Auf einen Blick

Gesetz zur Bekämpfung der Hasskriminalität im Netz

Ausgangslage

Am 30.10.2019 hat die Bundesregierung ein Maßnahmenpaket zur Bekämpfung von Rechtsextremismus und Hasskriminalität verabschiedet, welches unter anderem die Verbesserung der Identifizierung bei Hasskriminalität im Netz vorsieht. Das Bundesjustizministerium hat am 18.12.2019 einen Referentenentwurf vorgelegt, welcher der Umsetzung einiger Punkte des Maßnahmenpakets dienen soll und hierzu unter anderem Änderungen des Telemediengesetzes (TMG) und des Netzwerkdurchsetzungsgesetzes (NetzDG) vorsieht.

Bitkom-Bewertung

Es ist kompliziert: Der Referentenentwurf verfolgt mit der Verbesserung der Strafverfolgung im Netz ein wichtiges Ziel, welches unsere volle Unterstützung findet. Viele der vorgeschlagenen Neuerungen sind aber entweder aus politischen Erwägungen – z.B. mit Blick auf die Einhaltung bürgerlicher Grundrechte – oder wegen rechtlicher Unklarheiten problematisch – und das bei zweifelhaftem Nutzen. **Unser Ziel ist** eine Verbesserung der Strafverfolgung im Netz – durch effizientere, verhältnismäßigere und internationalere Maßnahmen als hier vorgesehen.

Das Wichtigste

- **Keine Verpflichtung zur proaktiven Ausleitung von Daten**
  Der Entwurf der Meldepflicht für soziale Netzwerke im NetzDG ist ein Systembruch: Strafverfolgung ist ureigene staatliche Aufgabe. Gleichzeitig sollen nutzerbezogene Daten ohne staatliche Abfrage proaktiv Ermittlungsbehörden zugeleitet werden. Das bisher bestehende System würde damit faktisch „umgedreht“ – und das lehnen wir ab. Diese Art der „Verdachts-Datei“ beim BKA, die auf Rechtsbewertungen privater Unternehmen basiert, birgt die Gefahr von Grundrechtsverletzungen.
- **Rechtliche Unklarheiten bei Auskunftsverfahren zur Datenweitergabe**
  Laut dem Entwurf für das TMG sollen jegliche Anbieter von Telemedien den Ermittlungsbehörden künftig auch Daten wie z.B. Passwörter, IP-Adressen usw. zuleiten, wenn sie angefragt werden. Dieses Auskunftsverfahren wirft viele Fragen auf, z.B. unter welchen Bedingungen solche Anfragen gestellt werden dürfen, ob ein Richter zustimmen muss und wie die TMG-Änderung mit anderen Befugnis-Normen wie z.B. Landespolizeigesetzen zusammenwirkt.

Stellungnahme

Zum Referentenentwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität

17. Januar 2020

Am 1. Oktober 2017 ist das Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) in Kraft getreten. Im entsprechenden Gesetzestext ist eine Evaluierung nach spätestens 3 Jahren nach Inkrafttreten des Gesetzes, also bis Oktober 2020, vorgesehen: „Dabei wird die Bundesregierung in fachlich geeigneter Weise prüfen, ob und inwieweit die beabsichtigten Wirkungen auf die sozialen Netzwerke mit Blick auf ihren Umgang mit Beschwerden über Hasskriminalität und andere strafbare Inhalte erreicht worden sind. Die Bundesregierung wird ferner untersuchen, wie sich der Erfüllungsaufwand für Wirtschaft und Verwaltung entwickelt hat und ob die Entwicklung in einem angemessenen Verhältnis zu den festgestellten Regelungswirkungen steht. Die Evaluierung wird die Frage nach unbeabsichtigten Nebenwirkungen sowie nach der Akzeptanz und Praktikabilität der Regelungen einschließen“.

Am 30.10.2019 hat die Bundesregierung ihr Maßnahmenpaket zur Bekämpfung von Rechtsextremismus und Hasskriminalität verabschiedet. Die ersten beiden Punkte dieses Maßnahmenpakets betreffen die Digitalwirtschaft: Zum einen soll die Identifizierung bei Hasskriminalität im Netz verbessert werden. Hierzu soll eine Meldepflicht nach dem NetzDG eingeführt werden, welche die Diensteanbieter dazu verpflichtet, relevante Inhalte und IP-Adresse und Portnummer des hochladenden Nutzers einer neu zu errichtenden Zentralstelle im Bundeskriminalamt (BKA) mitzuteilen. Außerdem soll im BKA Gesetz und in der StPO eine Auskunftsbefugnis gegenüber den Diensteanbietern geschaffen werden, damit die dort noch vorhandenen Daten zu strafrechtlich relevanter Hasskriminalität herausverlangt werden können. Zum anderen soll die Strafbarkeit von Beleidigungen an die Besonderheiten des Netzes angepasst werden.

