VERBAND DER INTERNETWIRTSCHAFT E.V.

STELLUNGNAHME

zum Vorschlag der Europäischen Kommission für eine Verordnung des Europäischen Parlaments und des Rates zur Verhinderung der Verbreitung terroristischer Online-Inhalte (2018/0031 (COD))

Berlin/ Brüssel, 18. Dezember 2018

Mitte September 2018 hat die Europäische Kommission den Vorschlag für eine „Verordnung des Europäischen Parlaments und des Rates zur Verhinderung der Verbreitung terroristischer Online-Inhalte“ vorgelegt.

eco nimmt zu dem Vorschlag wie folgt Stellung.

I. Allgemeines

Vorab kritisiert eco den Erlass einer Verordnung zur Löschung oder Sperrung bestimmter illegaler Inhalte und lehnt diesen als unverhältnismäßig ab. Die Maßnahme erscheint insgesamt weder notwendig noch nachvollziehbar. Gerade in den letzten Jahren sind insbesondere von den großen Plattformen multiple Anstrengungen unternommen worden, illegale Inhalte im Allgemeinen und terroristische Inhalte im Besonderen zu erkennen, zu löschen und damit deren Verbreitung einzudämmen. Einige große Unternehmen haben unter enormem Einsatz von Personal und finanzieller Ressourcen technische Möglichkeiten erprobt und an konstruktiven Mechanismen des Austauschs und der Zusammenarbeit mit den Behörden gearbeitet. Diese Anstrengungen haben bereits deutliche Resultate gezeigt, wie die jährlichen Auswertungen der Europäischen Union gezeigt haben.

Gerade jetzt eine sanktionsbewehrte Verordnung zu schaffen, die auch der Bevölkerung suggerieren soll, die Unternehmen seien in diesem Bereich untätig, ist weder sachgerecht noch zielführend. Des Weiteren ist die Verordnung in weiten Teilen unklar und widerspricht teilweise geltendem europäischen Recht.

Einige Artikel der Verordnung sind dabei als besonders problematisch einzustufen.

II. Zu den Regelungen im Einzelnen

- **Artikel 1 Nummer 2 – Anwendungsbereich**

Die Verordnung soll für alle Hostingdiensteanbieter gelten, die – unabhängig vom Ort ihrer Hauptniederlassung – Dienste in der Europäischen Union anbieten. Diesem Anwendungsbereich unterfallen somit alle Unternehmen, unabhängig von Größe und Umsatz. Dies geht viel zu weit. In der Praxis würden unter diesen Anwendungsbereich auch Dienste fallen, die z.B. bei Content-Delivery-Networks Daten bei der Durchleitung lediglich cachen. Daher begrüßt eco Überlegungen, B2B-Dienste von der Verordnung auszunehmen.

Dies ist nicht sachgerecht und führt zudem zu einer unverhältnismäßigen Belastung vor allem kleiner und mittlerer Unternehmen.

- **Artikel 4 - Entfernungsanordnungen**

Artikel 4 Nummer 2 der Verordnung legt fest, dass terroristische Inhalte innerhalb einer Stunde nach Erhalt einer Entfernungsanordnung der zuständigen Behörde gelöscht oder gesperrt werden müssen.

Diese kurze Frist wird damit begründet, dass terroristische Inhalte in der ersten Stunde nach ihrem Upload am gefährlichsten seien, da sie dann am häufigsten geteilt würden. Ein Beleg dieser Theorie fehlt jedoch. Deshalb erscheint die Festsetzung der Frist willkürlich. Ihre Einhaltung ist jedenfalls unrealistisch. Sogar große Unternehmen dürften mit der starren Frist vor eine große Herausforderung gestellt werden, die in der Umsetzung nicht nur im Einzelfall Probleme verursachen wird. Für jedes kleine oder mittlere Unternehmen ist eine fristgerechte Reaktion – ohne dezidierte Ressourcenwidmung – unmöglich.

