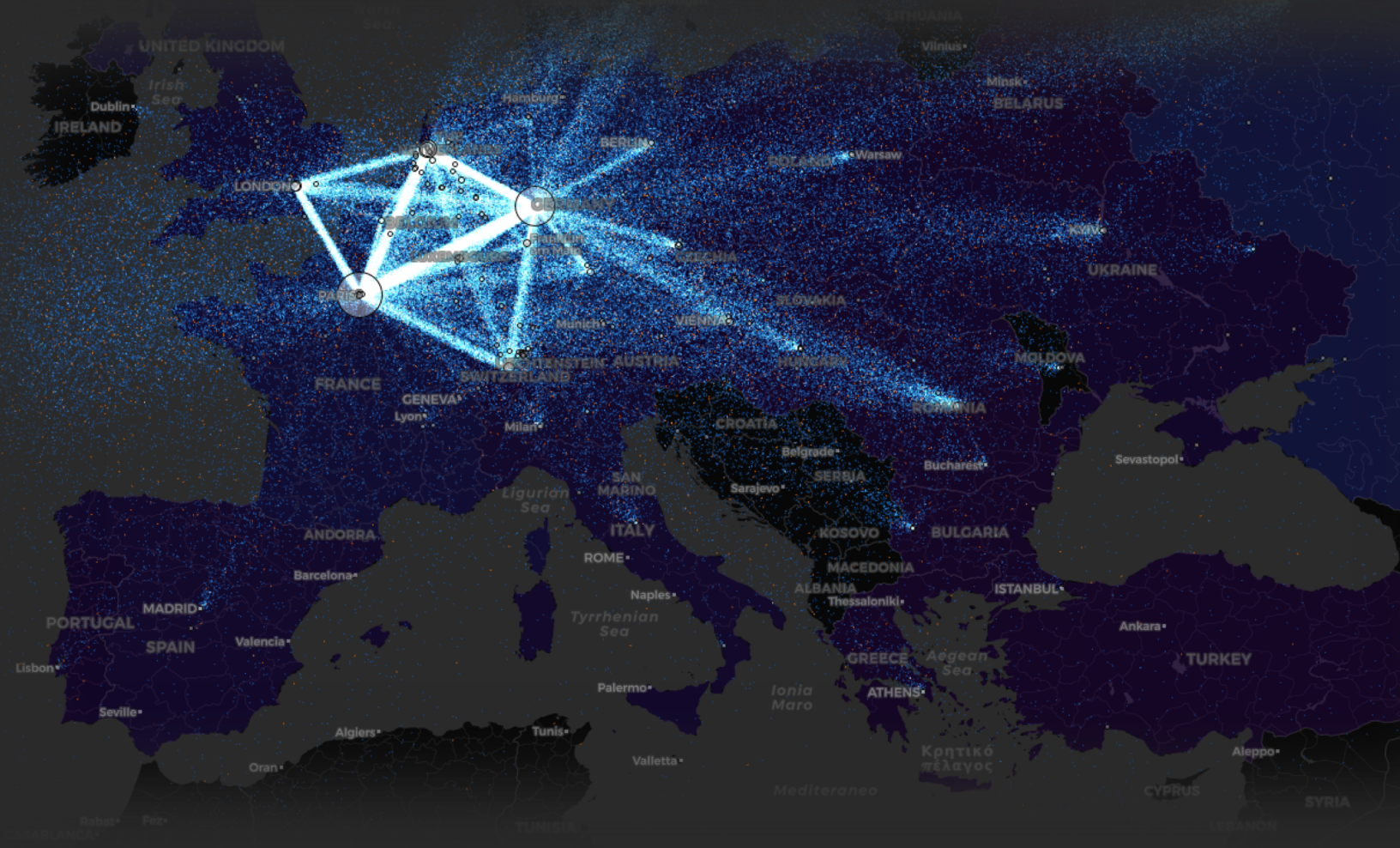


Screenshot: https://torflow.uncharted.software/

Angriff auf die Anonymität im Internet

Folgen des sogenannten “Darknet-Paragraphen” als § 126a Strafgesetzbuch für die rechtliche Praxis – und Kollateralschäden seines Einsatzes für die Presse-, Meinungs- und Telekommunikationsfreiheiten

Moritz Bartl, Zwiebelfreunde e.V.
Daniel Moßbrucker, Reporter ohne Grenzen e.V.
Dr. Christian Rückert, Friedrich-Alexander Universität Erlangen-Nürnberg

Zusammenfassung

Mit dem sogenannten “Darknet-Paragrafen” in der geleakten Version zum IT-Sicherheitsgesetz 2.0 gibt das Bundesinnenministerium vor, den Betrieb sogenannter “Darknet-Marktplätze” unter Strafe zu stellen und damit eine Lücke im deutschen Strafrecht zu schließen. Tatsächlich aber wird auch das Engagement für Anonymität kriminalisiert und ein abschreckender Effekt für den Betrieb und die Nutzung von Anonymisierungsdiensten wenn nicht intendiert, so doch billigend in Kauf genommen. Diese Diskussion über den “Darknet-Paragrafen” hat unter deutschen Betreiber:innen von Tor-Knoten zu Verunsicherung geführt, weil gegen sie durch den bloßen Betrieb der Infrastruktur ein Anfangsverdacht hergestellt werden kann.

Die in der Gesetzesbegründung aufgestellte These für die Notwendigkeit des § 126a StGB-Entwurf hält einer rechtswissenschaftlichen Analyse nicht Stand. Anders als postuliert bestehen keine entsprechenden Lücken. Stattdessen sind gerade die typischen “Darknet-Delikte” wie Betäubungsmittelhandel, Waffenhandel oder die Verbreitung kinder- und jugendpornografischer Schriften erschöpfend geregelt. Die in der Gesetzesbegründung aufgestellte These, wonach den Betreiber:innen von Handelsplattformen eine Beihilfe nur schwer nachgewiesen werden kann, ist nicht haltbar. Soweit nämlich die strafbarkeitsbegrenzenden Normen der §§ 8 - 10 Telemediengesetz (TMG) bereits heute auf Fallkonstellationen im „Darknet“ angewendet werden können[1], würde dies auch nach einer Einführung des § 126a StGB für diesen gelten. Insofern würde § 126a StGB keine spürbare Verbesserung der strafrechtlichen Erfassung von Plattform-Betreiber:innen bringen.

Weil die Norm nicht auf bestimmte Internetdienste respektive bestimmte Straftaten begrenzt werden soll, ist vielmehr zu befürchten, dass die Norm nahezu nach Belieben angewendet werden kann – zum Beispiel auch gegen Meinungsäußerungsdelikte im Internet. Dies ist umso gravierender, weil die Tatbestandsausnahmen für die Praxis letztlich ins Leere laufen. Im Ergebnis der juristischen Analyse steht damit fest, dass mit Hilfe des „Darknet-Paragrafen“ viele Tätigkeiten kriminalisiert werden können, die für die Gesellschaft eigentlich wünschenswert sind.

Hierzu zählen insbesondere Dienste, die eine anonyme oder pseudonyme Nutzung des Internets ermöglichen, beispielsweise das Tor-Netzwerk oder VPN-Provider. Ein Blick in die Realität des „Darknet“ zeigt, dass angesichts der extrem eng formulierten Tatbestandsausnahmen des § 126 a Abs. 4 StGB-Entwurf letztlich wohl nur anonyme Briefkästen erfasst würden, die von Medien selbst betrieben werden. Dies erfasst in der Praxis nur sogenannte Secure Drops – und klammert diverse Dienste aus, die auf der Onion-Technologie basieren. Viele von ihnen haben hohe Relevanz für die Arbeit von Medien. Zu nennen ist Wikileaks, welches nicht ausschließlich für journalistische Zwecke verwendet wird, jedoch bis heute über 100 Medien auf der ganzen Welt als Partner zählt, darunter zahlreiche in Deutschland. Für die Praxis bedeutend ist auch die Möglichkeit, über das „Darknet“ anonym Daten auszutauschen. Das Programm “Onion Share”, mit dem Korrespondent:innen in gefährlichen Gebieten vollends anonym auch größere Datenmengen übertragen können, ist gerade bei Exilmedien beliebt. Gravierend ist ferner, dass der bloße Betrieb von Tor-Knoten mittels des “Darknet-Paragrafen” kriminalisiert werden kann.

[1] Zum Beispiel § 8 TMG für Tor-Knoten-Betreiber:innen und – allerdings strittig – § 10 TMG für Betreiber:innen von „Darknet-Handelsplattformen“.

Selbst wenn eine solche Behinderung journalistischer Arbeit mit dem neuen § 126 a StGB-Entwurf vom Gesetzgeber nicht intendiert sein mag, dürfte die Kriminalisierung weiter Teile des Internets enorme Kollateralschäden mit sich bringen. Zu nennen sind insbesondere Chilling Effects von Personen, die diese Dienste nutzen und Angst haben, allein dadurch ins Fadenkreuz von Ermittlungen zu geraten.

Diese Sorge vor strafrechtlichen Repressalien gilt in gesteigerter Form für deutsche Betreiber:innen der Anonymisierungsdienste selbst: Mittels des "Darknet-Paragrafen" kann ihr Engagement für Anonymität kriminalisiert werden, nur weil sie einen Tor-Relay betreiben. Dies kann zu einer Abschreckung führen, was gerade für Deutschland problematisch ist. Denn die Zahl an Unterstützer:innen für das Tor-Netzwerk ist hier besonders hoch – und ein Rückgang ihres Engagements für den Erhalt des Netzwerks besonders problematisch. Deutschland steht weltweit an erster Stelle was die Gesamtkapazität des Netzwerks betrifft, denn aktuell laufen über 30 Prozent des Tor-Netzverkehrs über deutsche Server. Derzeit gibt es über 1300 Knoten allein in Deutschland, wovon über 100 auch als Exit-Knoten fungieren.[2]

Unter den Betreiber:innen dieser Knoten werden diese Pläne zum "Darknet-Paragrafen" seit Wochen diskutiert. Der Verein Zwiebelfreunde, der selbst einer der größten Betreiber von anonymen Infrastrukturen ist und auch Beratungen in diesem Bereich anbietet, erhielt bereits mehrere Anfragen von Betreiber:innen, die durch den Gesetzesentwurf verunsichert sind. Diese Personen sorgen sich, dass ihr Engagement rechtliche Folgen für sie haben könnte. Zwar mögen die §§ 8 - 10 TMG Schutz vor einer strafrechtlichen Verurteilung bieten, doch es ist zu befürchten, dass § 126a StGB-Entwurf die Begründung eines Anfangsverdachts gegen zahlreiche Anbieter:innen von Internetdienstleistungen ermöglicht und diese zum Ziel von grundrechtseingreifenden Ermittlungsmaßnahmen macht. Es ist in der Praxis wenig tröstlich, wenn Server zunächst beschlagnahmt werden und sich dann Monate später herausstellt, dass die Maßnahmen unbegründet waren. Genau dies ist Vertretern der Zwiebelfreunde im Jahr 2018 passiert.