Das Bundesministerium für Justiz und Verbraucherschutz hat am 18.12.2019 einen Referentenentwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität vorgelegt, welcher die ersten beiden Punkte des Maßnahmenpakets umsetzen soll und Änderungen des Strafgesetzbuchs, der Strafprozessordnung (StPO), der Bundeskriminalamtsgesetzes, des Telemediengesetzes (TMG) und des NetzDGs beinhaltet. Bitkom begrüßt die Initiative für eine effizientere Strafverfolgung im digitalen Raum und bedankt sich für die Gelegenheit, zu den konkreten Vorschlägen Stellung zu nehmen.

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Nick Kriegeskotte
Leiter Infrastruktur & Regulierung
T +49 30 27576-224
n.kriegeskotte@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

1. Zur zeitlichen Abfolge des Gesetzgebungsverfahrens

Grundsätzlich stellt sich in Anbetracht der geplanten Änderungen am NetzDG die Frage, wie weit die Evaluierung des geltenden Gesetzes durch die Bundesregierung bereits fortgeschritten ist. Entsprechende Fragebögen zur Evaluierung des Gesetzes sind im Herbst 2019 an die Unternehmen versandt worden, die das NetzDG befolgen müssen. Eine Änderung und Erweiterung bzw. Verschärfung des Gesetzes vor Abschluss der Evaluierung, die nun ohnehin stattfinden muss, deutet, wie bereits bei der Entstehung des Gesetzes, auf einen erneut übereilten Vorstoß hin, der der komplexen Problemlage nicht gerecht wird. Das erzeugt außerdem den Eindruck, dass es nicht darum geht, die Wirkungen und Nebenwirkungen des NetzDG nun aufzuarbeiten und das Gesetz wirklich nachzubessern.

2. Zur Verantwortung der Diensteanbieter

Die Bundesregierung möchte mit den vorgeschlagenen Regelungen die Rechtsdurchsetzung im Internet verbessern. Dieses wichtige Ziel anerkennen und unterstützen wir. Bitkom tritt ausdrücklich dafür ein, dass die Verbreitung von rechtswidrigen und erst Recht strafbaren Inhalten in sozialen Netzwerken bestmöglich bekämpft und tatsächliche Straftaten im Internet konsequent verfolgt und geahndet werden. Hierbei tragen selbstverständlich auch Diensteanbieter wie soziale Netzwerke Verantwortung. Dieser Verantwortung stellen sich die sozialen Netzwerke unter den Bitkom Mitgliedern ausdrücklich.

Das Internet ist kein rechtsfreier Raum. Es gibt etablierte Verfahren und Prozesse für Strafverfolgungsbehörden um Informationen abzufragen, insbesondere für im Inland ansässige Anbieter, aber auch für Anbieter mit Sitz in einem anderen Land. In Teilen wird jedoch der Funktionsweise von Online-Plattformen und den rechtlichen Grundlagen, auf denen diese operieren, nicht ausreichend Rechnung getragen. Diese Verfahren sind nicht mehr zeitgemäß und zu langwierig. Das Verfahren bspw. nach Rechtshilfeabkommen (MLATs (Mutual Legal Assistance Treaties)) kann bis zu einem Jahr dauern – dann sind die IP-Adressen, die die Strafverfolgung anfordert, schon nicht mehr gespeichert – das System funktioniert also nicht zufriedenstellend. Viele der im Bitkom organisierten Unternehmen gehen deshalb bereits heute über das gesetzlich vorgeschriebene Maß der Verpflichtungen hinaus, und zwar durch eine freiwillige Beauskunftung von Daten auf Anfrage seitens der Strafverfolgungsbehörden jenseits von Verfahren wie MLAT. Die Transparenzberichte der Anbieter geben Auskunft über die steigende Anzahl von Informationsanfragen der

Strafverfolgungsbehörden. Doch insbesondere bei diesen freiwilligen Maßnahmen müssen Unternehmen Mindeststandards berücksichtigen, die für die Anfragen erfüllt sein müssen, um nicht am unter Umständen von Deutschland abweichenden Heimatstandort für eine widerrechtliche Datenherausgabe zu haften.

Die technischen law-enforcement Potale, die einige Anbieter bereits freiwillig für die Abwicklung von Auskunftsanfragen eingerichtet haben, über die die Behörden schnell, effektiv und vor allem sicher und verschlüsselt Daten anfragen können, haben sich bewährt und sollten fortbestehen können ungeachtet der anvisierten Gesetzesänderung.

Außerdem verfolgen einige Bundesländer in Deutschland Projekte, in denen Medienunternehmen, Medienanstalten, Strafverfolgungsbehörden und teilweise auch NGOs zusammenarbeiten, um gemeinsam die Strafverfolgung im Bereich Hasskriminalität zu verbessern. „Verfolgen statt nur Löschen“ in NRW ist ein gutes Beispiel, wie dies funktionieren kann. Bitkom und seine Mitgliedsunternehmen begrüßen und unterstützen diese Projekte aktiv - nur durch einen derartigen Multi-Stakeholder Ansatz können zum einen prozessuale Barrieren identifiziert und überwunden und zum anderen eine umfassende Strafverfolgung gewährleistet werden.

