformbetreibern *allenfalls hypothetisch* in Betracht. Zum einen sind die unter „Nicknames" operierenden Betreiber solche virtuellen Marktplätze nicht bekannt und infolge der von ihnen verwendeten Verschlüsselungstechnik auch nicht ermittelbar. Zum anderen verweigern diese infolge ihres illegalen Geschäftsmodells regelmäßig ohnehin jede Kooperation mit den Strafverfolgungsbehörden.[23]

Hinzu kommt, dass Kriminelle stets nach digitalen Kommunikationswegen *außerhalb* des Radars von Polizei und Staatsanwaltschaft suchen. So haben etwa die Ermittlungen im Zusammenhang mit dem Amoklauf von München ergeben, dass sich der Täter vor seiner Bluttat mit Gleichgesinnten über die Text- und Videochatfunktion der Spieleplattform „Steam" ausgetauscht hat, auf der jeden Tag allein Hunderttausende den Ego-Shooter „Counterstrike" spielen.[24]

b) Verdeckte Ermittler

Bei Ermittlungen im Darknet erlebt deshalb der Einsatz von Verdeckten Ermittlern eine Renaissance.[25] Bei solchen *Verdeckten Ermittlern* handelt es sich nach der Legaldefinition des § 110a Abs. 2 S. 1 StPO um Polizeibeamte, die unter einer ihnen verliehenen, auf Dauer angelegten, veränderten Identität, einer sog. Legende, ermitteln. Durch das Kriterium der *Dauerhaftigkeit* unterscheiden sie sich von den *nicht öffentlich ermittelnden Polizeibeamten* (den sog. noePs),[26] durch ihre Beamtenstellung von sonstigen privaten Vertrauenspersonen (V-Leuten) aus dem Milieu. Zwar treten auch Angehörige der beiden letztgenannten Personengruppen in der digitalen Welt im Einzelfall als Käufer oder Verkäufer von Betäubungsmitteln oder Waffen auf. Meist wird es aber darum gehen, sich unter einer Legende *längerfristig* eine digitale Identität aufzubauen, um in der kriminellen Szene Vertrauen zu gewinnen und Zugang zu illegalen Handelsplattformen zu erhalten. In letzter Zeit gehen die Strafverfolgungsbehörden daher verstärkt dazu über, sich *bereits existierender* Accounts oder digitaler Identitäten zu bedienen, die über eine hohe Reputation in der Szene verfügen.[27] Das hat auch den Vorteil, dass von diesen regelmäßig keine sog. „Keuschheitsproben",[28] also die Begehung von Straftaten als Zugangsvoraussetzung wie das Posten von kinderpornografischem Bildmaterial oder die Mitwirkung an BtM-Geschäften, verlangt werden, was Polizeibeamten naturgemäß untersagt ist und diese dann im Weigerungsfall rasch enttarnt. Insofern versucht man, Beschuldigte *bereits laufender* Strafverfahren durch mehr oder minder geschickten Hinweis auf eine mögliche Strafmilderung nach der Kronzeugenregelung des § 46b StGB dazu zu bewegen, Profile und Passwörter sowie Adressen im Darknet preiszugeben. Diese werden dann von den Strafverfolgern übernommen und zur Erkenntnisgewinnung genutzt. Völlig unproblematisch ist das nicht. Schließlich ist nach § 136a Abs. 1 S. 3 StPO das Versprechen eines gesetzlich nicht vorgesehenen Vorteils verboten. Die Polizeibeamten dürfen den Inhabern der Profile daher keine konkreten Versprechungen zum Strafmaß machen, da die diesbezügliche Entscheidung den Strafrichtern vorbehalten ist.

---

22 *Krause*, NJW 2018, 678 (679); vgl. auch *Safferling*, DRiZ 2018, 206; allg. zur Problematik des „Going Dark" *Schulze*, APuZ 2017, 23 ff.

23 *Krause*, NJW 2018, 678 (679).

24 *Hartleb*, Kriminalistik 2018, 532 (534).

25 Vgl. *Göppner*, Kriminalistik 2018, 623 (625) sowie *Fiebig*, DRiZ 2019, 50 (51) mit Zitat von *May*: „Meist ist der Einsatz von verdeckten Ermittlern die einzige Chance, um Straftaten im Darknet zu ermitteln"; ebenso *Ihwas*, WiJ 2018, 138 (142): „Personale Ermittlungsmethoden versprechen im anonymen Darknet generell den größten Ermittlungserfolg".

26 Hierzu *Ihwas*, WiJ 2018, 138 (143 f.).

27 *Rath*, DRiZ 2016, 292 (293); *Ihwas*, WiJ 2018, 138 (146); *Krause*, NJW 2018, 678 (680).

