Rechtsanwalt Ralf Möbius LL.M.
Rechtsinformatik
Fachanwalt für IT-Recht
Am Ortfelde 100
D - 30916 Isernhagen

Tel.: 0511 - 844 35 35
Fax: 03212 - 844 35 35*
* 2,9 cent pro Minute
e-mail: ralfmoebius@gmx.de
www.rechtsanwaltmoebius.de

Dezember 2019

Das Maßnahmenpaket der Bundesregierung zur Bekämpfung des Rechtsextremismus und der Hasskriminalität als Bedrohung der Meinungsfreiheit im Internet

I. Einführung

Im Jahre 2019 ereigneten sich drei mutmaßlich rechtsextreme Taten, die mit dem Internet auf verschiedene Arten verknüpft waren. Die Terroranschläge auf zwei Moscheen im neuseeländischen Christchurch am 15. März 2019 und auf die Synagoge im Paulusviertel in Halle an der Saale am 09. Oktober 2019 wurden beide mittels Live-Streamings im Internet auf verschiedenen Online-Plattformen weltweit übertragen. Zahlreiche Internetnutzer äußerten zu diesen beiden Anschlägen anschließend ihre Zustimmung in öffentlich einsehbaren Kommentaren, genauso, wie dies im Anschluss an die Ermordung des Regierungspräsidenten Walter Lübcke der Fall war. Bei einer großen Anzahl dieser Kommentare handelte es sich um strafrechtlich relevante Äußerungen, deren Ahndung für die Strafverfolgungsbehörden schwierig war, da die Identität vieler Kommentatoren nicht ermittelt werden konnte. Im Lübcke-Fall wurden trotz dieser Schwierigkeiten mehr als einhundert Strafverfahren eingeleitet.[1] Um die Taten in einen gesellschaftlichen Kontext einordnen und mit einem gesetzlichen Regelungsbedürfnis verknüpfen zu können, bedarf es einer näheren Beschreibung der Tatumstände.

[1] „Mehr als 100 Verfahren wegen Hasskommentaren im Fall Walter“ Lübckehttps://www.zeit.de/gesellschaft/zeitgeschehen/2019-08/walter-luebcke-hasskommentare-internet

II. Die Anschläge in Wolfhagen, Halle an der Saale und Christchurch

Am 02. Juni 2019 wurde der Kasseler Regierungspräsident Walter Lübcke im hessischen Wolfhagen bei Kassel auf seinem Grundstück mit einem Pistolenschuss aus nächster Nähe in den Kopf getötet. Der Tatverdächtige legte am 25. Juni 2019 ein Geständnis ab, das er am 2. Juli 2019 widerrief. Das Tatmotiv des Geständnisses seien folgende Äußerungen von Walter Lübcke auf einer Bürgerversammlung am 14. Oktober 2015 in Lohfelden gewesen: "Ich bin stolz drauf, dass wir als Regierungspräsidium mit der Mannschaft, mit den Ehrenamtlichen hier dazu beitragen, da danke ich aber auch den Schülern, was ich in der Zeitung gesehen habe und den Lehrern. Ich hab´ mich hier mal für die Schule mal eingesetzt, das hier auch in der Schule das weitergeben, das trägt auch Früchte davon, dass wir eine tolle Schule haben, dass wir mit Kirchen hier eine Wertevermittlung haben, wo wir sagen, es lohnt sich in unserem Land zu leben. Da muss man für Werte eintreten. Und wer diese Werte nicht vertritt, der kann jederzeit dieses Land verlassen, wenn er nicht einverstanden ist. Das ist die Freiheit eines jeden Deutschen." Das Video der Bürgerversammlung in Lohfelden mit den Äußerungen Lübckes[2] wurde nach der Tat erneut im Internet verbreitet und zahlreiche Kommentatoren äußerten Zustimmung zu dem Mord an dem Kasseler Regierungspräsidenten.[3]

Am 09. Oktober 2019 ereignete sich in Halle an der Saale ein Anschlag auf die Synagoge im Paulusviertel mit selbstgebauten Schusswaffen[4], mit dem Ziel, in die Synagoge einzudringen um dort möglichst viele Menschen jüdischen Glaubens zu töten. Der Anschlag hatte in Bezug auf die jüdische Gemeinde bis auf einige Sachbeschädigungen keinen Erfolg. Jedoch erschoss der Täter nach dem gescheiterten Anschlag zwei Menschen, die mit dem Anschlagsziel nichts zu tun hatten und zufällig den Weg des Täters kreuzten. Zwei weitere Menschen wurden auf der Flucht verletzt, mehrere Schüsse auf Polizisten verfehlten ihr Ziel. Der Täter selbst wurde durch Schüsse der Polizei verletzt. Die Anschlagspläne hatte der Täter zuvor im Internet bekanntgegeben und die Tat selbst wurde per Helmkamera live auf der

---

[2] Erstaufnahme Asyl RP Lübke Kassel Lohfelden 14.10.2015
https://www.youtube.com/watch?v=KdnLSC2hy9E

[3] Rechte feiern den Tod von Walter Lübcke im Netz
https://www.stern.de/politik/deutschland/walter-luebcke--rechte-feiern-den-tod-von-kassels-regierungspraesidenten-8740780.html

[4] Anschlag in Halle (Saale) 2019
https://de.wikipedia.org/wiki/Anschlag_in_Halle_(Saale)_2019

Internet-Streaming-Portal Twitch übertragen. Das Video des Attentates von Halle wurde nach Angaben der Streaming-Plattform von rund 2200 Menschen angesehen, bevor es nach etwa 30 Minuten gelöscht wurde[5].

Schon der Attentäter im neuseeländischen Christchurch hatte am 15. März 2019 sein Attentat auf zwei Moscheen, bei der er 50 Menschen in einer Moschee erschoss, auf dem Internet-Portal Facebook live gestreamt. Das knapp 17 Minuten lange Video wurde von knapp 200 Menschen live auf Facebook gesehen und eine Kopie dieses Video anschließend vielfach auf anderen Plattformen im Internet veröffentlicht und dort von tausenden Menschen gesehen[6].