Die Autoren empfehlen, § 126a StGB-Entwurf weder in der geleakten Fassung des IT-Sicherheitsgesetzes 2.0 noch in der vom Bundesrat verabschiedeten Fassung zu beschließen. Zur Verbesserung der Verfolgung und Bekämpfung der Kriminalität im „Darknet" sollte vielmehr eine personelle und technische Aufstockung der auf Internetkriminalität spezialisierten Strafverfolgungsbehörden und der Justiz – inklusive der Einrichtung von speziellen Cybercrime-Kammern an den Landgerichten – erfolgen und die Entwicklung von effektiven, aber gleichzeitig grundrechtsschonenden Ermittlungswerkzeugen vorangetrieben werden.

[2] vgl. Tor Metrics, URL: https://metrics.torproject.org/rs.html#aggregate/cc, zuletzt aufgerufen am 03. Juli 2019.

Inhalt

Fokus der Stellungnahme

Diese Stellungnahme untersucht die grund- und menschenrechtlichen Auswirkungen des vorgeschlagenen 126a StGB-Entwurf und beleuchtet, welche negativen Kollateralschäden dieser für die Arbeit von Medien und die Privatsphäre aller Bürger:innen haben könnte. Werden andere Gesichtspunkte des 126a StGB-Entwurf in dieser Analyse nicht angesprochen, so ist dies nicht dahingehend zu interpretieren, dass sie als unbedenklich anzusehen wären.

Den Begriff „Darknet“ verwenden die Autoren, weil dieser durch die Gesetzesbegründung und die öffentliche Debatte de facto gesetzt ist. Verstanden wird hierunter die Onion Service-Technologie im Tor-Netzwerk.

Juristische Analyse: Kriminalisierung des gesamten Internets?

Der im IT-Sicherheitsgesetz 2.0 untergebrachte § 126a StGB-Entwurf hat bereits jetzt eine kurze, aber bemerkenswerte Gesetzgebungsgeschichte. Zunächst wurde von Nordrhein-Westfalen im Bundesrat ein Gesetzentwurf[3] eingebracht, der deutlich mehr Einschränkungen hinsichtlich der Strafbarkeit enthielt als der jetzige Entwurf. So waren nicht alle internetbasierten Dienstleistungen erfasst, sondern nur solche, "deren Zugang und Erreichbarkeit durch besondere technische Vorkehrungen beschränkt" sind. Damit sollte nach dem Willen der Verfasser eine Beschränkung auf das „Darknet" erreicht werden. Außerdem enthielt die Vorschrift einen Straftatenkatalog, der sich auf die in der Strafverfolgungspraxis relevantesten, typischen "Darknet-Delikte" (z.B. Handel mit Betäubungsmitteln und Waffen, Geldfälschungs- und Datendelikte) beschränkte.

Als Reaktion hierauf brachte Bayern einen konkurrierenden Entwurf[4] in den Bundesrat ein, der dem jetzt im IT-Sicherheitsgesetz verwendeten Entwurf exakt entsprach. Der verschärfte bayerische Vorschlag scheiterte jedoch in der Abstimmung und der Vorschlag von Nordrhein-Westfalen wurde vom Bundesrat als Gesetzentwurf verabschiedet.[5] Das Bundesinnenministerium hat nunmehr – trotz der bereits erfolgten politischen Willensäußerung des Bundesrats – den schärferen Entwurf aus Bayern aufgegriffen und diesen wortlautgleich in den Entwurf für das IT-Sicherheitsgesetz 2.0 aufgenommen.[6]

Die folgende juristische Analyse des nun vorliegenden § 126a StGB-Entwurf aus dem Entwurf für ein IT-Sicherheitsgesetz 2.0 wird zeigen, dass

(1) derzeit keine relevante Strafbarkeitslücke vorhanden ist, die durch eine neue Strafnorm geschlossen werden müsste,

(2) der Entwurf zu einer massiven Ausweitung der Vorfeldstrafbarkeit im Internet führt und in vielen Fällen nicht strafwürdiges Verhalten kriminalisiert und

(3) die im Entwurf enthaltenen Strafbarkeitsbeschränkungen nicht ausreichen, um Kollateralschäden an gesellschaftlich und politisch bedeutsamen Betätigungen zu vermeiden.

---

[3] vgl. Bundesrat DS 33/19 (2019, 18. Januar): Gesetzesantrag des Landes Nordrhein-Westfalen. Entwurf eines Strafrechtsänderungsgesetzes – Einführung einer eigenständigen Strafbarkeit für das Betreiben von internetbasierten Handelsplattformen für illegale Waren und Dienstleistungen. URL: https://www.bundesrat.de/SharedDocs/drucksachen/2019/0001-0100/33-19.pdf?__blob=publicationFile (zuletzt aufgerufen am: 03. Juli 2019).

[4] vgl. Bundesrat DS 33/1/19 (2019, 01. März): Empfehlungen der Ausschüsse zu Punkt … der 975. Sitzung des Bundesrates am 15. März 2019. URL: https://www.bundesrat.de/SharedDocs/drucksachen/2019/0001-0100/33-1-19.pdf?__blob=publicationFile (zuletzt aufgerufen am: 03. Juli 2019).

[5] vgl. Meister, Andre (2019, 15. März): Bundesrat bringt "Darknet"-Gesetz auf den Weg. URL: https://netzpolitik.org/2019/bundesrat-bringt-darknet-gesetz-auf-den-weg/ (zuletzt aufgerufen am 03. Juli 2019).

[6] vgl. Meister, Andre / Biselli, Anna (2019, 03. April): IT-Sicherheitsgesetz 2.0: Wir veröffentlichen den Entwurf, der das BSI zur Hackerbehörde machen soll. URL: https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/ (zuletzt aufgerufen am 03. Juli 2019).

Vermeintliche Lücken im Strafrecht, die nicht bestehen

Mit dem Entwurf sollen vermeintliche und aus Strafverfolgungskreisen beklagte Strafbarkeitslücken[7] für die Betreiber:innen von sog. „Darknet-Handelsplätzen“ und anderen Internetplattformen geschlossen werden. Diese Strafbarkeitslücken existieren nicht bzw. jedenfalls nicht in relevantem Umfang. In den praktisch bedeutsamsten Deliktsgruppen sind bereits Strafnormen mit sehr weitem Anwendungsbereich vorhanden, welche die Tätigkeit der Plattform-Betreiber:innen hinreichend erfassen.[8]

So ist z.B. das "Handeltreiben" mit **Betäubungsmitteln** i.S.v. § 29 Abs. 1 Nr. 1 Betäubungsmittelgesetz (BtMG) von der Rechtsprechung definiert als "jedes eigennützige Bemühen, das darauf gerichtet ist, den Umsatz von Betäubungsmitteln zu ermöglichen oder zu fördern"[9]. Von dieser extrem extensiven Auslegung ist bereits die Vermittlung von Geschäften mit Betäubungsmitteln umfasst. Wer eine „Darknet-Plattform“ betreibt, auf der andere Personen mit Drogen handeln, vermittelt solche Geschäfte und ist dementsprechend von der Vorschrift erfasst. Auch die “Eigennützigkeit” des Tuns wird von der Rechtsprechung denkbar weit interpretiert. Eigennützig handelt hiernach, “wem es auf seinen persönlichen Vorteil, insbesondere auf die Erzielung von Gewinn ankommt”[10].

Die meisten Handelsplattformen – insbesondere diejenigen, welche als professionell organisierte und gewinnorientierte Plattformen der sog. Underground Economy zugerechnet werden können – verfügen über Provisions- und Treuhandsysteme,[11] sodass in diesen Fällen unproblematisch auch die Eigennützigkeit bejaht werden kann. Daneben werden von der Rechtsprechung auch immaterielle Vorteile (z.B. (sexuelle Gefälligkeiten, Zahlungen an Familienmitglieder) einbezogen, wenn diese einen “objektiv messbaren Inhalt” haben und den Empfänger “tatsächlich besser stellen”.[12] Die anerkannten Fallgruppen dürften jedoch im „Darknet-Drogenhandel“ keine Rolle spielen. Insbesondere nicht erfasst sind damit Plattform-Betreiber:innen, welche die Plattform nur aus ideellen (Ermöglichung völlig unbeschränkten Handels) oder persönlichen (Erhöhung des Ansehens in der “Szene”) Motiven betreiben. In diesen Fällen verbleibt aber noch eine Strafbarkeit nach § 29 Abs. 1 Nr. 10 BtMG. Dieser stellt die Verschaffung oder öffentliche Mitteilung einer Gelegenheit zum Erwerb oder zur Abgabe von Betäubungsmitteln unter Strafe. Daneben sind die Betreiber:innen außerdem wegen Beihilfe zum Handeltreiben strafbar (dazu siehe noch unten).

Im **Waffenhandel** ist gem. § 52 Abs. 1 Nr. 1 Nr. 2 c) Waffengesetz (WaffG) i.V.m. Anlage 1 Abschnitt 2 Nr. 9 bereits die Vermittlung des Vertriebs von Waffen strafbar, worunter der Betrieb von Handelsplattformen für Drittverkäufer ohne weiteres subsumiert werden kann.

Im Bereich der **Verbreitung von Kinder- und Jugendpornographie** sind die Tathandlungsvarianten der §§ 184b ff. StGB ebenfalls sehr weit ausgestaltet. Für den Fall, dass

---

[7] vgl. Fiebig, Peggy (2019, 9. März): Wann ist der Betrieb einer Plattform strafbar? Regulierung des Darknet. URL: https://www.deutschlandfunkkultur.de/regulierung-des-darknet-wann-ist-der-betrieb-einer.1264.de.html?dram:article_id=443130 (zuletzt aufgerufen am 03. Juli 2019).

