Sammelband 2021

KriPoZ JuP

Kriminalpolitische Zeitschrift

KONTAKT
schriftleitung@kripoz.de

Herausgeber
Prof. Dr. Mark A. Zöller

Digitalisierung im Straf- und Strafprozessrecht

- Sammelband -

aus der Reihe:

KriPoZ | Junges Publizieren

in Zusammenarbeit mit

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

INHALT

VORWORT

Im Wintersemester 2020/21 fand an der Juristischen Fakultät der Ludwig-Maximilians-Universität München zum ersten Mal ein Grundlagen- und Schwerpunktseminar mit dem Generalthema „Digitalisierung im Straf- und Strafprozessrecht“ statt. Die schriftlichen Ausarbeitungen wurden im Spätsommer und Herbst 2020 angefertigt. Am 22. und 23. Januar 2021 folgten sodann die mündlichen Vorträge, die pandemiebedingt im Rahmen einer Videokonferenz gehalten werden mussten – ein weiterer Beleg dafür, wie weitreichend digitale Technik in unserem Alltagsleben Einzug gehalten hat. Das Ziel des Seminars lag darin, die Teilnehmerinnen und Teilnehmern mit aktuellen rechtspolitischen Fragestellungen im Bereich des materiellen und formellen Strafrechts vertraut zu machen, die in erheblichem Maße durch den Einfluss der Digitalisierung ausgelöst oder beeinflusst sind. Schließlich muss man kein Prophet sein, um zu wissen, dass es für künftige Juristinnen- und Juristengenerationen zu den wesentlichen Aufgaben- und Tätigkeitsfeldern gehören wird, den Prozess der Digitalisierung auch im Sicherheitsrecht gestaltend und kritisch zu begleiten.

Die einzelnen Seminarthemen weisen für universitäre Verhältnisse einen gehobenen Schwierigkeitsgrad auf. Insofern haben wir uns über das schon im Vorfeld der Veranstaltung von Seiten der Kriminalpolitischen Zeitschrift (KriPoZ) unterbreitete Angebot sehr gefreut, die besonders gelungenen Arbeiten im Forum Junges Publizieren einer breiteren Öffentlichkeit zugänglich machen zu dürfen. Für unsere Studierenden ist die erste eigene Publikation ein besonderer Anreiz und eine tolle Belohnung. Und das Forum ist ganz ohne Zweifel eine wichtige Plattform, um engagierte und begabte Nachwuchsjuristinnen und Nachwuchsjuristen frühzeitig an die nötigen wissenschaftlichen Standards für juristische Texte heranzuführen, von deren Beachtung sie für ihr gesamtes späteres Berufsleben profitieren könnten.

Dieser Sammelband enthält in alphabetischer Reihenfolge der Autorinnen und Autoren insgesamt acht Beiträge von Studierenden der LMU München, die allesamt mit Noten zwischen „vollbefriedigend“ und „sehr gut“ bewertet worden sind und einen selbst als betreuenden Dozenten doch mit einer nicht unerheblichen Freude darüber und einem gewissen Stolz darauf zurücklassen, wozu unsere Studierenden in der Lage sind. Sie haben das aus meiner Sicht richtig gut gemacht. Den Auftakt der Beitragsreihe macht *Anna Bildner* mit ihrer Arbeit zu „Zugriff auf und Auswertung von Massendaten im Strafverfahren“ und einem Blick auf aktuelle Herausforderungen, die sich für die Strafverfolgungspraxis zunehmend und nicht nur in Wirtschaftsstrafverfahren stellen. Im Anschluss daran ermöglicht *Yara von Baeckmann* unter Einbeziehung neuester Rechtsprechung von Europäischem Gerichtshof und Bundesverfassungsgericht einen Einblick in „Die Vorratsdatenspeicherung – eine (un-)endliche Geschichte“. *Maria Lesina* analysiert mit Blick auf Europa und die EU die Bestrebungen um eine „Europäische Herausgabe- und Sicherungsanordnung“. Im Anschluss daran beschäftigt sich *Theresa List* mit dem juristisch wie gesellschaftlich bedeutsamen Phänomen der „Strafverfolgung von Rechtsextremismus im Internet“ und den damit verbundenen Herausforderungen. *Ramon Kohler* bietet mit seiner Arbeit zu „Cybermobbing als Straftat“ ein engagiertes Plädoyer gegen ein weiteren wunden Punkt digitalisierter Gesellschaften, ebenso wie *Sabine Reschke* im Hinblick auf die „Strafbarkeit des Cyber-Grooming“. Wie sich aktuelle Probleme der Corona-Pandemie auf das geltende Strafprozessrecht auswirken, beleuchte *Laura Schachtner* in ihrer Arbeit „Der strafprozessuale Zugriff auf Handy-Daten und Gästelisten in Zeiten der Pandemie“. Den Abschluss bildet sodann der Beitrag von *Sophia Weis* „Der digitale Hausfriedensbruch als Straftat“, der ebenfalls die Frage nach gesetzgeberischem Reformbedarf stellt. Ich selbst habe bei der Lektüre und Korrektur aller Seminararbeiten viele neue Informationen, Ideen und Anregungen sammeln können. Möge es Ihnen als Leserinnen und Leser dieses Sammelbandes genauso ergehen!

Mein Dank gilt zunächst einmal den vorstehend genannten Seminarteilnehmerinnen und Seminarteilnehmern für

ihre klugen Gedanken und die Bereitschaft, ihre Texte für die Publikation in der Kriminalpolitischen Zeitschrift formal anzupassen. Meinem Münchner Lehrstuhlteam, insbesondere Frau Dr. *Tanja Niedernhuber*, Herrn *Ruben Doneleit*, Herrn *Dennis Falterbaum* und Herrn *Lauritz Öllerer*, bin ich für die redaktionelle Betreuung und Überarbeitung und die Vorbereitung der Publikation zu besonderem Dank verpflichtet. Und natürlich danken wir alle ganz besonders dem Team der KriPoZ aus Prof. Dr. *Anja Schiemann*, *Sabine Horn* und *Florian Knoop* an der Deutschen Hochschule der Polizei in Münster Hiltrup für ihre großartige Unterstützung und die Gastfreundschaft im Rahmen ihrer Zeitschrift.

Mark A. Zöller

KriPoZ Kriminalpolitische Zeitschrift JuP

„Junges Publizieren“

Seminararbeit von

Anna Bildner

Zugriff auf und Auswertung von Massendaten im Strafverfahren

Ludwig-Maximilians-Universität München
Juristische Fakultät
Prof. Dr. Mark A. Zöller
Abgabedatum: 26.10.2020

Inhaltsverzeichnis

I. Der Bedeutungszuwachs digitaler Beweismittel im Strafverfahren

Die Bedeutung digitaler Daten als Beweismittel für die Strafverfolgungsbehörden wächst stetig.[1] Ein Grund für diesen Bedeutungszuwachs ist in dem Phänomen „Big Data" zu sehen. Pausenlos werden allein durch die massenhafte Verbreitung von Smartphones vielfältige Daten über die Bevölkerung erhoben und ausgewertet. Noch nie zuvor bot eine solche Menge an Informationen in ihrer Zusammenschau einen derart detailreichen Einblick in die Persönlichkeiten der Bevölkerung.[2] Insoweit ist es mehr als naheliegend, dass auch die Strafverfolgungsbehörden ein immer größeres Interesse an digitalen Daten zeigen, um diese für wertvolle Ermittlungsansätze und schließlich als Beweismittel im Strafverfahren zu nutzen.[3] Dies geht jedoch zunächst mit rechtlichen und schließlich mit technischen Herausforderungen einher, welche im Folgenden dargestellt werden. Als Einführung in die Thematik gilt es zunächst die Besonderheiten digitaler Daten als Beweise und das Phänomen „Big Data" genauer darzustellen. Anschließend wird dargelegt, inwieweit die äußerst praxisrelevante Ermittlungsmaßnahme der Sicherstellung und Beschlagnahme gem. § 94 StPO den wachsenden Datenmengen begegnen kann, ohne dabei den Grundrechtsschutz der Betroffenen aus den Augen zu verlieren. Abschließend wird anhand der ermittlungstechnischen Methoden der IT-Forensik verdeutlicht, wie die Analyse von Massendaten effektiv gelingen kann und welcher gesetzlichen Normierungen es für eine rechtskonforme Anwendung bedarf.

II. Big Data und die allgemeinen Besonderheiten digitaler Beweise

1. Allgemeine Besonderheiten digitaler Beweise

Digitale Daten weisen als Beweismittel einige Besonderheiten auf, die es im Strafverfahren zu berücksichtigen gilt.[4] Im Kern lassen sich diese auf die fehlende Körperlichkeit zurückführen.[5] Digitale Daten sind nicht durch das menschliche Auge unmittelbar wahrnehmbar[6], sondern liegen in einer Notation aus zwei Variablen 0 und 1, genannt Bits oder Qubits vor.[7] Sie sind also Zahlenfolgen, die erst nach einem mehrstufigen Dechiffrierungsprozess als Beweismittel verwertbar sind und dann z.B. ein Foto, ein Dokument oder Standortdaten ergeben.[8] Die Verwertung digitaler Beweise erfolgt in der Hauptverhandlung üblicherweise auf dem Weg des Urkunden- oder Augenscheinbeweises.[9] Der Umwandlungsprozess in die wahrnehmbaren Formate geschieht wiederum mithilfe geeigneter Werkzeuge (Hard- oder Software).[10]

Dieser Verarbeitungsprozess bringt jedoch eine hohe Manipulationsanfälligkeit und das Risiko des Datenverlustes mit sich.[11] Zwar sind Manipulationen von Beweisen kein allein digitales Phänomen, allerdings gehen die Bearbeitungsmöglichkeiten weiter als bei analogen Beweismitteln. Benötigt werden lediglich ein Bearbeitungsprogramm und rudimentäre IT-Kenntnisse, um Texte oder Bilder zu verändern.[12] Meist haben mehrere Personen Zugriff auf die Datensätze und eine stabile Internetverbindung ermöglicht den Zugriff völlig ortsungebunden, z.B. durch die

1 *Warken,* NZWiSt 2017, 289 (289).
2 *Blechschmitt*, MMR 2018, 361 (361).
3 *Blechschmitt*, MMR 2018, 361 (363).
4 *Momsen*, in: FS Beulke, 2015, S. 871 (875).
5 *Warken,* NZWiSt 2017, 449 (449).
6 *BGH*, NJW 2012, 244 (245).
7 *Warken,* NZWiSt 2017, 289 (291).
8 *Fährmann,* MMR 2020, 228 (229).
9 *Sieber*, Gutachten C zum 69. Deutschen Juristentag, 2012, S. 67.
10 *Savić*, Die digitale Dimension des Strafprozessrechts, 2020, S. 48.
11 *Momsen*, in: FS Beulke, 2015, S. 871 (877).
12 *Knopp,* ZRP 2008, 156 (157).

Nutzung von Cloudspeicherungen.[13] Diese leichte Veränderbarkeit ist ein Unsicherheitsfaktor, der die Richtigkeit der durch das Beweismittel behaupteten Tatsache in Frage stellen kann und sich dadurch auch auf den Beweiswert digitaler Daten auswirkt.[14]
Eine weitere Herausforderung ist die eindeutige Zuordnung der Daten zu konkreten Individuen aufgrund der Möglichkeit anonymen Agierens im Internet, welche z.B. durch die Nutzung von Aliasidentiäten im Darknet entsteht.[15] Die Speicherung digitaler Daten erfolgt mittlerweile zunehmend im Ausland, was Zuständigkeitsfragen aufwirft.[16] Zudem geht die Erhebung digitaler Beweismittel, insbesondere von Massendaten, mit einer spezifischen Grundrechtsrelevanz einher.[17]

2. Das Phänomen „Big Data"

Eine weitere Besonderheit digitaler Beweismittel ist das Phänomen „Big Data". Der Begriff kennt keine allgemeingültige Definition.[18] Charakteristisch für das Phänomen ist die Komplexität der Daten, welche mit den „vier V`s"[19] umschrieben wird: Volume (Datenvolumen), Velocity (Datengeschwindigkeit), Variety (Datenvielfalt) und Veracity (Datenqualität). Big Data macht es also möglich, riesige Datenmengen aus unterschiedlichen Quellen in hoher Geschwindigkeit, teilweise sogar in Echtzeit zu sammeln, zu analysieren, auszuwerten und damit Aussagen über immer mehr Lebensbereiche zu treffen.[20] Die Masse der Daten findet ihre Ursache unter anderem in der Menge unterschiedlicher Datenquellen. Längst hat sich ein Großteil unseres Lebens von der analogen in die digitale Welt verlagert: mit elektronischen Foto- und Videoaufnahmen, kommunizierender Alltagstechnik, bargeldlosem Zahlen und der Teilnahme an Social-Media-Diensten seien nur ein paar Beispiele genannt. Auch im öffentlichen Bereich werden ständig elektronische Daten etwa in der Finanzverwaltung, bei den Krankenkassen und durch die Videoüberwachung öffentlicher Plätze erhoben.[21] Außerdem gelangen immer mehr internetfähige Geräte auf den Markt (sog. Internet of Things), welche sich untereinander vernetzen, wodurch unmittelbar große Datenmengen entstehen.[22] Die Strafverfolgung steht nun vor der Herausforderung, dieser Informationsflut zu begegnen.

III. Der Zugriff auf Massendaten im Strafverfahren

Aufgrund wachsender Datenmengen gibt es „mehr Sachverhalt"[23], den es gemäß dem rechtsstaatlichen Legalitätsprinzip (§ 152 Abs. 2 StPO) umfassend zu erforschen gilt. Gleichzeitig führt der technische Fortschritt zu besseren Auswertungsmöglichkeiten der gewonnenen Daten.[24] Im Folgenden wird die Erhebung digitaler Datenmengen auf Grundlage der Strafprozessordnung (StPO) und die Auswertung der dadurch gewonnenen Informationen beleuchtet. Im Fokus steht dabei der offene Zugriff auf gespeicherte Daten gem. §§ 94 ff. StPO. Anschließend wird beantwortet, wie mit der Hilfe von IT-Forensik die Auswertung großer Datenmengen gelingen kann.

13 *Warken,* NZWiSt 2017, 289 (295).
14 *Momsen*, in: FS Beulke, 2015, S. 871 (875).
15 *Müller,* NZWiSt 2020, 96 (100).
16 *Warken,* NZWiSt 2017, 417 (421 ff.).
17 *Warken,* NZWiSt 2017, 289 (293 f.).
18 *Dorschel*, Praxishandbuch Big Data, 2015, S. 6.
19 *Dorschel*, S. 6 ff.
20 *Savić*, S. 26.
21 *Warken,* NZWiSt 2017, 329 (332).
22 *Warken*, NZWiSt 2017, 329 (333).
23 *Schneider,* ZIS 2020, 79 (80).
24 *Singelnstein,* in: Hoffmann-Riem, Big Data – Regulative Herausforderungen (2018), S. 179 (181).

1. Bisherige gesetzgeberische Entwicklungen

Um den Herausforderungen der Digitalisierung angemessen begegnen zu können, war in den letzten Jahren gerade der Bereich der Telekommunikation (§§ 100a ff. StPO) ständigen Veränderungen ausgesetzt.[25] Mit den im Sommer 2017 eingeführten Regelungen zur Quellen-TKÜ (§ 100a StPO) und der verfassungsrechtlich umstrittenen[26] Online-Durchsuchung (§ 100b StPO) wurden die strafprozessualen Befugnisse erheblich ausgeweitet und sorgten für Diskussionen.[27]

Im Bereich der auf körperliche Gegenstände zugeschnittenen Rechtsgrundlagen der Sicherstellung und Beschlagnahme (§§ 94 ff. StPO) wird den informationstechnischen Entwicklungen hingegen seit der Entstehung der StPO im Jahr 1877 trotz ihrer praktischen Relevanz[28] nur vereinzelt Rechnung getragen.[29] Exemplarisch sind hier die Vorschriften über die Rasterfahndung in § 98c StPO und § 98a StPO zu nennen.[30] Mit der Umsetzung der Cybercrime Konvention[31] des Europarates wurde außerdem § 110 Abs. 3 StPO geschaffen, wonach die Durchsicht eines elektronischen Speichermediums „auch auf hiervon getrennte Speichermedien" erfolgen darf, „soweit auf sie von dem Speichermedium aus zugegriffen werden kann". Die Konvention enthält zudem in Art. 19 Abs. 3 Regelungen zur Sicherstellung gespeicherter Computerdaten, welche ein besonderes Augenmerk auf Sicherung der Integrität der Daten legen. [32] Dies hat sich der deutsche Gesetzgeber allerdings noch nicht zum Vorbild genommen, sondern erkennt die §§ 94 ff. StPO auch in der digitalen Welt als noch ausreichend an.[33] Daran schließt sich die Frage an, ob der Rückgriff auf für analoge Beweismittel intendierte Normen dem Phänomen Big Data mit besonderem Blick auf den Grundrechtsschutz der Betroffenen überhaupt noch gerecht werden kann.

2. Sicherstellung und Beschlagnahme gem. §§ 94 ff. StPO

Sinn und Zweck der Sicherstellung und Beschlagnahme gem. §§ 94 ff. StPO ist die Sicherung des Strafverfahrens.[34] Um den Verlust von Beweismitteln zu verhindern, müssen diese in staatlichen Gewahrsam genommen werden.[35] Im Zusammenhang mit der Erhebung von Massendaten werden die Vorschriften vor allem in umfangreichen Wirtschaftsstrafverfahren bei Sicherstellung großer EDV-Systeme relevant.[36] Doch auch in anderen Bereichen finden die §§ 94 ff. StPO ihre Anwendung, etwa bei der Sicherstellung von Smartphones, welche als Beweismittel aus modernen Strafprozessen nicht mehr wegzudenken sind.[37]

a) Allgemeine Voraussetzungen

Laut § 94 Abs. 1 StPO haben die Strafverfolgungsbehörden die Befugnis zur Sicherstellung von „Gegenständen", die z.B. bei einer Durchsuchung des Beschuldigten oder Dritten (§§ 102, 103 StPO) gefunden werden, sofern diese

25 *Sieber/Brodowski*, in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 52. EL April (2020), Teil 19.3, Rn. 8.
26 *Gercke*, in: HK-StPO, 6. Aufl. (2019), § 100b Rn. 7; *Roggan,* StV 2017, 821 (826 ff.).
27 BGBl. 2017 I Nr. 58; dazu *Singelnstein/Derin,* NJW 2017, 2646 ff.
28 *Park*, Durchsuchung und Beschlagnahme, 4. Aufl. (2018), § 1 Rn. 1.
29 *Schilling/Rudolph/Kuntze,* HRRS 2013, 207 (209).
30 BGBl. 1992 I S. 1302.
31 Convention on Cybercrime vom 21.11.2001, ETS Nr. 185, abrufbar unter: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008157a. (zuletzt abgerufen am 25.10.20).
32 *Sieber/Brodowski,* in: Hoeren/Sieber/Holznagel, Teil 19.3, Rn. 9.
33 BVerfGE 124, 43 (58f.).
34 *Wohlers/Greco*, in: SK-StPO, 5. Aufl. (2016), § 94 Rn. 1.
35 *Hauschild*, in: MüKo-StPO, 2014, § 94 Rn. 1.
36 *Schneider,* ZIS 2020, 79 (79); *Basar/Hièramente,* NStZ 2018, 681 (681).
37 *Wenzel,* NZWiSt 2016, 85 (86).

für die Beweisführung von Bedeutung sein können.[38] Beweisgegenstände können im Allgemeinen alle beweglichen oder unbeweglichen Sachen sein, die die Eigenschaft eines körperlichen Gegenstandes erfüllen.[39] Erst wenn die freiwillige Herausgabe verweigert wird, kann die förmliche Beschlagnahme (§ 94 Abs. 2 StPO) durch den Richter oder bei Gefahr im Verzug, durch die Staatsanwaltschaft oder ihre Ermittlungspersonen angeordnet werden (§ 98 Abs. 1 S. 1 StPO).[40] Anordnungsvoraussetzung ist lediglich der Anfangsverdacht i.S.d. § 152 Abs. 2 StPO.[41] Die Beschlagnahme darf aber keinesfalls ins „Blaue hinein" erfolgen, vielmehr bedarf es konkreter Anhaltspunkte, weshalb eine Straftat nach aktuellem Kenntnisstand zumindest möglich erscheint.[42] Schließlich darf das Objekt der Sicherstellung keinem Beschlagnahmeverbot i.S.d. § 97 StPO unterliegen.[43]

b) Daten als „Gegenstände" i.S.d. § 94 StPO

Im Jahr 1877 konnte der historische Gesetzgeber die rasante technische Entwicklung noch nicht vorhersehen, sodass die §§ 94 ff. StPO ursprünglich für analoge Beweismittel geschaffen wurden.[44] Fraglich ist, ob auch digitale Daten unter den Anwendungsbereich des § 94 ff. StPO fallen. Einigkeit besteht darin, dass § 94 StPO die Sicherstellung und Beschlagnahme von Datenträgern zulässt.[45] Umstritten ist hingegen, ob digitale Daten selbst sichergestellt werden können. Der Wortlaut „Gegenstände" ließe vermuten, dass digitale Daten aufgrund ihrer fehlenden Körperlichkeit, aus dem Anwendungsbereich auszuschließen seien, da man sonst den Wortlaut überdehne. Der Beschlagnahme unterlägen danach ausschließlich körperliche Speichermedien nicht aber die Daten selbst, diese wären keine Gegenstände i.S.d. Vorschrift.[46]
Das *BVerfG* erkennt an, dass die §§ 94 ff. StPO „zwar ursprünglich auf körperliche Gegenstände zugeschnitten seien", der „Wortsinn" des § 94 StPO gestatte jedoch auch die Einbeziehung nichtkörperlicher Gegenstände. Außerdem werde der Wortlaut schon mit Blick auf die Unterscheidung zum engeren Begriff der körperlichen Sache nicht überschritten.[47] Digital gespeicherte Informationen lägen somit innerhalb des Anwendungsbereichs.[48] Die Auslegung für die analoge Welt geschaffener Normen im digitalen Kontext erscheint zumindest fragwürdig und bringt Unsicherheiten mit sich. Insbesondere das verfassungsmäßig geforderte Gebot der Normklarheit wird dadurch berührt.[49] Die höchstrichterliche Rechtsprechung sieht § 94 StPO allerdings als hinreichend bestimmt an, sodass über § 94 StPO auch der Zugriff auf digitale Daten selbst erfolgen kann.[50] Der Streit entfaltet grundsätzlich „eher theoretischen Charakter und weniger praktische Relevanz"[51], da in der Ermittlungspraxis ohnehin zumeist physische Trägermedien sichergestellt werden, welche problemlos unter den Gegenstandsbegriff subsumiert werden können.[52] Es gilt trotzdem festzuhalten, dass der Zugriff auf umfassende Datenbestände gem. § 94 StPO lediglich auf Grundlage eines Anfangsverdachts damit unter den „denkbar geringsten Voraussetzungen"[53] möglich ist.

38 *Sieber/Brodowski*, in Hoeren/Sieber/Holznagel, Teil 19.3, Rn. 71.
39 *Gercke*, in: HK-StPO, § 94 Rn. 8.
40 *Köhler*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl. (2020), § 94 Rn. 13.
41 *Gercke*, in: HK-StPO, § 94 Rn. 31.
42 *Greven*, in: KK-StPO, 8. Aufl. (2019), § 94 Rn. 8.
43 *Köhler*, in: Meyer-Goßner/Schmitt, StPO, § 94 Rn. 20.
44 *Jahn/Brodowski*, in: Hoven/Kudlich, Digitalisierung und Strafverfahren (2020), S. 67 (72).
45 *Gercke*, in: HK-StPO, § 94 Rn. 17.
46 *Gercke*, in: HK-StPO, § 94 Rn. 18; *Kemper*, NStZ 2005, 538 (541); *Roxin/Schünemann*, Strafverfahrensrecht, 29. Aufl. (2017), § 43 Rn. 4; *Bär*, Handbuch zur EDV-Beweissicherung, 2007, Rn. 407; *Roggan*, NJW 2015, 1995 (1999).
47 BVerfGE 124, 43 (63).
48 BVerfGE 113, 29 (51 f.); *BVerfG*, NJW 2006, 976 (980); *BVerfG*, NJW 2009, 2431 (2434).
49 *Ludewig,* KriPoZ 2019, 293 (296).
50 BVerfGE 113, 29 (51 f.); BVerfGE 115, 166 (191 ff.).
51 *Bär*, Rn. 407.
52 *Gercke*, in: HK-StPO, § 94 Rn. 18.
53 *Singelnstein,* NStZ 2012, 593 (597).

c) Beschlagnahme von Telekommunikationsdaten

Ein spezielles Problem ist die Frage, inwiefern auf Grundlage des § 94 StPO eine Beschlagnahme von Telekommunikationsdaten erfolgen kann. Die Problemstellung lässt sich am Kommunikationsmedium der E-Mail erläutern. Dafür muss zwischen drei Mediums-Zuständen unterschieden werden: Die E-Mail kann sich erstens noch im laufenden Übertragungsvorgang befinden, zweitens noch bei Sender oder bereits beim Empfänger befinden oder drittens beim Anbieter zwischengespeichert sein.[54] Nach der Rechtsprechung des *BVerfG*[55] gehören Daten, die sich in der zweiten Phase befinden zu den sicherstellungsfähigen Gegenständen i.S.d. § 94 StPO, wenn diese bei Sender- oder Empfänger gespeichert sind. Der Kommunikationsvorgang hat dann noch nicht begonnen oder ist bereits abgeschlossen. Die Daten befinden sich damit im Herrschaftsbereich der Kommunikationsteilnehmer, die dann selbst über eine Speicherung oder Löschung der Daten entscheiden, sodass lediglich das Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs.1 i.V.m. Art. 1 Abs. 1 GG berührt ist.[56]

Befindet sich die E-Mail noch im laufenden Übertragungsvorgang ist Art. 10 Abs. 1 GG betroffen. Das Grundrecht schützt die Vertraulichkeit der Kommunikation und soll sicherstellen, dass die Grundrechtsträger ohne Vorbehalte kommunizieren können.[57] Die Datenerhebung erfolgt dann durch Ausleitung während des Kommunikationsvorgangs. Dies geschieht durch einen heimlichen und damit besonders intensiven Grundrechtseingriff, der nur auf Basis des § 100a StPO und seinen strengeren Voraussetzungen erfolgen kann.[58] Komplizierter ist der Zugriff auf beim Provider zwischengespeicherte Daten.

Das *BVerfG* sieht in dieser Phase den Schutzbereich des Art. 10 Abs. 1 GG ebenfalls als eröffnet an und nimmt damit eine Erweiterung dessen vor.[59] Jede Kenntnisnahme kommunikativer Daten stelle ohne Einwilligung des Betroffenen einen Grundrechtseingriff dar.[60] Die Auslagerung der E-Mails auf den nicht im Herrschaftsbereich des Nutzers liegenden Server des Providers habe nicht automatisch das Einverständnis des Nutzers eines Drittzugriffs zur Folge.[61] Aus diesem Mangel an Beherrschbarkeit ergebe sich vielmehr eine besondere Schutzbedürftigkeit, welche eine Verlängerung des Grundrechtsschutzes rechtfertige.[62] Trotz der Eröffnung des Schutzbereichs des Art. 10 Abs. 1 GG, betrachtet das *BVerfG* die §§ 94 ff. StPO als verfassungsmäßige Ermächtigungsgrundlage für diesbezügliche Grundrechtseingriffe.[63] Bisher war es einhellige Ansicht, dass die alleinige Rechtsgrundlage für Eingriffe in Art. 10 Abs. 1 GG in § 100a StPO zu sehen sei.[64] Die Eröffnung des Schutzbereiches von Art. 10 Abs. 1 GG schloss die Anwendung des § 94 StPO aus. Das *BVerfG* argumentiert nun, solange der Eingriff in Art. 10 Abs. 1 GG offen und punktuell erfolge, sei dieser durch § 94 StPO hinreichend gerechtfertigt.[65] Damit erfolgt die Bestimmung der Rechtsgrundlage nicht anhand des betroffenen Schutzbereichs, sondern anhand der Offen- oder Verdecktheit der geplanten Maßnahme.[66] Somit kann der offene Zugriff auf E-Mails, die beim Provider zwischengespeichert sind nach § 94 StPO erfolgen. Eine Katalogtat wie bei einem Zugriff nach § 100a StPO muss nicht vorliegen.[67] Diese Argumentation kann nicht überzeugen. Für den Nutzer ist es so letztendlich unerheblich, ob

54 *Singelnstein*, NStZ 2012, 593 (596); unabhängig davon, ob man den Prozess insgesamt in 3, 4 oder 7 Phasen unterteilt vgl. dazu *Brodowski,* JR 2009, 402.
55 *BVerfG*, NJW 2009, 2431 (2433).
56 BVerfGE 115, 166 (Ls. 1).
57 BVerfGE 85, 386 (389); BVerfGE 100, 313 (363).
58 *Singelnstein,* NStZ 2012, 593 (595).
59 BVerfGE 124, 43 (56).
60 BVerfGE 85, 386 (398).
61 *BVerfG*, MMR 2009, 673 (675).
62 BVerfGE 124, 43 (72).
63 BVerfGE 124, 43 (58 ff.).
64 *Krüger,* MMR 2009, 673 (682).
65 BVerfGE 124, 43 (58 ff.).
66 *Singelnstein,* NStZ 2012, 593 (596); *Kasiske,* StraFo 2010, 228 (230 f.); *Klein,* NJW 2009, 2996 (2998).
67 *Kasiske,* StraFo 2010, 228 (232).

seine Nachrichten durch Art. 10 Abs. 1 GG geschützt sind, wenn auf diese unter den deutlich einfacheren Voraussetzungen des § 94 StPO zugegriffen werden kann und der Schutz dadurch geschwächt wird.[68] Es ist außerdem nicht plausibel, dass für einen einheitlichen Kommunikationsvorgang je nach Phase andere Eingriffsvoraussetzungen gelten sollten. Richtigerweise müsste immer § 100a StPO einschlägig sein.[69] Die dargelegte Rechtsprechung lässt sich auch auf anderen Formen der Telekommunikation übertragen, bei denen eine Speicherung erfolgt.[70] Dazu gehören die Daten eines Nutzerkontos in sozialen Netzwerken sowie Cloud-Inhalte.[71] Folgt man der Ansicht des *BVerfG*, ist die Erhebung von umfassenden Kommunikationsdaten in der Praxis sowohl beim Beschuldigten als auch im Zwischenspeicher des Providers, nach § 94 StPO allein unter der Voraussetzung des Anfangsverdachts möglich. Die fehlende Beschränkung auf Seite der Rechtsgrundlage muss folglich durch die Begrenzung anhand verfassungsrechtlicher Grundsätze ausgeglichen werden.[72]

3. Grundrechtliche Grenzen des § 94 StPO

Die Strafverfolgung ist gem. Art. 1 Abs. 3 GG an die Grundrechte gebunden. Maßnahmen nach § 94 können also potentiell in verschiedene Grundrechte eingreifen.[73] Sofern nicht das speziellere Grundrecht der Telekommunikationsfreiheit gem. Art. 10 Abs. 1 GG eingreift[74], bildet im Bereich der Datenerhebung das allgemeine Persönlichkeitsrecht gem. Art. 2 Abs. 1 GG die Basis des grundrechtlichen Schutzes. Dieser Schutz wird bei der Sicherstellung umfangreicher Datenmengen durch das Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i.V.m. Art. I Abs. 1 GG verstärkt[75], welches die Befugnis des Einzelnen umfasst, „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“[76]. Der Schutzumfang beschränkt sich dabei nicht auf Informationen, die bereits ihrer Art nach sensibel sind und schon deshalb grundrechtlich geschützt werden, sondern umfasst auch personenbezogene Daten, die für sich genommen nur einen geringen Informationsgehalt haben.[77] Aufgrund der umfassenden technischen Möglichkeiten gäbe es kein „belangloses Datum“[78]; auch eine für sich unwichtige Information kann im Zusammenspiel mit anderen Informationen Rückschlüsse auf den Betroffenen zulassen.[79] Noch nicht abschließend geklärt ist welche Bedeutung dem subsidiären Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme (sog. IT-Grundrecht)[80], welches sich ebenfalls aus Art. 2 Abs.1 i.V.m. Art. 1 Abs. 1 GG herleiten lässt, für § 94 StPO zukommt.[81]

a) Besondere Eingriffsintensität der Maßnahme

Eine Maßnahme nach § 94 StPO geht aufgrund der Vielzahl vorzufindender Daten und der daraus folgenden großen Streubreite des Informationsgehalts regelmäßig mit einer besonderen Eingriffsintensität einher. Von der Da-

68 *Krüger*, MMR 2009, 673 (683).
69 *Roxin/Schünemann*, § 36 Rn. 6; *Wohlers/Greco*, in: SK-StPO, § 94 Rn. 27.
70 *Singelnstein,* NStZ 2012, 593 (597).
71 *Köhler*, in: Meyer-Goßner/Schmitt, StPO, § 94 Rn. 16b; *Blechschmitt,* MMR 2018, 361 (364).
72 *Singelnstein,* NStZ 2012, 593 (597).
73 *Gercke*, in: HK-StPO, § 94 Rn. 4.
74 BVerfGE 124, 43 (Ls. 1).
75 BVerfGE 113, 29 (45).
76 BVerfGE 65, 1 (Ls. 1)
77 BVerfGE 120, 274 (312); vgl. BVerfGE 118, 168 (184 f.).
78 BVerfGE 65, 1 (45).
79 *Di Fabio,* in: Maunz/Dürig-GG, 91. EL (April 2020), Art. 2 I Rn. 174.
80 BVerfGE 120, 274 (Ls. 1).
81 *Sieber/Brodowski*, in: Hoeren/Sieber/Holznagel, Teil 19.3, Rn. 66.

tenbeschlagnahme sind häufig nicht allein der Beschuldigte, sondern regelmäßig auch Dritte, etwa der Kommunikationspartner oder Zugangsberechtigte, wie Kommunikationsdienstleister, in ihren Grundrechten betroffen, auch wenn sie in keiner Beziehung zum Tatvorwurf stehen.[82] Auch der Umfang des erlangten Datenvolumens intensiviert die Eingriffstiefe.[83] Während eine einzelne Information zum Aufenthaltsort des Beschuldigten keine besonderen Rückschlüsse erlaubt, kann eine hinreichend große Zahl von zeitbezogenen Daten die Erstellung eines ganzen Bewegungsprofils ermöglichen. Auch die Erhebung von Daten aus dem Browserverlauf oder die Kenntnisnahme durchgeführter Downloads, kann den Betroffenen in seinen Lebensbereichen stark berühren.[84] Ein weiterer Einflussfaktor auf die Eingriffsintensität ist die Offen- oder Verdecktheit einer Maßnahme. Heimliche Eingriffe unterliegen aufgrund der fehlenden Einflussmöglichkeiten des Betroffenen einer höheren Rechtfertigung.[85] § 100e Abs. 2 S. 1 StPO normiert daher für die Onlinedurchsuchung (§ 100b StPO), dass ihre Anordnung durch die zuständige Kammer am Landgericht erfolgen muss. Bei Gefahr im Verzug kann der Vorsitzende entscheiden (§ 100e Abs. 2 S. 2 StPO), nicht aber die Staatsanwaltschaft und ihre Ermittlungspersonen, wie dies gem. § 98 Abs. 1 S. 1 StPO bei § 94 StPO der Fall ist. Für Eingriffe gem. § 100b StPO muss außerdem der Verdacht einer besonders schweren Straftat gem. § 100b Abs. 2 StPO vorliegen. Begründet wird die niedrigere Eingriffsschwelle für § 94 StPO damit, dass dieser nur offene und punktuelle Eingriffe erlaubt. Führt man sich aber die umfassenden Datenmengen, welche auf Grundlage des § 94 StPO z.B. aus einem Smartphone ausgelesen werden können vor Augen, besteht hinsichtlich des möglichen Umfangs der gewonnenen Daten zumindest eine Nähe zur Online-Durchsuchung.[86]

b) Anforderungen an den Verhältnismäßigkeitsgrundsatz

Die besondere Eingriffsintensität des § 94 StPO erfordert eine besondere Achtung des Verhältnismäßigkeitsgrundsatzes, welcher als übergeordnete Regel staatlichen Handelns auch im Strafverfahren gilt.[87] Vor allem im Beschlagnahmerecht kommt dem Grundsatz aufgrund der weiten Formulierungen im Gesetzestext erhebliche Bedeutung zu.[88] Die Sicherstellung muss daher zur Erreichung ihres Zwecks geeignet und erforderlich sein und in einem angemessenen Verhältnis zur Schwere der Tat und zur Stärke des Tatverdachts stehen.[89] Aus gleich geeigneten Maßnahmen ist stets diejenige mit der geringsten Grundrechtsbeeinträchtigung zu wählen.[90] Dabei ist vor allem die Beschränkung des zulässigen Umfangs der Datenbeschlagnahme in sachlicher, inhaltlicher und zeitlicher Hinsicht von Bedeutung.[91]

aa) Begrenzung auf verfahrensrelevante Daten

Der Grundsatz der Verhältnismäßigkeit begrenzt auch das rechtsstaatliche Legalitätsprinzip (§ 152 Abs. 2 StPO).[92] Es ist daher die verfassungsrechtliche Aufgabe der Strafverfolgungsbehörden den Zugriff auf verfahrensrelevante

82 Vgl. BVerfGE 100, 313 (380); BVerfGE 107, 299 (320f.).
83 Vgl. BVerfGE 113, 29 (55 ff.).
84 *Warken,* NZWiSt 2017, 289 (293).
85 *BVerfG*, NJW 2007, 2464 (2469f.).
86 *Ludewig,* KriPoZ 2019, 293 (297) m.V.a. *Momsen,* DRiZ 2018, 140 (143).
87 BVerfGE 20, 162 (187).
88 *Menges*, in: LR-StPO, 27. Aufl. (2019), § 94 Rn. 51.
89 BVerfGE 20, 162 (186); *Köhler,* in: Meyer-Goßner/Schmitt, StPO, § 94 Rn. 18.
90 *Grzeszick*, in: Maunz/Dürig-GG, Art. 20 VII Rn. 113.
91 *Sieber/Brodowski*, in: Hoeren/Sieber/Holznagel, Teil 19.3, Rn. 91.
92 BVerfGE 44, 353 (373).

Gegenstände zu beschränken.[93] Im Zeitalter von Big Data fällt es jedoch immer schwerer zwischen relevanten und irrelevanten Daten zu unterscheiden, sodass die Gefahr überschießender Beweisgewinnung entsteht.[94] Um eine umfassende Sachverhaltsaufklärung zu ermöglichen und keine beweisrelevanten Daten zu übersehen, gehen Ermittler in der Praxis oft nach der „Staubsaugermethode“[95] vor. Dies wiegt besonders schwer, wenn unbeteiligte Dritte von der Maßnahme betroffen sind.[96] Die Lösung dieses Problems steht vor praktischen Schwierigkeiten: Zum einen ist eine Trennung relevanter Daten von irrelevanten Daten schon aufgrund der fehlenden körperlichen Teilbarkeit schwer möglich. Außerdem ist den Daten ihr Inhalt nicht von außen anzusehen.[97] Ist noch nicht absehbar, inwieweit die Daten strafrechtlich relevante Informationen enthalten, können sie nicht gem. § 94 StPO sichergestellt werden. Hier kommt die vorläufige Sicherstellung gem. § 110 StPO ins Spiel, welche gerade auf die Feststellung potentieller Beweismittel abzielt[98] und laut *BVerfG* eine Begrenzung auf verfahrensrelevante Daten somit erst möglich mache.[99] Die Norm erlaubt die Durchsicht von „Papieren“ auf ihre Beweisrelevanz, um zu einem späteren Zeitpunkt über eine Beschlagnahme zu entscheiden.[100] Damit geht die Anwendung der Norm ähnlich der Handhabung bei § 94 StPO über den Wortlaut hinaus.[101] Um den praktischen Bedürfnissen der Staatsanwaltschaft gerecht zu werden, werden auch Unterlagen in Form digitaler Daten vom Begriff „Papiere“ umfasst.[102] Das *BVerfG* sieht in § 110 StPO eine mildere Maßnahme gegenüber der Beschlagnahme, da sie lediglich einen vorübergehenden Eingriff zur Feststellung der Beweiserheblichkeit bezweckt. Die Beschlagnahme wirkt hingegen bis zum Verfahrensabschluss, wodurch der staatliche Zugriff intensiviert würde.[103] Aufgrund des weiten Ermessensspielraums[104] erfolgt in der Praxis regelmäßig ein umfassender Zugriff auf den gesamten Datenbestand, was zu einer „vollständigen Durchleuchtung“[105] des Betroffenen führt. Über § 110 Abs. 3 StPO kann außerdem der Zugriff auf Cloud-Daten legitimiert werden, sofern sie vom Datenspeicher aus erreichbar sind und sich im Inland befinden.[106] Sieht man den Schwerpunkt des Eingriffs in der Offenlegung der Daten und nicht in dem vorübergehenden Datenentzug ist § 110 StPO gegenüber § 94 Abs. 2 StPO keinesfalls die mildere Maßnahme.[107] Die Eingriffstiefe wird zudem verstärkt, wenn der Datenträger aufgrund von Verschlüsselungen oder aufgrund des Datenvolumens in die Diensträume der Behörden mitgenommen werden müssen.[108] Die Durchsicht muss dann zügig geschehen.[109] Auch § 110 StPO rückt damit in die Nähe der verdeckten Maßnahmen. Zwar ist die Maßnahme dem Einzelnen bekannt und damit eine richterliche Überprüfung gem. § 98 Abs. 2 StPO möglich, allerdings zeigen die fehlende sachliche und zeitliche Begrenzung der Durchsicht sowie das nur vage zugestandene Anwesenheitsrecht[110], dass ihr wesentliche Gesichtspunkte einer offenen Maßnahme fehlen.[111] Folglich kann § 110 Abs. 1 StPO zwar den Umfang der beschlagnahmten Daten reduzieren, das Ausmaß der offengelegten Informationen ist jedoch ebenfalls enorm. Die Durchsicht der Daten darf dabei nur von der Staatsanwaltschaft und ihren Ermittlungspersonen (§ 152 GVG) durchgeführt werden, § 110 Abs. 1 StPO. In der Praxis sind dies meist eigens ausgebildete und

93 BVerfGE 113, 29 (Ls. 2).
94 Vgl. *BVerfG,* NJW, 2005, 1917, (1920 ff.).
95 *Basar/Hièramente,* NStZ 2018, 681 (681).
96 *Warken,* NZWiSt 2017, 289 (293).
97 *Czerner,* in: Labudde/Spranger, Forensik in der digitalen Welt (2017), S. 265 (271).
98 *Köhler*, in: Meyer-Goßner/Schmitt, StPO, § 110 Rn. 2.
99 *BVerfG*, NJW 2005, 1917 (1921).
100 *Köhler*, in: Meyer-Goßner/Schmitt, StPO, § 110 Rn. 2.
101 *Ludewig,* KriPoZ 2019, 293 (298).
102 Vgl. BVerfGE 113, 29 (51).
103 *BVerfG*, NJW 2005, 1917 (1921).
104 Vgl. *BGH*, NJW 1995, 3397 (3397).
105 *Peters,* NZWiSt 2017, 465 (473).
106 *Gercke,* in: HK-StPO, § 110 Rn. 16.
107 *Peters,* NZWiSt 2017, 465 (468).
108 *Ludewig,* KriPoZ 2019, 293 (298).
109 *BGH*, NStZ 2003, 670 (671).
110 Für eine gesetzliche Festschreibung *Peters*, NZWiSt 2017, 465 (469 ff.).
111 Vgl. *Peters,* NZWiSt 2017, 465 (469).

erfahrene Ermittlungspersonen im Bereich der IT-Forensik.[112] Bei fehlender Expertise ist allgemein anerkannt, dass die Staatsanwaltschaft im Stadium der Durchsicht, im Falle besonders spezieller und unbekannter Sachverhalte auf externe EDV-Sachverständige zurückgreifen darf (§§ 161 Abs.1, S. 1, 72 ff. StPO).[113] Eine eigenverantwortliche Durchsicht der Daten durch den externen Sachverständigen ist jedoch unzulässig.[114]

bb) Kopieren von Daten als eingriffsschwächere Methode?

Die Beschlagnahme kann entweder durch die Mitnahme des physischen Datenträgers oder durch die Erstellung einer Kopie erfolgen.[115] Dabei stehen sich zwei Prinzipien gegenüber. Zum einen fordert das Unmittelbarkeitsprinzip als Prozessmaxime, dass bei sachlichen Beweisen – zu denen auch Datenträger und Daten zählen – die Tatsachen aus der Quelle selbst geschöpft werden müssen und grundsätzlich keine Beweissurrogate genügen.[116] Das Beweismittel ist daher stets im Original zu sichten.[117] Bei Kopien schwinge ein gewisses Verfälschungsrisiko mit, was den Beweiswert der Daten schwächen könne.[118] Dies spräche dafür Datenträger stets selbst zu beschlagnahmen. Mit der körperlichen Sicherstellung und dem damit verbundenen Nutzungsentzug geht jedoch ein zusätzlicher Grundrechtseingriff in Art. 14 Abs. 1 GG einher.[119] Können IT-Systeme eines Unternehmens für einen längeren Zeitraum nicht genutzt werden, kann dadurch enormer wirtschaftlicher Schaden entstehen. Dem Verhältnismäßigkeitsgrundsatz ist deshalb auch mit Blick auf den Nutzungsentzug Rechnung zu tragen, was für die Erstellung einer Sicherungskopie spricht. Allerdings gilt es zunächst zu klären, inwieweit es rechtmäßig ist, Sicherungskopien zu erstellen.[120] Dazu müsste § 94 Abs. 1 StPO neben dem Zugriff auf die Originaldaten auch das Anfertigen von Kopien dieser Daten erlauben.[121]

Der Wortlaut „in Verwahrung nehmen“ umfasst nur die tatsächliche Mitnahme der Datenträger. *Bär*[122] sieht in der Anfertigung einer Sicherungskopie eine Sicherstellung „in anderer Weise“ gem. § 94 Abs. 1 StPO. Der Zweck der Maßnahme, die Herstellung staatlicher Sachherrschaft über den Beweisgegenstand zur Verfahrenssicherung, könne auch ohne Mitnahme des IT-Systems selbst gelingen. Dies ist überzeugend. Auch bei analogen Beweismitteln ist das Erstellen von Abbildern nicht konkret im Wortlaut des § 94 StPO geregelt, trotzdem ist es üblich Fotokopien von Beweisgegenständen anzufertigen.[123] Nicht jedes Minus zu einer Eingriffshandlung bedarf auch der Erwähnung im Gesetz, dies wäre nicht praktikabel, wollte man alle möglichen Ermittlungsmaßnahmen erfassen.[124] Zudem ist es mittlerweile technisch möglich, ein identisches Duplikat von Daten anzufertigen, wodurch das Verfälschungsrisiko deutlich gesenkt wird.[125] Auch das *BVerfG* sieht das Erstellen von Kopien als gleich effektive Maßnahme an und bezeichnet dieses Vorgehen mit Blick auf den Verhältnismäßigkeitsgrundsatz als vorzugswürdiges milderes Mittel.[126] Sicherungskopien anzufertigen ist damit als „Minus-Maßnahme“[127] grundsätzlich zulässig und verfassungsmäßig geboten.[128]

112 *Wenzel*, NZWiSt 2016, 85 (87).
113 *Bruns*, in: KK-StPO, § 110 Rn. 4; *Wenzel,* NZWiSt 2016, 85 (87).
114 *Bruns*, in: KK-StPO, § 110 Rn. 4; *Wenzel*, NZWiSt 2016, 85 (87).
115 *Basar*, in: FS Wessing, 2015, S. 634 (640).
116 *Fischer,* in: KK-StPO, Einleitung, Rn. 20.
117 *Warken,* NZWiSt 2017, 449 (450).
118 *Basar*, in: FS Wessing, 2015, S. 634 (641).
119 *Axer*, in: BeckOK-GG, 44. Ed. (Stand: 15.08.2020), Art. 14 Rn. 64.
120 *Heinson*, IT-Forensik, 2015, S. 215.
121 *Kemper,* NStZ 2005, 538 (541 f.).
122 *Bär*, Rn. 416.
123 *Köhler*, in: Meyer-Goßner/Schmitt, StPO, § 94 Rn. 16.
124 *Menges*, in: LR-StPO, § 94 Rn. 63.
125 *Bär,* Rn. 416.
126 *BVerfG,* NJW 2005, 1917 (1921).
127 *Gercke*, in: HK-StPO, § 94 Rn. 22.
128 *Menges*, in: LR-StPO § 94 Rn. 4; *Möhrenschlager,* wistra 1991, 321 (329); *Roxin/Schünemann*, § 34 Rn. 4; *Sieber*, S. 66.

c) Kernbereich privater Lebensgestaltung

Neben dem Verhältnismäßigkeitsgrundsatz ist der Schutz des Kernbereichs privater Lebensgestaltung als zweite Grenze staatlicher Eingriffe von wesentlicher Bedeutung. Definiert wird dieser als letzter unantastbarer Bereich menschlicher Freiheit, welcher der Einwirkung staatlicher Gewalt, auch in Abwägung mit dem Informationsbedürfnis der Strafverfolgungsbehörden, nicht zugänglich ist.[129] Sein Schutz ist Ausdruck der in Art. 1 Abs. 1 GG verankerten Menschenwürdegarantie[130] und unterliegt keiner Verhältnismäßigkeitsprüfung, sodass kein Eingriff in den Kernbereich gerechtfertigt werden kann. Lediglich der inhaltliche Umfang des Schutzes ist der Auslegung zugänglich.[131] Mit Blick auf den Schutzbereich des Rechts auf informationelle Selbstbestimmung umfasst der Kernbereich Angaben über Personen, die dem Staat zur Kenntnis gelangen können.[132] Damit werden die Möglichkeit innere Vorgänge wie Empfindungen und Gefühle sowie Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen sowie die vertrauliche Kommunikation mit anderen geschützt.[133] Die zunehmend starke Verflechtung von Informationstechnik mit dem Lebensalltag hat zur Folge, dass sich höchstpersönliche Erlebnisse auch digital abbilden lassen. Insoweit wird es sich bei der Auswertung von großen Datenmengen kaum vermeiden lassen, auch kernbereichsrelevante Daten, wie z.B. Informationen zur Sexualität[134], zu erfassen.[135] Es bedarf daher Vorkehrrungen, die eine staatliche Kenntnisnahme sensibler Daten vermeiden.[136] Das praktische Problem liegt jedoch darin, dass erst eine Kenntnisnahme des Aussagegehalts der Daten, also eine Verletzung des Kernbereichs, die Beurteilung der Kernbereichsrelevanz ermöglicht.[137] Um dem zu begegnen wird im Vorhinein versucht aus dem Kontext von Daten Schlüsse auf deren Inhalt zu ziehen. Betreffzeilen von E-Mails oder Namen von Ordnern können dafür Hinweise liefern. [138] Eine staatliche Kenntnisnahme kann so jedoch leicht durch entsprechende Bezeichnung der Daten vermieden werden. Die Erhebung von Kernbereichsdaten lässt sich folglich, besonders im Zeitalter von Big Data, nicht vollständig vermeiden ohne staatliche Ermittlungen dadurch teilweise unmöglich zu machen.[139] Aufgrund der Unvorhersehbarkeit des Inhalts der Daten lässt das *BVerfG* eine umfangreiche Erhebung grundsätzlich zu.[140] Diesem Umstand begegnete der Gesetzgeber bei der Online-Durchsuchung (§ 100b StPO) mit der Einführung des § 100d Abs. 3 StPO. Danach ist technisch soweit wie möglich sicherzustellen, die Erhebung kernbereichsrelevanter Daten zu vermeiden bzw. unverzüglich zu löschen. Trotz ähnlicher Eingriffstiefe, was Umfang und Informationsgehalt betrifft, fehlt eine solche Regelung für die §§ 94 ff. StPO.

d) Zwischenergebnis

Die Beschlagnahme digitaler Daten gem. § 94 StPO stellt trotz der Offenheit und einem nur punktuellen Zugriff einen intensiven Grundrechtseingriff dar. Die Norm erlaubt trotz ihres Wortlauts den Zugriff auf körperliche Datenträger sowie auf digitale Daten selbst, wovon auch jegliche Form von gespeicherten Kommunikationsdaten umfasst ist. Der Anfangsverdacht als materielle Voraussetzung für die Anwendung des § 94 StPO bildet für einen

129 BVerfGE 109, 279 (313).
130 BVerfGE 109, 279 (Ls. 2).
131 *Desoi/Knierim,* DÖV 2011, 398 (402, 404).
132 *Heinson*, S. 189.
133 BVerfGE 109, 279 (313).
134 BVerfGE 109, 279 (314).
135 BVerfGE 120, 274 (336).
136 *Heinson*, S. 189.
137 BVerfGE 109, 279 (313).
138 *Heinson*, S. 189.
139 Vgl. *Czerner*, in: Labudde/Spranger, S. 265 (274).
140 BVerfGE 113, 348 (392).

solch weitgehenden Eingriff die denkbar niedrigste Schwelle. Um die grundrechtlichen Vorgaben zu erfüllen besteht die Notwendigkeit verfahrensmäßiger Vorschriften, wie konkrete Regelungen zur Beschränkung der Erhebung verfahrensunerheblicher Daten sowie Daten aus dem Kernbereich privater Lebensgestaltung.

IV. Die Auswertung von Massendaten im Strafverfahren – Der Einsatz von IT-Forensik

Konnten digitale Daten gem. § 94 StPO rechtmäßig sichergestellt werden, folgt die genaue Untersuchung der beweisrelevanten Daten. Dafür werden in der Praxis die Methoden der IT-Forensik eingesetzt.[141]

1. Begriffsbestimmung

Aufgabe der Forensik ist es, mit modernster Technik und der Unterstützung von Experten, Spuren zu analysieren und so den Tathergang möglichst genau zu rekonstruieren.[142] Zur Behandlung digitaler Spuren hat sich die IT-Forensik als ein Teilgebiet der allgemeinen Forensik, welches auf IT-Systeme spezialisiert ist, herausgebildet.[143] Da die Forensik keine eigene Wissenschaft darstellt, sondern sich je nach Untersuchungsauftrag der Methoden unterschiedlicher wissenschaftlicher Disziplinen bedient, soll eine allgemeine Definition benutzt werden: IT-Forensik ist die Sicherung und Analyse von Daten aus IT-Systemen mit wissenschaftlichen Methoden zur Beweisführung vor Gericht.[144]

2. IT-Forensik im Ermittlungsverfahren

Die Vorgehensweise der IT-Forensik lässt sich grob in drei Schritte einteilen: ordnungsgemäße Sicherung, Analyse und verständliche Präsentation der Daten vor Gericht (secure, analyse, present; kurz: S-A-P).[145]

a) Beweiswertwahrung als Ziel der IT-Forensik

Zweck der Sicherstellung gem. § 94 StPO ist wie bereits erwähnt die Verfahrenssicherung. Gelingt dieser Schritt, erfolgt in der Hauptverhandlung die Bewertung der digitalen Beweismittel aufgrund einer freien richterlichen Beweiswürdigung (§ 261 StPO). Das Gericht ist dabei an keine Beweisregeln gebunden, die vorschreiben, wann eine Tatsache als erwiesen gilt oder welchen individuellen Wert ein Beweis hat.[146] Im Hinblick auf die Manipulationsanfälligkeit ist die Bestimmung des Beweiswerts von Daten jedoch schwierig.[147] Es ist daher das Ziel der IT-Forensik den Beweiswert der Daten während der Sicherung und Auswertung zu erhalten und sie vor Integritätsverletzungen zu schützen.[148] Um dies zu erreichen arbeitet die IT-Forensik mit Methoden der gerichtsfesten Sicherung und Analyse digitaler Spuren, wobei sachgerechte Kopie und Auswertung der Daten von großer Bedeutung sind.[149]

---

141 Grundlegend zur IT-Forensik *Heinson* (Fn. 119).
142 *Savić*, S. 291 m.w.N.
143 *Heinson*, S. 16.
144 *Heinson,* S. 17.
145 *Heinson,* S. 25.
146 *Eisenberg*, Beweisrecht der StPO, 10. Aufl. (2017), III. Rn. 88.
147 *Sieber*, S. 68.
148 *Heinson*, S. 4.
149 *Sieber*, S. 68.

b) Übliche Methoden der Sicherung

Während in der analogen Welt Untersuchungen überwiegend am Original stattfinden, wird in der digitalen Welt üblicherweise eine Sicherungskopie angefertigt.[150] In der Praxis erfolgt dies regelmäßig durch die sog. Spiegelung, bei der eine bitweise 1:1 Kopie erfolgt. Der Datenträger wird dabei ausgelesen und auf einem Zweiten abgespeichert.[151] Dabei entsteht ein identisches Duplikat, an welchem sodann verschiedene Untersuchungsschritte ausgeführt werden können, ohne die Originaldaten zu verändern.[152] Außerdem können mehrere Personen denselben Datenträger nach unterschiedlichen Gesichtspunkten und Methoden durchsuchen.[153] So kann ein Ergebnis jederzeit überprüft und das Risiko von Veränderungen der Datenbasis vermieden werden.[154] In der Praxis stößt diese Technik im Umgang mit Massendaten an Grenzen.[155] Aufgrund des zunehmenden Datenvolumens muss zum einen ausreichend Kapazität für forensische Duplikate zur Verfügung stehen, zum anderen kann die Auslesung einen enormen zeitlichen Mehraufwand bedeuten.[156] Außerdem muss in rechtlicher Hinsicht stets die Verhältnismäßigkeit der Datensicherung bedacht werden. Wie bereits dargestellt, darf es aufgrund der Zweckgebundenheit strafprozessualer Ermittlungsmaßnahmen nicht zu einem Komplettzugriff kommen.
Sind Daten nicht auf einem lokalen Speicher gesichert, sondern auf Servern von Drittanbietern, ist eine Spiegelung nicht möglich. Stattdessen wird mit einer Live-Sicherung ein direkter, nicht nur lesender Zugriff durch Softwareanwendung auf die Daten vorgenommen.[157] Die Live-Sicherung hat jedoch die große Schwäche, dass sie stets Veränderungen im System nach sich zieht und damit die Integrität der Daten verletzt.[158] So können z.B. die sog. Metadaten[159] verwischt werden. Auch bei der Live-Sicherung ist eine Selektion der Daten aufgrund zeitlicher und ressourcentechnischer Grenzen nur schwer möglich.[160]

c) IT-forensische Massendatenanalyse

Um der zunehmenden Komplexität und dem Umfang digitaler Daten angemessen zu begegnen werden spezielle forensische Massendatenanalysemethoden entwickelt. Dabei werden Daten auf kriminelle Handlungen hin untersucht, um diese aufzudecken, nachzuweisen oder bestimmte Muster zu erkennen.[161] Dafür stehen unterschiedliche Analysemethoden zur Verfügung. Bei regelbasierten Analysen werden bestimmte Muster als Grundlage genommen, diese Muster müssen erfüllt sein, um relevante Daten zu identifizieren. Nach der inhaltlichen Erarbeitung werden die Daten in einen Algorithmus überführt und abschließend näher untersucht.[162] Eine weitere Möglichkeit ist der Einsatz lernender Systeme („Machine Learning“). Der Begriff meint die Fähigkeit Künstlicher Intelligenz[163] (KI), basierend auf der Grundlage großer Datenmengen, die zugrundeliegenden Algorithmen zu entwickeln und

150 *Freiling/Sack,* DUD 2014, 112 (112).
151 *Schilling/Rudolph/Kuntze,* HRRS 2013, 207 (211).
152 *Heinson*, S. 31.
153 Leitfaden IT-Forensik des Bundesamts für Sicherheit in der Informationstechnik, 2011, S. 26, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=2 (zuletzt abgerufen am 25.10.2020).
154 BVerfGE 120, 274 (325); *Bär*, Rn. 417.
155 *Freiling/Sack*, DuD 2014, 112 (113).
156 Leitfaden IT-Forensik, 2011, S. 28.
157 *Basar/Hieramente,* NStZ 2018, 681 (682).
158 *Heinson*, S. 43.
159 Metadaten beschreiben die Eigenschaften der eigentlichen Daten und sind selbst spurlos veränderbar, *Heinson*, S. 4.
160 *Basar/Hièramente* NStZ 2018, 681 (683).
161 *Sauermann,* StraFo 2018, 449 (503).
162 *Sauermann*, StraFo 2018, 449 (503).
163 Eine gute Orientierung über den Begriff der Künstlichen Intelligenz und den Anwendungsmöglichkeiten für die Strafrechtspflege bieten *Staffler/Jany*, ZIS 2020, 164 ff.

diese zu trainieren, um anhand bereits vorhandener Datenauswertungen Aussagen für die Zukunft zu treffen.[164] Sie generieren ihr Wissen also aus historischen Datensätzen.[165] Durch entsprechende Softwareanwendungen lassen sich digitale Datenmengen elektronisch vorselektieren wodurch die Masse der zu sichtenden Daten reduziert wird.[166] Allerdings muss berücksichtigt werden, dass bei einer maschinellen Vorselektierung aufgrund der großen Datenmengen auch Unbeteiligte betroffen sein können. Schließlich besteht die Gefahr, dass umfassende Persönlichkeitsprofile von Bürgern erstellt werden.[167] Die grundrechtliche Schutzwirkung der informationellen Selbstbestimmung gilt auch für den Datenverarbeitungsprozess, sodass es gerade für die maschinelle Auswertung von Beweismitteln einer Ermächtigungsgrundlage bedarf.[168] Bei der Entwicklung von forensischen Methoden zur Vorselektierung muss es darüber hinaus das Ziel sein, so viele Daten wie nötig zu sichern, um dem Legalitätsprinzip gerecht zu werden und gleichzeitig so wenige Daten wie möglich zu erheben, um das Verhältnismäßigkeitsprinzip und das Verbot überschießender Beweisgewinnung zu wahren. Für die zu selektierende Datenmenge ergibt sich daher, dass diese relevant und erlaubt sein muss.[169] Trotz dieser verfassungsrechtlichen Bedenken ist die aktuelle Situation unbefriedigend. Mit der Hilfe von Selektierungsmethoden wäre eine Prüfung der vorhandenen Daten viel effektiver möglich. Gerade bei großen Datenmengen besteht die Gefahr, dass wichtige Beweise übersehen werden.[170] Dieses Risiko könnte erheblich minimiert werden. Rechtlich ist ein solches System jedoch nur umsetzbar, wenn der Gesetzgeber klare Grenzen für eine verhältnismäßige Verwendung der Systeme definiert und dies nicht der Praxis überlässt.[171]

An dieser Stelle soll außerdem nicht unerwähnt bleiben, dass die Staatsanwaltschaften im Rahmen ihrer Ermittlungstätigkeit vermehrt dazu tendieren, zur Auswertung digitaler Daten die Hilfe privater IT-Forensik Dienstleister in Anspruch zu nehmen, indem diese förmlich als Sachverständige bestellt werden (§§ 72 ff. StPO).[172] Die Aufträge beziehen sich häufig auf die Auswertung sensibler Kommunikationsdaten, die zuvor im Zuge umfangreicher Beschlagnahmemaßnahmen sichergestellt wurden.[173] In diesem Zusammenhang stellt sich zum einen die Frage, ob die Staatsanwaltschaft überhaupt im Wege der Sachverständigenbeauftragung auf die Dienste privater IT-Forensiker zurückgreifen darf oder ob es sich bei derartigen Tätigkeiten nicht vielmehr um genuine Ermittlungsarbeit handelt, die ausschließlich der Staatsanwaltschaft und ihren Ermittlungspersonen obliegt.[174] Daran schließt sich außerdem die Frage an, ob originär hoheitliche Ermittlungsaufgaben überhaupt auf Private übertragen werden können.[175] Dies kann an dieser Stelle jedoch nicht vertieft werden.

d) Ein Blick in die Praxis: Forschungsprojekt ZAC NRW

Wie durch eine Ermittlungssoftware Datenreduktion gelingen kann zeigt ein Beispiel aus der Praxis: Seit August

164 *Staffler/Jany,* ZIS 2020 164 (166).
165 *Sauermann,* StraFo 2018, 449 (503).
166 *Fährmann,* MMR 2020, 228 (232).
167 *Singelnstein,* NStZ 2012, 593 (606).
168 *Fährmann,* MMR 2020, 228 (232).
169 *Freiling/Sack,* DuD 2014, 112 (117).
170 *Fährmann,* MMR 2020, 228 (232).
171 *Fährmann*, MMR 2020, 228 (232f.); *Schneider* ZIS 2020, 79 (82).
172 Dieses Vorgehen war erstmals in Zusammenhang mit Ermittlungen wegen Verbreitung, Erwerb und Besitz kinderpornografischer Schriften (§ 184b StGB) zu beobachten, siehe https://www.spiegel.de/netzwelt/web/outsourcing-privatermittler-sichten-beweise-bei-kinderporno-anklagen-a-533078.html (zuletzt abgerufen am 10.3.21), dazu auch die Antwort der Bundesregierung auf eine Kleine Anfrage von Abgeordneten der FDP-Bundestagsfraktion, BT Drs. 16/8335, S. 1; vgl. dazu *Braun/Roggenkamp*, NK 2012, 141 (141 ff.); diese Methoden finden aber zunehmend auch in komplexen Wirtschaftsstrafverfahren Anwendung, ausführlich zu dieser aktuellen Problematik *Wackernagel/Graßie*, NStZ 2021, 12 (12 ff.).
173 *Wackernagel/Graßie*, NStZ 2021, 12 (12).
174 Im Ergebnis für den Großteil aller Fälle ablehnend *Wackernagel/Graßie*, NStZ 2021, 12 (13 ff.).
175 Für unzulässig haltend *Wackernagel/Graßie*, NStZ 2021, 12 (16 ff.); insbesondere kann nicht auf die Ermittlungsgeneralklausel (§ 161 Abs. 1 StPO) als gesetzliche Grundlage zurückgegriffen werden *Wenzel*, NZWiSt 2016, 85 (86).