Allen Taten ist gemein, dass ein einzelner Täter mit Schusswaffen Menschen wegen ihres politischen oder religiösen Bekenntnisses töten wollte und die Taten anschließend im Internet in den Kommentaren einer erheblichen Anzahl von Internetnutzern auf Zustimmung stieß. Die Attentate in Halle und Christchurch wurden zudem per Internet-Stream einem theoretisch unbeschränkten Nutzerkreis zur Verfügung gestellt. Technische Beschränkungen zur Wahrnehmbarkeit der gestreamten Gewaltvideos gab es nicht, einzig das durch die Thematik der Plattformen eingegrenzte Publikum und die dadurch begrenzte Reichweite des Streams der Tat bedingten zunächst eine relativ geringe Zuschauerzahl. Die Ubiquität des Internets ermöglichte grundsätzlich die weltweite Wahrnehmbarkeit der Attentate zum Zeitpunkt ihrer Ausführung und als Aufzeichnung darüber hinaus.

III. Das Maßnahmenpaket zur Bekämpfung des Rechtsextremismus und der Hasskriminalität und der Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz

Auch angesichts des Hintergrunds dieser Taten beschloss das deutsche Bundeskabinett am 30. Oktober 2019 ein Maßnahmenpaket zur Bekämpfung des

[5] „Streaming-Plattform: Bekennervideo sahen rund 2200 Menschen“ https://www.welt.de/regionales/sachsen-anhalt/article201675726/Streaming-Plattform-Bekennervideo-sahen-rund-2200-Menschen.html

[6] ANSCHLAG IN CHRISTCHURCH: 200 Nutzer sahen live auf Facebook zu https://www.faz.net/aktuell/politik/ausland/200-nutzer-sahen-dem-attentaeter-von-christchurch-live-auf-facebook-zu-16097505.html

Rechtsextremismus und der Hasskriminalität[7] und bezog sich zur Rechtfertigung des Pakets unmittelbar auf das fehlgeschlagene Attentat in Halle. Bundesjustizministerin Christine Lambrecht begründete das Maßnahmenpaket mit der Notwendigkeit, Rechtsextremismus und Antisemitismus mit allen Mitteln des Rechtsstaats entgegentreten zu müssen[8].

Der Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz vom 12.12.2019[9] betonte insbesondere, dass öffentlich ausgesprochene Drohungen dazu beitrügen, dass die Hemmschwelle zur Tatausführung beim Verfasser des Inhalts oder bei Dritten, die die Drohung wahrnehmen würden, sinke, wie die Ermordung des Kasseler Regierungspräsidenten Walter Lübcke sowie die Ermordung zweier Menschen im Rahmen des Attentats auf die Synagoge in Halle zeige. Im Internet und insbesondere in den sozialen Medien sei eine zunehmende Verrohung der Kommunikation zu beobachten, in welcher sich Personen immer öfter allgemein, vor allem aber gegenüber gesellschaftlich und politisch engagierten Personen in einer Weise äußerten, die gegen das geltende deutsche Strafrecht verstoße und sich durch stark aggressives Auftreten, Einschüchterung und Androhung von Straftaten auszeichne. Dadurch würde nicht nur das Allgemeine Persönlichkeitsrecht der Betroffenen angegriffen, sondern auch der politische Diskurs in der demokratischen und pluralistischen Gesellschaftsordnung in Frage gestellt.

Der Verfolgungsdruck solle daher weiter erhöht werden um Hetze und Drohungen im Internet härter und effektiver verfolgen zu können.

Dazu solle die Meldepflicht der Plattformen im Netzwerkdurchsetzungsgesetz dienen und Betroffene sollen durch Änderungen im Melderecht besser geschützt werden. Das Waffenrecht solle durch die Einführung der Regelabfrage bei den Verfassungsschutzbehörden verschärft werden.

Das Maßnahmenpaket solle im Einzelnen

---

[7] Maßnahmenpaket zur Bekämpfung des Rechtsextremismus und der Hasskriminalität
https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2019/massnahmenpaket-bekaempfung-rechts-und-hasskrim.html

[8] Bundesministerium des Innern, für Bau und Heimat, PRESSEMITTEILUNG vom 30.10.2019
Gegen Rechtsextremismus und Hasskriminalität, Bundesregierung beschließt Maßnahmenpaket
https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2019/10/kabinett-beschliesst-massnahmen-gg-rechtsextrem-u-hasskrim.html

[9] RefE: Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität
Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz
https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_BekaempfungHatespeech.html

die Identifizierung bei Hasskriminalität im Netz verbessern,

die Strafbarkeit von Cyber-Stalking, Hetze und aggressiver Beleidigung anpassen,

den Schutz von Kommunalpolitikerinnen und -politikern verbessern,

die Bearbeitung des Rechtsextremismus im Verfassungsschutzverbund intensivieren und den Austausch mit der Polizei verstärken,

das Waffen- und Sprengstoffrecht schärfen,

den Schutz des medizinischen Personals verbessern,

das Recht der Melderegister anpassen,

die Präventionsarbeit ausweiten und verstetigen und

Ressourcen stärken.

In Bezug auf konkrete rechtliche Veränderungen mit unmittelbarem Bezug zum Internet sah das Maßnahmenpaket zur Bekämpfung des Rechtsextremismus und der Hasskriminalität vom 30. Oktober 2019[10] einmal vor, zur Verbesserung der Identifizierung bei Hasskriminalität im Internet eine Meldepflicht für Diensteanbieter im Netzwerkdurchsetzungsgesetz (NetzDG) einführen. Ziel sei eine Verpflichtung der Telemediendiensteanbieter vor allem bei Morddrohungen und Volksverhetzung eigenständig an die Strafverfolgungsbehörden herantreten zu müssen, um die relevanten Inhalte und IP-Adressen einer neu zu errichtenden Zentralstelle im BKA mitzuteilen. Der Deliktskatalog in § 1 Absatz 3 NetzDG werde entsprechend angepasst und die Zahl der im NetzDG erfassten sozialen Netzwerke möglicherweise ausgeweitet. Im BKA-Gesetz und in der StPO soll eine Auskunftsbefugnis gegenüber den Diensteanbietern geschaffen werden, damit die dort vorhandenen Daten zur Verfolgung von Hasskriminalität herausverlangt werden können.