Jeder kleine Anbieter müsste – um keine Sanktionen zu riskieren – sicherstellen, dass 24 Stunden am Tag mindestens ein qualifizierter Mitarbeiter erreichbar ist, der im Fall einer Anordnung sofort auf den entsprechenden Inhalt zugreifen und diesen entfernen kann. Das würde zu einer unverhältnismäßigen finanziellen Belastung der Anbieter führen – gerade, wenn man annehmen muss, dass der Fall des Artikel 4 der Verordnung bei kleinen und mittleren Anbietern so gut wie nie eintreten dürfte. Eine stichprobenartige Umfrage des eco unter kleinen und mittelgroßen Mitgliedern hat ergeben, dass kein einziges der befragten Unternehmen in der Vergangenheit mit einem terroristischen Inhalt auf den eigenen Servern konfrontiert war.

Das vom Gesetzentwurf formulierte Ziel, terroristische Inhalte binnen der ersten Stunde zu löschen, um eine Verbreitung zu verhindern, geht deshalb gerade in Bezug auf kleine und mittlere Unternehmen fehl. Denn: Damit eine massenhafte Verbreitung eines Inhalts stattfinden kann, muss dieser zunächst überhaupt wahrgenommen werden, was bei kleinen Hostingdiensteanbietern praktisch nicht der Fall sein kann. Dann müsste er „massenhaft“ verbreitet werden, auch das ist bei der Nutzung einer kleinen Plattform eher auszuschließen. Deshalb richtet sich der Vorstoß der EU schon der Intention nach an große Plattformen, auf denen Inhalte potentiell binnen Minuten von tausenden Nutzern geklickt und weiterverbreitet werden.

Auch die Vorgaben der Artikel 8 und 14 – die Abgabe jährlicher Transparenzberichte und die Einrichtung von Kontaktstellen – dürften KMU überfordern, aber zu keinerlei Mehrwert im Kampf gegen terroristische Inhalte führen.

Unter anderem deshalb sind KMU von den Vorschriften der Verordnung auszunehmen.

- **Artikel 5 – Meldungen**

Im Gegensatz zu Artikel 4, der Entfernungsanordnungen aufgrund einer gerichtlich überprüften Entscheidung vorsieht, sieht Artikel 5 Nummer 2 für Behörden und zuständige Einrichtungen der Union die Möglichkeit vor, den

Hostingdiensteanbietern Inhalte „zur freiwilligen Prüfung“ zu übermitteln. Sodann soll der Diensteanbieter nach Nummer 5 diesen Inhalt zunächst auf dessen Vereinbarkeit mit seinen eigenen Nutzungsbedingungen überprüfen und ggf. Maßnahmen ergreifen. Die Behörde muss nach Artikel 5 Nummer 4 „ausreichend detaillierte Informationen“ unter anderem darüber weitergeben, „warum der Inhalt als terroristischer Inhalt erachtet wird“. Im Kern läuft diese Vorschrift also darauf hinaus, dass in unklaren bzw. schwer zu beurteilenden Fällen die Entscheidung über Löschung oder Entfernung auf die Diensteanbieter übertragen wird.

Diese Unterscheidung zwischen Entfernungsanordnungen einerseits und Meldungen andererseits überrascht und erschließt sich nicht. In Artikel 2 Absatz 4 und 5 der Verordnung ist festgelegt, wann es sich bei einem Inhalt um eine terroristische Straftat bzw. einen terroristischen Inhalt handeln soll. Wenn ein verdächtiger Inhalt einer zuständigen Behörde bekannt wird, sollte diese als staatliche Hoheitsträgerin in der Lage sein, zeitnah die mögliche Strafbarkeit verbindlich zu beurteilen.

Sinnvoll erscheint eine derartige Unterscheidung im Vorgehen nur dann, wenn sie Anbieter rechtlich privilegieren würde, die durch eine konstruktive Zusammenarbeit bereits ihr Interesse daran bewiesen haben, bestmöglich mit den Behörden zu kooperieren und aus eigenem Antrieb bereits alles dafür tun, terroristische Inhalte von ihren Servern zu entfernen. Dann wäre es konsequent, diesen Unternehmen nur Meldungen zu übermitteln, im Vertrauen darauf, dass sie schnellstmöglich und mit größter Sorgfalt behandelt werden.

Entfernungsanordnungen, die bei Nichtbeachtung zu Sanktionen führen können, wären für solche Fälle vorbehalten, in denen nach Auffassung der Behörden eine Notwendigkeit für ein verbindliches Vorgehen besteht; etwa deshalb, weil die Anbieter durch ihr bisherigen Verhalten belegt haben, dass sie kein ausreichendes Interesse an einer Bekämpfung und einen schnellen Entfernung terroristischer Inhalte haben.