28 Dazu *Safferling*, DRiZ 2018, 206 f.

c) Schnittstellen zwischen virtueller und realer Welt

Von besonderem ermittlungstaktischem Nutzen sind darüber hinaus die Schnittstellen, an denen virtuelle und reale Welt ineinander übergehen. Bei einer Handelsplattform im virtuellen Raum müssen die dort durch Kryptowährung bezahlten Waren logischerweise irgendwann an den Erwerber verschickt werden. Dazu müssen die Händler den geschützten Raum des Darknets verlassen und ihre Päckchen ganz analog auf den Versandweg zum Kunden bringen. Insofern ist es in der Szene ein offenes Geheimnis, dass hierfür häufig unter falschen Personalien angemeldete oder gehackte Packstationen des Dienstleisters DHL genutzt werden.[29] Bei entsprechender Verdachtslage, dass eine bestimmte Packstation zum Versand oder Erhalt illegaler Waren genutzt wird, kann sich dann deren Observation durch Polizeibeamte vor Ort und/oder der Einsatz von Videoüberwachungstechnik anbieten.[30] Zudem lassen sich an der Ware möglicherweise Fingerabdrücke oder DNA-Spuren finden, die jedenfalls dann Ermittlungsansätze liefern, wenn die Spurenleger bereits in den einschlägigen Datenbanksystemen wie dem beim BKA geführten Automatisierten Fingerabdruck-Identifizierungs-System (AFIS) oder der dortigen DNA-Analyse-Datei geführt werden.[31]

d) Spurensuche im Visible Web

Häufig kann auch die Spurensuche im Visible oder Clear Web wichtige Ermittlungsansätze in Bezug auf Personen liefern, die für ihre kriminellen Aktivitäten den Schutz des Darknets suchen. Erfahrungsgemäß werden zumindest von unvorsichtigen Händlern und Nutzern von Handelsplattformen im Darknet deren Pseudonyme, Profilbilder, Produktbeschreibungen oder Mail-Adressen auch im *ungeschützten* Bereich des Internets verwendet.[32] Insofern setzen auch die Strafverfolgungsbehörden mittlerweile auf die Suche in öffentlich zugänglichen Quellen mit Hilfe von sog. Open-Source-Intelligence.[33] Zu den mit Hilfe solcher, ursprünglich aus dem Bereich der Nachrichtendienste stammenden Tools durchkämmten Quellen zählen etwa soziale Medien oder Internetangebote von Tageszeitungen, Fernseh- und Radiosendern.

e) Internationale Zusammenarbeit

Schließlich müssen sich bei internetbasierten Handelsplattformen weder die Betreiber als Personen mit ihren Laptops, PCs oder Smartphones noch die von ihnen zum Betrieb genutzten Server zwingend im Inland befinden. Ohne intensive Kooperation mit ihren Kolleginnen und Kollegen im Ausland sowie bei inter- und supranationalen Einrichtungen, sind daher rein nationale Ermittlungsverfahren deutscher Strafverfolgungsbehörden häufig zum Scheitern verdammt. Bei inter- und transnational operierenden Händlern können insbesondere sog. Gemeinsame Ermittlungsgruppen (Joint Investigation Teams) entscheidende Vorteile bieten (vgl. § 93 IRG). Das zeigt auch der Fall „Wall Street Market“, bei dem der Beschlagnahme der Plattform und ihrer kriminellen Inhalte eine intensive Kooperation der Generalstaatsanwaltschaft Frankfurt am Main und des BKA mit US-amerikanischen und niederländischen Ermittlern, aber auch mit Europol und Interpol vorausging.

III. Die (vermeintliche) gesetzgeberische Lösung: ein neuer § 126a StGB

Erstaunlicherweise soll die Lösung für zukünftige Erfolge bei der Bekämpfung von internetbasierten Handelsplattformen für illegale Waren und Dienstleistungen aber vorrangig im materiellen Strafrecht zu suchen sein. Im aktuellen rechtspolitischen Diskurs wird derzeit lebhaft über die Einführung eines neuen § 126a StGB diskutiert, der das Anbieten bzw. Zugänglichmachen von internetbasierten Leistungen zur Begehung von Straftaten eigenständig mit Strafe bedrohen soll.[34]