Ein weiter Aspekt solle die Einführung der Strafbarkeit von Cyber-Stalking sein sowie die Schaffung eines neuen rechtlichen Rahmens für Hetze und aggressive Beleidigung. Der strafrechtlichen Ächtung von Gewalthetze in all ihren Erscheinungsformen komme herausragende Bedeutung zu und Personen, die auf

[10] Maßnahmenpaket zur Bekämpfung des Rechtsextremismus und der Hasskriminalität
Beschluss der Bundesregierung vom 30. Oktober 2019
https://kripoz.de/2019/10/30/massnahmenpaket-zur-bekaempfung-des-rechtsextremismus-und-der-hasskriminalitaet/

allen Ebenen für das demokratisches Gemeinwesen einstehen würden, verdienten den besonderen Schutz des Staates. Hinter diesen Worten scheint sich das Bedürfnis der Bundesregierung zu verbergen, Politikern einen besonderen Schutz vor Angriffen im Internet zu gewähren. Tatsächlich begründet der Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz einen besonderen Schutz von Politikern vor Meinungsäußerungen im Internet mit der Intensivierung der Kritik an deren politischen Äußerungen, welche die Meinungsfreiheit gefährden würden. So würden für das Gemeinwesen aktive und daher in der Öffentlichkeit stehende Repräsentanten nach politischen Äußerungen oft mit diffamierender Kritik oder Morddrohungen überzogen. Mit oft über einen langen Zeitraum für eine breite Öffentlichkeit wahrnehmbaren herabwürdigenden Inhalten sinke die Hemmschwelle für ähnliche Äußerungen. In diesem verrohten Umfeld komme es schon jetzt dazu, dass Meinungen aus Sorge vor unbotmäßiger Kritik nicht mehr geäußert werden und sich Menschen vollständig aus der öffentlichen politischen Debatte zurückziehen. Damit sei der freie Meinungsaustausch im Internet und letztendlich die Meinungsfreiheit selbst gefährdet.

Um die Meinungsfreiheit zu schützen, sollen deshalb die Regelungen des StGB mit Bezug zur Hasskriminalität was die Aspekte der Aufforderung zu Straftaten oder der Billigung oder Verharmlosung von Straftaten angeht ergänzt werden und der Tatbestand der Beleidigung soll an die Besonderheiten des Internets angepasst werden, weil dessen unbegrenzte Reichweite und die vermeintlicher Anonymität eine oft sehr aggressive Begehungsweise dieser Delikte bedingen würden.

Weil das seit 2017 geltende Netzwerkdurchsetzungsgesetz zwar zu zahlreichen Löschungen von Äußerungen geführt habe, aber nicht zur strafrechtlichen Verfolgung der Verfasser der gelöschten Inhalte, verstärke sich der Eindruck, dass sich das Internet zu einem rechtsfreien Raum entwickele. Bestimmte strafbare Inhalte sollen daher durch die Anpassung des NetzDG, die StPO und des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten gemeldet werden müssen, damit anschließend die zuständigen Strafverfolgungsbehörden tätig werden können.

Wichtigste Voraussetzung für den Erfolg sämtlicher Verschärfungen der relevanten Gesetze ist in jedem Fall die Identifizierung in Betracht kommender Täter. Dazu sei nach dem Referentenentwurf des Bundesministeriums der Justiz und für

Verbraucherschutz notwendig, dass die Tatverdächtigen identifiziert und Beweise gesichert werden könnten. Da in der Strafprozessordnung die Erhebung von Bestands- und Verkehrsdaten gegenwärtig nur für Maßnahmen gegenüber Telekommunikationsdiensteanbietern geregelt seien und entsprechende Vorschriften für die Datenerhebung gegenüber Telemediendiensteanbietern fehlten, seien diese nunmehr zu schaffen. Dieser zentrale Ansatz verdient daher, im Gegensatz zu Verschärfung bereits bestehender Tatbestände, genaueres Hinsehen.

1. Die Änderung des § 100g StPO

Weil § 100g Abs. 1 Nr. 2 StPO die Erhebung von Verkehrsdaten bei dem Verdacht, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung davon abhängig macht, dass eine Straftat mittels Telekommunikation begangen wurde, war lange Zeit unklar, ob die Vorschrift wegen der genannten Verkehrsdaten als Begriff des Telekommunikationsrechts auch auf einen internetbasierten E-Mail-Dienst wie Google-Mail, der selbst keinen Internetzugang vermittelt, anzuwenden ist. Wäre dies der Fall, so dürften bei Straftaten, die über Google-Mail oder vergleichbare Dienste begangen werden Verkehrsdaten (§ 96 Absatz 1 des Telekommunikationsgesetzes und § 2a Absatz 1 des Gesetzes über die Errichtung einer Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben) erhoben werden, soweit dies für die Erforschung des Sachverhalts erforderlich ist und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht.

a) Das Urteil des Verwaltungsgerichts Köln vom 11.11.2015

Das Verwaltungsgericht Köln VG Köln hatte in seinem Urteil vom 11.11.2015 zum Az.: 21 K 450/15[11] noch die Ansicht vertreten, der von Google bereitgestellte Dienst ermögliche den Nutzern des Dienstes Gmail über ein Web-Interface über das Internet per E-Mail zu kommunizieren und stelle damit einen Telekommunikationsdienst bereit. Der Einordnung von Gmail als Telekommunikationsdienst stehe dabei nicht entgegen, dass die Übertragung von Signalen im Wesentlichen über das offene Internet erfolge

[11] VG Köln, Urteil vom 11.11.2015 - 21 K 450/15; https://openjur.de/u/866817.html

und damit nicht von Google selbst, sondern von den Internetzugangsanbieter erbracht werde.

