IT-Strafrecht

Rechtsanwalt Dr. Saleh R. Ihwas, Wiesbaden

„Die digitale Unterwelt" – Strafprozessuale Ermittlungsmöglichkeiten im Darknet

I. Einleitung

„The Dark Net – Inside the Digital Underworld": Mit diesem Titel erschien im Jahr 2014 ein Buch, in dem der Autor über – teilweise persönliche – Erfahrungen in einem sog. Darknet[1] berichtet.[2] Nachdem er sowohl positive als auch negative Erlebnisse im Darknet beschrieben hat, kommt er zu dem Schluss, dass das Darknet im Ergebnis nichts weiter ist als ein „Spiegel der Gesellschaft"[3]. Dem Darknet haftet in der Gesellschaft jedoch ein eher schlechter Ruf an. Dies liegt sowohl an der negativen Medienberichterstattung[4] als auch am Namen: *Dark*net. Durch die Bezeichnung als „Dark" wird automatisch etwas Negatives mit dem Begriff verknüpft, denn Dinge, die man nur „im Dunklen" macht, sollen im Verborgenen bleiben. Vielfach wird behauptet, dass das Darknet primär zur Begehung von Straftaten genutzt werde. Teilweise heißt es, dass 57%[5] bzw. nahezu 100%[6] der Angebote im Darknet „illegalen Zwecken" dienten. Hierbei ist aber zu berücksichtigen, dass es sich um ein anonymes Netzwerk handelt, sodass belastbare Zahlen zur legalen oder illegalen Nutzung schwer zu ermitteln sein dürften.[7] Im Ergebnis ist jedenfalls festzuhalten, dass im Darknet oder unter Zuhilfenahme des Darknets Straftaten begangen werden können und diese durch die Strafverfolgungsbehörden aufzuklären sind.

II. Surface Web, Deep Web und Darknet: Terminologie

Das Internet kann in zwei Bereiche unterteilt werden: Das „Surface Web" und das „Deep Web". Das Surface Web meint sämtliche über einen Standardbrowser erreichbaren Internetseiten, die bei einer Suchmaschine indexiert[8] sind.[9] Das Deep Web umfasst dementsprechend sämtliche anderen Webseiten, die nicht bei Suchmaschinen indexiert sind. Das Darknet ist im Ergebnis als ein Teil des Deep Webs zu verstehen:

1. Unterschied zwischen Darknet und Surface Web

Das Darknet ist nicht über die gängigen Browser, wie z.B. Mozilla Firefox, zu erreichen, sondern über eine eigene Software. Im Darknet kann aber ebenso „gesurft" werden wie im Surface Web, der Unterschied ist jedoch, dass dies im Darknet anonym geschieht: Wird im Surface Web eine Webseite – z.B. www.facebook.de – aufgerufen, so ist die Information, dass man die Webseite besucht hat, bei jedenfalls zwei Unternehmen vorhanden. Zum einen sieht der Access-Provider des Nutzers (z.B. T-Online) welche Internetseite durch den Nutzer aufgerufen wurde. Zum anderen sieht Facebook von welcher IP-Adresse aus die Facebook-Webseite aufgerufen wurde und kann so den Nutzer identifizieren. Surft der Nutzer aber im Darknet, ist diese Identifikation grundsätzlich weder dem Access-Provider noch dem Internetseitenbetreiber möglich. Die Anonymität im Darknet ist damit der wesentliche Unterschied zum Surface Web.

---

[1] Im englischen Sprachgebrauch wird teilweise der Begriff „Dark Web" genutzt (s. https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/), der Übersichtlichkeit halber wird hier nur der Begriff „Darknet" verwendet, die beiden Begriffe sind synonym zu verstehen.
[2] *Bartlett*, The Dark Net – Inside the Digital Underworld, 2014.
[3] *Bartlett*, The Dark Net – Inside the Digital Underworld, S. 251.
[4] Über das Darknet wird in den Medien fast ausschließlich im Zusammenhang mit der Begehung von Straftaten berichtet; vgl. nur http://www.zeit.de/digital/internet/2017-07/alphabay-drogenhandel-darknet-geschlossen-usa-jeff-sessions-hansa.
[5] becklink 2004949.
[6] becklink 2003973.
[7] Vgl. BT-Drs. 18/9487, S. 1 unter Verweis auf einen Bericht auf netzpolitik.org: https://netzpolitik.org/2016/bka-hat-keine-belastbaren-zahlen-also-doch-keine-million-menschen-in-deutschland-die-im-darknet-drogen-waffen-und-falsche-paesse-kaufen/.
[8] Der Suchmaschinenindex stellt die Gesamtzahl der durch eine Suchmaschine gelisteten Webseiten dar. Es handelt sich dabei um die Webseiten, die bei einer Anfrage durchsucht werden.
[9] Vgl. Presseinformation des BKA v. 27.07.2016; teilweise wird auch vom „Visible Web" oder „Clearnet" gesprochen; *Meywirth*, Kriminalistik 2016, 355.

2. Existenz verschiedener Darknets

Es ist zunächst wichtig zu unterscheiden, dass es nicht nur „das Darknet" gibt, sondern mehrere Darknets. Jedes Darknet wird durch eine separate Software zugänglich gemacht. Das Darknet kann – bildlich gesprochen – mit einer Vielzahl einzelner verschlossener Räume verglichen werden, die jeweils nur mit einem separaten Schlüssel betreten werden können. Es gibt eine nicht unerhebliche Anzahl von Anwendungen, die eine verschlüsselte Kommunikation der Nutzer untereinander bzw. ein verschlüsseltes Surfen im jeweiligen Darknet ermöglichen.[10] Die bekannteste Software, mit der ein Darknet virtuell betreten werden kann, ist der sog. „Tor"-Browser. Der Browser kann frei zugänglich im Surface Web heruntergeladen und auf dem Endgerät des Nutzers installiert werden. Im Anschluss ist das Tor-Darknet für den Nutzer zugänglich. Daneben gibt es noch viele weitere Darknets wie z.B. das I2P (Invisible Internet Project)[11] oder Retroshare[12]; beides sind Anwendungen, die das anonyme Surfen bzw. die anonyme Kommunikation ermöglichen. Retroshare dient primär dazu, eine verschlüsselte Friend-to-Friend- bzw. Peer-to-Peer-Verbindung, also eine direkte Verbindung zwischen zwei Nutzern, herzustellen.