1. Bisheriger Gesetzgebungsverlauf

Der bisherige Gesetzgebungsverlauf für diese als „Darknet-Paragrafen“ betitelte Vorschrift ist allerdings kurios. Am 18. Januar 2019 hatte Nordrhein-Westfalen einen entsprechenden Gesetzesantrag in den Bundesrat eingebracht,[35] dem anschließend auch die Bundesländer Hessen und Bayern beigetreten sind. Am 15. März 2019 hat der Bundesrat mehrheitlich dafür gestimmt, den Gesetzentwurf in einer geänderten Fassung beim Deutschen Bundestag einzubringen. Dies ist am 17. April 2019 durch den „Entwurf eines Strafrechtsänderungsgesetzes – Einführung einer eigenständigen Strafbarkeit für das Betreiben von internetbasierten Handelsplattformen für illegale Waren und Dienstleistungen“ geschehen.[36] Darin wird u.a. die Einfügung eines neuen § 126a StGB mit folgendem Wortlaut vorgeschlagen:

§ 126a StGB-E [Anbieten von Leistungen zur Ermöglichung von Straftaten]

(1) Wer eine internetbasierte Leistung anbietet, deren Zugang und Erreichbarkeit durch besondere technische Vorkehrungen beschränkt und deren Zweck oder Tätigkeit darauf ausgerichtet ist, die Begehung von rechtswidrigen

---

29 *Rath*, DRiZ 2016, 292 (293); *Fünfsinn/Ungefuk/Krause*, Kriminalistik 2017, 440 (443); *Ihwas*, WiJ 2018, 138 (147); *Krause*, NJW 2018, 678 (680).

30 Vgl. *Göppner*, Kriminalistik 2018, 623 (625) mit Hinweis auf den Fall „Shiny Flakes“. Hier hatte der mutmaßliche Täter aus seinem Leipziger Jugendzimmer heraus über die Internetseite „Shiny Flakes“ sowohl im Clear Web als auch im Darknet von Dezember 2013 bis Februar 2015 in mehreren tausend Fällen Bestellungen über insgesamt rund 600 Kilogramm an illegalen Drogen verschickt. Die Ermittler waren ihm letztlich durch von ihm falsch frankierte Postsendungen auf die Schliche gekommen, die nicht an die falschen Absenderadressen zurückgeschickt werden konnten und dann von der Deutschen Post der Polizei übergeben wurden.

31 Vgl. *Rath*, DRiZ 2016, 292 (293).

32 Vgl. *Hostettler*, APuZ 2017, 10 (14 f.).

33 *Göppner*, Kriminalistik 2018, 623 (625 f.).

34 Erste Stellungnahmen hierzu bieten etwa *Oehmichen/Weißenberger*, KriPoZ 2019, 174 ff.; *Kubiciel/Mennemann*, jurisPR-StrafR 8/2019 Anm. 1; *Greier/Hartmann*, jurisPR-StrafR 13/2019 Anm. 1; *Greco*, ZIS 2019, 435 ff.

35 BR-Drs. 33/19.

36 BT-Drs. 19/9508.

Taten im Sinne von Satz 2 zu ermöglichen oder zu fördern, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist. Rechtswidrige Taten im Sinne des Satzes 1 sind

1. § 95 Absatz 1 des Gesetzes über den Verkehr mit Arzneimitteln,

2. §§ 29 Absatz 1 Nummer 1, 29a, 30, 30a des Betäubungsmittelgesetzes,

3. § 19 Absatz 1 des Grundstoffüberwachungsgesetzes,

4. § 52 Absatz 1 Nummer 1 und Absatz 3 Nummer 1 des Waffengesetzes,

5. § 40 Absatz 1 und 2 des Sprengstoffgesetzes,

6. §§ 19 Absatz 1, 20 Absatz 1, 20a Absatz 1, 22a Absatz 1 Nummer 1, 2 und 4 des Gesetzes über die Kontrolle von Kriegswaffen sowie

7. §§ 146, 147, 149, 152a, 152b, 184b Absatz 1, 202a, 202b, 202c, 263a, 275, 276, 303a und 303b des Strafgesetzbuches.

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

(3) Mit Freiheitsstrafe von sechs Monaten bis zu zehn Jahren wird bestraft, wer die Tat gewerbsmäßig begeht.

Allerdings handelt es sich hierbei nicht um den einzigen Entwurfstext, der derzeit im politischen Raum kursiert. In den Beschlussempfehlungen der zuständigen Bundesratsausschüsse fand sich auch eine auf Betreiben Bayerns deutlich verschärfte Fassung. Diese bayerische Vorschlagsfassung fand jedoch im Plenum des Bundesrates keine Mehrheit. Die bayerische Staatsregierung hatte das aber wohl schon vorhergesehen und entsprechend vorgesorgt. Schließlich existiert in Berlin mit dem Bundesministerium des Innern, für Bau und Heimat ein einflussreiches und vor allem CSU-geführtes Ministerium mit thematischem Bezug zum Sicherheitsrecht. Dort wurde mit Datum vom 27. März 2019 ein zwischenzeitlich von Netzpolitik.org geleakter Referentenentwurf für ein „IT-Sicherheitsgesetz 2.0“ vorgelegt, der sich derzeit noch in der Ressortabstimmung befindet. Art. 4 dieses Referentenentwurfs sieht ebenfalls die Einfügung eines neuen § 126a StGB vor. Dieser besteht – ein Schelm, wer Böses dabei denkt – exakt aus derjenigen Formulierung, mit der sich Bayern im Bundesrat nicht hatte durchsetzen können. Sie lautet wie folgt:

§ 126a StGB-E [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 schwererer 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 beruflichen Handlungen der in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Personen.