Bei der Frage nach einer den rechtsstaatlichen Erfordernissen entsprechenden Aufgabenverteilung und Verantwortungsaufteilung zwischen Behörden und Gerichten einerseits und privatwirtschaftlichen Unternehmen andererseits kommt Bitkom zu anderen Ergebnissen, als sie im jetzt vorgelegten Entwurf Ausdruck finden. Auslegung und Durchsetzung geltenden Rechts sind in Deutschland grundsätzlich Aufgaben von Behörden und Gerichten. Das gilt insbesondere für die Strafverfolgung. Diese Aufgaben sollten nicht privatwirtschaftlichen Unternehmen überlassen werden. Bitkom unterstützt ausdrücklich, dass die Betreiber sozialer Netzwerke bei der Rechtsdurchsetzung angemessenen mit den Behörden zusammenarbeiten. So stellen die sozialen Netzwerke auf freiwilliger Basis den Behörden nach Empfang eines gültigen Auskunfts-oder Rechtshilfeverfahrens Nutzerdaten über die Urheber der mutmaßlich illegalen Beiträge zur Verfügung, sofern dies nicht im Widerspruch zu anderen gültigen Gesetzen (wie zum Beispiel dem Völkerrecht) steht. Die im Bitkom organisierten Unternehmen möchten ihre Offenheit für ein gemeinsames Erarbeiten von Vorschlägen ausdrücken, die die Zusammenarbeit zwischen den Unternehmen einerseits und den Strafverfolgungsbehörden und Gerichten andererseits verbessern.

Abgesehen von diesen Bedenken besteht die Gefahr, dass andere Staaten, in denen das Prinzip der Rechtsstaatlichkeit weniger stark ausgeprägt ist als in Deutschland, ähnliches von den Unternehmen verlangen um die Daten der Verfasser von aus Sicht der jeweiligen Regierung unliebsamen Beiträgen zu erhalten.

3. Zur Sinnhaftigkeit eines nationalen Alleingangs in einem europarechtlich harmonisierten Bereich

Mittlerweile gibt es ziemlich klare Zeichen aus Brüssel, dass eine Revision der E-Commerce Richtlinie und eine Harmonisierung des notice-and-takedown Verfahrens bevorsteht, um besser mit illegalen Inhalten, vor allem Hassrede, umgehen zu können. Auch die Ermöglichung der Strafverfolgung ist ein zentrales Thema. Mit der Budapest Convention und insbesondere der E-Evidence Verordnung wird aktuell angestrebt, internationale bzw. europäische Verfahren zur Datenherausgabe aufzusetzen. Diese Bemühungen werden von dem Gesetzesentwurf nicht aufgegriffen, sondern ein nationaler Sonderweg eingeschlagen. Dies ist umso bedenklicher, wenn es sich um Auskunftsersuchen auch gegenüber grenzüberschreitend tätigen Unternehmen handelt. Es sollten vielmehr, ähnlich wie beim Geldwäschegesetz, in internationalen Prozessen eingebettete Vorgänge etabliert werden. Vor dem Hintergrund der bereits stattfindenden Diskussionen und Lösungsansätze ist also fraglich, wie sinnvoll ein nationaler Alleingang ist. Bei den Debatten zur E-Evidence Verordnung fordert die Bundesregierung zu Recht die Sicherung grundrechtlicher Standards und rechtsstaatlicher Garantiemaßnahmen ein – jene sind allerdings in dem vorliegenden Gesetzesentwurf nicht ausreichend vorhanden.

4. Zusammenfassung der Kritik zum Referentenentwurf

- Der nationale Vorstoß ist im Lichte der Bemühungen auf europäischer Ebene, Lösungen für eine effektivere Strafverfolgung durch erleichterte Prozesse bei Auskunftsersuchen der Behörden zu finden, nicht sinnvoll.

- Das wichtige Ziel der Bekämpfung von Hasskriminalität und Rechtsextremismus fordert starke Maßnahmen, jedoch stellen einige der jetzt gewählten Mittel erheblich weitgehende Eingriffe dar, die auf Verhältnismäßigkeit und Proportionalität überprüft werden müssen.

- Die im TMG vorgesehene Verpflichtung für Telemediendiensteanbieter, Auskunftsersuchen von Behörden bezüglich Verkehrs- und Bestandsdaten, inklusive Passwörtern, Folge zu leisten, wirft viele Fragen auf, insbesondere welche Anforderungen an die Ersuchen gestellt werden und welche prozeduralen Sicherungen gelten - auch im Zusammenhang mit den jeweiligen Ermächtigungsgrundlagen,

die jeweils auf die entsprechende Norm im Telekommunikationsgesetz (TKG) bzw. TMG verweisen.

