Universität Augsburg University

Lehrstuhl für Deutsches, Europäisches und Internationales
Straf- und Strafprozessrecht, Medizin- und Wirtschaftsstrafrecht

AUGSBURGER PAPIERE ZUR KRIMINALPOLITIK –

AUGSBURG PAPERS ON CRIMINAL LAW POLICY

Michael Kubiciel (Hrsg.)

Kriminalisierung internetbasierter Handelsplattformen im Darknet und Surface-Web

Michael Kubiciel

Augsburger Papier zur Kriminalpolitik 1/2019

Lehrstuhl für Deutsches, Europäisches und Internationales Straf- und Strafprozessrecht,
Medizin- und Wirtschaftsstrafrecht
Prof. Dr. Michael Kubiciel
Universität Augsburg
Universitätsstr. 24
86159 Augsburg
michael.kubiciel@jura.uni-augsburg.de

Kriminalisierung internetbasierter Handelsplattformen im Darknet und Surface-Web[*]

Michael Kubiciel

I. Hintergrund

Der von Politikern oft zu vernehmende Satz, dass das Internet kein rechtsfreier Raum sei,[1] wird in der öffentlichen und politischen Diskussion seit dem Amoklauf im Olympia-Einkaufszentrum in München vor allem auf das sog. Darknet bezogen. Gemeint ist damit jener Teil des Internets, der durch Peer-to-peer-Verbindungen (P2P) zwischen Nutzern geschaffen wird und daher nicht allgemein zugänglich ist. Nicht selten erfordert der Zugang zu solchen Netzen eine Einladung eines Nutzers und eine Bestätigung durch eine Art Administrator. Zudem wird der Datenverkehr zwischen den Nutzern oft verschlüsselt, etwa mit Hilfe des Tor-Browsers, so dass Identität, Herkunft oder IP-Adressen in der Regel nicht oder nur unter großem Aufwand ermittelt werden können. Derartige Netzwerke stellen Dual-Use-Produkte dar,[2] da digitale Strukturen und die sie nutzende Technik sowohl zu legalen als auch illegalen Zwecken verwendet werden können.[3] So ermöglicht es der Tor-Browser den Bürgern autoritärer Staaten, vergleichsweise anonym zu kommunizieren sowie Sperren für den Zugriff auf bestimmte Internetseiten zu umgehen, d.h. ein unzensiertes Internet zu nutzen.

Die arkane Struktur der P2P-Kommunikation und die schwierige Identifizierung der Nutzer macht das Darknet aber auch für Straftäter attraktiv: So finden sich dort auch illegale Angebote, u.a. von gestohlenen Daten, Schadprogramme, Kinderpornographie, Drogen und Waffen und anderem mehr. Derartiges wird häufig auf Plattformen, die vom Aufbau her eBay oder Amazon ähneln, oder in Diskussionsforen offeriert. Die Plattform- bzw. Forenbetreiber sind meist nicht direkt an am Handel beteiligt, wissen aber zumeist vom Gegenstand der Transak-

[*] Für Mitarbeit an einem ersten Entwurf bin ich Herrn Wiss. Mit. Malte Mennemann zu Dank verpflichtet.

[1] Zu diesem oft floskelhaft verwendeten Satz *Kubiciel*, ZIS 2018, 60, 63.

[2] Am Beispiel einer File-Sharing-Software *Kubiciel*, wistra 2012, 453 ff.

[3] *Aliens*, Researchers Claim the Darknet Has More Legal Sites Than Illegal Ones, online abrufbar unter: https://www.deepdotweb.com/2016/11/09/researchers-claim-darknet-legal-sites-illegal-ones/, zuletzt abgerufen am 28.3.2019. Siehe auch RefE IT-Sicherheitsgesetz 2.0, S. 76 f.

tionen, zumal sie spezielle Kategorien für Drogen(arten) oder Waffen(arten) einrichten. Teilweise erhalten sie sogar Provisionen für die Abwicklung der Geschäfte; im Übrigen finanzieren sich die Betreiber durch Werbung.[4]

II. Zwei Gesetzentwürfe

In naher Zukunft dürfte das Betreiben solcher Plattformen unter Strafe stehen.[5] Schon der Koalitionsvertrag hatte Anfang 2018 Strafvorschriften gegen „kriminelle Infrastrukturen" im Netz, insbesondere gegen Darknet-Handelsplätze, angekündigt.[6] Aus dieser Initiative sind zwei Entwürfe hervorgegangen, die im Folgenden vorgestellt werden.

