VERBAND DER INTERNETWIRTSCHAFT E.V.

Stellungnahme zur Empfehlung der Kommission

für wirksame Maßnahmen im Umgang mit illegalen Online-Inhalten

(C (2018) 1177)

Am 1. März 2018 hat die Kommission in Brüssel eine Empfehlung für wirksame Maßnahmen im Umgang mit illegalen Online-Inhalten vorgestellt. eco bedankt sich für die Möglichkeit, zu den Empfehlungen der Kommission Stellung nehmen zu dürfen und möchte auf folgende Punkte hinweisen:

Kapitel I – Gegenstand und Begriffsbestimmungen

Betroffen sind nach Nummer 4a der Empfehlung „Hostingdiensteanbieter" im Sinne des Artikel 14 der EC-Richtlinie. Allerdings ist unter Erwägungsgrund 15 ausgeführt, dass die Empfehlung „in erster Linie" die Tätigkeiten und Verantwortlichkeiten dieser Anbieter betreffe. Gegebenenfalls könnten die ausgesprochenen Empfehlungen aber auch „sinngemäß auf andere betroffene Anbieter von Online-Diensten angewandt werden". Damit bliebe es den Mitgliedstaaten überlassen, wen sie in die Pflicht nehmen und die Verpflichtungen auf beliebig viele andere Dienste auszuweiten. Das bedeutet Rechtsunsicherheit für alle Unternehmen, vor allem jedoch für reine Infrastrukturbetreiber, die den Zugang zum Internet bereitstellen (Access-Provider) oder Content-Delivery-Anbieter.

Kapitel II – Allgemeine Empfehlungen zu illegalen Inhalten jedweder Art

eco plädiert für die Festlegung von Mindestanforderungen an „Hinweise", die die Kenntnis der Unternehmen begründen – ohne jedoch dem Hostingdiensteanbieter die Verantwortung dafür aufzubürden, dass Hinweise hinreichend genau und substantiiert gegeben werden, wie es in Nummer 6 der Empfehlung angedeutet ist. Es sollte klargestellt werden, dass ein Hinweis nur dann hinreichend substantiiert ist und Kenntnis begründen kann, wenn er etwa die Fundstelle (wo ist der illegale Inhalt zu finden?) und eine kurze Begründung enthält, warum der Inhalt moniert wird. Um Missbrauch zu vermeiden, sollten Hinweise in Fällen des Urheberrechtes oder des Persönlichkeitsrechts außerdem eine Möglichkeit für das Unternehmen enthalten, den Hinweisgeber zu kontaktieren. Dies ermöglicht in vielen dieser Fälle überhaupt erst die Feststellung, ob es sich tatsächlich um einen illegalen Inhalt handelt.

In den Nummern 9 bis 13 der Empfehlung werden Verfahren beschrieben, nach denen die Hostingdiensteanbieter vorgehen sollen, wenn ein Inhalt entfernt wird. Der Inhalteanbieter soll hiernach – soweit seine Kontaktdaten bekannt sind – über die Entscheidung informiert werden. Er soll die Möglichkeit bekommen, der Entscheidung zu widersprechen und dem Widerspruch soll „gebührend Rechnung getragen werden" etc. Dies alles soll

„ohne ungebührliche Verzögerung“ geschehen. Ungeachtet dessen, dass natürlich auch den großen Unternehmen dadurch ein enormer finanzieller und administrativer Aufwand entsteht, trifft die Empfehlung insbesondere auch kleine Anbieter. Selbst Hostingdiensteanbieter mit nur wenigen Mitarbeitern würden verpflichtet, qualifiziertes Personal für derartige Fälle einzustellen oder geeignete Verfahren bereitzustellen, die sie im Zweifel überfordern dürften.

Dasselbe gilt für Nummer 17 der Empfehlung. Einer Verpflichtung zu derart detaillierten Transparenzberichten dürften kleine Anbieter kaum nachkommen können.

Als besonders problematisch ist Nummer 18 der Empfehlung zu bewerten. Hier wird der Einsatz von „Systemen zur automatischen Erkennung illegaler Inhalte“ empfohlen, um „besondere proaktive, verhältnismäßige Maßnahmen“ zu deren Entfernung zu ergreifen.