2019 forscht das Justizministerium Nordrhein-Westfalen gemeinsam mit der Zentral- und Ansprechstelle Cybercrime (ZAC NRW) [176] in Zusammenarbeit mit der Microsoft GmbH Deutschland und verschiedenen Experten zur Bekämpfung von Kinderpornografie im Internet anhand Analysemethoden Künstlicher Intelligenz.[177] Die unüberschaubare Menge des vorhandenen Untersuchungsmaterials wird derzeit noch manuell durch die Ermittler gesichtet. Immer besteht die Gefahr, dass dabei strafrechtlich relevante Bilder leicht in der Masse harmloser Dateien untergehen. Zudem sind die Ermittler bei der Sichtung enormen psychischen Belastungen ausgesetzt.[178] Die manuelle Ermittlung ist daher sowohl in zeitlicher als auch personeller Hinsicht wenig zweckmäßig.[179] Durch automatische Bilderkennung mit Hilfe eines Algorithmus soll kinderpornografisches Material erkannt und von sonstigen Dateninhalten getrennt werden.[180] Durch diese Datenselektion soll zum einen eine Beschleunigung der Datenauswertung, zum anderen eine Reduktion auf die verfahrensrelevanten Bilddateien erreicht werden. Der reduzierte Datensatz wird schließlich von den Ermittlern analysiert. Eine Herausforderung des Projekts liegt darin, durch die Weiterleitung der Daten zur Analyse an Dritte nicht selbst den Tatbestand der Verbreitung und des Besitzes kinderpornografischer Schriften gem. §§ 184b ff. StGB zu verwirklichen.[181] Diese Sorge wurde durch eine Komprimierung der Daten gelöst. Die Bilder sind zwar für die Software verwertbar, für Menschen hingegen nicht sichtbar.[182] Das Forschungsprojekt zeigte bereits Wirkung: Im September 2020 wurden bei Durchsuchungen von Tatverdächtigen in ganz Deutschland wegen des Verdachts auf Besitz und Verbreitung von Kinderpornografie (§ 184b StGB) Beweismittel sichergestellt, welche auf den bisherigen Auswertungen der ZAC gründen.[183] Das Potential solcher Systeme kann allerdings nur ausgeschöpft werden, wenn die Maßnahme auf einem festem Rechtssystem mit klaren Regeln für die Verwendung baut.[184]

An dieser Stelle lohnt sich außerdem ein Blick über die innerdeutschen Grenzen hinaus: innerhalb der Europäischen Union ist die Verbesserung der Ermittlungstätigkeiten der Strafverfolgungsbehörden durch den Einsatz von KI bereits seit Jahren ein Forschungsschwerpunkt.[185] Im Rahmen der Forschungsförderung *Horizon 2020*[186] werden zahlreiche Projekte gefördert, die speziell die Unterstützung der Strafverfolgungsbehörden durch innovative Technologien, wie Blockchain Analyse, Big-Data Analyse oder den Einsatz von KI und Machine Learning betreffen.[187] Diese Entwicklung ist nur zu begrüßen.

e) Problem: Fehlende rechtliche Vorgaben

Trotz weitreichender technischer Möglichkeiten finden diese bislang noch kaum Wiederhall in den Vorgaben der Strafprozessordnung.[188] Zu den wenigen Regelungen gehört § 100a Abs. 5 StPO, der sich allerdings nur auf die Quellen-TKÜ und gem. § 100b Abs. 4 StPO auf die Onlinedurchsuchung bezieht. Auch § 496 Abs. 2 StPO enthält

176 https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html(zuletzt abgerufen am 25.10.20).
177 https://www.land.nrw/de/pressemitteilung/kuenstliche-intelligenz-im-kampf-gegen-kinderpornographie (zuletzt abgerufen am 25.10.2020).
178 https://www.tagesspiegel.de/politik/depressionen-oder-psychosen-drohen-auswertung-von-kinderpornos-fuer-ermittler-eine-zumutung/25898696.html (zuletzt abgerufen am 25.10.20).
179 *Staffler/Jany,* ZIS 2020, 164 (169).
180 https://news.microsoft.com/de-at/features/automatische-bilderkennung-hilft-im-einsatz-gegen-kinderpornografie/ (zuletzt abgerufen am 25.10.20).
181 Zu dieser Problematik *Rückert/Goger,* MMR 2020, 373 ff.
182 https://www.handelsblatt.com/technik/forschung-innovation/cyberkriminalitaet-mit-kuenstlicher-intelligenz-will-die-justiz-kinderpornografie-bekaempfen/24871714.html?ticket=ST-806263-B7mZL7HfFVMTyPz9ffWq-ap3 (zuletzt abgerufen am 25.10.20).
183 https://www.presseportal.de/blaulicht/pm/12415/4694676 (zuletzt abgerufen am 25.10.20).
184 *Staffler/Jany,* ZIS 2020, 164 (169).
185 Siehe dazu EU Research for a Secure Society, Fighting crime and terrorism, including cybercrime, migration and home affairs, European Union, 2019, abrufbar unter https://op.europa.eu/en/publication-detail/-/publication/fba6e440-1f89-11e9-8d04-01aa75ed71a1/language-en (zuletzt abgerufen am 10.3.21); *Gercke*, ZUM 2019, 789 (803).
186 https://ec.europa.eu/programmes/horizon2020/en/h2020-sections-projects (zuletzt abgerufen am 10.3.21).
187 Mit der Nennung einiger Projektbeispiele *Gercke*, ZUM 2019, 789 (803).
188 *Basar*, in: FS Wessing, 2015, S. 634 (639); vgl. *Blechschmitt,* MMR 2018, 361 (364).

Vorgaben, die wiederum sehr allgemein gehalten sind und nur von den „erforderlichen organisatorischen und technischen Maßnahmen“ (§ 496 Absatz 2 Nr. 1 StPO) und „Grundsätzen einer ordnungsgemäßen Datenverarbeitung“ (§ 496 Absatz 2 Nr. 2 StPO) sprechen. Auch aus den §§ 483 ff. StPO folgen keine Regelungen zur Authentizitätsicherung der Daten.[189] Anhaltspunkte für konkrete Regelungen lassen sich dem Leitfaden IT-Forensik[190] des Bundesamts für Sicherheit und Informationstechnik (BSI) entnehmen.[191] Auch wenn die Vorgaben nicht rechtsverbindlich sind, können sie den Behörden als Orientierung dienen. Die Legislative ist daher aufgerufen, in dem höchst grundrechtsrelevanten Bereich der strafrechtlichen Ermittlungsbefugnisse klare gesetzliche Rahmenbedingungen für die technische Auswertung digitaler Daten zu schaffen, um so der Verhältnismäßigkeit Rechnung zu tragen und eine effektive Strafverfolgung zu ermöglichen.[192] Die Maßstäbe des „Leitfadens IT-Forensik“ bieten hierfür eine gute Grundlage.[193]

3. Zwischenergebnis

Der IT-Forensik ist es gelungen, technische Verfahren und Methoden für einen gekonnten Umgang mit digitalen Daten zu etablieren. In der Praxis erfolgt eine Orientierung an Leitfäden. Die wachsenden Kompetenzen werden in den Fachabteilungen (ZAC) im BKA und den LKA gebündelt.[194] Um die technischen Möglichkeiten, besonders im Bereich der Massendatenanalyse voll im Strafverfahren nutzen zu können, braucht es jedoch konkrete gesetzliche Vorschriften für die Auswertung digitaler Beweise und den Einsatz derartiger Software.

V. Reformbedarf

1. Beschränkende Eingriffsgrundlagen

Die vorangegangenen Ausführungen zeigen, dass § 94 StPO nur bedingt dazu geeignet ist, die intensiven Grundrechtseingriffe, die sich bei der Erhebung großer Datenmengen ergeben zu rechtfertigen.
Die tiefgreifenden Eingriffe stützen sich auf eine Ermächtigungsgrundlage, die seit 1877 beinahe unverändert besteht, was einen Anpassungsbedarf offenbart.[195] Die schlichte Übertragung einer Befugnis aus der analogen in die digitale Welt kann gesetzgeberisches Handeln nur vorübergehend ersetzen[196] und wird mit der Weiterentwicklung technischer Möglichkeiten nur zu mehr Unsicherheiten für die Rechtsanwender führen.[197] Die Forderung nach Normenklarheit ist keine Prinzipienreiterei, sondern für einen Rechtsstaat unerlässlich.[198] Vertraut man allein auf die verfassungskonforme Anwendung des § 94 StPO, wird dem Risiko von Grundrechtsverletzungen nur unzureichend begegnet. Gerade allgemeine Prinzipien wie der Verhältnismäßigkeitsgrundsatz erzielen im Verhältnis zu konkreten Regelungen im Tatbestand nur eine geringe Wirkung.[199] Daher wäre es mehr als sinnvoll, die An-

189 *Fährmann,* MMR 2020, 228 (231).
190 Leitfaden IT Forensik des Bundesamts für Sicherheit in der Informationstechnik, 2011, (Fn. 152).
191 *Schneider,* ZIS 2020, 79 (82).
192 Vgl. *Fährmann,* MMR 2020, 228 (231).
193 *Basar,* in: FS Wessing, 2015, S. 634 (647); *Sieber*, S. 127; *Fährmann,* MMR 2020, 228 (231); *Schneider,* ZIS 2020, 79 (82).
194 https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html (zuletzt abgerufen am 25.10.20).
195 *Ludewig,* KriPoZ 2019, 293 (297).
196 *Roggan,* NJW 2015, 1995 (1999).
197 Vgl. auch *Sieber*, S.14.
198 *Peters,* NZWiSt 2017, 465 (472).
199 *Singelnstein,* NStZ 2012, 593 (606).

forderungen, die sich aus dem Grundgesetz, speziell aus dem Verhältnismäßigkeitsgrundsatz, ergeben im Gesetzestext klarzustellen.[200] Schon das *BVerfG* setzte fest, dass der Gesetzgeber den Grundrechtsschutz bei staatlichen Ermittlungshandlungen durch Anpassung bestehender oder Schaffung ergänzender Regelungen effektiv sichern muss.[201] Während das *BVerfG* die Anforderungen an die Verhältnismäßigkeit im Bereich des Gefahrenabwehrrechts bereits stärker konturiert hat[202], steht dies im Strafverfahrensrecht noch aus.[203]

Die Beschlagnahme gem. § 94 Abs. 2 StPO erlaubt den Zugriff auf einen umfassenden Datenbestand, was bis zur Zusammensetzung eines Persönlichkeitsprofils führen kann. Damit geht die Maßnahme, welche als Grundlage nur den Anfangsverdacht erfordert, weit über ihren ursprünglichen Zweck hinaus. Dies lässt § 94 StPO zu einer „Super-Ermächtigungsgrundlage[204]“ für die Beweisgewinnung werden. Dem muss im Hinblick auf die Grundsätze der Zweckbindung und der Datensparsamkeit, welche mit dem Phänomen Big Data immer größere Relevanz entfalten, unbedingt entgegengewirkt werden. Außerdem erscheint eine ausdrückliche einfach gesetzliche Regelung zum Schutz des Kernbereichs persönlicher Lebensgestaltung aufgrund der Nähe zur Online-Durchsuchung notwendig. Als Vorbild kann § 100d StPO herangezogen werden. [205]

2. Regelungen zur Auswertung digitaler Daten

Darüber hinaus benötigt die StPO dringend konkrete Vorgaben zur Sicherung der Authentizität digitaler Daten, um diese nicht in ihrem Beweiswert zu schwächen.

Dafür werden verschiedene Maßnahmen vorgeschlagen, die sich auch im Leitfaden IT-Forensik wiederfinden: Um Verfälschungen auszuschließen, sollte der Datenverarbeitungsprozess chronologisch in Protokollen dokumentiert werden. So kann nachvollzogen werden, woher die Daten stammen und wie sie aus dem IT-System gewonnen wurden.[206] Die Integrität kann weiterhin mit einer frühzeitigen Erstellung von sogenannten Hashwerten gesichert werden. [207] Jede Datei hat einen individuellen Hashwert, der sich bei einer Manipulation verändert.[208]

Wurde ein Hashwert genommen, kann dieser mit dem Hashwert des Datensatzes im Strafverfahren jederzeit verglichen werden. Stimmen die Werte überein, kann eine Veränderung mit großer Sicherheit ausgeschlossen werden.[209] Durch ein Zugangssystem für die gespeicherten Daten sollte zudem garantiert werden, dass nur berechtigten Personen Zugriff auf die Daten erhalten. Dies trüge dem Grundrechtsschutz Rechnung und ließe erkennen, wer Zugang zu den Daten hatte.[210] Jeder Verarbeitungsschritt sollte reproduzierbar sein, weshalb Kopien für die Auswertung der Daten erstellt werden sollten, um stets einen unveränderten Datensatz zur Verfügung zu haben.[211] Da es sich bei im Strafverfahren relevanten Daten meist um sehr sensible Daten handelt, sind diese zudem durch ein besonderes Speicherungssystem vor dem Zugriff Unberechtigter zu sichern.[212] Es ist besorgniserregend, wenn sensible Daten auf privaten Servern, etwa bei Amazon, gespeichert werden.[213] Mit Blick auf die wachsenden Datenmengen sollte außerdem geprüft werden, wie forensische Massendatenanalyseverfahren die Ermittlungsarbeit

200 *Heinson*, S. 404.
201 *BVerfG*, NJW 2005, 1338 (Ls. 3).
202 BVerfGE 141, 220 (263 ff.).
203 *Singelnstein,* in: Hoffmann-Riem, S. 179 (181).
204 *Roggan,* NJW 2015, 1995 (1997).
205 *Ludewig,* KriPoZ 2019, 293 (299).
206 *Heinson*, S. 144 f.
207 *Müller,* NZWiSt 2020, 96 (100).
208 Hinsichtlich der technischen Grundprinzipien: *Erbguth,* MMR 2019, 654 (655).
209 *Heinson*, S. 149 f.
210 *Fährmann,* MMR 2020, 228 (230) m.V.a. Leitfaden IT-Forensik, 2011, S. 23.
211 *Heinson*, S. 147.
212 *Sieber*, S. 67 f.
213 https://netzpolitik.org/2019/bundespolizei-speichert-bodycam-aufnahmen-weiter-bei-amazon/ (zuletzt abgerufen am 25.10.20).

durch Datenreduktion und Datenselektion effektiver gestalten können, ohne eine unverhältnismäßige Beeinträchtigung von Grundrechten zu verursachen. Das Projekt der ZAC NRW liefert dafür erste Anhaltspunkte.

VI. Fazit

Im Laufe der letzten Jahre wurde die StPO immer mehr an die Herausforderungen der digitalen Welt angepasst. Dabei wurden jedoch die für körperliche Gegenstände zugeschnittenen Eingriffsgrundlagen der §§ 94 ff. StPO vom Gesetzgeber nicht ausreichend berücksichtigt. Das Resultat: Aufkommende Probleme mussten in der Praxis anhand möglichst verfassungskonformer Anwendung der Vorschriften und auf Grundlage teils widersprüchlicher Rechtsprechung gelöst werden. Eine solche Vorgehensweise wird jedoch der vielen Besonderheiten, die mit digitalen Daten im Strafverfahren verbunden sind, nicht gerecht.[214] Wie der Mathematiker *Norbert Wiener (1894-1964)* passend formulierte: „Information is information, not matter or energy. No materialism which does not admit this can survive at the present day".[215] Für die Rechtswissenschaften bedeutet dies, die noch anerkannte Praxis, für körperliche Gegenstände intendierte Ermittlungsbefugnisse auf digitale Daten anzuwenden, mit Blick auf technische Weiterentwicklungen kritisch zu hinterfragen. Für den Gesetzgeber ergibt sich daraus der dargestellte Handlungsbedarf.

Hierbei sollten zudem die Möglichkeiten der IT-Forensik berücksichtigt werden. Der Auswertung von Massendaten kommt dabei mit Blick auf Datenselektion und Datenreduktion eine besondere Bedeutung zu. Das Potential digitaler Ermittlungsmethoden mit zunehmenden Datenmengen ist evident und die Auseinandersetzung damit letztendlich unumgänglich.[216] Der Staat muss mit den technischen Entwicklungen Schritt halten und sich die daraus resultierenden Ermittlungsmethoden zu Nutze machen, damit auch in Zukunft eine effektive Strafverfolgung gelingen kann. Der digitale Fortschritt ist derart rasant, dass für staatlichen Organe im Zeitalter des Phänomens Big Data eine qualitative sowie quantitative Überforderung droht.[217] Vor den Konsequenzen einer solchen Überlastung ist der einzelne Grundrechtsträger unter allen Umständen zu schützen.

214 Vgl. *Sieber*, S. 14.
215 Zitiert nach *Sieber*, S. 14.
216 *Staffler/Jany* ZIS 2020, 164 (169).
217 *Eschelbach*, Big Data im Strafprozess, Vortrag 2016, letzte Seite.

KriPoZ Kriminalpolitische Zeitschrift JuP

„Junges Publizieren“

Seminararbeit von

Yara von Baeckmann

Die Vorratsdatenspeicherung – eine (un-)endliche Geschichte

Ludwig-Maximilians-Universität München
Juristische Fakultät
Prof. Dr. Mark Zöller
Abgabedatum: 11.3.2021

Inhaltsverzeichnis

I. Einleitung

Vielleicht eine Geschichte ohne Ende, doch jedenfalls eine Geschichte mit einem Anfang: dem 15.3.2006. An diesem Tag setzte das Europäische Parlament mit dem Erlass der Richtlinie 2006/24/EG den Startschuss für die bewegte Diskussion über eines der meistumstrittensten Themen im Spannungsfeld zwischen Sicherheit und Freiheit; der Vorratsdatenspeicherung.[1] Die verpflichtende Speicherung bestimmter Verkehrsdaten durch Telekommunikationsdienstanbieter (TKD) auf Vorrat und zum Zwecke der Gefahrenprävention und Strafverfolgung[2] sollte den Gefahren und Problemen entgegentreten, die eine Digitalisierung sämtlicher Lebensbereiche für Strafverfolgung und -prävention mit sich bringt.[3] Und obwohl auch in Deutschland schon Jahre vorher über die Einführung einer solchen Regelung diskutiert worden war,[4] waren es erst die Anschläge in Madrid und London, die zunächst innerhalb kürzester Zeit zum Erlass der Richtlinie,[5] später zum ersten deutschen Gesetz zur Vorratsdatenspeicherung und damit einhergehend immer lauter werdender Kritik führten.[6] Und nicht nur die Öffentlichkeit reagierte mit Skepsis auf das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ vom 21.12.2007, auch das *BVerfG* entschied 2010, dass die fraglichen Normen gegen die Verfassung verstießen und insoweit nichtig waren.[7] Noch bevor jedoch der Gesetzgeber ein neues verfassungskonformes Gesetz schaffen konnte, erledigte sich das Problem scheinbar von selbst, erklärte doch der *EuGH* 2014 die EU-Richtlinie diesmal in Bezug auf die Grundrechtecharta der EU ebenfalls für grundrechtswidrig.[8] Nichtsdestotrotz schuf der Bundestag 2015 ein zweites, nicht europarechtlich indiziertes Gesetz zur Vorratsdatenspeicherung.[9] Bereits ein Jahr später setzte der *EuGH* in seinem Urteil zu schwedischen und britischen Bestimmungen einer Vorratsdatenspeicherung neue Schranken,[10] welche das *OVG Münster* zu der Annahme verleitete, das deutsche Gesetz verstoße ebenfalls gegen europäisches Recht.[11] Auch wenn die Bundesnetzagentur daraufhin mitteilte, sie würde keine Durchsetzung der betroffenen Regelungen mehr erstreben, bzw. deren Nichtumsetzung nicht ahnden,[12] trat das Gesetz zum 1.7.2017 in Kraft und verpflichtet bis heute die Provider zur Speicherung.[13] Am 6.10.2020 bekräftigte der *EuGH* seine bisherige Linie grundsätzlich,[14] eine Bewertung der deutschen Rechtslage steht jedoch ebenso aus, wie eine durch das *BVerfG*.[15] Und so bleibt die Frage, wie eine europa- und verfassungsrechtkonforme Regelung in das deutsche Rechtssystem integriert werden könnte, vorerst bestehen. Dieser Frage soll die folgende Arbeit nachgehen, indem auf Basis der aktuellen Rechtslage die meistumstrittensten Problemfelder unter Bezugnahme auf Rechtsprechung von *BVerfG* und *EuGH* näher analysiert, Lösungsansätze sowie Verbesserungsvorschläge herauskristallisiert und insbesondere die Schwierigkeiten einer *EuGH*-konformen Umsetzung behandelt werden.

---

1 *Moser-Knierim,* Vorratsdatenspeicherung. Zwischen Überwachungsstaat und Terrorabwehr, 2013, S. 180; MPI, Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten (Gutachten), 2. Fassung (2011), S. 255; *Nelles,* Quo Vadis Vorratsdatensdatenspeicherung, 2014, S. 3.
2 *Moser-Knierim*, S. 139.
3 Vgl. *Münch,* ZRP 2015, 130 (132).
4 *Moser-Knierim*, S. 148, 150.
5 *Moser-Knierim,* S. 150; *Puschke,* ZIS 2019, 308 (310); *Szuba,* Vorratsdatenspeicherung. Der europäische Gesetzgeber im Spannungsfeld zwischen Sicherheit und Freiheit, 2011, S. 48.
6 *Bär,* in: KMR-StPO, 97. EL (2020), vor §§ 100a-100g Rn. 6; vgl. *Moser-Knierim*, S. 164.
7 BVerfGE 125, 260 (358).
8 *EuGH*, Urt v. 8.4.2014, C-293/12 und C-594/12, ECLI:EU:C:2014:238-Digital Rights (*EuGH*, Digital Rights), Rn. 25.
9 Gesetz zur Einführung einer Speicherfrist und Höchstspeicherfrist von Verkehrsdaten vom 10.12.2015.
10 *EuGH*, Urt. v. 21.12.2016, C-203/15 und C-698/15, ECLI:EU:C:2016:970 -Tele2 (*EuGH*, Tele2).
11 *OVG Münster*, NVwZ-RR 2018, 43 (48).
12 *Wolter/Greco,* in: SK-StPO, 5. Auflage (2018), § 100g Rn. 19c.
13 *Wolter/Greco,* in: SK-StPO, § 100g Rn. 19c.
14 *EuGH*, Urt. v. 6.10.2020, C-511/18, C-512/18 und C-520/180, ECLI:EU:C:2020:791-La Quadrature du Net (*EuGH*, La Quadrature du Net); *EuGH*, Urt. v. 6.10.2020, C-623/17, ECLI:EU:C:2020:790-Privacy International (*EuGH*, Privacy International).
15 Rechtshängig beim *BVerfG*: 1 BvR 141/16, 1 BvR 229/16, 1 BvR 2023/16, 1 BvR 2683/16, 1 BvR 2821/16; beim *EuGH*: C-793/19.

II. Vorbemerkungen

1. Überblick über die Regelungssystematik des § 100g StPO

Die Regelung der Datenspeicherung und -erhebung zum Zwecke der Strafverfolgung wird primär durch das Zusammenspiel von § 100g StPO mit Normen des Telekommunikationsgesetzes (TKG) bestimmt. § 100g Abs. 1 StPO regelt hierbei zum einen die Datenerhebung in Echtzeit, zum anderen - unter Ausschluss von Standortdaten - den Zugriff auf Verkehrsdaten, die im Rahmen des § 96 Abs. 1 TKG von TKD zu Abrechnungszwecken oder zur Störungsbeseitigung gespeichert werden dürfen. Diese Art der Datenspeicherung und Abfrage beanstandet das *BVerfG* in seiner Entscheidung nicht.[16] Da jedoch die Speicherdauer im Rahmen des § 96 Abs. 1 TKG meist sehr kurz ist[17] und gerade bei Flatrates eine derartige Speicherung häufig gar nicht erfolgt,[18] sind die gewünschten Daten oftmals nicht verfügbar. Diese Lücke sollte § 113b TKG schließen, indem er die in § 113a TKG genannten TKD zur Aufbewahrung bestimmter Daten auf Vorrat verpflichtet.[19] § 113b TKG bildet somit die Grundlage der Vorratsdatenspeicherung. § 100g Abs. 2 StPO bestimmt, inwieweit auf diese Daten im Rahmen der Strafverfolgung zurückgegriffen werden darf. Voraussetzung für eine Erhebung der gespeicherten Daten ist demnach, dass es sich bei der fraglichen Tat um eine Katalogtat des Absatz 3 handelt, welche auch im Einzelfall besonders schwer wiegt, die Abfrage verhältnismäßig ist und eine Ermittlung des Aufenthaltsortes des Beschuldigten oder die Aufklärung des Sachverhalts ohne Erhebung zumindest wesentlich erschwert wäre. § 100g Abs. 3 StPO normiert die Funkzellenabfrage, bei der alle bei einer Funkzelle innerhalb eines bestimmten Zeitraums angefallenen Daten erhoben werden. Satz 2 regelt dabei die Erhebung von Daten, die nach § 113b TKG auf Vorrat gespeichert wurden. Da § 113b TKG jedoch keine Speicherung von Funkzellendaten vorsieht, kann es nach aktueller Gesetzeslage nicht zu einer Speicherung oder Erhebung gespeicherter Funkzellendaten kommen.[20] Aus diesem Grund soll die Funkzellenabfrage aus den folgenden Überlegungen ausgeklammert werden. Das Hauptaugenmerk liegt somit auf den §§ 113a, 113b TKG und § 100g Abs. 2 StPO.

2. Vorbemerkungen zur Rechtsprechung von BVerfG und EuGH

In seiner Entscheidung vom 2.3.2010 prüfte das *BVerfG* eine Vereinbarkeit der §§ 113a, 113b TKG a.F. und § 100g StPO a.F. mit Art. 10 und 12 GG. Während es einen Verstoß gegen Art. 12 GG recht pauschal ablehnte,[21] widmete es Art. 10 GG – welcher Art. 2 Abs. 2 i.V.m. Art. 1 Abs. 1 verdränge - eine ausführliche Prüfung, in deren Rahmen es zu dem Ergebnis kam, die Normen stellten einen unverhältnismäßigen Eingriff dar.[22] Der *EuGH* wählte als Prüfungsmaßstab für seine Kontrolle der Richtlinie 2006/24/EG und der nationalen Gesetzgebung einzelner Mitgliedsstaaten Art. 7, 8 und 11 GrCh sowie die Richtlinie 2002/58/EG.[23] Sowohl *BVerfG* als auch *EuGH* sahen in der Speicherung von Daten durch die TKD und in der Erhebung durch die Strafverfolgungsbehörden jeweils einen selbstständigen Grundrechtseingriff.[24] Die Speicherung allein könne schon „ein diffus bedrohliches

16 BVerfGE 125, 260 (328).
17 BT-Drs. 17/1482, S. 3; *Wolter/Greco,* in: SK-StPO, § 100g Rn. 8.
18 *Wolter/Greco,* in: SK-StPO, § 100g Rn. 8.
19 BT-Drs. 17/1482, S. 3.
20 *Bär,* in: BeckOK-StPO, 37. Ed. (2020), § 100g Rn. 44.
21 Siehe BVerfGE 125, 260 (358 f.).
22 BVerfGE 125, 260 (358).
23 *EuGH*, Digital Rights, Rn. 25; *EuGH*, Tele2, Rn. 122, 125.
24 *EuGH*, Digital Rights, Rn. 34.

Gefühl des Beobachtetseins“[25] hervorrufen, welches die freie Wahrnehmung der Grundrechte beeinflusse. Beide Gerichte erklärten eine Vorratsdatenspeicherung nicht für per se rechtswidrig, betonten jedoch ihre Eingriffsintensivität sowie die besondere Sensibilität des Themas und stellten mehr oder minder genaue Anforderungen an nationale Regelungen.[26]

III. Zur Ausgestaltung im Einzelnen

1. Datenkategorien

Zunächst empfiehlt sich ein Blick darauf, welche Arten der Information von der Vorratsdatenspeicherung umfasst werden. Das TKG unterscheidet zwischen Bestands-, Inhalts- und Verkehrsdaten. Bestandsdaten sind Kundendaten, welche TKD im Rahmen des Vertragsverhältnisses erheben,[27] und deren staatliche Verwertung die §§ 112, 113 TKG regeln. Der Begriff „Verkehrsdaten“ bezeichnet die Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden.[28] Inhaltsdaten schließlich geben Aufschluss über den Inhalt einer Kommunikation.[29] § 113b TKG beschränkt die Vorratsdatenspeicherung auf Verkehrsdaten. Während *BVerfG* und *EuGH* in der Speicherung von Inhaltsdaten einen nicht zu rechtfertigenden Eingriff in den Wesensgehalt des Art. 10 GG[30] bzw. Art. 7, 8 GrCh sehen,[31] kritisieren sie die Speicherung von Verkehrsdaten grundsätzlich nicht.[32] Der Katalog des § 113b TKG ist somit wohl grundrechtskonform. Nichtsdestotrotz empfiehlt sich in Hinblick auf etwaiges Verbesserungspotential ein näherer Blick auf die zu speichernden Datenkategorien.

a) Internetnutzung

Die erste Kategorie sind hierbei die Internetnutzungsdaten. Diese umfassen die eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt, eine zugewiesene Benutzerkennung und den Zeitraum der Nutzung sowie die verwendete Internetprotokoll-Adresse (IP-Adresse). [33] Aus Effizienzgründen werden IP-Adressen meist nicht fest, sondern zeitlich begrenzt vergeben und stetig ausgetauscht (dynamische IP-Adresse).[34] Unter Zuhilfenahme von Informationen bezüglich Anschluss, Anschlussinhaber und Nutzungszeit kann ihre Kenntnis die Zuordnung ansonsten anonymer Aktivitäten zu einzelnen Anschlussinhabern ermöglichen.[35] Gerade im Bereich der Internetkriminalität können Internetnutzungsdaten so entscheidende Anhaltspunkte zur Aufklärung von Straftaten liefern.[36] Unmöglich bleibt jedoch die Feststellung, wer zu dem konkreten Zeitpunkt den betroffenen Anschluss genutzt hat.[37] Typischerweise erfolgt die Ermittlung im Ausgangspunkt von der Aktivität (bspw. dem Verfassen eines Kommentars) hin zum Nutzer und ermöglicht somit nur punktuelle Einblicke in das Verhalten desselben.[38] Die Erstellung eines umfassenden Persönlichkeitsprofils durch umgekehrte Ermittlung, d.h. das Ansetzen beim

25 BVerfGE 125, 260 (320).
26 BVerfGE 125, 260 (316 f.); *EuGH*, Tele2, Rn. 103 ff.
27 Siehe § 3 Nr. 3 TKG.
28 § 3 Nr. 30 TKG.
29 *Moser-Knierim*, S. 290.
30 BVerfGE 125, 260 (322).
31 *EuGH*, Tele2, Rn. 101.
32 *EuGH*, Tele2, Rn. 108; BVerfGE 125, 260 (316).
33 Art. 13b Abs. 3 Nr. 1-3.
34 *Freude,* Technische Fragen der Vorratsdatenspeicherung. Kurzgutachten für die SPD-Bundestagsfraktion (Gutachten), 2011, S. 8 f.; *Zöller,* GA 2007, 393 (406).
35 *Freude*, S. 20 f.
36 BVerfGE 125, 260 (343).
37 *Alsbih,* DuD 2011, 482.
38 *Freude*, S. 21.

Nutzer und die von dort folgende Abfrage aller je benutzten IP-Adressen und damit verbundener Aktionen ist insbesondere, da besuchte Webseiten von den TKD nicht mit gespeichert werden,[39] aufwendig und wenig erfolgversprechend, nichtsdestotrotz technisch möglich[40] und nicht zu unterschätzen.[41]

b) Sonderfall Portnummern

Besondere Probleme ergeben sich dort, wo, wie bei Hotspots oder WLANs, eine IP-Adresse durch mehrere Personen benutzt wird, da hier eine eindeutige Zuordnung von einer Aktion zum Handelnden nicht möglich ist.[42] Mitunter wird vorgeschlagen, nunmehr auch Portnummern, welche bisher von der Speicherpflicht ausgenommen waren,[43] jedoch eine eindeutige Zuordnung ermöglichen würden, in den Katalog des § 113b aufzunehmen.[44] Wenn nämlich der Zweck der Vorratsdatenspeicherung in Bezug auf IP-Adressen häufig gar nicht erfüllt werden kann, ist fraglich, ob hier eine Speicherung derselben überhaupt noch zu rechtfertigen ist. Der Wunsch, Portnummern in den Katalog des § 113b TKG aufzunehmen,[45] ist somit nachvollziehbar. Die Idee findet ihre Grenzen jedoch in der Realität. Auch unter Zuhilfenahme der Portnummer kann der Anschlussinhaber nur bei Kenntnis derselben ermittelt werden. Die Portnummern sind den Ermittlern in der Praxis allerdings meist gerade nicht bekannt, da Webseitenbetreiber sie in der Regel nicht speichern.[46] Die Vorratsdatenspeicherung von Portnummern hieße somit einen tiefgreifenden Eingriff mit hohem technischen Aufwand bei gleichzeitig geringem Nutzen.[47]

c) Telefonverkehr

Eine weitere Kategorie von Daten sind Informationen zum Telefonverkehr inklusive SMS und MMS. Details über Kommunikationspartner und -zeiten lassen mitunter Schlüsse auf Inhalte der Kommunikation zu und können Auskunft über Persönlichkeits- und persönliche Merkmale des Nutzers verschaffen.[48] Gleichzeitig unterstützen auch diese Daten eine Aufklärung und waren nach Aussagen von Ermittlern jedenfalls um das Jahr 2010 besonders in Bereichen organisierter Kriminalität nach wie vor wesentlich.[49] Es ist anzunehmen, dass die Bedeutung dieser Kommunikationsarten in den letzten Jahren abgenommen hat und in den kommenden Jahren noch weiter sinken wird.[50] Es ist jedoch auch mehr als wahrscheinlich, dass im Falle einer Ausklammerung aus der Speicherungspflicht, Kriminelle wieder auf diese traditionelle Form der Kommunikation zurückgreifen würden und die restliche Vorratsdatenspeicherung ineffektiv, wenn nicht sogar obsolet, würde.

d) Standortdaten

Die letzte Kategorie des § 113b TKG bilden sog. Standortdaten. Sie geben Aufschluss über den Aufenthaltsort

39 § 113b Abs. 5 TKG.
40 *Freude*, S. 21.
41 *Roßnagel et al.*, Interessensausgleich im Rahmen der Vorratsdatenspeicherung. Analyse und Empfehlungen, 2013, S. 133.
42 *Alsbih,* DuD 2011, 482 (483).
43 BNetzA, Häufig gestellte Fragen zur Speicherung und Übermittlung von speicherpflichtigen Verkehrsdaten nach den §§ 113a und 113b TKG, 2017, S. 5.
44 *Rudl*, Portnummern im NetzDG. Sinnlose Datenflut statt gezielter Ermittlungen, Netzpolitik 16.3.2020, abrufbar unter: https://netzpolitik.org/2020/sinnlose-datenflut-statt-gezielte-ermittlungen/ (zuletzt abgerufen am 12.10.20).
45 MPI, S. 160.
46 *Freude*, S. 23.
47 *Freude*, S. 23.
48 BVerfGE 125, 260 (319).
49 MPI, S. 138.
50 MPI, S. 138.

einer bestimmten Person, indem sie den Aufenthalt des Endgeräts eines Endnutzers in einer bestimmten Funkzelle bei Beginn der Verbindung bestätigen.[51] Die höhere Sensibilität dieser Daten begründet sich darin, dass sich mit ihrer Hilfe komplexe Bewegungsprofile erstellen lassen.[52] Auch ermöglichen sie so viele Rückschlüsse auf eine Person, dass bereits vier zufällig gewählte Standorte ausreichen, um 95% der Individuen zu identifizieren.[53] Dieser höheren Sensibilität hat der Gesetzgeber Beachtung geschenkt, indem er die Speicherdauer im Vergleich zu den Informationen zu Internet und Telekommunikation von 10 auf 4 Wochen herabgesetzt hat.

e) E-Mailverkehr

Ausgenommen aus der Speicherpflicht sind Daten bezüglich des E-Mailverkehrs. In der Gesetzesbegründung finden sich hierfür keine weiteren Erklärungen bis auf die Beschränkung des § 113b TKG auf das Notwendige.[54] Wieso jedoch die Speicherung von Verkehrsdaten von SMS notwendiger sein sollten als die von E-Mails, ist nicht ersichtlich.[55] Schon seit einigen Jahren haben E-Mails vielmehr größere Bedeutung als SMS,[56] eine Einbeziehung in den Anwendungsbereich des § 113b TKG ist somit durchaus denkbar.[57] Parallel zu den Regelungen bezüglich SMS könnten hierbei Postfach von Sender und Empfänger sowie Datum und Uhrzeit von Versendung und Empfang gespeichert werden.[58]

f) Over-the-top-Telekommunikationsdienstleistungen

Es ist umstritten, ob die §§ 113a ff. TKG auch sog. Over-the-top-Telekommunikationsdienste (OTT-TKD), d.h. Telekommunikationsdienste, die wie WhatsApp oder Threema über das Internet erbracht werden,[59] verpflichten.[60] Gerade in den letzten Jahren nahmen diese OTT-TKD im Vergleich zu herkömmlichen Telekommunikationsdiensten maßgeblich an Relevanz zu.[61] In seinem Referentenentwurf zum Telekommunikationsmodernisierungsgesetz (TKMoG)[62], nimmt der Gesetzgeber die OTT-TKD jedoch explizit aus dem Anwendungsbereich des § 175, der dem jetzigen § 113b TKG entspricht, heraus.[63] Dies spräche dafür, dass auch nach jetzigem Stand OTT-TKD nicht einbezogen werden sollten. Ob dies aus Effektivitätsgründen sinnvoll ist, bleibt zweifelhaft, die Eingriffsintensität der Vorratsdatenspeicherung wird hierdurch jedoch deutlich abgemildert.

51 § 3 Nr. 19 TKG.
52 BT-Drs. 18/5088, S. 27; *Hensel,* DuD 2009, 527 (528).
53 *De Montjoye et al.,* Unique in the Crowd. The privacy bounds of human mobility, Scientific Report 2013, abrufbar unter: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3607247/ (zuletzt abgerufen am 12.10.20).
54 BT-Drs. 18/5088, S. 23.
55 *Bär,* in: BeckOK-StPO, § 113b TKG Rn. 18.
56 Vgl. *Bulowski,* Regulierung von Internetkommunikationsdiensten. Zur Anwendbarkeit des Telekommunikationsrechts auf Voice over IP, Instant Messaging und E-Mail-Dienste, 2019, S. 31.
57 Vgl. *Bär,* in: BeckOK-StPO, § 113b TKG Rn. 18.
58 Vgl. § 113a Abs. 3 TKG a.F.
59 BNetzA, Nutzung von OTT-Kommunikationsdiensten in Deutschland. Bericht 2020, S. 5.
60 *Mayen,* in: Scheurle/Mayen, 3. Auflage (2018), § 113a Rn. 3.
61 BNetzA (Fn. 59), S. 5.
62 BMWi/BMVI, Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts, 14.12.20, abrufbar unter: https://www.bmwi.de/Redaktion/DE/Downloads/Gesetz/telekommunikationsmodernisierungsgesetz-referentenentwurf-20201612.pdf?__blob=publicationFile&v=8 (zuletzt abgerufen am 10.3.21).
63 A.a.O., § 175 Abs. 1 TKG-E.

2. Zweck der Speicherung

a) Verfolgung von Straftaten

Nach dem Grundsatz der Datenzweckbindung dürfen Daten in der Regel nur zu vorher festgelegten Zwecken gespeichert werden.[64] Gemäß Art. 15 Abs. 1 S. 1 RL 2002/58/EG darf eine Datenspeicherung nur erfolgen, wenn sie für die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit oder die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen notwendig, angemessen und verhältnismäßig ist. § 100g StPO i.V.m. § 113b regelt gerade die Verfolgung von Straftaten, so dass die Regelung bezüglich der Zwecksetzung ohne Weiteres als europarechtskonform gelten kann. Auch nach Vorgabe des *BVerfG* kann eine Vorratsdatenspeicherung zum Zwecke der Strafverfolgung erfolgen.[65]

b) Sonderfall § 100j StPO

Andere Anforderungen stellt das *BVerfG* in Bezug auf die Personenauskunft zu dynamischen IP-Adressen. Hierbei können Ermittler eine Auskunft über Bestandsdaten nach §§ 95, 111 TKG anhand dynamischer IP-Adressen fordern. Die Ermittler erhalten so selbst keinen Zugriff auf Verkehrsdaten, für eine Auskunft müssen jedoch die TKD eben solche Verkehrsdaten auswerten.[66]

aa) Beurteilung durch das BVerfG

Das *BVerfG* sieht hierin aus mehreren Gründen einen schwächeren Eingriff in Art. 10 Abs. 1 GG. Zum ersten erhielten die Behörden selbst keinen Zugriff auf die sensiblen Verkehrsdaten.[67] Darüber hinaus bleibe der Erkenntniswert verhältnismäßig gering[68] und der Ausschnitt der Daten, die verwendet werden müssten, sehr klein.[69] Daraus leitet das *BVerfG* ab, dass ein solches Auskunftsersuchen sogar zur Verfolgung von „besonders gewichtigen Ordnungswidrigkeiten“ möglich sei.[70] Der Gesetzgeber hat auf diese Möglichkeit zwar verzichtet, so dass Ordnungswidrigkeiten gemäß § 46 Abs. 2 OWiG gänzlich vom Anwendungsbereich des § 100j Abs. 2 ausgeschlossen sind. Dennoch sind die Anforderungen des § 100j Abs. 1, 2 deutlich geringer als die des § 100g StPO.

bb) Kritik

Die Einschätzung durch das *BVerfG* ist keineswegs unproblematisch. Für das Datenmengenargument gilt, dass eine gezielte Abfrage nur einer Verbindungsinformation ebenfalls eine deutlich geringere Menge an Daten verlangt, als die umfassende Vorratsdatenspeicherung bereithält. Doch gerade die Menge an Möglichkeiten dieser für sich genommen wenig datenintensiven Erhebungen ist es, die die Sensibilität der Speicherung und damit hohen Voraussetzungen an die strafprozessuale Verwertung, sei sie im Rahmen von § 100g Abs. 2 oder § 100j Abs. 2 StPO, begründet. Auch das Argument des fehlenden Verkehrsdatenzugriffs durch Behörden überzeugt nur begrenzt. Wenn das *BVerfG* in jeder Verwertung der Daten einen Eingriff[71] sieht und dem Gesetzgeber

64 Art. 6 Abs. 1 lit. c Datenschutzrichtlinie 95/46/EG; BVerfGE 65, 1 (46).
65 Vgl. BVerfGE 125, 260 (328).
66 *Bär,* MMR 2013, 700 (701).
67 BVerfGE 125, 260 (340 f.).
68 BVerfGE 125, 260 (340 f.).
69 BVerfGE 125, 260 (341).
70 BVerfGE 125, 260 (344).
71 BVerfGE 125, 260 (312 f.).

die Speicherung der Daten durch Unternehmen als unmittelbaren Eingriff zurechnet,[72] ist unklar, warum die Verwertung durch dieselben weniger eingriffsintensiv sein sollte als durch die Strafverfolgungsbehörden. Denkbar wäre eine geringere Intensität lediglich deshalb, da die Daten bei den TKD durch die Speicherung sowieso schon vorliegen und durch die Auswertung keine neue Institution Zugriff auf Verkehrsdaten erhält.[73] Zu bezweifeln bleibt auch der geringere Erkenntniswert. Inwieweit der Erkenntniswert, welche Rufnummer es war, die A zu einer bestimmten Zeit angerufen hat, höher sein soll als der, dass Person A es war, die zu einem bestimmten Zeitpunkt eine bestimmte IP-Adresse benutzt hat, bleibt unklar. In beiden Fällen können unter Kenntnis einer weiteren Information (der IP-Adresse zuzuordnende Aktion und Besitzer der Rufnummer) Rückschlüsse auf Aktions- bzw. Telekommunikationsinhalt gezogen werden. Überzeugender ist insoweit das Argument des *EuGH*, der Wert von IP-Adressen für Strafverfahren wäre besonders hoch.[74] Dies ändert jedoch nichts daran, dass die Verwertung von IP-Adressen per se sehr eingriffsintensiv ist, ermöglichen sie doch ebenso tiefe Einblicke in Person und Persönlichkeit wie andere Formen der Telekommunikation.[75] Vor diesem Hintergrund wirken die milden Vorgaben des *BVerfG* und die halbherzige Umsetzung durch den Gesetzgeber unbefriedigend.[76] Zumindest eine geringe Anhebung der Eingriffsvoraussetzungen, bspw. auf die des § 100g Abs. 1 StPO, wäre wünschenswert.

3. Zweck der Erhebung

Das *BVerfG* fordert eine klare Begrenzung des Anwendungsbereichs des § 100g Abs. 2 StPO auf Straftaten gegen überragend wichtige Rechtsgüter.[77] Auch wenn sich viele Ermittler eine dem § 100g Abs. 1 StPO vergleichbare Regelung gewünscht hätten,[78] welcher nicht nur leichte Straftaten umfasst, solange sie durch Telekommunikation erfolgen (Nr. 2), sondern auch einen größeren Spielraum bezüglich der zu verfolgenden besonders schweren Tat lässt (Nr. 1), hat das *BVerfG* solche Generalklauseln für § 100g Abs. 2 unmissverständlich untersagt.[79] Das Gesetz von 2015 kommt den Anforderungen des Gerichts nach, indem es den Anwendungsbereich des § 100g Abs. 2 StPO auf einen exklusiven Straftatenkatalog beschränkt.[80]

4. Datensparsamkeit/ Begrenzung auf das absolut Notwendige

Um die Schwere der Grundrechtseingriffe auf ein Minimum zu reduzieren,[81] müssen die Speicherung und Verwendung von Daten immer auf das absolut Notwendige begrenzt bleiben.[82] Indem der Gesetzgeber enge Voraussetzungen an die Erforderlichkeit der Erhebung und die Begründung derselben setzt,[83] erfüllt er diesen Grundsatz in Bezug auf die Verwertung. Anders präsentiert sich die Situation jedoch bezüglich der Speicherung von Daten. Fraglich ist bspw., ob eine Einbeziehung reiner Geschäftskundenanbieter in die Speicherpflicht, in Anbetracht ihrer geringen Bedeutung für die Aufklärung von Straftaten nach § 100g Abs. 2 StPO, als erforderlich betrachtet

72 BVerfGE 125, 260 (311).
73 Vgl. *BVerfG*, NJW 2020, 2699 (2713).
74 *EuGH*, La Quadrature du Net, Rn. 152.
75 *EuGH*, La Quadrature du Net, Rn. 153.
76 Vgl. *Greco,* in: SK-StPO, § 100j Rn. 4; *Hauck,* in: LR-StPO, 27. Auflage (2019), § 100j Rn. 15; *Nelles*, S. 223.
77 BVerfGE 125, 260 (328).
78 MPI, S. 160.
79 BVerfGE 125, 260 (329).
80 BT-Drs. 18/5088, S. 24.
81 *Nelles*, S. 35.
82 *EuGH*, Tele2, Rn. 96.
83 Vgl. §§ 100g Abs. 2 S. 1, 101a Abs. 2.

werden kann.[84] Darüber hinaus sollte möglichst keine doppelte Speicherung erfolgen. In Anlehnung an Erwägungsgrund 13 S. 2 der ehemaligen Richtlinie entschied sich der deutsche Gesetzgeber, nur TKD, nicht auch die Netzbetreiber zu verpflichten. Eine Mehrfachspeicherung ergibt sich dennoch in den Fällen, in denen die Kommunikationspartner Kunden unterschiedlicher TKD sind. Hier speichern beide Unternehmen die identischen Daten. Eine Möglichkeit, dies zu vermeiden, wäre die individuelle Verpflichtung nur einzelner TKD durch die Bundesnetzagentur.[85] Dies hätte außerdem den Vorteil, dass bei einer Fokussierung auf die großen Unternehmen höhere Sicherheitsstandards gewährleistet und Kosten gespart werden könnten.[86] Gleichzeitig würde es allerdings zwangsläufig dort zu Lücken führen, wo beide Kommunikationspartner über nichtverpflichtete Unternehmen agieren. Dies wäre nicht nur aus Gleichbehandlungsgesichtspunkten problematisch, sondern würde auch unter Umständen das Notwendige unterschreiten. Um diese Lücken zu vermeiden, müsste in jedem Einzelfall oder für jede Kombination von Dienstanbietern eine Regelung getroffen werden, was in Anbetracht der rund 2500 Anbieter,[87] und damit über 6 Millionen möglicher Kombinationen, eine schier nicht zu bewältigende Aufgabe sein dürfte. Deutlich zweckdienlicher und unkomplizierter scheint es, die Speicherpflicht auf den TKD des Absenders zu beschränken.[88]

5. Technische Ausgestaltung

Besonders detaillierte Vorgaben machen *BVerfG* und *EuGH* in Bezug auf die technische Ausgestaltung der Vorratsdatenspeicherung.[89] Dies ist kaum verwunderlich in Anbetracht der Tatsache, dass einer der größten Kritikpunkte die Möglichkeit des Zugangs und Missbrauchs der hochsensiblen Daten durch TKD, den Staat oder Dritte ist.[90] Unter anderem verlangt das *BVerfG*, dass die zutreffenden Sicherheitsvorkehrungen stets an den Stand der Technik angepasst werden und eine Speicherung dezentral bei den Unternehmen erfolgt.[91] Der Gesetzgeber ist dem in seinem Neuentwurf 2015 nachgekommen und hat alle wesentlichen Vorgaben des *BVerfG* eingearbeitet.[92] Lediglich § 101a Abs. 3 StPO, welcher in seinem Anwendungsbereich bisher auf „personenbezogene Daten" beschränkt ist, müsste sprachlich korrigiert werden, um sicherzustellen, dass sich die vom *BVerfG* geforderte Kennzeichnungs- und Löschungspflicht auf alle Verkehrsdaten bezieht.[93] Gerade kleinere Unternehmen dürften Schwierigkeiten haben, die technischen Anforderungen zu erfüllen.[94] Noch vor Verabschiedung des Gesetzes kritisierte der IT-Branchenverband *Eco*, die vorgesehene Speicherung auf vom Internet entkoppelten Rechnern und eine schnelle Übermittlung der geforderten Daten an die Polizei unter Einhaltung der geforderten komplizierten Verschlüsselung seien nicht umsetzbar.[95] Die *BNetzA* stellte jedoch klar, dass die Verschlüsselung nur so komplex sein müsse, dass eine effektive Abfrage noch möglich sei, und schlägt eine transparente Datenbankverschlüsselung

84 *Roßnagel et al.* (Fn. 41), S. 141.
85 *Roßnagel et al.* (Fn. 41), S. 141.
86 *Roßnagel et al.* (Fn. 41), S. 145.
87 *Greis*, Kritik an Gesetzentwurf. Eco hält Vorratsdatenspeicherung für nicht umsetzbar, Golem 20. Mai 2015, abrufbar unter: https://www.golem.de/news/eco-kritik-an-gesetzentwurf-vorratsdatenspeicherung-ist-technisch-nicht-umsetzbar-1505-114166.html (zuletzt abgerufen am 13.10.20).
88 *Roßnagel et al.* (Fn. 41), S. 140.
89 Vgl. BVerfGE 125, 260 (325 ff.).
90 Vgl. BVerfGE 125, 260 (318).
91 BVerfGE 125, 260 (321, 326).
92 Vgl. §§ 113d-g TKG.
93 *Kleen/Riegler,* AL 2017, 59 (63).
94 *Roßnagel et al.* (Fn. 41), S. 144.
95 *Greis* (Fn. 87).

oder eine Container-Verschlüsselung auf Basis des *Advanced Encryption Standards* vor.[96] Eine den aktuellen Gesetzesvorgaben genügende Verschlüsselung scheint somit durchaus möglich zu sein. Darüber hinaus gesteht die *BNetzA* ein, dass eine vollständige Abkopplung vom Internet nicht möglich sei und eine Sicherung gegen Zugriffe durch *Fire-Walls* genüge.[97] Da hier jedoch nicht wirklich von einer „Entkoppelung" gesprochen werden kann, ist der Gesetzestext insoweit anzupassen. Da das *BVerfG* entkoppelte Speicher nur als mögliche, nicht zwingende Maßnahme erachtet,[98] ist dies ohne Weiteres möglich. Kritisiert wird weiterhin, dass nach wie vor keine routinierte, flächendeckende Überprüfung der Umsetzung von Sicherheitskonzepten erfolgt, sondern sich die *BNetzA* auf eine Überprüfung des Sicherheitskonzeptes selbst und einzelne stichprobenartige Überprüfungen beschränkt.[99] Nur wenn regelmäßige, verdachtsunabhängige Kontrollen zur Einhaltung der technischen Anforderungen durchgeführt werden, kann jedoch der Schutz hochsensibler Daten ausreichend sichergestellt werden.[100] Darüber hinaus muss bei Zuwiderhandlung eine effektive Sanktionierung erfolgen.[101] Das *BVerfG* empfiehlt die Festlegung von Sanktionen, um die Sicherheit der Daten zu gewährleisten, betont allerdings zugleich den großen Spielraum des Gesetzgebers diesbezüglich,[102] welcher dementsprechend noch keine Repressalien festgelegt hat. Dies sollte möglichst bald nachgeholt werden. Kaum geregelt ist die Speicherung und Sicherung der Daten bei den Ermittlungsbehörden.[103] Aus datenschutzrechtlichen Erwägungen sollte und darf hier jedoch nichts anderes gelten als für die Speicherung bei den TKD.[104]

6. Kostentragung

Nach aktueller Gesetzeslage werden die Kosten der Speicherung von den TKD selbst getragen, solange keine unbilligen Härten entstehen.[105] Nur bei der Datenübermittlung und Auskunftserteilung entstehende Kosten werden gemäß § 23 JVEG ersetzt. Das *BVerfG* beurteilt eine Kostentragung durch die Unternehmen nicht als unverhältnismäßig, beschränkt sich jedoch bei der Analyse möglicher Kostenpunkte auf die Bereitstellung technischer Infrastruktur, über welche die TKD zu großen Teilen schon verfügten.[106] Das Gericht verkennt hierbei jedoch, dass die Sicherheitsanforderungen an die auf Vorrat zu speichernden Daten deutlich höher sind als für die schon früher gemäß §§ 96, 111 TKG gesammelten. So verwundert es kaum, dass die IT-Branchenverbände *Bitkom* und *Eco* mit Mehrkosten in Höhe von 200 bis 600 Millionen Euro rechnen.[107] Besonders kleinere Unternehmen, die mit Kosten von bis zu 80 000 Euro rechnen müssten, drohe deswegen die Insolvenz.[108] Es finden sich folglich viele Befürworter einer zumindest teilweisen Kostentragung.[109] Mitunter wird die Kostentragung durch die TKD sogar als verfassungswidrig erachtet.[110] Eine Kostenübernahme durch den Staat überzeugt vor allem unter dem Gesichtspunkt, dass die Strafverfolgung zu dem Kern staatlicher Aufgaben zählt, so dass, wird die Aufgabe schon nicht

96 BNetzA, Anforderungskatalog nach § 113f TKG. Katalog von technischen Vorkehrungen und sonstigen Maßnahmen zur Umsetzung des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, BGBl. I S. 2218, 10.12.2015, S. 15.
97 BNetzA (Fn. 96), S. 17.
98 BVerfGE 125, 260 (325 f.).
99 Siehe §§ 113f Abs. 2 S. 3 iVm 109 Abs. 7 S. 1 TKG; vgl. G*ärtner/Kipker,* DuD 2015, 593 (594).
100 G*ärtner/Kipker,* DuD 2015, 593 (594).
101 *Roßnagel et al.* (Fn. 41), S. 149.
102 BVerfGE 125, 260 (339).
103 G*ärtner/Kipker,* DuD 2015, 593 (596).
104 Vgl. *Roßnagel et al.,* DuD 2009, 536 (538).
105 § 113a TKG.
106 BVerfGE 125, 260 (361 f.).
107 *Greis* (Fn. 87); BT-Drs. 249/15.
108 *Greis* (Fn. 87).
109 *Freiling,* Zur Nutzung von Verkehrsdaten im Rahmen der Vorratsdatenspeicherung, Technischer Bericht TR-2009-005 Universität Mannheim Institut für Informatik, 2009, S. 23; G*ärtner/Kipker,* DuD 2015, 593 (595); *Roßnagel et al.* (Fn. 41), S. 154.
110 *Nelles,* S. 285.

durch ihn wahrgenommen, sie doch zumindest von ihm finanziell getragen werden sollte.[111] Erstrebenswert wäre eine Kostenübernahme zu nur 80%, um die Sparsamkeit der Unternehmen zu gewährleisten, und die Kostentragung von der Erfüllung der Sicherheitsvorgaben abhängig zu machen.[112]

7. Berufsgeheimnisträger

Mitunter wird kritisiert, die Vorratsdatenspeicherung verringere die Bereitschaft, Kommunikation innerhalb bestimmter Vertrauensbeziehungen wahrzunehmen.[113] Wie eine *Forsa*-Umfrage aus dem Jahr 2008 zeigt, sind diese Bedenken keineswegs unbegründet.[114] Aus diesem Grund fordert das *BVerfG,* eine Übermittlung von Daten, die einer Kommunikation i.S.d. § 99 Abs. 2 TKG zugrunde liegen, auszuschließen.[115] Der Gesetzgeber geht insoweit über diese Vorgaben hinaus, als er die Erhebung von Daten jeder Kommunikation unterbindet, bei der ein Berufsgeheimnisträger beteiligt ist.[116] Hier zeigt sich eine gewisse Diskrepanz zur Speicherung der Daten, welche gestattet ist, solange es sich nicht um Verbindungen i.S.d. § 99 Abs. 2 TKG handelt.[117] Wenn jedoch Daten von Berufsgeheimnisträgern nicht übermittelt werden dürfen, entfällt insoweit der strafrechtliche Zweck, der einen Eingriff in das Telekommunikationsgeheimnis durch die Speicherung rechtfertigen würde.[118] Folglich muss auch eine Speicherung dieser Daten so weit wie möglich verhindert werden.[119] Es liegt nahe, zur Ermittlung der auszunehmenden Anschlüsse, Listensysteme anzulegen, auf welche die TKD zurückgreifen können. Hierfür müssten Berufsgeheimnisträger unter Nachweis ihrer Geheimnisträgereigenschaft verpflichtend die von ihnen beruflich genutzten Anschlüsse und Rufnummern angeben. Nach einer Variante würde diese Angabe direkt bei den TKD erfolgen, indem Bestandskunden einmalig und neue Kunden bei Vertragsschluss nach ihrer Berufsgeheimnisträgereigenschaft befragt werden.[120] Ebenso denkbar wäre, ein System einzuführen, bei welchem eine Ausnahme bei der *BNetzA* zu beantragen ist, welche wiederum die TKD über die von der Speicherung auszunehmenden Anschlüsse informiert.[121] Dieses Vorgehen hätte den Vorteil, dass so auch keine Daten des Kommunikationsgegenübers und Nicht-Kunden mit Berufsgeheimnisträgereigenschaft gespeichert würden, dessen Status dem Unternehmen ansonsten nicht bekannt wäre. Sinnvollerweise sollten regelmäßige Angaben über den aktuellen Status erfolgen.[122] Bei den Telekommunikationsunternehmen müssten nun automatisiert eben diese Anschlüsse und Rufnummern entweder von Beginn an aus der Speicherung herausgefiltert werden oder im Falle, dass die Daten für Zwecke nach §§ 96, 100 TKG genutzt werden sollen, nach Ablauf der zulässigen Speicherfrist, d.h. unverzüglich nach Zweckerfüllung, gelöscht werden.

111 *Nelles*, S. 384.
112 *Roßnagel et al.* (Fn. 41), S. 154.
113 *Bizer,* DuD 2007, 586 (587).
114 Forsa, Meinungen der Bundesbürger zur Vorratsdatenspeicherung, P8475/ 20186 Ma, 2.6.2008, abrufbar unter: http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf (zuletzt abgerufen am 5.5.2021), S. 1.
115 BVerfGE 125, 260 (334).
116 § 100g Abs. 4 StPO.
117 § 113b Abs. 6 TKG
118 So auch *Mayen,* in: Scheurle/Mayen, § 113b Rn. 32.
119 Vgl. *EuGH*, Tele2, Rn. 105.
120 *Gärtner/Kipker,* DuD 2015, 593 (598).
121 *Roßnagel et al.* (Fn. 41), S. 156.
122 Vgl. *Gärtner/Kipker,* DuD 2015, 593 (599).

8. Anforderungen an die Anlass- und Personenbezogenheit

a) Anlass der Speicherung

Gemäß § 113b TKG hat die Speicherung sämtlicher aufgezählter Daten jeglicher Telekommunikationsnutzer zu erfolgen, die Speicherung ist somit anlasslos und allgemein. Während das *BVerfG* eine anlasslose Speicherung für mit Art. 10 GG unter bestimmten Voraussetzungen vereinbar hält,[123] verbietet der *EuGH* prinzipiell eine derartige Datenspeicherung.[124] Nach dem Gerichtshof soll die Vorratsdatenspeicherung die Ausnahme, nicht die Regel sein.[125] Diese Aussage war es auch, die das *OVG Münster* zu der Annahme brachte, die § 113a, 113b TKG verstießen gegen Europarecht.[126] Darüber, dass die aktuelle anlasslose Vorratsdatenspeicherung so nicht länger möglich ist, besteht überwiegend Einigkeit.[127] Deutlich schwieriger gestaltet sich jedoch die Suche nach einer alternativen Ausgestaltung. Während viele Stimmen für eine gänzliche Abschaffung der Vorratsdatenspeicherung plädieren,[128] gilt sie Ermittlern als unverzichtbar.[129] Es empfiehlt sich somit, nach einem Weg zu suchen, um aus der anlasslosen eine begründete, anlassbezogene Vorratsdatenspeicherung zu machen. Der *EuGH* fordert eine Einschränkung des Kreises der betroffenen Personen anhand objektiver Kriterien.[130] Demnach muss zumindest ein mittelbarer geographischer, zeitlicher oder personeller Zusammenhang zwischen der Überwachung und möglichen schweren Straftaten bestehen.[131] Fraglich ist, wie dieser im Bereich der Strafverfolgung aussehen könnte.

aa) Geographischer Bezug

Relativ unproblematisch erscheint insoweit die Begründung des geographischen Bezuges. Demnach soll eine Vorratsdatenspeicherung in einem bestimmten örtlichen Umfeld möglich sein, solange anhand objektiver Anhaltspunkte anzunehmen ist, dass in einem bestimmten Gebiet das Risiko benannter Straftaten erhöht ist.[132] Der Gerichtshof enthält sich jedoch weiterer Spezifikationen insbesondere, wie eng dieser Kreis gezogen sein muss. Aufgrund der hohen Eingriffsintensität ist jedoch unter Verhältnismäßigkeitsgesichtspunkten eine enge Begrenzung zu fordern, eben damit die Speicherung ihren Ausnahmecharakter behält.[133] Für die meisten Katalogtaten des § 100g Abs. 2 ist nicht ersichtlich, dass ihre Wahrscheinlichkeit in erheblicher Weise örtlichen Bezug aufweist. Denkbar wäre allerdings in Hinblick auf die Taten der Nr. 1c) und f) eine Speicherung im Bereich von Rotlichtmilieus anzuordnen, ist hier doch durchaus ein höheres Vorkommen dieser Straftaten feststellbar.[134] In Bezug auf Betäubungsmitteldelikte könnte eine Überwachung an den objektiv messbar größten Handelsplätzen angedacht werden. Schließlich erscheint auch möglich, gewisse Orte (bspw. Hauptbahnhöfe oder „Problemecken“) zu überwachen, solange in diesen Bereichen eine objektiv gesteigerte Kriminalität feststellbar ist. Vermieden werden muss dabei jedoch eine undifferenzierte Ausweitung auf ganze Stadtviertel. Obligatorisch bleibt jeweils die regelmäßige Feststellung, ob der betroffene Ort noch den Kriterien für die Speicherung entspricht.

123 BVerfGE 125, 260 (318).
124 *EuGH*, Tele2, Rn. 107.
125 *EuGH*, Tele2, Rn. 104.
126 *OVG Münster*, NVwZ-RR 2018, 43 (48).
127 *Bulowski*, S. 51; *Derksen,* Zur Vereinbarkeit der Richtlinie über die Vorratsspeicherung von Daten mit der Europäischen Grundrechtecharta (Ausarbeitung WD 11 – 3000 – 18/11), 2011, S. 24; *Kühling,* VerfBlog 2017, S. 2; *Marsch,* VerfBlog 2016, S. 3; *Roßnagel,* NJW 2017, 696 (698).
128 *AK Vorratsdatenspeicherung et al.,* Gemeinsame Erklärung zum 6-jährigen Bestehen der EU-Richtlinie zur Vorratsspeicherung, 14.12.2011, verfügbar unter http://www.vorratsdatenspeicherung.de/content/view/515/188/lang,de/ (zuletzt abgerufen am 12.10.20).
129 *Münch,* ZRP 2015, 130.
130 *EuGH*, Tele2, Rn. 111.
131 *EuGH*, Tele2, Rn. 106.
132 *EuGH*, Tele2, Rn. 111.
133 Vgl. *EuGH*, Privacy International, Rn. 68.
134 *BKA,* Menschenhandel und Ausbeutung. Bundeslagebild 2018, S. 37.

bb) Zeitlicher Bezug

In seinem Urteil vom 6.10.2020 präzisiert der *EuGH* seine Vorgaben dahingehend, dass eine allgemeine, lediglich zeitlich begrenzte Speicherung nur zum Schutze der nationalen Sicherheit, nicht zur Strafverfolgung zulässig ist.[135] Der zeitliche Bezug ist im Rahmen der Strafverfolgung folglich eher als weiteres eingrenzendes Kriterium für personen- oder ortsbegründete Überwachung zu verstehen.[136]

cc) Personeller Bezug

Schwieriger gestaltet sich eine Eingrenzung anhand persönlicher Merkmale.

(1) Bestimmte Bevölkerungsgruppen

Ein Abstellen auf einzelne, statistisch besonders delinquente Bevölkerungs- oder Berufsgruppen verbietet sich.[137] Bei einem Abstellen auf Abstammung oder Herkunft läge eine Verletzung des Art. 3 Abs. 3 GG vor. Auch in Bezug auf andere Kriterien ist von einer Verletzung des Art. 3 Abs. 1 GG auszugehen, wenn bei einer solchen Typisierung eine nicht nur sehr kleine Gruppe ungerecht behandelt wird und die Eingriffsintensität mehr als gering ist.[138] Da die meisten Menschen keine Straftaten begehen[139] und die Eingriffsintensität der Vorratsdatenspeicherung äußerst hoch ist,[140] läge wohl in jedem Falle eine Verletzung von Art. 3 Abs. 1 GG vor.