- Die im TMG vorgesehene Verpflichtung für Telemediendiensteanbieter mit mehr als 100 000 Kunden, für die Entgegennahme der Auskunftsverlangen sowie für die Übertragung der Daten eine elektronische „Behörden-Schnittstelle“ bereitzuhalten, ist weder notwendig oder verhältnismäßig, noch praktikabel für viele, insbesondere kleinere Anbieter.

- Die im NetzDG vorgesehene proaktive Meldepflicht von Inhalten, IP-Adressen und Portnummern stellt einen Systembruch mit geltendem Recht dar, das darauf basiert, dass die Strafverfolgung eine ureigene hoheitliche Aufgabe ist. Außerdem wäre es dahingehend ein Systembruch, dass Diensteanbieter nicht auf Ersuchen hin sondern proaktiv Daten an Behörden herausgeben müssen – das bisher bestehende System würde damit faktisch „umgedreht“.

- Es ist unklar, ob sich die Meldepflicht auf Meldungen nach dem NetzDG beschränkt oder für jegliche Beschwerden gilt, die eine Inhaltslöschung zum Ziel haben. Dies würde zur Ausleitung einer unüberschaubaren Menge an Inhalten führen, die kaum zu bearbeiten sein wird - insbesondere ohne massive Aufstockung der Ressourcen der Staatsanwaltschaften, womit insgesamt in einer erheblichen Zahl von Fällen die Gefahr ausbleibender Strafverfolgung bestehen dürfte.

- Durch die automatische Ausleitung von IP-Adressen und Portnummern, welche in vielen Fällen bereits für eine Identifizierung des Nutzers ausreichen, auf Basis einer rechtlichen Prüfung der sozialen Netzwerke, wird beim BKA eine Art „Verdachtsdatei“ von womöglich nach Bewertung einer Staatsanwaltschaft oder eines Gerichts unschuldigen Nutzern angelegt. Dies wirft Fragen nach der Vereinbarkeit mit Persönlichkeitsrechten und dem Rechtes auf ein angemessenes Verfahren auf sowie Fragen der Haftbarkeit der Unternehmen bei Fehleinschätzungen.

5. Zu den Regelungen im Einzelnen

a. Änderungen des Telemediengesetzes (Artikel 4 des Referentenentwurfs)

In der StPO sollen die Regelungen über die Verkehrs- und Bestandsdatenerhebung gegenüber Telekommunikationsdiensteanbietern auf Maßnahmen gegenüber Telemediendiensteanbietern erweitert werden. Zusätzlich soll im Telemediengesetz das Auskunftsverfahren gegenüber Telemediendiensteanbietern neu geregelt werden: Der neue § 15a TMG-E schafft die Grundlage für Telemediendiensteanbieter, den Ersuchen von Polizei und Staatsanwaltschaft Folge zu leisten, wenn Bestands- und Verkehrsdaten erhoben werden. Diese Regelung erstreckt sich auf alle Telemediendiensteanbieter (nicht nur auf soziale Netzwerke) und schließt explizit den Zugriff auf Passwörter ein. Problematisch ist in dem Zusammenhang, dass ein Passwort bei vielen Anbietern Zugriff auf Bereiche vermitteln kann, die von der polizeilichen Untersuchung gar nicht umfasst sind – wie z.B. E-Mails, in der Cloud hinterlegte Dokumente, historische Standortdaten, Suchhistorien, etc. Fast alle Anbieter speichern Passwörter zudem nur verschlüsselt, allein schon aufgrund der Vorgaben des Bundesamts für Informationssicherheit. Eine Möglichkeit der Entschlüsselung durch die Behörden ist bei dem aktuellen Stand der Technik nahezu ausgeschlossen. Es ist deshalb allein schon aus Gründen der Praktikabilität nicht nachvollziehbar, was mit diesem Vorschlag erreicht werden soll.

Übersehen wird im Entwurf, dass viele andere Gesetze – insbesondere z.B. Landespolizeigesetze – ebenfalls auf § 14 TMG verweisen. In zahlreichen dieser Gesetze werden das TKG und das TMG systematisch noch sehr unterschiedlich behandelt. Prozedurale Sicherungen für „besondere Bestandsdaten“ wie Zugriffskennungen bzw. Passwörter sind in den meisten dieser Gesetze gerade nur für den Bestandsdatenbegriff des TKG vorgesehen. Für Bestandsdatenabfragen an Telemediendiensteanbieter wird hingegen vielfach noch auf die jeweiligen Generalklauseln der Gesetze zurückgegriffen. Der Entwurf problematisiert diese gängige Behördenpraxis bezeichnenderweise für die Ermittlungsgeneralklausel §§ 161, 163 StPO, nicht aber für andere Regelungen, darunter andere Bundesgesetze, auf deren Ermächtigungsgrundlagen die in § 15a Abs. 3 TMG-E genannten Stellen regelmäßig zurückgreifen. Vor allem der Umstand, dass durch die vermeintliche „Klarstellung“ in § 15a TMG-E nun auch der Bestandsdatenbegriff des § 14 TMG „per Definition“ auf Passwörter erstreckt werden soll, hat daher weitreichende Folgen, wenn die Polizei (oder andere in § 15a Abs. 3 TMG-E aufgeführte Stellen) durch „andere Türen“ Zugriff auf das TMG nimmt. Diese sehen überwiegend keine prozeduralen Sicherungen vor wie nunmehr etwa in § 100j Abs. 1 S. 2 StPO. Gleichzeitig wird den Telemediendiensteanbietern durch die „Legaldefinition“ nunmehr jede Argumentation abgeschnitten, dass der Zugriff auf Passwörter bei einer Bestandsdatenabfrage (unter anderem auf Basis von Generalklauseln)