[8] Zum Folgenden bereits: Safferling/Rückert (2018): Das Strafrecht und die Underground Economy, in: Konrad-Adenauer-Stiftung (Hrsg.), Analysen & Argumente 291.

[9] BGHSt 29, 239; 50, 252; BVerfG NJW 2007, 1193.

[10] BGHSt 28, 308 (309); 34, 124 (126).

[11] Safferling/Rückert (2018): Das Strafrecht und die Underground Economy, in: Konrad-Adenauer-Stiftung (Hrsg.), Analysen & Argumente 291.

[12] BGH NStZ 1982, 384; NStZ-RR 2000, 234.

der Plattform-Betreiber/die Plattformbetreiberin selbst tatsächlich gar nicht mit den Inhalten in Kontakt kommt, verbleibt zumindest noch das “Bewerben” als Tathandlung (§§ 184b Abs. 1 Nr. 4 Var. 6, 184c Abs. 1 Nr. 1 Var. 6 StGB). Hierunter fällt nach der Rechtsprechung auch die reine Information über Bezugsquellen oder Betrachtungsmöglichkeiten, wobei auch das Bewerben durch Dritte genügt, die selbst nicht über die entsprechenden Darstellungen verfügen.[13] Mithin sind zumindest von dieser Tathandlungsvariante alle derzeit gängigen Plattformmodelle erfasst, auf denen kinderpornographische Videos und Bilder angeboten werden.

Für die wenigen praxisrelevanten Bereiche, in denen keine so weiten Deliktsnormen vorhanden sind (z.B. **Geldfälschungsdelikte, Datendelikte**) verbleibt noch die Strafbarkeit der Plattform-Betreiber:innen wegen Beihilfe gem. § 27 StGB. Hiernach steht allgemein die Förderung oder Ermöglichung fremder Straftaten unter Strafe, nach der Rechtsprechung sogar unabhängig davon, ob die fremde Straftat ohne die Beihilfehandlung nicht genauso hätte begangen werden können.[14] Diese Norm des Allgemeinen Teils des StGB gilt für alle Delikte und erfasst damit auch das Betreiben von (Internet-)Infrastruktur zur Ermöglichung von Straftaten durch Dritte Personen.

Soweit aus Kreisen der Strafverfolgungsbehörden bemängelt wird[15], der hierfür notwendige Vorsatz der Plattform-Betreiber:innen lasse sich häufig nicht nachweisen, ist dies nicht nachvollziehbar. Wie sonst auch, genügt der sog. Eventualvorsatz, der bereits vorliegt, wenn die Plattform-Betreiber:innen mit der Möglichkeit rechnen, dass auf ihrer Plattform Straftaten begangen werden und sie die Begehung dieser Straftaten billigend in Kauf nehmen. Gerade bei § 27 StGB genügt hierfür nach der Rechtsprechung, wenn der Gehilfe dem Täter willentlich ein entscheidendes Tatmittel zur Verfügung stellt und damit bewusst das Risiko erhöht, dass durch den Einsatz des Tatmittels eine "typischerweise" geförderte Haupttat verübt wird.[16] Wann diese Kriterien beim Betrieb einer „Darknet-Handelsplattform“ für den Handel mit illegalen Gütern nicht vorliegen sollen, erschließt sich nicht. Liegen sie nicht vor, erschließt sich nicht, warum strafwürdiges Verhalten vorliegen soll.

Exemplifizieren lässt sich dies an der Entscheidung des LG Karlsruhe zum Fall “Deutschland im Deep Web”. Dort hatte das LG eine Strafbarkeit des Betreibers allein wegen der Inbetriebnahme der Plattform deshalb verneint, weil die Plattform gerade nicht von Anfang an ausschließlich oder überwiegend auf die Förderung der Begehung von Straftaten durch andere ausgerichtet war und deshalb eine neutrale, sozial-adäquate Handlung und keine Beihilfe vorgelegen habe. Obwohl das LG keine einzelnen Verkäufe von Betäubungsmitteln nachweisen und noch nicht einmal die potentiell beteiligten Nutzer identifizieren konnte, wertete es bereits das Einstellen von Preislisten und Lichtbildern von Betäubungsmitteln als “Werben” für Betäubungsmittel iSv § 29 Abs. 1 S. 1 Nr. 8 BtMG. Der Angeklagte habe hierzu Beihilfe geleistet. Und zwar zum einen, in dem er die Beiträge selbst freischaltete. Zum anderen aber auch, in dem er den Händlern die Möglichkeit einräumte, die Angebote selbst einzustellen. Für den Vorsatz genügte es dem LG, dass der Angeklagte die Haupttaten der Händler “billigend in Kauf nahm”.

---

[13] OLG Hamburg, NStZ 2007, 487.
[14] BGHSt 2, 129; 14, 280; BGH NStZ 2007, 230.
[15] So heißt es auch in der Gesetzesbegründung: “In der strafrechtlichen Praxis stellt sich das Problem, dass eine Beihilfe gemäß § 27 StGB zu den über die Plattform begangenen Straftaten oft nicht nachweisbar ist, da die Haupttaten bilateral zwischen den Beteiligten über verschlüsselte Kommunikationskanäle abgewickelt werden, jedenfalls aber nicht offen im Forum sichtbar sind.”
[16] BGH NJW 1996, 2517 (2518); NStZ 2017, 274.

Für eine Beihilfe zum Waffenhandel genügte es dem LG, dass der Angeklagte eine für den Waffenhandel vorgesehene und so bezeichnete Unterkategorie seiner Plattform einrichtete und dort tatsächlich später einige Waffengeschäfte vereinbart wurden. Auch hier genügte für den Vorsatz, dass der Angeklagte mit der Vornahme solcher Geschäfte rechnete und diese billigend in Kauf nahm. Einzelheiten zu den Geschäften habe der Angeklagte dagegen nicht kennen müssen.

Schließlich hat das LG dem Angeklagten sogar die Tötungsdelikte, die im Münchener Olympia-Einkaufszentrum begangen wurden, zugerechnet, weil der Verkauf der Tatwaffe über das Forum des Angeklagten angebahnt wurde. Es hat den Angeklagten deshalb wegen fahrlässiger Tötung in neun Fällen verurteilt. Zu § 10 TMG findet sich in dem Urteil kein Wort, auch nicht in den Fällen, in denen sich die Beihilfehandlung des Angeklagten auf die Einrichtung bestimmter Unterkategorien oder die Ermöglichung der Einstellung eigener Angebote durch Händler beschränkte (siehe hierzu sogleich).[17]

Nicht abschließend geklärt ist, ob die **strafbarkeitseinschränkende Norm des § 10 Telemediengesetz (TMG)** auf die Fallgestaltungen der sog. Underground Economy angewendet werden kann. Hiernach haften Diensteanbieter für fremde Informationen, die sie für einen Nutzer speichern, nur, wenn sie entweder (a) positive Kenntnis von der rechtswidrigen Handlung oder Information haben oder (b), wenn sie nicht unverzüglich tätig geworden sind, um die Information zu entfernen oder den Zugang zu ihr zu sperren, sobald sie diese Kenntnis erlangt haben. Die Betreiber:innen der „Darknet-Handelsplattformen“ sind zwar grundsätzlich nach §§ 1 Abs. 1, 2 Nr. 1 TMG vom Anwendungsbereich des TMG erfasst.[18] Unklar ist dagegen, ob § 10 TMG und seine europarechtliche Grundlage in Art. 14 der E-Commerce-Richtlinie auch auf Fallgestaltungen anwendbar sind, bei denen – wie in der Underground Economy – der:die Anbieter:in seine:ihre Plattform von Anfang an ausschließlich oder überwiegend gezielt zur Förderung von Straftaten durch andere ausrichtet und zur Verfügung stellt.[19] Jedenfalls zu Art. 14 der E-Commerce-Richtlinie hat der Europäische Gerichtshof (EuGH) entschieden, dass dieser nicht anzuwenden ist, wenn der Betreiber “zwischen dem fraglichen als Verkäufer auftretenden Kunden und den potenziellen Käufern **keine neutrale Stellung eingenommen, sondern eine aktive Rolle gespielt hat** [Hervorhebung durch Verfasser], die ihm eine Kenntnis der diese Angebote betreffenden Daten oder eine Kontrolle über sie verschaffen konnte.”[20] Da dies vor allem dann anzunehmen ist, wenn der Plattform-Betreiber/die Plattform-Betreiberin eigene wirtschaftliche Vorteile aus den illegalen Geschäften zieht und/oder massive Anreize für eine illegale Nutzung seines Dienstes bietet,[21] spricht viel dafür, dass die Anbieter:innen in der Underground Economy häufig eine solche aktive Rolle spielen. Jedenfalls **würde § 10 TMG – wenn er Anwendung findet – auch für den neuen § 126a StGB-Entwurf gelten**, sodass die

[17] Die Urteilsgründe können nachlesen in: LG Karlsruhe StV 2019, 400.
[18] Safferling/Rückert (2018): Das Strafrecht und die Underground Economy, in: Konrad-Adenauer-Stiftung (Hrsg.), Analysen & Argumente 291; Hoffmann, in: Stiftung der Hessischen Rechtsanwaltschaft (Hrsg.), S. 49, 53 ff.
[19] Gegen eine Anwendung in diesen Fällen: Safferling/Rückert, Das Strafrecht und die Underground Economy, in: Konrad-Adenauer-Stiftung (Hrsg.), Analysen & Argumente 291 (2018); zumindest für eine Einschränkung: OLG München GRUR 2017, 619, 621 Rn 40; für eine Anwendung: KG NJW 2014, 3798; *Hoffmann*, in: Stiftung der Hessischen Rechtsanwaltschaft (Hrsg.), S. 49, 53 ff..
[20] EuGH GRUR 2011, 1025, 1032 Rn 116.
[21] Holznagel, CR 2017, 463, 468 f.

Reform für die einzige (möglicherweise bestehende) “Strafbarkeitslücke” keine Wirkung entfalten würde.

