



**Stellungnahme Twitter
an das
Bundesministerium der Justiz und für Verbraucherschutz zum
vorgeschlagenen Gesetz zur Bekämpfung des Rechtsextremismus und der
Hasskriminalität (GBRH-E)**

Am 18. Dezember 2019 hat das Bundesjustizministerium einen Gesetzentwurf zur Bekämpfung des Rechtsextremismus und der Hasskriminalität vorgelegt der u.a. die Änderungen mehrerer Gesetze, wie z.B. des Telemediengesetzes (TMG) und des Netzwerkdurchsetzungsgesetzes (NetzDG) enthält. Twitter begrüßt die Gelegenheit der Verbändeanhörung durch die Bundesregierung und bedankt sich für Möglichkeit eine Stellungnahme abzugeben und den Vorschlag zu kommentieren.

Mit diesem Entwurf und insbesondere mit den Anpassungen im NetzDG will die Bundesregierung erreichen, dass insbesondere Social-Media-Unternehmen, die vom NetzDG erfasst werden, proaktiv Zugang zu Nutzerdaten gewähren bzw. diese übermitteln.

Twitter bietet neben dem Verfahren für Strafverfolgungsbehörden, Daten über ein Rechtshilfeersuchen (MLAT) zu erhalten, derzeit einen entsprechenden gesicherten Kanal für Anfragen der Strafverfolgungsbehörden in bestimmten Fällen an, die sog. "Legal Request Submissions Site". Twitter arbeitet hier eng mit Strafverfolgungsbehörden zusammen um sicherzustellen, dass sie über die Werkzeuge und entsprechendes Wissen verfügen, um Anfragen an Twitter zu stellen. Unsere Richtlinien für Anfragen von Strafverfolgungsbehörden sind öffentlich zugänglich. Sie enthalten Einzelheiten zu den bei Twitter verfügbaren Informationen und Daten sowie zur Vorgehensweise bei Anfragen. Gerade bei diesen freiwilligen Maßnahmen müssen Unternehmen wie das unsere jedoch sicherstellen, dass die rechtlichen Standards eingehalten werden, um illegale und ungültige Anfragen zur Ausleitung von Daten zu vermeiden. Die Legal Request Submissions Site, die Twitter zur Bearbeitung von Informationsanfragen eingerichtet hat und über welche die Behörden Daten schnell, effektiv und vor allem sicher in verschlüsselter Form anfordern können, hat sich grundsätzlich bewährt. Der Twitter-Transparenz-Bericht, den wir ständig aktualisieren, informiert über die steigende Zahl der Informationsanfragen von Strafverfolgungsbehörden weltweit sowie über die Anzahl der Ausleitungen von Daten.

Auch wenn die Plattform außerhalb Deutschlands angesiedelt sind bestehen bereits etablierte Verfahren und Prozesse, mit denen Strafverfolgungsbehörden Informationen von Diensten wie dem unseren anfordern können. Diese Verfahren sind manchmal langwierig, da des öfteren unterschiedliche Gesetze bzw. gesetzliche Grundlagen in unterschiedlichen Territorien betroffen sein können. Die Europäische Kommission hat daher internationale Verhandlungen zum Austausch grenzüberschreitender elektronischer Beweismittel in Strafsachen aufgenommen. Die EU-Kommission schlägt neue Regeln vor, die den Polizei- und Justizbehörden den Zugang zu den elektronischen

Beweismitteln, die sie für ihre Ermittlungen benötigen, erleichtern und beschleunigen sollen und hat zwei Verhandlungsrichtlinien vorgelegt - eine für die Verhandlungen mit den Vereinigten Staaten und eine für das zweite Zusatzprotokoll zum Budapester Übereinkommen des Europarates über die Cyberkriminalität.

Angesichts der Mechanismen, die bereits von Diensten wie Twitter angeboten werden und der rechtlichen Rahmenbedingungen, die für Informationen zur Verfügung stehen, sieht der Entwurf weitreichende und übergreifende Verpflichtungen für die Anbieter sozialer Netzwerke vor. Dies stellt nicht nur einen Paradigmenwechsel dar, sondern steht auch im Widerspruch zum deutschen Verfassungsrecht, zu grundlegenden Prinzipien des EU-Rechts, zum lokalen Recht der Anbieter von Telemediendiensten und zum Völkerrecht. Im Folgenden konzentrieren wir uns auf einige Schwerpunkte.