unverhältnismäßig ist. Hier liegt das Risiko einer „Online-Hausdurchsuchung“ ohne jede zusätzliche Sicherung für die betroffenen Nutzer.

Es ist deshalb unter anderem unklar, inwieweit ein richterlicher Beschlusses für die Herausgabe von Bestandsdaten wie Nutzerpasswörter erforderlich wäre. Zwar ist zu erahnen, dass bei einem Zugriff auf entsprechende Bestandsdaten über die Strafprozessordnung der Richtervorbehalt erhalten bleibt, selbst wenn auch hier eine Klarstellung erfolgen muss, jedoch ist die StPO eben nicht das einzige Gesetz, welches auf § 14 TMG verweist. Das praktische Zusammenwirken der neu zu schaffenden Norm im TMG mit bestehenden Kompetenznormen in anderen Gesetzen muss klarer beschrieben werden. Ein Richtervorbehalt ist in jedem Falle als Voraberfordernis einer Ausleitung zu verankern.

Durch die breite Grundlage nach § 15a (2) TMG-E (erforderlich z.B. für die Verfolgung von Ordnungswidrigkeiten) und die Vielzahl der befugten Stellen nach § 15 a(3) TMG-E ist mit einem massiven Anstieg der Auskunftsersuchen zu rechnen. Es ist unklar, inwiefern die Telemediendiensteanbieter in der Lage sein werden, zu verifizieren, ob hinter den Ersuchen ein legitimes Interesse steht. Hier sind prozessuale Anforderungen an die Anfragen notwendig.

Die in § 15 a (5) TMG-E vorgesehene Verpflichtung für Telemediendiensteanbieter mit mehr als 100 000 Kunden, für die Entgegennahme der Auskunftsverlangen sowie für die Übertragung von Daten eine elektronische „Behörden-Schnittstelle“ bereitzuhalten, würde eine enorm hohe Anzahl von Diensten, darunter einfache kommerzielle Webseiten, umfassen und ist deshalb weder notwendig oder verhältnismäßig, noch praktikabel für viele, insbesondere kleinere Anbieter. Es wird voraussichtlich bei der überwiegenden Anzahl der Telemediendiensteanbieter keinen Bedarf für Datenaustausch und damit für eine elektronische Schnittstelle geben. Deshalb würde es zunächst völlig ausreichen, wie ebenfalls im Gesetz vorgesehen, dass die Diensteanbieter sicherstellen, dass eine Fachkraft für die Prüfung von Auskunftsverlangen zur Verfügung steht.

b. Änderungen des Netzwerkdurchsetzungsgesetzes (Artikel 5 des Referentenentwurfs)

I. Problematik der Verlagerung der Rechtsdurchsetzung auf Private

Durch einen neuen § 3a NetzDG-E soll eine Meldepflicht eingeführt werden, nach der aufgrund einer Beschwerde über rechtswidrige Inhalte entfernte Inhalte, die nach Ein-

schätzung des sozialen Netzwerks einen aus einer Reihe von Straftatbeständen erfüllen, an das BKA weitergeleitet werden müssen. Neben dem Inhalt sollen ebenfalls die IP-Adresse und Portnummer des Nutzers, der den Inhalt hochgeladen hat, proaktiv ausgeleitet werden. Neben der Auslegung des Rechts soll jetzt auch ein Teil der Rechtsdurchsetzung, nämlich die initiale Entscheidung darüber, welche Fälle strafrechtlich verfolgt werden sollten, privatwirtschaftlichen Unternehmen überlassen werden. In unserem, vor allem auf dem Grundgesetz basierenden Rechtssystem wird seit jeher ein Unterschied zwischen dem Bereich der Gefahrenabwehr und dem Bereich der Strafverfolgung gemacht. Die Löschpflichten des NetzDG sollen die anderen Nutzer davor schützen, strafbare Inhalte auf der Plattform zu sehen. Die Löschpflicht kann damit dem Bereich der Gefahrenabwehr zugeordnet werden. Ganz anders verhält es sich jedoch bei einer Pflicht zur Ausleitung der Daten aller Nutzer, die sich nach Prüfung des Betreibers des sozialen Netzwerks strafbar gemacht haben könnten. Hier würde durch die Ausleitung des Betreibers die Strafverfolgung überhaupt erst ausgelöst. Für die Strafverfolgung gelten jedoch zu Recht höhere Anforderungen als bei der reinen Gefahrenabwehr. Der Betreiber kann die Strafbarkeit nicht abschließend beurteilen. So ist es ihm beispielsweise unmöglich den subjektiven Tatbestand oder etwaige Rechtfertigungs- und Entschuldigungsgründe zu prüfen. Die Weiterleitungspflicht wäre somit ein Systembruch mit geltendem Recht, dem zu Grunde liegt, dass die Strafverfolgung eine ureigene hoheitliche Aufgabe ist. Außerdem wäre es dahingehend ein Systembruch, dass Diensteanbieter nicht auf Anforderung sondern proaktiv Daten an Behörden herausgeben müssten – das bisher bestehende System würde damit faktisch „umgedreht“. Anders als z.B. beim Geldwäschegesetz sind viele der nach NetzDG zu meldenden Inhalte für jeden sichtbar und daher auch von den Behörden kontrollierbar. Die Strafverfolgung darf nicht auf private Akteure übertragen werden. Eine Anzeigepflicht ist dem deutschen Recht außerdem grundsätzlich fremd.