Kriminalisierung nicht strafwürdigen Verhaltens

Unter diesen Prämissen ist es gar nicht so einfach, zu beschreiben, welche strafwürdigen Verhaltensweisen § 126a StGB-Entwurf nun (erstmals) unter Strafe stellen will. Analysiert man den Wortlaut der Vorschrift, so kann man feststellen, dass dieser aus verschiedenen Normen des StGB, die dem Bereich der Vorfeldkriminalität (also Kriminalitätsformen, die selbst kein konkretes Rechtsgut verletzen oder konkret gefährden, sondern lediglich eine abstrakte Gefahr für eine spätere Verletzung oder konkrete Gefährdung schaffen) zuzuordnen sind, “zusammengebastelt” wurde. So entstammt die Formulierung, “deren Zweck oder Tätigkeit auf die Begehung von Straftaten gerichtet ist”, aus dem Tatbestand der “Bildung krimineller Vereinigungen” gem. § 129 StGB. Die Wendung “zu ermöglichen, zu fördern oder zu erleichtern” ist dagegen eng an die Definition des “Hilfeleistens” in § 27 StGB durch die Rechtsprechung angelehnt. Was den Unrechtsgehalt der erfassten Tätigkeiten angeht, geht § 126a StGB-Entwurf jedoch weit über die beiden Normvorbilder hinaus.

Anders als § 129 StGB ist kein auf Dauer angelegter Zusammenschluss von mind. drei Personen und keine Unterordnung unter einen Gesamtwillen erforderlich[22] (§ 126a StGB verlangt keine “Vereinigung”). Da die Gesetzesbegründung auch Äußerungsdelikte als Anwendungsfall nennt, ist außerdem zu befürchten, dass - anders als bei § 129 StGB - auch Straftaten erfasst sein sollen, die keine erhebliche Gefahr für die öffentliche Sicherheit darstellen (so die einschränkende Rechtsprechung zu § 129 StGB).

Anders als bei § 27 StGB ist kein Nachweis einer durch einen anderen tatsächlich begangenen Haupttat notwendig, welche der Plattform-Betreiber/die Plattform-Betreiberin gefördert hat. § 126a StGB-Entwurf stellt damit erstmals die “versuchte Beihilfe” unter Strafe.

Zusammenfassend lässt sich sagen, dass § 126a StGB-Entwurf ein strafbarkeitserweiterndes “Spezialteilnahmerecht” für Internetdienstleister ist und so die bislang geltenden Grenzen der Vorfeldstrafbarkeit ohne Not für diese spezielle Gruppe massiv ausdehnt.

Einsatz nach Belieben – auch gegen Äußerungsdelikte?

Damit verbleibt als einziges beschränkendes Tatbestandsmerkmal und zur Abgrenzung von strafbarem zu straflosem Verhalten beim Betrieb von Internetinfrastruktur die “Ausrichtung des Zwecks oder der Tätigkeit” auf die Förderung fremder Straftaten. Das Merkmal ist aus dem Vereinigungsstrafrecht der §§ 129 ff. StGB bekannt. Allerdings kann man für die Auslegung wohl nicht auf die hierzu ergangene Rechtsprechung zurückgreifen. Bei den §§ 129 ff. StGB ist nämlich für die “Ausrichtung” des Zwecks oder der Tätigkeit auf die Begehung von Straftaten erforderlich, dass der gemeinsame Wille der Vereinigung “verbindlich” auf die Begehung von Straftaten festgelegt ist.[23]

[22] vgl. MüKoStGB-Schäfer, § 129 Rn. 14 ff. m.w.N.
[23] BGH NJW 2005, 80 (81).

Diese Verbindlichkeit des gemeinsamen Willens kann nicht auf § 126a StGB-Entwurf übertragen werden, da dort keine Vereinigung vorausgesetzt wird. Nach der Begründung des Gesetzentwurfs soll sich die Ausrichtung des Zwecks oder der Tätigkeit auf die Förderung fremder Straftaten vor allem aus folgendem ergeben: (a) die AGBs der Plattform-Betreiber:innen; (b) das tatsächliche Angebot auf der Plattform und (c) der Umgang der Plattform-Betreiber:innen mit Hinweisen auf den Handel mit illegalen Gütern auf der Plattform.[24]

Für die Praxis bedeutet dies zum einen, dass die Strafbarkeit bzw. die Begründung eines Anfangsverdachts auch davon abhängt, wie gut die Plattform-Betreiber:innen bei der Zusammenstellung ihrer AGBs rechtlich beraten worden sind. Zum anderen führt eine solche Auslegung dazu, dass **alle Plattform-Betreiber:innen** (und damit auch solche, für die Art. 14 der E-Commerce-Richtlinie und § 10 TMG unstreitig gelten, wie Social Media, "legale" Handelsplattformen, Diskussionsforen etc.) entgegen § 10 TMG und Art. 14 der E-Commerce-Richtlinie "durch die Hintertür" dazu gezwungen würden, aktiv nach Angeboten illegaler Waren und Dienstleistungen auf ihren Plattformen zu suchen. Denn wird das tatsächlich vorhandene Angebot illegaler Güter auf den Plattformen zu groß, liegt die Annahme der Ausrichtung des Zwecks auf die Förderung fremder Straftaten durch die Strafverfolgungsbehörden nahe. Eine solche Auslegung ist daher nicht mit der E-Commerce-Richtlinie der EU vereinbar und somit europarechtswidrig.

Überdies lässt sie die nahezu beliebige Begründung eines Anfangsverdachts gegen jede:n Plattform-Betreiber:in zu, der:die fremde Inhalte hostet. Hiervon sind nicht nur Hidden Services im „Darknet" betroffen, sondern auch sonstige Hosting-Plattformen wie Soziale Medien, Videoplattformen, Sharing-Plattformen, Foren-Betreiber:innen sowie Anbieter:innen von anderen Internetdienstleistungen (E-Mail-Provider, Anbieter:innen von Anonymisierungstechnologie, Tor-Knoten-Betreiber:innen, Node-Betreiber:innen in Kryptowährungssystemen). Durch die Einleitung eines Ermittlungsverfahrens sähen sich diese Anbieter:innen nicht nur potentiell zahlreichen grundrechtseingreifenden Ermittlungsmaßnahmen ausgesetzt, sondern wären auch in ihrer Arbeit erheblich behindert (z.B. wenn Arbeitswerkzeuge wie Computer, Server und E-Mail-Konten beschlagnahmt werden). Da viele dieser Anbieter:innen dem Bereich der "Gewerbsmäßigkeit" zuzuordnen sind, kommen durch die Aufnahme von § 126a Abs. 3 StGB-Entwurf in die Straftatenkataloge der §§ 100a, 100b und 100g StPO auch grundrechtserhebliche Überwachungsmaßnahmen zum Tragen wie die (Quellen-)Telekommunikationsüberwachung, die Online-Durchsuchung und die Verkehrsdatenabfrage. Da § 126a StGB-Entwurf zumindest auch auf die Ermöglichung von fremden Straftaten durch Anonymisierungsdienstleister abzielt, ist hierbei besonders misslich dass diese – soweit sie dem Anwendungsbereich des TMG unterfallen – nach § 13 Abs. 6 TMG sogar dazu verpflichtet sind, Nutzung und Bezahlung ihrer Dienstleistung anonym zu ermöglichen. Es ist hier durchaus denkbar (und in der Praxis auch schon vorgekommen), dass gerade die Erfüllung dieser Verpflichtung die Dienstleister in den Fokus strafrechtlicher Ermittlungen rückt.

Es besteht zumindest die Gefahr, dass § 126a StGB-Entwurf nahezu nach Belieben verwendet werden kann, um Ermittlungsverfahren einzuleiten und gegen missliebige Internetplattformen

[24] Meister, Andre / Biselli, Anna (2019, 03. April): IT-Sicherheitsgesetz 2.0: Wir veröffentlichen den Entwurf, der das BSI zur Hackerbehörde machen soll. URL: https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/ (zuletzt aufgerufen am 03. Juli 2019).

vorzugehen. Dies birgt auch die Gefahr einer politischen Verwendung dieses Werkzeugs. Eine solche liegt auch zumindest nicht ganz fern, wenn bereits im Begründungsentwurf der Wegfall des Straftatenkatalogs im Vergleich zum Vorschlag des Bundesrats auf die Miterfassung von Äußerungsdelikten gestützt wird.

Kein ausreichender Schutz für wünschenswerte Nutzung des „Darknet“

Die Tatbestandsausnahmen in § 126a Abs. 4 StGB-Entwurf sind nicht ausreichend, um die Gefahren vollständig einzudämmen. Die “Bagatellklausel” der Nr. 1 ist ebenfalls dem Vereinigungsstrafrecht entnommen (vgl. § 129 Abs. 2 Nr. 2 StGB), wonach von der Regelung keine Handlungen betroffen sind, bei denen “die Begehung von Straftaten nur einen Zweck oder eine Tätigkeit von untergeordneter Bedeutung darstellt”.

Zieht man die dort ergangene Rechtsprechung zur Auslegung heran, ergibt sich, dass hiervon nur eine “gelegentlich oder beiläufige” Förderung fremder Straftaten ausgenommen werden soll. Ein Ausschluss würde demnach nur vorliegen, wenn die Förderung fremder Straftaten im Vergleich zum Gesamtzweck oder der Gesamttätigkeit des:der Anbieters:Anbieterin der internetbasierten Leistung “so sehr nebensächlich” ist, dass dadurch das Erscheinungsbild der internetbasierten Leistung aus Sicht informierter Dritter nicht mehr in “nennenswerter Weise” mitgeprägt wird.[25] Angesichts der Tatsache, dass die Straftatbegehung auf Internetplattformen durch ihre Nutzer ein ubiquitäres Phänomen und medial sehr präsent ist, wird man diese Ausnahme in der Praxis nur sehr selten anwenden können. Stichworte hierfür sind Beleidigungsdelikte und Volksverhetzung in sozialen Medien, der Verkauf von Hehlerware auf Handelsplattformen, Urheberrechtsverletzungen auf Video- und Sharingplattformen oder die Nutzung von Anonymisierungstechnologie und “anonymen” Kryptowährungen auch durch Kriminelle.