1. Ursprünglicher Gesetzentwurf des Bundesrates: Fokussierung des Darknets

Im Januar 2019 haben die Länder Nordrhein-Westfalen und Hessen einen Gesetzantrag zur Kriminalisierung von Internethandelsplattformen mit illegalen Angeboten in den Bundesrat eingebracht,[7] den dieser im März 2019 in erheblich abgewandelter Form als Gesetzentwurf verabschiedet hat.[8] Nach der ursprünglichen Fassung des § 126a Abs. 1 StGB-E sollte sich strafbar machen, wer Dritten eine „internetbasierte Leistung" zugänglich macht, deren Zugang und Erreichbarkeit durch besondere technische Vorkehrungen beschränkt und deren Zweck oder Tätigkeit darauf ausgerichtet ist, die Begehung von in Abs. 2 näher bestimmten rechtswidrigen Taten zu ermöglichen, zu fördern oder zu erleichtern. § 126a StGB-E enthält eine Liste von Straftaten des Betäubungsmittel-, Arznei- und Waffenrechts und nennt überdies die §§ 146, 147, 149, 152a, 152b, 184b Abs. 1, 202a, 202b, 202c, 263a, 275, 276, 303a und 303b StGB. Dabei soll es sich um für das geschützte Rechtsgut besonders gefährliche „szenetypische" Delikte handeln.[9]

[4] *Fünfsinn/Krause*, FS Eisenberg, 2019, S. 641, 644.
[5] Dazu bereits *Fünfsinn/Krause*, FS Eisenberg, S. 641 ff.
[6] Siehe Koalitionsvertrag zwischen CDU, CSU und SPD 19. Legislaturperiode, Rn. 6006-6009; dazu *Kubiciel*, FAZ Einspruch v. 7.2.2018.
[7] Entwurf eines Strafrechtsänderungsgesetzes v. 18.1.2019, BR-Drs. 33/19. Kritisch dazu *Bäcker/Golla*, Verfassungsblog v. 21.3.2019, abrufbar unter: https://verfassungsblog.de/strafrecht-in-der-finsternis-zu-dem-vorhaben-eines-darknet-tatbestands/.
[8] BR-Drs. 33/19 v. 15.3.2019 (Beschluss). S. Beschlussempfehlung v. 1.3.2019, BR-Drs. 33/1/19.
[9] BR-Drs 33/19 (Beschluss), Anlage S. 13.

2. Deutliche Erweiterung

Durch eine Beschlussempfehlung ist dieser Entwurf kurz vor der Verabschiedung durch den Bundesrat erheblich ausgeweitet worden, indem der Darknet-Bezug gestrichen und die Begrenzung auf einen Kreis bestimmter illegaler Angebote aufgegeben wird.[10] Der Entwurf des Bundesministeriums des Innern, für Bau und Heimat eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (im Folgenden: REfE IT-Sicherheitsgesetz 2.0) greift diesen weiten Ansatz auf.[11]

Daher bezieht sich der RefE IT-Sicherheitsgesetz 2.0 (wie das schlussendlich vom Bundesrat verabschiedete Gesetz) nicht auf konkretisierte Straftaten, sondern begnügt sich mit dem Verweis auf „rechtswidrige Taten", verfolgt also einen „all-crime-approach". Eine Einschränkung auf nur bestimmte Delikte sei aus Gründen der Verhältnismäßigkeit nicht erforderlich und überdies nicht sachgerecht, da ein begrenzter Katalog von Straftaten Gefahr liefe, unvollständig zu bleiben. Zudem sei die Zugänglichmachung jedes internetbasierten Angebots, das auf die Begehung jeglicher Straftaten gerichtet ist, gleichermaßen strafwürdig.[12] Zudem erfasst der RefE IT-Sicherheitsgesetz 2.0 (wie die finale Gesetzesfassung des Bundesrates) auch internetbasierte Leistungen, deren Zugang oder Erreichbarkeit *nicht* durch besondere technische Vorkehrungen gesichert oder beschränkt ist. Er gilt daher nicht nur für Handelsplattformen im Darknet, sondern auch für solche im frei zugänglichen Netz. Der Anwendungsbereich ist damit erheblich weiter gefasst, was weitreichende Folgen hat (siehe unten II. 3).[13] Begründet wird diese massive Ausweitung mit der Erwägung, man wolle nicht die Dreistigkeit des „unverdeckt Handelnden" belohnen.[14]

Auch die Verfasser des RefE IT-Sicherheitsgesetzes 2.0 halten – wie der Bundesrat – § 126a StGB-E für notwendig, um Strafbarkeitslücken zu schließen. Der Nachweis der objektiven und vor allem subjektiven Voraussetzungen einer Beihilfe falle bei internetbezogenen, häufig

[10] Beschlussempfehlung v. 1.3.2019, BR-Drs. 33/1/19. Kritisch dazu *Rückert*, LTO v. 15.3.2019, abrufbar unter: https://www.lto.de/recht/hintergruende/h/bundesrat-strafrecht-fuer-darknet-strafbarkeitsluecke-kriminalisierung.