Die Internetwirtschaft wendet sich entschieden gegen jede verbindliche Vorschrift zu sogenannten Upload-Filtern. Der Einsatz anlassloser, proaktiver Maßnahmen steht im absoluten Gegensatz zu Artikel 15 der E-Commerce-Richtlinie, der die Verpflichtung der Unternehmen zur Überwachung sowie zur aktiven Forschung gerade ausschließt.

Eine verbindliche Vorschrift ist zum einen – gerade in den Fällen, die hier vorrangig adressiert werden (Kinderpornographie, Terrorismus) – nicht notwendig.

Es gibt Systeme, die bereits bekannte urheberrechtlich geschützte oder illegale Bilder oder Videos durch ein „Fingerabdruck-System“ vergleichen und so bei erneutem Upload wiedererkennen können.

Diese Systeme wurden meist von großen Unternehmen aus den USA oder Asien entwickelt (z.B. YouTube und Facebook sowie Audible Magic) und werden etwa dazu eingesetzt, zu verhindern, dass Kinderpornographie und extreme Gewaltdarstellungen (wie sie etwa häufig in terroristischen Inhalten gezeigt werden) auf die Plattformen gelangen. Keine Plattform duldet derartige Inhalte auf ihren Servern. Denn es besteht staatenübergreifend, in jeder Religion, in jeder politischen Ideologie und durch alle sozialen Schichten hinweg der Konsens, dass kinderpornographische Darstellungen oder Motive extremer Gewalt als zutiefst verwerflich abzulehnen sind. Diesen Grundsätzen fühlen sich auch alle seriösen Plattformbetreiber dieser Welt verpflichtet.

Zudem gibt es weitere, sehr gut funktionierende Maßnahmen der Selbstregulierung, etwa die Beschwerdestellen, die Hinweise über illegale Inhalte entgegennehmen und ggf. notwendige Schritte einleiten. Nach den Erfahrungen der letzten Jahre funktionieren die verschiedenen Ansätze im Kampf gegen derartige Inhalte immer besser. Dies belegen unter anderem die Zahlen der eco Beschwerdestelle. (https://www.eco.de/wp-content/blogs.dir/jahresbericht_beschwerdestelle_2017_web_fin.pdf)

Auch im urheberrechtlichen Kontext gehen Plattformen gegen den Upload geschützter Inhalte vor. Es existieren Lizenzvereinbarungen mit den Rechteinhabern, die die Voraussetzungen für die Bereitstellung und den Schutz von urheberrechtlich geschützten Inhalten regeln. Auch hier ist eine weitere Regulierung demnach nicht notwendig.

In diesem Zusammenhang erschließt sich gerade nicht, warum die Kommission nun die Notwendigkeit sieht, weitergehende Verpflichtungen zu schaffen.

Bei allen anderen Konstellationen, also allen Fällen, die weder Kinderpornographie noch extreme Gewaltdarstellungen betreffen, darf es aus anderen Gründen keine gesetzliche Verpflichtung für Upload-Filter geben:

Zunächst ist darauf hinzuweisen, dass „Systeme zur automatischen Erkennung illegaler Inhalte“ so grundsätzlich nicht existieren oder in der Praxis noch gar nicht umfassend eingesetzt werden können.

Es gibt zwar einzelne Technologien, die etwa in der Lage sind, Musikstücke relativ sicher zu identifizieren. Auch gibt es die oben genannten „Fingerabdruck-Systeme“. Andere Systeme, die beispielsweise noch unbekannte Inhalte durch Vergleich mit bereits bekannten geschützten oder illegalen Inhalten ausfiltern können, funktionieren zwar theoretisch, befinden sich in experimentellen 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 geschützter oder illegaler Inhalte, mit dem die Algorithmen neu hochgeladenes Material abgleichen können. Über diese verfügen vielleicht ein paar große Unternehmen, alle anderen aber nicht. Und ein Austausch dieser Datenbanken ist nicht nur technisch eine große Herausforderung, sondern auch datenschutzrechtlich und wirtschaftlich mindestens problematisch.