1. Proaktive Berichtspflichten im Rahmen der NetzDG

Durch den vorgeschlagenen § 3a NetzDG-E würde den Anbietern von sozialen Netzwerken eine proaktive Meldepflicht der Inhalte sowie der IP-Adresse und der Portnummer an das Bundeskriminalamt (BKA), d.h. eine Strafverfolgungsbehörde auferlegt werden. Dies würde die proaktive Meldung von *möglichen* Straftaten beinhalten. Dadurch würden die Plattformen ureigene staatliche Aufgaben übernehmen. Zudem wäre es ein Systembruch, da die Plattformen nicht auf Ersuchen hin, sondern proaktiv personenbezogene Daten ihrer Nutzer ausleiten, auf deren Grundlage eine strafrechtliche Verfolgung erfolgen kann oder nicht. Es wäre ein nicht ungefährlicher Präzedenzfall und ein Eingriff in die Persönlichkeitsrechte sowie in die bürgerlichen Freiheiten der Allgemeinheit.

1.1

Ein solches Erfordernis würde dem deutschen Verfassungsrecht und den vom Bundesverfassungsgericht (BVerfG) aufgestellten Grundprinzipien zum Schutz personenbezogener Daten (Recht auf informationelle Selbstbestimmung) widersprechen. Das Bundesverfassungsgericht hat in Bezug auf Datenverarbeitung und den sich daraus ergebenden informationellen Maßnahmen wichtige Schranken zum Schutz der Bürgerinnen und Bürger vor Bedrohungen und Verletzungen der Privatsphäre etabliert, (z.B. BVerfG-Urteil vom 24.01.2012 - 1 BvR 1299/05, NJW 2012, 1419). Die Anforderungen des Gesetzentwurfs sind mit diesen Schutzmaßnahmen nicht vereinbar. Insbesondere das Erfordernis, dass private Unternehmen personenbezogene Daten ihrer Nutzer nur auf der Grundlage der begrenzten Informationen aus den auf der Plattform veröffentlichten Inhalten proaktiv offenlegen, sowie die schwierigen Fragen der Auslegung der in § 3a Abs. (2) aufgeführten gesetzlichen Bestimmungen, der Anwendung völkerrechtlicher Vorschriften zur Anwendbarkeit deutschen Rechts auf die auf einer weltweiten Plattform veröffentlichten Inhalte und das Verbot, den Nutzer für eine Mindestfrist von 14 Tagen (die vom BKA unbefristet verlängert werden könnte) über die Offenlegung seiner Daten zu informieren (Stillhaltefrist), sind mit diesen Grundsätzen nicht vereinbar. Angesichts der Tatsache, dass eine Unterlassung der Meldung mit einem Ordnungswidrigkeitsverfahren geahndet werden kann, ist zudem fraglich, ob die Anforderungen hinreichend präzise sind. Dies gilt insbesondere für die Festlegung, wann eine Beschwerde als "Beschwerde über einen rechtswidrigen Inhalt" zu betrachten ist und

wann es "konkrete Anhaltspunkte" dafür gibt, dass ein bestimmter Inhalt unter den Anwendungsbereich der in § 3a Abs. 2 aufgeführten Straftaten fällt.

1.2

Darüber hinaus wirkt die Anwendung der Meldepflicht auf Anbieter mit Sitz im Ausland Fragen der Anwendung des EU-Rechts und des internationalen öffentlichen Rechts auf. Insbesondere könnte sie zu Verstößen gegen ausländische Gesetze im Heimatland des Unternehmens oder gegen internationale Verträge, die von Mitgliedsstaaten und Organisationen unterzeichnet wurden, führen. Schließlich wirkt diese Verpflichtung Bedenken aus Sicht der Meinungsfreiheit auf, wie weiter unten erläutert wird.