[11] Der Regierungsentwurf ist Ende März in die Ressortabstimmung gegeben worden, zwischenzeitlich aber auf diversen Internet-Seiten verbreitet worden, s. nur https://www.datenschutz-notizen.de/it-sicherheitsgesetz-2-0-massive-ausweitung-3122420/.

[12] RefE IT-Sicherheitsgesetz 2.0, S. 78.

[13] Der Koalitionsvertrag (Fn. 6) lässt diese weite Fassung zu, da dort das Darknet nur als Beispiel genannt wird, im Übrigen aber allgemein vom Internet die Rede ist.

[14] RefE IT-Sicherheitsgesetz 2.0, S. 79.

transnationalen Sachverhalten schwer, die Voraussetzungen der Bildung einer kriminellen Vereinigung oder einer Bande lägen häufig nicht vor.[15] Ungeachtet dessen erfasse „die strafrechtliche Ahndung unter dem Gesichtspunkt der Beihilfe in der Regel nicht hinreichend den aktiven Charakter der Tathandlung, die die Grundlagen der Underground-Economy schafft."[16]

II. Inhalt im Einzelnen

1. Internetbasierte Leistung

Der Gesetzentwurf des Bundesrats und der RefE IT-Sicherheitsgesetz 2.0 beziehen sich auf sog. internetbasierte Leistungen. Der Begriff ist sehr weit und zudem hochgradig unbestimmt. Als „internetbasiert" sollen sämtliche Dienste zu verstehen sein, die auf der Netzwerkschicht des OSI-Referenzmodells über das Internet-Protokoll (IP) vermittelt werden; Leistung seien „alle Angebote, die sich an einen oder mehrere Nutzer richten, ohne stets auf Dauer und wiederholte Nutzung abzuzielen."[17] Im Bestreben, die Tatbestandsfassung möglichst entwicklungsoffen zu halten und nicht an existierende Netzwerkmodelle zu koppeln, haben die Entwurfsverfasser eine Vorschrift verfasst, die jede Form internetgestützten Austausches erfasst. Nicht minder weit ist die Tatbestandshandlung des Zugänglichmachens. Letzteres erfordert nämlich kein Handeln im virtuelle Raum, sondern jede Form der Ermöglichung der Wahrnehmung[18] und damit auch das Bereitstellen eines Büros oder PCs, mittels dessen über das Internet ein Angebot an eine andere Person gerichtet wird. Diese extrem weite Fassung des Tatbestandes lässt nicht nur an der hinreichenden Bestimmtheit (Art. 103 Abs. 2 GG) zweifeln, sondern wirft auch die Frage auf, ob ein derart weitreichendes Verbot noch verhältnismäßig ist.

2. Zwecksetzung

Für eine Eingrenzung der Verbotszone ist daher nach beiden Fassungen die subjektive Zweckrichtung entscheidend: Der Zweck oder die Tätigkeit der internetbasierten Leistung muss darauf ausgerichtet sein, rechtswidrige Taten zu ermöglichen oder zu fördern. Von besonderer Bedeutung ist diese Wendung für den vom Bundesrat verabschiedeten Tatbestand sowie für

[15] BR-Drs. 33/19 (Beschluss), Anlage S. 5 f.; RefE IT-Sicherheitsgesetz 2.0, S. 77 f.
[16] RefE IT-Sicherheitsgesetz 2.0, S. 77.
[17] RefE IT-Sicherheitsgesetz 2.0, S. 80. S. auch BR-Drs. 33/19, S. 8, der allerdings „internetbasiert" nicht definiert.
[18] RefE IT-Sicherheitsgesetz 2.0, S. 80.

die Fassung des RefE IT-Sicherheitsgesetzes 2.0, da diese – anders als der Entwurf von Hessen und NRW – nicht nur das Darknet, sondern das gesamte Internet erfasst, inklusive Sozialer Medien wie Facebook und Handelsplattformen wie Ebay oder Amazon.

