

Endlich Licht ins Darknet?

Christian Rückert

2020-12-16T12:03:00

Ein neuer Vorschlag zur Einführung einer eigenständigen Strafbarkeit für die Betreiber von Darknet-Marktplätzen liegt auf dem Tisch. Auch wenn sich das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) mit dem Entwurf bemüht zeigt, die Anregungen und Kritik vergangener Monate aufzunehmen, bleiben Notwendigkeit, Europarechtskonformität und Verfassungsmäßigkeit des Entwurfs zweifelhaft.

Geschichte eines Regulierungsversuches

Der neueste Teil in der Trilogie „Strafbarkeit des Betreibens von Darknet-Marktplätzen“ ist der am 27. November 2020 veröffentlichte [Entwurf des BMJV](#). Ihm vorangegangen sind aus dem vergangenen Jahr ein [Entwurf zum IT-Sicherheitsgesetz 2.0](#) des Bundesministeriums des Innern (BMI) sowie im April diesen Jahres ein [eigenständiger Entwurf des Bundesrates](#) – initiiert von Nordrhein-Westfalen –, die [von zahlreichen kritischen Stellungnahmen](#) von Strafrechtswissenschaftler/innen, Journalist/innen und Netzaktivist/innen begleitet waren.

Das vom Entwurf verfolgte Ziel ist ein drängendes. Der Handel mit illegalen Gütern und Dienstleistungen verlagert sich zunehmend in das Internet. Dies gilt vor allem für den [Drogen- und Waffenhandel](#), den Tausch von kinderpornographischem Material (*Rückert/Goger MMR 2020, 373*), das Angebot von Hacking-Dienstleistungen, sowie den [Handel mit Falschgeld](#). Besonderes mediales Interesse erlangte das Forum [„Deutschland im Deep Web“](#), weil der rechtsradikale Attentäter, der 2016 den Terroranschlag auf das Münchener Olympia-Einkaufszentrum verübte, den Verkäufer der Tatwaffe über dieses Forum kennenlernte.

Underground Economy und Kinderpornographie

Aktuell richten sich die gesetzgeberische und gesellschaftliche Aufmerksamkeit auf zwei Phänomene: Die „Underground Economy“ und der Tausch mit Kinderpornographie. „Underground Economy“ bezeichnet dabei den „Schwarzmarkt“-Handel im Internet, vor allem im sogenannten Darknet. Dort werden illegale Güter und Dienstleistungen gehandelt, man kann nahezu alles erwerben, was verboten ist. Bezahlt wird mit Kryptowährungen wie Bitcoin, der Versand erfolgt im Regelfall über Postdienstleister und nicht selten an Postpackstationen.

Die Plattformen werden unter anderem als sogenannte ‚Hidden Services‘ im Tor-Netzwerk angeboten. Die [Anonymisierungstechnologie des Tor-Netzwerks](#) verbirgt dabei nicht nur die IP-Adressen der Verkäufer/innen und Käufer/innen, sondern auch des Servers, auf dem die Datenverarbeitung der Plattform abläuft. Durch die

Bezahlung mit Kryptowährungen wird eine effektive Verfolgung der Zahlungsströme zwischen Verkäufer/in und Käufer/in erschwert – wenngleich nicht ausgeschlossen (siehe hierzu *Rückert* in Maume/Maute (Hrsg.) *Rechtshandbuch Kryptowerte*, § 23 Rn. 1 ff.). Viele der erfolgreichen Handelsplattformen arbeiten hochprofessionell (inklusive des Angebots von Treuhandservices und der Nutzung ausgeklügelter Provisionssysteme) und haben [Nutzerzahlen im sechsstelligen Bereich](#).

Andererseits hat auch die Kinderpornographie-Szene das Tor-Netzwerk für sich entdeckt. Dort wird das illegale Material in der Regel nicht verkauft, sondern zwischen den Nutzer/innen getauscht. Um Verdeckte Ermittler „draußen“ zu halten, arbeiten viele der Tauschforen mit sogenannten ‚Keuschheitsproben‘, bei denen Mitglieder selbst inkriminiertes Material zur Verfügung stellen müssen, um Zugang zu erhalten. Hier hat der Gesetzgeber vor Kurzem Abhilfe geschaffen, um Ermittlungen in diesem Umfeld zu erleichtern (*Rückert/Goger MMR 2020*, 393).

Die dritte bedeutsame Form der Darknetkriminalität, die allerdings weniger öffentliche Aufmerksamkeit erhält, ist das sogenannte ‚Bulletproof Hosting‘. Darum geht es im laufenden ‚[Cyberbunker-Verfahren](#)‘ vor dem Landgericht Trier. Betreiber/innen von Bulletproof Hosting stellen anderen Täter/innen gegen Bezahlung anonyme Server und verschlüsselte Internetverbindungen zur Durchführung krimineller Aktivitäten zur Verfügung. Hierdurch werden, über den reinen Handelsplattformbetrieb hinaus, weitere illegale Geschäftsfelder im Darknet und unter Nutzung von Verschlüsselungstechnologie erschlossen.