(2) Bestimmte Individuen

Eine weitere Möglichkeit wäre die Speicherung bezüglich Personen, die im Verdacht stehen, in Zukunft eine Straftat zu begehen, um – sollte dies tatsächlich eintreten – die Aufklärung zu erleichtern. Die personenbezogene antizipierte Strafverfolgung ist der deutschen Rechtsordnung keineswegs fremd.[141] Alldieweil in derartigen Konstellationen keine Anknüpfung an einen Anfangsverdacht verlangt werden kann,[142] knüpft die Rechtsordnung Maßnahmen antizipierter Strafverfolgung meist an das Vorliegen einer Anlasstat und fordert eine Negativprognose, d.h. die Annahme, dass bezüglich des Betroffenen weitere Strafverfahren zu erwarten sind.[143] Bezogen auf die Vorratsdatenspeicherung müssten die zu erwartenden Straftaten nun denen des Katalogs in § 100g Abs. 2 StPO entsprechen, da nur in diesem Fall die Daten auch erhoben werden könnten. Vom Ausgangspunkt der bereits bestehenden Normen sind aufgrund des hohen Eingriffscharakters der Vorratsdatenspeicherung drei weitere Modifikationen ratsam. Erstens sollte die Überwachung nicht schon bei jedem Beschuldigten, sondern nur in Fällen des § 81g Abs. 4 StPO, insbesondere bei rechtskräftig Verurteilten möglich sein. Insoweit, als die Verhältnismäßigkeit des langen Zeitraums, in dem so eine Anordnung möglich ist, bezweifelt wird,[144] wäre denkbar, eine Anordnung zwingend an die Verkündung des Urteilsspruches zu knüpfen. Drittens sollte die Anordnung der Speicherung wie schon die Datenerhebung[145] auch bei Gefahr in Verzug unter Richtervorbehalt gestellt werden.[146] Mit Hilfe gespeicherter Bestandsdaten können die TKD die Rufnummern und Anschlusskennungen ermitteln, deren Kommunikationsvorgänge gespeichert werden sollen. Eine Pflicht zur Benachrichtigung des Betroffenen sollte

135 *EuGH*, La Quadrature du Net, Rn. 137.
136 Vgl. *EuGH*, La Quadrature du Net, Rn. 168.
137 *Ziebarth,* ZUM 2017, 398 (402).
138 *Nußberger,* in: Sachs, Grundgesetz Kommentar, 8. Auflage (2018), Art. 3 Rn. 109.
139 Siehe *BKA,* Polizeiliche Kriminalstatistik. Bundesrepublik Deutschland. Jahrbuch, Band 3: Tatverdächtige, 67. Ausgabe (2019), S. 27.
140 BVerfGE 125, 260 (328).
141 Siehe §§ 81b, 81g Abs. 1 StPO.
142 *Rudolph*, Antizipierte Strafverfolgung. Zum Regelungsstandort der Strafverfolgungsvorsorge unter Beachtung strafverfahrensrechtlich-funktionaler Aspekte, 2005, S. 13.
143 *Bock,* ZIS 2007, 129 (132).
144 *Bosch,* in: KMR-StPO, § 81g Rn. 15.
145 Vgl. § 101a Abs. 1 S. 2 StPO.
146 Anders § 81g Abs. 3 StPO.

grundsätzlich bestehen, indessen nur solange die Strafverfolgung nicht (mehr) gefährdet wird.[147]

(3) Daten zur Gefahrenabwehr

Ebenfalls denkbar wäre die Verwertung von Daten, die bezüglich bestimmter Personen zum Zwecke der Gefahrenabwehr gespeichert worden sind.[148] Grundsätzlich gilt, dass ohne ausdrückliche Ermächtigungsgrundlage Daten, die zu bestimmten Zwecken gesammelt wurden, nicht zu anderen Zwecken gebraucht werden dürfen.[149] Eine explizite Ermächtigungsgrundlage findet sich hierbei in § 161 Abs. 1 S. 1 StPO, der nach den Maßgaben des § 101a Abs. 5 StPO eine Verwendung von nach Polizeirecht erlangten Daten i.S.d. § 113b TKG zur Strafverfolgung gestattet. § 101a Abs. 5 StPO bezieht sich jedoch lediglich auf „personenbezogene Daten", nicht auf jegliche Verkehrsdaten. Insoweit wäre also eine Anpassung erforderlich. Des Weiteren beschränkt er sich auf „erlangt[e]" Daten, welches streng genommen nur bereits erhobene Daten, nicht die nur gespeicherten umfasst.[150] Wendet man § 101a Abs. 5 StPO dennoch (analog) an, so kann eine Verwertung dann erfolgen, wenn die Daten auf Grund des § 100g Abs. 2 StPO hätten erhoben werden dürfen. § 100g Abs. 2 StPO gestattet allerdings eine Erhebung der Daten nur bei Vorliegen eines Anfangsverdachts, der zu Beginn der präventiven Speicherung ja noch gar nicht vorliegen konnte. Denkbar wäre somit nur noch, die Normen dahingehend anzupassen, dass eine Speicherung gemäß § 113b TKG hätte zulässig sein müssen. Wenn § 113b TKG an europarechtliche Maßgaben angepasst wird, folgt, dass eine Verwertung von Daten, die zum Zwecke der Gefahrenabwehr und bezüglich einer bestimmten Person gesammelt wurden, nur erfolgen kann, wenn diese Daten auch Bezug zu einem Ort aufweisen, an dem gesteigerte Kriminalität zu erwarten ist oder der von der Erhebung Betroffene die unter III. 8. a) cc) (2) genannten Kriterien erfüllt.

dd) Kritik an den Lösungsvorschlägen

Die vorgeschlagenen Lösungsansätze entbehren keineswegs erheblicher Schwächen. So ist bspw. bei der Anwendung des geografischen Kriteriums mitnichten evident, wann denn ein besonders belastetes Gebiet vorliegen soll bzw. wie eng oder genau dieses abzugrenzen ist. Auch bedeutet ein erhöhtes Kriminalitätsaufkommen innerhalb eines bestimmten Areals nicht, dass die Kommunikation innerhalb dieses Bereichs für Ermittler auch besonders ergiebig ist. Eine Überwachung einzelner Geräte andererseits würde einen immensen technischen, finanziellen und organisatorischen Aufwand bedeuten. Daneben träte stets auch das Problem der mannigfaltigen Ausweichmöglichkeiten. Ohne Weiteres ließe sich Kommunikation auf ein nicht überwachtes Gebiet oder Medium übertragen, so dass die Vorratsdatenspeicherung bei beiden Varianten ins Leere liefe. In jedem Fall wäre der Gewinn für die Ermittlungsbehörden denkbar gering, denn eine Strategie, die davon lebt, keine Unterschiede zu machen und alles zu erfassen, kann nicht funktionieren, wenn die Erfassung auf ein Minimum reduziert werden soll. Im Ergebnis präsentiert sich eine Vorratsdatenspeicherung nach Maßgaben des *EuGH* somit doch eher als Gedankenspielerei, denn als realistische Umsetzungsmöglichkeit.

b) Ausnahme: IP-Adressen

Im Oktober 2020 revidierte der *EuGH* seine Einschätzung teilweise. Eine anlasslose Speicherung solle nun in

147 *EuGH*, La Quadrature du Net, Rn. 190.
148 *Engelhardt,* Verwendung präventivpolizeilich erhobener Daten im Strafprozess: Eine Untersuchung am Beispiel der Telekommunikationsüberwachung, 2011, S. 2.
149 Vgl. BVerfGE 65, 1 (46); 92, 191 (197).
150 Vgl. *Bär,* in: BeckOK-StPO, § 101a Rn. 11.

Bezug auf IP-Adressen möglich sein,[151] solange keine Informationen bezüglich der Telekommunikationspartner aufbewahrt werden.[152] Dies wird mit der geringeren Eingriffsintensität und der besonderen Bedeutung von IP-Adressen für die Aufklärung von Online-Kriminalität begründet.[153] Wirklich überzeugen kann diese Argumentation, die sich in ihrer Essenz darauf stützt, die Speicherung sei weniger eingriffsintensiv, da sie nur eine Person betrifft, während sie gleichzeitig gesteht, dass auch diese Daten detaillierte Profilbildungen ermöglichen,[154] nicht. Dass Daten nur einer einzelnen Person gespeichert werden, macht im Ergebnis keinen Unterschied, werden sie es im Rahmen einer flächendeckenden anlasslosen Vorratsdatenspeicherung doch von *jeder* einzelnen Person. Gleichzeitig ist nicht ersichtlich, wieso Informationen über die Telekommunikation mit anderen Individuen mehr Erkenntnisse bringen sollten als die über Aktivitäten im Internet.[155] Letzten Endes wirkt es vielmehr so, als wäre die Standhaftigkeit des *EuGH* dem Drängen der Mitgliedsstaaten zum Opfer gefallen.[156] Folgt man allerdings der neuen Linie des *EuGH*, so wäre eine anlasslose Speicherung im Rahmen von § 113b Abs. 3 möglich.

c) Personenbezug bei der Erhebung

Enger setzt der *EuGH* die Voraussetzungen der Datenabfrage durch die Behörden. Eine Erhebung erachtet er nur als rechtmäßig, wenn sie sich auf Daten der Personen beschränkt, die in Verdacht stehen, eine schwere Straftat begangen zu haben oder in eine solche verwickelt zu sein.[157] Ausnahmen sollen nur in besonderen Fällen möglich sein, wobei eine Ausnahme in Bezug auf die Strafverfolgung nicht genannt wird.[158] Dies bedeutet im Ergebnis, dass eine Datenerhebung durch die Behörden auf Daten des Verdächtigen beschränkt bleiben muss, solange nicht das Gegenüber ebenfalls verdächtig ist, zumindest mit der Straftat in Zusammenhang zu stehen. Der *EuGH* konkretisiert nicht weiter, welcher Qualität dieser Zusammenhang sein muss. Sachdienlich dürfte ein Abstellen auf die dem StGB bekannten Beteiligungsformen[159] sein, da nur in solchen Fällen eine strafrechtliche Verfolgung möglich ist, die einen Eingriff in die Telekommunikationsfreiheit rechtfertigt.[160] Da nicht ausgeschlossen werden kann, dass ein betroffener Anschluss von einer anderen Person genutzt wurde, sind für den unwahrscheinlichen Fall, dass dies schon vor Erhebung bekannt sein sollte, ein Erhebungsverbot und für die Fälle nachträglicher Kenntniserlangung ein Beweisverwertungsverbot vorzusehen.

d) Rekurs: Berufsgeheimnisträger

Auch die Schutzbedürftigkeit der Berufsgeheimnisträger endet dort, wo sie selbst der Beteiligung verdächtig sind.[161] Eine – oben grundsätzlich ausgeschlossene– Speicherung ihrer Daten kann somit erfolgen, wenn sich eine Anordnung direkt gegen den Berufsgeheimnisträger richtet oder eine solche Anordnung hätte erlassen werden können. Da allein durch die Anlegung von Listen eine lückenlose Erfassung aller Kommunikation von Berufsgeheimnisträgern nicht gewährleistet werden kann, müsste bei der alten Ausgestaltung der Vorratsdatenspeicherung

151 *EuGH*, La Quadrature du Net, Rn. 152.
152 *EuGH*, La Quadrature du Net, Rn. 152.
153 *EuGH*, La Quadrature du Net, Rn. 154.
154 *EuGH*, La Quadrature du Net, Rn. 153.
155 Vgl III. 2. b) bb).
156 Vgl. *Rath,* Urteil zur Vorratsdatenspeicherung. Klug Nachgegeben, Die Tageszeitung 6.10.2020, verfügbar unter https://taz.de/Urteil-zu-Vorratsdatenspeicherung/!5716106/ (zuletzt aufgerufen am 14.10.20).
157 *EuGH*, Tele2, Rn. 119.
158 *EuGH*, Tele2, Rn. 119.
159 Vgl. §§ 25 ff. StGB.
160 Vgl. BVerfGE 125, 260 (330).
161 BVerfGE 129, 208 (266 f.); vgl. *Zöller,* in: Gercke et al., 6. Auflage (2019), § 160a Rn. 17.

im Rahmen der Übermittlung der Daten eine weitere Filterung erfolgen.[162] Folgt man jedoch den Vorgaben des *EuGH*, so kann eine Erhebung stets nur dann erfolgen, wenn die Betroffenen in Verdacht stehen, an einer Tat beteiligt zu sein. In solchen Fällen sind jedoch auch Geheimnisträger nicht mehr schützenswert,[163] sodass hier eine gesonderte Regelung zur Erhebung obsolet ist.

e) Quick-Freeze als Alternative

Im Rahmen der Anlassbezogenheit wird häufig auf das Quick-Freeze-Verfahren als Alternative zur Vorratsdatenspeicherung verwiesen.[164] Bei diesem Verfahren können Daten im Sinne des § 96 TKG bei Vorliegen eines Anfangsverdachts „eingefroren", d. h. ihre Löschung vorläufig verhindert werden.[165] Nach dem erforderlichen richterlichen Beschluss werden nun die Daten an die Strafverfolgungsbehörde übermittelt.[166] Auf diese Weise lässt sich eine reguläre Löschung für den Zeitraum, in dem das Vorliegen der weiteren Voraussetzungen des § 100g Abs. 1 S. 1 StPO validiert werden und der richterliche Beschluss eingeholt wird, verhindern. Eine voreilige Erhebung in dem Wissen, dass die Daten bald nicht mehr vorhanden sein werden, dürfte so eher unterbleiben. Im Gegensatz zur anlasslosen Vorratsdatenspeicherung erfolgt hier staatliches Handeln erst bei Vorliegen eines Anfangsverdachtes, so dass auch die Eingriffsintensität geringer ist.[167] 2010 schlug die *FDP*-Fraktion die Einführung eines Quick-Freeze-Verfahrens in die StPO vor. Die Anordnung zum Einfrieren sollte hierbei von der Staatsanwaltschaft mit dreimonatiger Wirkung, in Eilfällen durch die Polizei für drei Tage erfolgen. Eine begründete Verlängerung wäre möglich. [168] Auch der *EuGH* gestattet ein Quick-Freeze-Vorgehen, wobei er betont, dass derartige Maßnahmen nicht auf Tatverdächtige beschränkt bleiben müssen.[169] Um einen möglichst grundrechtsschonenden Eingriff zu gewährleisten, müssen spätestens ab dem Moment des Einfrierens und damit dem Zeitpunkt, ab dem staatliche Behörden aktiv werden, dieselben Sicherheitsanforderungen wie bei der Vorratsdatenspeicherung gestellt und erfüllt werden.[170] Dieses Verfahren mag zwar weniger einschneidend sein als die klassische Vorratsdatenspeicherung, ist jedoch bei weitem nicht so effektiv.[171] Dies liegt vor allem daran, dass eine derartige Anordnung innerhalb sehr kurzer Zeit, nämlich vor der routinemäßigen Löschung, erfolgen muss und sich nur auf Daten erstrecken kann, die das Unternehmen aus geschäftlichen Gründen speichert.[172] Doch statt das Quick-Freeze-Verfahren als ungeeignet abzutun, bietet es sich an, diese Vorgehensweise als Ergänzung zur nunmehr sehr eingeschränkten Vorratsdatenspeicherung zu sehen.

IV. Nutzen einer Vorratsdatenspeicherung

Trotz vielfältigen Problembewusstseins schweigen *EuGH* und *BVerfG*, wenn es um die Frage nach dem tatsächlichen Nutzen der Vorratsdatenspeicherung geht. Beide Gerichte gehen somit wohl davon aus, dass der Nutzen die

162 *Roßnagel et al*. (Fn. 41), S. 156.
163 BVerfGE 129, 208 (266 f.); vgl. *Zöller,* in: Gercke et al., § 160a Rn. 17.
164 *Bizer,* DuD 2007, 586 (588); *Kiparski,* in: Specht/Mantz, 2019, § 18 Rn. 49; *Kunnert,* DuD 2014, 774 (783); *Szuba*, S. 100.
165 *Gercke/Brunst*, Praxishandbuch Internetstrafrecht, 2009, S. 37.
166 *Derksen,* S. 16; MPI, S. 40 f.
167 Vgl. *Sierck et al.,* Zulässigkeit der Vorratsdatenspeicherung nach europäischem und deutschem Recht (Ausarbeitung WD 3 – 282/06), 2006, S. 14; *Szuba*, S. 100.
168 FDP-Bundestagsfraktion: Eckpunkte zur Verbesserung der Kriminalitätsbekämpfung im Internet. Freiheit und Sicherheit im Internet bewahren, 9.11.2010, abrufbar unter: https://web.archive.org/web/20121122054959/http://www.fdp-fraktion.de/files/1228/Eckpunkte_Kriminalitaetsbekaempfung_Internet.pdf (zuletzt abgerufen am 13.10.20), S. 8.
169 *EuGH*, La Quadrature du Net, Rn. 163, 165.
170 Zu dieser Problematik *Nelles*, S. 187.
171 BVerfGE 125, 260 (318); *Nelles*, S. 188 f.
172 MPI, S. 41.

Kosten der Vorratsdatenspeicherung nach den von ihnen aufgestellten Maßgaben aufwiegen kann.[173] Diese Annahme ist jedoch alles andere als zwingend. Sogar wenn man die Effektivitätsdefizite einer anlassbezogenen Speicherung für einen Moment beiseite lassen möchte, ist es doch mehr als umstritten, wie viel selbst die anlasslose Vorratsdatenspeicherung wirklich zur Verbrechensaufklärung beitragen kann.[174] Nach einer zurückhaltenden, jedoch auf umfassende Daten gestützten Einschätzung des Max-Planck-Instituts für ausländisches und internationales Strafrecht ist keine Verbesserung der Aufklärungsquote anzunehmen.[175] Auch eine Studie des Europäischen Parlaments kann keinen messbaren Zusammenhang zwischen Speicherung und Aufklärung feststellen.[176] Gleichzeitig zeugen Einzelfälle davon, dass auf Vorrat gespeicherte Daten zumindest in bestimmten Situationen zur Aufklärung unabdingbar sind.[177] Doch gerade Täter in den Deliktsbereichen Kinderpornografie und organisierte Kriminalität, welche in ihrer Schwere meist als Hauptargument für eine Vorratsdatenspeicherung herangezogen werden, dürften wohl in Anbetracht ihrer an den Tag gelegten Professionalität und der hohen Strafandrohung auf Ausweichmöglichkeiten wie das Darknet oder die Verschleierung von IP-Adressen zurückgreifen.[178] Tritt nun hinzu, dass – wie vom *EuGH* gefordert – nur IP-Adressen anlasslos gespeichert werden dürfen, folgt aus der einerseits zweifelhaften Sinnhaftigkeit der anlassbezogenen Speicherung[179] und den andererseits vielfältigen Umgehungsmöglichkeiten im Bereich der IP-Adressspeicherung, dass sich der Wert dieses Vorgehens der Null annähern dürfte. Dass eine (anlasslose) Vorratsdatenspeicherung wirklich in dem Maße nützt, welches diesen schweren Grundrechtseingriff zu rechtfertigen vermag, kann somit entgegen der Vorstellungen von *EuGH* und *BVerfG* durchaus bezweifelt werden.

V. Fazit

Die aktuelle Regelung der Vorratsdatenspeicherung genügt in vielerlei Hinsicht nicht den Anforderungen des *EuGH*. Eine Reform müsste insbesondere die Anlassbezogenheit der Speicherung und die Zweckgebundenheit sowie Erforderlichkeit der Erhebung garantieren. Jenseits dessen besteht auch in praktischer Hinsicht Verbesserungspotential. Und wie immer im Spannungsfeld zwischen Sicherheit und Freiheit kann eine Lösung nur bei Zugeständnissen auf beiden Seiten gefunden werden. Eine europa- und verfassungsrechtskonforme Regelung ist wohl möglich. Ob sie aber auch sinnvoll ist, ist eine ganz andere Frage. Eine Vorratsdatenspeicherung 3.0 würde nicht nur enormen strukturellen und finanziellen Aufwand für Staat und Unternehmen bedeuten. Abgesehen von der Frage, ob die Vorgaben, bspw. zum Schutz der Berufsgeheimnisträger,[180] überhaupt technisch umsetzbar wären, führten die Einschränkungen von Anwendungsbereich und Zweckdienlichkeit über den ohnehin schon zweifelhaften Nutzen der Vorratsdatenspeicherung hinaus wohl zur kompletten Sinnlosigkeit dieses Vorgehens. Eine anlassbezogene Vorratsdatenspeicherung passt einfach nicht zur Strafverfolgung.

173 *EuGH*, Tele2, Rn. 108; BVerfGE 125, 260 (317).
174 *Derksen*, S. 15; *Moser-Knierim*, S. 191, *Puschke,* ZIS 2019, 308 (313); *Szuba*, S. 99.
175 MPI, S. 129.
176 European Parliament, General data retention/effects on crime, 27.1.2020, S. 3.
177 MPI, S. 82, 143 f.; *Münch,* ZRP 2015, 130.
178 Vgl. Hoppenstedt, Wie Pädokriminelle das Internet nutzen – und wie Ermittler sie finden können, Spiegel Netzwelt 1.7.2020, abrufbar unter: https://www.spiegel.de/netzwelt/web/kindesmissbrauch-wie-taeter-das-internet-nutzen-und-wie-ermittler-sie-finden-koennen-a-868362db-8a11-4847-a280-d748d79dbbf3 (zuletzt abgerufen am 15.12.20).
179 Siehe III. 8. a) dd).
180 Vgl. BT-Drs. 18/5088, S. 33.

VI. Schluss

Aktuell mehren sich erneut die Stimmen, die eine Vorratsdatenspeicherung zumindest bezüglich IP-Adressen fordern.[181] Es ließe sich wohl behaupten, dies sei die Schuld des *EuGH,* welcher, statt der Vorratsdatenspeicherung ein klares Ende zu setzen, in seinen Urteilen immer wieder Hintertüren für eine zumindest eingeschränkte Speicherung offen hält. So ergreift der Gerichtshof auch im jüngsten Urteil vom 02.03.2021 nicht die Chance, ein für alle Mal Klarheit zu schaffen.[182] Doch die Politik geht noch weiter. Diskutiert, gefordert und geplant wird nach wie vor eine anlasslose, allgemeine Vorratsdatenspeicherung, die eigentlich zwingenden Vorgaben des *EuGH* werden blindlings ignoriert.[183] Dabei wäre es vielleicht an der Zeit, zu akzeptieren, dass eine sinnvolle und legale Form der Vorratsdatenspeicherung nicht möglich ist. Der Rechtsstaat ist kein leerer Begriff. Er setzt feste Grenzen, über die sich staatliches Handeln nicht hinwegsetzen darf und wenn es bedeuten mag, dass eine Vorratsdatenspeicherung nicht effektiv umgesetzt werden kann. Dennoch: die Vorratsdatenspeicherung ist und bleibt Thema. Und so wie die Geschichte 2005 (*"The Never-Ending Story "*[184]) oder 2015 nicht endete (*A Never-Ending Story: Die Vorratsdatenspeicherung*[185]*, „Die unendliche Geschichte der Vorratsdatenspeicherung: Bürger unter Generalverdacht"*[186]*, „Es ist eine unendliche Geschichte"*[187]*, Vorratsdatenspeicherung: Eine unendliche (nervige) Geschichte*[188]), tat sie es auch 2016 (*Nein! Doch! Oh! Die unendliche Geschichte der Vorratsdatenspeicherung*[189]), 2017 (*Hintergrund: Vorratsdatenspeicherung, die endlose Geschichte*[190]) und 2019 *(„Die unendliche Geschichte der Vorratsdatenspeicherung"*[191]) nicht. Dass sie es 2021 tun wird, ist mehr als unwahrscheinlich und so bleibt nur abzuwarten, ob *BVerfG* und *EuGH* einen Schlusspunkt setzen und der Gesetzgeber die Urteile akzeptiert oder eine neue Runde im ewigen Kreislauf der Vorratsdatenspeicherung eröffnet werden wird.

181 Briegleb, Drei Bundesländer fordern Wiederaufnahme der Vorratsdatenspeicherung, Heise online 19.11.20, abrufbar unter: https://www.heise.de/news/Drei-Bundeslaender-fordern-Wiederaufnahme-der-Vorratsdatenspeicherung-4966157.html (zuletzt abgerufen am 10.1.21); European Council, European Council meeting (10 and 11 December 2020) – Conclusions, 11.12.2020, Rn. 26.

182 *EuGH*, Urt. v. 2.3.2021, C-746/18, ECLI:EU:C:2021:152- Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques).

183 Vgl. BMWi/BMVI, § 175 I TKG-E; Council of the European Union, Informal Outcome of Proceedings of the informal VTC of the members of CATS on 8 February 2021, 26.2.21, S. 4.

184 *Hülsmann,* The Never-Ending Story, Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. -Kommunikation 3/2005, S. 48.

185 *Spiecker/Simitis,* VerfBlog 5.5.2015, abrufbar unter: https://verfassungsblog.de/a-never-ending-story-die-vorratsdatenspeicherung/ (zuletzt abgerufen am 13.10.20).

186 ZDF-Frontal 21, Die unendliche Geschichte der Vorratsdatenspeicherung. Bürger unter Generalverdacht, 2015.

187 *Kurz,* Vorratsdatenspeicherung. An der Grenze geltenden Rechts, Frankfurter Allgemeine Zeitung 1.6.2015, abrufbar unter: https://www.faz.net/aktuell/feuilleton/aus-dem-maschinenraum/vorratsdatenspeicherung-an-der-grenze-des-geltenden-rechts-13622263.html (zuletzt abgerufen am 13.10.20).

188 *Rieß,* Vorratsdatenspeicherung, Eine unendliche (nervige) Geschichte, ComputerWeekly 20.4.2015, abrufbar unter: https://www.computerweekly.com/de/meinung/Vorratsdatenspeicherung-Eine-unendliche-nervige-Geschichte (zuletzt abgerufen am 13.10.20).

189 *Miraus,* Nein! Doch! Oh! Die unendliche Geschichte der Vorratsdatenspeicherung, BasicThinking 29.12.2016, abrufbar unter: https://www.basicthinking.de/blog/2016/12/29/vorratsdatenspeicherung-illegal/ (zuletzt abgerufen am 13.10.20).

190 *Faisst,* Hintergrund. Vorratsdatenspeicherung, die endlose Geschichte, Südwest Presse 12.8.2017, abrufbar unter: https://www.swp.de/politik/inland/hintergrund_-vorratsdatenspeicherung_-die-endlose-geschichte-23608613.html (zuletzt abgerufen am 13.10.20).

191 o.V., Vorratsdatenspeicherung: Deutsche Gerichte verweisen auf den EuGH, t3n 29.9.2019, abrufbar unter: https://t3n.de/news/vorratsdatenspeicherung-deutsche-1201909/ (zuletzt abgerufen am 13.10.20).

KriPoZ Kriminalpolitische Zeitschrift JuP

„Junges Publizieren“

Seminararbeit von

Maria Lesina

Europäische Herausgabe- und Sicherungsanordnung

Ludwig-Maximilians-Universität München
Betreuer: Prof. Dr. Mark Zöller
Abgabedatum: 26.10.2020

Inhaltsverzeichnis

I. Einleitung

Die fortschreitende Digitalisierung hat weitreichende Auswirkungen auf unseren Alltag. Heutzutage entstehen digitale Daten in nahezu jedem gesellschaftlichen Kontext.[1] Sie entstehen zum Beispiel durch die Nutzung von Social Media und Messenger-Diensten, bei der IP-Telefonie, beim bargeldlosen Bezahlen und bei der Verwendung von Smart Watches sowie Smart Home Systemen.[2] Wir leben in „den Zeiten des gläsernen Menschen“[3]. Noch nie zuvor lagen so viele Daten über uns vor. In der Zusammenschau haben diese Datenmengen eine große Aussagekraft.[4] Auch im Bereich der Kriminalität stellen E-Mail-, Messenger- und Social Media-Dienste wichtige Kommunikationsmittel dar.[5] Demgemäß haben Strafverfolgungsbehörden ein großes Interesse an den gespeicherten Daten.[6] Elektronische Beweismittel werden immer bedeutender für die Strafverfolgung.[7] Doch die zunehmende Digitalisierung bietet Strafverfolgungsbehörden nicht nur noch nie dagewesene Möglichkeiten bei der Aufklärung von Straftaten, sondern stellt diese auch vor neue Herausforderungen.[8] Die Behörden stehen bei der Erlangung und Sicherung dieser elektronischen Beweise vor zahlreichen rechtlichen und praktischen Hindernissen.[9] Digitale Daten sind nicht an einen bestimmten Ort gebunden und werden häufig auf Servern im Ausland gespeichert, sodass Ermittlungen zum Großteil grenzüberschreitend erfolgen müssen. Deshalb kommt es verstärkt auf eine internationale Zusammenarbeit an.[10] Doch die derzeit zur Verfügung stehenden Rechtsinstrumente der internationalen Zusammenarbeit sind nicht an die Flüchtigkeit von elektronischen Beweismitteln angepasst.[11] Der herkömmliche Rechtshilfeweg hat sich als zu umständlich und langwierig herausgestellt.[12] Deswegen ist in den letzten Jahren das Bedürfnis nach einem neuen Kooperationsinstrument entstanden.[13] So sieht z.B. *Burchard* in der Regelung des grenzüberschreitenden Zugriffs auf in der Cloud gespeicherte Daten „eine der drängendsten Aufgaben der Internetära“.[14]

Die Europäische Kommission hat im April 2018 einen Vorschlag für ein neues Kooperationsinstrument zum grenzüberschreitenden Zugriff auf elektronische Beweismittel in Strafsachen unterbreitet.[15] Es handelt sich dabei um die „Europäische Herausgabe- und Sicherungsanordnung“. Die vorliegende Arbeit befasst sich umfassend mit den aktuellen „E-Evidence“-Gesetzgebungsvorschlägen der Europäischen Kommission. Der erste Teil dieser Arbeit beleuchtet zunächst einige strafprozessual relevante Besonderheiten elektronischer Beweismittel und die Unzulänglichkeiten der derzeit zur Verfügung stehenden Rechtsinstrumente für die internationale Zusammenarbeit in Strafsachen. Anschließend werden die grundlegenden Regelungen des Gesetzgebungsvorschlages dargestellt. Der zweite Teil der Arbeit setzt sich kritisch mit den Vorschlägen auseinander und erörtert eine Reihe rechtsstaatlicher Bedenken.

1 *Fährmann*, MMR 2020, 228.
2 *Fährmann*, MMR 2020, 228.
3 *Burchard*, Das Ende der Souveränität (und anderer Fundamentalprinzipien der Rechtshilfe)?, S. 1.
4 *Blechschmitt*, MMR 2018, 361.
5 *Gössling/Nagel*, ITRB 2019, 41.
6 *Fährmann*, MMR 2020, 228.
7 *Warken*, NZWiSt 2017, 289.
8 *Fährmann*, MMR 2020, 228.
9 *Gössling/Nagel*, ITRB 2019, 41.
10 *Gössling/Nagel*, ITRB 2019, 41.
11 *Hamel*, in: Hoven/Kudlich, Digitalisierung und Strafverfahren, 2020, S. 107.
12 *Burchard* (Fn. 3), S. 1.
13 *Böse*, KriPoZ 2019, 140.
14 *Burchard* (Fn. 3), S. 1.
15 COM (2018) 225 final; COM (2018) 226 final.

II. Europäische Herausgabe- und Sicherungsanordnung

1. „E-Evidence“

a) Problemaufriss

Elektronische Beweismittel weisen eine Reihe von Besonderheiten auf, die ihre Erlangung und Sicherung erschweren. Ein wesentliches Kennzeichen elektronischer Daten ist ihre fehlende Körperlichkeit.[16] Herkömmliche Beweismittel befinden sich tatsächlich physisch auf dem Territorium eines Landes.[17] Daten hingegen sind nicht starr an einen Ort gebunden, vielmehr bestimmen vom Service-Provider generierte Algorithmen ihren Weg.[18] In der Regel bieten Service-Provider ihre Dienste weltweit an. Dabei haben sie meist eine Hauptniederlassung in einem Staat und einige weitere Niederlassungen in anderen Staaten. Die Datenspeicherorte sind jedoch unabhängig von diesen Niederlassungen verteilt.[19] Zudem findet die Speicherung elektronischer Daten nicht mehr zwingend als Gesamtheit an einem Ort statt, sondern erfolgt oftmals aus sicherheitsrelevanten und/oder unternehmerischen Gesichtspunkten in vielen Einzelteilen auf einer Vielzahl von Rechnern. Diese können dann weltweit verstreut sein, weshalb sich rechtliche und praktische Hürden für das Strafverfahren ergeben.[20] Möchten Strafverfolgungsbehörden auf Daten zugreifen, die im Ausland gespeichert sind, so stellen sich rechtliche Fragen hinsichtlich der Beachtung des Territorialitätsprinzips und der Beeinträchtigung der Souveränität des betroffenen ausländischen Staates.[21] Der herkömmliche Weg bei grenzüberschreitenden Ermittlungen in Strafsachen ist das Rechtshilfeverfahren. Befinden sich Beweismittel im Ausland, so können Strafverfolgungsbehörden ein traditionelles Rechtshilfeersuchen stellen, um mit Hilfe der Behörden des ausländischen Staates an diese Beweismittel zu gelangen.[22] Vor allem in Betracht der Flüchtigkeit von Daten hat sich jedoch das System der Rechtshilfe für den grenzüberschreitenden Zugriff auf elektronische Beweismittel als zu langsam und bürokratisch herausgestellt.[23] Elektronische Beweismittel sind durch ihre Volatilität gekennzeichnet und oft nur eine begrenzte Zeit verfügbar.[24] Oftmals ist Service-Providern die Löschung gespeicherter Daten aus Datenschutzgründen vorgeschrieben. Nur unter engen gesetzlichen Voraussetzungen kann eine längerfristige Sicherung der Daten erfolgen.[25] Zudem lassen sich elektronische Daten leicht und vor allem schnell verschieben. Zum Teil wird die permanente Ortsänderung der Daten automatisiert vom Service-Provider durchgeführt.[26] Diese Aspekte machen einen zügigen Zugriff auf die elektronischen Beweismittel erforderlich. Das Rechtshilfeverfahren kann jedoch durchschnittlich mehrere Monate andauern und ist damit nicht an die Besonderheiten der digitalen Welt angepasst.[27]

b) Europäische Ermittlungsanordnung

Wichtige Neuerungen für die grenzüberschreitende Sicherung von Beweisen im Rahmen von Strafermittlungen

16 *Warken*, NZWiSt 2017, 289 (290).
17 *Hamel*, in: Hoven/Kudlich, S. 105.
18 *Hamel*, in: Hoven/Kudlich, S. 105.
19 *Hamel*, in: Hoven/Kudlich, S. 105.
20 *Warken*, NZWiSt 2017, 289 (290).
21 *Warken*, NZWiSt 2017, 289 (295).
22 *Gössling/Nagel*, ITRB 2019, 41.
23 *Mosna*, ZStW 2019, 808 (811).
24 *Hamel*, in: Hoven/Kudlich, S. 104.
25 *Warken*, NZWiSt 2017, 289 (297).
26 *Warken*, NZWiSt 2017, 289 (297).
27 *Warken*, NZWiSt 2017, 289 (297).

brachte die im April 2014 verabschiedete Richtlinie 2014/41/EU über die Europäische Ermittlungsanordnung in Strafsachen.[28] In Deutschland wurde diese Richtlinie vornehmlich durch Änderungen im Gesetz über die internationale Rechtshilfe in Strafsachen im Jahr 2017 umgesetzt.[29] Die Europäische Ermittlungsanordnung ersetzt innerhalb der Europäischen Union das klassische Rechtshilfeabkommen in Strafsachen und ermöglicht den Strafverfolgungsbehörden der Mitgliedstaaten, die Sammlung und Weitergabe von Beweismitteln aller Art in einem anderen Mitgliedstaat zu verlangen. Zur Gewährleistung einer raschen und effektiven Zusammenarbeit zwischen den Mitgliedstaaten wurden verbindliche Fristen und Formblätter eingeführt.[30] Innerhalb von 30 Tagen nach Eingang einer Ermittlungsanordnung muss der Mitgliedstaat entscheiden, ob er der Anordnung Folge leistet. Die Vollstreckung einer Ermittlungsanordnung kann unter bestimmten Voraussetzungen verweigert werden,[31] beispielsweise wenn die Anordnung wesentlichen Rechtsgrundsätzen des Landes zuwiderläuft oder nationalen Sicherheitsinteressen schadet.[32] Entscheidet sich die Vollstreckungsbehörde, die Ermittlungsmaßnahme anzuerkennen, muss die Ermittlungsmaßnahme spätestens 90 Tage nach Erlass durchgeführt werden.[33] Diese Fristen sind jedoch, wenn man die Flüchtigkeit von Daten bedenkt, immer noch zu lang für den grenzüberschreitenden Zugriff auf elektronische Beweismittel.

c) „E-Evidence" – Vorschläge der Europäischen Kommission

Am 17. April 2018 hat die Europäische Kommission ihre Gesetzgebungsvorschläge zum grenzüberschreitenden Zugriff auf elektronische Beweismittel in Strafsachen präsentiert. Diese bestehen aus der Verordnung für Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (im Folgenden Verordnungsvorschlag) und der Richtlinie zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren.[34] Das Gesetzesvorhaben soll einen Rechtsrahmen für die direkte Zusammenarbeit von Ermittlungsbehörden und Service-Providern schaffen.[35] Die Erhebung und Sicherung von elektronischen Beweismitteln in der EU soll dadurch erleichtert und effizienter gestaltet werden.[36] Der Unterschied gegenüber der bisherigen internationalen Zusammenarbeit in Strafsachen besteht darin, dass die Behörde eine Anordnung unmittelbar an den in einem anderen Mitgliedstaat operierenden Service-Provider, besser gesagt an dessen Vertreter, richten kann, ohne die jeweilige nationale Behörde einzuschalten.[37] Der Service-Provider ist daraufhin zur Übermittlung bzw. vorläufigen Sicherung der Daten verpflichtet, ohne dass es einer vorherigen Entscheidung der jeweiligen nationalen Behörde bedarf.[38] So wird der umständliche und bürokratische Behördenweg der Rechtshilfe umgangen.[39]

aa) Der Vorschlag für eine Verordnung über Europäische Herausgabeordnungen und Sicherungsanordnungen

Kompetenzrechtlich ist der Verordnungsvorschlag gestützt auf Art. 82 AEUV, der die justizielle Zusammenarbeit

28 Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Europäische Ermittlungsanordnung in Strafsachen.
29 *Thomae*, in: Hoven/Kudlich, S. 139.
30 Art. 12 Abs. 3 und 4 RL 2014/41/EU.
31 *Thomae*, in: Hoven/Kudlich, S. 139.
32 Art. 12 Abs. 3 und 4 RL 2014/41/EU.
33 *Thomae*, in: Hoven/Kudlich, S. 139.
34 COM (2018) 225 final; COM (2018) 226 final.
35 *Gössling/Nagel*, ITRB 2019, 41 (44).
36 *Gössling/Nagel*, ITRB 2019, 41.
37 *Gössling/Nagel*, ITRB 2019, 41 (44).
38 *Böse*, KriPoZ 2019, 140 (143).
39 *Böse*, KriPoZ 2019, 140 (141).

basierend auf dem Grundsatz der gegenseitigen Anerkennung regelt.[40] Zuständige Justizbehörden sollen direkt von einem Service-Provider, der in der Union elektronische Dienstleistungen anbietet, verlangen können, elektronische Beweismittel im Hinblick auf ein späteres Herausgabeersuchen zu sichern (Sicherungsanordnung) oder herauszugeben (Herausgabeanordnung), ungeachtet, wo die Daten gespeichert sind oder wo der Dienst sitzt.[41] Die vom Anordnungsstaat erlassene Herausgabe- oder Sicherungsanordnung entfaltet eine transnationale Bindungswirkung, ohne dass es einer vorherigen Anerkennung durch eine Justizbehörde des Vollstreckungsstaates bedarf.[42] Der Verordnungsvorschlag stellt klar, dass der Zweck der Europäischen Herausgabe- und Sicherungsanordnung nicht die Verhütung von Straftaten ist, sondern die effektive Strafverfolgung.[43] Die Verordnung würde die Richtlinie 2014/41/EU über die Europäische Ermittlungsanordnung in Strafsachen nicht ersetzen, sondern nur ergänzen. Mit der Europäischen Herausgabe- und Sicherungsanordnung soll den Strafverfolgungsbehörden ein zusätzliches Rechtsinstrument zur Verfügung stehen, dass die Besonderheiten der digitalen Welt berücksichtigt.[44]

(1) Anwendungsbereich

Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen umfassen die Herausgabe und Sicherung gespeicherter Daten von einem Service-Provider und dürfen nur für Strafverfahren während des Ermittlungs- und des Gerichtsverfahrens erlassen werden.[45] Der Verordnungsvorschlag erstreckt sich auf alle Service-Provider, die ihre Dienste in der EU anbieten. Der Begriff „Service-Provider" wird in Art. 2 Nr. 3 des Verordnungsvorschlages definiert. Danach ist „Service-Provider" jede natürliche oder juristische Person, die „elektronische Kommunikationsdienste im Sinne des Artikels 2 Absatz 4 der Richtlinie über den europäischen Kodex für die elektronische Kommunikation, Dienste der Informationsgesellschaft im Sinne des Artikels 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates, bei denen die Speicherung von Daten ein bestimmender Bestandteil der für den Nutzer erbrachten Dienstleistung ist, einschließlich sozialer Netzwerke, Online-Marktplätze, die Transaktionen zwischen ihren Nutzern erleichtern, und anderen Anbietern von Hosting-Diensten, Internetdomänennamen- und IP-Adressendienste wie IP-Adressenanbieter, Domänennamen-Register, Domänennamen-Registrierungsstellen und damit verbundene Datenschutz- und Proxy-Dienste anbietet." Von der Verordnung sind ausdrücklich auch Service-Provider erfasst, die nicht in der EU niedergelassen sind.[46] Vorausgesetzt ist lediglich das Anbieten von Dienstleistungen in EU. Durch das Anbieten von Diensten in der Union ergeben sich für die Service-Provider zahlreiche Vorteile. Das rechtfertigt laut Kommissionsvorschlag die Tatsache, dass alle Service-Provider, die davon profitieren, gleichermaßen der Verordnung unterliegen. Durch die Ausweitung des Anwendungsbereiches sollen nicht nur gleiche Ausgangsbedingungen für die Teilnehmer derselben Märkte gelten, sondern auch eine Strafbarkeitslücke vermieden werden.[47]

(2) Voraussetzungen für den Erlass einer Herausgabe- und Sicherungsanordnung

Es gibt eine Reihe von Voraussetzungen für den Erlass einer Europäischen Herausgabeanordnung. Diese sind in Art. 5 des Verordnungsvorschlages festgelegt. Die Anordnung darf nur erlassen werden, wenn dies im Einzelfall notwendig und verhältnismäßig ist. Darüber hinaus kann sie nur erlassen werden, wenn im Anordnungsstaat in einer vergleichbaren innerstaatlichen Situation eine ähnliche Maßnahme zur Verfügung stünde. Dass sie auch im

40 *Hamel*, in: Hoven/Kudlich, S. 111.
41 *Basar,* jurisPR-StrafR 5/2019, Anm. 1.
42 *Böse*, KriPoZ 2019, 140 (141).
43 COM (2018) 225 final, S. 8.
44 *Basar*, jurisPR-StrafR 5/2019, Anm. 1.
45 Art. 3 Abs. 2 Verordnungsvorschlag, COM (2018) 225 final.
46 Art. 3 Verordnungsvorschlag, COM (2018) 225 final.
47 *Tosza*, NJECL 2020, 161 (172).

Vollstreckungsstaat rechtmäßig wäre, ist allerdings nicht erforderlich.

Der Vorschlag unterscheidet zwischen verschiedenen Datenkategorien. Je nach Datenkategorie gelten unterschiedliche Anforderungsmaßstäbe für den Erlass einer Herausgabeanordnung. Es können Teilnehmerdaten, Zugangsdaten, Transaktionsdaten und Inhaltsdaten von den zuständigen Behörden mit einer Europäischen Herausgabeanordnung eingeholt werden.[48] Diese werden in Art. 2 Nr. 7, 8, 9 und 10 des Verordnungsvorschlages legaldefiniert.

Als Teilnehmerdaten werden Daten kategorisiert, die Informationen über die Identität einer Person offenbaren. Dazu zählen beispielsweise der Name, das Geburtsdatum, die Postanschrift, Rechnungs- und Zahlungsdaten, die Telefonnummer und die IP-Adresse des Kunden. Auch die Art der Dienstleistung und ihre Dauer sind von dieser Datenkategorie umfasst.[49] Zugangsdaten umfassen Daten, die sich auf den Beginn und die Beendigung einer Zugangssitzung für einen Dienst beziehen, ausschließlich zu dem Zweck, den Benutzer des Dienstes zu identifizieren. Dazu gehören beispielsweise das Datum und die Uhrzeit der Nutzung oder Anmeldung und Abmeldung vom Dienst in Verbindung mit der IP-Adresse des Nutzers.

Bei Transaktionsdaten handelt es sich um Daten über die Erbringung einer von einem Service-Provider angebotenen Dienstleistung, die Kontext- oder Zusatzinformationen über eine solche Dienstleistung liefern und von einem Informationssystem des Service-Providers generiert oder verarbeitet werden. Das können z.B. Sende- und Empfangsdaten einer Nachricht sein oder auch Daten zum Standort des Geräts.

Inhaltsdaten sind alle in einem digitalen Format gespeicherten Daten wie Text, Sprache, Videos, Bilder und Tonaufzeichnungen, ausgenommen von Teilnehmer-, Zugangs- oder Transaktionsdaten.[50] Alle diese Datentypen enthalten personenbezogene Daten und fallen somit unter die Garantien im Rahmen der Datenschutzvorschriften der EU.[51]

Eine Herausgabeanordnung für Teilnehmer- und Zugangsdaten kann für jede Straftat erlassen werden. Bei Transaktions- und Inhaltsdaten liegen die Anforderungen etwas höher. Herausgabeanordnungen für Transaktions- und Inhaltsdaten können nur für Straftaten erlassen werden, die im Anordnungsstaat mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren geahndet werden oder die mittels eines Informationssystems begangen wurde.[52] Bei dem Erlass einer Europäischen Herausgabe- oder Sicherungsanordnung muss stets eine justizielle Behörde entweder als anordnende oder als validierende Behörde tätig werden. Für Anordnungen zur Herausgabe von Transaktions- oder Inhaltsdaten ist ein Richter oder ein Gericht erforderlich. Handelt es sich bei den betreffenden Daten um Teilnehmer- oder Zugangsdaten, so kann die Validierung auch von einem Staatsanwalt übernommen werden.[53]

Die Voraussetzungen für den Erlass einer Europäischen Sicherungsanordnung ähneln den Voraussetzungen für die Europäische Herausgabeanordnung. Eine Europäische Sicherungsanordnung kann jedoch unabhängig vom abgefragten Datentyp für jede Straftat erlassen werden und es genügt, wenn ein Staatsanwalt diese Anordnung validiert.

(3) Ausführung und Fristen

Die Herausgabe- und Sicherungsanordnungen werden unter Verwendung spezieller Formblätter (EPOC und

48 Art. 5 Abs. 3 Verordnungsvorschlag, COM (2018) 225 final.
49 Art. 2 Nr. 7 Verordnungsvorschlag, COM (2018) 225 final.
50 Art. 2 Nr. 10 Verordnungsvorschlag COM (2018) 225 final.
51 Art. 2 Verordnungsvorschlag COM (2018) 225 final.
52 *Von Galen*, in: Hoven/Kudlich, S. 127.
53 Art. 4 Verordnungsvorschlag, COM (2018) 225 final.

EPOC-PR) direkt an den Service-Provider übermittelt.[54] Diese Zertifikate enthalten Informationen zu den angewendeten Strafvorschriften, zu den konkret angeforderten Daten und zur Anordnungsbehörde und werden unmittelbar an den vom Vertreter des Service-Providers entsandt.

Für die Ausführung einer Herausgabeanordnung ist eine verbindliche Frist von zehn Tagen vorgesehen. In Eilfällen kann diese Frist gem. Art. 9 Abs. 2 des Verordnungsvorschlages auf sechs Stunden verkürzt werden.[55] Im Falle einer Sicherungsanordnung ist der Service-Provider dazu verpflichtet die betreffenden Daten vorerst für 60 Tage zu sichern.[56]

(4) Vertraulichkeit und Nutzerinformationen

Bei der Ausführung der jeweiligen Anordnung ist der Service-Provider gemäß Art. 11 des Verordnungsvorschlages verpflichtet, die Vertraulichkeit der gesicherten bzw. herausgegebenen Daten zu garantieren. Die Notifizierung der Person, deren Daten angefordert wurden, kann durch die Anordnungsbehörde untersagt werden. In diesem Fall ist die Anordnungsbehörde nach Art. 11 Abs. 2 des Verordnungsvorschlages verpflichtet die betroffene Person selbst zu informieren, wenn es sich bei der betreffenden Anordnung um eine Herausgabeanordnung handelt. Um eine Behinderung des Verfahrens zu vermeiden, ist es der Anordnungsbehörde jedoch gestattet, diese Unterrichtung aufzuschieben. Handelt es sich bei der Maßnahme um eine Sicherungsanordnung, so hat eine Information der betroffenen Personen nicht zu erfolgen.[57]

(5) Ablehnungsgründe

Der Service-Provider kann die Anordnung unter bestimmten Voraussetzungen ablehnen. Die Ablehnungsgründe sind für die Herausgabeanordnung in Art. 9 des Verordnungsvorschlages und für die Sicherungsanordnung in Art. 10 des Verordnungsvorschlages aufgezählt. Der Service-Provider kann der Anordnung entgegentreten, wenn er nicht in den persönlichen Anwendungsbereich der Verordnung fällt, ihm die Ausführung aus tatsächlichen Gründen unmöglich ist oder das Formular unvollständig oder fehlerhaft ausgefüllt ist. In diesem Fall wird der Service-Provider gleichwohl verpflichtet, die Anordnungsbehörde darüber in Kenntnis zu setzen und zunächst um „Klarstellung“ zu bitten. Wendet der Service-Provider ein, dass eine Herausgabeanordnung offenkundig gegen die Charta der Grundrechte der Europäischen Union (GRC) verstößt oder offensichtlich missbräuchlich ist, so hat er die Behörde des Vollstreckungsstaates zu kontaktieren. Diese kann dann nach Art. 9 Abs. 5 des Verordnungsvorschlages die Anordnungsbehörde um Klarstellung ersuchen. Entscheidet sich die Vollstreckungsbehörde davon abzusehen, so ist die Anordnungsbehörde dem Service-Provider gegenüber nicht verpflichtet, sich mit dessen Bedenken auseinanderzusetzen.[58] Darüber hinaus kann der Service-Provider die Anordnung ablehnen, wenn die Befolgung einer Europäischen Herausgabeanordnung im Widerspruch zu den geltenden Rechtsvorschriften eines Drittstaats steht.[59] Die Geltendmachung dieses Ablehnungsgrunds erfordert einen begründeten Einwand durch den Service-Provider und führt, sofern die Anordnungsbehörde die Anordnung aufrechterhält, zu einer Prüfung durch ein Gericht des Anordnungsstaats. Nur in dem Fall, dass die Rechtsvorschrift des Drittstaats den Grundrechtsschutz betrifft, sind dessen Behörden zu informieren, und deren etwaiger Widerspruch gegen eine Herausgabeanordnung zu beachten.[60]

54 Art. 8 Verordnungsvorschlag, COM (2018) 225 final.
55 *Gössling/Nagel*, ITRB 2019, 41 (45).
56 Art. 10 Verordnungsvorschlag, COM (2018) 225 final.
57 *Basar*, jurisPR-StrafR 5/2019, Anm. 1.
58 *Basar*, jurisPR-StrafR 5/2019, Anm. 1.
59 Art. 15 Verordnungsvorschlag, COM (2018) 225 final.
60 *Brodowski*, ZIS 2018, 493 (503).

(6) Vollstreckungsverfahren und Sanktionen

Verweigert der Service-Provider die Anordnung, so kommt dem Staat, in dem der betroffene Service-Provider niedergelassen ist, die Rolle zu, eine Sanktion zu verhängen und die Anordnung zu vollstrecken.[61] Dem Service-Provider drohen in diesem Fall Strafen von bis zu 2 % seines globalen Jahresumsatzes. [62]

(7) Rechtsschutz

Gem. Artikel 17 des Verordnungsvorschlages haben Verdächtige und Beschuldigte, deren Daten im Wege einer Europäischen Herausgabeanordnung eingeholt wurden, unbeschadet der nach der Richtlinie (EU) 2016/680 und der Verordnung (EU) 2016/679 verfügbaren Rechtsbehelfe das Recht, während des Strafverfahrens, für das die Anordnung erlassen wurde, wirksame Rechtsbehelfe gegen die Europäische Herausgabeanordnung einzulegen. Personen, deren Daten angefordert wurden, bei denen es sich aber nicht um Verdächtige oder Beschuldigte in einem Strafverfahren handelt, haben ebenfalls ein Recht auf einen Rechtsbehelf. Der Rechtsbehelf kann nur vor einem Gericht im Anordnungsstaat eingelegt werden. Betroffenen einer Sicherungsanordnung stehen keine spezifischen Rechtsbehelfe zur Verfügung.

bb) Der Vorschlag für eine Richtlinie zur Bestellung von Vertretern

Ergänzend zum Verordnungsvorschlag hat die Europäische Kommission einen Vorschlag für eine Richtlinie zur Bestellung von Vertretern unterbreitet.[63] Der Vorschlag stützt sich auf Art. 53 und 62 AEUV, die „den Erlass von Maßnahmen zur Koordinierung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung und Erbringung von Dienstleistungen vorsehen".[64] Ziel dieser Richtlinie ist es, zu bestimmen, an wen die Behörden der Mitgliedstaaten Anordnungen zur Erlangung von Beweismitteln, die sich im Besitz von Service-Providern befinden, richten können.[65] Die Zustellung gerichtlicher Anordnungen an Service-Provider soll über einen Vertreter erfolgen. Jeder Service-Provider, der seine Dienste in mehreren Mitgliedstaaten der EU anbietet, soll mindestens einen Vertreter in einem dieser Mitgliedstaaten benennen, an den die gerichtlichen Anordnungen adressiert werden können. Diese Vertreter sind dann im Namen der Service-Provider rechtlich dafür verantwortlich, dass den gerichtlichen Anordnungen und Beschlüssen nachgekommen wird. Das soll für mehr Rechtssicherheit sorgen und etwaige Hindernisse, bei der Zustellung von Anordnungen an Service-Provider verhindern.[66]

2. Kritische Auseinandersetzung mit den E-Evidence-Gesetzgebungsvorschlägen

Trotz des anzuerkennenden Bedarfs an einem schnellen grenzüberschreitenden Zugang zu elektronischen Beweismitteln bestehen erhebliche rechtstaatliche Bedenken gegen die geplanten Regelungen.[67] Für die Erlangung und Verwertung elektronischer Beweismittel gelten „die allgemeinen Verfahrensgrundrechte und -prinzipien, wie sie sich aus dem Rechtsstaatsprinzip oder ausdrücklich aus dem Grundgesetz, der GRC und der Konvention zum Schutz der Menschenrechte und der Grundfreiheiten (EMRK) ergeben".[68]

61 *Niekrenz*, Juridikum 2020, 160 (164).
62 *Thomae*, in: Hoven/Kudlich, S. 142.
63 COM (2018) 226 final.
64 COM (2018) 226 final, S. 5.
65 COM (2018) 226 final, S. 3.
66 COM (2018) 226 final, S. 3 f.
67 DAV, Stellungnahme Nr. 42/2018, S. 7.
68 *Warken*, NZWiSt 2017, 289 (292).

Die E-Evidence Gesetzgebungsvorschläge könnten eine unverhältnismäßige Beeinträchtigung der in der GRC garantierten Rechte darstellen.
Im Folgenden werden einige rechtstaatliche Bedenken gegenüber dem Verordnungsvorschlag geschildert und das Ausmaß der Grundrechts- und Interessenbeeinträchtigung dargestellt.

a) Verlust der innerstaatlichen justiziellen Überprüfungsinstanz

Die direkten Adressaten von Herausgabe- (bzw. Sicherungs-)Anordnungen sind die privaten Service-Provider bzw. deren Vertreter. Sie haben nach Art. 9 des Verordnungsvorschlages eine (oberflächliche) Rechtskontrolle durchzuführen.[69] Eine staatliche Überprüfungsmöglichkeit durch den Vollstreckungsstaat ist jedoch nicht vorgesehen. So werden hoheitliche Aufgaben privaten Unternehmen auferlegt, was kritisch zu sehen ist.[70] Denn die fehlende Einbeziehung von Justizbehörden führt zu einer mangelnden Kontrolle des Grundrechtschutzes. Die Service Provider müssen die Anordnung unter der Androhung von Strafzahlungen binnen knapp bemessener Fristen ausführen.[71] Fraglich ist, ob es unter solchen Bedingungen überhaupt zu einer umfassenden rechtlichen Prüfung der Anordnungen durch den Service-Provider kommen kann.[72] Die Prüfungsmöglichkeiten der Service-Provider sind zudem stark beschränkt. Denn ein etwaiger Grundrechtsverstoß kann nur auf der Grundlage der im zugesendeten Zertifikat enthaltenen Informationen überprüft werden.[73] Diese sind für eine rechtliche Prüfung wohl kaum aussagekräftig. So sind gemäß Art. 8 des Verordnungsvorschlages die komplette Begründung in Bezug auf die Notwendigkeit und Verhältnismäßigkeit oder weitere Einzelheiten zu dem Fall gerade nicht Bestandteil des Zertifikats. Unter diesen Umständen erscheint eine umfassende Grundrechtsprüfung schwierig.
Private Unternehmen handeln zudem meist aus wirtschaftlichen Überlegungen. Da dem Service-Provider durch die Verordnung bei Nichtbefolgung der Anordnungen Strafzahlungen drohen, wird dieser kaum gewillt sein, der Anordnungsbehörde zu widersprechen und sich dem Haftungsrisiko auszusetzen. [74]

b) Fehlende Benachrichtigungspflichten und Fehlen effektiver Rechtsmittel

Das neue Kooperationsinstrument weist zudem gravierende Defizite im gerichtlichen Rechtschutz auf.[75] Das betrifft sowohl die betroffenen Nutzer als auch die Service-Provider.

aa) Rechtsbehelfe der Betroffenen
Nach dem Verordnungsvorschlag sind die Betroffenen von Sicherungsanordnungen nicht über die Maßnahme in Kenntnis zu setzen, wenn der Sicherungsanordnung keine Herausgabeanordnung folgt.[76]
Die fehlende Benachrichtigungspflicht wird in dem Vorschlag mit dem Fehlen eines entsprechenden Rechtsbehelfes gegen Sicherungsanordnungen begründet.[77] Das ist wenig überzeugend. Eine Sicherungsanordnung stellt zwar insgesamt einen geringfügigeren Eingriff als die Herausgabeanordnung dar, doch die Tatsache, dass es sich dabei

69 *Burchard*, ZIS 2018, 249 (265).
70 DAV, Stellungnahme Nr. 42/2018, S. 7.
71 *Thomae*, in: Hoven/Kudlich, S. 142.
72 *Brodowski*, ZIS, 2018, 493 (503).
73 *Burchard*, ZIS 2018, 249 (265).
74 DAV, Stellungnahme Nr. 42/2018, S. 7.
75 *Böse*, KriPoZ 2019, 140 (143).
76 DAV, Stellungnahme Nr. 42/2018, S. 9.
77 DAV, Stellungnahme Nr. 42/2018, S. 9 ff.

um eine faktisch heimliche Maßnahme handelt, spricht für eine hohe Eingriffsintensität.[78] Die Sicherung personenbezogener Daten ohne Kenntnis des Betroffenen ist eine Beeinträchtigung der in Art. 7 und Art. 8 GRC garantierten Grundrechte auf die Achtung des Privatlebens und den Schutz personenbezogener Daten. Dem Betroffenen einer Sicherungsanordnung müsste folglich das Recht auf einen wirksamen Rechtsbehelf gem. Art. 47 Abs. 1 GRC zustehen.

Betroffene einer Herausgabeanordnung müssen zwar über die Maßnahme in Kenntnis gesetzt werden, die Notifizierung kann jedoch aufgeschoben werden, wenn der Anordnungsstaat das für erforderlich hält, um das Verfahren nicht zu gefährden. Die fehlende Kenntnis des Betroffenen führt dazu, dass er rechtlich gar nicht gegen die Maßnahme vorgehen kann, auch wenn ihm Rechtsbehelf zustehen würde.[79] Das stellt eine unverhältnismäßige Beeinträchtigung von Art. 47 Abs. 1 GRC dar.

Zu kritisieren ist weiterhin, dass der betroffene Nutzer den gerichtlichen Rechtsschutz gegen die Übermittlung seiner Daten allein im Anordnungsstaat erlangen kann.[80] Das kann diesen vor einige Hindernisse stellen und ist eine unverhältnismäßige Belastung des Betroffenen.

bb) Rechtsbehelfe des Service-Providers

Der Service-Provider als der direkte Adressat einer Herausgabe- oder Sicherungsanordnung hat nach Art. 47 Abs.1 GRC auch einen Anspruch auf gerichtlichen Rechtsschutz. Denn gemäß Art. 47 Abs.1 GRC hat jede Person, deren durch das Recht der Union garantierte Rechte oder Freiheiten verletzt worden sind, das Recht, einen wirksamen Rechtsbehelf einzulegen. Auch juristische Personen sind davon umfasst, soweit ihnen ein Recht zusteht.[81]

Service-Provider werden in ihrem Recht auf unternehmerische Freiheit (Art. 16 GRC) verletzt, indem sie Daten ihrer Nutzer herausgeben müssen. Darüber hinaus stellt die Sanktionierung bei Nichtbefolgung der Anordnung einen Eingriff in das Eigentumsrecht (Art. 17 GRC) dar. Nach dem Verordnungsvorschlag hat der Service-Provider jedoch kein Recht, die Rechtmäßigkeit einer gegen ihn ergangenen Europäischen Herausgabeanordnung im Ausstellungsstaat gerichtlich überprüfen zu lassen.[82] Er kann lediglich die Rechtmäßigkeit der Sanktion rechtlich prüfen lassen.

c) Unzureichender Schutz besonderer Vertrauensverhältnisse

Zu kritisieren ist weiterhin, dass besondere Vertrauensverhältnisse durch den Kommissionsentwurf nicht ausreichend geschützt werden. Sie können nicht als Versagungsgrund geltend gemacht werden.[83] So gefährdet die Verordnung unter anderem den Schutz der Anwalt-Mandanten-Kommunikation, aber auch Journalisten, Politiker, Oppositionelle und Ärzte sind dadurch beeinträchtigt.[84] Denn genau diese Personengruppen sind auf den Schutz ihrer Daten angewiesen und wählen ihren Datenspeicherort mit Bedacht. Bestimmte Cloudmodelle beruhen gerade darauf, dass Daten ihrer Nutzer an Orten sicher gespeichert werden, wo die Datenschutzstandards hoch sind.[85] Der Verordnungsvorschlag verkennt die Bedeutung solcher „Datenschutzhäfen“[86] und bietet diesen schützenswerten Personengruppen keinen ausreichenden Schutz.

78 DAV, Stellungnahme Nr. 42/2018, S. 9 ff.
79 DAV, Stellungnahme Nr. 42/2018, S. 9 ff.
80 *Böse*, KriPoZ 2019, 140 (143).
81 Art. 47 GRC
82 *Böse*, KriPoZ 2019, 140 (143).
83 *Basar*, jurisPR-StrafR 5/2019, Anm. 1.
84 DAV, Stellungnahme Nr. 42/2018, S. 12 f.
85 *Burchard*, ZRP 2019, 164 (165).
86 *Burchard*, ZRP 2019, 164 (165).

Das „digitale Asyl“ [87] wird Betroffenen genommen, indem für diese nur die Immunitäten und Vorrechte des Strafverfolgungsstaats gelten sollen, also nicht die Datenschutzrechte am Speicherort.[88]

d) Doppelbestrafung des Adressaten, der die Vollstreckung verweigert

Von Galen kritisiert die Tatsache, dass es zu einer Doppelbestrafung des Service-Providers kommen kann, wenn dieser die Vollstreckung einer Herausgabeanordnung hartnäckig verweigert.[89]
Wird die Herausgabeanordnung durch den Service-Provider nicht oder nicht korrekt ausgeführt oder verstößt er gegen die Pflicht, die Durchführung der Herausgabeanordnung gegenüber den Betroffenen vertraulich zu halten, so wird dieses Verhalten gem. Art. 13 des Verordnungsvorschlages sanktioniert.[90] Befolgt der Service-Provider die Herausgabeanordnung nicht, soll die Vollstreckung der Anordnung nach Art. 14 des Verordnungsvorschlages durch eine nationale Vollstreckungsbehörde erfolgen. Sollte der Adressat seiner Pflicht, die Anweisung der Vollstreckungsbehörde zu befolgen, nicht nachgehen, so kann er ein weiteres Mal von der Vollstreckungsbehörde sanktioniert werden.[91] Der Adressat, der also beharrlich die Ausführung der Herausgabeanordnung ablehnt – zunächst gegenüber der Anordnungsbehörde und dann gegenüber der Vollstreckungsbehörde – kann wegen derselben Verweigerungshaltung zweimal bestraft werden.[92]
Von Galen sieht darin einen Verstoß gegen den internationalen anerkannten Grundsatz ne bis in idem.[93] Dieser Grundsatz ist in Art. 50 GRC festgelegt. Gemäß Art. 50 GRC darf niemand wegen einer Straftat, derentwegen er bereits in der Union nach dem Gesetz rechtskräftig verurteilt oder freigesprochen worden ist, in einem Strafverfahren erneut verfolgt oder bestraft werden. Die hartnäckige Weigerung der Anordnung Folge zu leisten, kann durchaus als eine einheitliche Tat angesehen werden.[94] Folglich kann den Bedenken von *von Galen* zugestimmt werden.

e) Verzicht auf beidseitige Strafbarkeit

Zu kritisieren ist weiterhin, dass in dem Verordnungsvorschlag das Erfordernis beidseitiger Strafbarkeit im Gegenteil zur Europäischen Ermittlungsanordnung nicht als Erlassvoraussetzung für europäische Herausgabe- und Sicherungsanordnungen vorgesehen ist.[95] Die nationalen Strafrechtssysteme der Mitgliedsstaaten der EU sind in weiten Teilen unterschiedlich ausgestaltet.[96] So kann es dazu kommen, dass beispielsweise maltesische Behörden von einem deutschen Service-Provider die Herausgabe von Daten für ein Strafverfahren anordnen, das einen Schwangerschaftsabbruch betrifft, der in Deutschland allerdings legal wäre.[97] Es würde sinnvoller erscheinen, der europäische Gesetzgeber würde in einem Katalog die Straftaten festlegen, für welche die Verordnung gilt.[98]

87 *Niekrenz*, Juridikum 2020, 160 (167).
88 *Burchard,* ZRP 2019, 164 (165).
89 *Von Galen*, in: Hoven/Kudlich, S. 133.
90 *Von Galen*, in: Hoven/Kudlich, S. 133.
91 *Von Galen*, in: Hoven/Kudlich, S. 133.
92 *Von Galen*, in: Hoven/Kudlich, S. 133.
93 *Von Galen*, in: Hoven/Kudlich, S. 133.
94 *Von Galen*, in: Hoven/Kudlich, S. 133.
95 *Niekrenz*, Juridikum 2020, 160 (165).
96 *Hecker*, Europäisches Strafrecht, 5. Aufl. (2015), Rn. 5.
97 *Niekrenz*, Juridikum 2020, 160 (165).
98 *Thomae*, in: Hoven/Kudlich, S 142.

f) Zu weitreichender Anwendungsbereich

Wie bereits oben dargelegt, muss die Straftat, zu deren Verfolgung eine Herausgabeanordnung auf den Zugriff von Transaktions- und Inhaltsdaten ergeht, nach dem Recht des Ausstellungsstaates mit einem Höchstmaß von mindestens drei Jahren Freiheitsstrafe geahndet werden können.[99] Fraglich ist, ob diese Voraussetzung zur Verhältnismäßigkeit der Grundrechtseingriffe beiträgt. Denn eine Mindesthöchststrafe von drei Jahren ist bei einer Vielzahl von Straftaten vorgesehen, die keinesfalls nur den Bereich der schweren Kriminalität umfassen.[100] So würde zum Beispiel in Deutschland der Tatbestand des einfachen Diebstahls (§ 242 StGB) oder der Körperverletzung (§223 StGB) darunterfallen. Ob für diese Straftaten eine grenzüberschreitende Anordnung zur Herausgabe sensiblerer Daten verhältnismäßig wäre, ist allerdings zweifelhaft. Bloße Bagatelldelikte müssten von dem Anwendungsbereich ausgenommen werden.[101]

g) Folgen der Entterritorialisierung der Cloud

Herkömmlich werden Zugriffsmöglichkeiten auf Daten vom Datenspeicherort abhängig gemacht (Territorialitätsprinzip). Der Verordnungsvorschlag beruht jedoch auf der Annahme einer umfassenden Entterritorialisierung der Cloud.[102] Nach dem Kommissionsvorschlag wird die Zugriffsmöglichkeit auf Daten davon abhängig gemacht, ob der Service-Provider im Inland seine Dienste anbietet (Marktortprinzip). [103] Der Datenspeicherort spielt dabei keine Rolle.
Dies wird unter anderem mit dem Argument begründet, dass es Nutzern „egal“ wäre, wo ihre Daten abgespeichert werden. Diese Annahme trifft jedoch, wie bereits oben dargestellt, nicht zu. Zudem verletzen unilaterale Beibringungsanordnungen die Territorialhoheit des Staates des Serverstandortes, was zu Vertrauenskonflikten führen kann.[104]
Die EU sollte darüber hinaus berücksichtigen, dass wenn europäische Strafverfolger von Service-Providern aus Drittländern, die in der EU aktiv sind, die Herausgabe sämtlicher Daten verlangen dürfen, diese das gem. dem Reziprozitätsprinzip in Zukunft ähnlich handhaben könnten und von europäischen Service-Providern die Herausgabe von auf europäischen Servern gespeicherten und/oder europäische Bürger betreffenden Daten verlangen.[105] Fraglich ist, ob das wünschenswert ist.