Die Anforderungen an einen Telekommunikationsdienst im Sinne des § 6 TKG seien durch § 3 Nr. 24 TKG definiert, wonach "Telekommunikationsdienste" in der Regel gegen Entgelt erbrachte Dienste seien, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen. Diese Definition entspreche nahezu wortgleich der Definition der elektronischen Kommunikationsdienste (ESC) in Art. 2 lit. c) der Rahmenrichtlinie. Telekommunikationsdienste im Sinne der §§ 6, 3 Nr. 24 TKG würden daher maßgeblich durch zwei Merkmale gekennzeichnet, nämlich zunächst durch die regelmäßige Entgeltlichkeit der Dienste und des Weiteren durch einen Dienst, der zumindest überwiegend in einer Signalübertragung über Telekommunikationsnetze bestehen muss. Obwohl Google selbst die Signale nicht übertrage, sei Google die Signalübertragungsleistung der Internetzugangsanbieter zurechenbar, weil Google sich diese Signalübertragungsleistung für ihre Zwecke faktisch zu eigen mache und insbesondere mit ihren informationstechnischen Verarbeitungsleistungen selbst einen entscheidenden Beitrag für das Funktionieren des Telekommunikationsvorgangs erbringe. Für die Frage, ob ein Dienst ganz oder überwiegend in der Übertragung von Signalen bestehe, sei keine rein technische Betrachtung vorzunehmen, denn die Signalübertragungsleistung bilde den Schwerpunkt des E-Mail-Dienstes Gmail. Bei einer wertenden Betrachtung stünden die raumüberwindende Kommunikation mit anderen Nutzern und damit der Telekommunikationsvorgang selbst im Vordergrund, während andere inhaltsbezogene Komponenten des Dienstes keine eigenständige Bedeutung hätten.

b) Das Urteil des Europäischen Gerichtshofs vom 13. Juni 2019

Mit dem Urteil des Europäischen Gerichtshofs vom 13. Juni 2019 in der Rechtssache C-193/18[12] im Rahmen einer Vorlage zur Vorabentscheidung durch das Oberverwaltungsgericht für das Land Nordrhein-Westfalen wurde die Auffassung des Verwaltungsgereichts Köln jedoch nicht bestätigt.

[12] EuGH, Urteil vom 13.06.2019 - C-193/18
http://curia.europa.eu/juris/document/document.jsf?docid=214944&doclang=de

Denn unabhängig davon, dass der Erbringer eines internetbasierten E-Mail-Dienstes wie Gmail bei der Erbringung seines E-Mail-Dienstes von Inhabern eines GoogleMail-Kontos versendete und von ihnen empfangene, in Datenpakete zerlegte E-Mails über eigene E-Mail-Server in das offene Internet einspeise und aus diesem empfange und damit eine Übertragung von Signalen vornehme, sei dieser nicht als „elektronischer Kommunikationsdienst“ einzuordnen, da dieser Dienst nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestünde.

Denn es seien einerseits die Internetzugangsanbieter, der Absender und der Empfänger von E-Mails sowie die Anbieter von internetbasierten E-Mail-Diensten und andererseits die Betreiber der verschiedenen Netzen, aus denen das offene Internet besteht, für die Übertragung der für das Funktionieren jedes internetbasierten E-Mail-Dienstes erforderlichen Signale verantwortlich.

Dass der Erbringer eines internetbasierten E-Mail-Dienstes bei der Versendung und dem Empfang von Nachrichten aktiv tätig werde, sei es, indem er den E-Mail-Adressen die IP-Adressen der entsprechenden Endgeräte zuordnet oder die Nachrichten in Datenpakete zerlegt und sie in das offene Internet einspeist oder aus dem offenen Internet empfängt, damit sie ihren Empfängern zugeleitet werden, reiche nicht aus für die Einstufung dieses Dienstes als im Sinne von Art. 2 lit. c der Rahmenrichtlinie „ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze“. Daher könne insofern auch nicht von einem Telekommunikationsdienst im Sinne des § 6 TKG gesprochen werden.

Daraus ergibt sich, dass bei Telemediendiensten wie E-Mail-Kommunikation oder Livechats, die eben nicht ganz überwiegend oder ausschließlich die Übertragung von Signalen bedeuten, ein Auskunftsverlangen nicht mit § 100g StPO begründet werden kann, weil über Telemediendienste begangene Straftaten insoweit nicht erfasst werden und eine Auskunft wegen des insoweit zu beachtenden Bestimmtheitsgebots nicht in Betracht kommt.

Insoweit ist nunmehr geplant, durch die Erweiterung von § 100g StPO auf Nutzungsdaten nach § 15 Absatz 1 des Telemediengesetzes eine Rechtsgrundlage auch für die Erhebung von Metadaten bei Telemediendiensteanbietern zu schaffen, soweit die Telemedien geschäftsmäßig angeboten werden.

Weil im Telemediengesetz Regelungen zur Auskunft anhand von IP-Adressen und der Abfrage von Passwörtern fehlen, soll der neue § 15a TMG auch für die Abfrage von Passworten gelten und seinen Niederschlag in § 100g Absatz 1 Satz 2 StPO finden.

Nach dem Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz sollten daher folgende gesetzliche Änderungen erfolgen

In der Inhaltsübersicht wird die Angabe zu § 100g wie folgt gefasst:

„§ 100g Erhebung von Verkehrs- und Nutzungsdaten".