Meldungen nach Artikel 5 wären dann auch vom Sanktionenkatalog des Artikel 18 auszunehmen.

Anderenfalls – bei Inkrafttreten der Verordnung in ihrer jetzigen Form – bestünde die Gefahr, dass die staatlichen Stellen ihre ureigenen Aufgaben – über die Hilfskonstruktion des Artikel 5 – aus Mangel an personellen Ressourcen und adäquater Ausstattung an Privatunternehmen delegieren würden. Das ist nicht hinnehmbar.

- **Artikel 6 – Proaktive Maßnahmen**

Artikel 6 verpflichtet die Diensteanbieter „gegebenenfalls“ zur Ergreifung wirksamer und verhältnismäßiger proaktiver Maßnahmen. Gemäß Nummer 3 des Artikels kann die zuständige Behörde den Diensteanbieter auch auffordern, zusätzliche spezifische proaktive Maßnahmen zu ergreifen, wenn sie der Auffassung ist, dass die bereits ergriffenen Maßnahmen nicht ausreichen. Mit derartigen Maßnahmen soll ein erneutes Verbreiten durch Hochladen eines bereits als illegal erkannten Inhalts verhindert werden, es sollen aber auch neue terroristische Inhalte „erkannt und ermittelt“ werden.

Wie das technisch zu bewerkstelligen ist, sagt die Verordnung indes nicht. Aus gutem Grund – schließlich ist ein proaktives Monitoring nur mit Hilfe von Uploadfiltern denkbar. Verpflichtende Uploadfilter lassen sich aber unter keinen Umständen mit Artikel 15 der E-Commerce-Richtlinie in Einklang bringen, der eine allgemeine Verpflichtung der Diensteanbieter, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder aktiv nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen, gerade verbietet. Wie das Ziel der Verordnung erreicht werden kann, eine Umgehung des Artikel 15 der E-Commerce-Richtlinie nur in Ausnahmefällen zu ermöglichen, bleibt dann auch vollkommen unklar.

Zudem geht die Verordnung nicht auf die eklatant unterschiedlichen technischen Möglichkeiten und Voraussetzungen der einzelnen Diensteanbieter ein. Große Plattformen mögen über die Möglichkeiten verfügen, auch große Datenmengen zu filtern. Kleine und mittlere Unternehmen verfügen nicht über die erforderlichen technischen sowie personellen Ressourcen und Voraussetzungen. eco weist deshalb nochmals auf die technischen Gegebenheiten hin, die wir bereits in der Kommentierung der „Empfehlung der Kommission für wirksame Maßnahmen im Umgang mit illegalen Online-Inhalten“ thematisiert haben.[1]

Zunächst ist grundsätzlich darauf hinzuweisen, dass Systeme, die in der Lage sind, illegale oder terroristische Inhalte automatisch zu erkennen, so nicht existieren oder in der Praxis nicht umfassend eingesetzt werden können. Eine solche Beurteilung müsste etwa auch den Kontext einer Äußerung in die Bewertung mit einzubeziehen.

Systeme, die beispielsweise noch unbekannte Inhalte durch Vergleich mit bereits bekannten geschützten oder illegalen Inhalten ausfiltern können befinden sich in experimentellem Einsatz und Erprobung, sind aber (noch) nicht flächendeckend praxistauglich einsetzbar. Da es sich hierbei um KI-Systeme handelt, können sie auch immer nur eine Wahrscheinlichkeit benennen, mit der die Verbreitung eines Inhalts illegal ist. Um das herauszufinden, brauchen Unternehmen aber riesige Datenbanken illegaler Inhalte, mit dem die Algorithmen neu hochgeladenes Material abgleichen können. Über diese verfügen vielleicht einige wenige große Unternehmen, alle anderen aber nicht. Und ein Austausch bzw. ein Zurverfügungstellen dieser Datenbanken ist nicht nur technisch eine große Herausforderung, sondern auch datenschutzrechtlich mindestens problematisch und wirtschaftlich unverhältnismäßig.