Durch die Erweiterung der Definition „Beschwerden über rechtswidrige Inhalte“ in § 3a (2) 1 NetzDG-E ist unklar, ob die Meldepflicht an NetzDG Beschwerden geknüpft ist oder auf jegliche Beschwerden, die zum Ziel eine Inhaltslöschung haben, ausgedehnt wird. Dies würde sich nachteilig auf die Bemühungen der Anbieter auswirken, NetzDG Meldewege einzuführen, die eine klare Methode bieten, Verstöße gegen das deutsche Recht nach dem NetzDG zu melden. Außerdem würde es zu einer Ausleitung von Daten in einer unüberschaubaren Anzahl von Fällen führen. Dies wird gerade nicht das verfolgte Ziel unterstützen, die Strafverfolgung effizienter zu gestalten. Hier ist also eine Klarstellung erforderlich, dass sich die Meldepflicht auf Inhalte, über die Beschwerde nach dem NetzDG eingereicht wurde, bezieht.

Bei den Straftatbeständen, an die nach § 3a (2) 3 NetzDG-E eine Meldepflicht geknüpft werden soll, handelt es sich, zumindest teilweise, um hochgradig auslegungsbedürftige

Normen. Die Umstände der Äußerung, der Tonfall, der Verlauf der Diskussion, der Kontext, die Frage der Einbeziehung politisch umstrittener Themen, all dies und noch mehr muss in die Abwägung mit einbezogen werden. Auch Überzeichnung, Übertreibung und Polemik und erst recht Satire sind von der Meinungs- bzw. Kunstfreiheit gedeckt. Selbst bei Tatbeständen der Volksverhetzung und Morddrohung sind die allermeisten Fälle keinesfalls offensichtlich. Es wäre also zu erwarten, dass – gerade in Anbetracht drohender Bußgelder - die Unternehmen oftmals in einer bei Nachbetrachtung als irrtümlich zu bewertenden Weise einen Post und die IP-Adresse und Portnummer eines Nutzers an das BKA weiterleiten, der nichts Unrechtes getan hat. Der betroffene Nutzer ist dann durch den Inhalt und die IP-Adresse bzw. Portnummer in vielen Fällen bereits identifizierbar.

Diese Art der „Verdachts-Datei“ beim BKA, die auf Rechtsbewertungen privater Unternehmen basiert, wirft zum einen Fragen der Haftung für Fehlentscheidungen der Unternehmen auf. Die Plattformen müssten haftungsbefreit sein, wenn sie Inhalte "fälschlicherweise" weiterleiten oder nicht weiterleiten, in Fällen in denen sie zu einer anderen rechtlichen Einschätzung kommen – so auch im Geldwäschegesetz vorgesehen. Zum anderen sehen wir hier die Gefahr der Verletzung von Persönlichkeitsrechten und die Verletzung des Rechtes auf ein angemessenes Verfahren jener von der Weiterleitung betroffenen, am Ende aber unschuldigen Nutzer. Die Anbieter bekommen zudem keinerlei Rückmeldung vom BKA über den Verbleib der Daten sowie den Stand des Verfahrens. Kommt das BKA zu dem Schluss, dass ausgeleitete Inhalte strafrechtlich nicht relevant sind, so liegen dennoch für einen ungeklärten Zeitraum personenbezogene Daten der Betroffenen bei Strafverfolgungsbehörden, obwohl sich die Betroffenen rechtmäßig verhalten haben. Hinzu kommt, dass die durch das BKA als rechtmäßig befundenen Inhalte gesperrt bleiben und die Anbieter die Prüfkriterien und Entscheidungen des BKA nicht in ihre zukünftige Prüfpraxis mit aufnehmen können.