Wann eine internetbasierte Leistung nach ihrer Zweckrichtung bzw. Art der Tätigkeit darauf ausgerichtet ist, rechtswidrige Taten zu ermöglichen oder zu erleichtern, verrät die Begründung nicht. Vielmehr heißt es: „Die Prüfung der Ausrichtung einer Online-Plattform hat anhand des konkreten Einzelfalls zu erfolgen und ist allgemein verbindlichen Kriterien nicht zugänglich."[19] Damit wird die Gesetzeskonkretisierung von vornherein dem Anwender überlassen. Dies erleichtert es Staatsanwaltschaften und Gerichten, aus äußeren Indizien (illegaler Handel) auf die Zweckrichtung zu schließen. Für (potenziell) Beschuldigte ist es hingegen in Grenzbereichen schwierig, das Risiko einer eigenen Strafbarkeit vorherzusehen und ein Strafbarkeitsrisiko zu vermeiden. Im Ergebnis führt das dazu, dass Betreiber von Internetplattformen den Traffic auf ihren Plattformen, insbesondere die Art des Handels, der auf ihren Plattformen betrieben wird, deutlich stärker als bislang überprüfen müssen.[20] Damit wird ein (verkapptes) Unterlassungsdelikt geschaffen: Wer – auch außerhalb des Darknets – Dritten internetbasierte Leistungen zugänglich macht, muss das Handeln bzw. den Handel dieser Dritten überwachen und notfalls den Zugang sperren, wenn er nicht Gefahr laufen will, sich nach § 126a StGB-E strafbar zu machen. Nach allgemeinen Grundsätzen kann ein Unterlassen aber nur dann Straffolgen nach sich ziehen, wenn der Normadressat die Pflicht hat, zu handeln und einen schädigenden Erfolg abzuwenden (vgl. § 13 StGB). Eine solche Überwachungs- und Löschpflicht kennt das Recht für „Durchleiter" von Traffic aber gerade nicht (vgl. § 7 Abs. 2 TMG).

III. Bewertung

Die Gesetzentwürfe des Bundesrates und des Bundesinnenministeriums sehen eine Strafbarkeitslücke von Plattformbetreibern und versuchen diese zu schließen, indem in unbestimmter Weise das „Zugänglichmachen internetbasierter Leistungen" pönalisiert wird. Dabei ist schon zweifelhaft, ob die behaupteten Strafbarkeitslücken tatsächlich in diesem Ausmaß existieren.

[19] RefE IT-Sicherheitsgesetz 2.0, S. 80; BR-Drs. 33/19 (Beschluss), Anlage S. 8.
[20] Vgl. schon *Rückert*, LTO v. 15.3.2019: Dienstanbieter seien nun „durch die Hintertür" verpflichtet, aktiv nach illegalen Inhalten zu fahnden, um eigene Strafbarkeitsrisiken zu minimieren.

So ist der Nachweis einer Beihilfestraftat durchaus möglich. Denn die Betreiber von Darknet-Portalen und entsprechenden Foren erstellen häufig separate Kategorien für Drogen, Waffen und sonstigen Delikten. Dies indiziert einen Beihilfevorsatz, da der Gehilfe zwar die Haupttat in ihren wesentlichen Merkmalen kennen muss, nicht jedoch die Person des Haupttäters oder den genauen Tathergang, Ort, Zeit und Opfer.[21] Auf relevanten Deliktsfeldern dürften sich die Plattformbetreiber zudem nicht nur wegen Beihilfe strafbar machen: Erhalten die Betreiber, wie üblich, eine Provision der getätigten Verkäufe, so ist ein Handeltreiben bspw. nach § 29 Abs. 1 Nr. 1 BtMG erfüllt, welches als jedes eigennützige Bemühen definiert wird, das darauf gerichtet ist, den Umsatz von Betäubungsmitteln zu ermöglichen oder zu fördern.[22] Dies begründet Zweifel an der Erforderlichkeit des Tatbestandes.

Fragwürdig ist jedoch vor allem, ob der Tatbestand verhältnismäßig im engeren Sinne ist, da er nicht nur Betreiber von Darknet-Plattformen trifft, auf denen ausschließlich oder überwiegend illegaler Handel betrieben wird. Vielmehr implementiert er eine Art Dauerüberwachungspflicht für all jene eCommerce-Plattformen, Sozialen Medien und Einzelpersonen, die – legal – Dritten internetbasierte Leistungen zugänglich machen. In dieser Präventionswirkung liegt die eigentliche Pointe (und der vermutlich verfolgte Zweck) des Straftatbestandes. Im Ergebnis begründet der Tatbestand für die Internet-Industrie erhebliche Überwachungsplichten und Haftungsrisiken. Ob er hingegen ein wirksames Instrument gegen oft transnational agierende kriminelle Netzwerke ist, darf bezweifelt werden.

[21] *Joecks*, in: MüKo-StGB, 3. Aufl. 2017, § 27 Rn. 96; *Fünfsinn/Krause*, FS Eisenberg, 641, 646; *Ceffinato*, JuS 2017, 403, 408.
[22] BGH, Beschluss v. 21. November 2000, 1 StR 433/00, Rn. 5.