

# Stellungnahme

## Stellungnahme zum Kommissionsvorschlag einer Verordnung zur Verhinderung der Verbreitung terroristischer Online-Inhalte

21.12.2018

Seite 1

### Einleitung

Die Europäische Kommission hat am 12. September 2018 den Vorschlag KOM (2018) 238 für eine "Verordnung des Europäischen Parlaments und des Rates zur Verhinderung der Verbreitung terroristischer Online-Inhalte" ("die Verordnung") veröffentlicht. Bitkom begrüßt das Ziel der Verordnung, die Wirksamkeit der Bekämpfung terroristischer Inhalte im Internet zu verbessern und spricht sich außerdem für die Verfolgung von Straftaten in diesem Bereich aus. Die Mitglieder des Bitkom stehen ausdrücklich zu ihrer Verantwortung, hier ihren Beitrag zu leisten und begrüßen deshalb auch die Absicht der Kommission, die Zusammenarbeit zwischen privaten Unternehmen und den zuständigen Behörden zu verbessern. Es steht außer Zweifel, dass terroristische Inhalte inakzeptabel sind - offline wie online. Das Haftungsregime für illegale Inhalte, das in der Richtlinie über den elektronischen Geschäftsverkehr festgelegt und in mehreren Urteilen präzisiert wurde, ist ausgereift, ausgewogen und ausreichend, um den aktuellen Herausforderungen im Zusammenhang mit illegalen Inhalten im Internet zu begegnen. Darüber hinaus ergreifen viele Dienstleister freiwillig Maßnahmen, um ihre eigene Gemeinschaftsrichtlinien durchzusetzen.

Die Arbeit mit starren gesetzlichen Verpflichtungen und kurzen Fristen bei gleichzeitig hohen Strafen, wie im Vorschlag gefordert, ist gefährlich und wahrscheinlich sogar kontraproduktiv, da sie zu Fehlentscheidungen und übereifrigen Löschungen führen kann. Die vorgeschlagene Verordnung stellt einen schwerwiegenden Eingriff in das Geschäftsmodell der Unternehmen dar und erfordert daher eine solide Begründung. Ohne nachgewiesene Notwendigkeit sind alle Dienstleister gezwungen, eine Infrastruktur aufzubauen, die eine schnelle Überprüfung und Entfernung von Inhalten, proaktive, automatische Maßnahmen, Jahresberichte und einen 24/7-Ansprechpartner ermöglicht. Die Folgenabschätzung der Europäischen Kommission evaluiert jedoch die Auswirkungen dieser spezifischen Rechtsvorschriften auf die Industrie, insbesondere auf kleine und mittelständische Unternehmen, nicht ausreichend. Zudem liegt die Anwendung und Durchsetzung anwendbaren Rechts in der Verantwortung von Behörden und Gerichten und sollte nicht auf private Unternehmen übertragen werden. Aus den im folgenden Papier genannten Gründen fordert Bitkom die sorgfältige Überprüfung der Rechtsgrundlagen dieser Verordnung.

Mit dem Ziel, konstruktiv in den Gesetzgebungsprozess einzugreifen, möchten wir den Verordnungsvorschlag wie folgt kommentieren:

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

**Nick Kriegeskotte**  
**Leiter Infrastruktur & Regulierung**  
T +49 30 27576-224  
[n.kriegeskotte@bitkom.org](mailto:n.kriegeskotte@bitkom.org)

Albrechtstraße 10  
10117 Berlin

Präsident  
Achim Berg

Hauptgeschäftsführer  
Dr. Bernhard Rohleder

## Stellungnahme

### Verordnung zur Verhinderung der Verbreitung terroristischer Online-Inhalte

Seite 2|4

#### Anwendungsbereich (Artikel 1)

Der Anwendungsbereich der Verordnung ist äußerst umfangreich – es mangelt an Präzision und Klarheit. In der jetzigen Form gilt die Verordnung für „Hosting-Service-Provider“. Bei der Definition dieses Begriffs in Artikel 2 wurde die Chance, den Anwendungsbereich zu präzisieren, nicht wahrgenommen. Die Verordnung würde in ihrer jetzigen Form nicht nur soziale Netzwerke, sondern jegliche Plattformen, die Daten von Dritten “hosten“ umfassen. Inbegriffen wären also auch Messenger-Dienste, Web-Hoster, Appstores, Marktplätze, professionelle Netzwerke (z.B. LinkedIn/Xing), Nachrichten-Websites mit Kommentarfunktion, Software-Entwicklungsdienste und Cloud-Infrastrukturdienste. Außerdem ist keine Erleichterung für kleine und mittelständische Unternehmen vorgesehen, welche bei der Umsetzung der Verordnung zu großen Teilen an die Grenzen ihrer (finanziellen) Ressourcen stoßen würden.