Ähnliches gilt für die Bereichsausnahme für die “Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten”. Zwar wird hier explizit auf die “in § 53 Absatz 1 Satz 1 Nummer 5” der Strafprozessordnung genannten Personen verwiesen. Damit sind Personen erfasst, die

> “bei der Vorbereitung, Herstellung oder Verbreitung von Druckwerken, Rundfunksendungen, Filmberichten oder der Unterrichtung oder Meinungsbildung dienenden Informations- und Kommunikationsdiensten berufsmäßig mitwirken oder mitgewirkt haben.”

Hiervon sind jedoch nur diejenigen Personen erfasst, die “berufsmäßig” mitwirken. Dafür ist zwar keine Gewinnerzielungsabsicht erforderlich, jedoch zumindest die Absicht, ihre Tätigkeit zu einer dauernden, wenigstens wiederkehrenden Beschäftigung zu machen.[26]

Nicht erfasst sind hiervon somit “Privatpersonen”, die als Informanten oder Whistleblower agieren. Gerade für diese sind das „Darknet“ und entsprechende Whistleblowing-Plattformen wie Wikileaks jedoch besonders geeignet, weil die hohe Anonymität es ihnen erst ermöglicht, Informationen von besonderem öffentlichen Interesse zu leaken. Je höher das öffentliche Interesse an einer Information, desto höher sind potentiell auch die Repressalien, die dem Whistleblower drohen. Damit entfaltet das „Darknet“ als anonymste Möglichkeit des Leakens gerade dann seine volle Bedeutung, wenn die Gesellschaft in höchstem Maße von einem Informationsfluss profitiert.

---

[25] BGH NJW 2005, 80 (83).
[26] MüKoStPO-Percic, § 53 Rn. 38 m.w.N.

Unklar an der vorgeschlagenen Regelung ist weiterhin, wie weit die “ausschließlich der Erfüllung beruflicher Pflichten” genannten Handlungen abseits des Bereichs des Journalismus reichen. Moderner Journalismus ist heute gerade im investigativen Bereich auf eine Reihe von Hilfstätigkeiten angewiesen, die dem klassischen Verständnis des § 53 StPO gegebenenfalls nicht unterfallen. Genannt seien etwa Expert:innen, die Journalist:innen bei der Analyse und Einordnung von geleakten Informationen helfen, aber selbst keine Informant:innen sind.[27]

Ferner benötigen Medien technische Expert:innen, welche beispielsweise einen Tor-Server für ein Medium betreiben und die Sicherheit eines anonymen Briefkasten warten. Sie unterhalten damit eine Infrastruktur, die für modernen Journalismus essentiell ist, aber nicht ausschließlich von Journalist:innen genutzt werden kann und soll. Auch Organisationen, die selbst keinen Journalismus betreiben, sich aber als zivilgesellschaftliche Akteure für die Grundrechte auf Meinungs-, und Pressefreiheit sowie das Fernmeldegeheimnis einsetzen, betreiben Anonymisierungsdienste für Medien, ohne dafür im Auftrag von Medien zu handeln. So unterhält Reporter ohne Grenzen beispielsweise mit Unterstützung des Zwiebelfreunde e.V. zwei Tor-Knoten mit dem Ziel, den Journalismus zu stärken und anonyme Kommunikation zu ermöglichen. Eine Beschränkung der Nutzung auf journalistische Zwecke ist schon technisch nicht realisierbar.

Außerdem ist ohnehin unklar, ob sich auch Anonymisierungsdienste, Betreiber:innen von Knoten im Tor-Netzwerk und in virtuellen Kryptowährungssystemen sowie weitere Dienstleister:innen (z.B. das Lightning-Netzwerk oder Entwickler von Add-Ons wie die Electronic Frontier Foundation für “https-everywhere”) auf “rechtmäßige berufliche Pflichten” berufen können. Dies scheint angesichts des Gesetzestextes höchst fraglich, weil hiermit offensichtlich lediglich Dienste wie Secure Drop gemeint sein sollen, da diese von den Medien selbst betrieben werden.

Zwischenfazit

Anders als in der Gesetzesbegründung postuliert bestehen bei Analyse des Strafrechts keine entsprechenden Lücken, die der Regelungsentwurf vermeintlich zu schließen vermag. Stattdessen sind die typischen “Darknet-Delikte” wie Betäubungsmittelhandel, Waffenhandel oder die Verbreitung kinder- und jugendpornografischer Schriften erschöpfend geregelt. Die in der Gesetzesbegründung aufgestellte These, wonach den Betreiber:innen von Handelsplattform eine Beihilfe nur sehr schwer nachgewiesen werden kann, ist zudem nicht haltbar. Der Nachweis entsprechender Haupttaten ist wegen der weiten Auslegung der praxisrelevanten Vorschriften vergleichsweise einfach, für den Beihilfevorsatz gelten ebenfalls sehr extensive Maßstäbe. Eine mögliche Einschränkung durch § 10 TMG würde auch für § 126a StGB gelten.

Weil die Norm nicht auf bestimmte Internetdienste respektive Straftaten begrenzt werden soll, ist zu befürchten, dass die Norm nahezu nach Belieben angewendet wird. Dies ist umso schwerwiegender, weil die Tatbestandsausnahmen für die Praxis ins Leere laufen. Sie schließen schützenswerte Personengruppen aus. Im Ergebnis können Tätigkeiten kriminalisiert werden, die für die Gesellschaft wünschenswert sind. Hierzu zählt anonyme Informationsübermittlung an Medien ebenso wie der Schutz des Telekommunikationsgeheimnisses.

[27] Diese Problematik ist in einer Verfassungsbeschwerde über die Datenhehlerei aufgeworfen worden, vgl. Gesellschaft für Freiheitsrechte (2017, 13. Januar): GFF und ihre Partner klagen gegen Anti-Whistleblowing-Gesetz “Datenhehlerei”. URL: https://freiheitsrechte.org/datenhehlerei/ (zuletzt aufgerufen am 03. Juli 2019).

Kriminalisierung, Abschreckung – Abschaltung?

Wie die juristische Analyse des vorgeschlagenen “Darknet-Paragrafen” zeigt, fallen durch die quasi unbeschränkte Reichweite des §126a StGB-Entwurf auf “internetbasierte Leistungen” diverse Anwendungen und Personengruppen unter die Norm, deren Wirken nicht kriminalisiert, sondern eher gesellschaftlich gefördert werden sollte. In diesem Teil wird daher praxisnah aufgezeigt, welche Dienste von der Kriminalisierung betroffen wären, warum gerade Journalist:innen sie für ihre Arbeit benötigen – und welche Einschüchterungseffekte für Betreiber:innen von Anonymisierungsdiensten drohen.

Direkte Folgen: Aus von Diensten mit gesellschaftlichem Nutzen

Im Folgenden wird gezeigt, warum Leaking-Plattformen, anonyme Filesharing-Programme sowie Tor-Relays und VPN-Dienste wichtig sind für Medien und andere Personengruppen – und was ein Aus solcher Dienste für ihre Arbeit bedeuten könnte.

Leaking-Plattformen

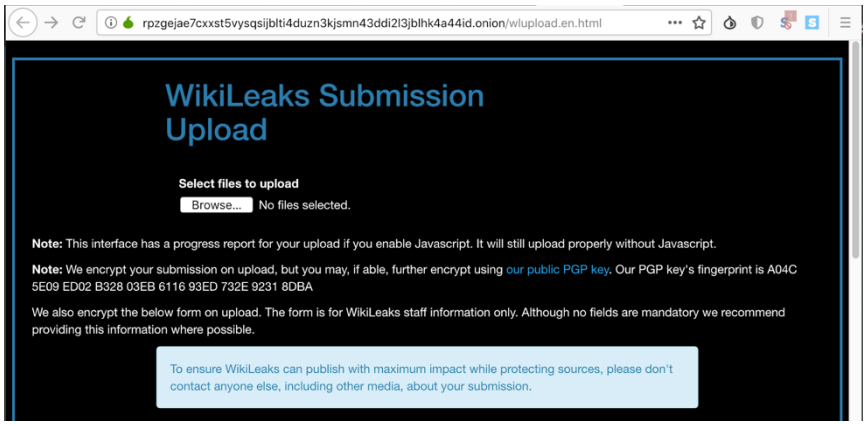
Durch die zunehmende Online-Überwachung seit Beginn der 2000er Jahre, die spätestens der Whistleblower Edward Snowden durch seine NSA-Files im Jahr 2013 ins öffentliche Bewusstsein getragen hat, ist das Bewusstsein von Journalist:innen und ihren Informant:innen für ihren eigenen Schutz spürbar gestiegen.[28] Als Reaktion auf staatliche Verfolgung sind daher eine Reihe von Leaking-Plattformen entstanden, die teilweise auch auf der Onion-Technologie des Tor-Netzwerkes basieren.

Besondere Relevanz im Bereich des Journalismus hat die Technologie **Secure Drop**[29] entfaltet, die ursprünglich von der US-basierten Freedom of the Press Foundation entwickelt worden war. Hierbei handelt es sich um eine Art anonymen Briefkasten, bei der beispielsweise ein Medienunternehmen einen eigenen Onion-Server aufsetzt. Hier laufen dann anonyme Hinweise und geleakte Dokumente ein, die anschließend redaktionell verarbeitet werden können. In

[28] vgl. PEN American Center (2015, 5. Januar): Global Chilling. The Impact of Mass Surveillance on International Writers. URL: https://pen.org/sites/default/files/globalchilling_2015.pdf (zuletzt aufgerufen am: 03. Juli 2019).
[29] vgl. Secure Drop. Share and accept documents securely. URL: https://securedrop.org/ (zuletzt aufgerufen am 03. Juli 2019).

Deutschland betreiben unter anderem die Süddeutsche Zeitung, die Huffington Post und der heise-Verlag einen Secure Drop-Briefkasten.

In diesen Fällen ließe sich im Lichte des “Darknet-Paragrafen” tatsächlich argumentieren, dass diese Dienste “ausschließlich” für journalistische Zwecke genutzt werden können, weil das betreibende Medium stets die Information empfängt. Da das Medium selbst den Server betreibt, laufen alle Informationen zwangsläufig nur in der Redaktion ein. Hierauf stellt die vorgesehene Tatbestandsausnahme im § 126a StGB-Entwurf offensichtlich ab. Diese Ausnahme für Secure Drop ist zwar wünschenswert, verkennt aber diverse weitere Anwendungsfelder für anonyme Leaking-Technologien, die für den Journalismus ebenfalls eine Rolle spielen. Dies fängt bereits bei Secure Drop selbst an: Die Technologie wird auch von Nicht-Regierungsorganisationen betrieben, wie etwa die auf Korruptionsbekämpfung spezialisierte Organisation Global Witness. In diesen Fällen erreicht die Information nicht Journalist:innen, sondern Aktivist:innen – die dann für die Themen Öffentlichkeit herstellen und gegebenenfalls bei der Publikation mit Medien zusammenarbeiten.