III. Ausblick

Mit dem Vorschlag der Kommission soll ein harmonisierter Rahmen für die direkte Zusammenarbeit zwischen Strafverfolgungsbehörden und Service-Providern geschaffen werden.[106] Der grenzüberschreitende Zugriff auf elektronische Beweismitteln in der EU soll dadurch effektiv gestaltet werden.[107] Der Verordnungsvorschlag ver-

99 *Böse*, KriPoZ 2019, 140 (143).
100 *Böse*, KriPoZ 2019, 140 (143).
101 DAV, Stellungnahme Nr. 42/2018, S. 9 ff.
102 *Burchard*, ZRP 2019, 164 (175).
103 *Burchard*, ZIS 2018, 249 (254).
104 *Burchard* (Fn. 3), S. 7.
105 *Burchard*, ZRP 2019, 164 (166).
106 *Böse*, An assessment of the Commission's proposals on electronic evidence, 2018, S. 48.
107 *Gössling/Nagel*, ITRB 2019, 41.

folgt damit zwar einen legitimen Zweck, entspricht jedoch nicht den unionsverfassungsrechtlichen Mindeststandards.[108] Der Grundrechtsschutz der Betroffenen kommt deutlich zu kurz, wenn die Wahrung der Grundrechte nicht von den Mitgliedstaaten, in deren Hoheitsgebiet der Auftrag ausgeführt werden soll, überprüft wird, sondern von dem Service-Provider und/oder der Anordnungsbehörde. [109] Diese sind faktisch nicht in der Lage einen angemessenen Schutz zu gewährleisten.[110] Die fehlenden Benachrichtigungspflichten der Betroffenen stellen einen intensiven und unverhältnismäßigen Grundrechtseingriff dar. Auch das Fehlen effektiver Rechtsmittel ist untragbar. Mit dem Verordnungsvorschlag der Kommission werden eine Reihe von Kooperationshindernissen beseitigt. Dies beschleunigt zwar das Verfahren, doch fällt zu Lasten des Grundrechtsschutzes. So wird der Einzelne des Schutzes beraubt, den ihm der traditionelle Rahmen der internationalen Rechtshilfe bietet.[111] Die Schutzinteressen der betroffenen Personen und die Interessen der Service-Provider sowie die Souveränitätsinteressen jener Staaten, in deren Territorium die angefragten Daten gespeichert sind, werden nicht hinreichend gewichtet.[112] Das Strafverfolgungsinteresse kann die weitreichenden rechtsstaatlichen Defizite nicht rechtfertigen. Die Beeinträchtigung der Grundrechte der Betroffenen und der Service-Provider ist unverhältnismäßig und der Vorschlag sollte umfassenden Änderungen unterzogen werden. Vollstreckungsbehörden müssten mehr in das Verfahren einbezogen werden, um den Grundrechtsschutz der Betroffenen zu gewährleisten. Die Voraussetzungen für den Erlass einer Herausgabe- oder Sicherungsanordnung müssten zudem präziser gestaltet werden. Der Rechtsschutz müsste ausgebaut werden. Daten schutzbedürftiger Personen und Berufsgruppen sollten nur unter bestimmten Bedingungen abgefragt werden dürfen.[113] Darüber hinaus erscheint es aus Gründen der Verhältnismäßigkeit sinnvoll, der Sicherungsanordnung den Vorrang zu lassen und die Herausgabeanordnung ohne vorheriges Sicherungsverfahren lediglich Fälle zu beschränken, in denen ansonsten der Verlust der elektronischen Beweiskette zu befürchten ist.[114] In seiner jetzigen Form kann dem Kommissionsvorschlag nicht zugestimmt werden.

[108] *Burchard*, ZRP 2019, 164 (166).
[109] *Basar*, jurisPR-StrafR 5/2019, Anm. 1.
[110] *Böse* (Fn. 107), S. 48.
[111] *Böse* (Fn. 107), S. 48.
[112] *Burchard*, ZRP 2019, 164 (164).
[113] *Burchard*, ZRP 2019, 164 (167).
[114] *Basar*, jurisPR-StrafR 5/2019, Anm. 1.

KriPoZ Kriminalpolitische Zeitschrift JuP

„Junges Publizieren“

Seminararbeit von

Theresa List

Strafverfolgung von Rechtsextremismus im Internet

Prof. Dr. Mark A. Zöller
Ludwig-Maximilians-Universität München
5.10.2020

Inhaltsverzeichnis

I. Netzwerke des Hasses und der Gewalt

„*Wegschauen ist nicht mehr erlaubt*."[1] Diesen eindringlichen Appell richtete Bundespräsident Frank-Walter Steinmeier an die Anwesenden einer Gedenkfeier zum 40. Jahrestag des Oktoberfestattentats und spielte damit auf zahlreiche Versäumnisse bei der Aufklärung rechtsextremistischer Anschläge in der Vergangenheit der Bundesrepublik an.[2] Rückblickend sei klar, dass die Täter in „*Netzwerke des Hasses und der Gewalt*" eingebunden waren.[3] Solche Netzwerke finden sich auch im Internet: In rechtsextremen Chatgruppen werden gewalttätige Angriffe auf Ausländer und politische Gegner geplant, in den sozialen Netzwerken steht die Verbreitung von Hassbotschaften auf der Tagesordnung. Eine zunehmende Verrohung der Kommunikations- und Diskussionskultur gefährdet den freien Meinungsaustausch im Internet.[4]

Auf diese Entwicklung muss der Staat reagieren und in den Fällen, in denen die Grenze zur Strafbarkeit überschritten ist, eine effektive Strafverfolgung von Rechtsextremismus auch bei Tatbegehung im Internet sicherstellen. Im Folgenden soll, nach einer knappen begrifflichen Eingrenzung, ein Überblick über die typischen Erscheinungsformen und die zahlenmäßige Verbreitung von Rechtsextremismus im Internet gegeben werden. Daran schließt sich eine Darstellung der zuständigen Strafverfolgungsbehörden und der durch die Strafverfolgung tangierten Grundrechte an, bevor auf die bestehenden strafprozessualen Rechtsgrundlagen für Ermittlungen im Internet eingegangen wird. Abschließend wird diskutiert, inwieweit das geplante „Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität"[5] die derzeit bestehenden Probleme bei der Bekämpfung von Rechtsextremismus im Internet zu lösen vermag.

II. Rechtsextremismus im Internet – alter Wein in neuen Schläuchen?

1. Begriffsbestimmung und -eingrenzung

a) Rechtsextremismus

Zunächst bedarf es einer Erläuterung, was unter dem Begriff *Rechtsextremismus* zu verstehen ist. Dieser ist in Politik- und Sozialwissenschaften weder klar definiert noch allgemein anerkannt, beherrscht aber die politische Alltagssprache.[6] Für die Zwecke der vorliegenden Arbeit soll folgende Definition herangezogen werden:

Bei Rechtsextremismus handelt es sich um eine Ideologie der Ungleichheit, wonach der Wert eines Menschen untrennbar mit dessen Ethnie, Nation oder Rasse verknüpft ist.[7] Daraus folgt die Überhöhung der eigenen sowie

---

1 Bundespräsidialamt, Bundespräsident *Frank-Walter Steinmeier* bei einer Gedenkfeier zum 40. Jahrestag des Oktoberfestattentats am 26. 9.2020 in München, abrufbar unter: https://www.bundespraesident.de/SharedDocs/Downloads/DE/Reden/2020/09/200926-Gedenkfeier-Oktoberfest.pdf?__blob=publicationFile (zuletzt abgerufen am 30.3.2021), S. 6.

2 Das Oktoberfestattentat wurde erst im Juli 2020 von der Generalbundesanwaltschaft als rechtsextrem eingestuft; die rechtsextreme Mordserie der Terrorgruppe „Nationalsozialistischer Untergrund" wurde von Verfassungsschutz und Polizei jahrelang als organisierte Kriminalität eingestuft.

3 Bundespräsidialamt, Rede Oktoberfestattentat, S. 7.

4 Einen allgemeinen Überblick über diese Phänomene bietet beispielsweise: Amadeu Antonio Stiftung, Alternative Wirklichkeiten, Monitoring rechts-alternativer Medienstrategien (https://www.amadeu-antonio-stiftung.de/wp-content/uploads/2020/01/Monitoring_2020_web.pdf, zuletzt abgerufen am 30.3.2021); im Übrigen wird auf die Ausführungen unter II.2.a), II.2.b) verwiesen.

5 BR-Drs. 339/20.

6 *Grumke*, in: Glaser/Pfeiffer, Erlebniswelt Rechtsextremismus, 3. Aufl. (2013), S. 24; *Virchow*, in: Virchow/Langebach/Häusler, Handbuch Rechtsextremismus, 2016, S. 17 ff.; *Wiacek*, Strafbarkeit rechts motivierter Cyberkriminalität in sozialen Netzwerken, 2019, S. 66.

7 *Birsl*, NPL 2016, 251 (254); *Salzborn*, Rechtsextremismus, 3. Aufl. (2018), S. 16 ff., 24; BMI, Verfassungsschutzbericht 2019, abrufbar unter: https://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/verfassungsschutzberichte/vsbericht-2019 (zuletzt abgerufen am 30.3.2021), S. 46.

die Degradierung anderer Nationalitäten bzw. Ethnien in Form von Nationalismus, Antisemitismus, Rassismus und Fremdenfeindlichkeit.[8]

Wie alle politischen Extremismen zielt der Rechtsextremismus auf die Abschaffung des demokratischen Verfassungsstaats, wobei zur Erreichung dieses Ziels auch der Einsatz von Gewalt akzeptiert wird.[9] Menschen mit einem rechtsextremen Weltbild lehnen den Wertepluralismus einer modernen Demokratie ab und stellen sich gegen die für die freiheitlich-demokratische Grundordnung[10] fundamentale Gleichheit aller Menschen.[11]

b) Straftaten mit Internetbezug – Cybercrime

Mit der rasanten Ausbreitung des Internets und seiner Entwicklung hin zum Web 2.0[12] ging das vermehrte Auftreten von Straftaten mit Internetbezug einher.[13] Deliktische Handlungsformen im Internet werden dabei unter dem Begriff *Cybercrime* zusammengefasst.

Zu unterscheiden ist zwischen Cybercrime im engeren Sinne und Cybercrime im weiteren Sinne. Cybercrime im engeren Sinne umfasst ausschließlich diejenigen Strafvorschriften, die bereits auf Tatbestandsebene Elemente der elektronischen Datenverarbeitung beinhalten, beispielsweise die §§ 202a, 263a StGB.[14] Im Gegensatz dazu lassen sich sämtliche Delikte, bei denen das Internet als Tatmittel zum Einsatz kommt, als Cybercrime im weiteren Sinne klassifizieren.[15]

c) Zusammenführung: Rechts motivierte Cyberkriminalität

Strafrechtlich relevante Handlungen im Internet, die aus rechtsextremer Überzeugung erfolgen, werden im Folgenden als *rechts motivierte Cyberkriminalität* bezeichnet.

Diese Bezeichnung ist an den Begriff der politisch motivierten Kriminalität-rechts (PMK-rechts) angelehnt, der von den deutschen Sicherheitsbehörden kollektiv verwendet wird.[16] Die PMK-rechts umfasst alle Delikte, bei denen in der Gesamtschau von einer „rechten" Motivationslage auszugehen ist, selbst wenn im Einzelfall nicht die Abschaffung der freiheitlich-demokratischen Grundordnung bezweckt wird.[17] Weil die Täter aber in nahezu allen Fällen der PMK-rechts aus extremistischen Beweggründen handeln,[18] kann die Bezeichnung *rechts motivierte Cyberkriminalität* gleichwohl synonym für strafrechtlich relevanten Rechtsextremismus im Internet verwendet werden.

---

8 *Dienstbühl*, Extremismus und Radikalisierung, 2019, S. 91; *Pfahl-Traughber*, in: Jesse/Mannewitz, Extremismusforschung, 2018, S. 303.

9 *Jesse*, NK 2017, 15 (17); BMI/BKA, Politisch motivierte Kriminalität im Jahr 2019, Bundesweite Fallzahlen, abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2020/pmk-2019.pdf?__blob=publicationFile&v=8 (zuletzt abgerufen am 30.3.2021), S. 12; *Neu/Pokorny*, in: Jesse/Mannewitz, S. 199; zum Gewaltbegriff *Salzborn*, S. 23 f.

10 Der Begriff der freiheitlich-demokratischen Grundordnung wurde maßgeblich durch das SRP-Urteil des *BVerfG* geprägt, vgl. BVerfGE 2, 1 (12).

11 *Jaschke*, Rechtsextremismus und Fremdenfeindlichkeit, 2. Aufl. (2001), S. 30; *Dienstbühl*, S. 94.

12 Von einem Web 2.0 spricht man, seit für Internetnutzer die Möglichkeit besteht, selbst die Inhalte des World Wide Web mitzubestimmen; elementare Bestandteile des Web 2.0 sind u.a. Soziale Netzwerke, Video- und Fotodienste sowie virtuelle Spielewelten; siehe hierzu *Ihwas*, Strafverfolgung in Sozialen Netzwerken, 2014, S. 34; *Salzborn/Maegerle*, ZfVP 2016, 213 (217).

13 Im Jahr 2018 wurden 87.106 Fälle von Cybercrime i.e.S. und 271.864 Fälle von Cybercrime i.w.S. im Hellfeld erfasst, vgl. BKA, Cybercrime, Bundeslagebild 2018, abrufbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2018.html?nn=28110 (zuletzt abgerufen am 30.3.2021), S. 6, 9.

14 *Wiacek*, S. 72 f.

15 *Wernert*, Internetkriminalität, 3. Aufl. (2017), S. 32; *Martin*, Kriminalistik 2015, 612 (613).

16 *Wiacek*, S. 62, 70.

17 Vgl. BT-Drs. 17/1928, S. 5; BT-Drs. 18/11970, S. 30.

18 Bei 21.290 der insgesamt erfassten 22.342 PMK-rechts Straftaten im Jahr 2019 handelte es sich um extremistische Taten; vgl. BMI, Politisch Motivierte Kriminalität im Jahr 2016, Bundesweite Fallzahlen, abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2017/pmk-2016.pdf?__blob=publicationFile&v=1 (zuletzt abgerufen am 30.3.2021), S. 2, 12.

Als Sammelbegriff umfasst rechts motivierte Cyberkriminalität sowohl Cybercrime im engeren als auch Cybercrime im weiteren Sinne. In der Praxis macht Letzteres den Großteil aller Fälle aus.[19]

2. Lagebericht: Rechts motivierte Cyberkriminalität in Deutschland

a) Hetze, Hass und Propaganda: Typische Erscheinungsformen von Rechtsextremismus im Internet

Schon früh entdeckte die rechtsextreme Szene das Internet für sich.[20] Seit 2010 sind es vor allem die sozialen Medien, in denen rechte Akteure sich vernetzen und an neue Zielgruppen wenden.[21] Insbesondere junge, charakterlich noch ungefestigte Nutzer sollen durch jugendgerechte Themen und subtil verpackte Propaganda mit rechtem Gedankengut in Kontakt gebracht werden,[22] ohne dass im virtuellen Raum eine soziale Kontrolle durch Familie oder Schule möglich ist.[23] Darüber hinaus sollen Anhänger rechter Ideologien in ihrem Weltbild bestärkt und für Veranstaltungen mobilisiert[24] sowie Gegner des Rechtsextremismus durch die scheinbare Übernahme der Meinungsführerschaft im digitalen Raum eingeschüchtert werden.[25] Infolge vermehrter Löschungen rechtswidriger Inhalte durch die Anbieter der großen sozialen Netzwerke[26] gewinnen private Chat-Gruppen bei internetbasierten Messenger-Diensten, insbesondere *Telegram*, zunehmend an Bedeutung.[27] Auch eine Abwanderung zum russischen sozialen Netzwerk *V-Kontakte* lässt sich beobachten.[28]
Die Schwerpunkte rechter Internetpräsenz lassen sich als Propaganda und Vernetzung, Rekrutierung und Mobilisierung sowie Bedrohung und Meinungsführerschaft zusammenfassen.[29] Nicht selten wird dabei gegen geltendes Recht verstoßen, wobei in der Praxis vor allem die Verbreitung von Hetzpropaganda und verfassungswidrigen Inhalten (§§ 86, 86a, 130, 131, 166 StGB), Beleidigungsdelikte (§§ 185 ff. StGB), Nötigung und Bedrohung (§§ 240, 241 StGB), straftatfördernde Delikte (§§ 111, 126, 130a, 140 StGB) sowie in Extremfällen Delikte gegen den Staat und seine Organe (§§ 89a ff., 129 Abs. 1, 129a Abs. 5 StGB) von Bedeutung sind.[30]

b) Rechts motivierte Cyberkriminalität in Zahlen

Der hohe Stellenwert, den das Internet für die Verbreitung rechtsextremen Gedankenguts und die Organisation innerhalb der rechten Szene mittlerweile einnimmt, spiegelt sich auch in den Fallzahlen verschiedener Statistiken wider.[31]

---

19 *Wiacek*, S. 74.
20 *Salzborn/Maegerle*, ZfVP 2016, 213 (221); *Pfeiffer*, in: Grevgen/Grumke, Globalisierter Rechtsextremismus, 2006, S. 160 ff.
21 *Dinar/Heyken*, in: Nerdinger, Nie wieder. Schon wieder. Immer noch. Rechtsextremismus in Deutschland seit 1945, 2017, S. 42.
22 *Fromm/Kernbach*, Rechtsextremismus im Internet, 2001, S. 16; zu rechtsextremer Präsenz und Propaganda auf Instagram jugendschutz.net, Rechtsextremismus im Netz, Bericht 2017, abrufbar unter: https://www.jugendschutz.net/fileadmin/download/pdf/Lagebericht_2017_Rechtsextremismus_im_Netz.pdf (zuletzt abgerufen am 30.3.2021), S. 14 f.
23 *Freter/Zimpelmann*, in: Beck/Meier/Momsen, Cybercrime und Cyberinvestigations, 2015, S. 120.
24 *Salzborn/Maegerle*, ZfVP 2016, 213 (216).
25 *Dinar/Heyken*, in: Nerdinger, S. 43.
26 Seit Oktober 2017 sind die Anbieter großer sozialer Netzwerke gem. § 3 Abs. 2 NetzDG zum Entfernen bzw. Sperren rechtswidriger Inhalte i.S.d. § 1 Abs. 3 NetzDG verpflichtet.
27 jugendschutz.net, Rechtsextremismus im Netz, Bericht 2018/2019, abrufbar unter: http://www.jugendschutz.net/fileadmin/download/pdf/Bericht_2018_2019_Rechtsextremismus_im_Netz.pdf (zuletzt abgerufen am 30.3.2021), S. 22.
28 jugendschutz.net, Rechtsextremismus im Netz, Bericht 2017, S. 18 f.; *Dinar/Heyken*, in: Nerdinger, S. 52: *Wiacek*, S. 52 ff.
29 *Dinar/Heyken*, in: Nerdinger, S. 43; vgl. auch BT-Drs. 19/11908, S. 7.
30 Ausführliche Erläuterungen zu den einzelnen Delikten und Erscheinungsformen bieten *Wiacek*, S. 110 ff. sowie *Martin*, Kriminalistik 2015, 612 (613 ff.).
31 Es existiert bis heute keine aussagekräftige Statistik, die sich spezifisch mit dem Phänomen rechts motivierter Cyberkriminalität auseinandersetzt; *Wiacek*, S. 75.

Wurden 1997 vom Bundesamt für Verfassungsschutz nur ca. 100 rechtsextreme deutsche Websites registriert, so waren es vier Jahre später schon ca. 1.300.[32] Im Jahr 2014 schließlich wurden von der gemeinnützigen, mit gesetzlichem Auftrag[33] handelnden Organisation *jugendschutz.net* über 6.000 rechtsextreme Angebote im Internet gesichtet, von denen ganze 70% auf Social-Media-Dienste zurückzuführen waren.[34] Dieser Anteil hat sich in den Folgejahren noch erhöht.[35] Besonders im Bereich der rechts motivierten Hasskriminalität durch das Tatmittel Internet (sog. Hasspostings) wurde in den Jahren 2014 bis 2016 ein enormer Zuwachs um ca. 284% registriert, wobei den öffentlich zugänglichen Fallzahlen der jährlichen PMK-Berichte leider keine detaillierte Aufschlüsselung hinsichtlich der verwirklichten Straftatbestände entnommen werden kann.[36] Aus den Berichten von *jugendschutz.net* geht jedoch hervor, dass in den Jahren 2018/2019 ca. 75% aller registrierten Delikte den Tatbestand des § 86a StGB oder des § 130 StGB verwirklichten.[37]

Bei all diesen Zahlen darf nicht vergessen werden, dass sie lediglich das polizeilich bekannte Hellfeld abbilden. Aufgrund der Tatsache, dass das Dunkelfeld bei Cyberkriminalität typischerweise außerordentlich groß ist,[38] dürften die tatsächlichen Fallzahlen um einiges höher liegen.

3. Zwischenergebnis

„*Dem Internet dürfte [...]in den nächsten Jahren bei der Verbreitung rechtsextremistischer Propaganda, aber auch bei der Koordination von Aktivitäten der rechtsextremistischen Szene eine erhebliche Bedeutung zukommen*.“[39] Diese Prognose des Bundesamts für Verfassungsschutz aus dem Jahr 1996 und damit aus einer Zeit, in der das Internet noch in den Kinderschuhen steckte, sollte sich in den folgenden Jahren in jeglicher Hinsicht bewahrheiten.

Es hat sich gezeigt, dass die erweiterten Partizipationsmöglichkeiten und basisdemokratisch anmutenden Meinungsbildungsprozesse des Internets für unsere Demokratie Fluch und Segen zugleich sein können. Rechtsextreme Aktivisten haben im Internet eine effektive Plattform zur Verbreitung ihrer Ideologien gefunden und schaffen es heute in bisher nie dagewesenem Ausmaß, in digitalen „Echokammern“[40] menschenverachtende Denkmuster zu verstärken und Anhänger zu radikalisieren.

Rechtsextremismus im Internet ist demnach alles andere als ein Randphänomen und lässt sich keineswegs als „alter Wein in neuen Schläuchen“ bezeichnen. Vielmehr stellen rechte Hetze und Propaganda im Netz aufgrund ihrer einschüchternden Wirkung eine nicht zu unterschätzende Gefahr für den offenen politischen Diskurs und die

---

32 BMI, Verfassungsschutzbericht 1997, abrufbar unter: https://verfassungsschutzberichte.de/pdfs/vsbericht-1997.pdf (zuletzt abgerufen am 30.3.2021), S. 80; Verfassungsschutzbericht 2001, abrufbar unter: https://publikationen.uni-tuebingen.de/xmlui/bitstream/handle/10900/62819/Verfassungsschutzbericht_2001.pdf (zuletzt abgerufen am 30.3.2021), S. 131.

33 § 18 JMStV.

34 jugendschutz.net, Rechtsextremismus online beobachten und nachhaltig bekämpfen, Bericht über Recherchen und Maßnahmen im Jahr 2014, abrufbar unter: https://www.hass-im-netz.info/fileadmin/public/main_domain/Dokumente/Rechtsextremismus/Rechtsextremismus_online_2014.pdf (zuletzt abgerufen am 30.3.2021), S. 13; in den Folgejahren erschienen die Berichte zu Rechtsextremismus im Internet leider nur lückenhaft und enthielten deutlich unpräzisere Angaben.

35 In den Jahren 2018/2019 wurde rechtsextreme Propaganda im Netz zu über 90% in den Social-Media-Diensten gesichtet; jugendschutz.net, Rechtsextremismus im Netz, Bericht 2018/2019, S. 26.

36 BMI, Politisch Motivierte Kriminalität im Jahr 2016, Bundesweite Fallzahlen, S. 5; *Wiacek*, S. 77; in den letzten drei Jahren sind die Fallzahlen deutlich gesunken, was möglicherweise mit der vermehrten Löschung rechtsextremer Inhalte durch die Anbieter sozialer Netzwerke gem. § 3 Abs. 2 NetzDG zusammenhängt (2019: 1.108 rechts motivierte Hasspostings; BMI/BKA, Politisch motivierte Kriminalität im Jahr 2019, Bundesweite Fallzahlen, S. 7).

37 jugendschutz.net, Rechtsextremismus im Netz, Bericht 2018/2019, S. 26.

38 *Eisenberg/Kölbel,* Kriminologie, 7. Aufl. (2017), S. 957; *Wiacek*, S. 77 f., 80; *Plank*, in: Rüdiger/Bayerl, Cyberkriminologie, 2020, S. 29.

39 BMI, Verfassungsschutzbericht 1996 (https://verfassungsschutzberichte.de/pdfs/vsbericht-1996.pdf, zuletzt abgerufen am 30.3.2021), S. 161.

40 jugendschutz.net, Rechtsextremismus im Netz, Bericht 2018/2019, S. 7, 23; *Dinar/Heyken*, in: Nerdinger, S. 52.

Meinungsfreiheit in unserer demokratischen und pluralistischen Gesellschaft dar.[41]

III. Möglichkeiten und Grenzen der Strafverfolgung rechts motivierter Cyberkriminalität

1. Zentrale Akteure

Grundvoraussetzungen einer effektiven Strafverfolgung rechts motivierter Cyberkriminalität sind eine enge Zusammenarbeit und ein umfangreicher Informationsaustausch zwischen dem BKA, den Landeskriminalämtern und den Staatsanwaltschaften.

Grundsätzlich liegt die Kompetenz für die Strafverfolgung bei den Ländern, Art. 83 GG. Dabei kommt der Staatsanwaltschaft, unterstützt durch ihre Ermittlungspersonen (§ 152 GVG), als „Herrin des Ermittlungsverfahrens“[42] eine zentrale Rolle zu. Um fachliche Expertise im Kampf gegen rechts motivierte Cyberkriminalität zu bündeln und eine schnellere Bearbeitung ähnlich gelagerter Fälle zu ermöglichen, kommt es inzwischen vermehrt zur Bildung von Schwerpunktstaatsanwaltschaften gem. § 143 Abs. 4 GVG, beispielsweise in Form einer *Schwerpunktstaatsanwaltschaft zur Bekämpfung von Hasskriminalität im Internet* in Göttingen.[43] Diese Schwerpunktstaatsanwaltschaft fungiert als Ansprechpartnerin für die im September 2019 gegründete *Zentralstelle zur polizeilichen Bekämpfung der Hasskriminalität* des LKA Niedersachsen.[44] Bei den meisten anderen Landeskriminalämtern existieren ebenfalls spezialisierte Organisationseinheiten zur Bekämpfung von PMK-rechts und Cyberkriminalität.[45] Zudem sichern die Landeskriminalämter als Ansprechpartner und Kooperationsstellen[46] für das BKA die Zusammenarbeit des Bundes und der Länder, § 1 Abs. 2 S. 1 BKG. Das geschieht beispielsweise im Rahmen der Informations- und Kommunikationsplattform *Gemeinsames Extremismus- und Terrorismusabwehrzentrum*.[47]

Das BKA als Zentralstelle gem. § 2 Abs. 1 BKAG unterstützt die Polizeien der Länder durch Service- und Koordinationstätigkeiten[48] sowie die Sammlung und Auswertung von Daten (§§ 2 Abs. 2 Nr. 1, 9 Abs. 1 BKAG). In naher Zukunft soll beim BKA eine *Zentralstelle zur Bekämpfung von Hasskriminalität* aufgebaut werden.[49]

2. Eingriffsrelevante Grundrechte

Bei der Strafverfolgung rechts motivierter Cyberkriminalität kommt es durch die teils heimlich erfolgende Erhebung, Sammlung, Speicherung und Auswertung von Daten zu unterschiedlich intensiven Eingriffen in die folgenden Grundrechte.

---

41 So auch BT-Drs. 19/17742, S. 1.

42 *Hussels*, Strafprozessrecht schnell erfasst, 4. Aufl. (2020), S. 38; *Ostendorf*, Strafprozessrecht, 3. Aufl. (2018), S. 76; vgl. *Heger/Pohlreich*, Strafprozessrecht, 2. Aufl. (2018), S. 96.

43 Nds. MBl. 25/2020, S. 563.

44 Zu Einrichtung und Zuständigkeitsbereich der Zentralstelle vgl. Niedersächsischer Landtag, Drs. 18/5388, S. 2 f. sowie Drs. 18/5555, S. 1 f.

45 Beim LKA NRW sind das beispielsweise die Abteilung 6 für „Staatsschutz und Ermittlungsunterstützung“, abrufbar unter: https://lka.polizei.nrw/artikel/abteilung-6; sowie das Cybercrime Kompetenzzentrum, abrufbar unter: https://polizei.nrw/artikel/das-cybercrime-kompetenzzentrum-beim-lka-nrw (beides zuletzt abgerufen am 30.3.2021).

46 *Engelhart*, Strafrechtspflege, 2019, S. 39 f.

47 *Frevel*, Innere Sicherheit, 2018, S. 92 f.

48 *BVerfG*, NJW 2020, 2699 (2718); *Graulich*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. (2019), § 2 BKAG Rn. 4; *Bäcker*, Stellungnahme zu dem Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (BT-Drs. 19/17741), abrufbar unter: https://kripoz.de/wp-content/uploads/2020/05/stellungnahme-baecker-hasskriminalitaet.pdf (zuletzt abgerufen am 30.3.2021), S. 4.

49 *Münch,* Kriminalistik 2020, 3 (5); derzeit existieren bereits eine „Koordinierte Internetauswertung Rechtsextremismus“ sowie die Informations- und Kommunikationsplattform „Gemeinsames Extremismus- und Terrorismusabwehrzentrum“ mit insgesamt 40 beteiligten Bundes- und Landesbehörden, darunter auch das BKA und die Landeskriminalämter.

a) Allgemeines Persönlichkeitsrecht

aa) Recht auf informationelle Selbstbestimmung

Werden im Zuge der Strafverfolgung Bestandsdaten[50] erhoben, liegt ein Eingriff in das *Recht auf informationelle Selbstbestimmung* vor.[51] Diese Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG schützt die Befugnis jedes einzelnen, selbst über die Preisgabe und Verwendung persönlicher Daten zu bestimmen.[52] Auf die Art und die Sensibilität der Daten kommt es dabei nicht an, weil durch die Möglichkeiten der elektronischen Datenverarbeitung auch scheinbar belanglose Daten so verknüpft bzw. verarbeitet werden können, dass sie tiefgreifende Einblicke in die private Lebensgestaltung ermöglichen.[53]

bb) Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Eine weitere eigenständige Ausformung des allgemeinen Persönlichkeitsrechts ist das umgangssprachlich als „Computergrundrecht“[54] bezeichnete *Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*.[55] Der Begriff des informationstechnischen Systems umfasst jedes hinreichend komplexe elektronische System, das der Verarbeitung von Informationen dient,[56] beispielsweise festinstallierte und tragbare PCs, Smartphones und das gesamte Internet.[57]

Die Online-Durchsuchung gem. § 100b StPO sowie die „kleine Online-Durchsuchung“ [58] gem. § 100a Abs. 1 S. 3 StPO stellen einen Eingriff in das Computergrundrecht dar.[59]

b) Fernmeldegeheimnis

Das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG umfasst die Übermittlung individueller Kommunikation durch unkörperliche Signale im Wege des Telekommunikationsverkehrs.[60] Es handelt sich um ein entwicklungsoffenes Auffanggrundrecht,[61] das unabhängig von der Ausdrucksform jegliche Übermittlungsart der Telekommunikation (also auch die Kommunikation über das Internet) vor einem Zugriff Dritter schützt.[62] Sowohl die Kommunikationsinhalte als auch die Umstände des Kommunikationsvorgangs unterfallen dem Schutz des Fernmeldegeheimnisses,[63] weshalb neben der (Quellen-)Telekommunikationsüberwachung[64] auch die Erhebung von Verkehrs-[65]

---

50 Dazu III.3.b).bb).
51 BVerfGE 130, 151 (184); *Bauer*, Soziale Netzwerke und strafprozessuale Ermittlungen, 2018, S. 335; *Grün*, Verdeckte Ermittlungen, 2018, S. 96; *Greco*, in: SK-StPO, 5. Aufl. (2016), § 100j Rn. 3.
52 BVerfGE 65, 1 (43); 84, 192 (194); 120, 274 (312); *Di Fabio*, in: Maunz/Dürig, GG, 90. EL. (2020), Art. 2 Abs. 1 Rn. 175; *von Münch/Mager*, Staatsrecht II: Grundrechte, 7. Aufl. (2018), S. 112; *Michael/Morlok*, Grundrechte, 7. Aufl. (2020), S. 221.
53 BVerfGE 65, 1 (45) stellt klar, dass es unter den Bedingungen der elektronischen Datenverarbeitung „kein belangloses Datum“ mehr gibt.
54 Vgl. *Ipsen*, Grundrechte, 23. Aufl. (2020), S. 90; *Horn*, in: Stern/Becker, Grundrechte Kommentar, 3. Aufl. (2019), Art. 2 Rn. 51; *Bäcker*, in: Rensen/Brink, Linien der Rechtsprechung, Band 1, 2009, S. 133; teilweise wird auch die Bezeichnung „IT-Grundrecht“ verwendet, vgl. ebd., S. 118.
55 Dieses Grundrecht wurde 2007 vom *BVerfG* in seinem Urteil zur Online-Durchsuchung aus Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG abgeleitet; BVerfGE 120, 274 (302 ff.).
56 *Ihwas*, S. 91 f. sowie *Bäcker*, in: Rensen/Brink, S. 126 f.
57 BVerfGE 120, 274 (276, 314).
58 *Hauck*, in: LR-StPO, 27. Aufl. (2019), § 100a Rn. 140.
59 *Bruns*, in: KK-StPO, 8. Aufl. (2019), § 100b Rn. 2; *Hauck*, in: LR-StPO, § 100a Rn. 146.
60 BVerfGE 120, 274 (306 f.); *Ipsen*, S. 83; *Ogorek*, in: BeckOK-GG, 44. Ed. (2020), Art. 10 Rn. 37.
61 *Durner*, in: Maunz/Dürig, GG, Art. 10 Rn. 82; *Guckelberger*, in: Hofmann/Henneke, GG, 14. Aufl. (2017), Art. 10 Rn. 21; *Ihwas*, S. 97.
62 BVerfGE 120, 274 (307); 124, 43 (54); *Schenke*, in: Stern/Becker, Art. 10 Rn. 45; *Guckelberger*, in: Maunz/Dürig, Art. 10 Rn. 22.
63 *Epping*, Grundrechte, 8. Aufl. (2019), S. 356; *von Münch/Mager*, S. 118; *Schenke*, in: Stern/Becker, Art. 10 Rn. 21.
64 *Köhler*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl. (2020), § 100a Rn. 1; *Eschelbach*, in: SSW-StPO, 4. Aufl. (2020), § 100a Rn. 2; *Bruns*, in: KK-StPO, § 100a Rn. 2; dazu III.3.c).
65 Dazu III.3.b).cc).

und Nutzungsdaten[66] einen Eingriff in Art. 10 Abs. 1 GG darstellt.[67]

3. Ermittlungen im Internet

a) Rechtsgrundlagen für einen Zugriff auf öffentlich und nichtöffentlich zugängliche Daten

aa) Der Zugriff auf öffentlich zugängliche Daten

(1) Recherchen im Internet

Zur Aufklärung von Straftaten im digitalen Raum führen verschiedene Polizeibehörden schon seit Längerem Recherchen im Internet durch,[68] die in Anlehnung an die analoge Welt gerne als „Online-Streife"[69] bezeichnet werden. Diese Bezeichnung ist jedoch nur zutreffend, solange es sich um eine verdachtsunabhängige Suche nach strafbaren Inhalten handelt, die – wie eine „echte Streife" – dem präventiven polizeilichen Aufgabenbereich der Gefahrenabwehr unterfällt und sich auf eine Befugnisnorm der Landespolizeigesetze oder des BKAG stützt.[70] Liegt hingegen ein Anfangsverdacht i.S.d. § 152 Abs. 2 StPO vor und richtet sich die Recherche gegen eine bestimmte, nicht notwendigerweise namentlich bekannte Person, dient die sodann repressive Maßnahme der Strafverfolgung und kann zumeist auf die Ermittlungsgeneralklausel gem. §§ 161, 163 StPO gestützt werden.[71]

(2) Anwendungsbereich der Ermittlungsgeneralklausel

Die Ermittlungsgeneralklausel gem. §§ 161, 163 StPO ist immer dann taugliche Rechtsgrundlage, wenn eine Ermittlungsmaßnahme mit keinem oder einem lediglich geringfügigen Grundrechtseingriff verbunden ist und nicht auf eine spezielle Eingriffsermächtigung gestützt werden kann.[72] Das ist im Kontext der anlassbezogenen Internetrecherche der Fall, solange ausschließlich auf öffentlich zugängliche Informationen zurückgegriffen wird.[73] Unter öffentlich zugänglichen Informationen sind dabei nicht nur Webseiten ohne Zugangssicherung, sondern auch jedermann offenstehende Mailinglisten sowie nicht zugangsgeschützte Chats zu verstehen.[74] Die §§ 161, 163 StPO reichen selbst dann als Rechtsgrundlage aus, wenn öffentlich zugängliche Daten gezielt zusammengetragen und ausgewertet werden.[75]

---

66 Dazu III.3.b).dd).

67 Zu Verkehrsdaten: *Hauck*, in: LR-StPO, § 100g Rn. 8; *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl. (2018), S. 766; *Bruns*, in: KK-StPO, § 100a Rn. 2; zu Nutzungsdaten: *Ihwas*, S. 245; *Karg*, DuD 2015, 85 (85 f.).

68 Im Jahr 1999 wurde eine „Zentralstelle für anlassunabhängige Recherche in Datennetzen" (ZArD) beim BKA eingerichtet; vgl. *Graulich*, in: Schenke/Graulich/Ruthig, § 2 BKAG Rn. 23 sowie *Zöller*, GA 2000, 563 (567); heute ist die „Koordinierte Internetauswertung Rechtsextremismus" (KIA-R) für anlassunabhängige sowie anlassbezogene Internet-Recherchen zu Sachverhalten mit rechtsextremistischen Bezügen zuständig; vgl. BT-Drs. 19/3552, S. 2.

69 So beispielsweise *Singelnstein*, NStZ 2012, 593 (600) sowie *Keller/Braun*, Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen, 3. Aufl. (2019), S. 87; andere sprechen von „virtuellen Streifenfahrten"; *Eisenmenger*, Die Grundrechtsrelevanz „virtueller Streifenfahrten", 2017, S. 21 sowie *Malek/Popp*, Strafsachen im Internet, 2. Aufl. (2015), S. 137 f. m.w.N.

70 *Keller*, Basislehrbuch Kriminalistik, 2019, S. 730 f.; *Dalby*, Grundlagen der Strafverfolgung im Internet und in der Cloud, 2016, S. 42 f.; *Ziegler*, in: SSW-StPO, § 163 Rn. 30; so auch schon *Zöller*, GA 2000, 563 (570 f.); vgl. *Bauer*, S. 99; das BKA kann im Rahmen seiner Zentralstellenaufgabe sowohl präventiv als aus repressiv tätig werden, § 2 Abs. 1 BKAG.

71 *Bauer*, S. 146; *ders.* verwendet für anlassbezogene Recherchen im Internet den Begriff der „repressiven Online-Streife"; *Ziegler*, in: SSW-StPO, § 163 Rn. 30; *Dalby*, S. 43 f.

72 *BVerfG*, NJW 2009, 1405 (1407); *Köhler*, in: Meyer-Goßner/Schmitt, StPO, § 161 Rn. 1; *Rückert*, ZStW 2017, 302 (319); *Erb*, in: LR-StPO, § 161 Rn. 44; *Sackreuther*, in: BeckOK-StPO, 37. Ed. (2020), § 161 Rn. 11; *Noltensmeier-von Osten*, in: KMR-StPO, 98. EL. (2020), § 161 Rn. 21; *Kochheim*, S. 724.

73 BVerfGE 120, 274 (344 f.); *Ihwas*, S. 117; *Kochheim*, S. 729; *Grün*, S. 47; *Zöller*, in: HK-StPO, 6. Aufl. (2019), § 163 Rn. 12; *Köhler*, in: Meyer-Goßner/Schmitt, StPO, § 100a Rn. 7.

74 BVerfGE 120, 274 (345).

75 BVerfGE 120, 274 (345); *Singelnstein*, NStZ 2012, 593 (600); *Kölbel*, in: MüKo-StPO, 2016, § 161 Rn. 11; *Müller*, Kriminalistik 2012, 295 (296); *Griesbaum*, in: KK-StPO, § 161 Rn. 12a.

bb) Der Zugriff auf nichtöffentlich zugängliche Daten

Für eine Identifizierung der Urheber strafbarer rechtsextremer Inhalte und die Sammlung von Daten zu Beweiszwecken sind die Ermittler jedoch häufig auf nichtöffentlich zugängliche Daten – namentlich Bestands-, Verkehrs- und Nutzungsdaten – angewiesen, die bei den Diensteanbietern gespeichert sind.

Dass viele dieser Daten auf ausländischen Servern liegen, stellt in der Praxis unter Umständen ein unüberwindbares Hindernis dar,[76] welches im Folgenden aber ausgeklammert werden soll.

(1) Abgrenzung: Telekommunikationsdienste und Telemediendienste

Die Wahl der Rechtsgrundlage für den Datenzugriff hängt davon ab, ob es sich im konkreten Fall um den Anbieter eines Telekommunikationsdienstes oder eines Telemediendienstes handelt.

Telekommunikationsdienste im Sinne des TKG bestehen ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze (§ 3 Nr. 24 TKG). Im Gegensatz dazu kommt es bei Telemediendiensten im Sinne des TMG – vereinfacht dargestellt – auf inhaltsbezogene Interaktionen an.[77] Soziale Netzwerke wie *Facebook* oder *Instagram* stellen bei einer Schwerpunktbetrachtung Telemediendienste im Sinne des TMG dar.[78] Ob die von der rechten Szene intensiv genutzten internetbasierten Messenger-Dienste als sogenannte Over-the-Top-Kommunikationsdienste (OTT-Kommunikationsdienste)[79] dem TKG oder dem TMG unterfallen, war lange Zeit umstritten.[80] Richtigerweise muss ein Urteil des *EuGH* aus dem Jahr 2019[81] so verstanden werden, dass OTT-Kommunikationsdienste bei unionsrechtskonformer, enger Auslegung des Begriffs der Telekommunikation nach deutschem Recht in der Regel als Telemediendienste einzustufen sind.[82]

Aus einem gemeinsamen Eckpunktepapier des BMWi und BMVI geht hervor, dass im Zuge der Umsetzung der EECC-Richtlinie[83] der Begriff des Telekommunikationsdienstes zukünftig auch „nummernunabhängige interpersonelle Kommunikationsdienste" – und damit internetbasierte Messenger-Dienste – umfassen soll.[84] Weil aber bis zu einer Umsetzung dieser Richtlinie die zentralen Schauplätze rechtsextremer Internetaktivität, nämlich soziale Netzwerke und internetbasierte Messenger-Dienste, nach deutschem Recht als Telemediendienste einzuordnen sind, beschränken sich die folgenden Ausführungen auf den Datenzugriff bei Telemediendiensteanbietern. Es wird diskutiert, auf welcher Rechtsgrundlage Auskunft über Bestands-, Verkehrs- und Nutzungsdaten verlangt werden kann. Rechtlich möglich wäre zudem eine Beschlagnahme von Daten nach den §§ 94 ff. StPO,[85] welche jedoch nicht Gegenstand der folgenden Ausführungen sein soll.

---

76 *Bauer*, S. 61; *Blechschmitt*, MMR 2018, 361 (364); *Grün*, S. 52; vgl. *Graf*, in: BeckOK-StPO, § 100a Rn. 243 ff.; ausführlich zu einzelnen Ermittlungsbefugnissen *Bär*, in: Wabnitz/Janovsky, Handbuch Wirtschafts- und Steuerstrafrecht, 5. Aufl. (2020), 28. Kapitel Rn. 140 ff.

77 *Grün*, S. 101; vertiefend *Spindler*, in: Spindler/Schmitz/Liesching, TMG mit NetzDG, 2. Aufl. (2018), § 1 TMG Rn. 18; § 1 Abs. 1 TMG enthält eine negative Generalklausel, wonach es sich bei allen elektronischen Informations- und Kommunikationsdiensten, die nicht Telekommunikationsdienste, telekommunikationsgestützte Dienste oder Rundfunk sind, um Telemedien handelt.

78 *Bauer*, S. 336; *Ihwas*, S. 175; ausführlich *Spindler*, in: Spindler/Schmitz/Liesching, § 2 TMG Rn. 23; vgl. auch § 1 Abs. 1 NetzDG.

79 Beispiele für OTT-Kommunikationsdienste sind *Gmail*, *WhatsApp*, *Telegram* und *Facebook Messenger*; vgl. *Kühling/Schall*, CR 2015, 641 (642).

80 *Spindler*, in: Spindler/Schmitz/Liesching, § 1 TMG Rn. 26; *Bär*, in: KMR-StPO, Vorb. zu § 100a-100j Rn. 57; für eine Einordnung unter das TKG exemplarisch *Kühling/Schall*, CR 2015, 641 (645 ff.) sowie *Bulowski*, Regulierung von Internetkommunikationsdiensten, 2019, S. 89; für eine Einordnung unter das TMG exemplarisch *Schuster*, CR 2016, 173 (173 ff.).

81 *EuGH*, Urt. v. 13.6.2019, C-193/18.

82 BT-Drs. 19/17741, S. 38; *Spies,* MMR 2019, 514 (517); *Bäcker*, Stellungnahme zu dem Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität, S. 9; *Kiparski*, CR 2019, 460 (463).

83 Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11.12.2018 über den europäischen Kodex für die elektronische Kommunikation, ABl 2018 L 321/36.

84 BMWi/BMVI, Eckpunkte zur TKG-Novelle 2019, abrufbar unter: https://cdn.netzpolitik.org/wp-upload/2019/05/bmwi-bmvi_eckpunktepapier-tkg-novelle-2019.pdf (zuletzt abgerufen am 30.3.2021), S. 2 f.; dazu *Bäcker*, Stellungnahme zu dem Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität, S. 9 f.

85 *Menges*, in: LR-StPO, § 94 Rn. 14; *Gerhold*, in: Graf, Strafprozessordnung mit Gerichtsverfassungsgesetz und Nebengesetzen, 3. Aufl. (2018), § 94 Rn. 4.

(2) Auskunft über Bestandsdaten

§ 14 Abs. 1 TMG definiert Bestandsdaten als personenbezogene Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer von Telemedien erhoben werden. Dazu zählen typischerweise Name, E-Mail-Adresse, Geburtsdatum und Passwort,[86] weshalb Bestandsdaten für die Identifizierung eines Nutzers von großer Bedeutung sein können.

Die Herausgabe von Bestandsdaten für Zwecke der Strafverfolgung ist in § 14 Abs. 2 TMG geregelt. § 14 Abs. 2 TMG stellt aber lediglich eine Öffnungsklausel dar.[87] Nach der Rechtsprechung des *BVerfG* braucht es korrespondierend zu dieser Übermittlungsnorm (erste Tür) eine spezialgesetzliche Ermächtigungsgrundlage zum Datenabruf (zweite Tür, sog. *Doppeltürmodell*).[88]

Eine solche könnte § 100j StPO darstellen, der seinem Wortlaut nach jedoch ausschließlich auf die Bestandsdatenauskunft bei Anbietern von Telekommunikationsdiensten anwendbar ist und deshalb als Abrufnorm nicht in Frage kommt.[89] Auch § 10 Abs. 1 S. 1 Nr. 1 BKAG, der das BKA als Zentralstelle zur Auskunft über Bestandsdaten berechtigt, bezieht sich auf Telekommunikations-Bestandsdaten und wurde zudem im Mai 2020 vom *BVerfG* für verfassungswidrig erklärt.[90]

Mangels einer speziellen Ermächtigungsgrundlage in der StPO wird überwiegend auf die Ermittlungsgeneralklausel zurückgegriffen.[91] Das ist zulässig, weil mit der Bestandsdatenauskunft ein nur geringfügiger Grundrechtseingriff[92] verbunden ist. Allerdings begründen weder § 14 Abs. 2 TMG noch die Ermittlungsgeneralklausel eine Verpflichtung der Diensteanbieter zur Datenherausgabe,[93] was sowohl Ermittler als auch Diensteanbieter mit erheblicher Rechtsunsicherheit konfrontiert.

Es bleibt die Möglichkeit einer Beschlagnahme von Bestandsdaten beim Diensteanbieter nach §§ 94, 95 StPO.[94] Die dadurch erlangten Daten befähigen die Ermittler jedoch nicht zur Identifizierung verdächtiger Nutzer anhand einer bekannten IP-Adresse,[95] was in der Praxis oft den einzigen Ermittlungsansatz darstellt.[96] Eine solche Personenauskunft anhand dynamischer IP-Adressen kann unter Berücksichtigung der ersten Entscheidung des *BVerfG* zur Bestandsdatenauskunft auch nicht auf die Ermittlungsgeneralklausel gestützt werden,[97] was die Schaffung einer expliziten strafprozessualen Abrufbefugnis erforderlich macht.

(3) Auskunft über Verkehrsdaten

Bei Verkehrsdaten handelt es sich gem. § 30 Nr. 30 TKG um diejenigen Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Dazu zählen auch IP-Adressen,[98] die zwar

---

86 *Ihwas*, S. 178; *Bauer*, MMR 2008, 435 (435 f.).

87 *Schmitz*, in: Spindler/Schmitz/Liesching, § 14 TMG Rn. 34; *Bär*, in: Wabnitz/Janovsky/Schmitt, Handbuch Wirtschafts- und Steuerstrafrecht, 5. Aufl. (2020), 28. Kapitel Rn. 115.

88 BVerfGE 130, 151 (184); *Hauck*, in: LR-StPO, § 100j Rn. 1; *Bruns*, in: KK-StPO, § 100j Rn. 1; *Eckhardt*, in: Geppert/Schütz, TKG, 4. Aufl. (2013), § 113 Rn. 12 ff.; *Wicker*, MMR 2014, 298 (298 f.).

89 *Bär*, in: BeckOK-StPO; § 100g Rn. 26; *Bauer*, S. 338; *Bär*, in: Wabnitz/Janovsky/Schmitt, 28. Kapitel Rn. 115.

90 *BVerfG*, NJW 2020, 2699 (2718).

91 *Grün*, S. 101; *Bär*, MMR 2013, 700 (702); *Bruns*, in: KK-StPO, § 100a Rn. 14; *Eisenberg*, Beweisrecht der StPO, 10. Aufl. (2017), Rn. 2480 Fn. 430; *Ihwas*, S. 183; bzgl. Zugangsdaten *Wicker*, MMR 2014, 298 (302); a.A. *Bauer*, S. 338 ff., der auf S. 342 ff. einen Gesetzgebungsvorschlag unterbreitet.

92 *Ihwas*, S. 178; *Bär*, in: Wabnitz/Janovsky/Schmitt, 28. Kapitel Rn. 115; *Graf*, in: BeckOK-StPO, § 100j Rn. 11; *Bauer*, S. 340 nimmt davon aber Zugangsdaten aus, weil deren Abruf eine deutlich höhere Eingriffsintensität aufweist.

93 *Bauer*, S. 341; *Ihwas*, S. 179; *Weßlau/Deiters*, in: SK-StPO, § 161 Rn. 13.

94 *Menges*, in: LR-StPO, § 94 Rn. 14; *Gerhold*, in: Graf-StPO, § 94 Rn. 4; *Schmitz*, in: Spindler/Schmitz/Liesching, § 14 TMG Rn. 36.

95 Dafür wäre als Zwischenschritt ein Rückgriff auf Verkehrsdaten erforderlich, vgl. *BVerfG* NJW 2012, 1419 (1422); *Graf*, in: BeckOK-StPO, § 100j Rn. 3.

96 *Keller/Braun*, S. 73.

97 Eine identifizierende Zuordnung dynamischer IP-Adressen erfordert nach Ansicht des *BVerfG* eine hinreichend klare Entscheidung des Gesetzgebers über Zulässigkeit und Voraussetzungen dieses Ermittlungsmaßnahme; vgl. *BVerfG,* NJW 2012, 1419 (1428 f.); eine solche Entscheidung kann den §§ 161, 163 StPO nicht entnommen werden.

98 *BGH,* NJW 2011, 1509 (1511); *Bruns*, in: KK-StPO, § 100a Rn. 10; *Braun*, in: Geppert/Schütz, § 96 Rn. 7.

keinen Rückschluss auf den konkreten Täter erlauben, aber zumindest Auskunft über den verwendeten Anschluss geben und deshalb für die Ermittlung des Täters gleichwohl von großer Bedeutung sind.[99]

Bisher wurde ein Auskunftsverlangen bei Anbietern von Telemedien, deren Dienstleistung zumindest auch in der Übermittlung von Signalen besteht und die in dieser Hinsicht als Telekommunikationsdienst tätig werden, als Erhebung von Verkehrsdaten auf § 100g Abs. 1 StPO i.V.m. § 96 TKG gestützt.[100] Allerdings geht aus dem bereits angesprochenen Urteil des *EuGH* hervor, dass internetbasierte Dienste, die selbst keinen Internetzugang vermitteln, nicht „ganz oder überwiegend in der Übertragung von Signalen [...] bestehen" und deshalb keine Telekommunikationsdienste i.S.d. § 3 Nr. 22 TKG darstellen.[101] Unter Berücksichtigung dieses Urteils scheidet – zumindest nach Ansicht des Gesetzgebers – eine auf § 100g Abs. 1 StPO i.V.m. § 96 Abs. 1 TKG gestützte Erhebung von Verkehrsdaten bei Telemediendiensten, die lediglich funktional ein Äquivalent zu Telekommunikationsdiensten darstellen, aus.[102]

Einen anderen Weg geht das *LG München I*, das die Erhebung von Verkehrsdaten bei einem internetbasierten E-Mail-Dienst auch weiterhin auf §§ 100g i.V.m. 101a Abs. 1, 100a Abs. 4 StPO stützen will.[103] Das Gericht stellt maßgeblich darauf ab, dass eine Herausgabepflicht nach dem Wortlaut des § 100a Abs. 4 StPO auch für diejenigen Anbieter besteht, die an der Erbringung von Telekommunikationsdiensten nur mitwirken.[104] Ob dieses Vorgehen mit der Rechtsprechung des *EuGH* vereinbar ist, kann im Hinblick auf eine baldige Änderung der Gesetzeslage[105] dahinstehen.

(4) Auskunft über Nutzungsdaten

Der Begriff der Nutzungsdaten findet ausschließlich im Telemedienrecht Verwendung. Nutzungsdaten sind gem. § 15 Abs. 1 TMG diejenigen personenbezogenen Daten, die erforderlich sind, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (z.B. IP-Adressen). Sie ähneln vor allem den Verkehrsdaten, weisen aber auch Bezüge zu den Inhaltsdaten auf.[106]

Etwas versteckt enthält §§ 15 Abs. 5 S. 4 i.V.m. 14 Abs. 2 TMG eine Öffnungsklausel für den Zugriff auf Nutzungsdaten.[107] In der StPO findet sich bisher allerdings keine korrespondierende Abrufnorm. Die Praxis stützt einen Zugriff auf Nutzungsdaten deshalb auf §§ 161, 163 StPO,[108] was nach einem Beschluss des *BVerfG* zur Herausgabe einer IP-Adresse zumindest nicht „in jedem Fall unzulässig" sein soll.[109]

Eine Erhebung von Nutzungsdaten auf Grundlage der Ermittlungsgeneralklausel kann jedenfalls keine zwangsbewehrte Herausgabepflicht der Anbieter nach sich ziehen.[110] Um der daraus resultierenden Rechtsunsicherheit zu begegnen, und weil der Zugriff auf Nutzungsdaten wegen deren Nähe zu den Inhaltsdaten in vielen Fällen eine

---

99 *Braun*, in: Geppert/Schütz, § 96 Rn. 7; *Rottmeier/Faber*, MMR 2020, 336 (340).

100 BT-Drs. 19/17741, S. 37 f.; *Ihwas*, S. 232, 239; *Bauer*, S. 346 f., 349; § 100g Abs. 2 StPO, der eine Erhebung der nach § 113b TKG gespeicherten Vorratsdaten regelt, ist wegen unpassender Katalogtaten für die Strafverfolgung von Rechtsextremismus im Internet nicht relevant; zudem ist die Speicherpflicht der Anbieter derzeit faktisch ausgesetzt, vgl. *OVG Münster*, Beschl. v. 22.6.2017 – Az. 13 B 238/17.

101 Vgl. *EuGH*, Urt. v. 13.6.2019, C-193/18, Rn. 41.

102 BT-Drs. 19/17741, S. 38.

103 *LG München I*, MMR 2020, 336 (336).

104 A.a.O., 337.

105 Dazu III.4.

106 *Graf*, in: BeckOK-StPO, § 100a Rn. 40; *Ihwas*, S. 241 f.

107 *Schmitz*, in: Spindler/Schmitz/Liesching, § 14 TMG Rn. 34.; *Ihwas*, S. 243; *Bauer*, S. 357; *Bär*, in: BeckOK-StPO, § 100g Rn. 26.

108 *Ihwas*, S. 245 ff.; *Graf*, in: BeckOK-StPO, § 100j Rn. 10; *Bär*, in: KMR-StPO, Vorb. zu §§ 100a-100j Rn. 62; *ders.*, MMR 2013, 700 (702); *Eisenberg*, Rn. 2480 Fn. 430; a.A. *Schmitz*, in: Spindler/Schmitz/Liesching, § 14 TMG Rn. 38, der § 100a StPO als taugliche Rechtsgrundlage ansieht; *Karg*, DuD 2015, 85 (87 f.) kann der StPO keine geeignete Ermächtigungsgrundlage für den heimlichen Zugriff auf Nutzungsdaten entnehmen.

109 *BVerfG*, Beschl. v. 13.11.2010 – 2 BvR 1124/10, Rn. 22.

110 *Bauer*, S. 358; *Ihwas*, S. 246; *Weßlau/Deiters*, in: SK-StPO, § 161 Rn. 13.

erhöhte Eingriffsintensität aufweist,[111] ist die Schaffung einer speziellen Rechtsgrundlage mit begrenzenden Eingriffsschwellen wünschenswert.

b) Verdeckte personale Ermittlungen in sozialen Netzwerken

Die sozialen Netzwerke präsentieren sich den Strafverfolgungsbehörden als „wahre Fundgruben für Ermittlungs- und Fahndungszwecke".[112] Der vollumfängliche Zugriff auf diese „Fundgruben" setzt eine Registrierung sowie das Anlegen eines Profils voraus. Für einen erfolgreichen Ausgang der Ermittlungen kann es zudem erforderlich sein, dass Polizeibeamte sich unter fingierten digitalen Identitäten an Diskussionsforen beteiligen und Kontakt zu verdächtigen Personen aufnehmen. Solche legendierten Online-Auftritte erfolgen, abhängig von der Intensität des damit einhergehenden Grundrechtseingriffs, entweder in der Rolle des virtuellen nicht offen ermittelnden Polizeibeamten[113] (virtueller noeP) auf Grundlage der §§ 161, 163 StPO[114] oder als virtueller verdeckter Ermittler (virtueller VE).[115]

Für die Abgrenzung zwischen virtuellem noeP und virtuellem VE kann auf das Urteil des *BVerfG* zur Online-Durchsuchung[116] Bezug genommen werden. Darin führt das Gericht aus, dass im Internet selbst bei Aufnahme von Kommunikationsbeziehungen über einen längeren Zeitraum ein Eingriff in das Recht auf informationelle Selbstbestimmung nur dann gegeben ist, wenn sich beim Betroffenen schutzwürdiges Vertrauen in die Identität des Kommunikationspartners gebildet hat und dieses Vertrauen von den Strafverfolgungsbehörden ausgenutzt wird.[117] Allerdings entsteht schutzwürdiges Vertrauen in die Identität des „digitalen Gegenübers" aufgrund der Anonymität und geringeren Verbindlichkeit im Internet sowie in Ermangelung hinreichender Überprüfungsmechanismen nur in Ausnahmefällen.[118] Mangels Grundrechtseingriff kann deshalb der Großteil der verdeckten personalen Ermittlungsmaßnahmen in sozialen Netzwerken als Einsatz eines virtuellen noeP auf die Ermittlungsgeneralklausel gestützt werden.[119]

Unter welchen Voraussetzungen im Einzelfall schutzwürdiges Vertrauen entstehen kann und den Einsatz eines virtuellen VE erforderlich macht, ist umstritten. Oft wird eine Gesamtbetrachtung unter Berücksichtigung der Intensität der Zugangskontrolle, der Ausschöpfung der Möglichkeiten zum Identitätsmanagement bei der Profilgestaltung, des Grades der Beteiligung an der Kommunikation sowie der Dauer der legendierten Ermittlungen vorgenommen.[120] Unklar ist auch, ob der Einsatz eines virtuellen VE – wie vom BKA praktiziert[121] – auf die

---

111 *Karg*, DuD 2015, 85 (86); *Dix/Schaar*, in: Roßnagel, Recht der Telemediendienste, 2013, § 15 TMG Rn. 23, 25.

112 *Henrichs/Wilhelm*, Kriminalistik 2010, 30 (32).

113 Als noeP bezeichnet man Beamte des Polizeidienstes, die nur gelegentlich verdeckt auftreten und deren Ermittlungsauftrag auf einzelne Ermittlungshandlungen beschränkt ist; vgl. *Engländer*, Examens-Repetitorium Strafprozessrecht, 10. Aufl. (2020), S. 62 sowie *Keller/Braun*, S. 136.

114 *Müller*, Kriminalistik 2012, 295 (296); *Ziegler*, in: SSW-StPO, § 163 Rn. 30; *Köhler*, in: Meyer-Goßner/Schmitt, StPO, § 110a Rn. 4; *Soiné*, NStZ 2014, 248 (251); *Keller/Braun*, S. 95; so im Ergebnis auch *Dalby*, S. 54.

115 § 110a Abs. 2 StPO definiert den „regulären" VE als Beamten des Polizeidienstes, der unter einer auf Dauer angelegten, veränderten Identität (Legende) ermittelt und unter dieser Legende auch am Rechtsverkehr teilnehmen darf.

116 BVerfGE 120, 274; dabei hat das Urteil zwar grundsätzlich das Amt für Verfassungsschutz in Nordrhein-Westfalen zum Gegenstand, jedoch spricht das *BVerfG* im relevanten Abschnitt (344 ff.) meist allgemein von „Behörden" oder „staatlichen Stellen", weshalb die Ausführungen zu den Befugnissen einer Behörde bei Ermittlungsmaßnahmen im Internet auf die Strafverfolgungsbehörden übertragen werden können; vgl. *Ihwas*, S. 83 ff.

117 Vgl. BVerfGE 120, 274 (345 f.).

118 BVerfGE 120, 274 (345 f.); *Griesbaum*, in: KK-StPO, § 161 Rn. 12a; *Graf*, in: Graf-StPO, § 100a Rn. 86; vgl. *Soiné*, NStZ 2014, 248 (249); krit. *Singelnstein*, NStZ 2012, 593 (600); *Eisenmenger*, S. 155 ff. weist auf den keineswegs anonymen Charakter der sozialen Netzwerke hin.

119 *Rosengarten/Römer*, NJW 2012, 1764 (1767); *Soiné*, NStZ 2014, 248 (249 f.); *Bruns*, in: KK-StPO, § 110a Rn. 7; a.A. *Drackert*, eucrim 2011, 122 (125 f.), wonach die Generalermittlungsklausel verdeckte personale Ermittlungen in sozialen Netzwerken nicht zu rechtfertigen vermag, weil deren Inhalte weitgehende und präzise Rückschlüsse auf die Persönlichkeit der Nutzer zulassen.

120 Einen guten Überblick über die verschiedenen Ansichten bieten *Ihwas*, S. 145 ff. sowie *Rosengarten/Römer*, NJW 2012, 1764 (1766 f.); ähnliche Kriterien nennen auch *Bruns*, KK-StPO, § 110a Rn. 7 und *Dalby*, S. 53.

121 BT-Drs. 17/6587, S. 5.

§§ 110a ff. StPO gestützt werden kann.[122] Ohnehin wird der virtuelle VE selbst bei entsprechender Anwendung der §§ 110a ff. StPO für die Strafverfolgung rechts motivierter Cyberkriminalität nur selten von Nutzen sein: Die Katalogtaten des § 110a Abs. 1 S. 1 StPO sind auf die Bekämpfung der Organisierten Kriminalität (insbes. Drogenkriminalität) zugeschnitten und bilden nicht die im Kontext rechts motivierter Cyberkriminalität typischerweise verwirklichten Straftaten ab.[123] Damit virtuelle VE zur Bekämpfung von Rechtsextremismus in sozialen Netzwerken eingesetzt werden können, muss der Gesetzgeber erst eine Ermächtigungsgrundlage mit angepasstem Straftatenkatalog schaffen.

c) Der Zugriff auf Inhalte rechtsextremer Chatgruppen

Private Chatgruppen bei internetbasierten Messenger-Diensten haben sich in den vergangenen Jahren zu beliebten Verteilerplattformen für rechtsextreme Inhalte entwickelt. Die beiden wichtigsten Diensteanbieter in diesem Bereich, *WhatsApp* und *Telegram*, schützen die Inhalte von Chats mittels einer Ende-zu-Ende-Verschlüsselung.[124] Für den Zugriff auf Beiträge verdächtiger Nutzer kommt deshalb eine Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) gem. § 100a Abs. 1 S. 2 StPO in Frage. Die Online-Durchsuchung gem. § 100b StPO spielt hingegen nur in Ausnahmefällen eine Rolle, weil die Katalogtaten des § 100b Abs. 2 StPO so gut wie nie einschlägig sind.

§ 100a Abs. 1 S. 2 StPO ermöglicht eine Echtzeit-Überwachung verschlüsselter Telekommunikationsvorgänge, indem mithilfe einer Spähsoftware die Kommunikation entweder vor der Verschlüsselung oder nach der Entschlüsselung auf einem der beteiligten Endgeräte abgefangen wird.[125] Auf Nachrichten, die über einen Messenger-Dienst versendet wurden und die auf dem Endgerät des Nutzers gespeichert sind, darf unter den Voraussetzungen des § 100a Abs. 1 S. 3, Abs. 5 S. 1 Nr. 1b StPO zugegriffen werden.[126]

Grundsätzlich kommt die Quellen-TKÜ für einen Zugriff auf die Inhalte rechtsextremer Chatgruppen in Frage. Der Straftatenkatalog des § 100a Abs. 2 StPO umfasst mit den §§ 86, 89a, 129, 130 StGB mehrere Tatbestände, die im Kontext rechts motivierter Cyberkriminalität immer wieder verwirklicht werden.[127] Auch sind OTT-Kommunikationsdienste vom Begriff der Telekommunikation in § 100a StPO umfasst: Dieser orientiert sich nicht am technischen Telekommunikationsbegriff des § 3 Nr. 22 TKG,[128] sondern am entwicklungsoffenen Telekommunikationsbegriff des Fernmeldegeheimnisses.[129]

Allerdings machen hohe technische und datenschutzrechtliche Anforderungen die Quellen-TKÜ überaus personal- und zeitintensiv, weshalb diese Ermittlungsmaßnahme in der Praxis nur in besonders brisanten Fällen zum Einsatz kommen dürfte.[130] Darüber, wie häufig der „Staatstrojaner" tatsächlich Verwendung findet, verweigert die Bundesregierung jegliche Auskunft.[131]

---

122 Zustimmend *Rosengarten/Römer*, NJW 2012, 1764 (1764); *Soiné*, NStZ 2014, 248 (250); *Dalby*, S. 47; ablehnend *Zöller*, in: HK-StPO, § 163 Rn. 12; *Henrichs*, Kriminalistik 2012, 632 (634); *Ihwas*, S. 167 ff.; *Malek/Popp*, S. 138; *Bauer*, S. 198; die überwiegend die Schaffung einer speziellen Ermächtigungsgrundlage für den virtuellen verdeckten Ermittler fordern.

123 Zu den typischerweise verwirklichten Straftaten s. II.2.a).

124 *Graf*, in: BeckOK-StPO, § 100a Rn. 72, 75.

125 *Engländer*, S. 56; *Keller/Braun*, S. 45; *Ruppert*, Jura 2018, 994 (1000).

126 *Graf*, in: BeckOK-StPO, § 100a Rn. 114; *Bruns*, in: KK-StPO, § 100a Rn. 44; *Heger/Pohlreich*, S. 123.