2. § 100g wird wie folgt geändert:

a) Die Überschrift wird wie folgt gefasst: „§ 100g Erhebung von Verkehrs- und Nutzungsdaten"

b) Absatz 1 wird wie folgt geändert:

aa) Nach Satz 1 wird folgender Satz eingefügt:

„Unter den Voraussetzungen des Satzes 1 dürfen von denjenigen, die geschäftsmäßig eigene oder fremde Telemedien zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln, Nutzungsdaten (§ 15 Absatz 1 des Telemediengesetzes) erhoben werden."

bb) In dem neuen Satz 5 werden nach dem Wort „Verkehrsdaten" die Wörter „und

Nutzungsdaten" eingefügt.

c) In Absatz 5 werden nach dem Wort „Telekommunikationsdienste" die Wörter „oder bei einem Diensteanbieter, der geschäftsmäßig Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt" eingefügt.

2. Die Einführung des § 15a TMG

Kern der Maßnahmen zur Identifizierung bei Hasskriminalität im Netz und der Strafbarkeit von Cyber-Stalking, Hetze und aggressiver Beleidigung stellt der neue § 15 a TMG dar:

„§ 15a

Auskunftsverfahren

(1) Wer geschäftsmäßig Telemediendienste erbringt, daran mitwirkt oder den Zugang zu Nutzung daran vermittelt, darf die nach § 14 Absatz 1 erhobenen Bestandsdaten und die nach § 15 Absatz 1 erhobenen Nutzungsdaten nach Maßgabe dieser Vorschrift zur Erfüllung von Auskunftspflichten gegenüber den in Absatz 3 genannten Stellen verwenden. Dies gilt auch für Bestandsdaten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird. Die in eine Auskunft aufzunehmenden Bestandsdaten, dürfen auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse bestimmt werden; hierfür dürfen Nutzungsdaten auch automatisiert ausgewertet werden. Für die Auskunftserteilung sind sämtliche unternehmensinternen Datenquellen zu berücksichtigen.

(2) Die Auskunft darf nur erteilt werden, soweit eine in Absatz 3 genannte Stelle dies unter Angabe einer gesetzlichen Bestimmung, die ihr eine Erhebung der in Absatz 1 in Bezug genommenen Daten erlaubt, in Textform im Einzelfall verlangt und dies zu einem der folgenden Zwecke erforderlich ist:

1. zur Verfolgung von Straftaten oder Ordnungswidrigkeiten,

2. zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder

3. für die Erfüllung der gesetzlichen Aufgaben der in Absatz 3 Nummer 3 und 4 genannten Stellen.

An andere öffentliche und nichtöffentliche Stellen dürfen Daten nach Absatz 1 nicht übermittelt werden. Bei Gefahr im Verzug darf die Auskunft auch erteilt werden, wenn das Verlangen nicht in Textform gestellt wird. In diesem Fall ist das Verlangen unverzüglich nachträglich in Textform zu bestätigen. Die Verantwortung für die Zulässigkeit des Auskunftsverlangens tragen die um Auskunft ersuchenden Stellen.

(3) Stellen im Sinne des Absatzes 1 sind

1. die für die Verfolgung von Straftaten oder Ordnungswidrigkeiten zuständigen Behörden;

2. die für die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung zuständigen Behörden;

3. die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst und der Bundesnachrichtendienst;

4. die Behörden der Zollverwaltung und die nach Landesrecht zuständigen Behörden, soweit die Datenerhebung zur Wahrnehmung ihrer Prüfungsaufgaben nach §

2 Absatz 1 und 3 des Schwarzarbeitsbekämpfungsgesetzes und für die Verhütung und Verfolgung von damit zusammenhängenden Straftaten und Ordnungswidrigkeiten erforderlich ist.

(4) Derjenige, der geschäftsmäßig Telemediendienste erbringt, daran mitwirkt o- der den Zugang zur Nutzung daran vermittelt, hat die zu beauskunftenden Daten unverzüglich und vollständig zu übermitteln. Über das Auskunftsersuchen und die Auskunftserteilung haben die Verpflichteten gegenüber den Betroffenen sowie Dritten Stillschweigen zu wahren.

(5) Wer geschäftsmäßig Telemediendienste erbringt oder daran mitwirkt, hat die in seinem Verantwortungsbereich für die Auskunftserteilung erforderlichen Vorkehrungen auf seine Kosten zu treffen. Wer mehr als 100 000 Kunden hat, hat für die Entgegennahme der Auskunftsverlangen sowie für die Erteilung der zugehörigen Auskünfte eine gesicherte elektronische Schnittstelle bereitzuhalten, die auch die gegen Kenntnisnahme der Daten durch Unbefugte gesicherte Übertragung gewährleistet. Jedes Auskunftsverlangen ist durch eine verantwortliche Fachkraft auf Einhaltung der in Absatz 2 genannten formalen Voraussetzungen zu prüfen und die weitere Bearbeitung des Verlangens darf erst nach einem positiven Prüfergebnis freigegeben werden.“

Der für den gewöhnlichen Internetnutzer bedeutsame Passus des neuen 15 a TMG, hinter dem sich die Möglichkeit der Abfrage bzw. Herausgabe des Passworts verbirgt lautet:

Dies (Anmerkung des Verfassers: die Erfüllung von Auskunftspflichten) gilt auch für Bestandsdaten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird. Die in eine Auskunft aufzunehmenden Bestandsdaten, dürfen auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse bestimmt werden.

Wenn also bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine

Straftat vorbereitet hat oder eine Straftat mittels **T**elekommunikation begangen hat, sollen In Zukunft von Telemediendiensten wir Google oder Facebook auch Bestandsdaten erhoben werden können, mit denen der Internetnutzer über sein Endgerät Zugriff auf seinen Speicherplatz bei Google oder Facebook erhält.

Das Gesetz selbst vermeidet den Begriff Passwort, allerdings ist der Referentenentwurf insoweit hinreichend deutlich, wonach die Regelung des 15 a TMG „ausdrücklich auch auf Passwörter erstreckt“ wird.