Es gibt jedoch auch abseits von Secure Drop eine Reihe weiterer Leaking-Technologien, die für den Journalismus wichtig sind, aber nicht ausschließlich von Journalist:innen genutzt werden. Die bekannteste Leaking-Plattform ist sicherlich **Wikileaks**, bei der unter anderem die US-Whistleblowerin Chelsea Manning Kriegsverbrechen der US-Armee öffentlich gemacht hat. Im Jahr 2016 veröffentlichte die Plattform ferner 90 Gigabyte aus dem NSA-Untersuchungsausschuss des Bundestages, aus denen unter anderem hervorging, dass die deutschen Geheimdienste BND und BfV aktiv Wege suchten, um die Kontrolle durch die Bundesregierung und die deutschen Parlamente zu umgehen.[30] Zwar ist Wikileaks auch im Clearweb unter wikileaks.org erreichbar, doch ein Upload von Daten ist nur über die Onion-Adresse möglich.[31]

Zwar bearbeitet Wikileaks die Leaks redaktionell zum Zwecke des Quellenschutzes, dürfte jedoch trotzdem nicht als Journalismus nach deutschem Rechtsverständnis gelten. Dies liegt vor allem daran, dass Wikileaks bei der redaktionellen Bearbeitung eher darauf achtet, keine personenbezogenen Daten von schutzwürdigen Personen zu veröffentlichen. Im Klartext: Auf Wikileaks wird ein Leak nicht beschnitten, nur weil einzelne Informationen gegebenenfalls nicht von öffentlicher Relevanz wären. Im Gegenteil setzt Wikileaks eher drauf, gerade nicht in ein Leak einzugreifen, um die Authentizität nicht zu beeinflussen. Eine journalistische Verarbeitung der

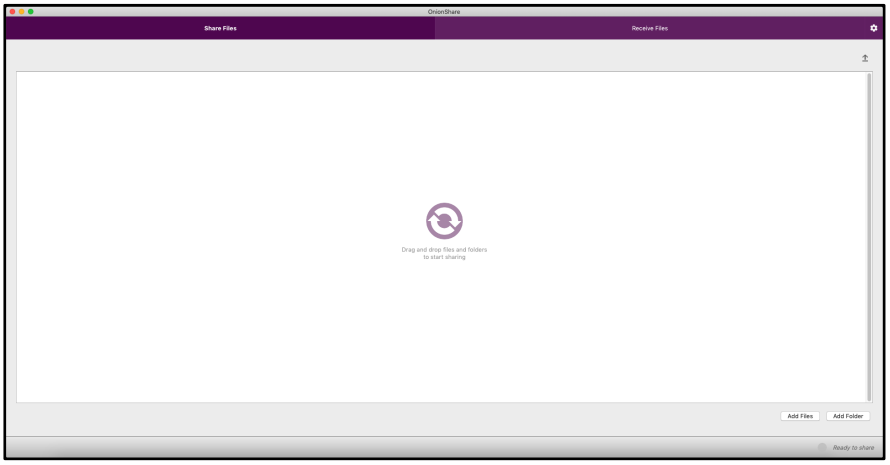
[30] vgl. WikiLeaks (2016, 1. Dezember): German BND-NSA Inquiry Exhibits. URL: https://wikileaks.org/bnd-inquiry/ (zuletzt aufgerufen: 03. Juli 2019).
[31] Die Onion-URL lautet: http://rpzgejae7cxxst5vysqsijblti4duzn3kjsmn43ddi2l3jblhk4a44id.onion/wlupload.en.html, zuletzt aufgerufen am 03. Juli 2019.

Roh-Informationen findet wohl unter der Schwelle dessen statt, was die deutsche Rechtsordnung als Journalismus anerkennt. Beispielhaft sei hierfür § 3 des Landespressegesetzes NRW zitiert:

> "Die Presse erfüllt eine öffentliche Aufgabe insbesondere dadurch, daß sie Nachrichten beschafft und verbreitet, Stellung nimmt, Kritik übt oder auf andere Weise an der Meinungsbildung mitwirkt."

Dies findet sich fast wortgleich in allen deutschen Landespressegesetzen so wieder. Mit einem deutschen "Daknet-Paragrafen" würde die Plattform und die dahinterliegende Organisation daher kriminalisiert, obwohl über Wikileaks bereits Skandale von globaler Dimension bekannt geworden sind und die Plattform derzeit Partnerschaften von über 100 Medien hat.[32]

Anonymes Filesharing



In einigen Fällen journalistischer Recherche ist es hingegen gar nicht zielführend, sich einen eigenen anonymen Briefkasten zu installieren. Viele gerade kleinere Medien können sich die Serverkosten gegebenenfalls nicht leisten oder besitzen nicht die technische Expertise, um den sicheren Betrieb eines Onion-Services zu gewährleisten. Dies gilt gerade für Exilmedien, bei denen die redaktionelle Bearbeitung und Veröffentlichung durch Personen in sicheren Drittländern wie Deutschland erledigt wird, doch Korrespondent:innen im gefährlichen Ursprungsland Informationen sicher "aus dem Land" heraus bringen müssen. Die finanzielle Lage dieser Medien ist häufig prekär, weshalb sie auf Massen-Kommunikationstechnologien zurückgreifen müssen. Ferner wollen sie ja geradezu keine Aufmerksamkeit auf sich lenken, sondern ihre Information gänzlich "unter dem Radar" austauschen.

Ein beliebtes Tool hierfür ist Onion Share. Dieses Programm ist kostenlos herunterladbar und eignet sich, um anonym Daten auszutauschen. Entweder lädt ein:e Nutzer:in ein Dokument hoch und verteilt einen Download-Link ähnlich Dropbox oder Google Drive. Im anderen Fall schaltet er:sie den sogenannten "Receive-Mode" ein und teilt einen Link, unter dem andere Daten hochladen können. Alles basiert auf der Onion-Technologie des Tor-Netzwerkes und ist damit geeignet für einen anonymen Informationsaustausch. Naturgemäß ist die Nutzung nicht auf den Journalismus beschränkt, sondern potentiell auch geeignet, um Kriminellen die Straftatbegehung zu erleichtern.

[32] vgl. Wikileaks.org, URL: https://wikileaks.org/-Partners-.html, zuletzt aufgerufen am 03. Juli 2019.

Anonymisierungsdienste und VPN

Zwar dürfte es nicht intendiert sein, mit dem neuen § 126 StGB-Entwurf gegen Betreiber:innen von Anonymisierungsdiensten wie Tor-Knotenbetreiber:innen oder kommerzielle VPN-Anbieter vorzugehen. Doch die rechtliche Analyse zeigt, dass ihr Handeln unter den Wortlaut der Norm fallen kann und die Ausnahmen des Absatz 4 nicht greifen. Durch die Erfassung jeglicher "internetbasierter" Leistung werden auch Betreiber:innen von Tor-Knoten und VPN-Anbieter erfasst.

Naturgemäß werden diese Technologien auch in signifikantem Umfang von Kriminellen zur Straftatbegehung missbraucht. Ferner ist eine inhaltliche Kontrolle der durchgeleiteten Kundendaten technisch häufig nicht möglich oder würde zumindest die – z.B. für die journalistische Nutzung – notwendige Anonymität konterkarieren. Zieht man die in der Gesetzesbegründung genannten Indizien zur Bestimmung der "Ausrichtung des Zwecks oder der Tätigkeit" heran, lässt sich in nahezu allen Fällen jedenfalls ein Anfangsverdacht begründen, häufig sogar eine Verurteilung. Bezüglich einer Verurteilung ist zwar zu beachten, dass dieser bei Tor-Knotenbetreiber:innen regelmäßig die Haftungsprivilegierung des § 8 TMG entgegensteht. Jedoch besteht ein realistisches Risiko der Begründung eines Anfangsverdachts mit den bereits geschilderten Konsequenzen.[33]

Reporter ohne Grenzen e.V. und der Zwiebelfreunde e.V. betreiben jeweils mehrere Tor-Knoten und unterstützen damit das Tor-Netzwerk als Ganzes. Dahinter steht keine Gewinnerzielungsabsicht, sondern eine ideelle Unterstützung des Tor-Netzwerkes, um Menschen auf der gesamten Welt die Wahrung des Menschenrechts auf Privatsphäre auch Online zu ermöglichen. Auch wenn dabei intendiert ist, dass davon vor allem Journalist:innen, Menschenrechtsaktivist:innen und andere für die Gesellschaftlich besonders wichtige Gruppen profitieren, kann dies seitens der Betreiber:innen nicht sichergestellt werden. Eine "ausschließliche" Nutzung für solche berufsmäßigen Zwecke von Journalist:innen liegt jedenfalls nicht vor.

Der Bedarf an anonymer Online-Recherche ist im Zuge der globalen Massenüberwachung jedoch gerade im Journalismus in den vergangenen Jahren stark angestiegen. Weil es das überlieferte Interesse von Geheimdiensten ist, möglichst alles zu erfassen, benötigen Medienschaffende eine Art digitale Tarnkappe, um ihre Arbeit so geheim wie möglich zu erhalten. Werden Recherchen schon frühzeitig online überwacht, können Storys im schlimmsten Fall verhindert werden durch staatliche Ermittler:innen oder die Journalist:innen werden abgeschreckt, sensible Themen überhaupt erst zu recherchieren (siehe hierzu sogleich).

Eine jüngst veröffentlichte Studie hat empirisch nachgewiesen, dass diese Sorgen bei Journalist:innen, die zu Themen der inneren und äußeren Sicherheit recherchieren und mit ihren Recherchen zur demokratischen Geheimdienstkontrolle beitragen, außerordentlich groß ist.[34] Gegen das reformierte BND-Gesetz, welches die flächendeckende Ausspähung ausländischer Medien legalisiert hat, sind Investigativjournalist:innen aus der ganzen Welt vor das

[33] Cornelius, Kai (2018, 31. Juli): Fluch und Segen von Anonymisierungsdiensten. URL: https://www.lto.de/recht/hintergruende/h/internet-anonymitaet-tor-server-persoenlichkeitsschutz-haftung-betreiber/, zuletzt aufgerufen am 03. Juli 2019.

