EUROPÄISCHE
KOMMISSION

Brüssel, den 12.9.2018
SWD(2018) 409 final

ARBEITSUNTERLAGE DER KOMMISSIONSDIENSTSTELLEN

ZUSAMMENFASSUNG DER FOLGENABSCHÄTZUNG

Begleitunterlage zum

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates

zur Verhinderung der Verbreitung terroristischer Online-Inhalte

{COM(2018) 640 final} - {SEC(2018) 397 final} - {SWD(2018) 408 final}

Zusammenfassung

Folgenabschätzung zur Verhinderung der Verbreitung terroristischer Online-Inhalte

A. Handlungsbedarf

Warum? Um welche Problematik geht es?

Die Verbreitung terroristischer Online-Inhalte stellt nach wie vor ein großes und dringliches gesellschaftliches und politisches Problem dar. Trotz einer Reihe nicht regulatorischer Maßnahmen werden Online-Hostingdienste auch weiterhin für die Verbreitung terroristischer Inhalte genutzt.

Was soll mit dieser Initiative erreicht werden?

Mit dieser Initiative soll ein größeres Vertrauen in das Online-Umfeld im digitalen Binnenmarkt geschaffen werden, indem die Verfügbarkeit terroristischer Online-Inhalte eingeschränkt und gleichzeitig ein hohes Maß an Sicherheit für die Bürgerinnen und Bürger der EU gewährleistet wird. Insbesondere soll die Wirksamkeit von Maßnahmen zur Erkennung und Entfernung terroristischer Inhalte sowie die Transparenz und Rechenschaftspflicht der Hostingdiensteanbieter erhöht werden. Die Initiative zielt auch darauf ab, die zuständigen Behörden besser in die Lage zu versetzen, gegen terroristische Inhalte im Internet vorzugehen. Zudem soll das Risiko einer irrtümlichen Entfernung legaler Inhalte gering gehalten und ein angemessener Schutz der Grundrechte gewährleistet werden.

Worin besteht der Mehrwert des Tätigwerdens auf EU-Ebene?

Die meisten Online-Plattformen sind grenzüberschreitend tätig und ermöglichen den Zugang zu Inhalten unabhängig davon, wo die Nutzer oder Anbieter der Informationen niedergelassen sind. Die Mitgliedstaaten haben Rechtsvorschriften für die Entfernung illegaler Inhalte im Internet erlassen, jedoch muss die Notwendigkeit zur Gewährleistung der öffentlichen Sicherheit auf nationaler Ebene gegen die Wahrung der Dienstleistungsfreiheit und der Niederlassungsfreiheit nach den Regeln des Binnenmarktes abgewogen werden.

Ein Flickenteppich an nationalen Vorschriften ist im Begriff zu entstehen und sich auszubreiten. Dies würde aufgrund höherer Befolgungskosten für die Unternehmen die effektive Ausübung der Niederlassungsfreiheit und der Dienstleistungsfreiheit in der EU gefährden und gleichzeitig die Wirksamkeit der Bekämpfung terroristischer Inhalte im Internet einschränken.

Angesichts der Art der betreffenden Dienstleistungen und der sich abzeichnenden Fragmentierung des Binnenmarkts lässt sich die Herausforderung, die Verfügbarkeit illegaler Online-Inhalte zu begrenzen, durch Maßnahmen der Mitgliedstaaten allein nicht wirksam angehen.

B. Lösungen

Welche gesetzgeberischen und sonstigen Maßnahmen wurden erwogen? Wird eine davon bevorzugt? Warum?