3. Technische Funktionsweise des Tor-Darknets

Das Tor-Netzwerk ist das bekannteste Darknet, das in der Regel auch in Presseberichten gemeint ist, wenn von „dem Darknet" gesprochen wird. „Tor" steht für „The Onion Router". Der Name kommt von dem „zwiebelförmigen" Aufbau der Verschlüsselungsstruktur der einzelnen hintereinander geschalteten sog. Nodes oder Knotenpunkte, über die der Nutzer die Verbindung zu seiner Zielwebseite aufbaut. Der technische Ablauf ist auf der Tor-Webseite beschrieben:[13] Zunächst lädt der auf dem Endgerät des Nutzers installierte Tor-Client eine Liste von Tor-Knotenpunkten von einem Tor-Directory-Server. Damit erhält die Tor-Anwendung eine Liste aller verfügbaren Knotenpunkte, die für die Verschlüsselung genutzt werden können. Ruft der Nutzer nun eine Internetadresse – z.B. die Tor-Adresse von Facebook: https://facebookcorewwwi.onion[14] – auf, wird keine direkte Verbindung zu dieser Webseite hergestellt, sondern eine Verbindung über die Knotenpunkte geschaffen. Von diesen Knotenpunkten werden drei zufällig ausgewählt, um als erste, zweite und dritte Lage der oben erwähnten zwiebelförmigen Verschlüsselung zu dienen. Die Verbindung wird also vom Endgerät des Nutzers zunächst zum ersten Knotenpunkt hergestellt, von dort an den zweiten und schließlich an den dritten Knotenpunkt weitergeleitet. Erst von diesem dritten Punkt aus wird eine Verbindung mit der Zielwebseite hergestellt. Jeder Knotenpunkt „kennt" dabei nur die IP-Adresse des vorangegangenen Knotenpunkts. Die hintereinander geschalteten Knotenpunkte werden nach einem bestimmten Zeitintervall – ca. alle 10 Minuten – ausgetauscht, sodass kein Rückschluss von späteren auf frühere Verbindungen möglich ist. Aufgrund der geschilderten Struktur des Verbindungsaufbaus ist es dem Access-Provider (z.B. T-Online) nicht möglich, die Zieladresse des Nutzers zu erkennen. Ebenso wenig kann in dem gewählten Beispiel Facebook nachvollziehen, von wo aus auf die Webseite zugegriffen wird. Lediglich die IP-Adresse des dritten Knotenpunkts kann von Facebook erkannt werden. Die IP-Adresse des Endgeräts bzw. des Routers des Nutzers ist für Facebook nicht sichtbar.

4. Abgrenzung zum Deep Web

Das Deep Web definiert sich als Summe aller Internetadressen, die nicht bei Suchmaschinen indexiert sind; Webseiten im Deep Web sind darum nicht durch die gängigen Suchmaschinen auffindbar. Das Deep Web funktioniert daher wie das Internet der 90er Jahre, als es noch keine Suchmaschinen wie z.B. Google oder Lycos gab. Damals musste dem Nutzer die konkrete Internetadresse der Webseite bekannt sein, um diese aufrufen zu können. Ansonsten war die Webseite nicht auffindbar. Diese Ausführungen gelten ebenso für das Darknet: auch Internetadressen im Darknet sind nicht bei Suchmaschinen des Surface Web indexiert, insoweit können die einzelnen Darknets als Bestandteil des Deep Webs begriffen werden. Ein Darknet unterscheidet sich aber in zwei wesentlichen Punkten vom Deep Web: Erstens, das Surfen im Deep Web wird nicht standardmäßig anonymisiert, wie es im Darknet der Fall ist. Zweitens, man braucht keine spezielle Software, wie den Tor-Browser, um in das Deep Web zu gelangen. Das Deep Web kann mittels der gängigen Browser, wie z.B. Mozilla Firefox, erreicht werden.

---

[10] Teilweise können mit der jeweiligen Software auch Webseiten im Surface Web aufgerufen werden.
[11] https://geti2p.net/en/.
[12] http://retroshare.net/.
[13] Vgl. zum Ganzen https://www.torproject.org/about/overview.html.en.
[14] Hierbei handelt es sich um die Darknet-Adresse von Facebook. Der Dienst ist bereits seit dem Jahr 2014 im Tor-Darknet erreichbar (vgl. https://www.heise.de/security/meldung/Facebook-geht-ins-Tor-Netz-2440221.html).

Ein Darknet stellt daher einen besonderen Teil des Deep Webs dar, der aber begriffsterminologisch vom Deep Web abzugrenzen ist, um den Besonderheiten des Darknets gerecht zu werden.

5. Historie und Definition des Begriffs „Darknet"

Der Begriff Darknet wurde durch eine Veröffentlichung von vier Microsoft-Mitarbeitern zum Thema „The Darknet and the Future of Content Distribution" geprägt.[15] Darin wird das Darknet direkt zu Beginn abstrakt beschrieben als *„a collection of networks and technologies used to share digital content."*[16] Im weiteren Verlauf der Arbeit beschreiben die Autoren das Darknet noch präziser als: *„The idea of the darknet is based upon three assumptions:*

1. Any widely distributed object will be available to a fraction of users in a form that permits copying.

2. Users will copy objects if it is possible and interesting to do so.

3. Users are connected by high-bandwidth channels.

The darknet is the distribution network that emerges from the injection of objects according to assumption 1 and the distribution of those objects according to assumptions 2 and 3."[17]

Diese Definition ist geprägt durch die damaligen technischen Entwicklungen: Internettauschbörsen waren ein neues Medium, die es jedem Nutzer erlaubten, Software oder andere digitale Inhalte – beispielsweise Musikdateien – miteinander zu teilen. Eine der damals bekanntesten Tauschbörsen war „Napster"; Napster wurde im Jahre 1999 gegründet und war bis einschließlich 2001 ein sehr beliebtes Medium. Darauf folgten verschiedene Filesharing-Plattformen, die auf dem sog. Gnutella-Protokoll basierten – z.B. die Plattform Morpheus. In diesen Netzwerken wurde nicht anonymisiert miteinander kommuniziert bzw. Inhalte wurden nicht anonymisiert miteinander ausgetauscht. Dies lag vermutlich daran, weil es schlicht nicht für erforderlich gehalten wurde: Zum einen fehlte den Nutzern das Unrechtsbewusstsein und zum anderen rechnete kaum jemand damit, wegen des Teilens von Musikdateien oder Software zivilrechtlich in Anspruch genommen oder strafrechtlich verfolgt zu werden.

Diese Tauschbörsen waren damals eine technische Neuerung, die die Strafverfolgungsbehörden vor erhebliche Schwierigkeiten stellten: Zunächst musste das Teilen von Inhalten als strafrechtlich relevantes Verhalten eingeordnet und dann der digitale Weg der Daten rekonstruiert werden, um den Teilenden – also den Täter – zu finden. Nachdem die Strafverfolgungsbehörden aber mehr und mehr Erfolge bei der Verfolgung von Urheberrechtsstraftaten erreichen konnten, überlegten sich die Nutzer neue Wege, um die Daten – nunmehr unerkannt – untereinander zu teilen. Man versuchte, seine digitalen Spuren mittels Verschlüsselung zu verschleiern. Der Aspekt der anonymen Kommunikation war in der Definition der Microsoft-Mitarbeiter zum Darknet nicht enthalten – aber aus den vorgenannten Gründen auch nicht notwendig. Es ging zur damaligen Zeit bloß darum, Dateien miteinander zu teilen und nicht darum, dabei unerkannt zu bleiben. In der heutigen Zeit ist die Verschlüsselung ein wesentlicher Zusatz, sodass die Definition der Microsoft-Mitarbeiter ergänzt werden muss. Zudem geht es nicht mehr nur um das Teilen bzw. Kopieren von Daten, sondern ebenso um die – bloße – anonyme Kommunikation. Dies unterstreicht auch die jüngst in den Duden aufgenommene Definition zum Begriff „Darknet".[18] Das Darknet wird darin definiert als *„besonders gegen Zugriffe von außen gesicherter Bereich des Internets, in dem u.a. illegale Inhalte, Angebote verbreitet werden."*

Teilweise existieren in der juristischen Fachliteratur bereits Definitionen für das Darknet, danach wird es wie folgt beschrieben: *„Als Darknet bezeichnet man Netzwerke, in denen Daten nur verschlüsselt übertragen werden und die nur mit speziellen Browsern zugänglich sind."*[19] Teilweise wird das Darknet darüber hinaus definiert als *„eine Variante eines Peer-to-Peer Netzwerks, in dem versucht wird, die Identität der Nutzer weitgehend zu verschleiern"*[20] bzw. als ein *„Netzwerk von Personen, die sich vertrauen und nur mit den anderen Nutzern dieser Gruppe verbinden"*.[21]

---

[15] *Biddle/England/Peinado/Willman*, The Darknet and the Future of Content Distribution, 2002, S. 1.
[16] *Biddle/England/Peinado/Willman*, The Darknet and the Future of Content Distribution, S. 1.
[17] *Biddle/England/Peinado/Willman*, The Darknet and the Future of Content Distribution, S. 2.
[18] http://www.duden.de/rechtschreibung/Darknet; vgl. auch *Meywirth*, Kriminalistik 2016, 355, der davon spricht, dass „größtenteils" illegale Inhalte im Darknet gehostet würden.
[19] *Rath*, DRiZ 2016, 292.
[20] *Prußl/Sarre* in: Auer-Reinsdorff/Conrad (Hrsg.), IT- und Datenschutzrecht, 2. Aufl. 2016, Technisches Glossar.
[21] *Bär* in: Wabnitz/Janovsky (Hrsg.), Handbuch des Wirtschafts- und Steuerstrafrechts, 4. Aufl. 2014, 14. Kapitel Rn. 200.