[34] vgl. Mills, Anthony (2018): Now You See Me – Now You Don't: Journalists' Experiences With Surveillance. In: Journalism Practice, URL: https://www.tandfonline.com/doi/full/10.1080/17512786.2018.1555006 (zuletzt aufgerufen am: 03. Juli 2019).

Bundesverfassungsgericht gezogen.[35] Reporter ohne Grenzen berät Journalist:innen aus Deutschland und anderen Teilen der Welt außerdem seit Jahren in Fragen digitaler Sicherheit und stellt dabei fest, dass der Bedarf an VPN-Clients und dem Tor-Browser seit Jahren steigt. Dies liegt einerseits daran, dass das Bewusstsein für die Online-Überwachung gestiegen ist, und andererseits durch zunehmendes DNS-Blocking gerade in repressiven Ländern einige Websites nur noch mittels dieses anonymen Umwegs erreichbar sind.

Kennzeichnend ist dafür auch, dass führende VPN-Anbieter damit werben, ihren Dienst für Journalist:innen und Aktivist:innen zu betreiben und diesen Gruppen ihre Technologie häufig kostenlos zur Verfügung zu stellen. Entsprechende Programme bieten beispielsweise NordVPN und ProtonVPN des Schweizer Email-Anbieters Protonmail an.

Indirekte Folgen: Chilling Effects

Eine Kriminalisierung der zuvor genannten Dienste hat unweigerlich Folgen für ihre Nutzung. Selbst wenn es staatlichen Stellen nicht gelingen sollte, manche Angebote “abzuschalten”, weil dies wie im Falle von Onion-Services technisch praktisch unmöglich ist, geht eine Kriminalisierung nicht spurenlos an Betreiber:innen und Nutzer:innen vorüber. Im Gegenteil: Da mit dem “Darknet-Paragrafen” Ermittlungen angestoßen werden können, drohen Betreiber:innen und Nutzer:innen in den Fokus von Überwachungs- und Durchsuchungsmaßnahmen zu geraten. Damit können Einschüchterungseffekte (sog. Chilling Effects) einhergehen, welche die Personen daran hindern, gesellschaftlich wünschenswertes Engagement fortzusetzen.

Einschüchterung für Nutzer:innen

Reporter ohne Grenzen hat täglich Kontakt zu Journalist:innen auf der gesamten Welt, die im Lichte verschiedenster Bedrohungen recherchieren müssen. In den vergangenen Jahren ist der Bedarf an Beratung in digitaler Sicherheit spürbar gestiegen. In einigen Ländern ist die Nutzung von VPN kriminalisiert oder zumindest de facto blockiert, auch das Tor-Netzwerk ist auf DNS-Ebene bisweilen gesperrt. ROG reagiert hierauf seit Jahren im Bereich der Nothilfe sowie mit Beratungen in Fragen der IT-Sicherheit. Nach einem Stipendienprogramm für digital verfolgte Medienschaffende von 2014 bis 2016 mit Mitteln des Auswärtigen Amts hat ROG mittlerweile mit finanzieller Unterstützung der Berliner Senatsverwaltung unter anderem ein Fellowship-Programm entwickelt, um ausländische Journalist:innen zu Trainer:innen in digitaler Sicherheit auszubilden. Neben der Verschlüsselung ihrer Kommunikation zählt die Anonymisierung ihres digitalen Rechercheverlaufs zu den Gebieten, die derzeit am stärksten nachgefragt werden.

Einer der ausgebildeten Trainer ist Farhan Janjua aus Pakistan, der in seinem Heimatland für regierungskritische Online-Medien gearbeitet und kürzlich das Portal Voice of Internet[36] gegründet hat. In Pakistan ist der Gebrauch von Verschlüsselung illegal, wenn damit der Zugriff für die Pakistanische Telekommunikations-Regulierungsbehörde erschwert wird. Selbst wenn

[35] vgl. Reporter ohne Grenzen (2018, 18. Januar): Verfassungsbeschwerde gegen das BND-Gesetz. URL: https://www.reporter-ohne-grenzen.de/pressemitteilungen/meldung/verfassungsbeschwerde-gegen-das-bnd-gesetz/ (zuletzt aufgerufen am: 03. Juli 2019).
[36] vgl. Voice of Internet. URL: https://voiceofinternet.com (zuletzt aufgerufen am: 03. Juli 2019).

VPN-Provider und Tor-Betreiber:innen nicht explizit genannt werden, gilt ihre Nutzung im Land als risikoreich:

"Als die digitalen Angriffe auf mich und mein Medium schlimmer wurden, begann ich, mich aus Angst selbst zu zensieren. Anonymisierungsdienste waren und sind daher essentiell für mich, meine Kolleg:innen und unsere Quellen. Ohne Anonymität können wir nicht mehr arbeiten. Ich beobachte jedoch, dass mehr und mehr Kolleg:innen abgeschreckt werden von der Nutzung. Selbst wenn der Staat Dein Verhalten nicht direkt kriminalisiert, fragst Du Dich ständig: Mache ich mich verdächtig, nur weil ich jetzt gerade einen VPN oder Tor nutze? Es gibt einen Chilling Effect, der schleichend Dein Verhalten verändert."

Die Gefahr solcher Chilling Effects wird zunehmend auch juristisch beachtet. Demnach kann allein die Möglichkeit einer Überwachung und Strafverfolgung menschliches Verhalten verändern. Nehmen Menschen (z.B. aus Angst vor Sanktionen) deswegen keine Freiheitsrechte mehr wahr, spricht man von Chilling Effects. Sie treten auf

> „where one is deterred from undertaking a certain action X as a result of some possible consequence Y. Additionally, a chilling effect is an indirect effect: it occurs when the deterrence does not stem from the direct restriction, but as an indirect consequence of the restriction's application"[37].

Die Theorie der Chilling Effects entstammt der angloamerikanischen Rechtstradition, wird aber verstärkt auch von deutschen und europäischen Gerichten anerkannt.[38] Sie werden in der Rechtsprechung gemeinhin negativ bewertet. Betroffen sind viele Grund- und Freiheitsrechte, am häufigsten wird die Möglichkeit von Chilling Effects jedoch zur Rechtsprechung im Bereich der Meinungs- und Pressefreiheit angewendet.[39] Sie wirken eher langfristig und unbewusst. Am stärksten betroffen von Chilling Effects sind sogenannte „Meinungsführer:innen" von „Minderheitsmeinungen", zum Beispiel regierungskritische Journalist:innen in einem autokratisch geführten Staat.[40]

Es gibt auch erste empirische Hinweise, dass Überwachung tatsächlich zu Chilling Effects führt. Die Schriftsteller-Organisation PEN America führte im Zuge des NSA-Skandals im Jahr 2013 eine Umfrage unter U.S.-amerikanischen Mitgliedern durch, wonach 24 Prozent der Befragten über bestimmte Themen per Telefon und E-Mail nicht kommunizieren wollten. 16 Prozent unterließen Online-Recherchen zu bestimmten Themen.[41] 2015 bestätigte die Organisation die Ergebnisse in einer weltweiten Umfrage und fand heraus, dass die Furcht vor Überwachung in autokratischen

---

[37] vgl. Youn, Monica (2013): The Chilling Effect and the Problem of Private Action, in: Vanderbilt Law Review, 66 (5), S. 1481.
[38] vgl. Assion, Simon (2014): Überwachung und Chilling Effects, in: Überwachung und Recht. Tagungsband zur Telemedicus-Sommerkonferenz, S. 31-82.
[39] vgl. wie Fn. 36, S. 42-46.
[40] vgl. wie Fn. 36, S. 62-70.
[41] vgl. PEN America (2013): Chilling Effects: NSA Surveillance Drives U.S. Writes to Self Censor. URL: https://pen.org/sites/default/files/2014-08-01_Full%20Report_Chilling%20Effects%20w%20Color%20cover-UPDATED.pdf (zuletzt aufgerufen am: 03. Juli 2019).

Ländern höher ist als in demokratischen, wobei die Bedenken in demokratischen Ländern steigen.[42]

Mit der Einführung eines "Darknet-Paragrafen" wird ein ähnlich abschreckendes Verhalten auch in Deutschland provoziert. Indem der Gesetzgeber zumindest die Tür öffnet, gegen die Betreiber:innen von VPN- und Tor-Servern vorzugehen, schwächt dies auch das Vertrauen, welches Nutzer:innen in diese Dienste haben können. Mag dies auch nicht das Ziel der Gesetzesinitiative sein, ist dies jedoch ein unweigerlicher Kollateralschaden, weil der Anwendungsbereich eben fast grenzenlos auf internetbasierte Dienste gefasst ist.

Einschüchterung für Betreiber:innen von Anonymisierungsdiensten

Wer sich heute für das Recht auf Anonymität im Internet einsetzt, nimmt bereits einige Bürden auf sich. Bei Personen zum Beispiel, die freiwillig das Tor-Netzwerk unterstützen, sind es vor allem

- Kosten für Hardware sowie den Internetanschluss,
- die Möglichkeit einer strafrechtlichen Verfolgung beim Betrieb eines Exit-Knotens wegen vermeintlich illegaler Handlungen durch die Betreiber:innen selbst, sowie
- eine bisweilen öffentlichen Anprangerung wegen der vermeintlichen Unterstützung eines "kriminellen Netzwerkes".

Dies ist unangenehm für die betreffenden Personen, gehört bis dato aber für das Einstehen eigener Überzeugungen gewissermaßen als "Preis" dazu. Gänzlich anders wird dies naturgemäß, wenn der Betrieb eines Relays selbst kriminalisiert würde – oder es zumindest deutlich vereinfacht würde, Ermittlungen gegen Betreiber:innen einzuleiten. Der "Darknet-Paragraf" wirkt damit abschreckend auf all' diejenigen, die derzeit aktiv das Tor-Netzwerk unterstützen oder es in Zukunft tun möchten. Selbst wenn am Ende des Ermittlungsverfahrens festgestellt wird, dass eine Ermöglichung rechtswidriger Taten eben nicht ausschließlicher Zweck des Dienstes ist, sondern schlicht nur die Folge aus dem Angebot.