In der Folgenabschätzung wurden zusätzlich zum Basisszenario drei Optionen mit ähnlicher Interventionslogik, jedoch mit unterschiedlicher Intensität in Bezug auf die Wirksamkeit und die Auswirkungen auf die Grundrechte, geprüft. Die grundlegenden Elemente für diese Optionen umfassen:

Bestimmungen zur **Harmonisierung der Verfahren zur Entfernung oder Sperrung terroristischer Inhalte** im Anschluss an eine Entfernungsanordnung einer nationalen Behörde. Um diese Verfahren zu ermöglichen, geht mit der Harmonisierung eine **gemeinsame Definition des Begriffs „terroristischer Inhalt" im Internet** (wobei die drei Optionen unterschiedliche Definitionen vorsehen) sowie eine Klarstellung der verfügbaren **Rechtsbehelfe** für Hostingdiensteanbieter und Inhalteanbieter gegen Entfernungsanordnungen (bei allen Optionen) einher.

Bestimmungen zur Gewährleistung **transparenter Verfahren und der Berichterstattung** an die Behörden und die Kommission (bei allen drei Optionen ähnlich) würden die Rechenschaftspflicht und das Vertrauen in die Inhaltsmoderation stärken, die politischen Entscheidungsträger und die nationalen Behörden bei der Bekämpfung terroristischer Inhalte unterstützen und darüber hinaus dazu beitragen, dass die Nutzer besser

verstehen, wie Hostingdiensteanbieter ihre Inhalte verwalten.

Die Zusammenarbeit zwischen den nationalen Behörden und Europol (je nach Option in unterschiedlichem Umfang) würde deren GeltuFähigkeit verbessern, gemeinsam gegen terroristische Inhalte vorzugehen und Doppelarbeit zu vermeiden. Im Zusammenhang mit der grenzüberschreitenden Erbringung von Diensten würden sich für die Hostingdiensteanbieter die Komplexität bei der Abstimmung mit den nationalen Behörden sowie die damit verbunden Kosten verringern.

Zudem Bestimmungen, mit denen sichergestellt wird, dass die Hostingdiensteanbieter in den Fällen, in denen Unternehmen terroristischen Inhalten ausgesetzt sind, **geeignete und angemessene Maßnahmen treffen, um terroristische Inhalte proaktiv zu erkennen** (je nach Option unterschiedliche Anforderungen).

Schutzvorkehrungen (bei allen Optionen) und Bestimmungen, mit denen sichergestellt wird, dass Maßnahmen zur Erkennung und Entfernung terroristischer Inhalte nicht zur irrtümlichen Entfernung legaler Inhalte oder zu einer Verletzung der Grundrechte führen.

Bestimmungen zur **Sicherstellung der Durchsetzbarkeit der Maßnahmen** (bei allen Optionen), einschließlich der Einführung gesetzlicher Vertreter für Nicht-EU-Unternehmen, der Einrichtung von Kontaktstellen und der Sicherstellung, dass die Mitgliedstaaten über ein kohärentes Sanktionspaket verfügen.

Der Bericht enthält eine Kombination der Maßnahmen, die im Hinblick auf die Bekämpfung terroristischer Online-Inhalte als besonders wirksam bewertet wurden. Er enthält zudem eine Bewertung der Vorteile verschiedener Elemente in Bezug auf ihre Wirksamkeit.

Die Folgenabschätzung kommt zu dem Schluss, dass die Berücksichtigung folgender Maßnahmen wirksamer zur Erreichung der politischen Ziele beitragen würde: eine umfassende Definition terroristischer Inhalte, die Anforderung, Inhalte infolge einer Entfernungsanordnung innerhalb einer Stunde zu entfernen, die Anforderungen zur Prüfung von Meldungen durch Europol und die Mitgliedstaaten und die Anforderung an Hostingdiensteanbieter, die terroristischen Inhalten ausgesetzt sind, proaktiv tätig zu werden, um neue terroristische Inhalte zu erkennen und das erneute Hochladen bereits bekannten Materials zu verhindern, sowie ein solides Paket mit Schutzvorkehrungen gegen die irrtümliche Entfernung legaler Inhalte und Transparenzanforderungen.

Wer unterstützt welche Option?