Die Straftatbestände, die nach § 3a (2) 3 NetzDG-E mit einer Offenlegungspflicht verbunden werden sollen, sind - zumindest in Teilen - Normen, die ein hohes Maß an Interpretation erfordern. Die Umstände der Äußerung, der Ton, der Kontext, die Frage der Einbeziehung politisch kontroverser Themen, all dies und mehr müssen bei der Abwägung der einzelnen Teile des gemeldeten Inhalts berücksichtigt werden. Übertreibung, Parodie und Satire fallen ebenfalls unter die Meinungsfreiheit, was die Komplexität der Abwägung, die vorgenommen werden muss, noch erhöht. Selbst im Falle von Volksverhetzung oder Morddrohungen sind die meisten Fälle keineswegs offensichtlich und auch sorgfältig abgewogene Begutachtungen können zu unterschiedlichen Auslegungen kommen. Es muss daher - insbesondere im Hinblick auf die Androhung von Bußgeldern - damit gerechnet werden, dass Unternehmen zur Vermeidung von Sanktionen übermäßig viele Nutzerdaten an das BKA weitergeben, auch wenn der Inhalt der Nebenabrechnung nicht gegen geltendes Recht verstößt.

Im Ergebnis kann durch die proaktive Offenlegung von IP-Adressen und Portnummern, die allein auf einer Einschätzung der Dienste wie dem unserem beruht, eine Art "Verdachtsdatei" des Bundeskriminalamtes über potenziell unschuldige Nutzer entstehen. Dies wirft Fragen nach der Vereinbarkeit mit den Persönlichkeitsrechten und dem Rechtsgrundsatz auf ein faires Verfahren, sowie Fragen nach der Haftung von Unternehmen bei Fehleinschätzungen auf.

Diese Verpflichtung zur Ausleitung von Nutzerdaten stellt womöglich einen Verstoß gegen das geltende Recht dar, da die Strafverfolgung eine eigenständige, souveräne Aufgabe des Staates ist. Im Gegensatz z.B. zum Geldwäschegesetz, ist in dem vorliegenden Fall der nach dem Gesetz an die Strafverfolgungsbehörden zu meldende Inhalt für jeden sichtbar und kann daher von den Behörden eingesehen werden. Zudem ist die Pflicht zur Strafanzeige im deutschen Recht auf sehr wenige Fälle beschränkt. Es kann nicht ausgeschlossen werden, dass eine Meldepflicht wie im Gesetzentwurf vorgesehen, die Daten vieler Nutzer betrifft, die nicht dem deutschen Recht unterliegen (d.h. außerhalb Deutschlands wohnen) und die nicht gegen die in ihrem Land geltenden Gesetze verstoßen.

Darüber hinaus sollte beachtet werden, dass nicht-deutsche Unternehmen betroffen sind und die entsprechenden Daten sich nicht in Deutschland befinden. Bei der Einhaltung des Gesetzentwurfs können Unternehmen gegen die nationalen Gesetze im Herkunftsland oder internationales Recht verstoßen. Zwar sieht das Datenschutzgrundverordnung Ausnahmen für die Verarbeitung personenbezogener Daten durch

die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten vor (Artikel 2 Abs. 2 lit. d). Die Offenlegung der Daten durch eine Online-Plattform ist laut Entwurf gerechtfertigt, wenn "die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung, der für die Verarbeitung Verantwortliche unterliegt, erforderlich ist" (Art. 6 Abs. 2 lit. d)). 1 lit (c)), was die Frage der territorialen Anwendbarkeit einer solchen Verpflichtung im NetzDG aufwerfen könnte.

Auch bestimmte strafbare Handlungen, wie die §§ 86, 86a und 131 StGb, sind nach deutschem Strafrecht nicht strafbar, wenn der Inhalt außerhalb Deutschlands hochgeladen wurde (Bundesgerichtshof vom 19. August 2014 (3 StR 88/14)). Dies führt zu Unsicherheit darüber, wie Unternehmen den Standort eines gemeldeten Accounts, der nach deutschem Recht illegal sein könnte, überprüfen und bestimmen könnten. Da NetzDG-Beschwerden über unseren Dienst in erheblichem Umfang Inhalte betreffen, die nicht in deutscher Sprache verfasst sind, kann davon ausgegangen werden, dass die meisten dieser Tweets nicht innerhalb Deutschlands veröffentlicht wurden, wenn sie auch in Deutschland zugänglich sind. Es ist daher fraglich, inwieweit diese Inhalte von der beabsichtigten Regelung erfasst würden und wie dies zu unterscheiden wäre.