Was der Entwurf besser macht als seine Vorgänger

Im Vergleich zu den Vorgänger-Entwürfen ist positiv zu bewerten, dass der Begriff der „internetbasierten Leistung“ durch den Begriff der „Handelsplattform“ ersetzt worden ist. [Nach der Gesetzesbegründung](#) werden hierdurch alle kommerziellen wie nicht-kommerziellen Foren und Online-Marktplätze erfasst, unabhängig davon, ob die illegalen Waren und Dienstleistungen dort gegen Entgelt angeboten, verschenkt oder getauscht werden ([Seite 11 des Entwurfs](#)). Letzteres ist vor allem für die Einbeziehung der Tauschplattformen für Kinderpornographie von Bedeutung. Von diesem Begriff ausgenommen sind jedoch die Anbieter/innen von Anonymisierungsdiensten, wie zum Beispiel die Betreiber/innen von Tor-Knoten oder von anonymen E-Mail-Diensten. Damit wird einer zentralen Forderung der Kritiker/innen Rechnung getragen (*Bartl/Moßbrucker/Rückert* *Angriff auf die Anonymität im Internet*, S. 10 ff.). Diese [befürchteten](#) zu Recht, dass der vorherige Gesetzesentwurf auch zur Verfolgung der oben genannten „neutralen“ Anonymisierungsdienstleister führen würde. Diese Dienstleister werden nicht selten sowohl zu gesellschaftlich wünschenswerten (zum Beispiel Quellen-Schutz von Journalist/innen, Kommunikation von Menschenrechtsaktivist/innen und Dissident/innen in autokratischen Systemen, Umgehung staatlicher Zensur) als auch kriminellen Zwecken genutzt.

Zum anderen ist zu begrüßen, dass der neue Entwurf auf eine Beschränkung auf Angebote im Darknet verzichtet. Neben den sich ergebenden Schwierigkeiten bei der Formulierung einer solchen Einschränkung sind auch keine Sachgründe

dafür ersichtlich, zwar den Betrieb im Darknet, nicht aber in anderen Bereichen des Internets zu kriminalisieren.

Ein unnötiges Gesetz?

Zentrale Probleme der Vorgängerentwürfe bestehen jedoch weiter. Überhaupt ist zweifelhaft, ob die in der Gesetzesbegründung behaupteten Strafbarkeitslücken tatsächlich bestehen. Im Bereich der besonders praxisrelevanten Deliktgruppen der §§ 29 ff. BtMG (Handel mit Betäubungsmitteln), § 52 WaffG (Handel mit Waffen) und §§ 184b f. StGB (Verbreitung und Besitz von Kinderpornographie) werden die notwendigen Tathandlungen der beteiligten Personen (zum Beispiel das „Handeltreiben“ in § 29 Abs. 1 S. 1 Nr. 1 BtMG und § 52 Abs. 1 Nr. 1 WaffG und der „Besitz“ in § 184b Abs. 3 Alt. 2 StGB) von der Rechtsprechung sehr extensiv ausgelegt und erfassen den Betrieb einer Handels- oder Tauschplattform als Vermittlungstätigkeit (für § 29 BtMG: MüKoBtMG/*Oglakcioglu* § 29 Rn. 291 f.; für § 52 WaffG siehe die Legaldefinition in Anlage 1 Abschnitt 2 Nr. 9) oder als eigenen Besitz (Hierzu MüKoStGB/*Hörnle* § 184b Rn. 40 ff.) der inkriminierten Bilder und Videos. § 29 Abs. 1 S. 1 Nr. 10 BtMG kriminalisiert sogar das öffentliche Mitteilen einer Erwerbsgelegenheit für Betäubungsmittel.