2. Gemeinsamkeiten und Unterschiede der Entwürfe

Beiden Entwürfen ist neben § 126a StGB als Regelungsstandort gemeinsam, dass sie sich inhaltlich auf internetbasierte Leistungen beziehen. Mit dem Begriff der „Leistung“ sollen denkbar weit alle Angebote bezeichnet werden, die sich an einen oder mehrere Nutzer richten, ohne auf Dauer und wiederholte Nutzung abzuzielen.[37] Das Adjektiv „internetbasiert“ soll technikbezogen auszulegen sein und alle Dienste erfassen, die auf der Netzwerkschicht des OSI (Open Systems Interconnection)-Referenzmodells über das Internetprotokoll (IP) vermittelt werden.[38] Erfasst werden damit nicht nur Dienste, die über das World Wide Web oder per E-Mail erbracht werden, sondern z.B. auch Voice-over-IP Dienste wie Skype, Facetime oder Whatsapp. Allerdings muss der Zweck oder die Tätigkeit der internetbasierten Leistung darauf ausgerichtet sein, die Begehung rechtswidriger Taten zu ermöglichen oder zu fördern. Zudem enthalten beide Entwürfe in Absatz 1 eine formelle Subsidiaritätsklausel. Danach kommt eine Strafbarkeit nach § 126a StGB nur in Betracht, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist. Nach dem jeweiligen Absatz 2 darf die Strafe nach § 126a StGB im Übrigen nicht schwerer sein, als die für die ermöglichte oder geförderte (Haupt-)Tat.

Vergleicht man beide Textfassungen, so fallen aber auch *gravierende Unterschiede* ins Auge. Während der Bundesratsentwurf als Tathandlung das „Anbieten“ internetbasierter Leistungen kriminalisieren will, knüpft der Referentenentwurf an den Begriff des „Zugänglichmachens“ an. Nur der Bundesratsentwurf formuliert auch tatsächlich einen „Darknet-Paragrafen“.[39] Demgegenüber verzichtet der Referentenentwurf gerade auf die Einschränkung, wonach der Zugang und die Erreichbarkeit der internetbasierten Leistung „durch besondere technische Vorkehrun-

[37] BT-Drs. 19/9508, S. 13.
[38] RefE, S. 80.
[39] Vgl. *Oehmichen/Weißenberger* KriPoZ 2019, 174 (176).

gen beschränkt" sein muss. Zusätzlich zum Bundesratsentwurf erfasst die Formulierung des Referentenentwurfs über das Fördern und Ermöglichen hinaus auch internetbasierte Leistungen, die darauf ausgerichtet sind, die Begehung von rechtswidrigen Taten zu „erleichtern". Während der Bundesratsentwurf an einen vergleichsweise überschaubaren Katalog typischer Darknet-Straftaten anknüpft, verzichtet der Referentenentwurf auf jede Einschränkung und lässt die Ausrichtung auf die Ermöglichung, Förderung oder Erleichterung *jeder denkbaren rechtswidrigen Tat* i.S. von § 11 Abs. 1 Nr. 5 StGB genügen. Auf diese Weise will das Bundesinnenministerium u.a. auch Plattformen erfassen, die auf die Begehung von Äußerungsdelikten oder die Vermittlung von Auftragsmördern gerichtet sind.[40] Im Vergleich zum Bundesratsentwurf, der im Grundtatbestand als Sanktion Freiheitsstrafe bis zu drei Jahren oder Geldstrafe vorsieht, soll nach dem Referentenentwurf die Strafobergrenze zudem erst bei fünf Jahren Freiheitsstrafe gezogen werden. Während in § 126a Abs. 3 des Bundesratsentwurfs nur die *gewerbsmäßige Tatbegehung* zu einer Qualifikation mit einem Strafrahmen von sechs Monaten bis 10 Jahren Freiheitsstrafe führt, soll dies nach der Formulierung des Referentenentwurfs zusätzlich auch bei der *bandenmäßigen Begehung* der Fall sein. Andererseits sieht lediglich der Referentenentwurf in Absatz 4 für die dort genannten Fälle einen Tatbestandsausschluss vor. Umgekehrt findet sich nur im Bundesratsentwurf eine Ergänzung des Katalogs von § 5 StGB um eine neue Nr. 10b, wonach deutsches Strafrecht unabhängig vom Recht des Tatorts auch auf solche Fallkonstellationen Anwendung finden soll, in denen die Leistung des Portalbetreibers zwar im Ausland angeboten wird, diese aber einen besonderen Inlandsbezug dadurch aufweist, dass sie sich auf die Ermöglichung von rechtswidrigen Taten im Inland bezieht.[41]