Zusammenfassend lässt sich ein Darknet daher folgendermaßen definieren: Ein Darknet ist ein Bereich des Deep Webs, der nur mittels einer jeweils speziellen Software betreten werden kann und in dem anonym kommuniziert oder Inhalte geteilt werden können.

III. Strafprozessuale Ermittlungsmöglichkeiten

Das Deep Web beinhaltet – wie oben geschildert – eine Vielzahl von Darknets, die jeweils durch separate Anwendungen betreten werden können. Das bekannteste Darknet ist über den Tor-Browser zugänglich. Dieses Darknet soll daher im Folgenden als Beispiel für strafprozessuale Ermittlungsmöglichkeiten dargestellt werden.

1. Navigieren im Darknet und verfügbare Dienste

Der Tor-Browser ermöglicht den Zugang zum Darknet. Um aber tatsächlich ins Darknet zu gelangen, muss der Nutzer erstmal wissen, wo er dort hin möchte. Einige wenige Webseiten finden sich relativ einfach, wie z.B. die bereits genannte Darknet-Präsenz von Facebook. Facebook hat hierfür einen eigenen Onion-Dienst im Tor-Darknet aufgesetzt.[22] Hier geht es Facebook aber lediglich darum, den eigenen Dienst anonym zugänglich zu machen, ohne Wert darauf zu legen, dass der eigene Dienst nicht im Darknet aufgefunden werden kann. Dies ist aber eher selten im Darknet, sofern es sich um eine für strafrechtliche Ermittlungen relevante Webseite handelt; die jeweilige Webseite soll vielmehr in den „dunklen Tiefen" des Darknets verborgen bleiben. Darum werden Webseiten im Darknet grundsätzlich nicht indexiert; zwar gibt es auch Suchmaschinen für das Darknet (wie Grams oder Torch), aber prinzipiell navigiert man dort über sog. Linklisten. Dies hängt auch damit zusammen, dass sich die Internetadresse einer Webseite im Darknet häufig ändert. Die Internetadressen im Darknet setzen sich in der Regel aus einer für den Leser unverständlichen Aneinanderreihung von Buchstaben und Zahlen zusammen, die auf „.onion" enden (z.B. 43456atwkfh.onion). Dies belegt bereits, dass Webseiten im Darknet längst nicht so einfach zu finden sind, wie es bei der Darknet-Präsenz von Facebook der Fall ist. Ändert sich die Internetadresse, können die Nutzer die Seite zunächst nicht mehr aufrufen, ohne die neue Adresse zu kennen. Darum gibt es die vorgenannten Linklisten. Dort werden die jeweils neuen Adressen der Webseiten eingetragen, um die Navigation im Darknet zu erleichtern. Hier gibt es etwa das sog. Hidden Wiki. Bei Aufruf dieser Webseite erhält man eine Vielzahl von – nicht zwingend funktionierenden – Links. Man ist nun nur noch den sprichwörtlichen Klick von der „digitalen Unterwelt" entfernt. Die Links sind nach Kategorien unterteilt; darunter finden sich auch einschlägige Kategorien wie z.B. „Drugs". In dieser Kategorie finden sich diverse Links zu Darknet-Handelsplätzen. Einer der bekanntesten dieser Handelsplätze war die „Silk Road".[23] Darauf folgten die erst kürzlich abgeschalteten Handelsplätze „AlphaBay" und „Hansa".[24] Neben diesen nunmehr bekannten Marktplätzen gibt es eine Vielzahl weiterer großer Handelsplattformen im Darknet. Das BKA geht davon aus, dass es ca. 50 Darknet-Plattformen gibt, die „Relevanz für das Kriminalitätsgeschehen in Deutschland haben".[25] Sie funktionieren grundsätzlich wie ein üblicher digitaler Marktplatz – etwa Amazon – auch: Es werden Waren zum Kauf und Verkauf angeboten. Die Käufer und Verkäufer agieren allerdings anonym. Eine Registrierung auf dem Marktplatz erfolgt allenfalls über einen frei zu wählenden und anonymisierten Benutzernamen. Es findet keinerlei Identifizierung statt – dies würde letztlich auch dem Ziel des anonymen Surfens diametral entgegenlaufen. Ein Käufer kann auf einem solchen digitalen Marktplatz allerlei verschiedene Waren erwerben – auf den einschlägigen Marktplätzen eben auch Waffen und Drogen. Daneben können ebenfalls Kreditkartendaten oder andere Dienste[26] gekauft werden, insoweit wird – angelehnt an die Cloud-Terminologie – von Crime-as-a-Service gesprochen.[27]

Darüber hinaus gibt es diverse Kommunikationsdienste, die zusätzlich den Austausch von Daten ermöglichen. Es handelt sich häufig um – geschlossene – Benutzergruppen, die aber auch auf dem Prinzip der Anonymität basieren. Oftmals kennen die Nutzer in der Gruppe lediglich den

[22] https://www.heise.de/security/meldung/Facebook-geht-ins-Tor-Netz-2440221.html.
[23] Der Gründer der „Silk Road" wurde im Februar 2015 durch ein New Yorker Gericht zu lebenslanger Freiheitsstrafe verurteilt, s. becklink 2000174.
[24] https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation?lipi=urn%3Ali%3Apage%3Ad_flagship3_feed%3B9sOW87ymTWuq0M0vvKz7bg%3D%3D; Europol berichtet häufiger über Erfolge im Darknet: https://www.europol.europa.eu/newsroom/news/darknet-dealer-of-drugs-and-arms-arrested-slovak-authorities.
[25] *Fünfsinn/Ungefuk/Krause*, Kriminalistik 2017, 440, 441; *Meywirth*, Kriminalistik 2016, 355, 356.
[26] Besonders relevant in diesem Zusammenhang ist auch die Anmietung sog. Botnetze zur Durchführung von Denial-of-Service-Attacks (DoS-Attacks), s. *Meier*, Kriminalistik 2016, 361 f.
[27] Zu den verschiedenen Diensten ausführlich *Meywirth*, Kriminalistik 2016, 355 ff.; s.a. *Fünfsinn/Ungefuk/Krause*, Kriminalistik 2017, 440, 442 f.; *Meier*, Kriminalistik 2016, 361 ff.

anonymisierten Benutzernamen der anderen Teilnehmer und haben keinerlei Information zu deren wahrer Identität.

Die Ermittlungen der Strafverfolgungsbehörden konzentrieren sich dementsprechend auf zwei Dienste: Handelsplätze und Kommunikationsdienste.