Nach § 3a (6) NetzDG-E dürfen die sozialen Netzwerke den Betroffenen innerhalb von 14 Tagen nach der Ausleitung der Daten nicht über die Datenherausgabe informieren; wenn das BKA innerhalb dieser 14 Tage Einspruch erhebt, dürfen sie es gar nicht. Ob, wann und wie Betroffene dann von solchen Verfahren in Kenntnis gesetzt werden (dürfen), ist unklar. Ebenfalls unklar ist, wie die Behörden mit ausgeleiteten Inhalten umgehen werden, die aus dem Ausland von nicht-deutschen Staatsbürgern verfasst bzw. hochgeladen wurden und ob in diesen Fällen überhaupt eine rechtliche Grundlage für das Speichern der Daten bzw. für die Strafverfolgung gegeben ist.

Positiv zu bewerten ist, dass im Gesetzentwurf in § 3 (2) 5 NetzDG-E vorgesehen ist, dass der Beschwerdeführer darauf hinzuweisen ist, dass er Strafanzeige erstatten und auf welchen Seiten er hierzu weitere Informationen erhalten kann. Dies stellt einen richtigen

und verhältnismäßigen Ansatz dar, dem Problem entgegenzutreten, dass nur die wenigsten Fälle zu einer Strafanzeige führen. Die im Bitkom organisierten Anbieter sind gern bereit, dadurch einen Beitrag zur Strafverfolgung zu leisten.

II. Ausgestaltung der Schnittstelle für die Ausleitung der Inhalte

Vorgesehen ist in § 3a (5) NetzDG-E die Schaffung einer Schnittstelle, über die die Anbieter Inhalte an das BKA ausleiten sollen. Hier stellen sich viele Fragen. Insbesondere ist zu klären, was genau ausgeleitet werden soll. Gerade bei Kommentaren zu einem Inhalt ist für die strafrechtliche Bewertung der Hauptinhalt, auf den sich die Kommentare beziehen, in die Bewertung mit einzubeziehen. Soll dieser Hauptinhalt mit ausgeleitet werden? Es stellen sich Fragen zur Anonymisierung der auszuleitenden Inhalte. Beispielsweise werden wohl Namen geschwärzt werden müssen. Wie genau eine solche Schnittstelle ausgestaltet werden soll, was genau auszuleiten ist, wie der Datenschutz insbesondere auch anderer Nutzer gewährleistet werden soll - diese wesentlichen Fragen müssen im Gesetzestext beantwortet werden um Rechtssicherheit zu schaffen. Darüber hinaus muss ein Dialog zwischen Anbietern, dem Gesetzgeber sowie dem BKA stattfinden, um alle offenen Fragen zu klären.

III. Problematik der Vereinbarkeit mit datenschutzrechtlichen Vorgaben

Die proaktive Ausleitung personenbezogener Daten stellt einen weitgehenden Eingriff in das Grundrecht auf Datenschutz bzw. informationelle Selbstbestimmung dar und wirft Fragen der Vereinbarkeit mit datenschutzrechtlichen Vorgaben (u.a. aus DS-GVO und JI-Richtlinie) auf. Aufgrund der Tatsache, dass es sich hier nicht zwingend nur um deutsche Unternehmen handelt und die entsprechenden Daten nicht in Deutschland liegen müssen, besteht daneben die Gefahr der Verletzung von „Heimatrechten“ bzw. internationalen Verträgen, die von den Mitgliedstaaten unterzeichnet sind. Die Datenschutzgrundverordnung sieht zwar Ausnahmen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Prävention, Ermittlung, Aufdeckung oder Verfolgung von Straftaten vor (Art. 2 Abs. 2 lit (d) DSGVO) und auch die Offenlegung der Daten auf der Online-Plattform könnte grundsätzlich auf den Erlaubnistatbestand aus Artikel 6 Abs. 1 lit. c i.V.m Abs. 2 DS-GVO gestützt werden, wenn "die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung, der der für die Datenverarbeitung Verantwortliche unterliegt, erforderlich ist". Jedoch müssen sich die entsprechenden Eingriffsnormen am Verfassungsrecht und an den grundrechtlichen Wertungen der DS-GVO (und ggf. für die polizei-

liche Verarbeitung der Daten an der JI-Richtlinie) messen lassen. An der Verfassungsmäßigkeit solch weitreichender Datenausleitungs- und Übermittlungspflichten bestehen zurzeit jedenfalls noch Zweifel. Zudem bestehen hinsichtlich der territorialen Anwendbarkeit aus unserer Sicht noch Bedenken, da die Herausgabeverpflichtung aus dem Netzwerkdurchsetzungsgesetz allein vom deutschen Recht abhängt – unabhängig davon, ob die Straftat überhaupt eine Straftat im Land des Betroffenen darstellt und von welchem Ort aus der entsprechende Verstoß begangen wird.