Die Hostingdiensteanbieter unterstützen in der Regel das Basisszenario und sind der Ansicht, dass zunächst die Auswirkungen nicht regulatorischer Maßnahmen umfassend bewertet werden sollten. Sollte ein Rechtsinstrument angenommen werden, unterstützen sie eine gezielte Intervention in spezifischen Bereichen, die von besonderem Wert für die Öffentlichkeit sind.

Die Mitgliedstaaten sind sich dessen bewusst, dass weitere Unterstützungsmaßnahmen (d. h. Weiterentwicklung des Basisszenarios) erforderlich sind und unterstützen eine Intervention, die sich gezielt gegen terroristische Inhalte richtet. Die Mitgliedstaaten haben insbesondere auf die Notwendigkeit einer gemeinsamen Definition des Begriffs „terroristischer Inhalt“ hingewiesen sowie darauf, dass Anforderungen an aufgrund einer Meldung ergriffene Maßnahmen, Anforderungen an proaktive Maßnahmen sowie Transparenzanforderungen festgelegt und Maßnahmen getroffen werden müssen, die den Zugang zu entfernten Inhalten zu Strafverfolgungszwecken erleichtern. Der Europäische Rat hat die Kommission aufgefordert, „einen Gesetzgebungsvorschlag zur Verbesserung der Erkennung und Entfernung von Inhalten, die Hass schüren und zu terroristischen Handlungen anstiften, zu unterbreiten.“

Die Zivilgesellschaft, die digitale Rechte vertritt, und die Wissenschaft haben sich für die Weiterentwicklung des Basisszenarios ausgesprochen. Sie rieten im Hinblick auf einige in den Regelungsoptionen enthaltene Komponenten, insbesondere in Bezug auf proaktive Maßnahmen und die Auswirkungen auf die Grundrechte, zur Vorsicht. Diese Bedenken werden von Einzelpersonen in ihren Antworten im Rahmen der öffentlichen Konsultation geteilt. Eine repräsentative Auswahl an Bürgerinnen und Bürgern, die an einer gezielten Eurobarometer-Umfrage teilnahmen, unterstützte zusätzliche Maßnahmen gegen illegale Online-Inhalte auf EU-Ebene.

C. Kosten und Nutzen der bevorzugten Option

In dieser Folgenabschätzung werden die Kosten und Nutzen der im Rahmen jeder Option vorgesehenen Maßnahmen aufgeschlüsselt. Die Folgenabschätzung kommt zu dem Schluss, dass Option 3 die wirksamste

Option darstellt. Diese Option würde erheblich dazu beitragen, die politischen Ziele zu erreichen und in Bezug auf Umfang und Reichweite des Problems größtmöglichen Nutzen zu erzielen. Es wird davon ausgegangen, dass die dritte Option in Bezug auf die zu erwartenden Kosten und den zusätzlichen Verwaltungsaufwand zwar die größten wirtschaftlichen Auswirkungen, aber auch den größten Nutzen mit sich bringen wird.

D. Folgemaßnahmen

Wann werden die Maßnahmen überprüft?

Es wird ein detailliertes Programm zur Überwachung der Leistungen, Ergebnisse und Auswirkungen der Rechtsvorschriften erstellt, um die Bewertung zu erleichtern. Die Überwachung wird in erster Linie auf der Grundlage von Informationen aus den Mitgliedstaaten erfolgen, die von den zuständigen Behörden im Rahmen ihrer Tätigkeit gesammelt wurden, ergänzt durch öffentlich zugängliche Transparenzberichte. Andere Daten, insbesondere über proaktive Maßnahmen, werden von den Hostingdiensteanbietern im Rahmen ihrer Berichterstattungspflichten zur Verfügung gestellt. Diese Überwachung wird in allen Optionen durch Forschungsarbeiten ergänzt, um die Verbreitung illegaler Online-Inhalte besser zu verstehen und die technologische Entwicklung automatisierter Werkzeuge für die Entfernung illegaler Inhalte zu verfolgen.