Im Hinblick auf das EU-Recht sind das in Artikel 3 der E-Commerce-Richtlinie vorgesehene Herkunftslandprinzip und das Verbot, Anbietern eine allgemeine Verpflichtung zur Überwachung der von ihnen gespeicherten Informationen oder zur aktiven Suche nach Fakten oder Umständen, die auf illegale Aktivitäten hinweisen, gemäß Artikel 15 ECD sowie die Datenschutzgrundverordnung zu berücksichtigen. Hinsichtlich der Datenschutzgrundverordnung gelten die gleichen Grundsätze, wie sie das Bundesverfassungsgericht hinsichtlich der Beschränkungen der Nutzung und Verarbeitung personenbezogener Daten aufgestellt hat. Hinsichtlich des Herkunftslandprinzips gelten die bereits in Bezug auf das NetzDG im Allgemeinen geäußerten Bedenken für die vorgeschlagenen Änderungen. In diesem Zusammenhang möchten wir auf die Stellungnahme der EU-Kommission zur Notifizierung 2019/412/F zum französischen Gesetz gegen Hasskriminalität im Internet verweisen (Loi visant à lutter contre les contenus haineux sur internet, Emission d'observations prévues à l'article 5, Abs. 2, de la directive (UE) 2015/1535 du 9 septembre 2015), die ernsthafte Zweifel an der Vereinbarkeit des französischen Gesetzesentwurfs mit dem Herkunftslandprinzip aufkommen lässt.

Ähnlich wie die Anmerkungen der EU-Kommission zum französischen Gesetzesentwurf, verstößt die Meldepflicht nach Artikel 3a, die den Anbieter verpflichtet, zu beurteilen, ob bestimmte Inhalte unter die im Entwurf aufgeführten strafrechtlichen Bestimmungen fallen, höchstwahrscheinlich gegen Artikel 15 der E-Commerce-Richtlinie, der es den Mitgliedstaaten untersagt, den Anbietern eine Überwachungspflicht aufzuerlegen.

1.3

Darüber hinaus wirft die Verpflichtung der im Ausland ansässigen Plattformen zur Bereitstellung von Nutzerinformationen an staatliche Behörden rechtliche Fragen zur Anwendbarkeit des deutschen (Straf-)Rechts im Ausland auf. Eine solche Inanspruchnahme einer universellen, extraterritorialen Gerichtsbarkeit auf der Grundlage von Äußerungsdelikten würde vermutlich die grundlegenden Menschenrechte von Personen außerhalb Deutschlands verletzen, insbesondere in Fällen, in denen keine gesetzlich

vorgeschriebene Verbindung zu Deutschland besteht. Sie würde auch zu einem Konflikt mit den lokalen Gesetzen, denen der Anbieter unterliegt und den lokalen Gesetzen, welche die im Ausland ansässigen Staatsangehörigen schützen, führen. Im Falle eines solchen Konflikts (z.B. mit dem Electronic Communication Privacy Act - ECPA der USA) wäre der Anbieter nicht in der Lage, der Meldepflicht nachzukommen, ohne ein erhebliches Haftungsrisiko nach lokalem Recht einzugehen. Abgesehen von diesen Bedenken besteht die Gefahr, dass andere Staaten (in denen ggf. das Rechtsstaatsprinzip weniger stark ausgeprägt ist als in Deutschland) von Unternehmen ein ähnliches Verfahren verlangen, um Daten von Autoren von Beiträgen zu erhalten, die aus Sicht der jeweiligen Regierung illegal sind. Dies könnte dann wiederum deutsche Bürger betreffen.

Durch den Verzicht auf eine internationale oder regionale Koordinierung in dieser Frage würde Deutschland in der Tat einen unilateralen und fragmentierten Ansatz normalisieren, der erhebliche Risiken für die Privatsphäre und das Recht auf freie Meinungsäußerung der deutschen Bürger und Einzelpersonen weltweit darstellt. Mit der Budapester Konvention und insbesondere der E-Evidence-Verordnung werden derzeit Anstrengungen unternommen, internationale und europäische Verfahren zur Ausleitung von Nutzerdaten zu schaffen. Diese Bemühungen werden im Gesetzesentwurf nicht aufgegriffen, sondern es wird ein besonderer nationaler Weg beschritten. Dies ist besonders besorgniserregend, wenn es um Informationsanfragen geht, einschließlich Anfragen von Unternehmen, die grenzüberschreitend tätig sind. Die Verfahren sollten in internationale Prozesse eingebettet und etabliert werden.