Für Fälle, in denen das Verhalten der Plattformbetreiber nicht unter die vorgenannten Normen subsumiert werden kann, verbleibt noch strafbare Beihilfe nach § 27 StGB. Allerdings äußern die Entwurfsverfasser/innen Zweifel daran, ob der vollautomatisierte Betrieb der Handelsplattformen nicht zur Verneinung des Beihilfevorsatzes in vielen Fällen führt ([Seite 6 des Entwurfs](#)). Was, wenn die Betreiber/innen keine Kenntnis von den konkreten Waren haben, die auf den von ihnen automatisiert betriebenen Plattformen gehandelt werden, selbst wenn die Plattform generell auf den Handel illegaler Waren ausgerichtet ist? Die Sorgen der Entwurfsverfasser/innen basieren auf einer [BGH-Entscheidung](#), die voraussetzt, dass der Gehilfe die „Haupttat in ihren wesentlichen Merkmalen kennt“. Doch die Schlussfolgerung der Verfasser/innen, dass die Plattformbetreiber/innen für eine Verurteilung wegen Beihilfe Kenntnis von den konkret gehandelten Waren haben müssen ([Seite 6 des Entwurfs](#)), ist unzutreffend. Wie ich bereits [an anderer Stelle dargestellt](#) habe, Greco in seiner ausführlichen Untersuchung [belegt hat](#), und wie [der BGH an anderer Stelle deutlich macht](#), leistet Beihilfe, wer „dem Täter ein entscheidendes Tatmittel willentlich an die Hand gibt und damit bewußt das Risiko erhöht, daß eine durch den Einsatz gerade dieses Mittels typischerweise geförderte Haupttat verübt wird“. Somit genügt bereits, wenn der/die Betreiber/in bei Inbetriebnahme der Plattform (oder späteren Wartungshandlungen) davon ausgeht, dass diese (auch) für die Begehung „typischer“ Delikte der Underground Economy genutzt werden wird. Ist dies nicht der Fall, entfällt die Strafbarkeit, es fehlt dann aber auch an der Strafwürdigkeit des in Frage stehenden Verhaltens.

(Versuchte) Beihilfe ohne (begangene) Haupttat

Der eigentliche „Vorteil“ des nun vorgeschlagenen § 127 StGB liegt für die Strafverfolger/innen also darin, dass keine einzige über die Plattform begangene

Haupttat nachgewiesen werden muss, weil es überhaupt nicht darauf ankommt, ob eine rechtswidrige Tat begangen wurde. Es genügt die reine Zweckausrichtung der Plattform. Dogmatisch betrachtet handelt es sich um die Einführung einer „versuchten Beihilfe“ für bestimmte Deliktsbereiche im Internet. Das entscheidende Abgrenzungsmerkmal zwischen legalem und illegalem Verhalten beim Betreiben einer Internethandelsplattform ist danach die Zweckausrichtung.

Den Entwurfsverfasser/innen nach kommt es bei der Zweckausrichtung auf die „Art und Weise der Darstellung der Plattform“ und die „Gesamtschau des Angebots“ an ([Seite 11 des Entwurfs](#)). Die erste Alternative ist durch kreative Gestaltung der Plattform leicht zu umgehen. Denkbar ist beispielsweise die Verwendung von „Warenkategorien“ mit alltäglichen Produktbezeichnungen oder szenentypische Fantasienamen sowie ein prominent dargestellter Hinweis, dass der Handel von illegalen Waren und Dienstleistungen von den Betreiber/innen der Plattform nicht gefördert wird und untersagt ist, gleichzeitig aber mit der besonderen Anonymität der Verkäufer/innen und Käufer/innen geworben wird und tatsächlich keine Kontrollen stattfinden.

Die zweite Alternative ist somit entscheidend und führt womöglich dazu, dass „durch die Hintertür“ eine Prüfpflicht für die Hosting-Provider/innen hinsichtlich des tatsächlichen Angebots auf den von ihnen zur Verfügung gestellten Plattformen eingeführt wird. Dies ist mit Art. 14 der [E-Commerce-Richtlinie](#) nicht zu vereinbaren. Danach sind die EU-Mitgliedstaaten – und damit auch Deutschland – verpflichtet, dafür zu sorgen, dass Hosting-Provider nicht für die von ihren Kunden bereitgestellten Inhalte zur Verantwortung gezogen werden. Hiervon sind Ausnahmen nur vorgesehen, wenn die Provider „tatsächliche Kenntnis von der rechtswidrigen Tätigkeit oder Information“ haben oder bei Mitteilung über illegale Inhalte nicht unverzüglich dagegen tätig werden. Dies bedeutet, dass auch Online-Handelsplattformen grundsätzlich nicht für die von den Nutzern dort angebotenen (illegalen) Waren verantwortlich sind, soweit sie keine konkrete Kenntnis von den illegalen Aktivitäten haben. Hiergegen kann auch nicht eingewendet werden, dass die Privilegierung aus Art. 14 der Richtlinie „keine Anwendung auf Anbieter eines Dienstes [finde], der maßgeblich zu kriminellen Zwecken betrieben wird“ ([Seite 9 des Entwurfs](#)). Denn es geht bei der mittelbaren Prüfpflicht gerade darum, festzustellen, ob eine solche Zweckausrichtung vorliegt. Hierdurch wird auch deutlich, dass das Abstellen auf das tatsächliche Warenangebot sogar als Einführung einer nach Art. 15 der E-Commerce-Richtlinie ausdrücklich unzulässigen, allgemeinen Überwachungspflicht für Hosting-Provider verstanden werden kann. Insofern ist die Argumentation der Entwurfsverfasser/innen an dieser Stelle zirkulär und europarechtswidrig.