Automatische Systeme sind spätestens regelmäßig dann nur sehr eingeschränkt einsetzbar, wenn es sich um Inhalte fernab von Audio und Video sowie um kontextuale Inhalte handelt. Entsprechende Technologien existieren derzeit einfach nicht bzw. liefern keine ausreichende Qualität.

Die Rechtswidrigkeit der allermeisten Inhalte ergibt sich aber erst aus ihrem Kontext, was eine automatische Ausfilterung unmöglich macht. Vor allem aber ist die Gefahr zu groß, eine Zensur-Infrastruktur zu etablieren, die überall auf der Welt – je nach Rechtslage – unterschiedliche Begehrlichkeiten weckt. Wenn immer mehr und immer verschiedenartigere Inhalte gelöscht werden müssen, wird es zwingend zu einem Overblocking kommen, weil auch große Anbieter dann nicht mehr in der Lage sein dürften, alle gelöschten Inhalte mittels „Sicherheitsvorkehrungen“ zu überprüfen.

Daneben ist auf den immensen personellen, finanziellen und administrativen Aufwand hinzuweisen, der den Unternehmen durch derartige proaktive Maßnahmen entstehen würde: Nach Nummer 4a sind von der Empfehlung

Hostingdiensteanbieter im Sinne des Art. 14 EC-RL erfasst, die ihre Dienste auf in der Union ansässige Verbraucher ausrichten – unabhängig von dem Ort ihrer Niederlassung. Nach Nummer 4b sind „illegale Inhalte“ alle Informationen, die nicht im Einklang mit Unionsrecht oder dem Recht eines betroffenen Mitgliedstaates stehen. Das bedeutet, dass jeder Anbieter verschiedene Filter für die einzelnen Mitgliedstaaten bauen müsste, weil es im Einzelfall erheblich abweicht, was rechtswidrig ist oder nicht. Oder er müsste Inhalte für die jeweiligen Länder „ausflaggen“ – in einem Land werden Bilder oder Videos gezeigt, im anderen nicht. Dies mag für ein paar große Unternehmen machbar sein, für die breite Masse der adressierten Unternehmen ist es das jedoch nicht.

Die in Nummer 20 der Empfehlung vorgesehenen „Sicherheitsvorkehrungen“ werfen indes weitere Fragen auf. Hiernach sollen Maßnahmen geschaffen werden, die sicherstellen, dass keine legalen Inhalte fälschlicherweise gelöscht werden. Diese Sicherheitsvorkehrungen sollen „insbesondere in einer menschlichen Aufsicht und Überprüfung bestehen“. Das widerspricht der Idee einer automatischen Ausfilterung. Die Kommission hat hier offensichtlich selbst die mit den Vorschlägen einhergehenden Probleme erkannt und versucht diese nun dadurch abzumildern bzw. zu begrenzen, dass „menschliche“ Sicherheitsvorkehrungen zu implementieren sind. Das ist paradox. Eine menschliche Überprüfung wäre bei der Masse der vermutlich gelöschten Inhalte daneben auch kaum möglich.

All diese Punkte betreffen in besonderer Weise kleinere und mittlere Unternehmen. Dabei hilft es auch nicht, wenn die Empfehlung in Nummer 28 vorsieht, dass sich Hostingdiensteanbieter im Rahmen freiwilliger Vereinbarungen untereinander austauschen sollen, um vor allem Anbietern zu helfen, die aufgrund ihrer Größe oder ihrer Reichweite über begrenzte Ressourcen und Fachkenntnisse verfügen. Zum einen ist vollkommen unklar, wie eine solche Hilfe aussehen sollte. Selbst wenn aber die großen Unternehmen ihr Know-how zur Verfügung stellen sollten, ist es für die allermeisten kleinen Unternehmen faktisch unmöglich, die Filter-Systeme zu implementieren oder zu fahren: Unternehmen nutzen beispielsweise vollkommen unterschiedliche Technologien, die nicht einfach kompatibel sind. Oder der „Empfang des Know-hows“ überfordert bereits die gesamte Rechenleistung des kleinen Unternehmens. Technisch denkbar wäre ausschließlich, dass jeder Unternehmer einen Inhalt an die großen Markteilnehmer schickt, damit diese ihn vor Upload durch ihre Filter spielen. Eine solche Lösung dürfte aber politisch kaum gewollt sein: So würde Europa alle Unternehmen abhängig von überwiegend nichteuropäischen Unternehmen machen. Dies ist nicht nur datenschutzrechtlich, sondern auch politisch kritisch zu hinterfragen.