3. Bewertung

a) Regelungszweck

Eine erste (verfassungsrechtliche) Bewertung fällt angesichts der divergierenden Regelungskonzepte nicht leicht. Klar ist: Die einschlägigen Handelsplattformen bieten einen niedrigschwelligen Zugriff auf logistische Infrastrukturen für die Begehung von Straftaten auch für Personen, die *herkömmliche Beschaffungswege* für Waffen, Betäubungsmittel oder kriminelle Dienstleistungen nicht beschreiten.[42] Mit ihrer Hilfe werden somit neue Kundenkreise erschlossen, die bislang keinen Zugang zu solchen Waren und Dienstleistungen hatten. Allerdings ist schon das hierfür bemühte Rechtsgut der „öffentlichen Sicherheit und der staatlichen Ordnung"[43] denkbar weit und damit unbestimmt. Wie etwa die parallele Diskussion zur Bestimmung des Schutzgutes der §§ 129 ff. StGB zeigt, verbergen sich hinter solchen wenig aussagekräftigen Kollektivrechtsgütern in Wirklichkeit immer die im Besonderen Teil des StGB und den strafrechtlichen Nebengesetzen geschützten Individualrechtsgüter wie z.B. Leben, körperliche Unversehrtheit, Vermögen, Eigentum oder Freiheit.[44] Um den durch das Betreiben illegaler Handelsplattformen hierfür folgenden Gefahren entgegenzuwirken, erscheint es durchaus als legitimes Mittel, das öffentliche Feilbieten von Gegenständen und Dienstleistungen zur Vorbereitung von Straftaten im Internet durch eine eigenständige Strafdrohung zu unterbinden.[45] Von diesem Zweck entfernt man sich allerdings erheblich, wenn man – wie im Referentenentwurf – nicht nur auf den Darknet-Bezug, sondern auch auf einen internetbezogenen Straftatenkatalog verzichtet. Als Begründung hierfür wird angeführt, man wolle nicht die Dreistigkeit des unverdeckt Handelnden belohnen.[46] Allerdings würden damit auch Fahrlässigkeitsdelikte erfasst, zu denen weder Anstiftung noch Beihilfe möglich ist.[47] Zudem fiele auch derjenige in den Anwendungsbereich von § 126a StGB, der im Internet lediglich Angebote zur Verwirklichung von *Bagatellstraftaten*, z.B. Mustertexte für Beleidigungsdelikte oder Phishing-Mails, unterbreitet.

b) Bestimmtheit

Beide Entwurfsfassungen werfen auch unter dem Blickwinkel *ausreichender Gesetzesbestimmtheit* Fragen auf. Problematisch erscheint insoweit vor allem das Kriterium der *Zweckrichtung* der internetbasierten Leistungen zur Ermöglichung, Förderung oder Erleichterung der Begehung rechtswidriger Taten. Mithilfe dieses Merkmals sollen die *tatbestandlich erfassten* Leistungen von den *nicht strafwürdigen* Angeboten abgegrenzt werden.[48] Es zieht also die Grenze zwischen Strafbarkeit und Straflosigkeit. Die Begründung beider Entwürfe gesteht aber offen zu, dass die Prüfung der Ausrichtung einer Online-Plattform stets anhand des konkreten Einzelfalls zu erfolgen habe und allgemein verbindlichen Kriterien nicht zugänglich sei. Als mögliche Indizien werden das tatsächliche Angebot der Plattform, der dortige Umgang mit Hinweisen auf Handel mit illegalen Waren und Dienstleistungen oder etwa auch Vorgaben in Allgemeinen Geschäftsbedingungen genannt.[49] Nicht immer werden die Plattformbetreiber aber so strafverfolgungsfreundlich sein und ihrem Forum einen so eindeutigen Namen geben wie z.B. die Betreiber der zwischenzeitlich abgeschalteten Seite „crimenetwork", bei der der Name zugleich Programm war. Zudem können und werden AGBs von Handelsplattformen im Darknet häufig nur auf dem (virtuellen) Papier bestehen.[50] Infolgedessen wird die Gesetzeskonkretisierung weitgehend dem Anwender überlassen.[51]

c) Verhältnismäßigkeit

Auch ein neuer § 126a StGB muss schließlich den Anforderungen des *Verhältnismäßigkeitsgrundsatzes* genügen.