2. Zugriff auf öffentliche zugängliche Informationen

Die Informationen auf digitalen Handelsplätzen und in Kommunikationsdiensten können öffentlich zugänglich sein. Die öffentliche Zugänglichkeit von Daten ist ein wichtiges Unterscheidungsmerkmal, da ein Zugriff auf eben diese Daten keinen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und ein Tätigwerden der Strafverfolgungsbehörden jedenfalls auf Grundlage der Vorschriften der §§ 161, 163 StPO möglich ist.[28] Daten sind öffentlich zugänglich, wenn sie einem unbestimmten Personenkreis zugänglich gemacht werden und zwischen den einzelnen Personen keine persönliche Beziehung besteht.[29] Daten, die im Internet frei zugänglich sind, sind daher öffentlich zugänglich: Jeder mit einem Internetanschluss und einem Browser kann auf diese Daten zugreifen. Um Zugriff auf das Darknet zu haben, ist der Tor-Browser, also eine spezielle Anwendung, erforderlich. Alleine die Erforderlichkeit der Nutzung einer bestimmten Anwendung ist kein ausreichendes Kriterium, um einen effektiven Schutz gegen einen Zugriff durch dritte Personen zu erlangen. Denn den Browser bzw. die Anwendung kann jedermann herunterladen und verwenden. Dies gilt auch für Strafverfolgungsbehörden.[30] Anderenfalls wären sämtliche im Internet verfügbaren Daten ebenfalls als zugangsgeschützt zu betrachten, da diese auch nur mittels eines Browsers, z.B. dem Internet Explorer, abgerufen werden können. Kann mittels des Tor-Browsers direkt auf die Seite im Darknet zugegriffen werden, ist dies mit dem Zugriff auf eine Webseite im Surface Web vergleichbar – und diese sind auch öffentlich zugänglich. Um das Merkmal der Öffentlichkeit zu verneinen, wäre eine Zugangssicherung erforderlich. Selbst wenn eine Registrierung zu erfolgen hat, ist hierfür im Darknet häufig nur ein fiktiver Benutzername erforderlich. Dies ist nicht ausreichend, um die Öffentlichkeit auszuschließen, denn jedermann kann sich letztlich dort registrieren. Das Tor-Netzwerk bietet insoweit lediglich Anonymität und keine Exklusivität in Form eines beschränkten Nutzerkreises. Es müsste sich bei der Webseite vielmehr um eine geschlossene Benutzergruppe handeln, zu der nur eine bestimmbare Anzahl von Personen Zutritt hat. Das bloße Platzieren einer Webseite im Tor-Darknet ist daher nicht geeignet, eine ausreichende Barriere gegen die Öffentlichkeit zu bilden. Es handelt sich insoweit allenfalls um ein bloßes Scheinhindernis.[31]

Anders kann dies zu bewerten sein, wenn eine Information zugangsgeschützt ist; sie beispielsweise nur mittels eines Passworts abgerufen werden kann oder der Zugang zu einer Webseite nur unter bestimmten und vom Webseitenbetreiber kontrollierten Voraussetzungen gestattet wird. Diesen Zugang zu erhalten, ist für die Strafverfolgungsbehörden in der Regel nur möglich, indem sie personale Ermittlungsmethoden einsetzen, deren Zulässigkeit im Folgenden betrachtet wird.

3. Personale Ermittlungen

Personale Ermittlungsmethoden versprechen im anonymen Darknet generell den größten Ermittlungserfolg.[32] Ermitteln Strafverfolgungsbehörden im Internet unter einer erfundenen Identität, muss es sich nicht zwingend um einen Verdeckten Ermittler nach § 110a StPO handeln.[33] Solange ein Beamter lediglich unter Geheimhaltung seiner Identität ermittelt – er also gerade

[28] BVerfGE 120, 274, 344 f.; *Zöller* in: Heidelberger Kommentar, StPO, 5. Aufl. 2012, § 163 Rn. 12; *B. Gercke*, GA 2012, 474, 481; *Henrichs*, Kriminalistik 2011, 622, 626. Im Zusammenhang mit Ermittlungen im Internet spielt auch das Völkerrecht stets eine Rolle, denn Daten sind häufig in einem Drittstaat gehostet und beim Zugriff darauf, werden – digital – die Landesgrenzen überschritten. Der Zugriff auf öffentlich zugängliche Informationen durch Strafverfolgungsbehörden stellt aber keinen Verstoß gegen den völkerrechtlichen Souveränitätsgrundsatz dar, da es sich insoweit um Völkergewohnheitsrecht handelt (*B. Gercke* in: Heidelberger Kommentar, StPO, § 110 Rn. 27, *ders.*, GA 2012, 474, 489). Vgl. generell zu den Herausforderungen für die internationale Zusammenarbeit im Bereich Cybercrime: *Goger/Stock*, ZRP 2017, 10 ff.

[29] BGH StV 2012, 539; BGHSt 11, 282; *Fischer*, StGB, 64. Aufl. 2017, § 184b Rn. 10.

[30] Soweit ersichtlich, enthält die Tor-Anwendung keine AGBs, die eine Nutzung nur „für private Zwecke" gestattet. Hier müsste man aber ohnehin annehmen, dass AGBs gegenüber den staatlichen Behörden insoweit nicht gelten, da sie bei der Strafverfolgung eine Hoheitsaufgabe mit Verfassungsrang (vgl. BVerfGE 77, 65, 76; 130, 1, 26) wahrnehmen. Ansonsten könnte den Strafverfolgungsbehörden auf diese Weise der Zutritt zu sämtlichen Diensten des Internets verwehrt werden, vgl. hierzu auch *Weichert*, in: Möllers/van Ooyen (Hrsg.), Jahrbuch Öffentliche Sicherheit 2012/2013, 379, 383; *Henrichs/Wilhelm*, Kriminalistik 2010, 218, 223.

[31] Vgl. hierzu etwa BGH StV 2012, 539; *Steinmetz* in: Münchener Kommentar, StGB, 3. Aufl. 2017, § 86 Rn. 35.

[32] *Fünfsinn/Ungefuk/Krause*, Kriminalistik 2017, 440, 444.

[33] *Bruns* in: Karlsruher Kommentar, StPO, 7. Aufl. 2013, § 110a Rn. 7; *Hegmann* in: Beck'scher Online-Kommentar, StPO, Stand: 01.01.2018, § 110a Rn. 6; *Rosengarten/Römer*, NJW 2012, 1764, 1767; *Soiné*, NStZ 2014, 248, 249 f.

nicht über eine Legende i.S.d. Vorschrift des § 110a Abs. 2 S. 1 StPO verfügt –, ist er kein Verdeckter Ermittler.[34] Bei personalen Ermittlungen im Internet ist daher – wie in der realen Welt – zwischen dem nicht offen ermittelnden Polizeibeamten (kurz: noeP) und dem Verdeckten Ermittler zu unterscheiden.

a) (Virtueller) Nicht offen ermittelnder Polizeibeamter

Die wohl häufigste Ermittlungsmethode im Darknet ist die Nutzung eines virtuellen nicht offen ermittelnden Polizeibeamten.

aa) Voraussetzungen zum Einsatz nicht offen ermittelnder Polizeibeamter in der realen Welt