Was es heißt, in solche – am Ende im Sande verlaufenden – Ermittlungen zu geraten, mussten führende Mitglieder der Zwiebelfreunde im Jahr 2018 am eigenen Leib erfahren. Bayerische Ermittler:innen hatten die Privaträume der Vorstände und mehrere Büroräume durchsucht, da sie (ohne es zu wissen) als Zeugen in einem Ermittlungsverfahren geführt wurden. Die Ermittler:innen wollten mit der Maßnahme an angeblich existierende Nutzerdaten gelangen. Zwar gelten hohe Hürden für Durchsuchungen bei Zeugen, dennoch fanden sie in diesem Fall statt – und wurden im Anschluss für eindeutig rechtswidrig erklärt.

Dieser "Freispruch" erfolgte jedoch erst im Nachgang. Die Polizei beschlagnahmte dennoch Material, sodass die Betroffenen mehrere Monate auf die Rückgabe aller elektronischen Geräte und ihrer Unterlagen warten mussten. Mit dem vorliegenden Gesetzesvorschlag würden die Rechte von Dienstleister:innen vollends ausgehebelt, da die Dienstleister:innen selbst – in diesem Beispiel: Tor-Relay-Betreiber:innen – zumindest zeitweise als Beschuldigte geführt würden. Dies

[42] vgl. PEN American Center (2015, 5. Januar): Global Chilling. The Impact of Mass Surveillance on International Writers. URL: https://pen.org/sites/default/files/globalchilling_2015.pdf (zuletzt aufgerufen am: 03. Juli 2019).

würde dann weitere Ermittlungen ermöglichen. Es ist dabei für die Betroffenen wenig tröstlich, wenn der Vorwurf später fallen gelassen wird.

Es besteht die reale Gefahr, dass Menschen diese Grundrechtseingriffe und finanzielle Risiken durch Anwaltskosten in Zukunft scheuen werden, sodass sie ihre Relays abschalten oder gar nicht erst ans Netz gehen werden. Dies trifft das Tor-Netzwerk im Kern, denn gerade in Deutschland gibt es verhältnismäßig viele Relay-Betreiber:innen. Deutschland steht weltweit an erster Stelle was die Gesamtkapazität des Netzwerks betrifft, denn aktuell läuft über 30 Prozent des Tor-Netzverkehrs über deutsche Server. Das aktuelle Register zählt über 1300 Knoten allein in Deutschland, wovon über 100 auch als Exit-Knoten fungieren.[43] Unter den Betreiber:innen dieser Knoten werden diese Pläne zum "Darknet-Paragrafen" seit Wochen diskutiert. Der Zwiebelfreunde e.V. erhielt bereits mehrere Anfragen von Betreiber:innen, die durch den Gesetzesentwurf stark verunsichert sind und besorgt sind, dass ihr Engagement rechtliche Folgen für sie haben könnte.

Auch Reporter ohne Grenzen betreibt zwei Tor-Knoten, da die Unterstützung von Anonymität im Internet eines der Kernanliegen der Organisation ist, um unabhängigen Journalismus zu ermöglichen und Journalist:innen digitalen Schutz zu gewähren. Zwar mag die latente Kriminalisierung dieses Engagements bei einer Organisation mit über 2000 Mitgliedern nicht direkt dazu führen, dass ROG den Betrieb aus Furcht einstellen würde. Die Sorge, selbst Ziel von Ermittlungen zu werden, ist indes groß. Da sich ROG als Menschenrechtsorganisation nicht auf das journalistische Redaktionsgeheimnis berufen kann, sind die Gefahren einer Durchsuchung höher als bei Medien selbst. Dennoch ist auch Reporter ohne Grenzen auf ein gewisses Grundvertrauen angewiesen, welches Journalist:innen auf der ganzen Welt in die Organisation haben. Medienschaffende aus dem In- und Ausland stehen regelmäßig mit ROG in Kontakt, um sensible Informationen zu teilen. Dies geschieht häufig mit der Bitte um Vertraulichkeit, sodass ROG die Informationen im eigenen Namen öffentlich macht. Müssten Quellen der NGO künftig befürchten, dass ihre Kommunikation im Zuge von Durchsuchungs- oder Überwachungsmaßnahmen in die Hände von Ermittler:innen fallen, wäre dies eine enorme Einschränkung der Arbeitsfähigkeit der Organisation.

[43] vgl. Tor Metrics, URL: https://metrics.torproject.org/rs.html#aggregate/cc, zuletzt aufgerufen am 03. Juli 2019.

Empfehlungen

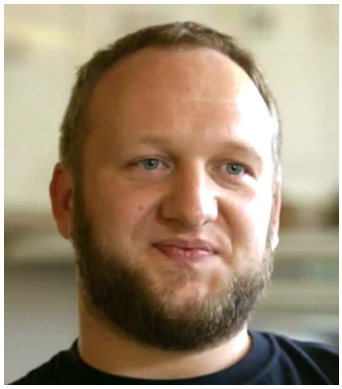
Da keine relevante Strafbarkeitslücke existiert, muss diese auch nicht geschlossen werden. Die Autoren empfehlen daher, die Norm des § 126a StGB-Entwurf nicht zu beschließen – auch nicht in der "entschärften Version", die im Bundesrat auf Vorschlag von Nordrhein-Westfalen beschlossen wurde.

Sowohl die relevanten „Darknet-Delikte" als auch § 27 StGB sind bereits hinreichend weit gefasst bzw. werden hinreichend weit interpretiert, um strafwürdige Konstellationen zu erfassen. Die -– möglicherweise tatsächlich bestehende – Strafbarkeitseinschränkung aus § 10 TMG (für Plattform-Betreiber:innen) und § 8 TMG für die Durchleitung von Informationen (z.B. für Tor-Knoten-Betreiber:innen) würde auch für § 126a StGB-Entwurf gelten und könnte wegen ihrer europarechtlichen Grundlage in den Art. 12 ff. der E-Commerce-Richtlinie auch nicht vom deutschen Gesetzgeber abgeschafft werden. § 126a StGB-Entwurf würde daher materiell-strafrechtlich keinerlei Verbesserung bei der Bestrafung von „Darknet-Kriminalität" bringen. Gleichzeitig erhöht er jedoch das Risiko für zahlreiche Online-Dienstleistungsanbieter:innen – vor allem, aber nicht nur Anbieter:innen von Anonymisierungsdienstleistungen – in das Zentrum eines strafrechtlichen Ermittlungsverfahrens zu geraten und die Arbeit massiv behindernden Ermittlungsmaßnahmen ausgesetzt zu sein.

Zur effektiven Bekämpfung der „Darknet-Kriminalität" bei gleichzeitiger Wahrung der grundrechtlichen Freiheiten der Bürger:innen, und unter Berücksichtigung des weltweiten Schutzes der Meinungs-, Informations- und Pressefreiheit, empfehlen die Autoren daher folgendes:

- Personelle und technische Aufstockung der Bundes- und Landespolizeien, insbesondere die verstärkte Einstellung von gut ausgebildeten IT-Fachkräften.
- Personelle und technische Aufstockung der Staatsanwaltschaften, insbesondere Ausbau der bereits bestehenden Schwerpunktstaatsanwaltschaften.
- Investition in Forschung und Entwicklung von effektiven, aber gleichzeitig grundrechtsschonenden Ermittlungswerkzeugen zur De-Anonymisierung von Straftäter:innen, die Anonymisierungs- und Verschlüsselungstechnologien missbrauchen, ohne dabei jedoch das Schutzniveau für alle anderen Nutzer:innen abzuschwächen.
- Einrichtung von speziellen Cybercrime-Strafkammern an den Landgerichten nach Vorbild der Wirtschaftsstrafkammern.
- Verbesserung der internationalen und europäischen Zusammenarbeit der Ermittlungsbehörden, sofern dabei gleichzeitig die Kontrolle dieser Kooperationen gestärkt und weiterentwickelt wird.

Über die Autoren



Moritz Bartl ist Vorstandsvorsitzender der Stiftung Erneuerbare Freiheit, die global Projekte aus dem Bereich der digitalen Menschenrechte fördert und unterstützt. Er engagiert sich ehrenamtlich für das Tor-Projekt und ist Mitgründer und Vorstand des Zwiebelfreunde e.V., einem der größten Betreiber von Anonymisierungsinfrastruktur weltweit. Bartl berät zivilgesellschaftliche Organisationen zu Themen der IT-Sicherheit, dem Einsatz und der Entwicklung von Open Source-Technologien und digitaler Souveränität. Als Projektleiter und Geschäftsführer der gemeinnützigen Center for the Cultivation of Technology GmbH ist er an der Entwicklung und Forschung zu freien Technologien beteiligt.

Daniel Moßbrucker ist Referent für Internetfreiheit bei Reporter ohne Grenzen. Die Organisation setzt sich weltweit für den Schutz der Pressefreiheit ein und kämpft online wie offline gegen Zensur. Das Referat für Internetfreiheit kümmert sich unter anderem um eine demokratische Kontrolle von Geheimdiensten, Schutzrechte für Medien in Sicherheitsgesetzen, eine restriktive Exportkontrolle von Überwachungstechnologie sowie die gesellschaftliche Kontrolle sozialer Netzwerke. Moßbrucker ist zudem Trainer für digitale Sicherheit und schult hierfür Journalistinnen und Journalisten im In- und Ausland in Fragen wie Verschlüsselung, Anonymisierung und Account Sicherheit.

Dr. Christian Rückert ist Akademischer Rat auf Zeit am Lehrstuhl für Strafrecht, Strafprozessrecht, Internationales Strafrecht und Völkerrecht der Friedrich-Alexander-Universität Erlangen-Nürnberg und wissenschaftlicher Mitarbeiter am Zentrum für Angewandte Rechtswissenschaft des Karlsruher Instituts für Technologie. Er ist außerdem Mitglied der Expertenkommission der Justizministerkonferenz in der Länderarbeitsgruppe “Digitale Agenda Straf- und Strafprozessrecht”. Sein Forschungsschwerpunkt liegt auf der Erhebung und Verarbeitung von Daten im Strafverfahren.