Von Rechtsextremismus, Antisemitismus und Hasskriminalität ist in dem Gesetzentwurf des Bundesministeriums der Justiz und für Verbraucherschutz als Voraussetzung für die Auskunftserteilung von Passwörtern und IP-Adressen durch die Telemediendienste nicht mehr die Rede.

Ab 100 000 Kunden sollen die für die Erteilung der zugehörigen Auskünfte sogar eine gesicherte elektronische Schnittstelle bereithalten. Welche Qualifikation eine Fachkraft haben muss, welche die Auskunftsverlangen dahingehend überprüft, ob die gesetzlichen Voraussetzungen für eine Auskunft vorliegen, wird ebenfalls nicht gesagt.

3. Die Einführung des § 3a NetzDG

Ein weiterer wichtiger Baustein für die Identifizierung verdächtiger Nutzer bei Verdacht von Hasskriminalität im Internet und der Strafbarkeit von Cyber-Stalking, Hetze und aggressiver Beleidigung ist die Einführung des neuen § 3a im Netzwerkdurchsetzungsgesetz vom 1. September 2017, der nunmehr eine Meldepflicht der sozialen Netzwerke vorsieht, um für die Strafverfolgungsbehörden ohne größeren technischen Aufwand Daten zum Zwecke der Identifizierung eines Nutzers wie IP-Adresse einschließlich der Portnummer zu erhalten, da diese vom Betreiber eines sozialen Netzwerks elektronisch an eine vom Bundeskriminalamt zur Verfügung gestellte Schnittstelle zu übermitteln sind. Die Meldepflicht soll wie folgt ausgestattet sein:

§ 3a Netzwerkdurchsetzungsgesetz

Meldepflicht

(1) Der Anbieter eines sozialen Netzwerks muss ein wirksames Verfahren für Meldungen nach den Absätzen 2 bis 5 vorhalten.

(2) Der Anbieter eines sozialen Netzwerks muss dem Bundeskriminalamt als Zentralstelle zum Zwecke der Ermöglichung der Verfolgung von Straftaten Inhalte übermitteln,

1. die dem Anbieter in einer Beschwerde über rechtswidrige Inhalte gemeldet worden sind,

2. die der Anbieter entfernt oder zu denen er den Zugang gesperrt hat und

3. bei denen konkrete Anhaltspunkte dafür bestehen, dass sie mindestens einen der

Tatbestände

a) der §§ 86, 86a, 89a, 91, 126, 129 bis 129b, 130, 131 oder 140 des Strafgesetzbuches,

b) des § 184b in Verbindung mit § 184d des Strafgesetzbuches oder

c) des § 241 des Strafgesetzbuches in Form der Bedrohung mit einem Tötungsdelikt (§§ 211 oder 212 des Strafgesetzbuches)

erfüllen und nicht gerechtfertigt sind.

(3) Der Anbieter des sozialen Netzwerks muss unverzüglich, nachdem er einen Inhalt entfernt oder den Zugang zu diesem gesperrt hat, prüfen, ob die Voraussetzungen des Absatzes 2 Nummer 3 vorliegen, und unverzüglich danach den Inhalt gemäß Absatz 4 übermitteln.

(4) Die Übermittlung an das Bundeskriminalamt muss

1. den Inhalt und,

2. sofern vorhanden, die IP-Adresse einschließlich der Portnummer, die der Nutzer verwendet hat, als er den Inhalt mit anderen Nutzern geteilt oder der Öffentlichkeit zugänglich gemacht hat, enthalten.

(5) Die Übermittlung an das Bundeskriminalamt hat elektronisch an eine vom Bundeskriminalamt zur Verfügung gestellte Schnittstelle zu erfolgen.

(6) Der Anbieter des sozialen Netzwerks informiert den Nutzer, für den der Inhalt gespeichert wurde, 14 Tage nach der Übermittlung an das Bundeskriminalamt über die Übermittlung nach Absatz 4 Satz 1 gilt nicht, wenn das Bundeskriminalamt binnen 14 Tagen anordnet, dass die Information wegen der Gefährdung des Untersuchungs-

zwecks, des Lebens, der körperlichen Unversehrtheit oder der persönlichen Freiheit einer Person oder von bedeutenden Vermögenswerten zurückzustellen ist. Im Fall der Anordnung nach Satz 2 informiert das Bundeskriminalamt den Nutzer über die Übermittlung nach Absatz 4, sobald dies ohne Gefährdung im Sinne des Satzes 2 möglich ist.

(7) Der Anbieter eines sozialen Netzwerks hat der in § 4 genannten Verwaltungsbehörde auf deren Verlangen Auskünfte darüber zu erteilen, wie die Verfahren zur Übermittlung von Inhalten nach Absatz 1 gestaltet sind und wie sie angewendet werden."

IV. Kritik

Es scheint, als ob mit den in den vorgesehenen Gesetzesänderungen weich umschriebenen Voraussetzungen lediglich des Verdachts einer „Straftat von auch im Einzelfall erheblicher Bedeutung", „konkrete Anhaltspunkte" oder „Beschwerde über rechtswidrige Inhalte" für die Ermittlung bzw. Herausgabe eines Passworts mit der dazugehörigen IP-Adresse das Tor zu den Konten zahlreicher Internetnutzer geöffnet werden soll. Ein Verdacht ist schließlich schnell ausgesprochen, konkrete Anhaltspunkte sind fast immer zu finden und die schlichte, von Jedermann zu erhebende Beschwerde über angeblich aber möglicherweise im Ergebnis nicht rechtswidrige Inhalte, ist gar vollkommen beliebig. Dementsprechend regt sich Widerspruch im Parlament und der einschlägigen Fachwelt.