Nicht offen ermittelnde Polizeibeamte werden auf Grundlage der Vorschriften der §§ 161, 163 StPO tätig.[35] Die Generalermittlungsklausel kann aber allenfalls geringfügige Eingriffe in das Recht auf informationelle Selbstbestimmung rechtfertigen.[36] Das Recht auf informationelle Selbstbestimmung ist nach der Rechtsprechung des Bundesverfassungsgerichts bei personalen Ermittlungen im Internet nicht mehr nur geringfügig betroffen, wenn der Betroffene in die – falsche – Identität des ermittelnden Beamten schutzwürdig vertraut und dadurch Informationen erhoben werden, die der Beamte sonst nicht erhalten hätte.[37] Die Schutzwürdigkeit des Vertrauens ist dementsprechend das zentrale Kriterium für die Abwägung, ob die Ermittlungsmaßnahme – noch – auf die Vorschriften der §§ 161, 163 StPO gestützt werden kann: Ob man den Vertrauensschutz bejaht, hängt insbesondere von den Gegebenheiten der Kommunikation ab. Es ist zunächst zu differenzieren, ob bzw. inwieweit eine Registrierung bei dem Internetdienst, über den der Betroffene mit dem Ermittler kommuniziert, kontrolliert wird,[38] denn dadurch würde die Identität von einer unabhängigen dritten Seite geprüft. Darüber hinaus ist von Bedeutung, ob eine Individualisierung der Identität möglich ist; hier ist dahingehend zu unterscheiden, ob anhand von Merkmalen zum Identitätsmanagement (etwa bei Angabe von Name, Geburtstag, Wohnort, Arbeitsplatz) eine Konkretisierung der Person möglich ist. Je mehr dieser Voraussetzungen zutreffen, desto eher kann ein Betroffener schutzwürdig in die Identität des ermittelnden Beamten vertrauen und damit ein nicht mehr nur geringfügiger Eingriff in das Recht auf informationelle Selbstbestimmung gegeben sein. Es kommt hierbei stets auf die besonderen Umstände des Einzelfalles an. Diese allgemeinen Kriterien sind auch auf personale Ermittlungen im Darknet anzuwenden:

bb) Ermittlungen durch nicht offen ermittelnde Polizeibeamte im Darknet

Das Tor-Darknet ist für jedermann zugänglich. Die Software ist frei im Surface Web erhältlich. Nach Herunterladen und Installation der Software kann der Nutzer das Darknet betreten. Die Besonderheit des Darknets liegt in seiner anonymen Kommunikationsstruktur. Registriert man sich dort auf einer Plattform, wie z.B. einem der digitalen Marktplätze, auf denen Drogen oder Waffen zum Kauf angeboten werden, ist in der Regel lediglich ein fiktiver Benutzername anzugeben. Weitere Merkmale zum Identitätsmanagement – wie man es etwa aus Sozialen Netzwerken wie Facebook kennt – sind bei der Anmeldung nicht erforderlich. Eine Individualisierung der Person ist daher insgesamt nur schwer möglich, weil genau diese Individualisierung im anonymen Darknet nicht gewollt ist – und auch der anonymen Kommunikation diametral entgegensteht.

Darüber hinaus ist insebsondere zu hinterfragen, ob es überhaupt möglich ist, dass ein Nutzer in die Identität seines virtuellen Gegenübers schutzwürdig vertraut, wenn der Nutzer selbst ganz bewusst einen – nahezu – völlig anonymen Kommunikationsweg über das Darknet gewählt hat. Dem Nutzer ist darum in der Regel bewusst, dass eine Identifikation des Kommunikationspartners nur schwer möglich ist. Da die Art der Kommunikation – auf die das Bundesverfassungsgericht maßgeblich abstellt, um die Schutzwürdigkeit des Vertrauens zu bestimmen[39] – anonym ist, wird man von der Schutzwürdigkeit des Vertrauens in die Identität des virtuellen

---

[34] *Bruns* in: Karlsruher Kommentar, StPO, § 110a Rn. 6; *B. Gercke* in: Heidelberger Kommentar, StPO, § 110a Rn. 11; *Hegmann* in: Beck'scher Online-Kommentar, StPO, § 110a Rn. 5 f.; speziell für Ermittlungen im Darknet: *Krause*, NJW 2018, 678, 680.

[35] *Rath*, DRiZ 2016, 292 (293); generell zum Einsatz eines nicht offen ermittelnden Polizeibeamten im Internet: BGHSt 55, 138 ff.; *Bruns* in: Karlsruher Kommentar, StPO, § 110a Rn. 6; *Kirkpatrick*, Der Einsatz von verdeckten Ermittlern, 2011, S. 166; *Krause*, NStZ 2016, 139, 141; *Rosengarten/Römer*, NJW 2012, 1764, 1765.

[36] BVerfG NJW 2009, 1405, 1407; *Zöller* in: Heidelberger Kommentar, StPO, § 163 Rn. 1; *B. Gercke*, GA 2012, 474, 480 f.

[37] BVerfGE 120, 274, 345.

[38] So *Henrichs*, Kriminalistik 2011, 622, 624 f.; *Rosengarten/Römer*, NJW 2012, 1764, 1767.

[39] Vgl. BVerfGE 120, 274, 345 f.

Gegenübers in der Regel im Darknet gerade nicht ausgehen können.[40] Aufgrund der Vielseitigkeit der Nutzungsmöglichkeiten der verschiedenen Darknets sollte man aber nicht so weit gehen, einer Identität im Darknet pauschal jegliche Vertrauenswürdigkeit abzusprechen.[41] Sollte das schutzwürdige Vertrauen aufgrund der besonderen Umstände des Einzelfalles einmal bejaht werden,[42] wäre zu prüfen, ob dieses Vorgehen auf eine bereits bestehende Ermächtigungsgrundlage gestützt werden kann. Es käme dann ein sog. virtueller Verdeckter Ermittler zum Einsatz.

b) (Virtueller) Verdeckter Ermittler

aa) Ermittlungen unter einer bereits bestehenden Legende

Die einschlägige Ermächtigungsgrundlage für den Einsatz eines Verdeckten Ermittlers in der realen Welt ist die Vorschrift des § 110a StPO. Danach wird der ermittelnde Beamte unter einer sog. Legende i.S.d. Norm des § 110a Abs. 2 S. 1 StPO tätig.[43] Dazu werden etwa Tarnpapiere erstellt, unter denen er am Rechtsverkehr teilnehmen kann und darf (§ 110a Abs. 2 S. 2 StPO). Diese Papiere umfassen beispielsweise Ausweisdokumente.[44] Darin wird dem ermittelnden Beamten ein anderer Name verliehen, mit dem er sich u.a. in Bücher und Register eintragen darf.[45] Wenn der Beamte sich sogar in ein offizielles Register eintragen darf, ist es ihm auch erlaubt, sich unter dieser Legende im Darknet zu bewegen bzw. die Dienste des Darknets zu nutzen. Das anonyme Darknet hat insoweit eine deutlich geringere Außenwirkung, wie es z.B. beim Handelsregister der Fall ist. Das Tätigwerden im Darknet bedeutet insoweit lediglich die Nutzung eines zusätzlichen Ermittlungsinstruments unter einer bereits bestehenden Legende.