Automatische Systeme sind spätestens regelmäßig dann nur sehr eingeschränkt einsetzbar, wenn es sich um dynamisch ändernde sowie kontextuale Inhalte handelt. Entsprechende Technologien existieren derzeit einfach nicht bzw. liefern keine ausreichende Qualität für einen praxistauglichen Einsatz und sind derzeit auch nicht absehbar. Die Rechtswidrigkeit der allermeisten terroristischen Inhalte ergibt sich aber erst aus ihrem Kontext, was eine automatische Ausfilterung nahezu unmöglich macht. In der Praxis dürfte

[1] https://www.eco.de/wp-content/uploads/dlm_uploads/2018/03/220180329_eco_STN_Illegale-Onlineinhalte_final.pdf

es zu vielen Fällen von Overblocking kommen, die nicht mit Grundrechten wie der Meinungs-, Presse- und Informationsfreiheit zu vereinbaren wären.

Für die allermeisten kleinen und mittleren Unternehmen ist es zudem faktisch unmöglich, derartige (effiziente) Filter-Systeme zu implementieren oder zu betreiben. Das gilt selbst dann, wenn die großen Unternehmen ihr Know-how zur Verfügung stellen sollten, wie es in der Empfehlung der Kommission im Frühjahr angedacht war: Unternehmen nutzen zum einen vollkommen unterschiedliche Technologien, die nicht notwendigerweise kompatibel sind. Zum anderen sind die erforderlichen technischen Infrastrukturen nicht vorhanden und würde die gesamte zur Verfügung stehende Rechenleistung der KMU-Unternehmen in der Regel nicht ausreichen.

Technisch denkbar wäre gegebenenfalls, dass jedes Unternehmen einen Inhalt an die großen Markteilnehmer schickt, damit diese ihn vor einem Upload durch ihre Filtersysteme analysieren. Eine solche Lösung dürfte aber politisch kaum gewollt sein: So würde Europa alle Unternehmen technologisch abhängig von überwiegend nichteuropäischen Unternehmen machen. Dies ist nicht nur politisch kritisch zu hinterfragen, sondern wirft auch dringende datenschutzrechtliche Fragen auf.

Wie also andere Unternehmen als große Plattformen überhaupt proaktive Maßnahmen umsetzen sollen, ist nicht ansatzweise nachvollziehbar. Der Erlass einer derart unklaren Verordnung, die zudem auch noch sanktionsbewehrt ist, wird erhebliche Rechtsunsicherheit hervorrufen. Auch aus diesen Gründen ist es unbedingt notwendig, kleine und mittlere Unternehmen vom Anwendungsbereich auszunehmen.

Die Verordnung ist kaum geeignet, eine Verbesserung der Lage im Kampf gegen den Terror herbeizuführen. Zum einen wenden große Plattformen, auf denen die Verbreitung terroristischer Inhalte möglicherweise gefährlich werden könnte, schon heute freiwillig Maßnahmen an, mit denen die Ziele der Verordnung bereits erreicht werden. Zum anderen werden die Verpflichtung und mögliche Sanktionierung kleinerer und mittlerer Unternehmen die Situation nicht verbessern, da es hier kein Problem mit der Verbreitung terroristischer Propaganda gibt. So führt der Vorschlag nur zu mehr Bürokratie und einer unverhältnismäßigen und unangemessenen Belastung von KMU.

Des Weiteren fehlt ein absolut zentraler Bestandteil im Kampf gegen den Terrorismus fast völlig: der Aufbau einer konsequenten Strafverfolgung. Werden terroristische Inhalte nur entfernt und fehlt eine entsprechende staatliche Sanktionierung, so besteht für die Personen, die diese Inhalte teilen, im Grunde kein Anreiz ihr Verhalten zu unterlassen. Das Schlimmste, was sie zu befürchten haben ist, dass der Inhalt rasch nicht mehr vorhanden ist. Dies ist sowohl aus general- als auch aus spezialpräventiven Gründen nicht hinnehmbar und gefährdet letztlich sogar den Rechtsstaat. Das ist im Sinne einer effizienten, ganzheitlichen Strategie gegen diese schweren Verbrechen nicht nachvollziehbar.

Über eco

Mit über 1.000 Mitgliedsunternehmen ist eco der größte Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, formt Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. Leitthemen sind Zuverlässigkeit und Stärkung der digitalen Infrastruktur, IT-Sicherheit und Vertrauen sowie Ethik und Selbstregulierung. Deshalb setzt sich eco für ein freies, technikneutrales und leistungsstarkes Internet ein.