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.).