---

40 RefE, S. 81.
41 BT-Drs. 19/9508, S. 12.
42 BT-Drs. 19/9508, S. 10; RefE, S. 78.
43 Vgl. RefE, S. 78.
44 Näher hierzu nur *Zöller*, Terrorismusstrafrecht – Ein Handbuch, 2009, S. 513 ff. m.w.N.
45 Vgl. BT-Drs. 19/9508, S. 2.
46 RefE, S. 79.
47 *Oehmichen/Weißenberger*, KriPoZ 2019, 174 (178).
48 Vgl. BT-Drs. 19/9508, S. 13.
49 BT-Drs. 19/9508, S. 13; RefE, S. 80 f.
50 Krit. auch *Oehmichen/Weißenberger*, KriPoZ 2019, 174 (178).
51 *Kubiciel/Mennemann*, jurisPR-StrafR 8/2019 Anm. 1 III. 2.

Insofern stellt sich bereits die Frage nach der *Erforderlichkeit*. Beide Entwürfe verweisen hierzu letztlich nur auf angebliche *Nachweisprobleme* im Rahmen einschlägiger Strafverfahren, ohne tatsächlich bestehende Strafbarkeitslücken aufzudecken.[52] Die Voraussetzungen einer *Beihilfe* (§ 27 StGB) zu den über die Plattform begangenen Straftaten seien oft nicht nachweisbar, da die Haupttaten bilateral zwischen den Beteiligten über verschlüsselte Kommunikationskanäle und vollautomatisierte Verkaufssysteme abgewickelt würden.[53] Zudem hätten die Plattformbetreiber häufig keine Kenntnisse von den Details der über ihren Dienst abgewickelten Geschäfte. Eine Zurechnung von Einzeltaten unter dem Gesichtspunkt einer *bandenmäßigen Tatbegehung* sei häufig nicht möglich, da die Führungsebene solcher Foren und Marktplätze häufig nur aus ein oder zwei Personen bestehe.[54] Und schließlich würden auch *Organisationsdelikte* wie § 129 StGB nicht weiterhelfen, da diese auf moderne, internetbasierte Beteiligungsstrukturen nicht übertragbar seien und sich die für den Tatbestand erforderliche Festigkeit der Struktur nicht nachweisen lasse.[55]

Diese Argumentation vermag im Ergebnis nicht zu überzeugen. Die These vom Bestehen nicht hinnehmbarer Strafbarkeitslücken wird schon durch die Realität der bislang geführten Strafverfahren weitgehend entkräftet, in denen man den Betreibern einschlägiger Plattformen gerade erfolgreich auch den Vorwurf der Beihilfe zu dort verwirklichten Haupttaten gemacht hat.[56] Zwar handelt es sich beim Erstellen, der Inbetriebnahme sowie der Aufrechterhaltung einer Diskussionsplattform im Darknet für sich genommen noch nicht um eine strafbare Beihilfehandlung i.S. des § 27 StGB.[57] Speziell für den subjektiven Tatbestand des Gehilfen sind die Bestimmtheitsanforderungen aber stark gelockert. Sein Vorsatz muss sich auf die Ausführung einer zwar nicht in allen Einzelheiten, wohl aber in ihren wesentlichen Merkmalen oder Grundzügen, insbesondere in ihrer Unrechts- und Angriffsrichtung konkretisierten Tat beziehen.[58] Für die Beihilfe genügt es mithin, dass der Gehilfe die Haupttat nur in ihren wesentlichen Merkmalen kennt. Das aber liegt auf der Hand, wenn er nach dem Vorbild *legaler* Verkaufsplattformen wie Amazon oder Ebay auch in seinem Darknet-Forum kundenfreundlich separate Kategorien für das Angebot evident illegaler Waren und Dienstleistungen erstellt.[59] Rein äußerlich unterscheiden sich die meisten Plattformen häufig kaum von den bekannten legalen Verkaufsplattformen im Visible Net. Auch illegale Waren und Dienstleistungen im Darknet sind regelmäßig nach Rubriken geordnet, ermöglichen es, Werbung zu schalten, bieten Treuhandmodelle[60] für die Abwicklung der Verkäufe und sogar Bewertungssysteme für Käufer und Verkäufer.[61] Vor allem aber leuchtet nicht ein, warum in einem neuen § 126a StGB eine zur Täterschaft hochgestufte Beihilfehandlung leichter nachweisbar sein soll, als etwa die klassische Beihilfe zu einem Waffen- oder Betäubungsmitteldelikt.[62] Hinzu kommt, dass sich das Betreiben von illegalen Handelsplattformen für Drogen häufig sogar schon als täterschaftliche Begehungsweise der nach dem BtMG einschlägigen Straftatbestände darstellt. So stellt etwa § 29 Abs. 1 S. 1 Nr. 8 BtMG die Werbung für Betäubungsmittel entgegen § 14 Abs. 5 BtMG unter Strafe. Unter einer solchen Werbung ist der an Dritte gerichtete Hinweis auf die Bereitschaft des Werbenden zu verstehen, Betäubungsmittel zu liefern.[63] Sofern es im Zusammenhang mit der Gestaltung der Handelsplattform an einem Hinweis auf eigene Liefermöglichkeiten fehlt, kommt eine täterschaftliche Begehung von § 29 Abs. 1 S. 1 Nr. 10 BtMG in Betracht, der es unter Strafe stellt, einem anderen eine Gelegenheit zum unbefugten Erwerb oder zur unbefugten Abgabe von Betäubungsmitteln zu verschaffen oder zu gewähren, eine solche Gelegenheit öffentlich oder eigennützig mitzuteilen oder einen anderen zum unbefugten Verbrauch von Betäubungsmitteln zu verleiten. Zudem kann sogar ein Handeltreiben nach § 29 Abs. 1 S. 1 Nr. 1 BtMG in Betracht kommen, sofern der Plattformbetreiber Provisionen oder Kommissionen für die mit seiner Hilfe getätigten Geschäfte erhält.[64] Und was eine Strafbarkeit wegen einer Beteiligung an einer kriminellen Vereinigung nach § 129 StGB anbelangt, so sei nur darauf hingewiesen, dass der Vereinigungsbegriff durch das 54. Gesetz zur Änderung des Strafgesetzbuchs vom 17. Juli 2017[65] in Umsetzung europäischer Vorgaben erweitert worden ist. Damit wurden zugleich die Anforderungen an den Nachweis des *organisatorischen Elements* einer Vereinigung erheblich herabgesetzt.[66] Die angeblichen Nachweisschwierigkeiten in den beiden Entwurfsbegründungen sind daher durch nichts näher belegt.