IV. Problematik der ausbleibenden Strafverfolgung

Das Melden des Inhalts und der IP-Adresse durch die Unternehmen nützt weiterhin nichts, wenn keine Verfolgung stattfindet. Aktuell besteht schon das Problem, dass oftmals nichts passiert, wenn Personen aufgrund von Rechtsverletzungen im Netz Strafanzeige erstatten. Daher sollten auch IP-Adressen nur dann herausgegeben werden, wenn ein Ermittlungsverfahren läuft und ein Anfangsverdacht vorliegt. So kann die rechtsstaatliche Verfolgung strafrechtlich relevanter Handlungen durch die zuständigen Ermittlungsbehörden und durch die Gerichte unterstützt werden.

Grundsätzlich zu begrüßen ist, dass für den Zweck der Strafverfolgung im Netz personelle Ressourcen erhöht werden sollen. Aber auch wenn das Bundeskriminalamt personell aufgestockt werden soll, gäbe es ein Mengenproblem, wenn die Unternehmen jegliche vermeintlich strafrechtlich relevanten Inhalte automatisch an die Behörden weiterleiten würden. Selbst bei einer Begrenzung auf schwere Straftatbestände bestünde dieses Problem: Allein bei YouTube wurden zwischen Januar und Juni 2019 fast 30.000 Inhalte auf Grund von Beschwerden entfernt, die auf Gewaltandrohungen oder auf Hassrede und politischen Extremismus abzielten und nach NetzDG gemeldet wurden[1]. Allein auf der Plattform Twitter wurden im gleichen Zeitraum im Bereich der im Referentenentwurf definierten Straftaten rund 23 000 Inhalte auf Grund von NetzDG-Beschwerden entfernt und müssten mit entsprechenden Daten ausgeleitet werden[2]. Diese Zahlen würden noch drastisch gesteigert werden, wenn die Eingrenzung der Beschwerden auf solche entfallen sollte, die nach dem NetzDG gemeldet werden.

[1] Youtube Transparenzbericht Januar bis Juni 2019 - Entfernungen von Inhalten nach dem Netzwerkdurchsetzungsgesetz: https://transparencyreport.google.com/netzdg/youtube?hl=de

[2] Twitter Netzwerkdurchsetzungsgesetzbericht Januar bis Juni 2019: https://cdn.cms-twdigitalassets.com/content/dam/transparency-twitter/data/download-netzdg-report/netzdg-jan-jun-2019.pdf

Weiterhin ist fraglich, ob die Zentralstelle für Meldungen beim BKA bei der richtigen Einrichtung angesiedelt ist. Es wäre vorzugswürdig, wenn eine solche Zentralstelle durch die Staatsanwaltschaften eingerichtet würde, da diese für die Strafverfolgung zuständig sind. Und nur durch eine frühzeitige Einbeziehung der Staatsanwaltschaften kann sichergestellt werden, dass nur in solchen Verfahren, in denen von der zuständigen Staatsanwaltschaft ein Anfangsverdacht festgestellt wurde, weitere Ermittlungen und weitere Datenauskünfte erfolgen.

6. Frist für das Inkrafttreten

Für die Einführung der Meldepflichten ist eine Frist von 3 Monaten vorgesehen. Dies ist, entgegen der Annahmen des Entwurfsverfassers, bei Weitem nicht ausreichend, um den sozialen Netzwerken notwendige Anpassungen zu ermöglichen, die sich aus dem Mehraufwand der Meldepflichten ergeben. Der Analyse, dass durch gesetzliche Änderung umfangreiche Umstrukturierungen bei den sozialen Netzwerken entbehrlich seinen, widersprechen wir vehement. In Folge dieses Vorhabens müsste nicht nur der Ablauf der Prüfungen nach NetzDG-Meldungen über rechtswidrige Inhalte verändert werden, sondern er würde sich auch erheblich verzögern. Vor allem aber müsste differenziert werden, ob die Inhalte von einem Nutzer bzw. in einem Territorium verbreitet wurden, dass unter deutsches Recht fällt.

7. Vorschläge zur Verbesserung der Strafverfolgung im Netz

Jenseits dieser grundsätzlichen Bedenken und über die bereits bestehende Kooperation zwischen Unternehmen und Strafverfolgungsbehörden- insbesondere bei Fällen in denen Leib und Leben in Gefahr sind- hinaus, sind die im Bitkom organisierten und von der Thematik betroffenen Unternehmen bereit, an einem funktionsfähigen und rechtssicheren Modell mitzuwirken, um den Strafvollzug effektiver zu gestalten. Ein solches Modell muss aber innerhalb des geltenden Rechtssystems datenschutzkonform entwickelt und ausgestaltet werden sowie für Plattformen und Strafverfolgungsbehörden handhabbar sein. Außerdem sollte es in eine Reform des überalterten und nicht funktionalen MLAT-Systems eingebettet sein. Ziel muss in jedem Fall eine internationale Lösung sein. Denn ohne die Ausräumung der Rechtskonflikte zwischen dem Recht des Sitzlandes der Betreiber sowie dem deutschen Recht verbleiben die Betreiber in einer rechtlichen Zwickmühle.