bb) Ermittlungen ohne bereits vorhandene Legende

Differenziert ist allerdings die Konstellation zu betrachten, in der eine Legende i.S.d. Vorschrift des § 110a Abs. 2 S. 1 StPO nicht vorliegt. Dies ist etwa dann der Fall, wenn sich der Beamte bloß in einem oder mehreren Diensten des Darknets unter einem Pseudonym registriert sowie anschließend mit anderen Nutzern in Kontakt tritt. Durch die Kommunikation mit anderen Personen im Darknet kann in deren Recht auf informationelle Selbstbestimmung eingegriffen werden, wenn sie schutzwürdig in die Identität ihres virtuellen Gegenübers vertrauen durften. Zwar ist die Kommunikation im Darknet grundsätzlich anonym, allerdings kann ein pauschaler Ausschluss der Vertrauenswürdigkeit der Kommunikation im Darknet nicht überzeugen. Gegebenenfalls könnte die Vertrauenswürdigkeit bei langanhaltenden Online-Beziehungen zu bejahen sein, die etwa zu einem oder mehreren Treffen in der realen Welt führen. Die Vertrauenswürdigkeit kann auch nicht pauschal ausgeschlossen werden, wenn etwa während der über einen langen Zeitraum geführten virtuellen Gespräche persönliche Details des eigenen Lebens bzw. der eigenen Identität ausgetauscht werden, sodass sich der Betroffene ein – schlüssiges – Bild über die Identität seines virtuellen Gegenübers machen kann.[46] Dies gilt insbesondere für die Nutzung anderer Darknets; es besteht eine Vielfalt an Nutzungsmöglichkeiten, sodass nicht generell davon ausgegangen werden kann, dass schutzwürdiges Vertrauen in keinem Darknet – also insbesondere einem anderen Darknet als dem Tor-Darknet – besteht. Es kommt letztlich auf die konkreten Umstände des Einzelfalles an.

Einen solchen Eingriff in das Recht auf informationelle Selbstbestimmung kann die Vorschrift des § 110a StPO grundsätzlich rechtfertigen. Darum nimmt auch ein Teil der Literatur an, dass Ermittlungen im Internet generell auf § 110a StPO gestützt werden können.[47] Eine beachtliche Gegenansicht fordert jedoch, dass der Gesetzgeber für den Einsatz eines virtuellen Verdeckten

---

[40] So *Krause*, NJW 2018, 678, 680.
[41] S. hierzu auch die Ausführungen unter III. 2. b) (2) sowie III. 3. d).
[42] Teilweise wird davon ausgegangen, dass im Darknet nur nicht offen ermittelnde Polizeibeamte zum Einsatz kommen: *Rath*, DRiZ 2016, 292 (293); so auch *Krause*, NJW 2018, 678, 680.
[43] Ausführlich zu den einzelnen Voraussetzungen für den Einsatz eines Verdeckten Ermittlers *B. Gercke* in: Heidelberger Kommentar, StPO, § 110a Rn. 12 ff. m.w.N.
[44] *Bruns* in: Karlsruher Kommentar, StPO, § 110a Rn. 10.
[45] *Bruns* in: Karlsruher Kommentar, StPO, § 110a Rn. 10.
[46] Das bloße Kommunizieren über einen längeren Zeitraum reicht nach Auffassung des Bundesverfassungsgerichts nicht aus. Denn jedem Teilnehmer sei bewusst, dass „er die Identität seiner Partner nicht kennt oder deren Angaben über sich jedenfalls nicht überprüfen kann" (BVerfGE 120, 274, 345). Es muss dementsprechend mehr als eine bloße zeitliche Komponente hinzukommen.
[47] *Bruns* in: Karlsruher Kommentar, StPO, § 110a Rn. 7; *Hauck* in: Löwe/Rosenberg, StPO, 26. Aufl. 2014, § 110a Rn. 26; *Römer/Rosengarten*, NJW 2012, 1764, 1767; für Ermittlungen in Sozialen Netzwerke halten § 110a StPO für anwendbar: *Drackert*, eucrim 2011, 122, 125 f.; *Soiné*, NStZ 2014, 248, 249 f.; vgl. außerdem BT-Drs. 17/6587, S. 5: Es handelt sich um eine Anfrage an die Bundesregierung, in der es um Ermittlungen in Sozialen Netzwerken geht. Die Bundesregierung gibt darin an, dass (virtuelle) Verdeckte Ermittler auf Grundlage der Vorschrift des § 110a StPO tätig würden; es habe insgesamt sechs Fälle in den letzten 24 Monaten gegeben.

Ermittlers bzw. für personale Ermittlungen im Internet eine neue und klare Regelung schaffen muss.[48] Dieser Ansicht ist für den Einsatz virtueller Verdeckter Ermittler im Darknet zuzustimmen. Jede Ermächtigungsgrundlage muss dem Bestimmtheitsgebot genügen, es muss klar ersichtlich sein, welche Maßnahmen auf sie gestützt werden dürfen. Die Anforderungen an die Normenklarheit und Tatbestandsbestimmtheit ergeben sich nach der Rechtsprechung des Bundesverfassungsgerichts für strafprozessuale Ermächtigungen – anders als für das materielle Strafrecht – aus dem Rechtsstaatsprinzip (Art. 20 Abs. 3, 28 Abs. 1 GG).[49] Die Voraussetzungen und die Rechtsfolge der Ermächtigungsnorm müssen dabei so klar formuliert sein, dass der Betroffene die Rechtslage erkennen und sein Verhalten danach ausrichten kann.[50] Das Bestimmtheitsgebot verlangt vom Gesetzgeber, dass dieser technische Eingriffsinstrumente genau bezeichnet und dadurch sicherstellt, dass der Adressat den Inhalt der Norm jeweils erkennen kann.[51] Diese Voraussetzungen sind aufgrund der Unterschiede zwischen virtueller Identität und realer Legende vorliegend nicht gegeben:

Zu der Legende eines Ermittlers gehören Name, Anschrift, Beruf, familiäre oder sonstige persönliche Umstände.[52] Diese Angaben werden grundsätzlich in einem vorzeigbaren Ausweisdokument festgehalten. Im anonymen Darknet ist es bereits unüblich, so viele Informationen über die eigene Person preiszugeben. Registriert man sich auf einem der Marktplätze, wird grundsätzlich nur gefordert, dass man einen Nickname – also ein Pseudonym – angibt. Dies ist aber nicht ausreichend für eine Legende. Selbst wenn der Beamte im Rahmen mehrerer Unterhaltungen mit anderen Nutzern des Darknets seine persönlichen Verhältnisse darstellt und sich so selbst einen fiktiven Namen, Beruf und dergleichen verleiht, ist dies mit der Schaffung einer tatsächlichen Legende, mit der er am Rechtsverkehr teilnehmen könnte, nicht vergleichbar. Die Teilnahme am Rechtsverkehr gemäß § 110a Abs. 2 S. 2 StPO ist mit einer erfundenen Identität im Darknet vielmehr gar nicht möglich; insbesondere eine Eintragung in einem Register könnte nicht auf Grundlage eines Pseudonyms erfolgen. Dies unterstreicht noch einmal die Unterschiedlichkeit von realem und virtuellem Verdeckten Ermittler.

Die Unanwendbarkeit des § 110a StPO wird auch dadurch belegt, dass die Norm in einem völlig anderen Kontext geschaffen wurde: Die Regelung des § 110a StPO wurde bereits im Jahre 1992 in die Strafprozessordnung eingefügt.[53] Die Vorschrift existierte somit lange Zeit bevor der Begriff „Darknet" überhaupt entstanden war – dies geschah erst zehn Jahre später. Die Norm wurde in die Strafprozessordnung eingeführt, um die Organisierte Kriminalität in der realen Welt zu bekämpfen. Sie bildet eine Ermächtigung für reale Treffen und nicht für eine nur virtuelle Begegnung. Die Grundkonstellation, die dem § 110a StPO zugrunde liegt, ist darum eine andere. In den Gesetzesmaterialien ist der Gesetzgeber zudem davon ausgegangen, dass der Einsatz eines Verdeckten Ermittlers „*hohen organisatorischen und finanziellen Aufwand*" erfordere.[54] Das bloße Anlegen eines Pseudonyms in einem Darknet-Marktplatz wird kaum diese Art von Aufwand erfordern. Dies belegt noch einmal, dass der Gesetzgeber ein anderes Tätigkeitsfeld eines Verdeckten Ermittlers vor Augen hatte.