Der *Nutzen* einer solchen Strafnorm könnte daher – wie so häufig – auf einer *ganz anderen Ebene* gewollt sein. Mit

---

52 Vgl. *Oehmichen/Weißenberger* KriPoZ 2019, 174 (177); für das Bestehen von Strafbarkeitslücken demgegenüber *Fünfsinn/Krause*, FS Eisenberg, 2019, S. 641 (645 ff.).

53 BT-Drs. 19/9508, S. 9 f.; RefE, S. 77.

54 BT-Drs. 19/9508, S. 10; RefE, S. 77.

55 Vgl. BT-Drs. 19/9508, S. 10; RefE, S. 78.

56 S. nur *LG Karlsruhe*, StV 2019, 400 (401), das den Betreiber des Forums „Deutschland im Deep Web" im Zusammenhang mit dem sog. „Amoklauf von München" wegen Beihilfe zum vorsätzlichen unerlaubten Handeltreiben mit Waffen und Munition in Tateinheit mit fahrlässiger Tötung in 9 Fällen in Tateinheit mit fahrlässiger Körperverletzung in 5 Fällen und des unerlaubten Erwerbs der Waffe und Munition nach §§ 2 Abs. 2, 21 Abs. 1 S. 1, 52 Abs. 1 Nr. 2 lit. c WaffG, Anlage 2 Abschnitt 2 Unterabschnitt 1 S. 1 zum WaffG, §§ 222, 229, 230, 52 StGB verurteilt hat. Ausführlich zur Begründung der Beihilfestrafbarkeit *Greco*, ZIS 2019, 435 (441 ff.); zur – regelmäßig fehlenden – Haftungsbeschränkung nach den §§ 7 ff. TMG *Fünfsinn/Krause*, FS Eisenberg, 2019, S. 641 (645) sowie *Greco*, ZIS 2019, 435 (447 f.).

57 *LG Karlsruhe*, StV 2019, 400 f.

58 *BGH*, NStZ 2011, 399 (400); *LG Karlsruhe*, StV 2019, 400 (402); *Rengier*, AT, 11. Aufl. (2019), § 45 Rn. 115.

59 So auch *Kubiciel/Mennemann*, jurisPR-StrafR 8/2019 Anm. 1 IV.

60 Hierzu *Tzanetakis*, APuZ 2017, 41 (45 f.).

61 *Rath*, DRiZ 2016, 292 (293); *Fiebig*, DRiZ 2019, 50.

62 Zweifelnd auch *Oehmichen/Weißenberger*, KriPoZ 2019, 174 (178).

63 *Patzak*, in: Körner/Patzak/Volkmer, Betäubungsmittelgesetz, 9. Aufl. (2019), § 29 Teil 18 Rn. 7.