Nach Ansicht des Nachrichtendienstes „heise online" will die Regierung *„nicht nur das an sich bereits heftig umstrittene Netzwerkdurchsetzungsgesetz (NetzDG) deutlich verschärfen. Sie plant auch eine Pflicht für WhatsApp, Gmail, Facebook, Tinder & Co., schon jedem Dorfpolizisten und zahlreichen weiteren Sicherheitsbehörden auf Anfrage sensible Daten von Verdächtigen wie Passwörter oder IP-Adressen teils ohne Richterbeschluss herauszugeben."*[13]

„Mit ihrem undurchdachten Versuch, das Problem rechter Hetze und Gewalt in den Griff zu bekommen, schießt die Regierung weit über das eigentliche Ziel hinaus.

[13] „Justizministerium: WhatsApp, Gmail & Co. sollen Passwörter herausgeben müssen" https://www.heise.de/newsticker/meldung/Justizministerium-WhatsApp-Gmail-Co-sollen-Passwoerter-herausgeben-muessen-4615602.html

Selbstverständlich muss die Strafverfolgung von Hasskriminalität möglich sein, doch panisches Horten von Daten schützt weder vor Rechten noch vor Hass. Und so drängt sich der Eindruck auf, dass erneut ein konkreter Anlass dazu genutzt werden soll, allgemeine Zugriffsrechte auf sensible Daten durchzusetzen.“[14]

Der Informationsdienst „golem.de“ zitiert Bitkom-Hauptgeschäftsführer Bernhard Rohleder, wonach das geplante Gesetz Grundwerte über Bord werfe, *„die unser Zusammenleben online wie offline seit Jahrzehnten prägen"* Es sei hochproblematisch, dass die Polizei künftig auf einfaches Ersuchen hin die Nutzerpasswörter von allen Telemediendiensteanbietern verlangen kann. Dazu genügt die Aufforderung einer Behörde oder Polizeidienststelle, ein richterlicher Beschluss ist nicht nötig."[15]

Das Tech-Portal „BASIC thinking“ bemängelt, dass sich die neue Rechtsgrundlage in einem Gesetzentwurf zur Bekämpfung des Rechtsextremismus und der Hasskriminalität befindet. *„Damit sollen soziale Medien wie Facebook oder Twitter verpflichtet werden, offensichtlich rechtswidrige Inhalte nicht nur zu löschen, sondern auch den Behörden zu melden. Die geplanten Änderungen beim Telemediengesetz (TMG) beziehen sich aber nicht nur auf Rechtsextremismus und Hasskrimininalität, sondern allgemein auf "Verfolgung von Straftaten oder Ordnungswidrigkeiten" oder "Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung.“*[16]

Nach Ansicht der FAZ werfe der Gesetzentwurf Fragen auf und zitiert Renate Künast, Abgeordnete von Bündnis90/Die Grünen im Bundestag: *„Soll hier unter dem Deckmantel der Bekämpfung von Rechtsextremismus nun von den Sicherheitsbehörden Zugang zu Informationen erlangt werden, die man immer schon wollte?“* und *„Wir brauchen jetzt eine sehr präzise und seriöse Beratung des Gesetzes*

[14] „Datenweitergabe torpediert die Privatsphäre“
https://www.heise.de/newsticker/meldung/Gastbeitrag-Datenweitergabe-torpediert-die-Privatsphaere-4621379.html
[15] „Ermittler sollen leichter an Passwörter kommen“
https://www.golem.de/news/internetdienste-ermittler-sollen-leichter-an-passwoerter-kommen-1912-145549.html
[16] „Dürfen Behörden bald ohne richterlichen Beschluss unsere Passwörter einholen?“
https://www.basicthinking.de/blog/2019/12/18/gesetzentwurf-behoerden-passwoerter-zugriff/

im Bundestag, sonst landet es sowieso in Karlsruhe und wird dort sicherlich aufgehoben.“[17]

Die Süddeutsche Zeitung fragt sich, wie die IT-Unternehmen auf solche Anfragen von Polizisten oder Geheimdienstlern reagieren werden: *„Die Passwörter, um die es geht, werden bei den Unternehmen in der Regel gar nicht im Klartext gespeichert. Aus dem Google-Konzern heißt es deshalb, Passwörter zum Beispiel für Online-Cloud-Dienste wie Google Drive oder die Online-Backups könne man den Sicherheitsbehörden gar nicht herausgeben. Der Konzern speichere sie nur verschlüsselt.“*[18]

V. Fazit

Mit der Ausbreitung sozialer Netzwerke im Internet hat sich die Massenkommunikation auch in Deutschland verändert. Die überwiegende Mehrheit der deutschen Bevölkerung hat durch Computer und Mobiltelefon Zugang zu den sozialen Netzwerken und ist in der Lage, ohne technischen Aufwand seine Meinung durch Kommentare zu tagesaktuellen Ereignissen abzugeben und zu verbreiten. Auch wenn sich Medienwissenschaftler einig sind, dass die sozialen Netzwerke die klassischen Medien zunächst nicht verdrängen werden,[19] ist die Möglichkeit der Interaktion für den Konsumenten von Nachrichten sehr viel größer geworden und diese Möglichkeiten werden auch intensiv genutzt. Diese Situation ist auch für die deutsche Politik ein Novum, die Entscheidungsprozesse werden transparenter, die Kritik daran erfolgt weltweit rund um die Uhr.

Die deutsche Politik ist dem Umstand, dass nahezu jeder Bundesbürger über die Möglichkeit verfügt, seine Meinung 24 Stunden pro Tag auf der ganzen Welt zu verbreiten, bereits im Jahre 2017 mit dem Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG) begegnet, um über die

[17] GESETZ GEGEN HASSREDE: Bundesregierung will an E-Mail-Passwörter https://www.faz.net/aktuell/wirtschaft/digitec/kampf-gegen-hassrede-bundesregierung-will-an-e-mail-passwoerter-16535665.html

[18] Gesetzespaket gegen Hasskriminalität: Regierung will Ermittlern Zugriff auf Online-Passwörter ermöglichen https://www.sueddeutsche.de/digital/hatespeech-hassrede-passwort-email-social-media-drohung-beleidigung-1.4724108

[19] Funktionswandel der Massenmedien durch das Internet? Von Ekkehardt Oehmichen* und Christian Schröter** http://www.ard-zdf-onlinestudie.de/files/2003/Online03_Ver_nderung.pdf

Ermittlungsbehörden und Gerichte größeren Einfluss auf die geäußerten Meinungen zu erlangen.