Die in Nummern 24 und 38 der Empfehlung enthaltene Aufforderung an die Mitgliedstaaten, die Hostingdiensteanbieter rechtlich zu verpflichten, die Strafverfolgungsbehörden zu Zwecken der Verfolgung, Ermittlung etc. in bestimmten Fällen zu informieren, ist überflüssig. Bereits heute existieren in vielen Bereichen Arbeitsabläufe auf freiwilliger Basis, im Rahmen derer

Unternehmen die Behörden auf bestimmte Gefahren oder Belege für Straftaten hinweisen. Eine rechtliche Verpflichtung würde diese bewährten Strukturen gefährden.

Kapitel III – Besondere Empfehlungen zu terroristischen Inhalten

In Nummer 35 der Empfehlung ist zusätzlich geregelt, dass ein gemeldeter terroristischer Inhalt in aller Regel binnen einer Stunde ab Eingang der Meldung zu prüfen und gegebenenfalls zu entfernen oder sperren ist.

In den Erwägungen heißt es dazu, dass terroristische Inhalte binnen der ersten Stunde den größten Schaden anrichteten, ein Beleg zu dieser Theorie fehlt indes.

Es ist nochmals darauf hinzuweisen, dass alle Unternehmen ein starkes Eigeninteresse daran haben, jede Art terroristischer Inhalte umgehend von ihren Plattformen zu verbannen. Deshalb ist eine scharfe Regulierung in dieser Frage weder nachvollziehbar noch erscheint sie notwendig.

Für die Einführung starrer Fristen besteht in diesem Zusammenhang erst recht kein Anlass. Diese führen nur dazu, dass ein Unternehmen im Zweifel alles löscht, was auch nur annähernd verdächtig erscheinen könnte, ohne eine qualifizierte Prüfung vorzunehmen. Im Zweifel kann eine solche Praxis zu einer Einschränkung der Meinungsfreiheit führen. Zudem erscheint die Festsetzung der Frist willkürlich und ihre Einhaltung unrealistisch. Sogar große Unternehmen dürften mit der starren Frist vor eine große Herausforderung gestellt werden, die nicht nur im Einzelfall Probleme verursachen wird. Für jedes kleinere oder mittlere Unternehmen ist eine fristgerechte Reaktion in jedem Fall unmöglich.

Zusammenfassung

In der Empfehlung fällt auf, dass offensichtlich einige wenige große Unternehmen adressiert werden sollen. Durch die geforderten Maßnahmen könnte die Kommission aber das Gegenteil dessen erreichen, was gewünscht ist: Nämlich eine Verdrängung kleinerer Anbieter und einen Ausbau der Marktmacht einiger weniger großer.

Des Weiteren fehlt ein absoluter zentraler Bestandteil im Kampf gegen Terrorismus und Kinderpornographie fast völlig: der Aufbau einer konsequenten Strafverfolgung. Werden illegale Inhalte nur gelöscht, 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. Zudem werden so nur sehr wenige Täter ermittelt. Das ist im Sinne einer effizienten, ganzheitlichen Strategie gegen diese schweren Verbrechen nicht nachvollziehbar.

Über eco

eco - Verband der Internetwirtschaft e.V. ist Interessenvertreter und Förderer aller Unternehmen, die mit oder im Internet wirtschaftliche Wertschöpfung betreiben. Der Verband vertritt derzeit mehr als 1000 Mitgliedsunternehmen.

Hierzu zählen unter anderem ISP (Internet Service Provider), Carrier, Hard- und Softwarelieferanten, Content- und Service-Anbieter sowie Kommunikationsunternehmen. eco ist der größte nationale Internet-Service-Provider-Verband Europas.