127 Zu den typischerweise verwirklichten Delikten s. II.2.a).

128 So allerdings der *BGH*; vgl. *BGH*, NJW 2003, 2034 (2034); *BGH*, NJW 2007, 930 (931 f.).

129 *Keller/Braun*, S. 19 f.; *Ruppert,* Jura 2018, 994 (996); *Graf*, in: BeckOK-StPO, § 100a Rn. 18 f.; *Bulowski*, S. 129; für einen weites, an Art. 10 Abs. 1 GG angelehntes Begriffsverständnis spricht sich auch das *BVerfG* aus, vgl. *BVerfG,* NJW 2016, 3508 (3509); von einem solchen Begriffsverständnis geht auch der Gesetzgeber aus, vgl. BT-Drs. 19/17741, S. 38.

130 *Kochheim*, KriPoZ 2018, 60 (63).

131 BT-Drs. 19/1505, S. 5.

4. Das „Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität" als Antwort auf Hass und Hetze in sozialen Netzwerken?

Der Blick auf die strafprozessualen Rechtsgrundlagen für Ermittlungen im Internet hat gezeigt, dass sich die Strafverfolgungsbehörden *de lege lata* mit zum Teil erheblichen Rechtsunsicherheiten konfrontiert sehen. Durch den Entwurf eines *Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität*, den der Deutsche Bundestag am 18.6.2020 angenommen hat,[132] werden einige dieser Unsicherheiten beseitigt, gleichzeitig aber neue Probleme aufgeworfen. Das Ziel des Gesetzes, Hasskriminalität mit rechtsextremistischem Hintergrund auch bei Tatbegehung im Internet effektiv zu verfolgen und dadurch der zunehmenden Verrohung der Kommunikation insbesondere in den sozialen Medien entgegenzuwirken,[133] wird durch die vorgesehenen Gesetzesänderungen nur teilweise erreicht.

a) Ausgewählte Änderungen in StPO, TMG und BKAG

Zu begrüßen ist die geplante Erweiterung der §§ 100g, 100j StPO auf eine Abfrage von Bestands- und Nutzungsdaten bei Telemediendiensteanbietern, wodurch den Strafverfolgungsbehörden zukünftig eine rechtssichere und normenklare Ermächtigungsgrundlage für den Zugriff auf Telemediendaten zur Verfügung stehen wird. Lediglich die tatbestandliche Gleichstellung von Verkehrs- und Nutzungsdaten überrascht, da die Erhebung von Nutzungsdaten im Vergleich eine höhere Eingriffsintensität aufweist.[134]
Als korrespondierende telemedienrechtliche Übermittlungsregelung soll der neue § 15a TMG-E fungieren, der allerdings nahezu wortgleich mit dem jüngst für verfassungswidrig erklärten § 113 TKG ist.[135] Hier muss der Gesetzgeber nachbessern und beide Normen mit tatbestandlichen Eingriffsschwellen versehen, die den Vorgaben des *BVerfG* genügen.[136]
Im gleichen Beschluss hat das *BVerfG* festgestellt, dass das BKA als Zentralstelle im Bereich der Strafverfolgung grundsätzlich keine Befugnis zur Abfrage von Bestandsdaten hat.[137] Das stellt die in § 10 Abs. 1 S. 2 BKAG-E vorgesehene Möglichkeit eines Zugriffs auf Telemedien-Bestandsdaten durch das BKA in Frage.

b) Probleme im Zusammenhang mit der Meldepflicht aus § 3a NetzDG-E

An § 10 Abs. 1 S. 2 BKAG-E hängt auch die vorgesehene Pflicht der Telemedienanbieter zur Übermittlung strafbarer Inhalte sowie der zugehörigen IP-Adressen an das BKA (§ 3a NetzDG-E). Denn ohne eine Befugnis zur Bestandsdatenabfrage anhand der übermittelten IP-Adressen wird es dem BKA nicht möglich sein, die möglich-

---

132 Vgl. BR-Drs. 339/20 sowie zur Gesetzesbegründung BT-Drs. 19/17741, S. 37 ff.
133 Vgl. BT-Drs. 19/17741, S. 1.
134 So auch *Bundesbeauftragter für Datenschutz und Informationssicherheit*, Stellungnahme zum Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (https://www.bfdi.bund.de/DE/Infothek/Transparenz/Stellungnahmen/2020/Stellungnahme_Gesetz_Bekämpfung_Hasskriminalität.html?nn=12818400, zuletzt abgerufen am 30.3.2021), S. 7; *Bäcker*, Stellungnahme zu dem Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität, S. 15.
135 *BVerfG*, NJW 2020, 2699 (2707).
136 Für den Bereich der Strafverfolgung ist das Vorliegen eines Anfangsverdachts erforderlich, die Zuordnung dynamischer IP-Adressen muss zusätzlich dem Schutz von Rechtsgütern von hervorgehobenem Gewicht dienen; *BVerfG,* NJW 2020, 2699 (2710, 2714).
137 *BVerfG*, NJW 2020, 2699 (2718).

erweise unter falschen Namen registrierten Verfasser strafbarer Inhalte zu identifizieren – die gerne als „Kernstück“[138] des Gesetzesentwurfs dargestellte Meldepflicht liefe ins Leere. Hinzu kommt, dass die Begrenzung der Meldepflicht auf soziale Netzwerke mit mehr als zwei Millionen Nutzern (§ 1 Abs. 2 NetzDG-E) keinen Rückgang rechtsextremer Internetaktivität, sondern lediglich eine Abwanderung rechtsextremer Akteure auf kleinere Alternativplattformen zur Folge haben könnte.[139]

In Zusammenhang mit der Meldepflicht nach § 3a NetzDG-E und der Möglichkeit einer Telemedien-Bestandsdatenauskunft durch das BKA steht zudem eine massenhafte Bevorratung von Nutzerdaten beim BKA im Raum, die Bundesrechtsanwaltskammer befürchtet gar eine „Vorratsdatenspeicherung durch die Hintertür“.[140] Auch die sofortige Übermittlung von IP-Adressen ohne Vorliegen eines Anfangsverdachts ist kritisch zu sehen, besser wäre ein zweistufiges Meldeverfahren.[141]

Überhaupt ist fragwürdig, ob die im Gesetzesentwurf vorgesehene Schaffung von nur 180 neuen Stellen bei den Staatsanwaltschaften und 75 neuen Stellen in der Strafjustiz zur Bewältigung der erwarteten 150 000 zusätzlichen Ermittlungsverfahren ausreicht.[142]

c) Aktuelle politische Entwicklung

Aus diesen Gründen verwundert es nicht, dass zwei Gutachten das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität als teilweise verfassungswidrig einstufen[143] und die Ausfertigung derzeit auf der Kippe steht.[144] Es bleibt zu hoffen, dass der Bundespräsident nicht dem gemeinsamen Vorschlag des Justiz- und Innenministeriums nachkommt und das Gesetz trotz entgegenstehender Zweifel an der Verfassungsmäßigkeit unterschreibt, nur damit anschließend ein wegen der nahenden Bundestagswahl vermutlich übereiltes und unausgereiftes „Reparaturgesetz“ nachgeschoben werden kann. Besser sollte, wie in einem Antrag der Fraktion Bündnis 90/Die Grünen vorgeschlagen, eine verfassungskonforme Neufassung des Gesetzes durch den Bundestag erfolgen.[145]

---

138 BT-Drs. 19/17741, S. 17; vgl. auch Tagesschau, abrufbar unter: https://www.tagesschau.de/inland/hasskriminalitaet-internet-101.html (zuletzt abgerufen am 30.3.2021).

139 Vgl. DAV, Stellungnahme des Deutschen Anwaltvereins durch den Ausschuss Strafrecht zum Referentenentwurf eines Gesetzes zur Bekämpfung der Hasskriminalität und des Rechtsextremismus, abrufbar unter: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2020/Downloads/012820_Stellungnahme_DAV_RefE__Belaempfung-Rechtsextremismus-Hasskriminalitaet.pdf?__blob=publicationFile&v=3 (zuletzt abgerufen am 30.3.2021), S. 4.

140 Bundesrechtsanwaltskammer, Stellungnahme Nr. 12 März 2020 zum Regierungsentwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität i.d.F. 18.2.2020, abrufbar unter: https://www.brak.de/zur-rechtspolitik/stellungnahmen-pdf/stellungnahmen-deutschland/2020/maerz/stellungnahme-der-brak-2020-12.pdf (zuletzt abgerufen am 30.3.2021), S. 3, 6; die Bevorratung von Daten beim BKA ohne Vorliegen eines Tatverdachts sehen auch kritisch *Bäcker*, Stellungnahme zu dem Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität, S. 7.

141 So auch *Bäcker*, Stellungnahme zu dem Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität, S. 5 f.; Bundesbeauftragter für Datenschutz und Informationssicherheit, Stellungnahme zum Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität, S. 2 f.; BT-Drs. 19/22888, S. 2 f.

142 Vgl. BT-Drs. 19/17741, S. 31; kritisch auch DRB, Stellungnahme des Deutschen Richterbundes zum Referentenentwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität, abrufbar unter: https://www.drb.de/fileadmin/DRB/pdf/Stellungnahmen/2020/DRB_200110_Stn_Nr_1_Bekaempfung_Rechtsextremismus_und_Hasskriminalitaet.pdf (zuletzt abgerufen am 30.3.2021), S. 3 f.

143 *Bäcker*, Folgerungen aus dem zweiten Bestandsdatenbeschluss des BVerfG für die durch das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität geschaffenen Datenverarbeitungsregelungen, abrufbar unter: https://www.gruene-bundestag.de/fileadmin/media/gruenebundestag_de/themen_az/rechtspolitik/PDF/200917-Baecker-Gutachten-Gesetz_zur_Bekaempfung_des_Rechtsextremismus_und_der_Hasskriminalitaet.pdf (zuletzt abgerufen am 30.3.2021), S. 3 ff.; Wissenschaftliche Dienste des Deutschen Bundestages, Mögliche Auswirkungen des Beschlusses des Bundesverfassungsgerichts vom 27. Mai 2020, 1 BvR 1873/13 – Bestandsdatenauskunft II – auf das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (BT-Drs. 19/17741 und 19/20163) und das Netzwerkdurchsetzungsgesetzänderungsgesetz, abrufbar unter: https://www.bundestag.de/resource/blob/691848/3be358ed1c526e33c946a453f0b60aaa/WD-10-037-20-pdf-data.pdf (zuletzt abgerufen am 30.3.2021), S. 22 ff.

144 Zur medialen Berichterstattung vgl. *Mascolo/Steinke*, Bedenken in Bellevue, SZ 17.9.2020, abrufbar unter: https://www.sueddeutsche.de/politik/hate-speech-hasskriminalitaet-gesetz-steinmeier-1.5034929 (zuletzt abgerufen am 30.3.2021).

145 BT-Drs. 19/22888.

IV. Plädoyer für Zivilcourage im Internet

Die Strafverfolgungsbehörden stehen rechtsextremen Inhalten im Internet keineswegs hilflos gegenüber. Schon jetzt beinhaltet die StPO weitreichende Abrufnormen für den Zugriff auf Telekommunikationsdaten[146] und eine Rechtsgrundlage für den Einsatz virtueller nicht offen ermittelnder Polizeibeamter in sozialen Netzwerken. Sobald das *Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität* in hoffentlich überarbeiteter Form in Kraft tritt, stehen den Ermittlern zudem rechtssichere und normenklare Ermächtigungsgrundlagen für die Erhebung von Telemediendaten zur Verfügung.

Allerdings sind die Möglichkeiten staatlicher Präsenz im Netz begrenzt und die Zahl rechtsextremer Inhalte ist hoch. Viele dieser Inhalte sind zwar verletzend, erfüllen aber keinen Straftatbestand. Die Mittel des Strafrechts allein reichen deshalb nicht aus, um der Verrohung der Kommunikation im Internet entgegenzutreten. Vielmehr kommt es auf jeden einzelnen Internetnutzer an.

Es liegt in unserer Verantwortung, Auseinandersetzungen im digitalen Raum sachlich zu führen und eine respektvolle Gesprächskultur zu pflegen. Wir müssen auch im Netz für unsere demokratischen Werte und unsere pluralistische Gesellschaft eintreten, indem wir menschenverachtenden und gewaltverherrlichenden Beiträgen widersprechen. Nur eine Kultur der Zivilcourage kann rechtsextremistischen Bestrebungen im Internet die Stirn bieten – Wegschauen ist nicht mehr erlaubt.

[146] Voraussetzung dafür ist eine den Vorgaben des *BVerfG* entsprechende Änderung des derzeit verfassungswidrigen § 113 TKG; vgl. *BVerfG*, NJW 2020, 2699 (2707 ff.).

KriPoZ Kriminalpolitische Zeitschrift JuP

„Junges Publizieren“

Seminararbeit von

Ramon Kohler

Cybermobbing als Straftat

Abgabedatum:
5.10.2020

Prüfer: Prof. Dr. Mark A. Zöller
Juristische Fakultät der Ludwig-Maximilians-Universität München

Inhaltsverzeichnis

I. Einführung

Wir leben in einem Zeitalter, das von digitalen Medien geprägt ist.
Die durch das Internet neugewonnenen Möglichkeiten der schnellen und weitreichenden Interaktion und Kommunikation haben allerdings auch neue Kriminalitätsphänomene mit sich gebracht.
Eines hiervon stellt das sogenannte „Cybermobbing" dar.
Diese Schwerpunktseminararbeit beschäftigt sich daher unter anderem mit der Frage, inwieweit strafrechtlicher Schutz vor Cybermobbing nach aktueller Rechtslage besteht und ob beziehungsweise inwieweit Strafbarkeitslücken bestehen. Abschließend soll auch auf die Frage eingegangen werden, ob die Einführung eines Cybermobbing-Tatbestandes in das Strafgesetzbuch der Bundesrepublik Deutschland notwendig ist oder nicht.

1. Begriff des „Cybermobbings"

Der Begriff des „Cybermobbings" ist aktuell noch nicht genau und einheitlich definiert.[1] Viele Definitionsversuche beziehen sich zunächst auf *Dan Olweus'* Verständnis von „Mobbing", welches ihm zufolge vorliegt, wenn ein Schüler über einen längeren Zeitraum wiederholt absichtlich schädigenden Handlungen eines oder mehrerer anderer Schüler ausgeliefert ist.[2] Hierbei müsse nach *Olweus* ein Ungleichgewicht der Kräfte vorliegen.[3]
Erwähnenswert ist, dass das Element des Kräfteungleichgewichts zwischen Opfer und Täter nicht unumstritten ist.[4] Festzuhalten ist im Ergebnis allerdings, dass das Element des asymmetrischen Kräfteverhältnisses zwischen Täter und Opfer insbesondere deshalb einleuchtend erscheint, weil es hierdurch von symmetrischen Konflikten, bei dem Opfer und Täter auf „Augenhöhe" kommunizieren, abgegrenzt werden kann.[5]
Folgt man den Wissenschaftlichen Diensten des Deutschen Bundestages, so stellt Cybermobbing eine Form des psychischen Schikanierens dar, wobei es mithilfe von Internet- und Mobiltelefondiensten über einen längeren Zeitraum hinweg erfolgt.[6]
Unter Berücksichtigung der vertretenen Ansichten und Definitionsversuche ist im Rahmen dieser Schwerpunktseminararbeit somit Folgendes festzuhalten:
Cybermobbing liegt dann vor, wenn durch einen Einzelnen oder eine Gruppe Handlungen vorgenommen werden, die die Intention haben, eine andere Person zu schädigen, wobei diese Handlungen über einen längeren Zeitraum wiederholt vorkommen müssen und zwischen Täter(n) und dem Opfer ein asymmetrisches Kräfteverhältnis bestehen muss. Hierzu muss oder müssen sich der oder die Täter der modernen Informations- und Telekommunikationstechnik bedienen.[7]

---

1 *Vandebosch/van Cleemput*, New Media & Society 2009, 1349 (1371).
2 *Olweus*, Gewalt in der Schule, 2. Auflage (1996), S. 22.
3 *Olweus*, S. 23.
4 *Specht*, Vernetzt, verletzt?: Cyberbullying unter Jugendlichen in Deutschland, Masterarbeit zur Erlangung des Grades Master of Arts (M.A.) an der Philosophisch-Sozialwissenschaftlichen Fakultät der Universität Augsburg, 19.2.2010, abrufbar unter: http://websquare.imb-uni-augsburg.de/files/Masterarbeit_Tamara_Ranner.pdf (zuletzt abgerufen am 4.10.2020), S. 26.
5 *Sitzer et al.*, Ergebnisbericht der Online-Studie „Cybermobbing bei Schülerinnen und Schülern", Universität Bielefeld, Juli 2012, abrufbar unter: https://pub.uni-bielefeld.de/download/2515055/2939612/Ergebnisbericht-Cyberbullying.pdf (zuletzt abgerufen am 4.10.2020), S .17.
6 Wissenschaftliche Dienste des Deutschen Bundestages, Dokumentation: Mobbing an Schulen, Arbeit abgeschlossen am 2.10.2018, abrufbar unter: https://www.bundestag.de/resource/blob/592494/4ee825520cb3b29d7a6c0b6555f01657/WD-9-056-18-pdf-data.pdf (zuletzt abgerufen am 4.10.2020), S. 4.
7 *Patchin/Hinduja*, Youth Violence and Juvenile Justice, Vol. 4 No. 2 2006, 148 (152).

2. Erscheinungsformen des Cybermobbings

Im Folgenden werden einige Erscheinungsformen des Cybermobbings dargestellt. Hierbei wird zwischen direktem und indirektem Cybermobbing differenziert.[8]

a) Direktes Cybermobbing

Ist das Opfer der Adressat der negativ zu bewertenden Einzelhandlungen, so liegt eine Form des direkten Mobbings vor.[9]
Eine Handlungsform des direkten Cybermobbings stellt das sogenannte „Online Harassment" dar.[10] Darunter versteht man die zielgerichtete und wiederkehrende Belästigung oder Schikanierung einer Person.[11] Eine weitere Form des direkten Cybermobbings können die „Cyberthreats" darstellen. Unter diesen versteht man „Androhungen physischer Gewalt, etwa in der Gestalt von Morddrohungen oder Vergewaltigungsszenarien"[12].
Einige Autoren sehen auch das „Cyberstalking", worunter man „eine Form des Stalkings [versteht], die unter Verwendung von Informations- und Kommunikationstechnologie ausgeübt wird"[13], als eine Form des Cybermobbings an.[14]
Vom Begriff des „Cybermobbings" abzugrenzen[15] ist das sogenannte „Flaming", mit dem ein kurzer Konflikt zwischen zwei oder mehreren Personen (in der Regel im Internet) gemeint ist, bei dem wechselseitige Beleidigungen geäußert werden[16].

b) Indirektes Cybermobbing

Werden die negativ zu bewertenden Einzelhandlungen zwar gegen das Opfer gerichtet, aber nicht ihm gegenüber vorgenommen, liegt eine Form des indirekten Mobbings vor.[17]
Eine Handlungsform des indirekten Cybermobbings stellt der Begriff „Denigration" dar. Hierunter fasst man die Schädigung des Rufes einer Person, indem im Internet unwahre oder diffamierende Informationen über diese verbreitet werden.[18] Hierunter kann auch die Versendung manipulierten Fotomaterials fallen.[19]
Auch die Handlungsform der „Impersonation" stellt eine Form des indirekten Cybermobbings dar. Hierbei wird sich Zugang zu Accounts oder Geräten des Opfers verschafft, um so in dessen Namen für das Opfer nachteilige Handlungen im Internet vorzunehmen.[20]
Schließlich ist auch das „Happy Slapping" anzuführen. Hierunter versteht man das Fotografieren oder Filmen einer gezielt inszenierten Gewaltaktion unter anschließender Verbreitung dieser Aufnahme.[21]

---

8 *Doerbeck*, Cybermobbing: Phänomenologische Betrachtung und strafrechtliche Analyse, 2019, S. 96 m.w.N.
9 A.a.O.
10 *Leffler*, Der strafrechtliche Schutz des Rechts am eigenen Bild vor dem neuen Phänomen des Cyber-Bullying, 2012, S. 123.
11 *Willard*, Cyberbullying and cyberthreats, 2007, S. 6; siehe auch: *Doerbeck*, S. 131.
12 *Jülicher*, NJW 2019, 2801 (2802).
13 *Doerbeck*, S. 118.
14 So etwa *Giebel*, NJW 2017, 977 (977); *Fawzi*, Cyber-Mobbing: Ursachen und Auswirkungen von Mobbing im Internet, 2. Auflage (2015), S. 53; *Willard*, S. 256.
15 Siehe zu dieser Abgrenzung: *Sitzer et. al*, S. 13.
16 Siehe zum Begriff des „Flamings": *Willard*, S. 5, 255.
17 *Doerbeck*, S. 96 m.w.N.
18 *Willard*, S. 7 f., 255.
19 Vgl. *Jülicher*, NJW 2019, 2801 (2802); *Willard*, S. 1.
20 *Willard*, S. 255.
21 *Sitzer et al.*, S. 13.

II. Strafrechtliche Erfassung des Cybermobbings de lege lata

In diesem Teil soll untersucht werden, inwieweit nach aktueller Rechtslage strafrechtlicher Schutz vor dem Phänomen des Cybermobbings besteht und ob oder inwieweit Strafbarkeitslücken vorhanden sind und hieraus Reformerfordernisse folgen.
Zunächst ist festzustellen, dass es im StGB aktuell keinen eigenen Cybermobbing-Straftatbestand gibt.
Daher ist es notwendig, einen Anknüpfungspunkt für die Strafbarkeit von Cybermobbing zu finden. Ein solcher ergibt sich unter Bezugnahme auf die konkreten Inhalte der Kommunikationsvorgänge.[22]
Im Folgenden wird also näher betrachtet, welche Strafnormen bei gewissen Cybermobbinghandlungen einschlägig sein können.

1. Straftaten gegen die Ehre (§§ 185 ff. StGB)

Denkt man an „jegliche[] Formen von Beleidigungen, d[ie] Verbreitung von Gerüchten, Lügen oder Verleumdungen über Internet oder Handy“[23], so kommen die Ehrschutzdelikte der §§ 185 ff. StGB als einschlägige Strafnormen in Frage.[24]

a) Ehrbegriff der §§ 185 ff. StGB

Das zu schützende Rechtsgut der §§ 185-188 StGB ist die persönliche Ehre.[25] Nach Auffassung des *BGH* liegt ein Angriff auf die Ehre vor, wenn einem anderen durch den Täter unrechtmäßigerweise Mängel nachgesagt werden, die, wenn sie vorlägen, den Geltungswert des Betroffenen mindern würden.[26] Geschützt ist damit „allein der aus der verdienten Wertgeltung hervorgehende Anspruch auf Achtung der Persönlichkeit“[27].

b) Beleidigungsfähigkeit

Jeder Mensch, das heißt auch jedes Kind und auch ein geistig kranker[28] Mensch, ist beleidigungsfähig.[29]

c) Voraussetzungen der Kundgabe

Die Beleidigungsdelikte klassifizieren sich als Kundgabedelikte, weshalb jede ehrenkränkende Äußerung einen Inhalt haben muss, der bestimmt oder objektiv bestimmbar ist, an eine andere Person gerichtet und zudem auch noch dazu bestimmt sein muss, von anderen zur Kenntnis genommen zu werden.[30]
Der Täter muss bezüglich der Kundgabe mit Vorsatz handeln. Dies ergibt sich aus § 15 StGB.

22 *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Auflage (2012), Rn. 419.
23 *Katzer*, Cybermobbing – Wenn das Internet zur W@ffe wird, 2014, S. 74.
24 A.a.O.
25 BGHSt 1, 288 (289); 11, 67 (70 f.); *Wessels/Hettinger/Engländer*, Strafrecht BT I, 42. Auflage (2018), Rn. 520 m.w.N.
26 BGHSt 36, 145 (148).
27 *Wessels/Hettinger/Engländer*, Rn. 520.
28 Vgl. BGHSt 7, 129, 132; 23, 1, 3.
29 *Wessels/Hettinger/Engländer*, Rn. 520.
30 *Wessels/Hettinger/Engländer*, Rn. 535 m.w.N.

d) Grundsatz der Straflosigkeit wahrer Tatsachenbehauptungen

Wahre Tatsachenbehauptungen werden, selbst wenn ihnen ein ehrrühriger Sinn innewohnt, nicht von den §§ 185 ff. StGB erfasst, da es insoweit zu keiner Berührung eines verdienten Geltungsanspruchs kommt.[31]
Eine Ausnahme von diesem Grundsatz bildet die sogenannte „Formalbeleidigung" (§§ 185, 192 StGB). Diese liegt vor, wenn der Form oder den äußeren Umständen einer Äußerung ein selbständiger Beleidigungsinhalt zukommt und bereits hierdurch eine Ehrabschneidung bewirkt wird, deren ehrverletzender Charakter nicht mehr von der Äußerung der wahren Tatsache(n) gedeckt ist und somit vom Betroffenen nicht hingenommen werden muss.[32]

e) Antragserfordernis

Nach § 194 Abs. 1 StGB wird die Tat nur auf Antrag verfolgt. Ausnahmen hierzu finden sich in § 194 Abs. 2, 3, 4 StGB. Aus den §§ 374 Abs. 1 Nr. 2, 376 StPO ergibt sich ferner die Möglichkeit zur Privatklage. Ausgenommen hiervon ist § 194 Abs. 4 StGB.

f) Überblick zu den §§ 185 ff. StGB

Im Folgenden sollen die Beleidigungstatbestände der §§ 185-187 StGB und deren Anforderungen vorgestellt werden.

aa) Beleidigung (§ 185 StGB)
Unter dem Begriff der „Beleidigung" versteht man allgemein die Kundgabe von Geringschätzung, Nicht- oder Missachtung.[33]
Nicht- oder Missachtung werden durch eine Äußerung zum Ausdruck gebracht, wenn der im Grundsatz uneingeschränkte Achtungsanspruch des Betroffenen verletzt wird, indem ihm sein sozialer oder ethischer Wert ganz beziehungsweise zum Teil oder sein elementarer Menschenwert abgesprochen wird.[34]
Für die Norm ergeben sich drei Begehungsformen: Die Äußerung eines Werturteils gegenüber dem Betroffenen selbst (1) oder gegenüber einem Dritten (2) sowie die Behauptung einer ehrrührigen Tatsache gegenüber dem Betroffenen (3).[35] Bei letzterer geht die herrschende Meinung davon aus, dass die Behauptung unwahr sein muss.[36] Folgt man dieser Ansicht, so ist die Unwahrheit der Tatsachenbehauptung als objektives Tatbestandsmerkmal anzusehen, weshalb sie nachzuweisen ist und vom Vorsatz des Täters umfasst sein muss.[37] Insgesamt erfasst § 185 StGB somit alle von den §§ 186, 187 StGB nicht abgedeckten Ehrverletzungen.[38]
Unter Werturteilen versteht man Äußerungen, die durch Elemente der subjektiven Stellungnahme oder der Meinung geprägt sind und daher nur nach persönlicher Auffassung falsch oder richtig, nicht aber wahr oder unwahr sein können.[39] Hierzu werden unter anderem Meinungsäußerungen, Schlussfolgerungen und Prognosen gezählt.[40]

31 *Doerbeck*, S. 149 m.w.N.
32 *Regge/Pegel*, in: MüKo-StGB, 3. Auflage (2017), § 192 Rn. 1.
33 *Regge/Pegel*, in: MüKo-StGB, § 185 Rn. 3.
34 *Kühl*, in: Lackner/Kühl, StGB, 29. Auflage (2018), § 185 Rn. 4 m.w.N.
35 *Kühl*, in: Lackner/Kühl, StGB, § 185 Rn. 2; *Regge/Pegel*, in: MüKo-StGB, § 185 Rn. 3.
36 *Kühl*, in: Lackner/Kühl, StGB, § 185 Rn. 2.
37 *Zaczyk*, in: Kindhäuser/Neumann/Paeffgen, NK-StGB, 5. Auflage (2017), § 185 Rn. 11 m.w.N.
38 *Regge/Pegel*, in: MüKo-StGB, § 185 Rn. 3.
39 *Eisele/Schittenhelm*, in: Schönke/Schröder, StGB, 30. Auflage (2019), § 186 Rn. 3 m.w.N; *Regge/Pegel*, in: MüKo-StGB, § 186 Rn. 6 m.w.N.
40 *Regge/Pegel*, in: MüKO-StGB, § 186 Rn. 6 m.w.N.

Als Tatsache versteht man einen konkreten, wahrnehmbaren Zustand oder Vorgang der Vergangenheit oder Gegenwart, der in die Wirklichkeit getreten ist, also der Wirklichkeit angehört und deshalb dem Beweis zugänglich ist.[41] Tatsachenaussagen sind folglich „nur solche Äußerungen, deren Gehalt einer objektiven Klärung zugänglich ist und als etwas Geschehenes oder Vorhandenes mit den prozessualen Möglichkeiten festgestellt werden kann“[42]. Scheinbar unbearbeitete Audio-, Video- oder Bilddateien stellen auch Tatsachenbehauptungen dar, da sie ein reales Geschehen zeigen, das vermeintlich so stattgefunden hat.[43]

Der subjektive Tatbestand des § 185 StGB setzt voraus, dass der Täter mit dolus eventualis hinsichtlich der objektiven Tatbestandsmerkmale handelt. Er muss also zumindest die Möglichkeit sehen, dass seiner Äußerung ein ehrverletzender Inhalt innewohnt.[44] Hierzu gehört „auch die Kenntnis der Unwahrheit der Tatsachen […], die gegenüber dem Betroffenen behauptet oder einem Werturteil zugrunde gelegt w[ird]“[45]. Die Kenntnisnahme dieser Äußerung durch eine andere Person muss ebenfalls vom Vorsatz erfasst sein, wie auch das Verständnis des ehrverletzenden Gehalts durch diese.[46]

Das Strafmaß der einfachen Beleidigung beträgt bis zu einem Jahr Freiheitsstrafe oder Geldstrafe.

bb) Üble Nachrede (§ 186 StGB)

Im Gegensatz zu § 185 StGB schützt § 186 StGB vor Angriffen auf die Ehre, die der Ermöglichung fremder Missachtung dienen.[47] Somit wird ein Kommunikationsvorgang mit einem Dritten vorausgesetzt, über den eine ehrrührige Tatsache dem Opfer zugeschrieben wird.[48]

Als Tathandlungen nennt § 186 StGB das Behaupten und Verbreiten einer ehrherabsetzenden Tatsache.

Die Behauptung einer Tatsache meint, diese nach eigener Überzeugung so hinzustellen, als wäre sie wahr.[49]

Unter dem Verbreiten einer Tatsache versteht man, dass eine fremde Tatsachenbehauptung an Dritte weitergegeben wird.[50]

Straffrei ist der Täter nach § 186 StGB dann, wenn die behauptete Tatsache erweislich wahr ist. Streitig ist allerdings, welche Rolle die Nichterweislichkeit beziehungsweise die Unwahrheit der behaupteten Tatsache spielt.

Nach der herrschenden Meinung stellt die Nichterweislichkeit eine objektive Bedingung der Strafbarkeit dar.[51] Folgt man dieser Ansicht, muss sich der Vorsatz des Täters also nicht hierauf beziehen.[52]

Eine Gegenansicht in der Literatur ist dafür, die Unwahrheit der Tatsachenaussage bereits im Tatbestand zu berücksichtigen, lässt es aber ausreichen, wenn der Täter in diesem Bezug sorgfaltspflichtwidrig handelt.[53]

Folgt man der in der Literatur zunehmend vertretenen Gegenmeinung, ist der subjektive Tatbestand daher erfüllt, wenn der Täter (zumindest bedingt) vorsätzlich hinsichtlich des Behauptens oder Verbreitens seiner Äußerung handelt, wobei er bezüglich der Unwahrheit der Tatsache wenigstens sorgfaltswidrig handeln muss.[54]

Die Straftat der üblen Nachrede ist nach § 186 StGB qualifiziert, wenn sie öffentlich oder durch Verbreiten von

41 *BGH*, NJW 1994, 2614 (2615) m.w.N; *Hilgendorf*, in: LK-StGB, 12. Auflage (2009), § 185 Rn. 4 m.w.N; *Eisele/Schittenhelm*, in: Schönke/Schröder, StGB, § 186 Rn. 3 m.w.N.
42 *Eisele/Schittenhelm*, in: Schönke/Schröder, StGB, § 186 Rn. 3.
43 *Eisele*, Computer- und Medienstrafrecht, 2013, Kap. 6 Rn. 69 f.
44 *Eisele/Schittenhelm*, in: Schönke/Schröder, StGB, § 186 Rn. 3 m.w.N; *Regge/Pegel*, in: MüKo-StGB, § 186 Rn. 6 m.w.N.
45 A.a.O.
46 A.a.O.
47 *Valerius*, in: v. Heintschel-Heinegg, BeckOK-StGB, 47. Ed. (2020), § 186 Rn. 1 m.w.N.
48 *Zaczyk*, in: NK-StGB, § 186 Rn. 1 m.w.N.
49 *Zaczyk*, in: NK-StGB, § 186 Rn. 8 m.w.N.
50 *Regge/Pegel*, in: MüKo-StGB, § 186 Rn. 18 m.w.N.
51 A.a.O.
52 *Eisele* (Fn. 43), Kap. 6 Rn. 84.
53 *Fischer*, StGB, 67. Auflage (2020), § 186 Rn. 13a; *Hilgendorf*, in: LK-StGB, § 186 Rn. 4; vgl. auch *Zaczyk*, in: NK-StGB, § 186 Rn. 19 m.w.N.
54 *Regge/Pegel*, in: MüKo-StGB, § 186 Rn. 31.

Schriften begangen ist.
In diesen Fällen beträgt das Strafmaß bis zu zwei Jahren Freiheitsstrafe oder Geldstrafe. In den übrigen Fällen bis zu einem Jahr Freiheitsstrafe oder Geldstrafe.

cc) Verleumdung (§ 187 StGB)

Für § 187 StGB gelten die Ausführungen zu § 186 StGB entsprechend. Im Unterschied zur üblen Nachrede setzt der Verleumdungstatbestand die Verbreitung oder Behauptung unwahrer Tatsachen voraus. Damit ist die Unwahrheit der Tatsache ein objektives Tatbestandsmerkmal und muss vom Vorsatz des Täters (dolus directus zweiten Grades ist erforderlich) erfasst sein.[55]
Ähnlich zu § 186 StGB ist die Tat qualifiziert, wenn sie öffentlich, in einer Versammlung (dies findet man nicht bei § 185 StGB) oder durch das Verbreiten von Schriften begangen ist. In diesen Fällen beträgt das Strafmaß bis zu fünf Jahren Freiheitsstrafe oder Geldstrafe.
In den übrigen Fällen beträgt das Strafmaß bis zu zwei Jahren Freiheitsstrafe oder Geldstrafe.

g) Cybermobbingspezifische Aspekte und Probleme der §§ 185 ff. StGB

Da die §§ 185 ff. StGB nun umfassend vorgestellt wurden, werden im Folgenden speziell Aspekte und Probleme dieser Tatbestände in Bezug auf das Phänomen des Cybermobbings behandelt.

aa) Kundgabe über Kommunikationstechnologie

Grundsätzlich kann die Äußerung des Täters in unmittelbarer sowie vermittelter Weise erfolgen.[56]
Die Kundgabe der Missachtung bei § 185 StGB kann also auch über die modernen Medien und allgemein über das Internet erfolgen.[57]
Dies ist auch auf die Kundgabe bei den §§ 186 f. StGB übertragbar.[58]

bb) Auswirkungen von privaten Räumlichkeiten auf den Kundgabevorsatz

Die durch das Internet gewonnene räumliche Unabhängigkeit der Täter ermöglicht es diesen, auch aus privaten (für sie geschützten) Räumen Cybermobbinghandlungen vorzunehmen. Problematisch ist hinsichtlich der Beleidigungstatbestände, inwiefern sich das Handeln aus einem privaten Raum heraus auf den – wie unter II. 1. c) festgestellten – erforderlichen Kundgabevorsatz des Täters auswirkt.
Hierbei ist insbesondere in Frage zu stellen, inwiefern die Täter, die aus einem privaten Raum und damit aus einer abgeschiedenen Position heraus ehrverletzende Äußerungen in das Internet stellen, sich des Kundgabecharakters ihres Handelns bewusst sind.[59] Trotz des unter diesen Umständen möglicherweise vorhandenen Gefühls der Sicherheit und Vertrautheit, kann im Hinblick auf die Kundgabe der ehrverletzenden Äußerung dolus eventualis nicht ausgeschlossen werden, da die beleidigende Äußerung durch ihr Einstellen ins Internet ja gerade dazu bestimmt ist, von anderen Personen zur Kenntnis genommen zu werden.[60]
Aus diesen Gründen ist der Kundgabevorsatz der Täter, die aus privaten Räumen heraus handeln, nicht per se ausgeschlossen.

55 *Regge/Pegel*, in: MüKo-StGB, § 187 Rn. 8, 10 m.w.N.
56 *Fischer*, StGB, § 185 Rn. 7.
57 *Eisele* (Fn. 43), Kap. 6 Rn. 77; *Kühl*, in: Lackner/Kühl, StGB, § 185 Rn. 8 m.w.N.
58 *Fischer*, StGB, § 185 Rn. 7.
59 *Hilgendorf*, ZIS 2010, 208 (210).
60 *Hilgendorf*, ZIS 2010, 208 (210).

cc) Privatheit im Internet

In cybermobbingspezifischer Hinsicht stellt sich zudem die Frage, wie besondere Vertrauensverhältnisse im Internet zu behandeln sind.

Grundsätzlich spricht sich die wohl überwiegende Meinung dafür aus, den Anwendungsbereich der §§ 185, 186 StGB in Bezug auf vertrauliche Äußerungen über einen Dritten in engsten Vertrauensverhältnissen, wie etwa dem Familienkreis, teleologisch zu reduzieren, wobei hierfür teils unterschiedliche Begrenzungs- und Begründungsansätze herangezogen werden.[61] Eine andere Ansicht stellt hingegen auf eine Rechtfertigung über § 193 StGB, also der Figur der „Wahrnehmung berechtigter Interessen", ab.[62]

Besonders enge Freundschaften können auch ein Vertrauensverhältnis im oben genannten Sinne darstellen.[63] Dies wirft die Frage auf, inwiefern beziehungsweise ob soziale Gruppen im Internet, private Chatrooms oder Foren beziehungsweise andere Netzwerke als „besondere Vertrauensverhältnisse" angesehen werden können, was im Ergebnis, sofern es bejaht werden kann, zu einer Privilegierung der Täter in Hinblick auf §§ 185, 186 StGB führen könnte.

Ob eine Privilegierung des Täters in diesen Fällen an eine solche bei Äußerungen im engsten Familienkreis angelehnt werden kann, erscheint allerdings bereits deshalb fraglich, da die Privilegierung bei Äußerungen im engsten Familienkreis unter anderem darauf beruht, dass Art. 6 Abs. 1 GG die Familie unter besonderen Schutz stellt, wohingegen ein solcher Schutz für vertraute Usergruppen im Internet nicht besteht.[64] Zudem sind soziale Gruppen, private Chatrooms, Foren etc. im Internet in ihrem Charakter nicht unwesentlich von der Anonymität der Nutzer bestimmt, weshalb es sich in diesen Fällen wohl regelmäßig nicht um ein besonderes Vertrauensverhältnis handelt, sondern vielmehr um das Gegenteil hiervon.[65]

Daher muss eine Privilegierung der Täter in Cybermobbingfällen ausscheiden.

dd) Heimliches Anfertigen und Verbreitung von unbearbeiteten Audio-, Foto- oder Videodateien

Beim heimlichen Anfertigen von Audio-, Foto- oder Videodateien scheidet eine Strafbarkeit nach den §§ 185 ff. StGB mangels Kundgabe aus.[66] Sind diese Dateien unbearbeitet (und damit tatsächlich wahr), scheidet eine Strafbarkeit nach §§ 185 ff. StGB ebenfalls bei der Verbreitung dieser aus (Grundsatz der Straflosigkeit wahrer Tatsachenbehauptungen), es sei denn, eine Formalbeleidigung liegt vor.

ee) Bearbeitete Audio-, Bild- oder Videoaufnahmen im Rahmen der §§ 186, 187 StGB

Fraglich ist allerdings, ob das Verbreiten von bearbeiteten Audio-, Bild- oder Videodateien über das Internet von den §§ 186, 187 StGB erfasst ist.

Dies ist zu bejahen. Tatsachenbehauptungen solcher Art sind dann als unwahr anzusehen, wenn sie vom Täter derart manipuliert wurden, dass sie nicht mehr der Realität entsprechen und diese Manipulation auch nicht ohne Weiteres als solche erkennbar ist.[67] Werden diese im Internet kundgegeben, so besteht eine Strafbarkeit nach den §§ 186, 187 StGB.

---

61 *Wessels/Hettinger/Engländer*, Rn. 537 f. m.w.N; *Fischer*, StGB, § 185 Rn. 12c m.w.N; *Kühl*, in: Lackner/Kühl, StGB, § 185 Rn. 9 m.w.N.
62 *Hilgendorf*, in: LK-StGB, § 185 Rn. 14 m.w.N.
63 BVerfGE 90, 255.
64 *Hilgendorf*, ZIS 2010, 208 (210).
65 *Regge/Pegel*, in: MüKo-StGB, Vor § 185 Rn. 64 m.w.N.
66 *Hilgendorf*, in: LK-StGB, § 185 Rn. 27.
67 *Doerbeck*, S. 152 m.w.N.

ff) Impersonation-Handlungen

Problematisch ist in Hinsicht auf die Strafbarkeit einiger Impersonation-Handlungen nach den §§ 186, 187 StGB, dass das bloße Schaffen kompromittierender Sachlagen (wenn die geäußerte Tatsachenaussage bei einem Dritten den Eindruck erweckt, dass sie vom Opfer selbst stammt) nicht ausreichend ist, da die Behauptung der Aussage durch den Täter im Verborgenen bleibt.[68] In Betracht kommt hingegen in solchen Fällen eine Strafbarkeit nach § 185 StGB, wenn das Opfer den Fake-Account selbst bemerkt oder von Dritten darauf aufmerksam gemacht wird und dadurch als gutgläubiges Werkzeug des Täters in seiner Ehre herabgesetzt wird.[69]

gg) Qualität der Beleidigung im Internet

Bei der Beurteilung von herabwürdigenden Äußerungen im Internet ist ein großzügiger Maßstab anzulegen, da die Sprache im Internet als plakativ und provokativ bezeichnet werden kann und das Internet sich auch nicht vorwiegend durch den Austausch von Höflichkeiten auszeichnet.[70] Es sind allerdings stets im Einzelfall die Kommunikationsstandards innerhalb eines Kommunikationsraumes festzustellen.[71] Eine Straflosigkeit aller Beleidigungen innerhalb eines Kommunikationsraums, in dem herablassende Unterhaltungen Usus sind, kommt allerdings nicht in Betracht.[72]

hh) Öffentliche Tatbegehung bei §§ 186, 187 StGB

Die §§ 186, 187 StGB enthalten einen Qualifikationstatbestand, der die öffentliche Tatbegehung zum Inhalt hat. Dieser ist aus cybermobbingspezifischer Sicht sehr bedeutsam.

Die Tat ist öffentlich begangen, wenn die Äußerung einer ehrrührigen Tatsache vor einem größeren, individuell nicht bestimmten Personenkreis getätigt wird.[73]

Unter Öffentlichkeit in Bezug auf das Internet versteht man die Bereiche des Internets, die für jedermann frei zugänglich sind.[74] Nicht-öffentlich im Internet sind damit Äußerungen, die nur an eine geschlossene Gruppe gerichtet sind.[75]

Die Qualifikation der öffentlichen Tatbegehung nimmt gerade deshalb in Bezug auf Cybermobbing eine wichtige Rolle ein, da ihr auch eine gewisse lückenfüllende Funktion zukommt, weil gerade die Variante der an eine unbestimmte Vielzahl von Personen gerichtete Übermittlung erfasst wird, die aufgrund fehlender körperlicher Weitergabe nicht unter den körperlichen Verbreitensbegriff[76] im Rahmen der Qualifikation der „Verbreitung von Schriften“ bei §§ 186, 187 StGB zu subsumieren ist (der internetspezifische Verbreitensbegriff[77] des *BGH* ist in der Literatur sehr umstritten[78]).[79]

Ein Streitentscheid kann im Rahmen dieser Schwerpunktseminararbeit allerdings hinsichtlich der lückenfüllenden Funktion der Qualifikation des öffentlichen Begehens dahinstehen.

---

68 *Eisele*, Strafrecht BT I, 5. Auflage (2019), Rn. 610 m.w.N.
69 Vgl. *BGH*, NStZ 1984, 216 (216); vgl. *Eisele* (Fn. 68), Rn. 610.
70 *Regge/Pegel*, in: MüKo-StGB, § 185 Rn. 10.
71 *Hilgendorf*, ZIS 2010, 208 (210) m.w.N.
72 *Hilgendorf/Valerius*, Rn. 354.
73 *Kindhäuser/Hilgendorf*, LPK-StGB, 8. Auflage (2020), § 186 Rn. 16.
74 *Heinrich*, ZJS 2016, 698 (708) m.w.N.
75 *Kindhäuser/Hilgendorf*, § 186 Rn. 17 m.w.N; vgl. *Fischer*, StGB, § 186 Rn. 19.
76 Hierzu *Heinrich*,ZJS, 2016, 569 (570) m.w.N.
77 BGHSt 47, 55 (59).
78 Kritisch z.B. *Doerbeck*, S. 158 ff.; *Heinrich*, ZJS 2016, 569 (578 ff.) m.w.N.
79 *Heinrich*, ZJS 2016, 698 (708) m.w.N.

ii) Angemessenheit der Rechtsfolgen

Problematisch im Hinblick auf Cybermobbing erscheinen allerdings die Rechtsfolgen der §§ 185 ff. StGB.

Wirft man einen Blick auf den Tatbestand des § 185 StGB, so sieht man, dass die einfache Beleidigung im Höchstmaß mit einem Jahr Freiheitsstrafe oder Geldstrafe bestraft wird. Die Qualifikation der tätlichen Beleidigung ist in Cybermobbingfällen irrelevant.

Festzustellen ist also, dass es für Cybermobbinghandlungen keinen einschlägigen Qualifikationstatbestand bezüglich der Beleidigung nach § 185 StGB gibt, obwohl die Beleidigung praktisch einen der wichtigsten Fälle in Bezug auf Cybermobbing darstellt.[80] Der cybermobbingspezifische Unrechtsgehalt ergibt sich in Bezug auf die §§ 185 ff. StGB aus den Faktoren der Ubiquität (weltweite Empfangbarkeit von Publikationen im Internet), der permanenten Verfügbarkeit von Publikationen im Internet und einer (Quasi-)Nicht-Eliminierbarkeit eben dieser, da sie nur schwerlich aus dem Internet zu löschen sind.[81] Besagter Unrechtsgehalt ist aus genannten Gründen deutlich höher als der Unrechtsgehalt, der einer einfachen Beleidigung außerhalb des Internets innewohnt. Das Strafmaß der einfachen Beleidigung nach § 185 StGB auf Beleidigungen im Rahmen von Cybermobbinghandlung anzuwenden ist daher nicht sachgerecht. Zudem sollte berücksichtigt werden, dass bei dem Phänomen des Cybermobbings nicht nur die bloßen Einzelhandlungen betrachtet werden dürfen, sondern auch dem Cybermobbingprozess als solchem strafrechtliche Beachtung geschenkt werden muss. Denn Cybermobbing zeichnet sich unter anderem durch seine Nachhaltigkeit und Perpetuierungswirkung aus.[82] Der hieraus entstehende zusätzliche Unrechtsgehalt muss im Strafmaß ebenfalls Berücksichtigung finden, was de lege lata im Rahmen des § 185 StGB nicht der Fall ist.[83] Hier besteht also Handlungsbedarf.

Die §§ 186, 187 StGB besitzen mit der Variante der öffentlichen Tatbegehung bereits eine Qualifikation, die in Cybermobbingfällen relevant ist, und deren Strafmaß bis zu zwei Jahren Freiheitsstrafe oder Geldstrafe im Falle einer üblen Nachrede und bis zu fünf Jahren oder Geldstrafe im Falle einer Verleumdung hergibt. Trotzdem bleibt hier zu diskutieren, ob dieser Strafrahmen (auch unter Berücksichtigung der teils erheblichen Folgen für Cybermobbingopfer, wie etwa starke psychische Beeinträchtigungen oder auch körperliche Belastungen[84]) zumindest moderat anzuheben ist. Auch hier muss Cybermobbing als Prozess Berücksichtigung finden.

h) Reformbedürftigkeit der §§ 185 ff. StGB

Nach den gewonnenen Erkenntnissen bleibt festzuhalten, dass es einer Reform des Beleidigungsstrafrechts bedarf. Erwähnenswert sind dabei insbesondere die Ansätze in dem Diskussionsentwurf des Bayerischen Staatsministeriums der Justiz (BayStMJ) zur Modernisierung der Beleidigungsdelikte sowie in dem von *Heckmann* und *Paschke* verfassten Gesetzesentwurf zur Verbesserung des Persönlichkeitsrechtsschutzes im Internet[85], worin ein von den Autoren entwickeltes Persönlichkeitsrechtsschutzgesetz (PRG) vorgestellt wird.

Nach dem Diskussionsentwurf des BayStMJ soll der § 188 StGB, der nach geltendem Recht die üble Nachrede und Verleumdung gegen Personen des politischen Lebens regelt, neu gefasst werden, dass er als Qualifikationstatbestand der §§ 185 ff. StGB fungiert und die „schwere Beleidigung", „schwere üble Nachrede" und „schwere Verleumdung" erfasst. Hierbei bleiben die Strafrahmen der Grundtatbestände (§§ 185 ff. StGB) unverändert, es

80 Vgl. *Eisenreich*, RuP 2020, 6 (8).
81 *Hilgendorf*, ZIS 2010, 208 (213).
82 *Heckmann/Paschke*, DRiZ 2018, 144 (146).
83 Vgl. hierzu *Eisenreich*, RuP 2020, 6 (8).
84 BayStMJ, Diskussionsentwurf zur Modernisierung der Beleidigungsdelikte, abrufbar unter: https://www.justiz.bayern.de/media/pdf/gesetze/diske_by_modernisierung_beleidigungsdelikte.pdf (zuletzt abgerufen am 4.10.2020), S. 13.
85 Abrufbar unter: https://www.arag.com/medien/pdf/presse/prg_gesetzentwurf_heckmann_paschke_konsolidiert.pdf (zuletzt abgerufen am 4.10.2020).

erfolgt lediglich eine Erweiterung der bereits bestehenden Qualifikationstatbestände um weitere (qualifizierte) Fallkonstellationen.[86] Aus cybermobbingspezifischer Sicht sind insbesondere Abs. 1 Nr. 1 und Nr. 4 des § 188 StGB-E interessant. Abs. 1 Nr. 1 führt eine Qualifikation der Beleidigung (§ 185 StGB) ein, „wenn die Tat öffentlich, in einer Versammlung oder durch Verbreiten von Schriften (§ 11 Abs. 3 [StGB]) begangen ist", die im Strafrahmen mit bis zu zwei Jahren Freiheitsstrafe oder Geldstrafe geahndet wird. Insofern wurde die Qualifikation des § 187 StGB übernommen und der Strafrahmen der qualifizierten üblen Nachrede (§ 186 StGB) für die „schwere Beleidigung" gewählt. Dies stellt eine moderate Strafmaßanhebung unter Orientierung an bekannten Maßstäben dar und ist daher, insbesondere unter dem Gesichtspunkt der zuvor bereits erläuterten Notwendigkeit einer Qualifikation für § 185 StGB, gutzuheißen.

§ 188 Abs. 1 Nr. 4 StGB-E stellt eine weitere Fallkonstellation der „schweren Beleidigung" dar, die vorliegt, „wenn die Tat Bestandteil einer über längere Zeit fortgesetzten erheblichen und systematischen Belästigung der beleidigten Person ist". Erfasst werden soll hiermit unter anderem das Phänomen des Cybermobbings, das „durch eine fortgesetzte und systematische Beleidigung gekennzeichnet [ist]"[87]. *Eisenreich* spricht davon, dass es für eine angemessene strafrechtliche Ahndung nicht ausreiche, einzelne Beleidigungstaten herauszugreifen, um Cybermobbing wirkungsvoll entgegenzutreten.[88] Dafür brauche es einen eigenen Qualifikationstatbestand.[89] Auch wenn die Intention, die mit § 188 Abs. 1 Nr. 4 StGB-E verbunden ist, nachvollziehbar ist, so ist zu kritisieren, dass für eine einzelne öffentliche Beleidigung (egal ob sie im Internet erfolgt oder nicht) nach diesem Entwurf der gleiche Strafrahmen angesetzt würde, wie für eine Beleidigung, die sich als Bestandteil von Cybermobbing darstellt und somit als Cybermobbinghandlung zu qualifizieren ist. Bei einer solchen besteht aber wohl regelmäßig ein höherer Unrechtsgehalt, aufgrund der Nachhaltigkeit und Perpetuierungswirkung[90] des Cybermobbings und die nicht unerheblichen Folgen[91] für Cybermobbingopfer. Insofern scheint es bedenklich, den der Beleidigung im Rahmen des Cybermobbings innewohnenden Unrechtsgehalt und das damit verbundene Ausmaß der Höchststrafe mit dem einer einzelnen öffentlich getätigten Beleidigung im Sinne des § 188 Abs. 1 Nr. 1 StGB-E gleichzusetzen. So wird dem erhöhten Unrechtsgehalt des Cybermobbingprozesses nicht ausreichend Rechnung getragen. Das Strafmaß einer Beleidigung im Sinne des § 185 StGB sollte in solch qualifizierten Fällen der Beleidigung höher angesetzt werden als bei einzelnen öffentlich getätigten Beleidigungen. Anzumerken ist hierbei, dass § 188 Abs. 1 Nr. 4 StGB-E nicht ausschließlich der Erfassung des Cybermobbings gewidmet ist, sondern vielmehr der Erfassung von Mobbing in seinen verschiedenen Erscheinungsformen dienen soll (also auch dem „klassischen" Mobbing außerhalb des Internets).[92] Dies stellt ein Problem dar, da mit dem Cybermobbing durch die zuvor eingehend beschriebenen Faktoren regelmäßig ein höherer Unrechtsgehalt einhergeht als mit „klassischem" Mobbing. Daher sollte hier auch (zumindest im Strafmaß) eine Abgrenzung stattfinden.

Insofern wäre auch die Einordnung einer speziellen Cybermobbing-Konstellation im Rahmen des § 188 StGB-E anzudenken; die Subsumtion und Erfassung von Cybermobbing unter Abs. 1 Nr. 4 erscheint aus den dargelegten Gründen systematisch unangebracht.

§ 188 Abs. 2 StGB-E normiert die „schwere üble Nachrede", § 188 Abs. 3 StGB-E die „schwere Verleumdung". Abs. 2 und 3 verweisen jeweils auf das Vorliegen der Voraussetzungen der Nummern 1, 2, 3 oder 4 des Abs. 1. Die Strafrahmen dieser Absätze (bis zu drei Jahren Freiheitsstrafe oder Geldstrafe bei Abs. 2 und drei Monate bis

86 *Eisenreich*, RuP 2020, 6 (7).
87 *Eisenreich*, RuP 2020, 6 (8).
88 *Eisenreich*, RuP 2020, 6 (8).
89 *Eisenreich*, RuP 2020, 6 (8).
90 *Heckmann/Paschke*, DRiZ 2018, 144 (146).
91 BayStMJ, S. 13.
92 Vgl. BayStMJ, S. 12 f.

fünf Jahre Freiheitsstrafe bei Abs. 3) sind, soweit man sich an dem qualifizierten Strafmaß bei öffentlicher Tatbegehung bei den §§ 186, 187 StGB de lege lata orientiert, ungeachtet der Kritik an einer ausbaufähigen Würdigung des durch Cybermobbing verwirklichten Unrechts im Strafrahmen bezüglich einer Beleidigung im Sinne des § 185 StGB als angemessen anzusehen.

Es soll noch Erwähnung finden, dass dieser Diskussionsentwurf (wie aufgezeigt) keinen eigenen Cybermobbing-Straftatbestand etablieren möchte.

Der Gesetzesentwurf von *Heckmann* und *Paschke* ist vergleichsweise anders aufgebaut. Der wohl gravierendste Unterschied liegt darin, dass besagter Gesetzesentwurf mit § 190 StGB-E einen speziellen Cybermobbing-Straftatbestand, namentlich die „besonders schwere Ehrverletzung im Internet", vorschlägt.[93] Gemäß § 190 StGB-E wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft, „wer einen ehrverletzenden Inhalt [§§ 185 bis 187] im Internet zugänglich macht, dass dieser von einer erheblichen Anzahl von Personen wahrgenommen werden kann, wenn die Tat geeignet ist, das Opfer in seiner Lebensgestaltung schwerwiegend zu beeinträchtigen". Anders als in dem Diskussionsentwurf des *BayStMJ* wird hier Rücksicht auf den Unrechtsgehalt genommen, der dem Cybermobbing als Prozess und den teils erheblichen Folgen für die Opfer innewohnt. Angesichts dieser Anknüpfung an die Voraussetzung der Eignung zur schwerwiegenden Beeinträchtigung der Lebensgestaltung erscheint das Strafmaß auch als angemessen. § 190 StGB-E Abs. 2 sieht bei leichtfertiger Verursachung der Selbsttötung des Opfers eine Freiheitsstrafe bis zu fünf Jahren vor. Eine bloße Geldstrafe ist nach § 190 Abs. 2 StGB-E ausgeschlossen. Auch dies erscheint im Hinblick auf den Opferschutz und auch aus Präventionsaspekten angemessen, da hierdurch eine gewisse Abschreckungswirkung oder Sensibilisierung auf Täterseite hervorgebracht wird.

Insgesamt erscheint der Gesetzesentwurf von *Heckmann* und *Paschke* somit vorzugswürdig.

Auf die Frage, ob die Einführung eines eigenen Cybermobbing-Straftatbestands tatsächlich notwendig ist, wird an späterer Stelle eingegangen.

2. Verletzung des persönlichen Lebens- und Geheimbereichs (§ 201 ff. StGB, § 33 KUG i.V.m. §§ 22 f. KUG)

Denkbar in Bezug auf Cybermobbingfälle ist auch die Verwirklichung der Straftatbestände der §§ 201, 201a StGB sowie § 33 KUG i.V.m. §§ 22 f. KUG.

a) Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen (§ 201a StGB)

Stellt ein Täter Bildaufnahmen des Opfers her oder überträgt solche, könnte § 201a StGB einschlägig sein.

Schutzgut des § 201a StGB ist das Recht am eigenen Bild, welches als Ausprägung des in der Verfassung geregelten Rechts auf informationelle Selbstbestimmung (Ausprägungsform des allgemeinen Persönlichkeitsrechts nach Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG[94]) angesehen werden kann, allerdings auf den höchstpersönlichen Lebensbereich eingegrenzt ist, wobei sich der Begriff des „höchstpersönlichen Lebensbereichs" dabei an dem der „Intimssphäre" orientieren kann.[95] § 201a Abs. 1 Nr. 1 StGB ist nur einschlägig, wenn sich die aufgenommene Person in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet. Für einen „besonders geschützten Raum" muss ein dauerhafter oder vorübergehender Sichtschutz bestehen, öffentlich zugängliche

93 Vgl. *Heckmann/Paschke*, DRiZ 2018, 144 (145).
94 *Di Fabio* in: Maunz/Dürig, GG, 90. EL (2020), Art. 2 I GG Rn. 173 ff. m.w.N.
95 *Graf*, in: MüKo-StGB, § 201a Rn. 10 m.w.N.

Räume stellen dabei keine Räumlichkeiten im oben genannten Sinne dar.[96] Klassenzimmer, Vorlesungsräume und Lehrerzimmer sind grundsätzlich (beschränkt) öffentlich zugängliche Räume und daher keine „besonders geschützten Räume“ im Sinne des § 201a Abs. 1 Nr. 1 StGB.[97] Der Anwendungsbereich des Abs. 1 Nr. 1 erstreckt sich in Fällen des Cybermobbings also eher auf heimliche Anfertigungen von Bildaufnahmen des Opfers, wie etwa durch das Nutzen der Webcam des Opfercomputers, da es nicht darauf ankommt, von welchem Ort aus die Tat begangen wird.[98]

§ 201a Abs. 1 Nr. 2 StGB bestraft die unbefugte Herstellung oder Übertragung von Bildaufnahmen, die die Hilflosigkeit einer anderen Person zur Schau stellt und besitzt daher auch für Cybermobbingfälle Relevanz, in denen etwa Personen in Rauschzuständen[99] oder Prügelattacken[100] aufgenommen oder übertragen werden.

§ 201a Abs. 1 Nr. 3 StGB stellt auch das Gebrauchen oder das einer dritten Person Zugänglichmachen einer Bildaufnahme nach Nr. 1 und 2 unter Strafe. Ein Gebrauchen liegt bei jeder Nutzung der Bildaufnahme vor.[101] Unter Zugänglichmachung versteht man jede Ermöglichung einer Kenntnisnahme oder eines Zugriffs durch Dritte.[102]

§ 201a Abs. 1 Nr. 4 StGB regelt die wissentlich unbefugte Zugänglichmachung einer befugt hergestellten Bildaufnahme. Das Erfordernis der Wissentlichkeit von der Unbefugtheit der Weitergabe zur Erfüllung des subjektiven Tatbestands (dolus directus 1. Grades) schränkt jedoch den Anwendungsbereich ein.[103]

Große Bedeutung in cybermobbingspezifischer Hinsicht kommt § 201a Abs. 2 StGB zu, nach dem bestraft wird, wer unbefugt eine Bildaufnahme von einer anderen Person, die geeignet ist, dem Ansehen der abgebildeten Person erheblich zu schaden, einer dritten Person zugänglich macht. Gefordert wir hier also keine Verletzung des höchstpersönlichen Lebensbereichs. Vielmehr werden bloßstellende Bildaufnahmen erfasst, „die Personen in Zuständen oder Situationen zeigen, die nach allgemeiner gesellschaftlicher Bewertung als eklig, peinlich, minderwertig oder unfreiwillig angesehen werden und bei denen üblicherweise ein Interesse besteht, dass diese Dritten nicht zugänglich gemacht werden“[104]. Daher besteht hier ein großer Anwendungsbereich für Cybermobbingfälle. Ob auch bearbeitete Bildaufnahmen, die eben nur durch ihre Bearbeitung die Eignung erlangt haben, dem Ansehen des Opfers erheblich zu schaden, § 201a Abs. 2 StGB erfüllen können, ist in der Rechtsprechung noch nicht geklärt, wird in der Literatur allerdings zum Teil bejaht.[105]

b) Verletzung der Vertraulichkeit des Wortes (§ 201 StGB)

Enthält eine Videoaufnahme eine entsprechende Tonspur oder wird eine sprachliche Äußerung aus Internetchats weitergegeben, so könnte auch § 201 StGB einschlägig sein.[106]

Vom Tatbestand erfasst wird jedes nichtöffentlich gesprochene Wort eines anderen, also jedes kundgetane Wort, das „nicht an die Allgemeinheit gerichtet und nicht über einen durch persönliche oder sachliche Beziehung abgegrenzten Personenkreis hinaus ohne Weiteres wahrnehmbar ist“[107]. Tathandlungen sind das Aufnehmen auf einen

96 *Doerbeck*, S. 169 m.w.N.
97 A.a.O.
98 A.a.O.
99 *Fischer*, StGB, § 201a Rn. 10a.
100 *Eisele/J. Sieber*, StV 2015, 312 (314).
101 *Valerius*, in: LK-StGB, § 201a Rn. 24.
102 *Eisele* (Fn. 68), Rn. 712.
103 Vgl. *Mitsch*, Medienstrafrecht, 2012, § 3 Rn. 107.
104 *Doerbeck*, S. 181 m.w.N.
105 Siehe etwa *Doerbeck*, S. 184.
106 *Cornelius*, ZRP 2014, 164 (165).
107 *Cornelius*, ZRP 2014, 164 (165) m.w.N.

Tonträger (Abs. 1 Nr. 1) beziehungsweise das Gebrauchen einer so hergestellten Aufnahme oder die Zugänglichmachung dieser (Abs. 1 Nr. 2). Tonträger in diesem Sinne können auch die Speichermedien der digitalen Aufzeichnungstechniken, aber auch die (im Hinblick auf Cybermobbing wichtigen) sonstigen elektronischen Geräte mit dieser Technik sein, wie etwa Smartphones.[108] Somit ist die Aufnahme des nichtöffentlichen Wortes sowie die Zugänglichmachung einer so hergestellten Aufnahme im Cyberspace durch § 201 Abs. 1 Nr. 1 StGB im ersten beziehungsweise durch § 201 Abs. 1 Nr. 2 StGB im zweiten Fall geschützt.[109]
Da nur das gesprochene Wort erfasst ist, sind Äußerungen in elektronischer Textform nicht vor einer Weitergabe geschützt.[110]

c) Recht der Selbstdarstellung (§ 33 KUG i.V.m. §§ 22 f. KUG)

Außerdem könnte § 33 KUG i.V.m. §§ 22 f. KUG bei einigen Cybermobbinghandlungen einschlägig sein.
§ 33 KUG bestraft denjenigen, der entgegen den §§ 22, 23 KUG ein Bildnis verbreitet oder öffentlich zur Schau stellt.
Nicht erfasst wird damit das Herstellen eines Bildnisses. Unter einem Bildnis im Sinne des § 22 KUG versteht man eine Abbildung, die die äußere Erscheinung einer Person erkennbar wiedergibt.[111] Die Verbreitung kann auch in Form der Übermittlung von Bilddateien mittels elektronischer Kommunikation erfolgen, sofern die tatsächliche Verfügungsgewalt über die Bilddaten durch einen Dritten erlangt wird.[112] Die Tatbestandsvariante des „öffentlichen Zur-Schau-Stellens“ greift im Übrigen bei einer Verbreitung über den allgemein zugänglichen Bereich des Internets.[113]
Abschließend ist festzustellen, dass § 33 KUG im Unterschied zu § 201a StGB auch die Abbildung bloßer (einzelner) Körperteile erfasst, und die Art der Herstellung des Bildnisses keine Rolle spielt.[114]

3. Straftaten gegen die persönliche Freiheit (§§ 238 ff. StGB)

Die §§ 238, 240, 241 StGB schützen das Rechtsgut der persönlichen Freiheit.[115] Einige Cybermobbinghandlungen könnten dieses Rechtsgut beeinträchtigen.

a) Nachstellung (§ 238 StGB)

Mit dem Tatbestandsmerkmal der „Beharrlichkeit“ der Nachstellung enthält § 238 StGB ein auch für Cybermobbing „typisches Dauerelement“[116].
Insbesondere § 238 Abs. 1 Nr. 2 StGB normiert eine Nachstellung unter Verwendung von Telekommunikationsmitteln, unter die auch die für Cybermobbing genutzten Medien fallen.[117] So kann diese Tatbestandsvariante in

[108] *Graf*, in: MüKo-StGB, § 201 Rn. 20.
[109] *Cornelius*, ZRP 2014, 164 (165) m.w.N.
[110] *Cornelius*, ZRP 2014, 164 (165) m.w.N.
[111] *Kaiser*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 231. EL (Stand: Juli 2020), § 33 KUG Rn. 5 m.w.N.
[112] *Kaiser*, in: Erbs/Kohlhaas, § 33 KUG Rn. 10 m.w.N.
[113] *Cornelius*, ZRP 2014, 164 (166).
[114] *Cornelius*, ZRP 2014, 164 (166) m.w.N.
[115] *Wieck-Noodt*, in: MüKo-StGB, Vor § 232 Rn. 1.
[116] *Cornelius*, ZRP 2014, 164 (166).
[117] *Doerbeck*, S. 195 m.w.N.