Übergeordnet ist es bemerkenswert, dass sich die Zweckausrichtung der Plattformen zur Förderung rechtswidriger Taten im Vorsatz der Betreiber/innen widerspiegeln muss. Zumindest wird der/die Täter/in die Plattform in dem Bewusstsein betreiben müssen, dass das Angebot „typischerweise“ zur Begehung entsprechender Delikte genutzt werden wird. Da „Zweck“ darüber hinaus ein angestrebtes Ziel meint, ist auch für den Vorsatz erforderlich, dass der/die Betreiber/innen in die Plattform gezielt zur Förderung rechtswidriger Taten in Betrieb nimmt,

beziehungsweise in Betrieb hält. Damit liegen die Vorsatzhürden bei § 127 StGB jedoch tatsächlich höher als diejenigen, welche die Rechtsprechung (bei richtiger Lesart) an den Beihilfevorsatz stellt.

Online-Durchsuchungen bei angestrebtem Verkauf von Marihuana und gefälschten Handtaschen

Die bedenkliche Weite des geplanten § 127 StGB führt auch zu prozessualen Folgen. Ein Anfangsverdacht nach § 152 Abs. 2 StPO erfordert lediglich, dass aufgrund konkreter Tatsachen nach kriminalistischer Erfahrung das Vorliegen einer verfolgbaren Straftat als „möglich“ erscheint (*Meyer-Goßner/Schmitt* § 152 Rn. 4). Wenn es demnach genügt, dass es „möglich“ erscheint, dass der Zweck einer Internethandelsplattform auf die Förderung rechtswidriger Taten gerichtet ist (iSv § 127 Abs. 1 S. 2 StGB-Entwurf), lässt sich ein solcher Anfangsverdacht schon bei einer Häufung von entsprechenden Angeboten auf einer Plattform bejahen. Es sei in diesem Zusammenhang auch darauf hingewiesen, dass hierfür auch Marken- und Designrechtsverstöße nach § 127 Abs. 1 S. 2 lit. g und lit. h StGB-Entwurf genügen können.

Die Problematik wird dadurch vertieft, dass für die Fälle gewerbsmäßigen Handelns – eine Kategorie in die professionell betriebene Plattformen regelmäßig fallen – als Ermittlungsbefugnisse auch die (Quellen-)Telekommunikationsüberwachung und die Onlinedurchsuchung nach §§ 100a, 100b StPO vorgesehen sind. Ob eine „versuchte Beihilfe“ den hohen verfassungsrechtlichen Anforderungen an die Befugnis zur Online-Durchsuchung im Allgemeinen und im Speziellen, wenn es um „versuchte Beihilfe“ zu Design- und Markenrechtsverstößen, Hacking-Straftaten oder Handel mit sogenannten weichen Drogen in geringen Mengen geht, erscheint mehr als zweifelhaft. Im präventiven Bereich [verlangt das BVerfG](#) eine konkrete Gefahr „für ein überragend wichtiges Rechtsgut“, namentlich „Leib, Leben und Freiheit der Person“ sowie „Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt“. Hieraus ist in der Literatur zu Recht der Schluss gezogen worden, dass bei der repressiven Online-Durchsuchung – bei der es nicht mehr (unmittelbar) um die Abwendung von Gefahren geht – das entsprechende Delikt eine Handlung kriminalisieren muss, durch die solche „überragend wichtigen Rechtsgüter“ verletzt oder gefährdet worden sind (*Großmann* GA 2018, 440 (451)). Es erscheint äußerst zweifelhaft, ob das Betreiben einer Plattform zu dem Zweck, den Handel mit Marihuana oder gefälschten Handtaschen zu ermöglichen, eine „konkrete Gefahr für überragend wichtige Rechtsgüter“ darstellt. Dies umso mehr, als eine Online-Durchsuchung (theoretisch) sogar möglich wäre, ohne dass auch nur ein einziges Gramm Haschisch oder eine einzige Handtasche tatsächlich verkauft worden ist.

Ein bemühter Versuch

Der Entwurf ist ersichtlich darum bemüht, viele der zu seinen Vorgängern geäußerten Kritikpunkte aufzugreifen. Zentrale Probleme bleiben aber bestehen.

Dass § 127 StGB-Entwurf ein Verhalten weit im Vorfeld einer Rechtsgutsgefährdung unter Strafe stellt, ohne die den §§ 129 ff. StGB zugrunde liegende und gefahrerhöhende feste Organisationsstruktur zu verlangen, ist nicht zuletzt im Hinblick auf das strafrechtliche ultima ratio-Prinzip (siehe hierzu *Jahn/Brodowski* ZStW 129 (2017), 363) und [den Verhältnismäßigkeitsgrundsatz bedenklich](#).