Das wichtige Ziel der Bekämpfung von Hasskriminalität und Rechtsextremismus erfordert entschlossene und ernsthafte Maßnahmen, angesichts der weitreichenden Auswirkungen auf die Menschenrechte einiger der vorgeschlagenen Änderungen sollte der Entwurf auf die Verhältnismäßigkeit geprüft und bewertet werden, wie es das Völkerrecht verlangt.

Es gibt verschiedene Möglichkeiten, die dazu beitragen könnten, die Verfolgung von Straftaten, die online begangen wurden, zu verbessern: Die Dienstleister könnten zum Beispiel die Beschwerdeführer auf die Möglichkeit aufmerksam machen, eine Online-Strafanzeige bei den Strafverfolgungsbehörden einzureichen und sie mit weiteren hilfreichen Informationen zur Untermauerung einer Anzeige unterstützen.

2. Änderungen des Telemediengesetzes (Artikel 4 des Gesetzesentwurfs) einschließlich der Offenlegung von Passwörtern nach dem Telemediengesetz

Aufgrund der weiten Ausgestaltung des § 15a Abs. 2 TMG-E (z.B. für die Verfolgung von Ordnungswidrigkeiten) und der großen Zahl der nach § 15 a Abs. 3 berechtigten Stellen ist mit einem starken Anstieg der Auskunftersuchen zu rechnen. Es ist unklar, inwieweit die Anbieter von Telemedien in der Lage sein werden, zu prüfen, ob hinter den Anfragen ein berechtigtes Interesse steht. Daher wären prozessuale Voraussetzungen für diese Anträge notwendig.

Die im Telemediengesetz vorgesehene Verpflichtung für Telemedienanbieter, behördlichen Auskunftersuchen über Verkehrs- und Bestandsdaten einschließlich Passwörtern nachzukommen, wirft viele Fragen auf. Insbesondere ist unklar, welche

Voraussetzungen für die Ausleitung von Nutzerdaten bei Auskunftersuchen zu erfüllen sind und welche verfahrensrechtlichen Schutzmaßnahmen gelten würden - auch im Zusammenhang mit den jeweiligen Rechtsgrundlagen, die auf die entsprechende Norm im Telekommunikationsgesetz bzw. Telemediengesetz verweisen.

Offenlegung von Passwörtern

Vorab möchten wir klarstellen, dass der bei weitem überwiegende Anteil von Twitter-Accounts und damit auch die online-gestellten Inhalte öffentlich verfügbar sind, so dass jeder sie sehen kann. Daher stellt sich die Frage der Zweckmäßigkeit einer Offenlegung von Passwörtern. Die angedachte Pflicht zur Herausgabe von Passwörtern ist ein weiter Eingriff, da ein Passwort Zugang zu weiteren Bereichen bieten kann, die nicht von den Ermittlungsbefugnissen der Polizei abgedeckt sind - wie E-Mails, in der Cloud gespeicherte Dokumente, historische Ortsdaten, Suchverläufe usw. Die Anbieter von Telemediendiensten wären zudem nicht in der Lage, dieser Verpflichtung nachzukommen, da Artikel 32 Abs. 1 lit. der DSGVO die unverschlüsselte Speicherung von Passwörtern verbietet (siehe: Bußgelder, die der Landesdatenschutzbeauftragte des Landes Baden-Württemberg gegen den Anbieter eines sozialen Netzwerks verhängt hat. Um dieser Verpflichtung nachzukommen, müssten Unternehmen entsprechend Passwörter im Klartext führen, was die Kontoinhaber einem erheblichen Risiko aussetzt.

3. Definition der Beschwerde über rechtswidrige Inhalte (§ 1 Abs. 4 NetzDG)

In der StPO sollen die Vorschriften über die Erhebung von Verkehrs- und Bestandsdaten bei den Anbietern von Telekommunikationsdiensten auf die Anbieter von Telemediendiensten ausgeweitet werden. Darüber hinaus soll das Telemediengesetz eine Verpflichtung für Telemedienanbieter schaffen, bei der Erhebung von Bestands- und Verkehrsdaten den Aufforderungen von Polizei und Staatsanwaltschaft nachzukommen.