Cybermobbingfällen durch Formen des Online Harassments, wie etwa dem Belästigen, Schikanieren oder Beleidigen des Opfers durch SMS, E-Mails etc., erfüllt sein.[118] Nicht erfüllt ist sie allerdings nach herrschender Meinung, wenn keine Kommunikation zwischen Opfer und Täter erfolgen soll, wie etwa bei einseitigen Kommunikationsvorgängen, bei denen es dem Täter nicht notwendigerweise um eine Antwort oder eine Reaktion des Opfers geht, wodurch nur § 238 Abs. 1 Nr. 5 StGB als Auffangtatbestand in Frage kommt.[119]

§ 238 Abs. 1 Nr. 3 StGB, der als Tatbestandsmerkmal die missbräuchliche Verwendung von personenbezogenen Daten des Opfers enthält, kann durch Impersonation-Handlungen des Täters erfüllt werden.[120]

§ 238 Abs. 1 Nr. 4 StGB enthält eine Drohung als Merkmal. Diese Tatbestandsvariante kann durch Cybermobbinghandlungen des Online Harassments ohne Probleme erfüllt werden.[121]

Wichtig ist bei allen Tatbestandsvarianten, dass das Kriterium der Beharrlichkeit im Sinne des § 238 StGB erfüllt ist.

Für die Annahme eines beharrlichen Nachstellens ist ein zeitlicher und innerer Zusammenhang zwischen den einzelnen Handlungen notwendig.[122] Es erfordert also mehrere Cybermobbinghandlungen, wodurch § 238 StGB nur durch Cybermobbing als Gesamtgeschehen verwirklicht werden kann.[123]

Problematisch hierbei ist allerdings, dass die Beharrlichkeit ein besonderes persönliches Merkmal im Sinne des § 28 StGB darstellt, weshalb es auch bei einer arbeitsteiligen Arbeitsweise bei mehreren Tätern (was beim Cybermobbing nicht ungewöhnlich ist) bei jedem Einzelnen vorliegen muss, weshalb es in diesen Fällen an der Beharrlichkeit fehlen kann.[124]

Die Qualifikation des § 238 Abs. 2 StGB scheidet aufgrund des nach der herrschenden Meinung erforderlichen Vorsatzes des Täters hinsichtlich des Gefahrenerfolgs in Cybermobbingfällen wohl häufig aus.[125]

§ 238 Abs. 3 StGB enthält eine Erfolgsqualifikation hinsichtlich der Verursachung des Todes einer der in Abs. 2 genannten Personen durch den Täter. Fraglich ist hier im Hinblick auf Cybermobbing, ob dem Täter auch der Tod des Opfers durch Suizid zugerechnet werden kann.

Grundsätzlich muss der Täter hierfür den Suizidwillen des Opfers voraussehen können und das Opfer darf nicht freiverantwortlich gehandelt haben.[126] Ein Handeln, das nicht frei verantwortlich ist, liegt jedenfalls dann vor, wenn die Tathandlungen des § 238 StGB ursächlich für eine psychische Erkrankung des Opfers sind, die den Umstand der Unfreiheit begründet, wodurch eine Zurechnung möglich ist.[127] Verlangt wird darüber hinaus ein spezifischer Gefahrzusammenhang zwischen der Nachstellung und dem Tod des Opfers.[128] Dieser ist bei § 238 Abs. 3 StGB bereits dann gegeben, wenn die Motivation für das Verhalten des Opfers auf die Grundtatbestandsverwirklichung zurückzuführen ist und eben diese für das selbstschädigende Verhalten des Opfers handlungsleitend war.[129]

In diesen Fällen kommt § 238 Abs. 3 StGB auch bei Cybermobbing in Betracht.

118 *Doerbeck*, S. 195.
119 *Doerbeck*, S. 195 m.w.N.
120 Hierzu ausführlich: *Doerbeck*, S. 195 f. m.w.N.
121 *Doerbeck*, S. 197 m.w.N.
122 BT-Drs. 16/575, S. 7.
123 *Doerbeck*, S. 198.
124 *Cornelius*, ZRP 2014, 164 (166).
125 *Doerbeck*, S. 198.
126 *Doerbeck*, S. 200 m.w.N.
127 *Doerbeck*, S. 201 m.w.N.
128 BGHSt 62, 49 (55).
129 BGHSt 62, 49 (57).

b) Nötigung und Bedrohung (§§ 240, 241 StGB)

Hinsichtlich § 240 Abs. 1 StGB findet die Tatbestandsvariante der Gewalt als Nötigungsmittel in Fällen von Cybermobbing eher geringe Bedeutung, da der Täter hierfür die durch seine Cybermobbinghandlungen beim Opfer hervorgebrachten körperlichen Zwangswirkungen (wie etwa psychosomatische Folgen für das körperliche Wohlbefinden) mit in seinen Vorsatz aufnehmen müsste, was wohl in der Regel nicht der Fall beziehungsweise nicht nachzuweisen ist.[130]
Im Übrigen kann die Tatbestandsvariante der Drohung mit einem empfindlichen Übel durch Online Harassment-Handlungen erfüllt werden.
Hinsichtlich § 241 StGB ergeben sich keine cybermobbingspezifischen Besonderheiten, auch diese Norm kann durch Online Harassment-Handlungen erfüllt werden.

4. Straftaten gegen das Leben (§§ 211 ff. StGB)

Fraglich ist, ob bei einem Suizid des Cybermobbingopfers die §§ 211 ff. StGB einschlägig sind.

a) Totschlag (§ 212 StGB)

Der § 212 Abs. 1 StGB setzt als Tathandlung die Tötung eines anderen Menschen voraus. Der Suizid des Opfers ist damit nicht als teilnahmefähige Haupttat anzusehen.[131] Allerdings wäre in diesen Fällen eine Tatbegehung in mittelbarer Täterschaft denkbar.[132] Der Täter muss dabei als Hintermann den Tatverlauf beherrschen[133] und das Opfer darf nicht freiverantwortlich handeln[134]. Im Falle eines Suizids muss der Täter im Rahmen des subjektiven Tatbestands erkennen, dass die Möglichkeit einer nicht freiverantwortlichen Begehung eines Suizids auf Opferseite besteht.[135] In Cybermobbingfällen wird es wohl oftmals an diesem Vorsatz mangeln, da der Suizid des Opfers „kein typisches Ziel der Cybermobbingtäter ist“[136] und die Täter die Selbstmordgedanken des Opfers aufgrund fehlender Offenbarung im Internet wohl in der Regel nicht erkennen.[137]
Es bleibt festzuhalten, dass § 212 StGB zwar vom Grundsatz her auf Cybermobbingfälle anwendbar ist, eine Strafbarkeit allerdings in der Regel auf der Ebene des subjektiven Tatbestands scheitern wird.

b) Mord (§ 211 StGB)

Die Ausführungen zu § 212 StGB gelten entsprechend. Anzumerken ist, dass (wenn überhaupt) in besonderen Fällen des Cybermobbings einzig das Mordmerkmal der „sonst niedrigen Beweggründe“ nach § 211 Abs. 2 1. Gruppe Var. 4 StGB einschlägig sein könnte.[138]

130 *Doerbeck*, S. 208 m.w.N.
131 BGHSt 2, 150 (151 f.).
132 *Kühl*, in: Lackner/Kühl, StGB, Vor § 211 Rn. 9.
133 *Fischer*, StGB, Vor § 211-217 Rn. 20 f.
134 *Fischer*, StGB, Vor § 211-217 Rn. 22.
135 *Eser/Sternberg-Lieben*, in: Schönke/Schröder, StGB, Vor § 211 Rn. 37.
136 *Doerbeck*, S. 222 m.w.N.
137 A.a.O.
138 *Doerbeck*, S. 222.

c) Fahrlässige Tötung (§ 222 StGB)

Scheitert eine Strafbarkeit nach den §§ 211, 212 StGB, so kommt jedenfalls noch eine Strafbarkeit nach § 222 StGB in Betracht. Diese kann allerdings „an der Vorhersehbarkeit der suizidalen Gedanken des Betroffenen scheitern“[139].

5. Straftaten gegen die körperliche Unversehrtheit (§§ 223 ff. StGB)

Wirken sich Cybermobbinghandlungen des Täters auf das körperliche Wohlbefinden oder die Gesundheit des Opfers aus, ist an die §§ 223 ff. StGB zu denken.
Problematisch in cybermobbingspezifischer Hinsicht ist allerdings, dass § 223 StGB zwar bei Cybermobbinghandlungen, die beim Opfer körperliche Folgen hervorrufen, aber nach noch herrschender Ansicht nicht bei rein psychischen Beeinträchtigungen des Opfers durch die Cybermobbinghandlungen angewendet werden kann.[140]
Bezüglich des Schutzes der Psyche besteht somit eine Strafbarkeitslücke.[141]
Außerdem wird in Fällen des Cybermobbings wohl häufig der Tätervorsatz hinsichtlich des Körperverletzungserfolgs fehlen, da die Täter die Cybermobbinghandlungen in der Regel als nicht besonders schwerwiegend betrachten werden.[142]
Größere Bedeutung im Rahmen des Cybermobbings könnte daher dem § 229 StGB zukommen. Er „kommt in Betracht, wenn der Täter zwar nicht vorsätzlich hinsichtlich der gesundheitlichen Folgen handelt, diese aber hätte erkennen können“[143]. Scheitern kann es allerdings wie bei § 222 StGB auch hier an der Vorhersehbarkeit des Erfolgs, die wohl in der Regel nicht bereits zu Beginn des Cybermobbingverlaufs gegeben sein wird.[144]

6. Fazit

Das Phänomen des Cybermobbings wird de lege lata von vielen Strafvorschriften des StGB erfasst, vorwiegend jedoch durch seine einzelnen Cybermobbinghandlungen und weniger durch den Gesamtprozess des Cybermobbings. Strafbarkeitslücken haben sich hinsichtlich des Anfertigens von Video- oder Bildaufnahmen (soweit sie nicht den höchstpersönlichen Lebensbereich des Opfers betreffen), dem Schutz der psychischen Verfassung des Opfers und der Erfassung des Gesamtunrechtsgehalts des Cybermobbingprozesses ergeben. Strafbarkeitsprobleme bestehen außerdem bei den §§ 223 ff. StGB und §§ 211 ff. StGB.

III. Notwendigkeit eines Cybermobbing-Straftatbestands

Es soll nicht unerwähnt bleiben, dass man in Bezug auf Cybermobbing noch an die §§ 184 ff. StGB, § 253 StGB, § 111 StGB oder die §§ 130 ff. StGB denken könnte. Festzustellen ist also, dass der strafrechtliche Schutz vor Cybermobbing bereits de lege lata nicht ins Leere läuft. Trotzdem wurden Strafbarkeitslücken (insbesondere im Beleidigungsstrafrecht) offenbart. So wird das Cybermobbing vorwiegend durch seine Einzelhandlungen erfasst,

139 *Doerbeck*, S. 225 m.w.N.
140 *Doerbeck*, S. 232.
141 *Doerbeck*, S. 328.
142 *Doerbeck*, S. 232 m.w.N.
143 *Doerbeck*, S. 240 m.w.N.
144 *Doerbeck*, S. 232 m.w.N.

wobei der Unrechtsgehalt, der dem Cybermobbing als Gesamtgeschehen innewohnt, keine Berücksichtigung findet. Auch den erheblichen (insbesondere psychischen) Folgen für Cybermobbingopfer bis hin zum Suizid wird nicht ausreichend Rechnung getragen, wie auch nicht den Besonderheiten des Internets (enorme Reichweite, schwere Löschbarkeit von Inhalten, schnelle Verbreitung von Informationen etc.).

Fest steht damit, dass strafrechtlicher Handlungsbedarf hinsichtlich des Cybermobbings besteht.

Zu diskutieren ist daher, ob die Notwendigkeit eines eigenen Cybermobbing-Straftatbestands besteht oder ob eine anderweitige strafrechtliche Reform (insbesondere des Beleidigungsstrafrechts) ausreicht beziehungsweise vorzugswürdig ist.

Die Bundesregierung lehnt die Schaffung eines eigenen Cybermobbing-Tatbestands aus dem Grund ab, dass die Heterogenität der zu erfassenden Lebenssachverhalte große Probleme aufwerfe.[145] Gemeint ist damit die Problematik, die Komplexität der verschiedenen Handlungsformen des Cybermobbings in nur einem Straftatbestand vollständig zu erfassen und dieser gerecht werden zu können. Die nach aktueller Gesetzeslage in Frage kommenden Straftatbeständen würden eine weitaus flexiblere und situationsgerechtere Reaktion auf Mobbing erlauben.[146]

Der *Bundesregierung* ist hinsichtlich ihrer Argumente der Komplexität und Flexibilität dahingehend zuzustimmen, als dass das Cybermobbing in seinen komplexen Formen nicht durch eine einzelne Strafnorm vollständig erfasst und definiert werden kann. Was die *Bundesregierung* allerdings nicht in Betracht zieht, ist der Umstand, welche Außenwirkung ein möglicher Cybermobbing-Straftatbestand haben könnte. So wurde etwa in Österreich mit dem § 107c StGB-Ö ein solcher eingeführt, womit „ein klares Signal gesendet [wurde], dass in der dargestellten Begehungsform ein besonderer Unrechtsgehalt liegt, der mit jenem der Grundtatbestände in den §§ 185 ff. StGB nicht ausreichend abgedeckt ist“[147]. Zudem war es gerade die Intention, dass nicht nur Teilakte von Cybermobbing, sondern auch der Unrechtsgehalt von Cybermobbing in der Gesamtheit erfasst werden sollte.[148] Dies spiegelt also auch die strafrechtliche Problemstellung in Deutschland wieder. Anzudenken wäre also, einen Cybermobbing-Straftatbestand in Deutschland an § 238 StGB anzulehnen[149], um eben das Cybermobbing als Gesamtgeschehen zu erfassen und nicht nur dessen Teilakte. Insbesondere ist hier an eine Übernahme des Tatbestandsmerkmals der „Eignung zur schwerwiegenden Beeinträchtigung der Lebensgestaltung“ im Sinne des § 238 StGB zu denken. Dieses liegt vor, wenn die Freiheit menschlicher Entschlüsse und Handlungen durch die Handlungen des Täters oder der Täter dadurch beeinträchtigt wird, dass es zu einer erzwungenen Veränderung der bisherigen Lebensumstände des Opfers oder der Opfer kommt, die zumindest zu einer Einbuße von Lebensqualität führt.[150] Unter „schwerwiegenden Beeinträchtigungen“ versteht man solche, die im Einzelfall objektivierbar gravierend, gewichtig und ernst zu nehmen sind.[151] Ähnlich ist es in § 107c StGB-Ö bereits vorzufinden. Betrachtet man den § 107c Abs. 1 StGB-Ö, so findet man dort das tatbestandsmerkmal der Eignung (der Tat), „eine Person in ihrer Lebensweise unzumutbar zu beeinträchtigen“. Für eine Übernahme des besagten Tatbestandsmerkmals aus § 238 StGB in einen eigenen Cybermobbing-Straftatbestand spräche, dass das Tatbestandsmerkmal der „Eignung zur schwerwiegenden Beeinträchtigung der Lebensgestaltung“ im Sinne des § 238 StGB für die Opfer von Cybermobbing eine Vorverlagerung des strafrechtlichen Schutzes aufgrund einer Ausgestaltung als Eignungsdelikt bedeuten würde, der angesichts der in dieser Schwerpunktseminararbeit dargelegten teils schweren und erheblichen

145 BT-Drs. 19/6174, S. 5.
146 *Doerbeck*, S. 328.
147 *Heckmann/Paschke*, DRiZ 2018, 144 (145).
148 *Heckmann*/Paschke, DRiZ 2018, 144 (146).
149 So auch *Heckmann/Paschke* in ihrem Gesetzesentwurf (vgl. Fn. 85).
150 *Gericke*, in: MüKo-StGB, § 238 Rn. 47 m.w.N.
151 *Gericke*, in: MüKo-StGB, § 238 Rn. 49 m.w.N.

Folgen für die Opfer auch als angemessen erscheinen würde. Ob auch das Tatbestandsmerkmal der „Beharrlichkeit“ im Sinne des § 238 StGB in einen Cybermobbing-Straftatbestand aufgenommen werden sollte, erscheint indes zweifelhaft. Hierunter versteht man nicht nur ein wiederholendes Verhalten des Täters oder der Täter, vielmehr muss die Tat mit einer gewissen Hartnäckigkeit ausgeführt werden, bei der der Täter oder die Täter aus Missachtung des entgegenstehenden Willens des Opfers oder aus Gleichgültigkeit gegenüber den Wünschen des Opfers willentlich hinsichtlich eines auch in Zukunft immer wiederkehrenden entsprechenden Verhaltens handeln müssen.[152] Zwar erscheint es sinnvoll, das Element der „sich wiederholenden Begehungsweise“ in einen Cybermobbing-Straftatbestand aufzunehmen, da sich das Cybermobbing ja gerade, wie unter I. 1. festgestellt, unter anderem durch sich wiederholende Handlungen über einen längeren Zeitraum hinweg auszeichnet, jedoch ist zumindest unter dem Gesichtspunkt des Opferschutzes beim Cybermobbing zweifelhaft, ob über eine tatbestandliche Voraussetzung der „Eignung der Tat zur schwerwiegenden Beeinträchtigung der Lebensgestaltung des Opfers“ in Verbindung mit einer „sich wiederholenden Tatbegehungsweise“ hinaus auch noch eine gewisse „Hartnäckigkeit“ des Täters oder der Täter gefordert werden sollte. Angesichts der Anforderungen, die bereits an eine „schwerwiegende Beeinträchtigung“ gestellt werden und unter der Voraussetzung der Aufnahme des Tatbestandsmerkmals der „sich wiederholenden Tatbegehungsweise“ in einen Cybermobbing-Straftatbestand, könnte das Element der „Hartnäckigkeit“ für einen Cybermobbing-Straftatbestand entfallen. Inhaltlich müsste zudem eine Bezugnahme insbesondere zu den Ehrschutzdelikten (§§ 185 ff. StGB) und zu den §§ 201, 201a StGB erfolgen, die, wie aufgezeigt, eine wichtige Bedeutung in Hinblick auf Cybermobbing haben. Hier müssten die Strafrahmen der Grunddelikte angehoben werden. In einem Cybermobbing-Straftatbestand bestünde ebenfalls die Notwendigkeit der Benennung der Tatmittel, über deren Benutzung oder Verwendung durch den oder die Täter der tatbestandliche Erfolg überhaupt erst herbeigeführt werden könnte. Hier könnte auf die unter I. 1. herausgearbeitete Definition von Cybermobbing Bezug genommen werden. Als Tatmittel kämen für einen Cybermobbing-Straftatbestand somit die moderne Informations- und Telekommunikationstechnik in Betracht. Die Signalwirkung eines Cybermobbing-Straftatbestandes nach außen könnte dabei die Menschen für das Phänomen des Cybermobbings sensibilisieren und mit erhöhter Strafandrohung diesem auch präventiv entgegenwirken. Unabhängig davon, dass es aus den weiter oben genannten Gründen nicht möglich ist, das Cybermobbing in seinen komplexen Formen in einer einzelnen Strafnorm zu erfassen, besteht somit auch gar nicht die Notwendigkeit hierzu. Die besagte Signalwirkung würde auch bei einem Cybermobbing-Straftatbestand erreicht werden, der inhaltlich „nur“ auf die Tatbestände der Ehrschutzdelikte, der §§ 201, 201a StGB sowie die herausgearbeiteten Tatbestandsmerkmale des § 238 StGB und die besagten Tatmittel Bezug nimmt, durch die viele Cybermobbinghandlungen allerdings bereits erfasst werden könnten. Ein weiterer Vorteil eines eigenen Cybermobbing-Straftatbestands wäre die Möglichkeit, diesen als Offizialdelikt auszugestalten, was zur Entlastung der Opfer (die meist psychisch bereits sehr belastet sind) beitragen würde, da die Opfer nicht noch zusätzlich einen Strafantrag zwingend stellen müssten. Die Strafverfolgung würde hierdurch erleichtert beziehungsweise gewährleisten werden können. Zu überlegen wäre auch, innerhalb eines neuen Cybermobbing-Straftatbestands eine Erfolgsqualifikation mit erhöhter Strafdrohung einzuführen, die eingreift, wenn durch die Tathandlung der Tod des Opfers verursacht wird.

Aufgrund der dargelegten Gründe, ist die Einführung eines eigenen Cybermobbing-Straftatbestands in dargelegter Form als notwendig beziehungsweise vorzugsweise anzusehen.

[152] *Gericke*, in: MüKo-StGB, § 238 Rn. 44 m.w.N.

IV. Fazit

Cybermobbing wird de lege lata von einigen Straftatbeständen erfasst, allerdings insbesondere in Hinblick auf dessen Unrechtsgehalt als Gesamtgeschehen, die niedrigen Strafrahmen und die nicht berücksichtigten erheblichen Folgen für die Opfer, in nicht ausreichendem Umfang. Die Einführung eines eigenen Cybermobbing-Straftatbestandes ist notwendig. Er sollte inhaltlich bezüglich seiner Tathandlungen an die Ehrschutzdelikte der §§ 185 ff. StGB sowie die §§ 201, 201a StGB anknüpfen. Einer vollständigen Erfassung des Phänomens des Cybermobbings in einer einzelnen Strafvorschrift bedarf es nicht. Dies erscheint hinsichtlich der Komplexität dieses Phänomens auch als nicht umsetzbar.

KriPoZ Kriminalpolitische Zeitschrift JuP

„Junges Publizieren“

Seminararbeit von

Sabine Reschke

Strafbarkeit des Cyber-Grooming

Ludwig-Maximilians-Universität München

Betreuer: Prof. Dr. Mark Zöller

Abgabedatum: 26.10.2020

Inhaltsverzeichnis

I. Einleitung

„Hoffe, bin nicht zu alt (Helmut45)“, „Guten Tag, Hi, mag jüngere (Berliner53)“, „Willst du mal was aufregendes sehen (Arnold1991)“ und „Bist du noch Jungfrau (Anaconda33)“. Solche Chatanfragen erhielten Ermittler des BKA, als sie sich mit dem Profil eines 13-jährigen Mädchens in einem Chatroom anmeldeten. Diese Stichprobe lässt vermuten, dass entsprechende Chatverläufe in Deutschland an der Tagesordnung sind.[1] gesetzliche Reaktion auf solche Kommunikationsversuche mit Kindern hat der Gesetzgeber vor einiger Zeit als das sog. „Cyber-Grooming“ unter Strafe gestellt. Dabei wird unter „Cyber-Grooming“ die Anbahnung von Kontakten zu Kindern über das Internet zur Vorbereitung von sexuellem Missbrauch verstanden.[2] Vor allem jetzt in Zeiten der Corona-Pandemie wird in den Medien das Cyber-Grooming als eine enorme Gefahr gesehen. Kinder und Jugendliche verbringen aufgrund des Online-Unterrichts noch mehr Zeit im Netz, was sie zum leichten Ziel für Cyber-Grooming in sozialen Netzwerken und Online-Spielen mache.[3] Bis vor kurzem war der Versuch, mit einem vermeintlichen Kind in sexueller Absicht im Internet in Kontakt zu treten, ausdrücklich nicht unter Strafe gestellt.[4] Seit dem 13.03.2020 hat der Gesetzgeber nun auch diejenigen Fälle unter Strafe gestellt, deren Vollendung der Tat allein daran scheitert, dass der Täter irrig annimmt, sein Handeln beziehe sich auf ein Kind.[5] Mit der Neueinführung der Strafbarkeit des untauglichen Versuchs bestrebt der Gesetzgeber, der Missbrauchsgefahr im Netz besser zu begegnen. Damit gerät der kontroverse Tatbestand des Cyber-Grooming erneut in das juristische Diskussionsfeld.

II. Einführung in das Thema

1. Gesetzgeberische Entwicklung

Im Jahr 2003 wurde der deutsche Gesetzgeber erstmals auf die bestehende Gefahr, im digitalen Raum Opfer von Cyber-Grooming zu werden, aufmerksam. Mit dem „Gesetz zur Änderung der Vorschriften über die Straftaten gegen die sexuelle Selbstbestimmung“ (SexualdelÄndG) vom 27.12.2003 fand das Cyber-Grooming in Gestalt von § 176 Abs. 4 Nr. 3 (a.F.) Aufnahme in das StGB.[6] In der Gesetzesbegründung wird darauf verwiesen, dass die Presse von Fällen der Missbrauchsanbahnung im Internet berichtet hätte, die sich in den Vereinigten Staaten zugetragen haben sollen, die in mehreren Fällen mit einer Vergewaltigung geendet hätten.[7] Des Weiteren wird eine Stellungnahme des europäischen Wirtschafts- und Sozialausschusses angeführt, die eine Anpassung der Strafvorschriften fordert, um Verbrechen, bei denen Kinder durch Tricks oder Verführungskünste zu Treffen verleitet werden, zu erfassen.[8] Bis zu diesem Zeitpunkt war das auf die Verwirklichung des sexuellen Missbrauchs von Kindern abzielende Einwirken durch Schriften, insbesondere in Chatrooms im Internet, lediglich eine straflose Vorbereitungshandlung. Mit der Einführung des § 176 Abs. 4 Nr. 3 StGB (a.F.) schloss der Gesetzgeber diese Strafbarkeitslücke. [9] Danach macht sich bereits derjenige strafbar, der auf ein Kind durch Schriften

1 *Schneider*, KriPoZ 2020, 137.
2 *Eisele*, in: FS Heinz, 2012, S. 697 (697 f.).
3 *Stukenberg*, Online-Chats und –Spiele als Einfallstor für sexuellen Missbrauch, DLF 24.5.2020, abrufbar unter: https://www.deutschlandfunk.de/cybergrooming-online-chats-und-spiele-als-einfallstor-fuer.724.de.html?dram:article_id=477289 (zuletzt abgerufen am 14.10.2020).
4 BT-Drs. 19/13836, S. 1.
5 *Van Edern*, NJW 2020, 1033.
6 *Duttge/Hörnle/Renzikowski,* NJW 2004, 1065.
7 BT-Drs. 15/350, S. 17.
8 *Eisele*, in: FS Heinz, 2012, S. 697 (698).
9 BT-Drs. 19/13836, S. 9.

(§ 11 Abs. 3 StGB) einwirkt, um es zu sexuellen Handlungen zu bringen, die es an oder vor dem Täter oder einem Dritten oder von dem Täter oder einem Dritten an sich vornehmen lassen soll. Dabei ist unter „Einwirkung" nach der Gesetzesbegründung auch ein Handeln ohne jegliche sexuelle Bedeutung zu verstehen. Der Sexualbezug soll hierbei lediglich durch die Intentionen des Täters hergestellt werden. So sollten vor allem Fälle erfasst werden, in denen sich Erwachsene als vermeintliche Kinder ausgeben, um später ihre sexuellen Absichten durchzusetzen, sobald sie das Vertrauen des Kindes gewonnen haben.[10] Erwähnenswert im Zusammenhang des SexualdelÄndG ist auch die Anhebung der Mindeststrafe in § 176 Abs. 4 StGB für den Kindesmissbrauch ohne Körperkontakt von einer ursprünglichen Geldstrafe auf drei Monate Freiheitsstrafe. Durch das 49. Strafrechtsänderungsgesetz (StÄG) vom 21.1.2015 wurde die Norm zum Zwecke der vollständigen Umsetzung des Übereinkommens des Europarats zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch (Konvention Nr.201) sowie der EU-Richtlinie 2011/93/EU erneut geändert. Dabei wurde § 176 Abs. 4 Nr. 3 StGB in zweierlei Hinsicht erweitert: Die Verwendung von Informations- und Kommunikationstechnologie wurde in die Reihe der tauglichen Tatmittel aufgenommen. Hintergrund für die Erweiterung der Tatmittel war, dass der erweiterte Schriftenbegriff des § 11 Abs. 3 StGB, auf den § 176 Abs. 4 Nr. 3 StGB Bezug nahm, grundsätzlich nur Speichermedien umfasste. Um der Informationsübertragungen über reine Datenleitungen Rechnung zu tragen, bei der es zu keiner Speicherung von Daten kommt, wurde die Erweiterung auf Informations- und Kommunikationstechnologie als Mittel der Einwirkung vorgenommen.[11] Zusätzlich wurde bei den Taten, die der Täter nach der Einwirkung zu begehen beabsichtigen muss, Delikte nach § 184b Abs. 1 Nr. 3 und Abs. 3 StGB hinzugenommen.[12] Strafbar macht sich demnach auch, wer auf ein Kind in der Absicht einwirkt, eine kinderpornographische Schrift, die ein tatsächliches Geschehen wiedergibt, herzustellen bzw. sich daran Besitz zu verschaffen.[13] Mit dem 57. Gesetz zur Änderung des Strafgesetzbuches wurde schließlich noch eine eingeschränkte Versuchsstrafbarkeit nach § 176 Abs. 6 S. 2 StGB eingeführt.

2. Problemaufriss

Die dynamische Entwicklung des § 176 StGB zeigt, dass der Gesetzgeber dem besonderen Schutzbedürfnis der Kinder besondere Beachtung beimisst. Der sexuelle Missbrauch von Kindern hat sich in den letzten Jahren erfolgreich als ein soziales Problem etabliert. Dabei ist das Strafrecht ein naheliegendes, weil durch Gesetzesänderungen beeinflussbares Feld politischer Aktivitäten.[14] Es stellt sich jedoch bei dieser dynamischen Gesetzgebung und der immer weiteren Vorverlagerung der Strafbarkeit die Frage, wo die Grenze zwischen dem noch legitimerweise strafbaren und dem nicht mehr strafbaren Vorfeldverhalten verläuft.[15] Mit der Einführung des § 176 Abs. 3 Nr. 4 StGB wurde die Pönalisierung der bisher straflosen Vorgänge im Vorfeld des sexuellen Kindesmissbrauchs vorgenommen und somit vom Grundsatz der Straflosigkeit der Vorbereitungshandlung abgewichen.[16] Ein Versuch des sexuellen Kindesmissbrauchs beginnt erst mit Handlungen des Täters, die nach seinem Tatplan der Vornahme der sexuellen Handlung unmittelbar vorgelagert sind.[17] Das für die Versuchsstrafbarkeit erforderliche unmittelbare Ansetzen liegt regelmäßig erst dann vor, wenn das Kind an einen anderen Ort verbracht

10 *Duttge/Hörnle/Renzikowski,* NJW 2004, 1065.
11 *Gercke*, CR 2014, 687 (688).
12 BGBl. I 2015, S. 10.
13 *Fischer*, StGB, 67. Aufl. (2020), § 184b Rn. 26.
14 *Dessecker*, KriPoZ 2019, 282.
15 *Beck*, Unrechtsbegründung und Vorfeldkriminalisierung – zum Problem der Unrechtsbegründung im Bereich vorverlegter Strafbarkeit, erörtert unter besonderer Berücksichtigung der Deliktstatbestände des politischen Strafrechts, 1992, S. 26.
16 *Funcke-Auffermann/Amelung,* StraFo 2004, 265 (267).
17 *Renzikowski*, in: MüKo-StGB, 3. Aufl. (2017), § 176 Rn. 23.

wurde, wo die sexuelle Handlung alsbald vollzogen werden soll. Sofern der Täter jedoch darauf abzielt, das Kind durch weitere Zwischenhandlungen erst gefügig zu machen, so genügt für das unmittelbare Ansetzen nicht mal das Verbringen an einen anderen Ort.[18] Da eine Verabredung vor diesem Hintergrund bis zur Einführung des § 176 Abs. 4 Nr. 3 StGB keinen Straftatbestand erfüllt hat, sollte diese Strafbarkeitslücke geschlossen werden.[19]Auch wenn der gesetzgeberische gute Wille im Hinblick auf die Bemühungen, den Kindern einen besseren Schutz zu gewährleisten, aus moralisch-bürgerlicher Sicht zu befürworten ist, darf nicht verkannt werden, dass dieser gute Wille kein hinreichender Grund ist, um dem Gesetzgeber einen „Freibrief" zum gesetzlichen Aktionismus zu erteilen.[20] Der Tatbestand des Cyber-Grooming ist vor allem aufgrund seiner weiten Vorverlagerung der Strafbarkeit in heftige Kritik geraten, die die Frage nach seiner grundsätzlichen Legitimierbarkeit aufwirft. Dies gilt umso mehr für den neu eingeführten untauglichen Versuch des Cyber-Grooming.[21]

III. Gesetzgeberische Ausgestaltung

1. Normzweck und geschütztes Rechtsgut

Die Bestimmung des Rechtsgutes im Rahmen des § 176 Abs. 4 Nr. 3 StGB ist vor allem deswegen von enormer Bedeutung, da eine zentrale tatbestandliche Voraussetzung dieser Norm die sexuelle Handlung ist. Gem. § 184h Nr. 1 StGB sind sexuelle Handlungen nur solche, die im Hinblick auf das jeweils geschützte Rechtsgut von einiger Erheblichkeit sind.[22] Außerdem spielt das Rechtsgut bei der Legitimation einer Strafnorm eine überragende Rolle.[23]

a) Eigenständiger Rechtsgutsbegriff in § 176 Abs. 4 Nr. 3 StGB

Fraglich ist, ob § 176 Abs. 4 Nr. 3 StGB ein eigenständiges Rechtsgut schützen will. Der § 176 Abs. 4 Nr. 3 StGB ist als eine eigenständige Strafvorschrift ausgestaltet.[24] Der Gesetzesbegründung lässt sich kein eigenständiges Rechtsgut des § 176 Abs. 4 Nr. 3 StGB entnehmen.[25] Zu der Fragestellung, ob ein abweichendes Rechtsgut durch § 176 Abs. 4 Nr. 3 StGB geschützt werden soll, finden sich auch in der Literatur keine Anhaltspunkte. Da sich die Regelung des § 176 Abs. 4 Nr. 3 StGB in systematischer Hinsicht im 13. Abschnitt des StGB befindet, kann darauf geschlossen werden, dass sie dem einheitlichen Rechtsgut der „sexuellen Selbstbestimmung" unterfällt. Dem Gesetzgeber zur Folge sollte aber dieses einheitliche Rechtsgut in den einzelnen Tatbeständen konkretisiert werden.[26] Im Hinblick darauf, dass sich § 176 Abs. 4 Nr. 3 StGB im Normgefüge des sexuellen Kindesmissbrauchs gem. § 176 StGB auffinden lässt, liegt es nahe, das Rechtsgut des § 176 StGB als das von § 176 Abs. 4 Nr. 3 StGB geschützte Rechtsgut anzusehen.[27] Das Rechtsgut des 176 StGB ist jedoch nicht unumstritten.[28]

---

18 *Eisele*, in: Schönke/Schröder, StGB, 30. Aufl. (2019), § 176 Rn. 24.
19 BT-Drs. 15/350, S. 17 f.
20 *Alexiou*, Cyber-Grooming: Eine kriminologische und strafrechtsdogmatische Betrachtung, 2018, S. 24.
21 *Fischer*, Stellungnahme Prof. Dr. Fischer zu BT-Drs. 19/13836 v. 05.11.2019, abrufbar unter: https://kripoz.de/wpcontent/uploads/2019/11/stellungnahme-fischer-cybergrooming.html (zuletzt abgerufen am 14.10.2020), S. 2
22 *Wilmer*, Sexueller Mißbrauch von Kindern: Empirische Grundlagen und kriminalpolitische Überlegungen, 1996, S. 21.
23 *Graul*, Abstrakte Gefährdungsdelikte und Präsumtionen im Strafrecht, 1991, S. 41 ff.
24 *Renzikowski*,in: MüKo-StGB, § 176 Rn. 18.
25 BT-Drs. 15/350, S. 17 f.
26 *Schroeder*, in: FS Welzel, 1974, S. 859 (868 ff.).
27 *Stoiber*, "Cyber-Grooming" aus empirischer und strafrechtlicher Sicht: Eine Analyse von § 176 Abs. 4 Nr. 3 StGB, 2020, S. 106 ff.
28 *Lederer,* in: AnwaltK-StGB, 3. Aufl. (2020), § 176 Rn. 2.

b) Rechtsgut des § 176 StGB

aa) Schutz der ungestörten sexuellen (Gesamt-)Entwicklung

Nach überwiegender Ansicht in Rechtsprechung und Literatur ist das Rechtsgut bei § 176 StGB in der „ungestörten sexuellen Entwicklung" von Kindern zu sehen. Diese Ansicht wird gestützt durch die Ausführungen des Gesetzgebers zum 4. StrRG.[29] Dabei wird in Bezug auf sexuellen Missbrauch von Kindern geäußert, dass hiermit die ungestörte sexuelle Entwicklung des jungen Menschen geschützt werden solle.[30] Dem liegt der Gedanke zugrunde, dass sich die sexuelle Identität einer Person prozesshaft entwickelt und fremdbestimmte Eingriffe in die kindliche Sexualität in besonderer Weise geeignet sind, diese Entwicklung zu stören.[31] Kritisch gesehen wird jedoch, dass die Maßstäbe für eine „normale Entwicklung" unbekannt sind und, dass die Bestimmung einer „Fehlentwicklung" kaum greifbar ist. Dies gilt umso mehr, als jede Entwicklung eines Menschen äußeren (nicht wertend schlechten) Einflüssen ausgesetzt ist.[32] Diese Kritik wird dadurch relativiert, dass zum heutigen Stand der Wissenschaft in sexualwissenschaftlichen Studien zumindest typische Stadien der sexuellen Entwicklung von Kindern belegbar sind.[33] Einige Stimmen in der Literatur empfinden den Begriff der „sexuellen Entwicklung" aber dennoch als zu eng gefasst, denn mögliche negative Konsequenzen können sich für das spätere Leben der Betroffenen nicht nur in Problemen im Sexualbereich äußern, sondern auch in unspezifischen psychischen Auffälligkeiten wie Depressionen, Angstsymptomen u. Ä. Daher wird im Zusammenhang mit dem Schutzgut des § 176 StGB vermehrt auch von einer Beeinträchtigung der „Gesamtentwicklung" der Kinder gesprochen.[34] Ob zwischen den Formulierungen „Gesamtentwicklung" und „sexuelle Entwicklung" ein inhaltlicher Unterschied besteht, bleibt allerdings offen. Festzustellen ist an dieser Stelle lediglich, dass der Begriff „sexuelle Entwicklung" den Sexualbezug und somit den Ursprung der Störung deutlicher hervorhebt, wohingegen der Begriff der „Gesamtentwicklung" vielmehr alle möglichen Folgen im Hinblick auf diese Störung erfasst.[35] Teilweise werden auch beide Begriffe kombiniert.[36] Insgesamt kann aber davon ausgegangen werden, dass das Rechtsgut nach überwiegender Auffassung die „ungestörte sexuelle Entwicklung" ist, deren Fernziel der Schutz vor Beeinträchtigungen der „Gesamtentwicklung" der Kinder darstellt.[37]

bb) Rechtsgut der sexuellen Selbstbestimmung

Andere Stimmen in der Literatur lehnen die ungestörte sexuelle Entwicklung bzw. die Beeinträchtigung der Gesamtentwicklung von Kindern als Rechtsgut komplett ab. Die Gegenansicht ist der Auffassung, dass § 176 StGB das sexuelle Selbstbestimmungsrecht schützt.[38] Dieser Ansicht nach würde die herrschende Meinung bei § 176 StGB ein Rechtsgut annehmen, dem durch die Tathandlungen der Norm nicht stets (unmittelbar) Gefahr droht. Dies wird damit begründet, dass die Tatsache, ob ein sexueller Übergriff negative Folgen für das betroffene Kind hat und von welcher Intensität diese sind, von vielen Einzelumständen abhängt.[39] Die sexuelle Selbstbestimmung sei das zutreffendere Rechtsgut, da jedenfalls sexuelle Handlungen mit Körperkontakt in die Rechtssphäre

[29] *Brockmann*, Das Rechtsgut des § 176 StGB: Zugleich ein Beitrag zur Leistungsfähigkeit des Rechtsgutsbegriffs als Hilfsmittel der Auslegung, 2015, S. 182.
[30] BT-Drs. 6/1552, S. 9 f.
[31] *Renzikowski,* in: MüKo-StGB, § 176 Rn. 3.
[32] *Wolters*, in: SK-StGB, 9. Aufl. (2017), § 176 Rn. 2.
[33] *Hörnle,* in: LK-StGB, 12. Aufl. (2010), § 176 Rn. 1.
[34] *BGH*, Beschl. v. 21.9.2000 – 3 StR 323/00.
[35] *Brockmann*, S. 183.
[36] *Eisele*, in: Schönke/Schröder, StGB, § 176 Rn. 1a.
[37] *Brockmann*, S. 184.
[38] *Stoiber*, S. 123.
[39] *Renzikowski*, in: MüKo-StGB, § 176 Rn. 3.

des anderen eingriffen und somit seine körperliche Integrität berührten. Das solle unabhängig davon gelten, ob ein Erwachsener oder ein Kind betroffen sei. Somit kann nur die Zustimmung der anderen Person den Eingriff durch eine solche sexuelle Handlung rechtfertigen.[40] Das Problem, dass sexuelle Selbstbestimmung die Fähigkeit zu autonomen Entscheidungen voraussetzt, an der es bei (am offensichtlichsten sehr jungen) Kindern fehle, wird von der Minderheitsansicht damit gelöst, dass das sexuelle Selbstbestimmungsrecht auch als ein Abwehrrecht gegenüber Dritten gesehen werden kann. Dabei bestehen Abwehrrechte in vollem Umfang auch für Personen, die konstitutionsbedingt derartige Rechte noch nicht selbst durchsetzen können.[41] Somit ist in Bezug auf Kinder ihr negatives sexuelles Selbstbestimmungsrecht als das Rechtsgut anzusehen. Der Umweg, das Unrecht bei § 176 StGB über die möglicherweise drohenden physischen und psychischen Schäden zu konstruieren, hält diese Ansicht für überflüssig.[42]

c) Zusammenfassung

Das Rechtsgut des § 176 ist insgesamt sehr umstritten, wobei die herrschende Meinung trotz der Kritik am Schutz der „ungestörten sexuellen (Gesamt-) Entwicklung" festhält.[43] Was den hier zu betrachtenden Tatbestand des § 176 Abs. 4 Nr. 3 StGB betrifft, so kann nach der hier vertretenen Ansicht weder die eine noch die andere Ansicht überzeugen. In der Literatur wird teilweise die Ansicht vertreten, dass hier aufgrund der weiten Vorverlagerung der Strafbarkeit im Gegensatz zu anderen Alternativen des Abs. 4 überhaupt keine Verletzung der Selbstbestimmung des Kindes gegeben ist.[44] Andere sehen das Rechtsgut des § 176 Abs. 4 Nr. 3 StGB im „substratlose[n] öffentlichen Frieden". [45] *Wolters* ist der Ansicht, dass ein vergleichbarer und messbarer Bezug des § 176 Abs. 4 Nr. 3 StGB zum geschützten Rechtsgut der Vorschrift überhaupt nur dann hergestellt werden kann, wenn die Tathandlung auch objektiv ein sexualisiertes Klima schafft, das die geplante nachfolgende sexuelle Handlung begünstigt.[46] Diese Stimmen aus der Literatur deuten auf einen Aspekt hin, der angesichts des nicht unmittelbar herzustellenden Rechtsgutsbezugs Kernelement der vielfach am Tatbestand des § 176 Abs. 4 Nr. 3 StGB geäußerten Kritik ist; mithin der bereits erwähnten weiten Vorverlagerung der Strafbarkeit des § 176 Abs. 4 Nr. 3 StGB.[47]

2. Tatbestand des § 176 Abs. 4 Nr. 3 StGB

a) Objektiver Tatbestand

aa) Täter

Der § 176 Abs. 4 Nr. 3 StGB ist ein Jedermanns-Delikt.[48] Zu beachten ist, dass sich das Delikt auch auf Jugendliche und Heranwachsende als mögliche Täter erstreckt.[49] Im Gegensatz zu § 176 Abs. 1 und Abs. 4 Nr. 1 StGB impliziert die Tathandlung „Einwirken" des § 176 Abs. 4 Nr. 3 StGB keine Eigenhändigkeit.[50] Somit ist es möglich,

40 *Laubenthal*, Handbuch Sexualstrafrecht: Die Delikte gegen die sexuelle Selbstbestimmung, 2012, Rn. 29.
41 *Hörnle*, in: FS Eisenberg, 2009, S. 321 (335).
42 *Renzikowski*, in: MüKo-StGB, § 176 Rn. 3.
43 *Alexiou*, S. 287.
44 *Renzikowski*, in: MüKo-StGB, § 176 Rn. 41.
45 *Sick/Renzikowski*, in: FS Schroeder, 2006, S. 603 (613).
46 *Wolters*, in: SK-StGB, § 176 Rn. 24b.
47 *Alexiou*, S. 288.
48 *Kindhäuser/Hilgendorf*, LPK-StGB, 8. Aufl. (2020), § 176 Rn. 2.
49 *Stoiber*, S. 152.
50 *Kindhäuser/Hilgendorf*, LPK-StGB, § 176 Rn. 2.

sowohl als Mittäter als auch mittelbarer Täter auf ein Kind einzuwirken.[51] Ein Einwirken durch Unterlassen ist rechtlich nicht möglich, da bereits der Begriff des Einwirkens begriffsnotwendig ein aktives Tun voraussetzt. Somit scheiden untätig bleibende Garanten als Mittäter aus.[52] Als Vorsatzdelikt sind auf § 176 Abs. 4 Nr. 3 StGB die allgemeinen Regeln zur Täterschaft und Teilnahme anwendbar, sodass sowohl eine Anstiftung als auch eine Beihilfe zu einer solchen Tat vorstellbar ist.[53]

bb) Opfer

Opfer der Tathandlung ist ein „Kind", mithin eine Person, die das 14. Lebensjahr noch nicht vollendet hat. Für die Tatbestandsmäßigkeit spielt die Geisteshaltung des Opfers keine Rolle.[54] Selbst wenn ein Kind bei Beginn der Einwirkungshandlung fest dazu entschlossen oder nur geneigt ist, mit dem Täter sexuelle Handlungen auszuführen, so ist dies von keinerlei Bedeutung.[55] Grund dafür ist die Tathandlung, die lediglich ein „Einwirken" erfordert. Ein Einwirkungserfolg in der Form, dass durch das Einwirken im Opfer bereits die konkrete Bereitschaft zur Vornahme oder Duldung der anvisierten sexuellen Handlung geschaffen wird, ist nicht erforderlich.[56]

cc) Verhältnis Täter – Opfer

Trotz der oben erwähnten Gesetzesbegründung[57] des § 176 Abs. 4 Nr. 3 StGB, die vorwiegend auf den Schutz vor anonymen Kontaktanbahnungen im Internet abstellt, beschränkt sich der Schutz des Tatbestands nicht nur auf Fälle dem Kind unbekannter Täter. Es gibt weder im Wortlaut der Norm noch in den Gesetzgebungsmaterialien Anhaltspunkte dafür, dass die Anonymität eine Voraussetzung des Tatbestandes des § 176 Abs. 4 Nr. 3 StGB ist.[58] Mithin können sich durchaus nahe Bekannte oder auch Familienmitglieder gem. § 176 Abs. 4 Nr. 3 StGB strafbar machen.[59]

dd) Tathandlung „Einwirken"

Die Tathandlung des § 176 Abs. 4 Nr. 3 StGB ist das „Einwirken" auf Kinder. Die Gesetzesbegründung des § 176 Abs. 4 Nr. 3 StGB bietet keine (eigene) Definition von „Einwirken" im Sinne des § 176 Abs. 4 Nr. 3 StGB an, sondern verweist auf die Rechtsprechung und Literatur zum Einwirkungsbegriff des § 180b Abs. 1 S. 2 StGB a.F.[60], die zur Auslegung des Begriffes „Einwirken" des § 176 Abs. 4 Nr. 3 StGB herangezogen werden solle.[61] Danach erfasst das Einwirken i.S.v. § 180b Abs. 1 S. 2 StGB a.F. alle Formen der intellektuellen Beeinflussung, verlangt darüber hinaus aber auch eine gewisse Hartnäckigkeit.[62] Als Mittel kommen wiederholtes Drängen, Überreden, Versprechungen, Wecken von Neugier, Einsatz von Autorität, Täuschung, Einschüchterung, Drohung und auch Gewalteinwirkung in Betracht.[63] Dabei ist das Einwirken unabhängig vom Eintritt des Erfolges. Das Kind muss lediglich die Einflussnahme tatsächlich zur Kenntnis genommen haben.[64] Erforderlich ist eine Konkretisierung auf ein Kind oder (bestimmte) Kinder.[65] Hierfür spricht die Gesetzesbegründung, die explizit ein „gezieltes"

51 *Eschelbach*, in: Matt/Renzikowski, StGB, 2. Aufl. (2020), § 176 Rn. 35.
52 *Renzikowski*, in: MüKo-StGB, § 176 Rn. 42.
53 *Hörnle*, in: LK-StGB, § 176, Rn. 112.
54 *Stoiber*, S. 156.
55 *Frühsorger*, Der Straftatbestand des sexuellen Kindesmissbrauchs gemäß § 176 StGB, 2011, S. 161.
56 *Frühsorger*, S. 157.
57 BT-Drs. 15/350 S. 17 f.
58 *Heger*, in: Lackner/Kühl, StGB, 29. Aufl. (2018), § 176 Rn. 4a.
59 *OLG Hamm*, Beschl. v. 14.01.2016 – 4 RVs 144/15; vgl. auch: *BGH*, Beschl. v. 16.07.2015 – 4 StR 219/15.
60 § 180b StGB ist durch das 37. StÄG aufgehoben worden.
61 BT-Drs. 15/350, S. 18.
62 *Lederer*, in: AnwaltK-StGB, § 176 Rn. 21; a.A.: *Frühsorger*, S. 151 ff.
63 *OLG Hamm*, Beschl. v. 14.01.2016 – 4 RVs 144/15.
64 *Renzikowski*, in: MüKo-StGB, § 176 Rn. 42.
65 a.A. *Frühsorger*, S. 155 f.

einwirken auf ein „konkretes Kind“ fordert.[66] Auch der Zweck der Norm spricht dafür, da erst mit dem Bezug zu einem bestimmten Kind von einer Gefahr für dessen ungestörte sexuelle Entwicklung auszugehen ist.[67]

ee) Tatmittel

§ 176 Abs. 4 Nr. 3 StGB sanktioniert ein Vorgehen mittels klar bestimmter Mittel: Schriften i.S.v. § 11 Abs. 3 StGB oder Informations- oder Kommunikationstechnologie. Im Gegensatz zu Nr. 4 muss der Inhalt weder einen pornographischen noch überhaupt einen Sexualbezug aufweisen.[68] Dies entspricht auch dem gesetzgeberischen Willen, da laut Gesetzesbegründung gerade auch solche Täter erfasst werden sollen, die durch Tricks oder Verführungskünste auf Kinder in sexueller Absicht einwirken.[69]

b) Subjektiver Tatbestand

aa) Vorsatz

Auf subjektiver Seite ist bezüglich der einzelnen Merkmale des objektiven Tatbestandes jede Vorsatzform ausreichend. Insbesondere genügt bereits der bedingte Vorsatz im Hinblick auf das Kind-Sein des Gesprächspartners.[70] Nimmt der Täter irrig an, dass das Kind älter ist, so entfällt der Vorsatz aufgrund eines Tatbestandsirrtums gem. § 16 Abs. 1 S. 2 StGB.[71] Bei der Konstellation, dass er irrig annimmt, ein Erwachsener sei ein Kind, wird er seit der Einführung der Versuchsstrafbarkeit gem. § 176 Abs. 6 S. 2 StGB des versuchten Cyber-Grooming strafbar.[72]

bb) Besondere Absicht

Das Cyber-Grooming ist ein Delikt mit überschießender Innentendenz und erfordert die Absicht, das Kind durch die Einwirkung zu sexuellen Handlungen zu motivieren oder eine Tat nach § 184b Abs. 1 Nr. 3 oder Abs. 3 StGB zu begehen.[73] Es muss dem Täter gerade darauf ankommen, dass das Kind als End- oder auch Zwischenziel sexuelle Handlungen ausführt bzw. eine Tat nach § 184b Abs. 1 Nr. 3 oder Abs. 3 StGB begeht. Auf das Erreichen dieses Zieles kommt es hierbei aber nicht an.[74] Dem Wortlaut der Gesetzesbegründung zur Folge soll der Täter an den sexuellen Handlungen ferner ein Interesse haben. Ausgenommen sollen von der Strafbarkeit somit Fälle sein, in denen in Büchern, Internet oder auch in Chatrooms auf Kinder zugegangen wird, um sie darin zu unterstützen, ein positives Gefühl zu ihrem Körper und ihrer Sexualität zu entwickeln.[75]

IV. Kritik an der Ausgestaltung der Strafbarkeit

1. Vollendetes Cyber-Grooming

Für die Vollendung des § 176 Abs. 4 Nr. 3 StGB ist allein ein Einwirken ohne jeglichen objektiven Sexualbezug auf das Opfer ausreichend. Auf das Stattfinden eines realen Treffens mit Vollziehung der sexuellen Handlung

66 BT-Drs. 15/350, S. 18.
67 *Lederer*, in: AnwaltK-StGB, § 176 Rn. 21.
68 *Eisele*, in: Schönke/Schröder, StGB, § 176 Rn. 14c.
69 BT-Drs. 15/350, S. 18.
70 *Wolters*, in: SK-StGB, § 176 Rn. 28.
71 *Eisele*, in: FS Heinz, 2012, S. 697 (700).
72 *Van Edern*, NJW 2020, 1033.
73 *Lederer,* in: AnwaltK-StGB, § 176 Rn. 23.
74 *Stoiber*, S. 186.
75 BT-Drs. 15/350, S. 18.

kommt es nicht an. § 176 Abs. 5 Var. 3 StGB stellt auch die Verabredung zum Cyber-Grooming (im gleichen Strafmaß) unter Strafe. Bildlich gesprochen: Es wird bereits die Verabredung strafrechtlich erfasst, mit einem anderen irgendwann zum späteren Zeitpunkt auf Kontaktsuche zu gehen.[76] Durch den Verweis in § 176 Abs. 5 Var. 3 StGB wird die Strafbarkeit noch weiter vorverlagert. Der sexuelle Missbrauch des Kindes *kann* im Anschluss der Tathandlung des § 176 Abs. 4 Nr. 3 StGB erfolgen und begründet dann eine eigene Strafbarkeit.[77] Bei § 176 Abs. 4 Nr. 3 StGB handelt es sich um eine strafbare Vorbereitungshandlung und somit um ein abstraktes Gefährdungsdelikt.[78]

a) Problem: Vorfeldkriminalisierung

aa) Grundsatz Straflosigkeit von Vorbereitungshandlungen

Grundsätzlich sind nach dem geltenden Recht Vorbereitungshandlungen straflos, da in diesem Stadium noch viele Unwägbarkeiten das Ziel zunichtemachen können.[79] Es ist dem Wesen eines rechtsstaatlichen Strafrechts zugrunde gelegt, dass manche Verhaltensweisen, die eine Mehrheit der Bevölkerung als unmoralisch oder verwerflich ansehen würde, rechtlich erlaubt sind.[80] So werden Vorbereitungshandlungen zu einem Mord von fast jedem Bürger als moralisch verwerflich angesehen. Dennoch ist es nicht strafbar, sich ein Messer im Haushaltsgeschäft zu kaufen, da zwischen dem An-der-Kasse-Stehen und sich ein Küchenmesser kaufen und dem Verletzen eines Menschen in Tötungsabsicht eine sehr lange Zeitspanne liegt und viele Zwischenschritte erforderlich sind. Die Kriminalisierung von Vorbereitungshandlungen ist aber nicht neu in unserem Strafgesetzbuch. So sieht der Gesetzgeber bei enormer Gefährlichkeit eines Verhaltens eine Strafbarkeit mancher Vorbereitungshandlungen im Strafgesetzbuch explizit vor. So seien an dieser Stelle die Vorbereitung eines Sprengstoffverbrechens (§ 310 StGB) oder die Verabredung zu einem Verbrechen (§ 30 Abs. 2 StGB) zu nennen.[81] Vorbereitungsdelikte sind abstrakte Gefährdungsdelikte, bei denen die gesetzgeberische Vermutung davon ausgeht, dass bestimmte Handlungen für das geschützte Rechtsgut generell gefährlich sind.[82] Verfassungsrechtlich begegnet das abstrakte Gefährdungsdelikt an sich grundsätzlich keinen Bedenken.[83] Hinsichtlich der Beurteilung der Gefährlichkeit eines Verhaltens kommt dem Gesetzgeber eine weite Einschätzungsprärogative bei der verfassungsrechtlichen Prüfung zu, innerhalb derer er entscheiden kann, welche kriminalpolitischen Maßnahmen er für geeignet hält.[84]

bb) Rechtsgüterschutz als Legitimationsmaßstab

Zu beachten ist jedoch, dass ein liberales Strafrecht seine Legitimationsbedingung für die Verhängung von Kriminalstrafen als Sanktion und damit der Schaffung von Freiheitsbeeinträchtigungen allein bei dem Vorliegen strafwürdigen Unrechts findet. Dieses wiederum stellen jedoch grundsätzlich nur solche sozialschädlichen Verhaltensweisen dar, welche ein Rechtsgut beeinträchtigen.[85] Die abstrakten Gefährdungsdelikte werden zwar als „Ungehorsams-Delikte“ oder als „rechtsgutslose“ Straftaten umschrieben, dennoch ist an dieser Stelle besonders hervorzuheben, dass bei dieser Deliktsgruppe materiell nicht die Zuwiderhandlung gegen ein bestimmtes Verbot, sondern

76 *Renzikowski*, in: MüKo-StGB, § 176 Rn. 19.
77 *Bezjak*, Grundlagen und Probleme des Straftatbestandes des sexuellen Missbrauchs von Kindern gemäß § 176 StGB, 2015, S. 127.
78 *Bezjak* (Fn. 77), S. 137 ff.; a.A.: *Wolters*, in: SK-StGB, § 176 Rn. 37; *Eschelbach*, in: Matt/Renzikowski, StGB, § 176 Rn. 21.
79 *Schmidt*, Strafrecht AT, 21. Aufl. (2019), Rn. 633.
80 *Dessecker,* KriPoZ 2019, 282.
81 *Schmidt*, Strafrecht AT, Rn. 633.
82 *Frühsorger*, S. 20.
83 *Heine/Bosch*, in: Schönke/Schröder, StGB, Vor §§ 306 ff. Rn. 5.
84 *Bezjak* (Fn. 77), S. 128.
85 *Steinsiek*, Terrorabwehr durch Strafrecht? – verfassungsrechtliche und strafrechtssystematische Grenzen der Vorfeldkriminalisierung, 2012, S. 152.

die Vermeidung von Rechtsgutsverletzungen im Vordergrund steht.[86] Es ist zwar gerade bei der Vorfeldkriminalisierung kennzeichnend, dass ein Verhalten kriminalisiert wird, das nicht unmittelbar das Rechtsgut beeinträchtigt, sondern lediglich eine abstrakte Gefahr hierfür schafft, doch ist ein hinreichender Rechtsgutsbezug auch hier nicht unentbehrlich. Auch eine jede Vorfeldnorm muss in einem strikten Zusammenhang zu einem bestimmten Rechtsgut stehen.[87] Fehlt ein solcher hinreichender Bezug zum geschützten Rechtsgut, ist für das abstrakte Gefährdungsdelikt keine Legitimation ersichtlich. Das Verhalten würde lediglich um seiner selbst willen bestraft.[88] Für die Erfüllung des objektiven Tatbestands des § 176 Abs. 4 Nr. 3 StGB ist bereits die neutrale Kommunikation in der Absicht, irgendwann das Kind zu sexuellen Handlungen zu bewegen, ausreichend.[89] Fraglich ist, ob ein hinreichend enges Verhältnis zwischen der Tathandlung und dem geschützten Rechtsgut besteht. Ein Vergleich mit § 176 Abs. 1 StGB ergibt, dass bereits dieser Tatbestand keinen Verletzungserfolg bzw. keine konkrete Gefährdung des Rechtsguts voraussetzt und mithin seinerseits auch eine Vorfeldkriminalisierung darstellt [90] Im Gegensatz zu § 176 Abs. 4 Nr. 3 StGB ist hier aber ein Rechtsgutsbezug herstellbar, denn der Tatbestand setzt einen körperlichen Kontakt und eine objektive Sexualbezogenheit der Tathandlung voraus. Auch der Vergleich mit den anderen Begehungsformen des Kindesmissbrauchs ohne Körperkontakt des Abs. 4 zeigt, dass im Gegensatz zu der Tathandlung des Abs. 4 Nr. 3 in allen bezeichneten Tathandlungen das Kind zumindest unmittelbar in irgendeiner Form mit Sexualität konfrontiert wird.[91] Insofern kann hier im Gegensatz zu § 176 Abs. 4 Nr. 3 StGB ein hinreichender Rechtsgutsbezug über die objektive Sexualbezogenheit hergestellt werden. Auch wenn das Kindeswohl verfassungsrechtlich in Art. 2 GG und Art. 1 GG sowie Art. 6 Abs. 2 GG verankert ist und die Schutzwürdigkeit unbestritten gegeben und als sehr hoch einzustufen ist, muss man sich dennoch die Frage stellen, ob die Pönalisierung der Tathandlung im § 176 Abs. 4 Nr. 3 StGB im Hinblick auf die entfernte Kausalität noch zu rechtfertigen ist.[92] Nach der Ausgestaltung des objektiven Tatbestands und nach dem ausdrücklichen gesetzgeberischen Willen, der den Tatbestand als bereits erfüllt sieht, ohne dass nur ansatzweise ein objektiver Sexualbezug gegeben sein muss, ist dies zu verneinen.[93] Die Tathandlung des Einwirkens mit neutralen Inhalten ist nicht ansatzweise geeignet, das Rechtsgut der ungestörten sexuellen Entwicklung des Kindes zu beeinträchtigen.

cc) Verbot eines reinen Täter- und Gesinnungsstrafrechts

Der Verzicht auf jede objektive Sexualbezogenheit der Tathandlung verlagert die Strafbarkeit außerdem vollkommen ins Subjektive.[94] Allein durch den subjektiven Tatbestand und das Feststellen einer Absicht zu sexuellen Missbrauchshandlungen erfährt der weit gefasste Tatbestand aus der hier vertretenen Sicht nicht die notwendige Beschränkung. Es ist zwar anerkannt, dass Absichten, Vorsätze, Pläne, Motive und Gesinnungen zu einer strafwürdigen Tat als einschränkende subjektive Merkmale hinzutreten können. Sie können aber nicht allein oder verknüpft mit einem ohne Weiteres auch als neutral bzw. als ein nicht eindeutig rechtsgutsschädigend einzustufendes

86 *Anastasopoulou*, Deliktstypen zum Schutz kollektiver Rechtsgüter, 2005, S. 127.
87 *Beck*, S. 21.
88 *Kindhäuser*, Gefährdung als Straftat: Rechtstheoretische Untersuchungen zur Dogmatik der abstrakten und konkreten Gefährdungsdelikte, 1989, S. 166.
89 *Fischer*, StGB, § 176 Rn. 14.
90 *Laubenthal*, Rn. 439.
91 *Frühsorger*, S. 141.
92 *Funcke-Auffermann*, Symbolische Gesetzgebung im Lichte der positiven Generalprävention – eine Untersuchung am Beispiel des ‚Gesetzes zur Änderung der Vorschriften über die Straftaten gegen die sexuelle Selbstbestimmung und zur Änderung anderer Vorschriften' vom 27. Dezember 2003, 2007, S. 109; *Peters*, Kindheit im Strafrecht: Eine Untersuchung des materiellen Strafrechts mit besonderem Schwerpunkt auf dem Kind als Opfer und Täter, 2014, S. 5 f.
93 *Alexiou*, S. 307; *Stoiber*, S. 276; *Wolters*, in: SK-StGB, § 176 Rn. 37.
94 *Alexiou*, S. 289.