Eine Anwendung des § 110a StPO als Ermächtigungsgrundlage für einen virtuellen Verdeckten Ermittler ist daher aus den vorgenannten Gründen abzulehnen. Eine andere Ermächtigungsgrundlage ist nicht ersichtlich, sodass es der Strafprozessordnung insoweit an einer Norm fehlt, auf die eine solche Ermittlungsmaßnahme gestützt werden kann.

c) Sonderfall 1: Agent Provocateur

Eine weitere personale Ermittlungsmaßnahme stellt die Nutzung eines sog. Agent Provocateur bzw. Lockspitzels dar. Obgleich Zweifel an der Zulässigkeit jeglicher staatlicher Tatprovokation bestehen,[55] ist es dennoch in Rechtsprechung und Literatur weitestgehend anerkannt, dass diese Maßnahme auf die Generalermächtigungsklausel (§§ 161, 163 StPO) gestützt werden kann.[56]

---

[48] *Petri* in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 5. Aufl. 2012, S. 835 f.; *Zöller* in: Heidelberger Kommentar, StPO, § 163 Rn. 12; *Brenneisen/Staack*, Kriminalistik 2012, 627, 630; *Henrichs*, Kriminalistik 2012, 632, 635; *ders./Wilhelm*, Kriminalistik 2010, 30, 35; vgl. zu einem konkreten Vorschlag zu einer Ermächtigungsgrundlage für den virtuellen Verdeckten Ermittler in Sozialen Netzwerken: *Ihwas*, Strafverfolgung in Sozialen Netzwerken, 2014, S. 172.
[49] BVerfG NJW 2005, 1338, 1339.
[50] BVerfG NJW 2005, 1338, 1339 m.w.N.
[51] BVerfGE 87, 287, 317 f.; BVerfG NJW 2005, 1338, 1340.
[52] *B. Gercke* in: Heidelberger Kommentar, StPO, § 110a Rn. 7.
[53] BGBl. I v. 22.07.1992, S. 1302.
[54] BT-Drs. 12/989, S. 41.
[55] Zutreffend krit. zum Agent Provocateur: *Kölbel* in: Müchener Kommentar, StPO, 2016, § 163 Rn. 25 ff.
[56] BGHSt 32, 345; *Griesbaum* in: Karlsruher Kommentar, StPO, § 163 Rn. 18; Meyer-Goßner/*Schmitt*, StPO, 60. Aufl. 2017, § 163 Rn. 34a f.; konkret für den Einsatz eines Agent Provocateur in Sozialen Netzwerken: *Soiné*, NStZ 2014, 248, 250.

Hierzu ist erforderlich, dass ein bereits bestehender starker Verdacht schwerwiegenden strafbaren Verhaltens auf seine Richtigkeit geprüft werden soll.[57] Es ist nicht zulässig, den – späteren – Täter erst durch nachhaltige Einflussnahme zur Tat zu bestimmen (sog. „Quantensprung").[58] Von einem Agent Provocateur kann insbesondere dann auszugehen sein, wenn ein Ermittler zum Schein Drogen oder Waffen im Darknet zum Kauf anbietet.[59] Dabei ist allerdings zu beachten, dass dieses Kaufangebot nur gegenüber Personen unterbreitet werden darf, die verdächtig sind, entsprechende Delikte zu planen oder darin verwickelt zu sein.[60] Dies kann etwa der Fall sein, wenn es eine konkrete Nachfrage zum Kauf von Waffen in einem Darknet-Forum gibt.

d) Sonderfall 2: Übernahme eines bereits bestehenden Accounts

Durch die Übernahme bestehender Accounts können Strafverfolgungsbehörden tief in bereits bestehende Strukturen von Nutzergruppen innerhalb des Darknets eintreten. Bei der Beurteilung der Zulässigkeit einer solchen Maßnahme kommt es stets auf die konkreten Umstände des Einzelfalles an. Bei der Übernahme ist etwa zu unterscheiden, ob dies mit oder ohne Einwilligung des Betroffenen geschieht. Die Nutzung bestehender Accounts mit Einwilligung des Betroffenen spricht jedenfalls grundsätzlich für die Zulässigkeit der Maßnahme, die aufgrund der Generalermächtigungsklausel durchgeführt werden kann.[61] Gegen die Zulässigkeit der Maßnahme kann sprechen, dass der Betroffene mit der Nutzung seines Accounts hingegen nicht einverstanden ist. Bei der Bewertung der Zulässigkeit wird man außerdem berücksichtigen müssen, ob der Kommunikationspartner schutzwürdig in die Identität seines virtuellen Gegenübers vertrauen darf. Jedenfalls sollte man – wie erörtert - nicht so weit gehen, einer Identität im Darknet pauschal jegliche Vertrauenswürdigkeit abzusprechen.[62] Gerade in der vorliegenden Konstellation ist es denkbar, dass das Darknet nur als zusätzlicher Kommunikationsweg genutzt wird und sich etwaige Kommunikationspartner auch im realen Leben kennen, sodass eine Vertrauenswürdigkeit nicht generell ausgeschlossen werden kann. Da hier jedenfalls im Raum steht, dass sowohl in das Recht auf informationelle Selbstbestimmung des Betroffenen als auch dessen Kommunikationspartner eingegriffen werden könnte, kann es sich in einem solchen Fall nicht mehr um einen nur geringfügigen Eingriff handeln, der durch die Generalermächtigungsklausel gerechtfertigt werden kann. In diesem Falle wären die Vorschriften der §§ 161, 163 StPO keine geeignete Ermächtigungsgrundlage. Dass dies auch für die Norm des § 110a StPO gilt, wurde bereits oben dargestellt, sodass es auch hier insoweit an einer tauglichen Ermächtigungsgrundlage in der Strafprozessordnung fehlt.

4. Herausgabeersuchen von Bestands-, Verkehrs- oder Nutzungsdaten

Ein Herausgabeersuchen von Bestands-, Verkehrs- oder Nutzungsdaten ist aufgrund der verschlüsselten Verbindung nicht geeignet, für die Ermittlung weiterführende Erkenntnisse zu liefern.[63] Access-Provider können aufgrund des zwiebelförmigen Aufbaus der Verschlüsselungsstruktur die Zielwebseite nicht erkennen. Es kann auf diese Weise also bereits nicht der Nachweis geführt werden, dass eine bestimmte Webseite im Darknet aufgerufen wurde. Des Weiteren sind die Betreiber der verschiedenen Marktplätze im Darknet in der Regel nicht bekannt, sodass an diese ohnehin keine Herausgabeersuchen gerichtet werden können.