In offiziellen Verlautbarungen dient bereits das am 01. Oktober 2017 in Kraft getretene Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) nur dem Zweck, bereits bestehendes Recht einzuhalten und durchzusetzen.[20]

Nach den Worten der Bundesregierung seien Debatten in sozialen Netzwerken oft aggressiv, verletzend und hasserfüllt und gefährden „das friedliche Zusammenleben einer freien, offenen und demokratischen Gesellschaft."[21]

Knapp zwei Jahre später scheint die Bundesregierung die Debatten der Bürger in den sozialen Netzwerken immer noch nicht ausreichend unter Kontrolle zu haben und versucht dies nun mit einer neuen Gesetzesinitiative zu ändern.

Die Begründung für die Verschärfung der Gesetze ist nun nicht mehr allgemeiner Natur, wie dies bei der Einführung des Netzwerkdurchsetzungsgesetzes der Fall war, sondern beinhaltet den Hinweis auf Rechtsextremismus und Antisemitismus und nimmt konkret Bezug auf die Ermordung des Kasseler Regierungspräsidenten Walter Lübcke und die Ermordung zweier Menschen im Rahmen des Attentats auf die Synagoge in Halle.

Es wird damit deutlich, dass in der Regierung seit der Verbreitung der Meinungen von Bürgern über soziale Netzwerke und die über Kommentare auszulesende Stimmung im Volk große Unsicherheit in der Politik herrscht. Wie gewohnt wird auch hier bei geäußerter Kritik an der Politik nicht mit einer Änderung der Politik reagiert, sondern mit einer Beschneidung der Möglichkeiten für Bürger, Kritik äußern zu können. Die bereits von Gegnern des Netzwerkdurchsetzungsgesetzes befürchteten „katastrophalen Folgen für die Meinungsfreiheit"[22], da die Aufgaben der Polizei und Staatsanwaltschaft auf Mitarbeiter der sozialen Netzwerke abgewälzt würden, die im

[20] Fair im Netz: Startschuss für die Rechtsdurchsetzung in sozialen Netzwerken. Bundesministerium für Justiz und Verbraucherschutz, 18. September 2017;
https://web.archive.org/web/20171102171222/https://www.bmjv.de/SharedDocs/Artikel/DE/2017/091817_Rechtsdurchsetzung_in_sozialen_Netzwerken.html

[21] Deutscher Bundestag Drucksache 18/12727 vom 14.06.2017
http://dipbt.bundestag.de/doc/btd/18/127/1812727.pdf

[22] Patrick Beuth: Heiko Maas: Breites Bündnis gegen das Facebookgesetz. In: Die Zeit, 11.April 2017,
http://www.zeit.de/digital/internet/2017-04/heiko-maas-netzdg-allianz-meinungsfreiheit

Zweifel nicht einmal über eine juristische Ausbildung verfügen und damit ein „Angriff auf das Prinzip der Gewaltenteilung“[23] erfolge, scheinen unausweichlich.

Insoweit dürften die am Anfang geschilderten Mordfälle mit rechtsextremem Hintergrund nur ein willkommener Anlass für die Regierung zu sein, unter dem Deckmantel der Bekämpfung des Rechtsextremismus die Möglichkeiten der Bürger, ihre Meinung frei zu äußern, geschickt zu verringern. Durch die Übertragung von Auskunfts-, Lösch- und Meldepflichten an die Betreiber sozialer Netzwerke scheint zunächst die Taktik verfolgt zu werden, sich als Staat nicht unmittelbar selbst als Initiator von Meldungen und Löschungen präsentieren zu müssen. Zum anderen haben die oben beschriebenen Gesetzesverschärfungen zur Folge, dass ein beachtlicher Anteil von Äußerungen zusätzlich unter Strafe gestellt und somit die Bandbreite zulässiger Äußerungen weiter eingeengt wird. Durch die Übertragung zahlreicher Pflichten an die sozialen Netzwerke ohne die Qualifizierung des dafür zuständigen Personals zu beschreiben, scheint der Gesetzgeber zu versuchen, den Bestand tatsächlich strafloser Äußerungen zu minimieren, da unqualifiziertes Personal angesichts drohender Bußgelder im Interesse der eigenen Arbeitgeber eher dazu neigen wird, Kommentare, die ungehörig aber zulässig sind, zu löschen und im Zweifel den Verfasser nebst identifizierender Daten an die Strafverfolgungsbehörden zu melden. Insbesondere der Umstand, dass sich die Handlungspflichten der Betreiber sozialer Netzwerke nicht auf Kommentare beschränken, die dem rechtsextremen Spektrum zuzuordnen sind, zeigt, dass ein großflächiger Angriff auf die Meinungsfreiheit im Internet erfolgen könnte. Zutreffend wird allerdings die Zielgruppe für den verschärften gesetzlichen Schutz im Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz genannt, die sich der ungebremsten Kritik im Internet ausgesetzt sieht: Für das Gemeinwesen aktive und daher in der Öffentlichkeit stehende Repräsentanten des Volks, allgemein auch „Politiker“ genannt. Der Bürger erfährt in der Regel schon lange und auch ohne Gesetzesverschärfung kaum Schutz durch die Strafverfolgungsbehörden bei unzulässigen Meinungsäußerungen im Internet, denn die längst überlasteten Staatsanwaltschaften stellen bei derartigen Delikten die Verfahren mit Internetbezug mit der Behauptung mangelnden öffentlichen Interesses überwiegend ein.

[23] Harald Martenstein: Erdoganismus in Reinkultur. In: Tagesspiegel, 19. März 2017, http://www.tagesspiegel.de/politik/gesetzentwurf-von-heiko-maas-erdoganismus-in-reinkultur/19537970.html