Bitkom fordert den Gesetzgeber eindringlich auf, den Anwendungsbereich der Verordnung auf jene Anbieter zu begrenzen, die einen Zugang zur Öffentlichkeit gewähren, und Cloud-Infrastruktur Anbieter vom Anwendungsbereich auszunehmen. Für den Schutz der überwältigenden Mehrheit der gesetzestreuen Nutzer ist es wichtig, die Privatsphäre bei der Weitergabe von Material über einen privaten Cloud-Service zu schützen. Diese Anbieter sind höchstwahrscheinlich nicht in der Lage, bestimmte Nutzer-generierte Inhalte abzurufen, da dies bedeuten würde, dass komplette Dienste, die auf ihre Infrastruktur angewiesen sind, abgeschaltet werden müssen. Sie haben in der Regel keinen Zugriff auf die in der Cloud gespeicherten Daten, der es ihnen erlauben würde, Inhalte zu überwachen, zu filtern oder anderweitig zu kontrollieren.

#### Zuständige Behörden (Artikel 17)

Es ist unklar, wie die "zuständigen Behörden", die Entfernungsanordnungen und Meldungen verschicken können, ernannt werden. Dies sollte genauer definiert werden, da für die Unternehmen klar sein muss, welche Behörde für sie zuständig ist. Jeder Mitgliedstaat sollte über eine einzige Justizbehörde verfügen, die für Unternehmen mit Sitz im jeweiligen Mitgliedstaat zuständig ist. Aufgrund der mangelnden EU-weiten Definition von Terrorismus, bedingt durch kulturelle und gesellschaftliche Unterschiede, sollte es nicht möglich sein, dass Behörden Mitgliedsstaaten-übergreifend tätig werden können.

#### Definition von “terroristischen Inhalten“ (Artikel 2)

Die Definition des Begriffs "terroristischer Inhalt" der Verordnung ist zu vage und bietet zu viel Interpretationsspielraum. Um terroristische Inhalte effektiv und rasch entfernen zu können, muss eine kohärente Interpretation der Definition durch die zuständigen Behörden gegeben sein, wenn sie Löschanordnungen erlassen. Außerdem benötigen die Unter-

## Stellungnahme

### Verordnung zur Verhinderung der Verbreitung terroristischer Online-Inhalte

Seite 3|4

nehmen Leitlinien, die aufzeigen, wie sie "terroristische Inhalte" bei der Überprüfung von Meldungen oder der Durchführung proaktiver Maßnahmen interpretieren müssen.

Es ist außerdem unklar, wer im Zweifelsfall die endgültige Entscheidung trifft, ob Inhalte als terroristisch einzustufen sind - dies kann nicht dem Ermessen privater Unternehmen überlassen werden, sondern muss in der Verordnung klarer definiert bzw. von Behörden oder Gerichten entschieden werden.

#### **Löschanordnung und Empfehlung (Artikel 4, bzw. 5)**

Dem Text des Vorschlags kann nicht entnommen werden, aus welchen Gründen sich eine zuständige Behörde für eine Löschanordnung und gegen eine Empfehlung, oder umgekehrt, entscheiden würde. Der relevante Inhalt ist in beiden Fällen terroristischer Natur, weshalb es ohne weitere Präzisierung der Vorgehensweise schwierig abzuschätzen ist, aus welchen Gründen ein weicheres oder härteres Instrument gewählt werden sollte. Es ist jedoch unerlässlich, dass die betroffenen Unternehmen in der Lage sind zu verstehen, in welchen Fällen sie mit einer Anordnung oder einer Empfehlung rechnen können, da eine der beiden Maßnahmen bußgeldbehaftet ist. Außerdem ist problematisch, dass im Falle einer Empfehlung die privaten Unternehmen entscheiden müssen, ob es sich um terroristische Inhalte handelt – dies sollte jedoch Aufgabe staatlicher Behörden, bzw. Gerichten sein. Abgesehen davon führt grundsätzlich die Kombination aus extrem kurzen Fristen und hohen Strafen zu einem Anreiz, Inhalte zu löschen, ohne sie gründlich zu prüfen. Dies ist in Bezug auf die in der Charta der Grundrechte der Europäischen Union verankerten Meinungs- und Informationsfreiheit kritisch zu bewerten. Es sollte ein Mechanismus in der Verordnung verankert werden, der es den Unternehmen ermöglicht, sowohl Löschanordnungen als auch Empfehlungen anfechten zu können; beispielsweise aufgrund von Bedenken bezüglich der Kompatibilität mit diesen Grundrechten.

#### **Proaktive Maßnahmen (Artikel 6)**

Zu den proaktiven Maßnahmen, deren Anordnung durch zuständige Behörden in der Verordnung vorgesehen ist, gehört der Einsatz automatisierter Instrumente zur Erkennung und Entfernung terroristischer Inhalte. Es ist nicht klar, welche Art von Maßnahmen die Kommission hier in Betracht gezogen hat, die mit dem Verbot einer allgemeinen Verpflichtung zur Überwachung der von Dienstleitern übermittelten oder gespeicherten Daten (festgeschrieben in Artikel 15 der Richtlinie über den elektronischen Geschäftsverkehr) vereinbar ist. Besonders beunruhigend ist in diesem Zusammenhang, dass die Kommission ausdrücklich automatisierte Instrumente als mögliche proaktive Maßnahmen erwähnt.

## Stellungnahme Verordnung zur Verhinderung der Verbreitung terroristischer Online-Inhalte

Seite 4|4

---

---

Bitkom vertritt mehr als 2.600 Unternehmen der digitalen Wirtschaft, davon gut 1.800 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.