64 *Kubiciel/Mennemann*, jurisPR-StrafR 8/2019 Anm. 1 IV.; vgl. auch *Greco*, ZIS 2019, 435 ff., der zudem auf die Möglichkeit einer Geldwäschestrafbarkeit nach § 261 StGB verweist.

65 BGBl. I S. 2440.

66 Näher hierzu *Zöller*, KriPoZ 2017, 26 ff.

der eigenständigen Kriminalisierung des bloßen Anbietens oder Zugänglichmachens von internetbasierten Leistungen wird die Strafbarkeit auf einen Zeitpunkt vorverlagert, in dem lediglich die Infrastruktur für *andere*, noch in der Zukunft liegende *Straftaten* geschaffen wird. Der geplante § 126a StGB ist nach der bisherigen Konzeption ein *abstraktes Gefährdungsdelikt* und ein typischer *Vorfeldtatbestand*. Nach beiden Entwurfsfassungen soll jedenfalls die Qualifikation nach Absatz 3 Anlasstat für Telekommunikationsüberwachungsmaßnahmen nach § 100a StPO werden. Der Referentenentwurf will die Qualifikation des § 126a Abs. 3 StGB-E sogar in den Straftatenkatalog der Online-Durchsuchung nach § 100b StPO und der Vorratsdatenspeicherung nach § 100g StPO aufnehmen. Man will also deshalb auf dem Gebiet des *materiellen Strafrechts* in das zeitliche Vorfeld von Internetkriminalität eindringen, um *Strafverfolgungsmaßnahmen* früher beginnen lassen zu können. Diese Idee dürfte sich in der Praxis als zirkelschlüssig erweisen. Schließlich wurde bereits eingangs darauf hingewiesen, dass jedenfalls klassische Telekommunikationsüberwachungsmaßnahmen im anonymen Darknet meist nicht weiterführen. Letztlich vermögen auch inkonsistente Regelungen zum *Tatbestandsauschluss* wie § 126a Abs. 4 Nr. 1 des Referentenentwurfs das Gesamtgefüge nicht entscheidend *zugunsten* einer Einstufung als *angemessene Vorschrift* zu beeinflussen. Wenn bei einer internetbasierten Leistung die Ausrichtung auf die Begehung von Straftaten nur von *untergeordneter Bedeutung* ist, wird es regelmäßig auch *nicht Zweck* dieser Leistung sein, die Begehung von Straftaten zu ermöglichen, zu fördern oder zu erleichtern.[67]

IV. Fazit

Nach alledem zeigt sich, dass die bislang auf dem Tisch liegenden Konzepte zur Kriminalisierung der Betreiber von internetbasierten Plattformen für illegale Waren und Dienstleistungen zwar ein wichtiges gesellschaftliches und rechtspolitisches Anliegen verfolgen. Der materiell-strafrechtliche Ansatz in Gestalt der Einführung eines neuen § 126a StGB ist aber weder das Licht am Ende des Darknets noch der Weisheit letzter Schluss. Er ist mit einer Reihe von Unsicherheiten und Widersprüchlichkeiten behaftet und vermag es nicht, das Bestehen von echten Strafbarkeitslücken überzeugend darzulegen. Vielleicht sollte der Blick des Gesetzgebers stattdessen in das *Strafprozessrecht* gehen. Ein erster Schritt könnten *neue strafprozessuale Befugnisse*, etwa spezialgesetzliche Vorschriften für Ermittlungen im Internet jenseits der allgemeinen Vorschriften über den Einsatz Verdeckter Ermittler nach §§ 110a ff. StPO oder zum Zugriff auf bereits bestehende Benutzerkonten und Zugangsdaten sein, die aber ihrerseits den Rahmen des Verfassungsmäßigen zu wahren haben.[68] Zumindest im Bereich des materiellen Strafrechts besteht aktuell kein dringender gesetzgeberischer Handlungsbedarf.[69]

---

[67] Treffend bemerkt von *Oehmichen/Weißenberger*, KriPoZ 2019, 174 (178).

[68] Diese Voraussetzungen erfüllt der ebenfalls im Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat v. 23.3.2019 enthaltene Vorschlag eines neuen § 163g StPO-E zum staatlichen Zugriff auf Benutzerkonten erkennbar nicht; vgl. dazu *Oehmichen/Weißenberger*, KriPoZ 2019, 174 (180 f.).

[69] Zweifel an der Erforderlichkeit eines neuen § 126a StGB äußern auch *Kubiciel/Mennemann*, jurisPR-StrafR 8/2019 Anm. 1 IV sowie *Greco*, ZIS 2019, 435 (448).