5. Folgeermittlungen außerhalb der digitalen Welt

Das Darknet bietet wenig Anknüpfungspunkte, um einen Täter nur mit digitalen Hinweisen zu überführen; etwaige digitale Spuren sind schwer bis gar nicht zurückzuverfolgen. So geschieht auch die Zahlung im Darknet mittels sog. Kryptowährungen, wie beispielsweise Bitcoins, die ebenfalls Anonymität garantieren, sodass auch der Zahlungsweg im Darknet grundsätzlich nicht zurückverfolgt werden kann.[64] Darum ist es häufig so, dass der zuvor beschriebene nicht offen

---

[57] BGHSt 32, 345; *Griesbaum* in: Karlsruher Kommentar, StPO, § 163 Rn. 18.
[58] BGH NJW 1981, 1626 f.
[59] Zur aktiven Generierung von Ermittlungsansätzen vgl. *Krause*, NJW 2018, 678, 679 f.
[60] BGH NStZ 1995, 506; *Soiné*, NStZ 2014, 248, 250 m.w.N.; anderenfalls wäre der Einsatz des Agent Provocateur unzulässig; die Folgen hiervon sind umstritten, vgl. hierzu *Zöller* in: Heidelberger Kommentar, StPO, § 163 Rn. 16.
[61] *Krause*, NJW 2018, 678, 680.
[62] So aber *Krause*, NJW 2018, 678, 680.
[63] So auch ausdrücklich das BKA in einer Presseinformation vom 27.07.2016. *Krause*, NJW 2018, 678, 679, bezeichnet technische Ermittlungen im Darknet als „regelmäßig aussichtslos". Es wird teilweise behauptet, dass die sog. Eingangsnodes ins Tor-Darknet durch Nachrichten- bzw. Geheimdienste überwacht würden. Der Eingangsnode ist der erste Server, mit dem sich der Nutzer verbindet, wenn er das Darknet betritt. Dieser Eingangsserver „kennt" daher auch die IP-Adresse des Nutzers, der gerade das Darknet betritt. Es ist nicht ersichtlich, dass deutsche Strafverfolgungsbehörden einen Eingangsserver ins Darknet überwachen.
[64] S. zur Funktionsweise des Bitcoin-Systems *Brenneis*, APuZ 2017, 29 ff.; *Goger*, MMR 2016, 431 ff.; zur steuer(straf-)rechtlichen Behandlung von Kryptowährungen s. *Gerst*,WI-J 2017, S. 171 ff.

ermittelnde Polizeibeamte bzw. Lockspitzel Kontakt zu Käufern bzw. Verkäufern illegaler Waren aufnimmt und diese dann in der realen Welt überführt werden. Denn die Ware muss letztlich zum Käufer bzw. Konsumenten gelangen, was einen physischen Vorgang darstellt, der über das Darknet nicht vollzogen werden kann. Dazu wird die Ware in der Regel auf dem Postweg an eine Packstation[65] oder einen fremden Briefkasten verschickt. Diese Orte können durch Strafverfolgungsbeamte observiert werden, um so festzustellen, wer die illegale Ware abholt. Aber auch wenn Strafverfolgungsbeamte als Käufer auftreten, können sie anhand der versandten Ware versuchen, Fingerabdrücke zu erhalten oder andere weiterführende Spuren. Über diesen Weg werden die Täter dann letzten Endes überführt.

IV. Fazit und Ausblick

Ein Großteil der Ermittlungsmaßnahmen im Darknet kann – noch – auf die Generalermächtigungsklausel gestützt werden. Die Strafprozessordnung stößt aber insbesondere beim Einsatz von virtuellen Verdeckten Ermittlern an ihre Grenzen, sodass keine Ermächtigungsgrundlage vorhanden ist, wenn der ermittelnde Beamte ohne eine bestehende Legende i.S.d. Vorschrift des § 110a Abs. 2 S. 1 StPO tätig wird. Aufgrund der Anonymität des Darknets sind technische Ermittlungsmethoden, insbesondere Herausgabeverlangen von Bestands-, Verkehrs- und Nutzungsdaten, in der Regel nicht erfolgversprechend. Daher bedarf es Ermittlungen in der realen Welt, um Beweise für eine Täterschaft des Betroffenen zu erlangen.

Die Ermittlungsmaßnahmen im Darknet beschäftigen auch die Justizminister der Bundesländer und den Rat der Europäischen Union, die ihre Ermittlungsbemühungen im Darknet verstärken wollen.[66] Auf der Justizminiserkonferenz 2018 wurde sogar ein Beschluss erlassen, worin es heißt, dass *„die Verwendung computergenerierten Materials eine wirksame und zugleich Individualrechtsgüter schonende Methode sein kann, um im Bereich der Kinderpornographie Täter zu ermitteln"*.[67] Dies zeigt, welche Brisanz das Thema Darknet derzeit hat.

Das Darknet gewinnt – nicht zuletzt aufgrund seiner dauernden medialen Präsenz – stetig mehr Nutzer. So haben bereits im April 2016 mehr als eine Millionen Nutzer die Facebook-Präsenz im Darknet genutzt.[68] Das Darknet taucht aber auch in der strafgerichtlichen Judikatur immer häufiger auf, weil es etwa als Tatwerkzeug genutzt wurde.[69] Ob sich das Darknet nun als „digitale Unterwelt" darstellt, hängt letztlich von der konkreten Art der Nutzung ab. Denn das Darknet wird nicht nur von Kriminellen genutzt, sondern ermöglicht auch die anonyme Kommunikation für Oppositionelle oder Journalisten in totalitären Staaten und bietet diesen damit unverzichtbaren Schutz. Darüber hinaus schützt es Personen, die Missstände anzeigen wollen, aber ohne Verschleierung ihrer Identität Repressalien zu befürchten haben.[70] Letztlich wird aber auch Datenschutz und damit Anonymität im Internet für jeden einzelnen Bürger immer wichtiger. Niemand möchte zum „gläsernen Menschen" werden. Gerade im heutigen Zeitalter von „Big Data" und dem „Internet of Things" wird darum die Möglichkeit der anonymen Kommunikation einen immer größeren positiven Nutzen haben, sodass das Darknet insoweit jedenfalls auch seine gute Seite hat.

---

[65] S. zur retrograden Auskunft BGH, Beschl. v. 27.10.2016 – 1 BGs 107/16 (m. abl. Anm. *Krause*, NZWiSt 2017, 60); generell zu strafprozessualen Auskunftsersuchen über Postsendungen s. *Weisser*, wistra 2016, 387 ff.; s. a. den Beschluss der Justizministerkonferenz vom 21./22.06.2017 zu „TOP II.3 Auskunftsverlangen gegenüber Postdienstleistern", worin eine klarstellende Regelung gefordert wird, nach der es zulässig sein soll, von Postdienstleistern „Auskünfte auch über noch nicht ein- sowie bereits ausgelieferte Sendungen zu verlangen" (online abrufbar unter: https://jm.rlp.de/fileadmin/mjv/Jumiko/Fruehjahrskonferenz_neu/II.3_Auskunftsverlangen_gegenueber_Postdienstleistern.pdf).

[66] Vgl. zur Herbstkonferenz der Justizminister vom 17.10.2016: FD-StrafR 2016, 384048.

[67] Der Beschluss ist abrufbar unter: http://www.jm.nrw.de/JM/jumiko/beschluesse/2018/Fruehjahrs konferenz_2018/II-9-BY---Effektive-Verfolgung-und-Verhinderung-von-Kinderpornografie-und-Kindesmissbrauch-im-Darknet.pdf. Vgl. zur zutreffenden ablehnenden Haltung gegenüber dem Begehen milieubedingter Straftaten bei personalen Ermittlungen im Darknet *Krause*, NJW 2018, 678, 680.

[68] https://www.facebook.com/notes/facebook-over-tor/1-million-people-use-facebook-over-tor/865624 066877648/.

[69] Vgl. nur LG München I, Urt. v. 19.01.2018 – 12 KLs 111 Js 239798/16; AG Iserlohn, Beschl. v. 10.3.2017 – 16 Ds 139/17; LG Stuttgart, Urt. v. 3.11.2016 – 18 KLs 242 Js 121202/15; LG Heidelberg, Urt. v. 28.7.2016 – 2 KLs 430 Js 26796/14.

[70] S. zur *„hellen Seite im Darknet"*: *Moßbrucker*, APuZ 2017, 16 ff.