Verhalten eine Strafe begründen.[95] Die rechtliche Missbilligung eines Verhaltens darf - um die Grenze zum verfassungsrechtlich bedenklichen Gesinnungsstrafrecht zu wahren - allein ein ex ante störendes Verhalten sein. Die Reglementierung rechtlich neutralen Verhaltens läuft auf den Verdacht böser Absichten des so Agierenden hinaus, die durch eine entsprechende Vorschrift missbilligt würde.[96] Im Falle des § 176 Abs. 4 Nr. 3 StGB wird durch den subjektiven Tatbestand weder das objektiv gegebene Unrecht konkretisiert noch begrenzt, sondern schafft dieses erst. Wenngleich die Einwirkung eine gewisse Hartnäckigkeit voraussetzt, ist darin trotzdem keine ausreichende Konkretisierung zu sehen, da wiederum der Begriff der „Hartnäckigkeit" einen weiten Interpretationsspielraum lässt und seinerseits nicht geeignet ist, die Tathandlung des „Einwirkens" zu begrenzen. [97] Auch der Vergleich mit § 30 StGB zeigt, dass § 176 Abs. 4 Nr. 3 StGB einen erheblich größeren Anwendungsbereich hat. Bei § 30 StGB wird eine deutliche Beschränkung der Strafbarkeit dadurch erreicht, dass der Täter in jedem Fall einer zweiten Person seine rechtsfeindlichen Absichten offenbaren muss. Beim tatbestandsmäßigen Einwirken mit neutralen Nachrichten verbleibt die (nur *möglicherweise* vorhandene) rechtsfeindliche Gesinnung des Täters lediglich ein Internum. Im Vergleich zu § 176 Abs. 4 Nr. 3 StGB bezieht sich § 30 StGB auf Verbrechen, wodurch § 30 StGB eine noch weitere Begrenzung erfährt.[98] Eine solche ausreichende Begrenzung kann bei § 176 Abs. 4 Nr. 3 StGB nicht festgestellt werden. Stellt man also nur auf die Absicht des Täters ab, kommt auch das praktische Problem hinzu, dass die Absicht nur schwer erforschbar und nachweisbar ist, da diese allein in der Vorstellung des Täters existent ist.[99] Dies kann zu einer uneinheitlichen Rechtsanwendung und somit zu Einzelfallungerechtigkeiten führen, da die Feststellung der besonderen Absicht von vagen Prognosen einzelner Richter abhängt. Und das wiederum führt zu Unsicherheiten bezüglich der Reichweite der Strafnorm und widerspricht dem Bestimmtheitsgrundsatz.[100] Zwar ordnet der Gesetzgeber explizit an, dass bestimmte Handlungen dann den Tatbestand nicht erfüllen sollen, wenn der Täter mit der Kommunikation lediglich bezweckt, ein positives Gefühl der Kinder zu ihrem Körper und ihrer Sexualität zu entwickeln.[101] Hierbei ist aber wiederum die Qualifizierung der Handlung als strafwürdig lediglich von der Einbeziehung der Motivation des Täters möglich.[102] Der Versuch des Gesetzgebers, eine Ausklammerung von sozialadäquaten Verhaltensweisen vorzunehmen, muss an der Stelle als missglückt bewertet werden. Angesichts der Verlagerung des Unrechtsgehalts ins Subjektive und der damit einhergehenden Beweisschwierigkeiten erfährt der Tatbestand in seiner aktuellen Ausgestaltung kaum praktische Relevanz. Zurecht wird dem Tatbestand lediglich symbolischer (Droh-) Charakter zugesprochen.[103] Im Hinblick auf diese Ungereimtheiten und die Uferlosigkeit der Tathandlung des „Einwirkens", die stark an ein reines Gesinnungsstrafrecht grenzt, bedarf es an dieser Stelle einer einschränkenden Auslegung, um den vorgebrachten verfassungsrechtlichen Bedenken zu begegnen.[104]

dd) Notwendigkeit der restriktiven Auslegung

In der Literatur finden sich einige Ansatzpunkte hinsichtlich der restriktiven Auslegung des § 176 Abs. 4 Nr. 3 StGB. Teilweise wird vertreten, dass § 176 Abs. 4 Nr. 3 StGB nur auf Tathandlungen beschränkt werden solle, die auch tatsächlich einen sexuellen Inhalt vorweisen können. Anhaltspunkt dafür biete der

95 *Dencker,* StV 1988, 262 (263).
96 *Frauke*, Gesinnung und Straftat: Besinnung auf ein rechtsstaatliches Strafrecht, 2012, S. 234.
97 *Alexiou*, S. 335.
98 *Stoiber*, S. 229.
99 *Stratenwerth*, in: FS von Weber, 1963, S. 171 (189).
100 *Alexiou*, S. 338; *Wolters*, in: SK-StGB, § 176 Rn. 37.
101 BT-Drs. 15/350, S. 18.
102 *Alexiou*, S. 337.
103 *Fischer*, StGB, § 176 Rn. 15; *Funcke-Auffermann*, S. 148 f.
104 *Bezjak* (Fn. 77), S. 261.

systematische Vergleich von § 176 Abs. 4 Nr. 3 StGB mit § 176 Abs. 4 Nr. 4 StGB, der auf objektiver Ebene zwingend ein pornografisches Medium voraussetzt. Der identische Strafrahmen und ihre fehlende Versuchsstrafbarkeit würden eine gleiche Handhabung bekräftigen.[105] Diese sehr radikale Restriktion auf Schriften mit (nur) eindeutig sexuellem Inhalt widerspricht aber dem ausdrücklichen Willen des Gesetzgebers und scheint an der Stelle auch als zu kategorisch. Andere Stimmen in der Literatur wollen den weit gefassten Tatbestand des § 176 Abs. 4 Nr. 3 StGB über ein manipulatives Element des Einwirkens einschränken. Dieser Ansicht nach muss die Einwirkung in objektiver Hinsicht zwar keinen Sexualbezug enthalten, aber es muss ein nach außen sichtbares, manipulatives Moment aufweisen. Durch die Einwirkung muss das Kind in Richtung auf die vom Täter erstrebte sexuelle Handlung gelenkt werden.[106] Auch dieser Versuch einer restriktiven Auslegung ist aus der hier vertretenen Sicht abzulehnen, denn Manipulation zeichnet sich gerade dadurch aus, dass der Manipulierende sehr geschickt vorgeht und seine wahren Absichten nicht durchschaubar sind.[107] Der Manipulierende weiß (höchstens) nur selber um seine manipulativen Absichten. Schließlich sei der bereits erwähnte Vorschlag einer teleologischen Reduktion des Tatbestands von *Wolters* zu erwähnen. Demnach sollten die Fälle der neutralen Kommunikation dahingehend teleologisch reduziert werden, dass die Tathandlung auch objektiv ein sexualisiertes Klima schaffen soll, das die geplante nachfolgende sexuelle Handlung begünstigt. Hierfür sei es zwar nicht erforderlich, dass der Inhalt explizit ein sexuelles Geschehen enthält, wohl aber, dass sie durch einen eindeutigen Körperbezug objektiv dazu geeignet ist, die Neigung des Opfers zu spezifischem Sexualverhalten zu erhöhen.[108] Eine solche teleologische Reduktion scheint aus der hier vertretenen Sicht als geboten. Zwar wird gegen eine solche teleologische Reduktion zutreffend kritisch eingewandt, dass diese nicht mit dem Wortlaut als auch gesetzgeberischen Willen vereinbar ist.[109] Doch kann der Vergleich mit § 184h StGB als ein Argument für eine solche teleologische Reduktion angeführt werden. Auch § 184h StGB erfordert einen objektiven Sexualbezug. Handlungen, die aus der Sicht eines objektiven Betrachters offensichtlich nicht sexuell sind, können auch nicht als solche interpretiert werden. Dies selbst dann nicht, wenn eine sexuelle Absicht des Handelnden gegeben ist.[110] Dies kann in gleicher Weise auf § 176 Abs. 4 Nr. 3 StGB übertragen werden. Handlungen ohne jeglichen objektiven Sexualbezug können die ungestörte sexuelle Entwicklung der Kinder nicht beeinträchtigen.[111]

b) Weitere Kritikpunkte an der gesetzgeberischen Ausgestaltung des § 176 Abs. 4 Nr. 3 StGB

aa) Weitere Vorverlagerung durch § 176 Abs. 5 StGB

Es kommt wie bereits erwähnt bei § 176 Abs. 5 Var. 3 StGB zu einer noch weiteren Vorverlagerung der Strafbarkeit des § 176 Abs. 4 Nr. 3 StGB.[112] Es erscheint nicht verhältnismäßig, dass § 176 Abs. 5 Var. 3 StGB die Verabredung zu der Vorbereitung nach Abs. 4 Nr. 3 mit (derselben!) Strafe bedroht.[113] Die Kombination stellt eine Kriminalisierung einer Vorfeldhandlung in Bezug auf eine Vorfeld-Tat dar. Hierbei tritt der Gedanke eines am Rechtsgüterschutz orientierten Strafrechts noch weiter in den Hintergrund und es wird im Sinne eines reinen Gesinnungsstrafrechts Strafbarkeit konstruiert.[114] Da dieser Verweis aufgrund der Beweisschwierigkeiten und des

105 *Frühsorger*, S. 141.
106 *Bezjak* (Fn. 77), S. 262.
107 Duden, abrufbar unter: https://www.duden.de/rechtschreibung/manipulieren#bedeutungen (zuletzt abgerufen am 20.10.2020).
108 *Wolters*, in: SK-StGB, § 176 Rn. 37; a.A.: *Renzikowski,* in: MüKo-StGB, § 176 Rn. 44.
109 *Renzikowski*, in: MüKo-StGB, § 176 Rn. 44, *Eisele*, in: Schönke/Schröder, StGB, § 176 Rn. 14c.
110 *Laubenthal*, Rn. 103 f.
111 *Hörnle*, in: MüKo-StGB, § 184h Rn. 4.
112 *Bezjak* (Fn. 77), S. 325.
113 *Renzikowski*, in: MüKo-StGB, § 176 Rn. 15; *Stoiber*, S. 282.
114 *Lederer*, in: AnwaltK-StGB, § 176 Rn. 26.

geringeren Unrechtgehalts praktisch nicht bedeutsam sein dürfte, wäre es angemessen, die Tathandlung des § 176 Abs. 4 Nr. 3 StGB aus dem Verweis des § 176 Abs. 5 StGB herauszunehmen.[115]

bb) Begrenzte Einwirkungsformen

Im Schrifttum wird vermehrt kritisiert, dass es wenig überzeugend ist, dass nur die Einwirkung mittels Schriften oder Kommunikationsmitteln strafbar ist, während Einwirkungen anderer Art, bei dem es zu sexuellen Kontakten kommen soll, nicht darunterfallen. Unter „Schriften" im Sinne des § 11 Abs. 3 StGB versteht man Gedankenäußerungen durch Buchstaben, Bilder oder andere stoffliche Zeichen, die mit dem Seh- oder Tastsinn wahrnehmbar sind.[116] Darunter fallen also auch handgeschriebene Briefe, Bücher, aber auch Comics und Autogrammkarten.[117] Das heißt es macht sich strafbar, wer in der Absicht, das Kind zu sexuellen Handlungen zu bewegen, dem Kind ein Comic-Heft oder eine Autogrammkarte schenkt. Nicht strafbar macht sich aber derjenige, der in der gleichen Absicht das Kind mit Süßigkeiten oder Geldgabe oder anderen nicht unter den Schriftenbegriff zu subsumierenden Geschenken gefügig machen will.[118] Nicht strafbar sind auch nur rein verbale Überredungen unter Anwesenden, selbst wenn diese eindeutig einen Sexualbezug aufweisen und es noch vor Ort zum Sexualkontakt kommen soll, d. h. Einwirkung und Treffen zeitlich eng verbunden sind.[119] Es ist nicht nachvollziehbar, weshalb einerseits das Einwirken in sexueller Absicht im Internet mit § 176 Abs. 4 Nr. 3 StGB unter Strafe gestellt wird, aber reale Einwirkungshandlungen unter Anwesenden straflos bleiben sollen.[120] Die Gesetzesbegründung spricht zwar von der besonderen Gefährlichkeit der Anonymität, doch ist eine Gefahr außerhalb der virtuellen Welt genauso gegeben. Diese Konstellation ist aber nach geltendem Recht straflos.[121] Hier lässt sich zwar zu Gunsten des Gesetzgebers anführen, dass die Anonymität eine sehr große Rolle hinsichtlich der Hemmschwelle eines potentiellen Täters spielen kann, doch ist die Beschränkung auf die genannten Tatmittel dennoch wertungswidersprüchlich.[122] Wir schützen Kinder, aber nur online. Kinder sind sowohl in der virtuellen als auch in der realen Welt gleichermaßen vor Einwirkungen in sexueller Absicht schutzwürdig. Teilweise wird eine Ergänzung auf alle möglichen Einwirkungsarten, also auch verbaler Art, gefordert.[123] Ein Beispiel hierfür bietet das österreichische Recht, das insoweit bei der Ausgestaltung des Cyber-Grooming-Tatbestands an Einwirkungen „sonstiger Art unter Täuschung über die Absicht" anknüpft.[124] Andere Stimmen in der Literatur sehen dem „offline"-Einwirken mit der Strafbarkeit des unmittelbaren Ansetzens zum Missbrauch nach § 176 Abs. 6 StGB als Genüge getan.[125] Das österreichische Beispiel kann eine gute Lösungsmöglichkeit auch für Deutschland darstellen, um die Wertungswidersprüche zu beseitigen.

cc) Problem der starren Altersgrenze

Wie oben bereits erwähnt beschränkt sich die Strafbarkeit des Cyber-Grooming nicht nur auf Kontaktanbahnungen von Erwachsenen, sondern erstreckt sich auch auf Jugendliche und Heranwachsende. Als problematisch erweisen

115 *Bezjak* (Fn. 77), S. 325.
116 *Gercke,* in: Spindler/Schuster, Recht der elektronischen Medien Kommentar, 4. Aufl. (2019), § 176 Rn. 7.
117 *Frühsorger*, S. 136.
118 *Lederer*, in: AnwaltK-StGB, § 176 Rn. 21.
119 *Fischer*, StGB, § 176 Rn. 15.
120 *Eisele*, Computer- und Medienstrafrecht, 2013, S. 142.
121 *Fischer*, StGB, § 176 Rn. 15.
122 *Meier*, in: Hilgendorf/Rengier, S. 216.
123 *Frühsorger*, S. 269.
124 *Leinzinger*, Neue Tatbestände im Sexualstrafrecht zum Schutz Kinder und Jugendlicher: Notwendige Umsetzung von EU-Recht oder Exzess des Gesetzgebers?, 2012, S. 31.
125 *Eisele,* Abschlussbericht der Reformkommission zum Sexualstrafrecht v. 19.7.2017, abrufbar unter: https://www.bmjv.de/SharedDocs/Downloads/DE/Service/StudienUntersuchungenFachbuecher/Abschlussbericht_Reformkommission_Sexualstrafrecht.html (zuletzt abgerufen am 22.10.2020), S. 905 f.

sich in diesem Zusammenhang Konstellationen der einvernehmlichen Sexualkontakte zwischen beispielsweise einer oder einem 13-Jährigen und einer oder einem 14-Jährigen. Diese können aber gerade altersgemäße Erfahrungen darstellen, die für eine gesunde sexuelle Entwicklung notwendig sind. Die Kriminalisierung solcher Kontakte liefe gerade der „ungestörten sexuellen Entwicklung" der Kinder entgegen.[126] Es stellt sich also das allgemeine Problem, wie mit sexuellen Handlungen zwischen älteren Kindern und (geringfügig älteren) Jugendlichen umgegangen werden soll. Auf § 176 Abs. 4 Nr. 3 StGB übertragen sind solche Fälle diskussionswürdig, in denen Jugendliche mit sexuellen Absichten auf ältere Kinder einwirken (z.B. im Internet sexuelle Fantasien austauschen).[127] Dies kann eine altersgemäße Erfahrung darstellen. Daher grenzt das Kriminalisieren solcher Verhaltensweisen an Absurdität. Doch kann hier argumentiert werden, dass vor allem aus Rechtssicherheitsgründen der Gesetzgeber eine klare Grenze ziehen muss.[128] Unbillige Ergebnisse können im Wege der strafprozessualen Einstellungsmöglichkeiten korrigiert werden.[129] Stimmen in der Literatur fordern bei § 176 StGB eine dem § 174 Abs. 5 StGB entsprechende Lösung, der eine Möglichkeit des Absehens von Strafe vorsieht, wenn das Unrecht der Tat gering ist.[130] Dies könnte auch eine mögliche Korrektur darstellen, aber es ist nicht ersichtlich, welchen Vorteil es gegenüber der strafprozessualen Einstellungsmöglichkeiten darstellen soll.[131] Die starre Altersgrenze kann zu Grenzfällen führen, die tatsächlich im Einzelfall nicht strafwürdig sind, aber zum einen muss es erst zu einer Strafverfolgung in solchen Fällen kommen, was bei Einvernehmlichkeit in der Regel nicht der Fall sein dürfte und zum anderen sprechen gewichtigere, auch praktikable Gründe dafür, bei einer klaren Altersgrenze zu verbleiben.

dd) Absichtserfordernis in § 176 Abs. 4 Nr. 3 lit. a)

Eine Inkonsistenz lässt sich auch im Hinblick auf das Absichtserfordernis des § 176 Abs. 4 Nr. 3 lit. a) StGB verzeichnen, denn es wird nicht die subjektive Absicht erfasst, dass *der Täter* gem. § 176 Abs. 4 Nr. 1 StGB sexuelle Handlungen *vor* einem Kind *an sich selbst oder einem Dritten* vornimmt.[132] Es scheint wertungswidersprüchlich, dass sich einerseits nicht strafbar macht, wer das Kind dazu bringen will, mit dem Täter über eine Internetkamera in Kontakt zu treten, damit der Täter vor dem Kind sexuelle Handlungen an sich oder einem Dritten vornehmen kann, sich andererseits aber dann strafbar macht, wenn er in dieser Situation die Absicht hat, das Kind dazu zu bringen, dass es sexuelle Handlungen vor dem Täter oder einem Dritten vornimmt. Ein Unterschied im Unrechtsgehalt dieser Handlungsalternativen lässt sich nicht verzeichnen.[133] Somit wäre das Absichtserfordernis zur Vollständigkeit zu erweitern.

ee) Unverhältnismäßigkeit des Strafrahmens

Des Weiteren ist zu bemängeln, dass der Strafrahmen für § 176 Abs. 4 Nr. 3 StGB im Vergleich zu den Nr. 1, 2 und 4 des § 176 Abs. 4 StGB nicht angemessen ist.[134] Während bei Nr. 1, 2 und 4 das Kind jeweils unmittelbar mit Sexualität konfrontiert wird, umfasst § 176 Abs. 4 Nr. 3 StGB lediglich eine Vorbereitungshandlung, die objektiv gar keinen Sexualbezug aufweisen muss.[135] Aufgrund der geringeren Rechtsgutsgefährdung der in

126 *Fischer*, StGB, § 176, Rn. 2.
127 *Stoiber*, S. 153.
128 *Schetsche*, MSchrKrim 1994, 201 (212 f.).
129 *Stoiber*, S. 154.
130 *Bezjak* (Fn. 77), S. 335.
131 *Hörnle*, in: LK-StGB, Vor §§ 174, Rn. 63.
132 *Eschelbach*, in: Matt/Renzikowski, StGB, § 176 Rn.21.
133 *Bezjak* (Fn. 77), S. 332.
134 *Stoiber*, S. 264.
135 *Frühsorger*, S. 141.

§ 176 Abs. 4 Nr. 3 StGB normierten Tathandlung wäre eine Anpassung des Strafrahmens bei § 176 Abs. 4 Nr. 3 StGB erforderlich.[136] Die Erhöhung der Mindeststrafe von der bisherigen Geldstrafe auf drei Monate Freiheitsstrafe ist, angesichts der zu erwartenden Vielzahl von Bagatelldelikten der zuvor beschriebenen Art, jedenfalls unangemessen.[137]

2. Versuchsstrafbarkeit am untauglichen Objekt

Trotz der vorbezeichneten Kritikpunkte an der gesetzgeberischen Ausgestaltung des vollendeten Cyber-Grooming hat der Gesetzgeber die eingeschränkte Versuchsstrafbarkeit für den Versuch des Cyber-Grooming an einem untauglichen Tatobjekt gem. § 176 Abs. 6 S. 2 StGB eingeführt. Durch die Neufassung von § 176 Abs. 6 StGB soll die Versuchsstrafbarkeit auf sog. „Scheinkind"-Fälle konzentriert werden. Der Gesetzgeber begründet die Einführung der Strafbarkeit des Versuchs damit, dass im Sinne einer Spezial- und Generalprävention die Strafbarkeit nicht davon abhängen könne, ob das vom Täter kontaktierte Kind seiner Vorstellung entsprechend tatsächlich ein Kind ist oder nicht.[138] In der am Anfang dieser Arbeit aufgezeigten Stichprobe des BKA verwirklichten die entsprechenden Chatpartner schon deshalb nicht den Cyber-Grooming-Tatbestand, weil sie statt eines 13-jährigen Mädchens tatsächlich einen BKA-Ermittler adressierten. Den Ermittlern waren in solchen Fällen selbst dann die Hände gebunden, wenn es tatsächlich zu einer Verabredung zum Zweck der Anfertigung pornographischer Bilder kam.[139] Einerseits ist der Ärger von Strafverfolgungsbeamten nachvollziehbar, dass es unbefriedigend ist, wenn der Täter straflos bleibt, weil er nicht auf ein Kind, sondern eine erwachsene Ermittlungsperson einwirkt. Dies gilt vor allem dann, wenn es sogar zu einem konkreten Treffen kommt und der Täter z.B. Werkzeuge mit sich führt, um das Kind zu missbrauchen. In solchen Handlungen kann auch noch kein unmittelbares Ansetzen zu einem versuchten sexuellen Missbrauch nach § 176 Abs. 1 und Abs. 6 StGB gesehen werden. Von einem solchen Blickwinkel kann die zuvor fehlende Versuchsstrafbarkeit beim Cyber-Grooming, die immer wieder gefordert wurde, tatsächlich Bedenken hervorrufen.[140] Aber andererseits kann nicht zum scharfen Schwert des Strafrechts bei so fernliegenden Gefahren durch Verhaltensweisen gegriffen werden, die mangels tauglichen Tatobjekts rein faktisch zu keiner Rechtsgutsbeeinträchtigung führen können. Eine solche Gesetzespraxis wird nur zu einer unübersehbaren Ausuferung des Strafrechts führen.[141] Nach dem Subsidiaritätsgedanken des Strafrechts muss da, wo Gefahren wirksam auch mit anderen Mitteln begegnet werden kann, das Strafrecht als Ultima-Ratio zurücktreten.[142] Es besteht schon gar kein Strafbedürfnis im Hinblick auf sog. „Schein-Kind"- Fälle. Das Ziel der Abschreckung potentieller Täter kann auch durch bestehende gefahrenabwehrrechtliche Maßnahmen erreicht werden. Durch das an sich legale Verhalten des Chattens mit einem Erwachsenen (Polizeibeamten) kann bereits ein Anfangsverdacht für weitere Ermittlungstätigkeiten begründet werden.[143] Der Anfangsverdacht kann seinerseits eine Hausdurchsuchung und eine Beschlagnahme des Computers rechtfertigen, weil sich der Beschuldigte durch sein Verhalten nach der kriminalistischen Erfahrung hinreichend verdächtig macht, bereits eine Straftat nach § 176 Abs. 4 Nr. 3 StGB zum Nachteil von „echten" Kindern begangen zu haben.[144] Des Weiteren besteht die

136 *Stoiber*, S. 264.
137 *Funcke-Auffermann/Amelung,* StraFo 2004, 266.
138 BT-Drs. 19/13836, S. 1.
139 *Schneider,* KriPoZ 2020, 137 (138).
140 *Eisele* (Fn. 125), S. 901.
141 *Lagodny*, in: Hefendehl, Die Rechtsgutstheorie – Legitimationsbasis des Strafrechts oder dogmatisches Glasperlenspiel?, 2003, S. 87.
142 *Roxin/Greco*, Strafrecht AT, Band 1, 5. Aufl. (2020), § 2 Rn. 97.
143 *Van Edern,* NJW 2020, 1035.
144 *Bezjak,* Abschlussbericht Reformkommission (Fn. 125), S. 850.

Möglichkeit einer polizeilichen Gefährderansprache.[145] Der Gesetzgeber führt in der Gesetzesbegründung auf, dass es keinen Unterschied mache, ob die Äußerung des Täters ein Kind erreicht oder nicht, denn seine rechtsfeindliche Gesinnung träte in beiden Fällen zum Vorschein.[146] Das Argument ist hierbei jedoch sehr widersprüchlich, denn der „böse Wille" des Täters tritt auch bei einem tauglichen Versuch zum Vorschein, der aus beispielsweise technischen Gründen im Versuchsstadium bleibt. Dieser ist jedoch nicht unter Strafe gestellt. Einer Rechtsgutsgefährdung kommt aber ein solcher tauglicher Versuch viel näher als derjenige, der von vornherein nicht geeignet ist, das Schutzobjekt „Kind" zu gefährden. Durch die Einführung der Versuchsstrafbarkeit für § 176 Abs. 4 Nr. 3 StGB in seiner jetzigen Fassung werden Handlungen strafrechtlich erfasst, die sich noch weiter im Vorfeld der eigentlichen Rechtsgutsgefährdung bewegen, als dies bei § 176 Abs. 4 Nr. 3 StGB ohnehin schon der Fall ist, bzw. den Rechtsgutsbezug gänzlich verlieren. Ein Gewinn an Rechtsgüterschutz ist durch die beschränkte Versuchsstrafbarkeit nicht gegeben, da bereits keine unmittelbar gefährliche Handlung verboten wird.[147] Die Kriminalisierung des untauglichen Versuchs beim Cyber-Grooming verstößt gegen das Ultima-Ratio-Prinzip eines am Rechtsgüterschutz orientierten Strafrechts und ist verfassungsrechtlich mehr als fragwürdig.

V. Zusammenfassung und Fazit

In der Gesamtbetrachtung lässt sich festhalten, dass die Norm des § 176 Abs. 4 Nr. 3 StGB in der jetzigen Ausgestaltung strafrechtlichen Normsetzungsbefugnissen nicht standhält. Die sehr weite Vorfeldkriminalisierung und der damit einhergehende fehlende Rechtsgutsbezug im Hinblick auf nur online-verbleibende Kontakte mit neutraler Kommunikation macht den § 176 Abs. 4 Nr. 3 StGB schon de lega lata restriktionsbedürftig. Auch die anderen Inkonsistenzen in Bezug auf § 176 Abs. 4 Nr. 3 StGB schreien nach einem dringenden Korrektur- und Überarbeitungsbedarf. Wie bereits erwähnt handelt es sich beim Cyber-Grooming-Tatbestand einerseits um die prompte Reaktion des Gesetzgebers auf immer wieder bekanntgewordene Fälle von Cyber-Grooming, andererseits folgte er europarechtlichen Vorgaben. Der Vergleich mit den europarechtlichen Vorgaben zeigt jedoch, dass die jetzige Ausgestaltung des Cyber-Grooming-Tatbestands die europäischen Vorgaben übererfüllt.[148] Nach Art. 6 Abs. 1 der Richtlinie 2011/93/EU soll ein Erwachsener unter Strafe gestellt werden, der mit Hilfe der Informations- und Kommunikationstechnologien ein Treffen mit einem Kind vorschlägt, um dieses sexuell zu missbrauchen, sofern auf diesen Vorschlag Handlungen vorgenommen werden, die auf ein solches Treffen hinführen.[149] Nach EU-Recht ist nämlich eine *konkrete* Vorbereitung eines *konkreten* sexuellen Übergriffs strafwürdig.[150] Die Tathandlung ist also nach der europäischen Vorgabe viel enger gefasst. Die Fassung der europäischen Richtlinie scheint aus der hier vertretenen Sicht vorzugswürdig. Der Gesetzgeber muss zwar aus europarechtlicher Sicht – da es sich bei der EU-Richtlinie um Mindestvorschriften handelt – die Norm des § 176 Abs. 4 Nr. 3 StGB nicht korrigieren, aber aufgrund der vorbezeichneten Kritikpunkte sollte er es, vor allem in Hinblick auf verfassungsrechtliche Bedenken, dringend tun. Hierbei bietet es sich bei der Überarbeitung der Vorschrift an, sich mehr an den europäischen Vorgaben zu orientieren. Erst nach der Überarbeitung des § 176 Abs. 4 Nr. 3 StGB kann über eine sinnvolle Versuchsstrafbarkeit, dann aber auch des tauglichen Versuchs, gesprochen werden.

145 *Fischer* (Fn. 21), S. 3.
146 BT-Drs. 19/13836, S. 10.
147 *Fischer* (Fn. 21), S. 2 f.
148 *Eisele*, in: Hilgendorf/Rengier, S. 710.
149 *Eisele*, in: Hilgendorf/Rengier, S. 708.
150 *Renzikowski* in: MüKo-StGB, § 176 Rn. 54.

VI. Schlusswort

„Reflektierte Gesetzgebung sieht anders aus!“[151]

Diese empörte Äußerung aus dem Schrifttum kann hier lediglich durch ein weiteres Ausrufezeichen ergänzt werden. Es wäre wünschenswert, dass die verfassungsrechtlich fundierten Gestaltungsgrundsätze wieder zunehmend Einfluss gewinnen; namentlich das Ultima Ratio-Prinzip.[152]

[151] *Renzikowski*, in: MüKo-StGB, § 176 Rn. 44.
[152] *Britz,* jM 2018, 389.

KriPoZ Kriminalpolitische Zeitschrift JuP

„Junges Publizieren“

Seminararbeit von

Laura Schachtner

Der strafprozessuale Zugriff auf Handy-Daten und Gästelisten in Zeiten der Pandemie

Prüfer: Prof. Dr. Mark Zöller
Universität: Ludwig-Maximilians-Universität München
Abgabedatum: 30.9.2020

Inhaltsverzeichnis

I. Die Corona-Pandemie

Seit Jahresbeginn wird die Welt von einer Krise beherrscht: der Corona-Pandemie. Seit seiner Entdeckung hat das Sars-CoV-2-Virus sich sehr schnell ausgebreitet, da es durch „Tröpfcheninfektion" leicht übertragen werden kann. Das Virus hat durch hohe Infektionszahlen in manchen Ländern zu einer Überlastung des Gesundheitssystems geführt.[1] Um die Ausbreitung des Virus in Deutschland zu verhindern, sind daher Schutzmaßnahmen ergriffen worden. Zum Beispiel ist eine Corona-Warn-App entwickelt worden, die den Nutzer bei Kontakt mit einer infizierten Person benachrichtigt.[2] Zudem sind Restaurants verpflichtet, Gästelisten zu führen, um bei einer Infektion alle Kontaktpersonen informieren zu können. Bei diesen Prozessen werden sehr viele Daten von den Bürgern aufgezeichnet. Diese sind in einigen Bundesländern von der Polizei genutzt worden, um die Aufklärung von Straftaten voranzutreiben.[3] Dies hat die Frage aufgeworfen, ob solche Datenerhebungen zulässig sind. Daher soll diese Arbeit die Rechtslage in Bezug auf den strafprozessualen Zugriff auf zur Eindämmung der Pandemie erhobene Handy-Daten und Gästelisten zu Strafverfolgungszwecken aufzeigen.

II. Strafprozessualer Zugriff auf zur Eindämmung der Pandemie erhobene Handy-Daten und Gästelisten zu Strafverfolgungszwecken

Um die strafprozessuale Rechtslage einordnen zu können, müssen zunächst ein paar grundlegende Fragen geklärt werden. Begonnen wird hierbei mit der Rechtsgrundlage für die Erhebung der Daten.

1. Die Erhebung der Daten aufgrund der Pandemie

Jedes staatliche Handeln beruht auf einer Ermächtigungsgrundlage.[4] So muss auch das Erheben von Handy-Daten und Gästelisten auf einer Rechtsgrundlage beruhen. Die Handy-Daten, die zur Zeit einer Pandemie erhoben werden, beinhalten den Aufenthaltsort, den Kontakt mit anderen Menschen und die Möglichkeit sich infiziert zu haben.[5] Je nach angegebenen Daten lassen sich aus den Gästelisten der Aufenthaltsort, der Name, die Adresse, die Telefonnummer und die E-Mail-Adresse ableiten.[6] Hierbei handelt es sich um personenbezogene Daten, da sie sich auf eine identifizierte beziehungsweise identifizierbare Person beziehen.[7] Zwar ist es möglich, die Daten, wie bei der Warn-App, durch temporäre Identifikationsnummern zu anonymisieren, die Person muss aber dennoch identifizierbar sein, um sie über eine mögliche Infektion zu informieren.[8]

Als Rechtsgrundlage für den Zugriff auf personenbezogene Daten fungiert die Datenschutz-Grundverordnung (DSGVO), die als Öffnungsklausel die Nutzung der Daten gestattet. Laut Art. 6 Abs. 1 S. 1 lit. a und Art. 9 Abs. 2 S. 2 lit. a DSGVO i. V. m. Art. 4 Nr. 11 DSGVO ist die Datenerhebung grundsätzlich nach einer

1 *Busch*, Corona-Krise: Welche Folgen hat die Pandemie für unser Gesundheitssystem? vom 11.5.2020, abrufbar unter: https://www.bpb.de/politik/innenpolitik/coronavirus/309530/gesundheitsversorgung (zuletzt abgerufen am 28.9.2020), Frage 2; *Dochow*, GuP 2020, 129 (130); WHO Europa, Pandemie der Coronavirus-Krankheit (COVID-19), abrufbar unter: https://www.euro.who.int/de/health-topics/health-emergencies/coronavirus-covid-19/novel-coronavirus-2019-ncov (zuletzt abgerufen am 28.9.2020).
2 *Dochow*, GuP 2020, 129 (131); *Kuhlmann*, GSZ 2020, 115 (116); *Müller*, MMR 2020, 355 (355).
3 *Aden/Arzt/Fährmann*, Corona-Gästelisten – maßlose polizeiliche Datennutzung, vom 14.8.2020, abrufbar unter: https://verfassungsblog.de/corona-gaestelisten-masslose-polizeiliche-datennutzung/ (zuletzt abgerufen am 28.9.2020), Einleitung.
4 *Zöller*, Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaft und Nachrichtendiensten, 2002, S. 32.
5 *Dochow*, GuP 2020, 129 (131); *Kuhlmann*, GSZ 2020, 115 (115).
6 *Aden/Arzt/Fährmann*, Einleitung.
7 Art. 4 Nr. 1 DSGVO.
8 *Kuhlmann*, GSZ 2020, 115 (117).

freiwilligen Einwilligung des Betroffenen möglich.[9] Es gibt aber durchaus Ausnahmeregelungen, die den Zugriff auf die Daten ohne Einwilligung erlauben, wenn das Allgemeininteresse überwiegt. Bei einer Pandemie besteht dieses Interesse im Schutz der Bürger vor Gesundheitsgefahren.[10] Die Art. 6 Abs. 1 S. 1 lit. e, d, f DSGVO erlauben die Datenverarbeitung nicht sensibler Daten bei Wahrnehmung von Aufgaben im öffentlichen Interesse und zum Schutz lebenswichtiger oder berechtigter Interessen. Der Schutz der Gesundheit der Bevölkerung vor einer Pandemie stellt gerade ein solches Interesse dar. Für Art. 6 Abs. 1 S. 1 lit. d DSGVO wird dies explizit in Erwägungsgrund 46 S. 3 festgesetzt, da dieser als Grund der Datenerhebung die Überwachung der Ausbreitung von Epidemien benennt.[11] Die Verarbeitung sensitiver Daten wird durch Art. 9 Abs. 2 lit. i DSGVO ermöglicht. Dieser billigt die Verarbeitung von Gesundheitsdaten, wenn dies im Bereich der öffentlichen Gesundheit notwendig ist, um vor grenzüberschreitenden Gesundheitsgefahren zu schützen.[12] All diese Normen sind jedoch lediglich „Öffnungsklauseln". Man benötigt für die Datenerhebung noch eine gesetzliche Rechtsgrundlage im deutschen Recht. Im Bundesdatenschutzgesetz (BDSG) ist mit § 3 eine Generalklausel geschaffen worden, die die Datenverarbeitung erlaubt, wenn der Verantwortliche sie für seine Tätigkeit benötigt.[13] § 22 Abs. 1 Nr. 1 lit. c BDSG stellt die Rechtsgrundlage dar, um im Bereich der öffentlichen Gesundheit auch sensible Daten zu verarbeiten. Des Weiteren gestattet § 13 Abs. 1 Infektionsschutzgesetz (IfSG), die Daten zur Überwachung von Epidemien zu verarbeiten.[14] Zum Zwecke der Bekämpfung der Pandemie sind zudem Verordnungen durch die Bundesländer geschaffen worden, die die Erhebung von Daten zur Eindämmung der Pandemie gestatten.[15] Diese Normen verkörpern somit die Ermächtigungsgrundlagen zur Erhebung personenbezogener Daten zur Bekämpfung und Eindämmung der Pandemie.

2. Der Eingriff in das Recht auf informationelle Selbstbestimmung durch Zugriff der Strafverfolgungsbehörden

Wie im Zusammenhang mit den Rechtsgrundlagen festgestellt, handelt es sich bei den aufgezeichneten Informationen um personenbezogene Daten. Um diese in Zeiten moderner Technologien vor staatlichen Eingriffen zu schützen, hat das *BVerfG* im Volkszählungsurteil das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 und Art. 1 Abs. 1 GG herausgearbeitet. Es gewährleistet das Recht, selbst zu bestimmen, wie, wann, von wem und in welchem Umfang persönliche Daten erhoben und verwendet werden.[16] Dies umfasst den Schutz vor unbegrenzter Erhebung, Speicherung, Weitergabe und Verwendung persönlicher Daten und erteilt dem Betroffenen die Befugnis, über die Verwendung selbst zu bestimmen.[17] Dieser Schutz ist wichtig, damit der Staat sich mit den zugänglichen Informationen kein komplettes Bild der Betroffenen erschaffen und der Bürger die Verwendung seiner Daten nachvollziehen kann.[18] Aber auch dieses Grundrecht ist nicht schrankenlos gewährleistet. Da der Mensch in die Gemeinschaft eingebunden ist, betreffen viele seiner Daten die Allgemeinheit.[19] Daher kann das Recht auf informationelle Selbstbestimmung wegen überwiegender Interessen der Allgemeinheit nach

9 *Kuhlmann*, GSZ 2020, 115 (118).
10 *Kuhlmann*, GSZ 2020, 115 (119).
11 *Kuhlmann*, GSZ 2020, 115 (119, 120, 121).
12 *Kuhlmann*, GSZ 2020, 115 (121).
13 *Dochow*, GuP 2020, 129 (139); *Kuhlmann*, GSZ 2020, 115 (119 f.).
14 *Kuhlmann*, GSZ 2020, 115 (120).
15 *Aden/Arzt/Fährmann*, Einleitung.
16 *Zöller*, S. 25, 26, 27.
17 *Zöller*, S. 28.
18 *Zöller*, S. 29.
19 *Zöller*, S. 40 f.

dem Gebot des Gesetzesvorbehalts durch ein Gesetz eingeschränkt werden.[20] Ein Eingriff in das Recht auf informationelle Selbstbestimmung liegt grundsätzlich dann vor, wenn Informationen zwangsweise vom Staat erhoben werden.[21] Bei den Gästelisten liegt Zwang vor, da die Bürger ihre Angaben hinterlassen müssen.[22] Dieser Eingriff zur Bekämpfung der Pandemie lässt sich durch eine Abwägung mit der Gefahr für die Gesundheit der Bevölkerung rechtfertigen.[23] Die Sammlung von Handy-Daten hingegen erfolgt durch eine freiwillige Einwilligung,[24] welche den Verzicht auf den Schutz des Grundrechtes darstellt.[25] Daher ist die Datenerhebung zur Eindämmung der Pandemie rechtmäßig. Wenn nun die Strafverfolgungsbehörden auf diese rechtmäßig erhobenen Daten zugreifen, stellt dies einen weiteren Eingriff in das Recht auf informationelle Selbstbestimmung dar, da es sich bei jeder Weitergabe an eine Behörde um einen neuen Eingriff handelt.[26] Daher wird für diesen Zugriff eine eigene gesetzliche Grundlage, etwa in der StPO, benötigt.

3. Allgemeine verfassungsrechtliche Grundlagen

Um die Rechtmäßigkeit eines Eingriffs durch und auf Grund strafprozessualer Vorschriften beurteilen zu können, müssen die allgemeinen verfassungsrechtlichen Grundlagen beachtet werden. Die Ermächtigungsgrundlagen müssen mit den verfassungsrechtlichen Vorschriften vereinbar sein, um einen Eingriff zu rechtfertigen.[27]

a) Allgemeine Voraussetzungen der gesetzlichen Grundlagen

Wie bereits erwähnt, muss jeder Eingriff in ein Grundrecht auf einer Rechtsgrundlage beruhen. Diese Rechtsgrundlage muss die verfassungsrechtlichen Gebote der Bestimmtheit und der Normenklarheit erfüllen.[28] Sie muss so formuliert sein, dass der Bürger die Rechtslage klar erkennen kann.[29] Die Eingriffsermächtigungen müssen daher den Anlass, den Zweck und die Grenzen der Datenverarbeitungsbefugnis ausweisen.[30] Die Verpflichtung, den Zweck der Datenverarbeitung gesetzlich festzulegen, wird Zweckbindungsgebot genannt. Dieses soll vor übermäßiger Verwendung personenbezogener Daten schützen, da die Daten nur zu einem bestimmten Zweck erhoben und verwendet werden dürfen. So schützt dieses Gebot vor einer zweckentfremdenden Nutzung.[31] Jede Zweckänderung benötigt daher eine eigene Eingriffsgrundlage.[32] Eine solche Ermächtigungsgrundlage muss auch verhältnismäßig sein. Dementsprechend müssen die vorgegebenen Datenerhebungs- und Datenverarbeitungsmaßnahmen ein legitimes Ziel verfolgen und zu dessen Erreichung geeignet, erforderlich und angemessen sein.[33]

b) Zweckentfremdung

Auch die Datenerhebung von Handy-Daten und Gästelisten muss nach dem Zweckbindungsgedanken an einen

20 *Engelhardt*, Verwendung präventivpolizeilich erhobener Daten im Strafprozess, 2011, S. 96.
21 *Zöller*, S. 34.
22 *Aden/Arzt/Fährmann*, Einleitung.
23 *Aden/Arzt/Fährmann*, Staatlicher Schutzauftrag.
24 *Kuhlmann*, GSZ 2020, 115 (118).
25 *Bodenbenner*, Präventive und repressive Datenverarbeitung unter besonderer Berücksichtigung des Zweckbindungsgedankens, 2017, S. 35.
26 *Zöller*, StV 2019, 419 (420).
27 *Bodenbenner*, S. 35; *Engelhardt*, S. 96.
28 *Engelhardt*, S. 103.
29 *Bertram*, Die Verwendung präventiv-polizeilicher Erkenntnisse im Strafverfahren, 2009, S. 131.
30 *Bodenbenner*, S. 69.
31 *Engelhardt*, S. 78, 86 f.; *Zöller*, StV 2019, 419 (420).
32 *Bodenbenner*, S. 126.
33 *Bertram*, S. 134, 136; *Zöller*, S. 46.

bestimmten Zweck gebunden sein. Da diese Daten zur Nachvollziehung der Infektionsketten aufgezeichnet werden, werden sie zum Schutz der Gesundheit der Bevölkerung erhoben. Die Strafverfolgungsbehörden greifen aber zum Zweck einer effektiven Strafverfolgung auf diese Daten zu.[34] Die Daten würden demnach zweckentfremdet werden. Fraglich ist daher, ob der Zweckbindungsgedanke durch eine zweckändernde Datenverarbeitung durchbrochen werden darf. Eine zweckändernde Datenverarbeitung muss generell möglich sein, da das Recht auf informationelle Selbstbestimmung nicht schrankenlos gewährleistet ist und wegen überwiegender Allgemeininteressen eingeschränkt werden kann.[35] Die Übermittlung der Daten an die Strafverfolgungsorgane stellt einen eigenständigen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Zudem vertieft sie den Grundrechtseingriff der Erhebung, da die Daten nochmals verwendet werden. Daher müssen besonders hohe Ansprüche an die Zweckänderungsermächtigung gestellt werden.[36] Zur verfassungsrechtlichen Rechtfertigung des neuen Eingriffs wird eine neue Rechtsgrundlage benötigt. Diese muss als Zweckänderungsermächtigung den Zweck der Übermittlung, deren Voraussetzungen und den Umfang der neuen Nutzung klar beinhalten und stellt somit die Übernahmeklausel für die Annahme der Daten dar. Überdies muss es eine Öffnungsklausel geben, die die Übermittlung der Daten erlaubt.[37] Die Vorschrift muss zudem die allgemeinen verfassungsrechtlichen Anforderungen, wie die Gebote der Bestimmtheit, der Normenklarheit und der Verhältnismäßigkeit, erfüllen.[38] Im Laufe der Zeit hat das *BVerfG* im Bereich der Verhältnismäßigkeit im Hinblick auf die Strafverfolgung eine neue Rechtsfigur für die Abwägung entwickelt: Den qualifizierten hypothetischen Ersatzeingriff. Dieser soll dafür Sorge tragen, dass der Erhebungszweck mit dem geänderten Verwendungszweck vereinbar ist und die Erhebungsbegrenzungen eines Rechtsgebiets nicht umgangen werden.[39] Der qualifizierte hypothetische Ersatzeingriff erlaubt die zweckändernde Datennutzung daher nur, wenn die Behörde die Daten für den geänderten Zweck auf dieselbe Weise hätte erheben dürfen.[40] Dabei muss auf die Eingriffstiefen, Anordnungsbefugnisse und die spezifischen Voraussetzungen der Maßnahme geachtet werden.[41]

c) Die allgemeinen Abwägungskriterien der Verhältnismäßigkeitsprüfung im Falle der Handy-Daten und der Gästelisten

Die strafprozessualen Ermächtigungsgrundlagen müssen diese allgemeinen Anforderungen erfüllen, damit ihre Anwendung rechtmäßig ist. Die Rechtmäßigkeit entscheidet sich vor allem im Rahmen der Verhältnismäßigkeitsprüfung. Beim Zugriff auf Handy-Daten und Gästelisten müssen hierbei einige Aspekte besonders berücksichtigt werden, die im Folgenden kurz erläutert werden.

aa) Entgegenstehendes Interesse: effiziente Strafverfolgung

Um den Eingriff in das Recht auf informationelle Selbstbestimmung rechtfertigen zu können, müssen die entgegenstehenden Interessen in der Verhältnismäßigkeitsprüfung gegeneinander abgewogen werden.[42] Ziel der strafprozessualen Vorschriften ist eine funktionierende und effektive Strafverfolgung.[43] Durch das Strafprozessrecht

34 *Aden/Arzt/Fährmann*, Einleitung; *Kuhlmann*, GSZ 2020, 115 (119); *Zöller*, S. 55 f., 59 f.
35 *Bodenbenner*, S. 125 f.
36 *Bodenbenner*, S. 130 f., 170; *Zöller*, StV 2019, 419 (421).
37 *Engelhardt*, S. 219 f.; *Zöller*, StV 2019, 419 (421).
38 *Engelhardt*, S. 103; *Zöller*, StV 2019, 419 (421).
39 *Bodenbenner*, S. 137, 140.
40 *Bodenbenner*, S. 138, 143.
41 *Bodenbenner*, S. 144.
42 *Bodenbenner*, S. 130, 134, 135.
43 *Bodenbenner*, S. 134; *Zöller*, S. 55 f., 59 f.

werden aufgrund eines Anfangsverdachts Straftatbestände untersucht, die Wahrheit ermittelt und Sanktionen verhängt.[44] So sorgt das Strafprozessrecht für ein geordnetes Zusammenleben der Gesellschaft und für Rechtsfrieden.[45] Um diesen Pflichten nachkommen zu können, müssen die Strafverfolgungsbehörden Zugriff auf personenbezogene Daten erhalten, da diese einen Anfangsverdacht begründen, bei den Ermittlungen helfen und als Beweismittel dienen können.[46] Werden in diesem Bestreben jedoch Freiheitsrechte von Bürgern beeinträchtigt, muss gegebenenfalls die Strafverfolgung hinter diesen zurückstehen.[47] Dabei wird das Strafverfolgungsinteresse in der Abwägung nach der Schwere der Tat, der Aufklärungswahrscheinlichkeit und dem Verdachtsgrad bemessen.[48]

bb) Allgemeine Abwägungskriterien beim Zugriff auf Handy-Daten

Um die Rechtmäßigkeit des Zugriffs auf Handy-Daten überprüfen zu können, muss die Bedeutung der Daten bei der Abwägung beachtet werden. Nur so kann festgestellt werden, wie hoch die Anforderungen an die Ermächtigungsgrundlage und den Zugriff sind. Hierbei sind drei Punkte besonders zu beachten: die Anonymisierung und Bedeutsamkeit der Daten sowie die Streubreite des Eingriffs. Handy-Daten, die zur Bekämpfung einer Pandemie gesammelt werden, sind Kontaktdaten. Diese Daten zeigen an, mit wem man Kontakt hatte, und verdeutlichen das Vorliegen einer (möglichen) Infektion. Dabei können die Daten bei dem Nutzer selbst oder auf einem Server eines Providers gespeichert sein. Bei der Corona-Warn-App wird festgestellt, wer sich nahe und lange genug für eine Infektion neben einer weiteren Person aufgehalten hat. Diese Daten werden als temporäre Identifikationsnummern für 14 Tage auf dem Gerät des Nutzers gespeichert. Zudem wird diese Nummer im Falle einer Infektion an einen Server gesendet, von dem die anderen Nutzer diese herunterladen können.[49] Daher müssen bei dieser Art der Datensammlung bezüglich des strafprozessualen Zugriffs auf Handy-Daten einige Punkte beachtet werden. Der erste Punkt betrifft die Anonymisierung. Anonym sind Daten, die keiner natürlichen Person mehr zuzuordnen sind. Daher sind anonyme Daten keine personenbezogenen Daten mehr und erhalten nicht den Schutz des Rechts auf informationelle Selbstbestimmung.[50] Laut der DSGVO sind Daten einer Person zuzuordnen, wenn sie sich anhand einer Kennung oder besonderer Merkmale zuordnen lassen. Die temporären Identifikationsnummern stellen zwar keine direkten Angaben zu einer Person dar, sie schließen aber eine Zuordnung zu einer bestimmten Person nicht aus. Diese kann vor allem während der Kommunikation zwischen Nutzer und Server stattfinden, da bei diesem Vorgang viele Daten benötigt werden, die eine Identifizierung erleichtern. Daher stellen diese Daten nur Pseudonyme dar, die als personenbezogene Daten gewertet werden.[51] Des Weiteren ist die Streubreite der Maßnahme in diesem Zusammenhang zu beachten, d. h., wie viele Menschen von der Datenerhebung betroffen sind.[52] Wenn die Strafverfolgungsbehörden auf die Handy-Daten zugreifen, ist es ihnen möglich, sämtliche Kontaktpersonen ausfindig zu machen. Somit sind alle Personen, die sich über einen bestimmten Zeitraum nahe des Verdächtigen aufgehalten haben, betroffen. Demnach liegt eine große Streubreite vor, wodurch der Grundrechtseingriff intensiver ist.[53] Als letzter Punkt muss die Bedeutung der erhobenen Daten berücksichtigt werden. Die gesammelten Daten handeln von dem (möglichen) Vorhandensein einer Infektion. Der Infektionsstatus einer Person stellt ein Gesundheitsdatum dar, da er Aufschluss über deren körperliche Gesundheit gibt. Das gilt auch für die Daten, die

44 *Bertram*, S. 149; *Zöller*, S. 59 f.
45 *Zöller*, S. 59 f.
46 *Zöller*, StV 2019, 419 (419 f.).
47 *Zöller*, S. 60.
48 *Bertram*, S. 250, 251, 252.
49 *Dochow*, GuP 2020, 129 (131).
50 *Kuhlmann*, GSZ 2020, 115 (117).
51 *Kuhlmann*, GSZ 2020, 115 (117 f.).
52 *Bertram*, S. 108.
53 *Bertram*, S. 108 f.

nur eine mögliche zukünftige Infektion betreffen.[54] Gesundheitsdaten stellen nach Art. 9 Abs. 1 DSGVO besondere personenbezogene Daten dar, die daher besonders zu schützen sind.[55]

cc) Allgemeine Abwägungskriterien beim Zugriff auf Gästelisten

Auch im Fall des Zugriffs auf eine Gästeliste greifen zwei Kriterien, die bei einer Verhältnismäßigkeitsprüfung in Bezug auf die Ermächtigungsgrundlage besonders zu beachten sind: die Streubreite der Maßnahme und die Bedeutsamkeit der Daten. Bei dieser Maßnahme werden auch die Kontaktdaten der Bürger erfasst, die mit der zu ermittelnden Straftat nicht in Berührung gekommen sind. Dies kann deren Recht innerhalb einer Abwägung schwerer wiegen lassen, da sie keinen Anlass zu der Maßnahme gegeben haben.[56] Daher muss die Streubreite bei der Verhältnismäßigkeitsprüfung des Zugriffs auf Gästelisten berücksichtigt werden. Ein weiterer Punkt, der beachtet werden muss, ist die Bedeutsamkeit der Daten. Die Gästeliste kann Name, Adresse, Telefonnummer oder E-Mail-Adresse enthalten. Außerdem zeigen diese Daten, welche Person sich wann an welchem Ort aufgehalten hat und eventuell sogar mit wem.[57] Ergänzt durch andersartig erlangte Daten, kann viel über einen Bürger preisgegeben werden.[58] Daher muss dies bei der Abwägung berücksichtigt werden.

4. Mögliche Rechtfertigungen: Verhältnismäßigkeitsprüfung

Nachdem die allgemeine Verfassungs- und Rechtslage und die Problematiken in den Fällen Handy-Daten und Gästelisten aufgezeigt wurden, werden nun die einzelnen Ermächtigungsgrundlagen zum strafprozessualen Zugriff auf die Daten dargelegt und ihre Rechtmäßigkeit in den Fällen der Zugriffe auf die Handy-Daten und Gästelisten überprüft.

a) Die Ermittlungsgeneralklauseln, §§ 161, 163 StPO

Begonnen wird zunächst mit den Ermittlungsgeneralklauseln der StPO, die die Befugnisse der Staatsanwaltschaft und der Polizei bei der Ermittlung von Straftaten und deren Grenzen festlegen. [59] Nach den §§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 2 StPO können die Staatsanwaltschaft, sowie die Polizei, Ermittlungen jeder Art vornehmen und Auskunft von den Behörden verlangen, um einen Sachverhalt aufzuklären.[60] Diese Vorschriften sollen für Grundrechtseingriffe dienen, die nicht so intensiv sind, dass sie speziell geregelt werden müssen.[61] Das Recht zu ermitteln beinhaltet auch das Erheben von Daten, soweit dies nicht speziell geregelt ist.[62] Diese Normen stellen somit sowohl Ermittlungs- als auch Datenerhebungsgeneralklauseln dar.[63] Die Strafverfolgungsbehörden können daher die personenbezogenen Daten im Laufe einer Ermittlungsanfrage gegenüber Behörden und privaten Stellen erheben.[64] Einzige Voraussetzung hierfür ist der Anfangsverdacht. Dieser liegt vor, wenn es nach der Auswertung der konkreten Tatsachen mit Bezug auf die kriminologische Erfahrung danach aussieht, dass eine Straftat

54 *Dochow*, GuP 2020, 129 (132).
55 *Dochow*, GuP 2020, 129 (133).
56 *Bertram*, S. 108 f.
57 *Aden/Arzt/Fährmann*, Einleitungsgedanke.
58 *Zöller*, S. 29.
59 *Zöller*, in: HK-StPO, 6. Aufl. (2019), § 161 Rn. 1, 2, § 163 Rn. 1.
60 *Griesbaum*, in: KK-StPO, 8. Aufl. (2019), § 163 Rn. 9; *Zöller*, in: HK-StPO, § 161 Rn. 1, 19, § 163 Rn. 10.
61 *Zöller*, S. 69.
62 *Bertram*, S. 175.
63 *Bodenbenner*, S. 42.
64 *Sackreuther*, in: BeckOK-StPO, 37. Ed. (Stand: 1.7.2020), § 161 Rn. 10, 11.

begangen wurde.[65] Zum Zweck der Strafverfolgung ermöglichen die Generalklauseln daher eine kaum begrenzte Datenerhebung und -übermittlung. Da dies jedoch einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt, muss für die Rechtmäßigkeit des Zugriffs das Verhältnismäßigkeitsgebot erfüllt werden.[66] Dabei sind der Gesetzesvorbehalt, das Bestimmtheitsgebot und das Übermaßverbot besonders zu beachten.[67] Wie bereits bei den allgemeinen Ausführungen erwähnt, müssen außerdem die speziellen Voraussetzungen für die zweckändernde Datennutzung erfüllt sein, falls die Datenerhebung durch eine zweckändernde Übermittlung der Daten erfolgt. Hieraus folgt, dass die Ermittlungsgeneralklauseln grundsätzlich für den Zugriff auf Handy-Daten und Gästelisten als Ermächtigungsgrundlagen anwendbar wären, da sie Datenübermittlungen an die Strafverfolgungsbehörden ermöglichen. Dennoch muss die Verfassungsmäßigkeit noch in den Einzelfällen überprüft werden, um über die Rechtmäßigkeit der Datenverarbeitung zu entscheiden.

aa) Handy-Daten

Wie gerade ausgeführt, muss eine Verhältnismäßigkeitsprüfung stattfinden. Da die Datenerhebungsgeneralklauseln allgemeingültig bestimmt sind, darf das Recht, in das eingegriffen wird, nicht zu stark wiegen. Dies führt besonders dann zu Problemen, wenn Ermittlungsmethoden, die die Grundrechte stark beeinträchtigen können, beim Fehlen spezieller Regelungen auf Grund der Generalklauseln eingesetzt werden.[68] Dies ist nicht möglich, da die Generalklauseln nur angewendet werden dürfen, wenn der Eingriff das Recht nur so leicht beeinträchtigt, dass keine speziellere Regelung nötig ist.[69] Durch den Zugriff auf die Handy-Daten wird nicht nur in ein technisches System eingegriffen,[70] sondern auch, wie erwähnt, in Gesundheitsdaten. Des Weiteren werden die Daten aller Kontaktpersonen eingesehen. So sind die Daten vieler unbeteiligter Personen betroffen. Gesundheitsdaten sind nach dem Datenschutzrecht besonders geschützt, da dieses den Zugriff auf diese Daten stark einschränkt.[71] Auch die betroffenen Rechte der unbeteiligten Dritten lassen den Eingriff schwerer rechtfertigen.[72] Zudem wird das Mobiltelefon als technisches System zusätzlich durch das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme geschützt.[73] All diese Faktoren sorgen dafür, dass hohe Ansprüche an die Eingriffsermächtigung zu stellen sind. Daher kann eine Generalklausel den Zugriff auf die Handy-Daten nicht erlauben, da sie für den Eingriff in solche sensiblen Daten von unbeteiligten Personen zu unbestimmt ist.[74] So kann der Zugriff auf die Handy-Daten nicht durch die Ermittlungsgeneralklauseln gerechtfertigt werden.

bb) Gästelisten

Fraglich ist daher, ob zumindest der Zugriff auf die Gästelisten auf Grundlage der Ermittlungsgeneralklauseln möglich ist. Die Ermittlungsgeneralklauseln besitzen seit 2007 eine Ergänzung in § 161 Abs. 3 S. 1 StPO, die die zweckändernde Nutzung von Daten, die durch andere Vorschriften als die der StPO erhoben worden sind, begrenzt.[75] Diese Vorschrift könnte also die Anwendung der Generalklauseln für die zweckändernde Verwendung der Gästelistendaten zu Strafverfolgungszwecken sperren. § 161 Abs. 3 S. 1 StPO beinhaltet eine Normierung des

65 *Bodenbenner*, S. 48, 170.
66 *Bodenbenner*, S. 48 f.; *Zöller*, StV 2019, 419 (421, 423).
67 *Bodenbenner*, S. 49; *Zöller*, in: HK-StPO, § 161 Rn. 19.
68 *Bodenbenner*, S. 49.
69 *Bertram*, S. 176.
70 *Singelnstein*, NStZ 2012, 593 (598).
71 *Dochow*, GuP 2020, 129 (133).
72 *Bertram*, S. 108 f.
73 *Singelnstein*, NStZ 2012, 593 (598).
74 *Bodenbenner*, S. 49.
75 *Bertram*, S. 229; *Zöller*, in: HK-StPO, § 161 Rn. 1.

hypothetischen Ersatzeingriffs in bestimmten Fällen.[76] Dieser beschränkt die Verwendung von durch andere Gesetze erlangte personenbezogene Daten zu Beweiszwecken ohne Einwilligung der betroffenen Person. Die Regelung gilt aber allein für Zugriffsmaßnahmen, die nach der StPO nur bei Verdacht bestimmter Straftaten angewendet werden dürfen. Diese Daten dürfen nur zu Strafverfolgungszwecken genutzt werden, wenn die Maßnahme zur Aufklärung der bestimmten Straftat nach den strafprozessualen Regelungen auch hätte angeordnet werden können. Somit öffnet diese Vorschrift die Tür für die Verwendung von Daten im Strafverfahren, die durch außerstrafprozessuale hoheitliche Maßnahmen erhoben wurden.[77] Durch den hypothetischen Ersatzeingriff soll trotz der Zweckänderung dem Zweckbindungsgrundsatz Genüge getan werden.[78] Entscheidend ist, ob nach einer hypothetischen Betrachtung die Daten auf Grund einer entsprechenden Vorschrift der StPO rechtmäßig hätten erhoben werden können.[79] Diese Eingriffsfigur fordert eine entsprechende Maßnahme in einem Gesetz und die reelle Möglichkeit, diese Maßnahme nach der StPO zur Aufklärung einer Katalogtat anzuordnen.[80] Das sich gegenseitig Entsprechen der Maßnahmen bedeutet, dass die personenbezogenen Daten auch nach der StPO mit vergleichbar schwerwiegenden Mitteln hätten erhoben werden dürfen.[81] Es ist nicht erforderlich, dass alle Voraussetzungen der Erhebungsmaßnahmen denen der StPO entsprechen.[82] Für die Möglichkeit der Anordnung reicht der Verdacht bezüglich einer Katalogtat aus.[83] Dabei macht es keinen Unterschied, ob die Daten nach dem anderen Gesetz rechtmäßig oder rechtswidrig erhoben worden sind.[84] Ist § 161 Abs. 3 S. 1 StPO erfüllt, können die erhobenen Daten auch im Strafverfahren als Beweismittel verwendet werden.[85] Diese Rechtsfigur trägt dafür Sorge, dass die strafprozessualen Anordnungsvoraussetzungen nicht umgangen werden.[86] Diese Vorschrift gilt allerdings nur als Beschränkung der Nutzung der Daten als Beweismittel in der Hauptverhandlung gemäß §§ 243 ff. StPO. Sobald die Daten als Spurenansatz oder zu weiteren Ermittlungen benutzt werden, können sie wieder uneingeschränkt nach den Ermittlungsgeneralklauseln verwendet werden.[87] Daher ist die Nutzung der Gästelisten als Ermittlungsansatz ausschließlich nach §§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 2 StPO zu beurteilen. Fraglich bleibt noch, ob § 161 Abs. 3 StPO die Benutzung der Gästelisten als Beweismittel beschränkt. Das Benutzungsverbot gilt jedoch nur für solche Vorschriften, die eine Maßnahme an einen Straftatenkatalog oder bestimmte schwerwiegende Straftaten knüpfen. Sollte dies nicht zutreffen, richtet sich die Datenverwendung wieder nach den allgemeinen Vorschriften der §§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 2 StPO.[88] Diese müssen bei dem Zugriff auf die Gästelisten allein angewendet werden, da es dafür keine vergleichbare Norm der StPO gibt.[89] Die Rechtmäßigkeit des Zugriffs muss daher allein anhand der Verfassungskonformität der §§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 2 StPO und der Verhältnismäßigkeit dieser Ermächtigungsgrundlage im Einzelfall eingeschätzt werden. Daher ist nun zu überprüfen, ob die Generalklauseln die zweckändernde Datennutzung im vorliegenden Fall erlauben. Die §§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 2 StPO bilden nicht nur die Datenerhebungsgeneralklauseln, sondern auch die Zweckänderungsgeneralklauseln. Sie beinhalten daher auch eine Verwendungsermächtigung, durch die bereits

[76] *Bodenbenner*, S. 170.
[77] *Bodenbenner*, S. 177.
[78] *Bodenbenner*, S. 177.
[79] *Bodenbenner*, S. 178.
[80] *Engelhardt*, S. 172.
[81] *Griesbaum*, in: KK-StPO, § 161 Rn. 35a.
[82] *Engelhardt*, S. 185.
[83] *Engelhardt*, S. 200.
[84] *Bodenbenner*, S. 311.
[85] *Engelhardt*, S. 172 f.
[86] *Bertram*, S. 229 f.
[87] *Bodenbenner*, S. 79, 182.
[88] *Zöller*, in: HK-StPO, § 161 Rn. 31.
[89] *Aden/Arzt/Fährmann*, Verstoß gegen den Grundsatz der Zweckbindung.

durch andere Stellen erhobene Daten für ein Strafverfahren übermittelt werden können. Diese dürfen dann aufgrund der Ermächtigung von den Strafverfolgungsbehörden genutzt werden, solange sie rechtmäßig erhoben worden sind.[90] Fraglich ist, ob die Generalklauseln die Anforderungen an eine Zweckänderungsvorschrift erfüllen. Eine Zweckänderungsvorschrift durchbricht den Zweckbindungsgrundsatz und muss daher den neuen Zweck und die zweckentfremdende Datennutzung genau bestimmen.[91] Da die Daten ohne große Einschränkungen durch die §§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 2 StPO generell zweckentfremdet werden dürfen, verstößt diese Auslegung der Norm gegen den Bestimmtheitsgrundsatz und das Verhältnismäßigkeitsprinzip. Eine zweckändernde Verwendung benötigt eine klar bestimmte gesetzliche Erlaubnisnorm.[92] Zudem verstößt dies gegen das Übermaßverbot, da keine Verwendungsvoraussetzungen außer eines Anfangsverdachts vorliegen.[93] Eigentlich müssten an die zweckändernde Verwendung stärkere Anforderungen gestellt werden, da diese den durch die Datenerhebung entstandenen Eingriff vertieft und gleichzeitig einen neuen begründet.[94] Somit muss die Norm an die Intensität des Eingriffs angepasst sein. Dies ist bei den Generalklauseln nicht der Fall. Sie erlauben sogar mehr Datenverwendungen als eigentlich gestattet, da auch Daten verarbeitet werden können, die nach der StPO gar nicht hätten erhoben werden dürfen.[95] Dadurch wird kein genauer Rahmen für die Datenverarbeitung festgelegt. Zudem gibt es außer Absatz 3 keine festgesetzten Grenzen für die Verwendung der Daten. Daher sind die Vorschriften zu unbestimmt und verstoßen gegen das Übermaßverbot.[96] Des Weiteren ist diese Universalerlaubnis bei der Verwendung als Ermittlungsansatz kritisch zu bewerten, da mit dieser meist weitere Grundrechtseingriffe verbunden sind. Die Vorschrift hätte daher besonders ausführlich geregelt werden müssen, um verhältnismäßig zu sein.[97] Somit wird die allgemeine Verfassungsmäßigkeit dieser Generalklauseln im Bezug zur zweckändernden Datennutzung bezweifelt. Um mit den Vorschriften der Verfassung vereinbar zu sein, müssten die Normen konkreter sein und die Verwendung einschränken. Dies hätte durch den hypothetischen Ersatzeingriff geregelt werden können, indem dieser allgemein für die zweckändernde Datenverwendung angewandt wird. So würden klare Grenzen für die Verwendung der Daten gesetzt werden.[98] Ferner kann die Verhältnismäßigkeit direkt im Einzelfall des Zugriffs auf die Gästelisten bezweifelt werden. Bei Gästelisten liegt eine große Streubreite der Maßnahme vor. Daher muss das Interesse, das dem Recht auf informationelle Selbstbestimmung entgegensteht, besonders beachtenswert sein.[99] Zudem kann es in einzelnen Bundesländern vorkommen, dass detaillierte Informationen gespeichert werden.[100] Aus diesem Grund ist das Recht des Bürgers in der Abwägung besonders zu berücksichtigen. Das entgegenstehende Interesse der Strafverfolgung ist allerdings nicht an bestimmte Straftaten gebunden, da die Ermittlungsgeneralklauseln keine Einschränkungen enthalten.[101] Deshalb kann der Zugriff aufgrund jedweder Straftat erfolgen. Gerade jedoch in Fällen kleiner Kriminalität lässt sich ein so intensiver Eingriff in das Grundrecht nicht rechtfertigen.[102] Daher ist der Einsatz der Generalklauseln in manchen Fällen auch im konkreten Einzelfall unverhältnismäßig. Aus diesen Gründen können diese Vorschriften den Zugriff der Strafverfolgungsbehörden auf die Gästelisten nicht rechtfertigen. Wie bereits ausgeführt, benötigt eine Zweckänderungsermächtigung zudem eine Empfangs- und eine Übermittlungsermächtigung. Eine Vorschrift muss die Übermittlung und eine andere den Empfang der Daten erlauben.

90 *Bodenbenner*, S. 169 f.; *Zöller*, StV 2019, 419 (421).
91 *Engelhardt*, S. 219 f.; *Zöller*, StV 2019, 419 (421, 423).
92 *Bodenbenner*, S. 170, 173; *Zöller*, StV 2019, 419 (422).
93 *Bodenbenner*, S. 173.
94 *Bodenbenner*, S. 130 f., 170.
95 *Bodenbenner*, S. 172.
96 *Bodenbenner*, S. 170, 173.
97 *Zöller*, StV 2019, 419 (422).
98 *Bodenbenner*, S. 172 f.; *Zöller*, StV 2019, 419 (423).
99 *Bertram*, S. 108 f.; *Bodenbenner*, S. 173.
100 *Aden/Arzt/Fährmann*, Einleitung.
101 *Bodenbenner*, S. 173.
102 *Hauschild*, in: MüKo-StPO, 2014, § 94 Rn. 24; *Singelnstein*, NStZ 2012, 593 (603).