Die sehr weit gefasste Definition der "Beschwerde über unrechtmäßige Inhalte" verstößt gegen das Prinzip der Verhältnismäßigkeit und der Rechtssicherheit und Bestimmtheit. In Anbetracht der Schwierigkeiten bei der Feststellung, ob ein bestimmter Inhalt als eines der unter die NetzDG-Bestimmungen fallenden Verbrechen eingestuft werden kann, und aufgrund des Mangels an Hintergrundinformationen und der Notwendigkeit einer Auslegung der gesetzlichen Bestimmungen sollte die Verantwortung für diese Beurteilung bei den Strafverfolgungsbehörden und nicht bei einem privaten Unternehmen liegen. Insbesondere die in Abschnitt 1 Abs. 1 vorgesehene vorgesehene Beweislastumkehr, ob bestimmte Inhalte unter das NetzDG fallen oder nicht, ist nicht akzeptabel. Es ist zu bedenken, dass ein Verstoß gegen die Bestimmung des NetzDG über den Umgang mit rechtswidrigen Inhalten mit Verwaltungsstrafen geahndet wird. Es ist ein grundlegendes Rechtsprinzip, dass nicht nur die Bestimmungen, die eine Geldbuße auslösen, klar sein müssen, sondern auch, dass die Beweislast für eine Verletzung bei den Behörden und nicht bei dem mutmaßlichen Rechtsverletzer liegt.

Nach § 3a (6) NetzDG-E dürfen soziale Netzwerke den Betroffenen innerhalb von 14 Tagen nach der Weitergabe der Daten über die Weitergabe nicht informieren; erhebt das BKA innerhalb dieser 14 Tage Einspruch, so darf dies überhaupt nicht geschehen.

Es ist unklar, ob, wann und wie die Betroffenen dann über solche Verfahren informiert werden (dürfen). Unklar ist auch, wie die Behörden mit Inhalten umgehen werden, die von außerhalb Deutschlands geschrieben oder hochgeladen wurden und nur in Deutschland illegal wären. Unklar ist zudem, wie lange die Daten beim BKA vorgehalten werden dürften.

Zusammenfassung:

Wenn es als wichtig erachtet wird, dass rechtswidrige Inhalte, wie sie im Änderungsantrag spezifiziert sind, den Strafverfolgungsbehörden gemeldet werden, sind solche Personen dafür die entsprechenden, die den angeblich rechtswidrigen Inhalt an die Plattform melden. Sie haben bereits eine Bewertung vorgenommen, als sie den Inhalt an die Plattform gemeldet haben und verfügen - im Gegensatz zum Plattformanbieter - über weitere Hintergrundinformationen. Der Umweg über die Anbieter der Telemediendienste erscheint nicht notwendig. Stattdessen wäre die Möglichkeit einer vereinfachten Strafanzeige für die Meldenden von Inhalten ein besser geeigneter und effizienterer Weg als illegale erachtete Inhalte von den sozialen Netzwerken direkt den Strafverfolgungsbehörden zu melden.

Wir sind bereit zu solchen Verfahren beizutragen, indem wir in unsere Rückmeldung an Nutzer, die eine NetzDG-Beschwerde eingereicht haben, Informationen darüber aufnehmen, wie ein NetzDG-Beschwerdeführer die Strafverfolgungsbehörden informieren und Strafanzeige erstatten könnte. Wir könnten entsprechend auf eine Website verweisen, auf welcher der Beschwerdeführer weitere Informationen dazu erhalten kann. Wir sind auch bereit, zu einem funktionierenden und rechtssicheren internationalen Modell beizutragen, um das Gesamtsystem effektiver zu gestalten. Ein solches Modell muss jedoch in Übereinstimmung mit den Anforderungen des internationalen Rechts, des EU-Rechts, anderer in der jeweiligen Situation anwendbarer lokaler Gesetze und in Übereinstimmung der geltenden Menschenrechte und bisher geltender rechtsstaatlicher Schutzmechanismen entwickelt und gestaltet werden und muss für die Plattformen und Strafverfolgungsbehörden handhabbar sein.