Nur wenn beides gegeben ist, darf ein solcher Datenaustausch stattfinden. §§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 2 StPO stellen nur die Empfangsermächtigung dar.[103] Die Übermittlungsermächtigungen sind, im Falle der Gästelisten, die Verordnungen der Bundesländer, die das Anfertigen von Gästelisten in der Pandemie regeln. Diese erlauben aber bisher nur die Weitergabe an die Gesundheitsbehörden. Manche Verordnungen verbieten die zweckentfremdende Verarbeitung, andere erlauben explizit nur die Verwendung zur Infektionsnachverfolgung und wieder andere beinhalten keine offensichtlichen Regelungen zu diesem Thema. Außerdem gibt es im Infektionsschutzgesetz keine Regelung zur Verwendung der Daten zu Strafverfolgungszwecken.[104] Daher gibt es keine Übermittlungsermächtigung, die den Zugriff auf die Daten gestatten kann. Aus diesen Gründen lässt sich die zweckändernde Verwendung der Daten durch Zugriff der Strafverfolgungsbehörden auf die Gästelisten nicht durch die Ermittlungsgeneralklauseln der StPO rechtfertigen.

cc) Zusammenfassung

Die Ermittlungsgeneralklauseln sind daher nicht geeignet, den strafprozessualen Zugriff auf Handy-Daten und Gästelisten zu Zeiten der Pandemie zu ermöglichen.

b) Auskunftsrecht von Polizei und Staatsanwaltschaft

Des Weiteren ist fraglich, ob der Zugriff auf die Handy-Daten und Gästelisten nicht auf Grund des Auskunftsrechts der Staatsanwaltschaft und der Polizei erlangt werden kann. Dieses Auskunftsrecht findet sich in den §§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 2 StPO wieder. Die Strafverfolgungsbehörden können hierdurch Ermittlungsanfragen an öffentliche und private Stellen, wie Privatpersonen oder Wirtschaftsunternehmen, stellen. Da durch das Anfragen gegenüber Privatpersonen deren Daten in den öffentlichen Bereich gelangen, liegt für diese ab der Anfrage Grundrechtsbindung vor.[105] Das Auskunftsrecht stellt gegenüber Privatpersonen zudem keine Verpflichtung zur Herausgabe der Daten dar. Von ihnen kann nur verlangt werden, sich vor der Staatsanwaltschaft oder einem Richter als Zeuge zu äußern.[106] Die Handy-Daten liegen beim Besitzer bzw. auf einem Server des Providers vor.[107] Bei den Gästelisten sind sie im Besitz des Geschäftsinhabers.[108] Diese Daten sind somit nicht in den Händen staatlicher Behörden, sondern in denen privater oder nicht öffentlicher Stellen. Daher können die Strafverfolgungsbehörden durch das Auskunftsrecht keinen Zugriff auf die Handy-Daten und Corona-Gästelisten verlangen. Sie können durch dieses Recht nur dann Zugriff auf die Daten erlangen, wenn diese freiwillig herausgegeben werden.[109]

c) Die Beschlagnahme, § 94 StPO

Der Zugriff auf die Handy-Daten und Gästelisten könnte aber durch die formlose Sicherstellung und die Beschlagnahme gemäß § 94 StPO zulässig sein.[110] Diese Vorschrift stellt gegenüber den Generalklauseln und dem Auskunftsrecht eine speziellere Eingriffsbefugnis für den Zugriff auf Daten durch die Strafverfolgungsbehörden dar.[111]

[103] *Zöller*, StV 2019, 419 (421).
[104] *Aden/Arzt/Fährmann*, Verstoß gegen den Grundsatz der Zweckbindung.
[105] *Bodenbenner*, S. 47; *Zöller*, in: HK-StPO, § 161 Rn. 7.
[106] *Singelnstein*, NStZ 2012, 593 (603).
[107] *Dochow*, GuP 2020, 129 (131).
[108] *Aden/Arzt/Fährmann*, Einleitung.
[109] *Radtke*, in: FS Meyer-Goßner, 2001, S. 321 (325).
[110] *Gercke*, in: HK-StPO, 6. Aufl. (2019), § 94 Rn. 37.
[111] *Singelnstein*, NStZ 2012, 593 (603).

Sie gestattet die Sicherstellung von Gegenständen, damit sie als Beweis für die Strafverfolgung zur Verfahrenssicherung genutzt werden können.[112] Ein Beweismittel kann jeder körperliche Gegenstand sein, der mittelbar oder unmittelbar einen Beweis für eine Tat oder deren nähere Umstände erbringen kann.[113] Dies bezieht sich nicht nur auf den Beweis in der Hauptverhandlung, sondern auch auf Gegenstände, die als Erkenntnisquellen dienen.[114] Daten können nur über den Datenträger beschlagnahmt werden, da sie für sich allein keine beschlagnahmefähigen körperlichen Gegenstände sind.[115] Erforderlich für die Sicherstellung ist ein bereits eingeleitetes Strafverfahren mit Untersuchung.[116] Dafür muss ein Anfangsverdacht gemäß § 152 Abs. 2 StPO vorliegen.[117] Durch das Legalitätsprinzip sind die Strafverfolgungsbehörden dann verpflichtet, Beweismittel sicherzustellen, sobald ihnen eine potentielle Beweisbedeutung zugewiesen werden kann.[118] Sicherstellung stellt dabei den Oberbegriff für zwei Arten der Herstellung staatlicher Gewalt über den Gegenstand dar. Es gibt die formlose Sicherstellung nach § 94 Abs. 1 StPO und die förmliche Beschlagnahme nach § 94 Abs. 2 StPO.[119] Eine formlose Sicherstellung ist die freiwillige Herausgabe des Gegenstandes durch den Gewahrsamsinhaber. Dabei ist zu beachten, dass die Freiwilligkeit nur vorliegen kann, wenn dem Betroffenen bewusst ist, dass ihn keine Pflicht zur Herausgabe trifft.[120] Eine förmliche Beschlagnahme wird dann benötigt, wenn der Gegenstand nicht freiwillig herausgegeben wird und somit die Sicherstellung erzwungen werden muss.[121] Dann müssen die Formvorschriften des § 98 StPO gewahrt werden.[122] Durch die Wegnahme des Gegenstands wird in grundrechtlich geschützte Positionen eingegriffen.[123] Bei der Weitergabe von Datenträgern werden Daten übermittelt. Wenn Datenträger beschlagnahmt werden, ist daher das Recht auf informationelle Selbstbestimmung betroffen.[124] § 94 StPO stellt hierfür die wegen des Gesetzesvorbehalts notwendige gesetzliche Eingriffsermächtigung dar.[125] Der Paragraph weist jedoch nur geringe Voraussetzungen für einen Eingriff auf, obwohl auch sensible Daten betroffen sein können. Daher müssen im Einzelfall die allgemeinen strafprozessualen und verfassungsrechtlichen Grenzen, wie die Verhältnismäßigkeit, zur Einschränkung der Eingriffsmaßnahme herangezogen werden.[126] So untersteht auch die Beschlagnahme dem Verhältnismäßigkeitsgebot. Dabei muss die Beschlagnahme in einem angemessenen Verhältnis zur Schwere der Tat und zur Stärke des Tatverdachts stehen. Außerdem muss der Gegenstand für die Ermittlungen notwendig sein, da nur so das Übermaßverbot beachtet wird.[127] Ein Eingriff in sensible Daten kann nicht verhältnismäßig sein, sofern nur eine leichte Straftat oder eine geringe Beweisbedeutung vorliegt.[128] Zudem wiegen die betroffenen Rechte der Verletzten bzw. der Unbeteiligten mehr als die des Beschuldigten und es ist zu prüfen, ob nicht ein milderes Mittel, wie die formlose Sicherstellung, für den Zugriff angewendet werden kann.[129] Es muss demnach stets eine umfassende Abwägung der Interessen erfolgen. Dabei stehen sich die funktionstüchtige Strafrechtspflege und in diesem Fall das Recht auf informationelle Selbstbestimmung mit Berücksichtigung der Intensität ihrer Beeinträchtigung gegenüber.[130] Bei der formlosen Sicherstellung ist dies unbeachtlich, da bei einer freiwilligen Einwilligung keine

112 *Gercke*, in: HK-StPO, § 94 Rn. 1, 2.
113 *Gercke*, in: HK-StPO, § 94 Rn. 6, 8.
114 *Gercke*, in: HK-StPO, § 94 Rn. 7.
115 *Gercke*, in: HK-StPO, § 94 Rn. 18.
116 *Gercke*, in: HK-StPO, § 94 Rn. 29.
117 *Gercke*, in: HK-StPO, § 94 Rn. 31.
118 *Gercke*, in: HK-StPO, § 94 Rn. 35.
119 *Gercke*, in: HK-StPO, § 94 Rn. 37, 42.
120 *Gercke*, in: HK-StPO, § 94 Rn. 39, 40.
121 *Gercke*, in: HK-StPO, § 94 Rn. 42.
122 *Kipker/Voskamp*, ZD 2013, 119 (120).
123 *Hauschild*, in: MüKo-StPO, § 94 Rn. 2.
124 *Radtke*, in: FS Meyer-Goßner, 2001, S. 321 (332).
125 *Hauschild*, in: MüKo-StPO, § 94 Rn. 2.
126 *Singelnstein*, NStZ 2012, 593 (597).
127 *Burhoff*, Handbuch für das strafrechtliche Ermittlungsverfahren, 8. Aufl. (2019), Rn. 986, 987; *Hauschild*, in: MüKo-StPO, § 94 Rn. 23.
128 *Singelnstein*, NStZ 2012, 593 (597).
129 *Burhoff*, Rn. 988, 990; *Radtke*, in: FS Meyer-Goßner, 2001, S. 321 (331).
130 *Gercke*, in: HK-StPO, § 94 Rn. 52.

solche Prüfung stattfindet, da der Eingriff erlaubt wird.[131] Liegt jedoch bei der Beschlagnahme ein Verstoß gegen das Verhältnismäßigkeitsgebot vor, dann führt dies zu einem Beschlagnahmeverbot.[132] Daher ist bei der Verhältnismäßigkeit eines Zugriffs nach § 94 StPO auf die Handy-Daten und die Gästelisten in Zeiten der Pandemie die Unterscheidung dieser zwei Arten der Sicherstellung besonders wichtig. Bei der formlosen Weitergabe des Datenträgers kommt es nur darauf an, dass dies durch eine freiwillige Einwilligung geschieht. Dies setzt voraus, dass die Einwilligung mit den Zielen der Ermächtigung übereinstimmt, zur Erreichung dieser Ziele geeignet ist, der Gewahrsamsinhaber dispositionsbefugt ist und dass Freiwilligkeit vorliegt.[133] Der Inhaber ist dabei dispositionsbefugt, die Daten des Kunden herauszugeben, da dieser bei Beweisbedeutung des Datenträgers dies dulden muss.[134] Die formlose Sicherstellung stellt also lediglich einen Realakt dar, der keine Anordnungsbefugnis benötigt.[135] Bei einer förmlichen Beschlagnahme sind die Vorschriften des § 98 StPO zu beachten, welcher eine formelle Anordnung durch einen Richter beinhaltet. Diese muss die zu beschlagnahmenden Gegenstände bestimmt genug bezeichnen, den Beschlagnahmezweck aufzeigen und aktenkundig gemacht werden.[136] Dabei muss sie inhaltlich so konkretisiert sein, dass der Eingriff messbar und kontrollierbar bleibt und kein Zweifel bezüglich des Umfangs der Maßnahme aufkommen kann.[137] Zudem sind die Person des Beschuldigten, der Sachverhalt, der Strafbarkeitsvorwurf, der Tatverdacht und die Stellung des Gegenstands als Beweismittel in die Anordnung aufzunehmen.[138] Dieser Richtervorbehalt des § 98 Abs. 1 StPO dient der Kontrolle des staatsanwaltschaftlichen Grundrechtseingriffs.[139] Wegen des Grundrechtseingriffs fordert das Verfassungsrecht daher eine Verhältnismäßigkeitsprüfung im Rahmen der Anordnung.[140] Aufgrund dieser Unterschiede im Sicherstellungsverfahren ist die Verfassungsmäßigkeit, gerade wenn es um die Daten Dritter geht, in den Fällen der formlosen Sicherstellung und der förmlichen Beschlagnahme unterschiedlich zu bewerten. Dies wird im Folgenden anhand der Anwendbarkeit der §§ 94 ff. StPO in den Fällen des Zugriffs auf Handy-Daten und Gästelisten erläutert.

aa) Handy-Daten

Wie bereits erörtert, sind beim Zugriff auf die Handy-Daten zu Zeiten der Pandemie sensible Gesundheitsdaten betroffen. Daher muss der Eingriff besonders gerechtfertigt sein. Wenn die Daten direkt beim Besitzer des Mobiltelefons erhoben werden, wäre eine formlose Sicherstellung denkbar. Zwar wird auch hier der Zweck der Datenverarbeitung verändert, aber der Inhaber wird darüber informiert. Er weiß somit, was mit seinen Daten geschieht und kann durch eine Einwilligung den Eingriff in sein Grundrecht erlauben.[141] Bei einer förmlichen Beschlagnahme kann sich der Betroffene gegen die Datenerhebung nicht wehren. Ihm wird aber durch die Anordnung mitgeteilt, aus welchen Gründen seine Daten erhoben und wie sie genutzt werden. Außerdem wird vor dem Zugriff die Lage von einem Richter überprüft. Da dieser auch die Frage der Verhältnismäßigkeit mitberücksichtigen muss, wird für die Verhältnismäßigkeit von Maßnahme und Eingriff Sorge getragen.[142] Sollte im konkreten Einzelfall das Interesse des Betroffenen überwiegen, kann der Richter den Zugriff verbieten. Zudem wird der Betroffene

131 *Gercke*, in: HK-StPO, § 94 Rn. 39; *Radtke*, in: FS Meyer-Goßner, 2001, S. 321 (339).
132 *Park*, Durchsuchung und Beschlagnahme, 4. Aufl. (2018), § 3 Rn. 638.
133 *Gercke*, in: HK-StPO, § 94 Rn. 39; *Radtke*, in: FS Meyer-Goßner, 2001, S. 321 (339, 341).
134 *Radtke*, in: FS Meyer-Goßner, 2001, S. 321 (343).
135 *Hauschild*, in: MüKo-StPO, § 94 Rn. 43.
136 *Gercke*, in: HK-StPO, § 98 Rn. 1, 4; *Kipker/Voskamp*, ZD 2013, 119 (120).
137 *Gercke*, in: HK-StPO, § 98 Rn. 15.
138 *Park*, § 3 Rn. 481, 483, 484, 488.
139 *Park*, § 3 Rn. 476.
140 *Burhoff*, Rn. 835.
141 *Kipker/Voskamp*, ZD 2013, 119 (120); *Radtke*, in: FS Meyer-Goßner, 2001, S. 321 (339).
142 *Burhoff*, Rn. 835; *Gercke*, in: HK-StPO, § 94 Rn. 42, § 98 Rn. 4.

rechtlich angehört.[143] Daher ist der Zugriff auf die Handy-Daten durch die förmliche Beschlagnahme beim Betroffenen verfassungsgemäß. Fraglich ist allerdings, ob auch der Zugriff auf Daten beim Serverprovider verhältnismäßig ist, da der Betroffene nicht in das Geschehen der zweckändernden Datenverarbeitung eingebunden ist. Bei der formlosen Sicherstellung würde die Einwilligung des Providers ausreichen, um die zweckändernde Datenverarbeitung zu erlauben.[144] Somit wären in einem solchen Fall keine weiteren Anforderungen als die Einwilligung und ein Anfangsverdacht nötig, um einen strafprozessualen Zugriff auf sensible Daten eines Dritten zu erlauben.[145] Diese Situation gleicht daher dem Zugriff durch die Ermittlungsgeneralklauseln, vor allem, da die Beweismittel auch als Ermittlungsansatz genutzt werden können. Die drei Vorschriften haben nur den Anfangsverdacht als Einschränkung bzw. als Voraussetzung und erlauben fast jeglichen Eingriff. Sie geben weder einen bestimmten Rahmen noch Grenzen für die Datenverarbeitung vor. Wenn schon bei den Ermittlungsgeneralklauseln die Verfassungskonformität eines solchen Eingriffs bestritten wird, dann ist dies auch hier der Fall. Daran ändert auch die Voraussetzung der Einwilligung nichts, da diese nicht von der Person kommt, deren Daten betroffen sind. Aus diesen Gründen verstößt eine formlose Sicherstellung in diesem Fall gegen Bestimmtheitsgebot und Übermaßverbot. Der Zugriff könnte aber durch die förmliche Beschlagnahme zulässig sein. Dabei liegt eine richterliche Anordnung vor.[146] Die förmliche Beschlagnahme benennt die genauen Umstände des Zugriffs und der Verwendung in einem bestimmten Verfahren und benötigt eine Verhältnismäßigkeitsprüfung eines Richters.[147] Somit ist diese bestimmter als die formlose Sicherstellung und die Ermittlungsgeneralklauseln, da die Datenverwendung durch die Zustimmungsbedürftigkeit eingegrenzt wird. So können das geforderte Übermaßverbot, Bestimmtheitsgebot und der Zweckbindungsgrundsatz bei der Zweckänderung eingehalten werden.[148] Somit ist die zweckändernde Datenverwendung verfassungsgemäß, nicht zuletzt da dem Betroffenen nach der Beschlagnahme gemäß § 33 Abs. 3 StPO rechtliches Gehör gewährt werden muss.[149] So wird nochmals sichergestellt, dass der Bürger über die Verwendung seiner Daten Kenntnis hat und dass der Zugriff rechtmäßig ist. Daher kann eine förmliche Beschlagnahme den Zugriff auf die Handy-Daten beim Provider erlauben. Dennoch gibt es noch ein weiteres Kriterium der zweckändernden Datenverwendung, das vom *BVerfG* gefordert wird: die Öffnungsklausel. Wie bereits festgestellt, fehlt eine solche im Infektionsschutzgesetz, welches das Erheben von Gesundheitsdaten während einer Pandemie erlaubt. Nur wenn eine solche Klausel hinzugefügt wird, kann die Datenübermittlung gestattet werden.[150]

bb) Gästelisten

Die Gästelisten, die zur Überwachung der Infektionsketten erstellt werden müssen, befinden sich ausschließlich bei den Betreibern der Geschäfte.[151] Daher kann keine Anfrage zur Herausgabe an den in seinen Grundrechten betroffenen Dritten gestellt werden. Demnach folgen dieselben Überlegungen wie beim Zugriff auf die Handy-Daten beim Provider. Ohne die Anordnung durch einen Richter und die Anhörung des Dritten kann die formlose zweckändernde Sicherstellung der Daten nicht gerechtfertigt werden. Sie ist auch in diesem Kontext zu unbestimmt und verstößt gegen das Übermaßverbot. Wie vorher ausgeführt, kann daher nur die förmliche Beschlagnahme die verfassungsrechtlichen Anforderungen erfüllen, da die Anordnung bestimmt genug ist, Grenzen setzt

143 *Burhoff*, Rn. 835; *Singelnstein*, NStZ 2012, 593 (598).
144 *Radtke*, in: FS Meyer-Goßner, 2001, S. 321 (339, 343).
145 *Gercke*, in: HK-StPO, § 94 Rn. 31; *Singelnstein*, NStZ 2012, 593 (597, 598).
146 *Gercke*, in: HK-StPO, § 98 Rn. 1, 4.
147 *Burhoff*, Rn. 835; *Park*, § 3, Rn. 481, 483, 484, 488.
148 *Bodenbenner*, S. 49, 69; *Zöller*, in: HK-StPO, § 161 Rn. 19.
149 *Singelnstein*, NStZ 2012, 593 (598).
150 *Aden/Arzt/Fährmann*, Verstoß gegen den Grundsatz der Zweckbindung.
151 *Aden/Arzt/Fährmann*, Einleitung, Verstoß gegen den Grundsatz der Zweckbindung.

und das Verhältnismäßigkeitsgebot eingehalten wird. Die §§ 94 Abs. 2, 98 Abs. 1 StPO kommen also auch in den Fällen der Gästelisten als Ermächtigungsgrundlage in Betracht. Bei Gästelisten liegt jedoch eine große Streubreite der Maßnahme vor und es werden zum Teil viele Daten des Bürgers aufgezeichnet. Daher muss das Interesse der Bürger in der Abwägung stärker beachtet werden.[152] So kann der Richter in der Verhältnismäßigkeitsprüfung zum Ergebnis kommen, dass die Anwendung der Vorschrift im konkreten Einzelfall unverhältnismäßig ist. Abschließend kann nochmals angefügt werden, dass auch beim Zugriff auf Gästelisten die Öffnungsklausel in den Pandemie-Verordnungen fehlt. Erst wenn eine solche in den Verordnungen vorhanden ist, kann der Zugriff gestattet werden. Nur wenn der Dritte bei seiner rechtlichen Anhörung den Zugriff erlaubt, kann dieses Problem durch den Grundrechtsverzicht umgangen werden.

cc) Zusammenfassung

Da eine Öffnungsklausel in den Gesetzen fehlt, kann nur die freiwillige Aufgabe des Grundrechtsschutzes den Zugriff auf die personenbezogenen Daten rechtfertigen. Wäre eine solche Klausel gegeben, dann könnte ein rechtmäßiger strafprozessualer Zugriff in Form der förmlichen Beschlagnahme auf die Handy-Daten und die Gästelisten erfolgen.

d) Zwischenergebnis

Nachdem nun die möglichen Eingriffsermächtigungen der StPO untersucht worden sind, lässt sich feststellen: Der zweckverändernde strafprozessuale Zugriff auf die zur Pandemiebekämpfung erhobenen Daten lässt sich nur nach den §§ 94, 98 Abs. 1 StPO rechtfertigen. Die anderen Regelungen sind zum einen für die Datenerhebungen in den konkreten Fällen zu ungenau und nicht verhältnismäßig und zum anderen fehlt es an der Öffnungsklausel in den notwendigen Gesetzen. Daher ist ein Datenzugriff nur in wenigen Fällen möglich. Dies kann unter anderem behoben werden, indem eine Öffnungsklausel in den entsprechenden Gesetzen eingefügt wird. Zukünftige, ähnliche Konfliktlagen können aber nur gelöst werden, wenn der Gesetzgeber die Regelungen für die allgemeine und zweckändernde Datenverwendung der Strafverfolgungsbehörden den Anforderungen des Verfassungsrechts anpasst.

5. Die Bedeutung des rechtswidrigen Zugriffs für die Verwertbarkeit der Daten

Wie ausgeführt, haben die Strafverfolgungsbehörden in den konkreten Fällen meist keine Zugriffserlaubnis für die Daten besessen. Daher muss nun die Frage gestellt werden, ob die Daten, die ohne gültige Ermächtigung erhoben worden sind, dennoch als Beweismittel im Strafverfahren genutzt werden dürfen. Denn nicht jeder Verstoß gegen eine Beweiserhebungsvorschrift oder ein Datenverwendungsverbot führt automatisch zu einem strafprozessualen Verwertungsverbot. Dies ist immer nach den Umständen des Einzelfalls zu bewerten, wenn eine ausdrückliche Vorschrift oder übergeordnete, gewichtige Gründe ein solches Verbot verlangen.[153] In diesen Fällen dürfen die Daten nicht für die Beweiswürdigung und die Entscheidungsfindung verwendet werden.[154] Im Falle der §§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 2 StPO könnte ein Verstoß gegen ein Datenverwendungsverbot vorliegen, denn sie sind nicht dafür geeignet, die zweckändernde Datennutzung in den Fällen des Zugriffs auf die Handy-Daten

[152] *Bertram*, S. 108 f.; *Singelnstein*, NStZ 2012, 593 (597).
[153] *Eisenberg*, Beweisrecht der StPO, 10. Aufl. (2017), Rn. 335; *Hauschild*, in: MüKo-StPO, § 94 Rn. 57, 58.
[154] *Eisenberg*, Rn. 356.

und Gästelisten zu gestatten. Datenverwendungsverbote sperren die weitere Verarbeitung der Daten. Daher führen sie automatisch auch zu dem Verbot, die Daten als Beweismittel oder als Ermittlungsansatz zu nutzen.[155] Ein Datenverwendungsverbot kann aus dem Verfassungsrecht und dem einfachen Recht abgeleitet werden. Da eine Datenverwendung eine verfassungsrechtliche Legitimation benötigt, wird eine nicht legitimierte Datenverwendung wie ein ausdrückliches Verbot gewertet.[156] Da die Ermittlungsgeneralklauseln nicht geeignet sind, die zweckändernde Nutzung der Handy-Daten und Gästelisten für die Strafverfolgung zu rechtfertigen, wären die Daten nicht legitim erlangt worden. Dies verbietet ihre Verwendung und damit auch ihre Verwertung. Fraglich ist noch, wie die §§ 94, 98 StPO dies regeln. Wenn gegen die Verfassung verstoßen wird, leitet sich aus diesem Verstoß ein Verwertungsverbot für den sichergestellten Gegenstand ab.[157] Der Verhältnismäßigkeitsgrundsatz begründet dabei ein Beweisverwertungsverbot, wenn die Vorgaben des *BVerfG* nicht eingehalten werden.[158] Beim Zugriff auf die Handy-Daten und Gästelisten ist das Erfordernis der Öffnungsklausel nicht eingehalten und zum Teil gegen das Bestimmtheitsgebot und Übermaßverbot verstoßen worden. Daher liegt ein Beweisverwertungsverbot vor. Aus diesen Gründen können die rechtswidrig erlangten Daten nicht als Beweismittel oder Ermittlungsansatz eingesetzt werden.

III. Appell und Lösungsvorschläge

Abschließend lässt sich feststellen: Die vorliegenden Vorschriften würden grundsätzlich ohne nähere Überprüfung den Zugriff auf die zur Pandemiebekämpfung erhobenen Daten erlauben. Zieht man jedoch die notwendigen verfassungsrechtlichen Anforderungen heran, kann festgestellt werden, dass die strafprozessualen Vorschriften hinsichtlich der zweckändernden Datenverarbeitung diesen Ansprüchen beim Zugriff auf Handy-Daten und Gästelisten meist nicht genügen. Dies kann der Bürger als Laie aber nicht vorhersehen. Um daher Klarheit zu schaffen und Unmut in der Bevölkerung zu vermeiden, muss eine klare Stellungnahme erfolgen. Ein guter Anfang wäre dabei, Transparenz zu ermöglichen. Der Grundrechtseingriff wäre geringer, wenn der Bürger weiß, wie seine Daten verarbeitet werden können und wie er sich dagegen wehren kann. Das verpflichtende Anzeigen einer Rechtsbelehrung beim Herunterladen der Corona-Warn-App oder auf der Gästeliste würde hierzu einen großen Beitrag leisten. Letztendlich müsste aber der Gesetzgeber Öffnungsklauseln in den Vorschriften ergänzen und die strafprozessualen Normen den Anforderungen des *BVerfG* anpassen.

[155] *Bodenbenner*, S. 224.
[156] *Bodenbenner*, S. 226 f.
[157] *Gercke*, in: HK-StPO, § 94 Rn. 61.
[158] *Burhoff*, Rn. 915.

KriPoZ Kriminalpolitische Zeitschrift JuP

„Junges Publizieren“

Grundlagenseminararbeit von

Sophia Regina Weis

„Der digitale Hausfriedensbruch als Straftat“

Ludwig-Maximilians-Universität München
Prof. Dr. Mark Zöller

Abgabedatum: 5.10.2020

Inhaltsverzeichnis

I. Einleitung

Während die Digitalisierung es ermöglicht, sich immer schneller zu vernetzen und Daten auszutauschen, steigen auch im Bereich der digitalen Kriminalität (Cyberkriminalität) die Zahlen immer weiter an.
Große Identitätsdiebstähle wie Collection #1- #5[1], Hackerangriffe auf den deutschen Bundestag[2], massive Verbreitung von persönlichen Daten von Politikern und Prominenten[3] sowie Ransomeware-Angriffe auf Krankenhäuser[4] zeigen die Schattenseite der Digitalisierung auf.
Gerade im Hinblick auf solche Vorkommnisse wird die Thematik bezüglich der Bekämpfung von Cyberkriminalität immer präsenter. Dabei wird unter anderem darüber diskutiert, inwieweit das Strafrecht als „ultima-ratio" bereits Anwendung findet oder gegebenenfalls noch Anwendung finden muss. Insbesondere das Themengebiet des „digitalen Hausfriedensbruchs" steht dabei im Raum.

II. Der „digitaler Hausfriedensbruch"

Unter einem „digitalen Hausfriedensbruch" versteht man den unbefugten Zugang zu einem informationstechnischen System.
Dieser kann zum einen ohne eine Schadsoftware, beispielsweise durch die Eingabe eines zuvor erspähten Pins oder durch das Erlangen und anschließende Eindringen in ein nicht gesichertes System, erfolgen. Zum anderen erfolgt ein digitaler Hausfriedensbruch, vor allem im Bereich schwerwiegender Cyberkriminalität, durch den Einsatz einer Schadsoftware.
Von einem digitalen Hausfriedensbruch mittels einer Schadsoftware wird dann gesprochen, wenn die Schadsoftware auf dem System installiert wird, da bereits die reine Infiltration, also die Zugangserlangung zum System, ausreichend ist.[5]

1. Zugangserlangung mittels einer Schadsoftware

Um Zugang zu einem informationstechnischen System zu erlangen, muss zunächst das jeweilige Zielsystem mit einer Schadsoftware infiltriert werden. Dies kann auf verschiedene Weise erfolgen.
Neben der relativ seltenen Methode eine Schadsoftware direkt durch einen USB-Stick oder eine CD-ROM aufzuspielen, findet die Infektion durch eine im Anhang einer E-Mail oder als Teil einer Nachricht in einem sozialen Netzwerk befindliche Software häufiger Anwendung.[6]
Die derzeit gängigste Methode ist jedoch die sog. „Drive-by-Infektion". Dabei hackt der Täter eine Website und manipuliert diese so, dass durch das alleinige Aufrufen dieser Website die Schadsoftware automatisch im Hintergrund auf das System heruntergeladen wird.[7]

---

1 Abrufbar unter: https://www.pc-magazin.de/ratgeber/datenklau-aktuell-collection-1-betroffen-pruefen-have-i-been-pwned-3200357.html (zuletzt abgerufen am: 27.9.2020).
2 Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2016, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.html (zuletzt abgerufen am: 27.9.2020).
3 *Eisenkrämer*, Riesiges Datenleck bei Politikern und Prominenten, abrufbar unter: https://www.springerprofessional.de/internetkriminalitaet/datensicherheit/riesiges-datenleck-bei-politikern-und-prominenten/16374550 (zuletzt abgerufen am 10.9.2020).
4 Abrufbar unter: https://www.zdf.de/nachrichten/panorama/hacker-angriff-uniklinik-duesseldorf-100.html (zuletzt abgerufen am: 27.9.2020).
5 *Mavany,* KriPoZ 2016, 106 (108).
6 *Mavany,* KriPoZ 2016, 106 (107).
7 *Roos/Schumacher,* MMR 2014, 377 (378).

Nach den Angaben des Bundesamts für Sicherheit in der Informationstechnik werden nachweislich jeden Tag allein bis zu 110.000 Systeme mit einer sog. „Botnetz-Schadsoftware“ (Botware) infiziert.[8] Jedoch kann aufgrund der nicht entdeckten Infektionen von einer durchaus höheren Infektionsrate ausgegangen werden.
Botnetze stellen das zentrale Werkzeug des Täters, mithin die infrastrukturelle Grundlage von Cyberkriminalität, dar.[9]

2. Entstehung eines Botnetzes

Zuerst muss die sog. „Botware“ programmiert werden. Anschließend, in der zweiten Phase des sog. „Spreadings“, werden möglichst viele Systeme (Bots) mit der Botware in einer solchen Weise infiziert, dass diese auch einen Neustart überstehen kann. Dabei kommt als Bot jedes mit dem Internet ständig oder teilweise verbundene System in Betracht.[10] Neben Computern werden vermehrt auch mobile sowie sog. intelligente Endgeräte des Internet of Things (IoT) infiziert, wodurch diese auch Teil eines Botnetzes sein können.[11]
Somit wird der digitale Hausfriedensbruch im Zusammenhang mit Botnetzen in der Phase des „Spreadings“ verwirklicht.[12]
In einer dritten Phase verbinden sich dann die einzelnen Bots über das Internet mit dem zentralen „Command and Control-Server“ (CC-Server), welcher vom sog. „Botmaster“ ferngesteuert und für kriminelle Zwecke missbrauchen werden kann, ohne dass der eigentliche Nutzer dies bemerkt.[13] Da die „Bots“ die über den CC- Server vom Botmaster erteilten Befehle blind ausführen, werden diese als „Zombie“ und das zusammengeschlossene Botnetz selbst als „Zombie-Armee“ bezeichnet.[14]

3. Nutzungsmöglichkeiten eines Botnetzes

Auch wenn es in letzter Zeit gelungen ist, große Botnetze wie „Avalanche“ und „Andromeda“ zu zerschlagen, spielen Botnetze in der Cyberkriminalität aufgrund ihrer vielfältigen Nutzungsmöglichkeiten weiterhin eine zentrale Rolle.[15]
Darunter fällt beispielsweise die Möglichkeit des Spam-Mail-Versands[16], aber auch das Ausspähen und Kopieren von (persönlichen) Daten oder die Verbreitung einer Ransomware bis hin zum Betrug im Online-Banking und dem „Bitcoin-Mining“[17] ist durch den Einsatz eines Botnetzes möglich.[18]
Vor allem aber werden Botnetze zur Ausübung von „Distributed-Denial-of-Service-Attacken (DDoS-Attacken) genutzt, die zu den größten Gefährdungen im Cyberraum zählen.[19]

---

8 Bundesamt für Sicherheit in der Informationstechnik, BSI-Magazin 2019, „Mit Sicherheit – IT-Grundschutz als Fundament für Informationssicherheit“, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2019_02.pdf?__blob=publicationFile&v=6 (zuletzt abgerufen am 26.9.2020).
9 *Mavany,* KriPoZ 2016, 106 (107).
10 BT-Drs. 19/1716, S. 1.
11 BKA-Cybercrime, Bundeslagebild 2018, abrufbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2018.html;jsessionid=F293BBB6E2C2D5A62651D10296BAA05F.live2292?nn=28110 (zuletzt abgerufen am 26.9.2020).
12 *Mavany,* KriPoZ 2016, 106 (108).
13 *Mavany,* KriPoZ 2016, 106 (107).
14 *Kahler/Hoffmann-Holland,* KriPoZ 2018, 267 (270); *Mavany,* KriPoZ 2016, 106 (107).
15 *Roos/Schumacher,* MMR 2014, 377 (378).
16 *Roos/Schumacher,* MMR 2014, 337 (378).
17 *Heine,* NStZ 2016, 441 (442).
18 *Roos/Schumacher,* MMR 2014, 377 (378).
19 *Roos/Schumacher,* MMR 2014, 377 (378).

Dabei werden massive Datenanfragen an einen ausgewählte Server gestellt, um diesen unter der großen Anfragelast „zusammenbrechen“ zu lassen und somit die dort bereitgestellten Dienste zu stören oder sogar ganz zu eliminieren.[20]
Aufgrund seiner Größe von bis zu 9 Millionen Bots und seiner vielseitigen Einsetzungsmöglichkeiten galt das Necurs-Botnetz bis 2020 als eines der gefährlichsten Botnetze der Welt.[21]
Auch stellt die Möglichkeit des „Cybercrime-as-a-Service“, bei welchem Cyberkriminelle ihre Dienste oder die Nutzung, beispielsweise eines Botnetzes, gegen Bezahlung anbieten, eine zusätzliche Bedrohung im Cyberraum dar, da es dadurch jedermann ermöglicht wird das kriminelle „Know-How“ zu erwerben.[22]

III. Vorhandener strafrechtlicher Schutz des digitalen Hausfriedensbuchs

Nicht nur Privatpersonen, sondern vor allem auch Unternehmen und kritische Infrastrukturen (KRITIS) sind von Botnetz-Angriffen, mithin auch von „digitalen Hausfriedensbrüchen“ betroffen. Demnach stellt sich die Frage, inwieweit ein strafrechtlicher Schutz bereits existiert.

1. Strafrechtlicher Schutz nach dem Strafgesetzbuch und deren Strafbarkeitslücken

a) § 202a StGB – Ausspähen von Daten

aa) Straftatbestand des § 202a StGB

Zunächst kommt bei der Infiltration einer Schadsoftware, durch die ein digitaler Hausfriedensbruch verwirklicht wird, eine Strafbarkeit nach § 202a StGB in Betracht.
Voraussetzung hierfür ist, dass der Täter sich oder einem Dritten Zugang zu Daten, die nicht für ihn bestimmt sind und gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung, verschafft.[23] Geschützt ist nach herrschender Ansicht die formelle Verfügungsbefugnis des Berechtigten hinsichtlich der in den Daten enthaltenen Informationen.[24]
Unter dem Begriff der Daten versteht man alle durch Zeichen oder kontinuierliche Funktionen dargestellte Informationen, die sich als Gegenstand oder Mittel der Datenverarbeitung für eine Datenverarbeitungsanlage codieren lassen oder die das Ergebnis eines Datenverarbeitungsvorgangs darstellen.[25] Unter den weiten Datenbegriff fallen auch Programmdaten, da diese aus einer Vielzahl von Daten zusammengefügt sind.[26] § 202a Abs. 2 StGB schränkt den Datenbegriff dahingehend ein, dass nur solche Daten in Betracht kommen, welche nicht unmittelbar wahrnehmbar sind und zudem gespeichert oder übermittelt werden können.[27]
Eine Strafbarkeit nach § 202a StGB kommt somit nur dann in Betracht, wenn der Dateninhaber zum einen durch eine mechanische oder technische Zugangssicherung sein Interesse an der Geheinhaltung der Daten zum Ausdruck

[20] *LG Düsseldorf*, MMR 2011, 624 (625).
[21] *Tom Burt*, New action to disrupt world’s largest online criminal network, abrufbar unter: https://blogs.microsoft.com/on-the-issues/2020/03/10/necurs-botnet-cyber-crime-disrupt/ (zuletzt abgerufen am 27.9.2020).
[22] *Roos/Schumacher* MMR 2014, 377 (380 f.).
[23] *Eisele*, in Schönke/Schröder, StGB, 30. Auflage (2019), § 202a Rn. 7.
[24] *Weidemann*, in BeckOK-StGB, 47. Ed. (Stand: 1.8.2020), § 202a Rn. 2; *Hassemer*, in Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Auflage (2019), S. 2672 Rn. 80.
[25] *Eisele*, in Schönke/Schröder, StGB, § 202a Rn. 3.
[26] *Eisele/Nolte,* CR 2020, 488 (498).
[27] *Eisele*, in Schönke/Schröder, StGB, § 202a Rn. 4.

gebracht hat und diese durch den Täter überwunden worden ist.[28] Eine solche Zugangssicherung liegt dann vor, wenn sie objektiv geeignet und subjektiv gewollt ist, Dritte vom Zugriff auf die Daten auszuschließen oder den Zugang wenigstens nicht unerheblich zu erschweren, beispielsweise durch die Vergabe von Passwörtern, der Benutzung von Tastaturschlössern und Antivirensoftware.[29]

Zum anderen ist es nach § 202a StGB nötig, dass der Täter mit der Infiltration der Schadsoftware auf die gespeicherten oder übermittelten Daten des Zielsystems zugreifen könnte. Die bloße Zugangsmöglichkeit zu den Daten des befallenen Systems ist demnach ausreichend. Ein tatsächliches Ausspähen oder eine Besitzerlangung muss nicht stattgefunden haben,[30] wodurch § 202a StGB das Hacking strafrechtlich erfasst.[31]

bb) Strafbarkeitslücken des § 202a StGB in Bezug auf den digitalen Hausfriedensbruch

Nach dem Wortlaut des § 202a StGB ist allein die Zugangsverschaffung zu Daten unter Strafe gestellt. Der digitale Hausfriedensbruch ist jedoch nicht erst mit der Möglichkeit der Kenntnisnahme von Daten, sondern bereits mit dem alleinigen unbefugten Zugang zu einem informationstechnischen System gegeben.

Eine Strafbarkeitslücke bezüglich § 202a StGB kommt demnach dann in Betracht, wenn der Täter zwar Zugang zu dem IT-System erlangt, jedoch nicht die Möglichkeit hat, auf gespeicherte Daten zuzugreifen.[32]

In der technischen Realität erscheint diese juristische Strafbarkeitslücke jedoch so gut wie nicht vorhanden zu sein, da beispielsweise eine Botware, die nicht auch in der Lage ist, einen Zugang, zu den auf dem Zielsystem gesicherten Daten zu verschaffen, dem Botmaster kaum nützlich sein wird, da üblicherweise die Daten des Betroffenen für weitere Straftaten erforderlich sind.[33]

Eine Konstellation, in der der Täter durch die Infiltration einer Schadsoftware nicht auch die Möglichkeit der Kenntnisnahme der auf dem IT-System befindlichen Daten erlangt, scheint somit kaum vorstellbar, weshalb bei einem digitalen Hausfriedensbruch regelmäßig § 202a StGB verwirklicht wird.[34]

Aufgrund dessen, wird in der Literatur § 202a StGB bereits als „elektronischer Hausfriedensbruch" bezeichnet.[35]

Jedoch bleibt einem Betroffenen der strafrechtliche Schutz des § 202a StGB dann verwehrt, wenn keine oder eine nach § 202a StGB unzureichende Zugangssicherung der Daten vorliegt, da der Täter dann entweder keine Zugangssicherung zu überwinden hat oder ihm dies nicht ausreichend erschwert worden ist. Somit hängt ein strafrechtlicher Schutz unter anderem von den technischen Fähigkeiten jedes einzelnen Nutzers ab.

Insbesondere im wirtschaftlichen Bereich kann zwar von ausreichenden Zugangssicherungen ausgegangen werden, da insbesondere im Bereich kritischer Infrastrukturen durch das IT-Sicherheitsgesetz IT-Mindeststandards zur Sicherung von informationstechnischen Systemen, mithin der darauf vorhandenen Daten, vorgeschrieben werden,[36] jedoch sind insbesondere im privaten Bereich nicht ausreichende Zugangssicherungen vorhanden[37], sodass in diesen Fällen ein strafrechtlicher Schutz des § 202a StGB nicht eingreift.

---

28 *Bär*, in Wabnitz/Janovsky/Schmit, Handbuch Wirtschafts- und Steuerrecht, 5. Auflage (2020), 5. Kapitel Rn. 72; *Stömer*, Online-Recht: Juristische Probleme der Internet-Praxis erkennen und vermeiden, 4. Auflage (2006), S. 450; *Marberth-Kubicki*, Computer – und Internetstrafrecht, 2. Auflage (2010), Rn. 88.

29 *Roos/Schumacher*, MMR 2014, 337 (379); *Eisele,* Jura 2012, 922 (925); *Eisele*, Computer- und Medienstrafrecht, 2013, Kapitel 4 § 6 Rn. 15.

30 *Graf,* in: MüKo-StGB, 3. Auflage (2017), § 202a Rn. 62; *Marberth-Kubicki*, Rn. 95; *Eisele*, Jura 2012, 992 (925).

31 *Ernst,* NJW 2007, 2661 (2661).

32 *Eisele/Nolte,* CR 2020, 488 (489).

33 *Mavany,* KriPoZ 2016, 106 (109).

34 *Buermeyer/Golla,* K&R 2017, 14 (15).

35 *Mavany,* KriPoZ 2016, 106 (109); *Golla/Mühlen*, Russen-Hacker und Zombie-Rechner: Gesetzesentwurf zu digitalem Hausfriedensbruch, abrufbar unter: https://www.telemedicus.info/russen-hacker-und-zombie-rechner-gesetzesentwurf-zu-digitalem-hausfriedensbruch/ (zuletzt abgerufen am: 25.8.2020); *Buermeyer/Golla*, K&R 2017, 14 (15); *Marberth-Kubicki*, Rn. 84.

36 § 8a I 1 ITSichG, *Oehmichen/Weißenberger,* KriPoZ 2019, 174 (174 f.).

37 BVerfGE 120, 274 (306); BT-Drs. 19/1716, S. 3; *Marbeth-Kubicki,* Rn. 117; *Malek/Popp,* Strafsachen im Internet, 2. Auflage (2015), Rn. 169.

b) § 202b StGB – Abfangen von Daten

Auch kann die Infiltration einer Schadsoftware nach § 202b StGB strafbar sein.
Nach § 202b StGB macht sich strafbar, wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten aus einer nichtöffentlichen Datenübermittlung verschafft. Demnach kann § 202b StGB dann erfüllt sein, wenn der Täter die Infiltration durch Zugriff auf eine Datenübermittlung vornimmt. Dies ist beispielsweise dann gegeben, wenn der Täter alle ein- und ausgehenden E-Mails abfängt und diese mit schadhaftem Anhang weiterleitet.[38]

c) § 303a StGB – Datenveränderung

aa) Straftatbestand des § 303a StGB
In den meisten Fällen kommt bei der Infiltration mit einer Schadsoftware jedoch eine Strafbarkeit gemäß § 303 StGB in Betracht.
Nach § 303a StGB macht sich strafbar, wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert.[39] Dadurch wird das Interesse des Verfügungsberechtigten an der unversehrten Verwendbarkeit, der in den gespeicherten Daten enthaltenen Informationen, geschützt.[40]
In Bezug auf die Infiltration einer Schadsoftware kann eine Strafbarkeit aufgrund einer Veränderung von Daten einschlägig sein. Verändert werden Daten, wenn sie, wenn auch nur vorübergehend, einen anderen Informationsgehalt erhalten und dadurch ihr Aussagewert inhaltlich umgestaltet wird.[41]
Das Aufspielen einer Schadsoftware müsste somit, um den Tatbestand des § 303a StGB zu erfüllen, den Informationsgehalt anderer, bereits vorhandener Daten verändern.[42]
Dabei ist im Folgenden zu differenzieren, auf welches Betriebssystem die Schadsoftware infiltriert wird.
Ist das Betriebssystemen eine einzige Programmdatei, so wird durch jedes neue Aufspielen eines Programms dieses insgesamt verändert.[43] Dies ist unter anderem bei Unix-ähnlichen Programmen wie macOS oder Linux der Fall, bei dem das Betriebssystem als ein hierarchisches Verzeichnis mit beliebigen Unterverzeichnissen organisiert ist.[44] Nach dem Grundprinzip „Alles ist eine Datei“, bedeutet jedes „Hinzufügen“, mithin auch das einer Schadsoftware, einen zusätzlichen Eintrag in das Verzeichnis und führt dadurch zu einer Veränderung des Betriebssystems insgesamt.[45] Der Tatbestand der Datenveränderung gemäß § 303a StGB ist somit mit der Installation der Schadsoftware erfüllt.
Anders verhält es sich jedoch beispielsweise bei Betriebssystemen wie Windows, die über eine sog. „Registry“ verfügen. Diese ist nicht Teil des eigentlichen Programms, sondern stellt die zentrale hierarchische Konfigurationsdatenbank dar, auf welcher alle systemrelevanten Informationen für Windows und installierte Programme hinterlegt und abgerufen werden können.[46]
Durch das „Hinzufügen“ eines weiteren Eintrags in eine Datenbank beispielsweise durch die Installation einer

38 *Mavany,* KriPoZ 2016, 106 (109).
39 *Wieck-Noodt,* in: MüKo-StGB, 3. Auflage (2019), § 303a Rn. 11.
40 *Wieck-Noodt,* in: MüKo-StGB, § 303a Rn 2; *Zaczyk*, in: Kindhäuser/Neumann/Paeffgen, StGB, 29. Auflage (2018), § 303a Rn. 2; *Ernst,* NJW 2003, 3233 (3237); *Eisele*, Kapitel 4 § 6 Rn. 62.
41 *Marberth-Kubicki*, Rn. 142.
42 *Marberth-Kubicki,* Rn. 142.
43 *Heine,* NStZ 2016, 441 (443).
44 *Heine,* NStZ 2016, 441 (443).
45 *Heine,* NStZ 2016, 441 (443).
46 *Heine,* NStZ 2016, 441 (443).

(Schad)-Software, werden jedoch bereits vorhandenen Daten oder Computerprogramme nicht in ihrem Aussagewert verändert, sondern lediglich die Datenbank in ihrer Gesamtheit vergrößert, weshalb der Tatbestand des § 303a StGB dann nicht verwirklicht ist.[47]
Jedoch kann eine Datenveränderung im Sinne des § 303a StGB dann angenommen werden, wenn die Schadsoftware, insbesondere eine Botware, so auf dem Zielsystem installiert wird, dass diese einen Neustart übersteht, da dies nicht ohne die Veränderung der entsprechenden Systemsteuerdateien möglich ist.[48]

bb) Strafbarkeitslücken des § 303a StGB in Bezug auf den digitalen Hausfriedensbruch
Eine Strafbarkeitslücke nach § 303a StGB besteht somit dann, wenn das Hinzufügen der Schadsoftware keine Datenveränderung herbeiführt, weil das Betriebssystem auf eine Datenbank zurückgreift und die Software nicht in einer solchen Weise auf das System installiert wird, dass diese einen Neustart überstehen soll.
Jedoch ist eine Schadsoftware, die nicht auch einen Neustart zu überstehen vermag, für den Täter nur von geringem Nutzen.

2. Schutz nach datenschutzrechtlicher Strafvorschrift § 42 BDSG

Über das materielle Kernstrafrecht hinaus, käme ein Schutz nach § 42 BDSG (i.V.m. Art. 84 DSGVO) in Betracht. Jedoch ist bereits der persönliche Anwendungsbereich dieser Norm strittig. Einer Auffassung nach ist die Norm auf jeden anwendbar, da der Wortlaut keine Beschränkungen hinsichtlich bestimmter Tätergruppen vornimmt.[49]
Die Gegenansicht nimmt im Hinblick auf den Bestimmtheitsgrundsatz an, dass die Norm nur für die Personen gilt, die die Regelungen des BDSG zu befolgen haben, mithin Verantwortliche (Art. 4 Nr. 7 DSGVO) bzw. Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO) öffentlicher (§ 2 Abs. 1-3 BDDG) bzw. nichtöffentlicher (§ 2 Abs. 4, 5 BDSG) Stellen.
Da das Gesetz sich jedoch auf die Verarbeitung personenbezogener Daten bezieht, ist es nicht primär für die Strafbarkeit eines digitalen Hausfriedensbruchs heranzuziehen.

IV. Vorschläge zur „Lückenschließung“ im Bereich des digitalen Hausfriedensbruchs

1. Gesetzesentwurf des § 202e StGB

a) Zielsetzung und Notwendigkeit des Gesetzesentwurfs

Insbesondere im Zusammenhang mit der Botnetz-Kriminalität hat der Bundesrat in der 19. Wahlperiode einen vom Land Hessen ursprünglich eingebrachten und zuvor dem Diskontinuitätsprinzip zum Opfer gefallenen wortlautidentischen Gesetzesentwurf in den Bundestag eingebracht.[50]
Dieser soll, durch die Einführung eines neuen Straftatbestandes § 202e StGB, die unbefugte Benutzung informationstechnischer Systeme unter Strafe stellen, um einen erweiterten strafrechtlichen Schutz des Grundrechts auf

47 *Heine,* NStZ 2016, 441 (443).
48 *Eichelberger,* MMR 2004, 594 (595); *Heine,* NStZ 2016, 441 (443).
49 *Eisele/Nolte,* CR 2020, 488 (493).
50 BT-Drs. 19/1716.

Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht) gewährleisten zu können.[51]

Insbesondere sollte eine bessere Bekämpfung der Botnetz-Kriminalität ermöglicht werden, da durch die Verwendung derer weitreichende Rückschlüsse auf die Persönlichkeit, bis hin in den Kernbereich höchstpersönlicher Lebensgestaltung, möglich sind.[52] Es sei die Aufgabe des Strafrechts, den lückenlosen Schutz des IT- Grundrechts sicherzustellen insbesondere, da sich der Einzelne nicht ausreichend gegen eine Infiltration seines Computers mit einer Schadsoftware, mithin gegen eine unbefugte Benutzung seines Systems schützen könne.[53]

Darüber hinaus würde dem Ziel der vollständigen Umsetzung des Art. 2 des Budapester Übereinkommens über Computerkriminalität[54] und des Art. 3 der EU-Richtlinie über Angriffe auf Informationssysteme[55] nachgegangen werden. Dort heißt es in beiden Vorschriften, dass jeder Vertragspartei bzw. jeder Mitgliedsstaat erforderliche Maßnahmen zu treffen hat, um den unbefugten Zugang zu einem Informationssystem als Ganzes oder zum Teil unter Strafe zu stellen.

Der Gesetzesbegründung nach wären die bereits bestehenden Straftatbestände nicht für die Durchsetzung dieser Ziele ausreichend, da insb. § 202a StGB, § 303a StGB und § 303b StGB nur bestimmte Daten, nicht aber das technische System als solches schützen.[56] Schon das ausschließliche Gebrauchsrecht des rechtmäßigen Nutzers sei schützenswert.[57]

Aufgrund dessen sollen die Rechtsgedanken der § 123 StGB und § 248b StGB in die digitale Welt übertragen und dadurch der neue Straftatbestand des § 202e StGB geschaffen werden.[58]

b) Der neue Straftatbestand des § 202e StGB

Der durch den Bundesrat eingebrachte Gesetzesentwurf § 202e StGB - Unbefugte Benutzung informationstechnischer Systeme - soll nach den Angaben des § 202d StGB in das Strafgesetzbuch mit folgendem Inhalt eingefügt werden:

„ (1) Wer unbefugt

1. sich oder einem Dritten den Zugang zu einem informationstechnischen System verschafft,
2. ein informationstechnisches System in Gebrauch nimmt oder
3. einen Datenverarbeitungsvorgang oder einen informationstechnischen Ablauf auf einem informationstechnischen System beeinflusst oder in Gang setzt,

wird mit Geldstrafe oder Freiheitsstrafe bis zu einem Jahr bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist. Die Tat nach Satz 1 ist nur strafbar, wenn sie geeignet ist, berechtigte Interessen eines anderen zu beeinträchtigen.“[59]

In den folgenden sechs Absätzen werden Qualifikationen, besonders schwere Fälle, eine Versuchsstrafbarkeit, Begriffsdefinitionen und Antragserfordernisse normiert.

[51] BT-Drs. 19/1716, S. 3, 5.
[52] BT-Drs. 19/1716, S. 3; *Winkelmeier-Becker,* R&P 2019, 181 (182).
[53] BT-Drs. 19/1716, S. 3.
[54] Übereinkommen über Computerkriminalität vom 23.11.2001, Sammlung Europäischer Verträge (SEV) - Nr. 185, Artikel 2.
[55] Richtlinie 2013/40/EU des Europäischen Parlaments und Rates vom 12.8.2013 über Angriffe auf Informationssysteme zur Erlassung eines Rahmenbeschlusses 2005/222/JI des Rates, ABl. EU L 218, S. 8.
[56] BT-Drs. 19/1716, S. 11.
[57] BT-Drs. 19/1716, S. 11.
[58] BT-Drs. 19/1716, S. 5.
[59] BT-Drs. 19/1716, S. 9.

c) Kritische Stellungnahme

Grundsätzlich ist dem Ziel des Gesetzesentwurfes, den strafrechtlichen Schutz des IT-Grundrechts zu erweitern und die Botnetz-Kriminalität effektiver bekämpfen zu wollen, zuzustimmen.
Jedoch ist im Hinblick auf das „Ultima-ratio-Prinzip" des Strafrechts eine kritische Betrachtung dahingehend nötig, ob der „digitale Hausfriedensbruch", wie ihn § 202e StGB normiert, in dieser Art und Weise zielführend ist.

aa) Übertragung der Rechtsgedanken der §§ 123, 248b StGB
Allein die Übertragung der Rechtsgedanken der §§ 123, 248b StGB in die virtuelle Welt lässt sich nicht ohne weiteres, wie es der Gesetzesvorschlag annimmt, konstruieren.
Nach § 123 StGB wird das Hausrecht, das heißt die Freiheit zu bestimmen wer sich innerhalb einer bestimmten räumlichen Sphäre aufhalten darf und wer nicht, geschützt.[60]
Allein diesbezüglich ist auffällig, dass die Tathandlung des § 123 StGB das „widerrechtliche Eindringen" und nicht die „unbefugte Benutzung" ist, weshalb die Bezeichnung des „digitalen Hausfriedensbruchs" nicht zu der Normüberschrift der „unbefugten Benutzung informationstechnischer Systeme" passt.[61]
Überträgt man dennoch § 123 StGB in die digitale Welt, so müsste zunächst die Sphäre des „digitalen Hauses" zu bestimmen sein. Dies ist jedoch in technischer Hinsicht aufgrund der flächendeckenden Vernetzung und dem Nutzen von Clouds nicht genau möglich[62] und wäre mit dem Bestimmtheitsgrundsatz nicht vereinbar.
Auch ist es weiterhin fraglich, was das „virtuelle Hausrecht" genau umfasst[63] und wem dieses Recht zustehen soll, da Eigentümer, Nutzer und Dateninhaber unterschiedliche Personen sein können; man denke an einen geleasten, vermieteten oder unter Eigentumsvorbehalt verkauften Computer.[64]
Auch überzeugt die Übertragung des Rechtsgedanken der Ausnahmevorschrift des § 248b StGB in die virtuelle Welt nicht. Während in § 248b StGB der Eigentümer, welcher vor einer unbefugten Ingebrauchnahme geschützt werden soll,[65] bei einer Gebrauchsanmaßung vollständig um seine Nutzungsmöglichkeit gebracht wird, wird es der Berechtigte eines IT-Systems während einer „virtuellen Gebrauchsanmaßung" meist nicht. [66] Der „Betroffene" kann das System für seine Zwecke weiterhin nutzen und bekommt von alledem meist nichts mit, sodass die Gebrauchsanmaßung unterhalb der strafrechtlichen Erheblichkeitsschwelle läge.[67]
Der Schutz einer unbefugten Benutzung informationstechnischer Systeme durch die Übertragung der Rechtsgedanken der §§ 123, 248b StGB zu kreieren, geht somit an der technischen Realität vorbei.

bb) Schutzgut
Laut der Gesetzesbegründung soll das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme das Schutzgut des § 202e StGB sein. Dieses Grundrecht wurde vom Bundesverfassungsgericht in seiner Entscheidung zur „Online-Durchsuchung" aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) hergeleitet.[68]

60 *Heger*, in: Lackner/Kühl, StGB, 29. Auflage (2018), § 123 Rn. 1.; *Schäfer,* in: MüKo-StGB, § 123 Rn. 2; *Tassi,* DuD 2017, 175 (177).
61 *Kahler/Hoffmannn-Holland,* KriPoZ 2018, 267 (268).
62 *Mavany,* KriPoZ 2016, 106 (110).
63 *Tassi*, DuD 2017, 175 (177 f.).
64 *Mavany,* KriPoZ 2016, 106 (110).
65 *Hohmann,* in: MüKo-StGB, § 248 b Rn. 1.
66 *Kahler/Hoffmannn-Holland,* KriPoZ 2018, 267 (268).
67 *Mavany,* ZRP 2016, 221 (222).
68 BVerfGE 120, 274 (313); BT-Drs. 19/1716 S. 11.

Nach dem *BVerfG* schützt das IT-Grundrecht das Interesse des Nutzers, dass die von den vom Schutzbereich erfassten informationstechnischen Systeme erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Dies soll dadurch gewährleistet werden, dass nicht auf ein IT-System zugegriffen werden darf, wenn hierfür keine Berechtigung vorliegt.[69]

Die Integrität der informationstechnischen Systeme ist nur deshalb gefährdet, weil durch deren Verletzung letztendlich der Zugriff auf die in dem System gespeicherten Daten möglich ist.[70]

Bei der Gefährdung des IT-Systems handelt sich somit um eine „Annex-Gefahr"[71]. Das IT-Grundrecht schützt somit nicht primär das System selbst oder dessen unbeeinflussten Gebrauch, sondern stellt vielmehr eine Form des „vorgezogenen Datenschutzes" dar, welcher jedoch bereits durch die §§ 202a, 202b, 303a, 303b StGB sichergestellt wird.[72]

Das Grundrecht somit primär als Schutzgut einer Norm zur Bekämpfung des digitalen Hausfriedenbruch zu postulieren, überzeugt demnach nicht.

cc) Ausufernd weite Strafbarkeit

Darüber hinaus ist der Tatbestand des § 202e StGB durch die nahezu vollständige Einbeziehung aller IT-Systeme uferlos und entspricht nicht dem verfassungsrechtlichen Schutzgut des Grundrechts, welches dem Gesetzesentwurf zugrunde gelegt worden ist.

Verfassungsrechtlich geschützt werden allein solche IT-Systeme, die personenbezogene Daten des Betroffenen in einem solchen Umfang enthalten können, dass sie im Falle eines Eingriffs einen Einblick in wesentliche Lebensgestaltung der Person oder gar ein aussagekräftiges Bild der Persönlichkeit ermöglichen können.[73]

Die umfassende Einbeziehung hätte zur Folge, dass nahezu jede unbefugte Benutzung eines IT-Systems den objektiven Tatbestand des § 202e StGB erfüllt und somit auch alltägliche Handlungsweisen unter Strafe gestellt werden würden, wodurch die Grenzen des Übermaßverbotes gesprengt zu werden drohen.[74]

Auch vermag die in Abs. 1 S. 2 eingefügte Geringfügigkeitsklausel den Tatbestand nicht einzuschränken, da der Gesetzesbegründung nach ein „berechtigtes Interesse" wiederum nahezu jedes Interesse des Nutzers und sogar der Allgemeinheit darstellen kann.[75]

Somit geht die Einbeziehung nahezu aller IT-Systeme weit über den verfassungsrechtlichen Schutz hinaus, wodurch § 202e StGB strafrechtlich mehr schützen wollen würde, als verfassungsrechtlich vorgesehen ist.[76]

dd) Zwischenfeststellung

Aufgrund der aufgezeigten Unstimmigkeiten innerhalb des Tatbestandes und der Gesetzesbegründung ist der Tatbestand nicht zur gezielten Bekämpfung des digitalen Hausfriedensbruchs heranziehen und deswegen in seiner jetzigen Fassung abzulehnen.

69 BVerfGE 120, 274 (314).
70 *Eifert*, NVwZ 2008, 521 (522).
71 *Eifert,* NVwZ 2008, 521 (522).
72 *Mavany,* ZRP 2016, 221 (222); *Mavany,* KriPoZ 2016, 106 (112).
73 BVerfGE 120, 274 (314).
74 *Buermeyer/Golla,* K&R 2017, 14 (17); *Kahler/Hoffmannn-Holland,* KriPoZ 2018, 267 (275)*; Graf,* in: MüKo-StGB, § 202 a Rn. 8; *Basar,* JurisPR-StrafR 2016, IV. Bewertung und Ausblick, abrufbar unter: https://www.strafrecht.de/media/files/docs/180227_Basar_digitaler_Hausfriedensbruch_jurisPR-StrafR_26_2016.pdf (zuletzt abgerufen am: 15.9.2020).
75 BT-Drs. 19/1716, S. 16.
76 *Kahler/Hoffmannn-Holland,* KriPoZ 2018, 267 (269).

2. Ein Entwurf von Buermeyer/ Golla zur „Lückenschließung"

a) Der Entwurf

Ein Entwurf der Literatur möchte gezielt die Infektion mit einer Schadsoftware unter Strafe zu stellen. Nach *Dr. U. Buermeyer* und *Br. S. J. Golla* wäre die Ergänzung des § 202c Abs. 1 StGB um einen zweien Satz zielführend, welcher wie folgt lauten solle:
„Ebenso wird bestraft, wer eine Straftat vorbereitet, indem er einen Programmcode auf ein informationstechnisches System ohne Einwilligung einer berechtigten Person in der Absicht aufbringt, diesen ausführen zu lassen."[77]

b) Kritische Stellungnahme

Grundsätzlich ist der Idee, gezielt die Infektion eines IT-Systems mit einer Schadsoftware strafrechtlich unter Strafe stellen zu wollen, zuzustimmen. Jedoch berücksichtigt der Vorschlag nicht, dass die Absicht eines Hackers nicht zwingend in der Vorbereitung einer Straftat liegen muss.[78]
Es sollte allein das Eindringen in das IT-System mittels einer Schadsoftware unter Strafe gestellt werden. Dies an die Absicht zu knüpfen, den Programmcode auch ausführen zu lassen, ist in Bezug darauf, die bloße Installation einer Schadsoftware, mithin den digitalen Hausfriedensbruch unter Strafe stellen zu wollen, ein zu einschränkendes Kriterium.

3. Entwurf von Eisele/Nolte zur „Lückenschließung"

a) In Bezug auf § 202a StGB

Ein anderer Vorschlag in der Literatur, um die vorhandenen Lücken des § 202a StGB zu schließen und eine umfassende Strafbarkeit zu ermöglichen, wird von Eisele und Nolte wie folgt formuliert:
„(1) Wer unbefugt sich oder einem Dritten Zugang zu nicht für ihn bestimmte Daten oder Informationssystemen, die gegen unberechtigten Zugang besonders gesichert sind
1. unter Überwindung der Zugangssicherung oder
2. unter Verwendung unbefugt erlangter Passwörter oder sonstiger Sicherheitscodes oder
3. unter Ausnutzung eines von einem Dritten unbefugt geschaffenen Zugangs
verschafft
wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft."[79]
In den folgenden 4 Absätzen werden zudem die unbefugte Datenverschaffung, der Versuch und die Qualifikationen der Straftat nach Absatz 1 normiert.

77 *Buermeyer/Golla,* K&R 2017, 14 (18).
78 *Kahler/Hoffmann-Holland,* KriPoZ 2018, 267 (272).
79 *Eisele/Nolte,* CR 2020, 488 (491).

b) Kritische Stellungnahme

Zuzustimmen ist dem Vorschlag dahingehend, dass nunmehr der bloße Zugang zu einem informationstechnischen System unter Strafe gestellt wird, mithin der digitale Hausfriedensbruch mittels einer Schadsoftware. Durch Abs. 1 Nr. 2 wäre es unter anderem möglich, Fälle des „Phishings“[80] strafrechtlich eindeutig zu erfassen.[81] Durch die Einführung der Nr. 3 könnten zudem sogenannte „Backdoor[82] -Fälle“ erfasst werden.[83]
Auch die in Abs. 4 des Vorschlags genannte Versuchsstrafbarkeit ist zu befürworten. Denn bis dato ist zwar die Vollendung gem. § 202a StGB und die Vorbereitungshandlung gem. § 202c StGB unter Strafe gestellt, nicht jedoch das unmittelbare Ansetzen zur Tat, welches häufig jedoch allein von technischen Einzelheiten und Fähigkeiten des Täters abhängt.[84]
Jedoch wäre es unter anderem auch im Hinblick auf das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme erstrebenswert, den alleinigen Zugriff auf ein informationstechnisches System, das speziell dazu geeignet ist, tiefe Einblick in persönliche Teile der Lebensgestaltung geben zu können, unter Strafe zu stellen, ohne dass hierbei eine Zugangssicherung bestehen und überwunden werden muss.
Ein weiterer Tatbestand könnte somit wie folgt lauten:
– Wer sich unbefugt Zugang zu einem informationstechnischen System verschafft, welches personenbezogene Daten enthält, die dazu geeignet sind, wesentliche Einblicke in die Lebensgestaltung zu ermöglichen, wird mit Geldstrafe oder einer Freiheitsstrafe von sechs Monaten bis zu zehn Jahren bestraft. –

c) In Bezug auf § 303a StGB

Möchte man die Strafbarkeitslücken im Hinblick auf den digitalen Hausfriedensbruch mittels einer Schadsoftware schließen, so wäre dies nach Eisele/ Nolte dadurch möglich, dass der Tatbestand des § 303a StGB um die Handlungsvariante des „unbefugten Einschleusens eines Programmcodes in ein Informationssystem“ ergänzt wird.[85]

d) Stellungnahme

Diesem Vorschlag zur Ergänzung des § 303a StGB ist beizupflichten, da es durch diese Erweiterung möglich ist, den digitalen Hausfriedensbruch mittels einer Schadsoftware unzweifelhaft unter Strafe stellen zu können.

V. Fazit

Abschließend ist festzuhalten, dass der digitale Hausfriedensbruch, insbesondere durch die Normen der §§ 202a, 202b StGB und § 303a StGB, bereits als Straftat erfasst ist. Jedoch wäre es unter Achtung des „Ultima-Ratio-Prinzips“ durch gezielte Gesetzesänderungen möglich, den strafrechtlichen Schutz bezüglich eines digitalen Hausfriedensbruchs zu erweitern und noch eindeutiger zu normieren.
Wirksamer für die Praxis wäre es jedoch, künftig mehr in die Entwicklung von Hard- und Software zu investieren, um eine unbefugte Zugangsverschaffung bestmöglich im Vorhinein verhindern zu können.

80 *Graf,* NStZ 2007, 129 (129).
81 *Eisele/Nolte,* CR 2020, 488 (491).
82 *Eisele*, 4. Kapitel § 6 Rn. 19.
83 *Eisele/Nolte,* CR 2020, 488 (491).
84 *Ernst,* NJW 2007, 2661 (2662); *Eisele/Nolte,* CR 2020, 488 (491).
85 *Eisele/Nolte,* CR 2020, 488 (491).

Zudem sollte in Zukunft noch mehr die Lösung des Problems hinsichtlich der schweren Fassbarkeit vieler Täter durch die Möglichkeit der Anonymisierung und internationalen Arbeitsteilung, insbesondere für die Strafverfolgungsbehörden, ins Auge gefasst werden, denn das Vorhandensein von Rechtsvorschiften ist nur so lange von Bedeutung, wie diese auch durchgesetzt werden können.