Auf einen Blick

Digital Services Act | Revision der E-Commerce Richtlinie

Ausgangslage

Die E-Commerce Richtlinie wurde am 8. Juni 2000 verabschiedet. Derzeit wird in den europäischen Institutionen ein "Digital Services Act" (DSA) diskutiert, der sich unter anderem auf Themen bezieht, die bislang in den Regelungsbereich der E-Commerce Richtlinie fallen, und der zu einer Überarbeitung der Richtlinie führen kann. Zwar gibt es bislang noch keine formellen Vorschläge. Bitkom möchte sich dennoch gern im Vorfeld der Konsultation mit den folgenden Eckpunkten konstruktiv in die Diskussion rund um Fragen der Haftung von Diensteanbietern einbringen.

Das Wichtigste

- Die geplante Gesetzesnovelle sollte dazu genutzt werden, für die Anbieter digitaler Dienste einen klaren, einheitlichen und aktuellen, innovationsfreundlichen Rechtsrahmen für die Bekämpfung illegaler Inhalte zu schaffen; dabei sind der Schutz und die Befähigung der Nutzer beim Zugriff auf digitale Dienste zentral. Außerdem ist es wichtig, die erforderliche Zusammenarbeit zwischen den Mitgliedstaaten sowie eine angemessene Aufsicht über die Anbieter digitaler Dienste in der EU sicherzustellen. Dienste, die auf dem europäischen Markt aktiv sind, müssen sich an die in der EU geltenden Rechtsvorschriften halten. Dafür ist es von entscheidender Bedeutung, dass alle relevanten Akteure zusammenarbeiten, um einen funktionierenden digitalen Binnenmarkt und einen ausreichenden Schutz für Verbraucher zu gewährleisten.

- Die E-Commerce Richtlinie ist ein Grundbaustein für den Erfolg des Internets und hat das Entstehen erfolgreicher Dienste entscheidend mit ermöglicht. Ohne das sogenannte Haftungsprivileg, das Herkunftslandprinzip und das Verbot einer allgemeinen Überwachungspflicht, welche durch die Richtlinie etabliert wurden, hätte sich die Internetwirtschaft vermutlich nicht so entwickeln können, wie wir es heute sehen. Dieses gilt es für alle Diensteanbieter beizubehalten. Heute, wie vor 20 Jahren, sind die Grundregeln der Richtlinie von herausragender Bedeutung für die Funktion der digitalen Wirtschaft. Gleichzeitig hat die gesellschaftliche und wirtschaftliche Bedeutung von Diensten der Informationsgesellschaft aber massiv zugenommen, was teils neue politische Herausforderungen schafft.

- Wichtig ist die Unterscheidung zwischen der Übernahme freiwilliger Verantwortung und rechtlicher Haftung. Unter Beibehaltung des allgemeinen Haftungsprivilegs sollten Möglichkeiten der Verantwortungsübernahme, abhängig von und differenziert nach der Art des Diensteanbieters und des Inhalts, diskutiert werden. Es sollten außerdem Anreize für die Diensteanbieter geschaffen werden, freiwillige proaktive Maßnahmen zu ergreifen.

- Mit Blick auf Haftungsfragen unterstützen wir den Plan, auf EU-Ebene eine Konkretisierung und begriffliche Aktualisierung in Bereichen vorzunehmen, in denen die E-Commerce Richtlinie nicht mehr den technischen und marktbedingten Fortschritt widerspiegelt.

Eckpunktepapier

Eckpunkte für eine Revision der E-Commerce Richtlinie/ einen Vorschlag zu einem Digital Services Act | Haftungsfragen

05. Mai 2020

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

Marie Anne Nietan
Referentin Medienpolitik
T +49 30 27576-221
m.nietan@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Zusammenfassung

Die Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (E-Commerce Richtlinie - eCD) wurde am 8. Juni 2000 verabschiedet. Derzeit wird in den europäischen Institutionen ein "Digital Services Act" (DSA) diskutiert, der sich unter anderem auf Themen bezieht, die bislang in den Regelungsbereich der E-Commerce Richtlinie fallen, und der zu einer Überarbeitung der Richtlinie führen kann. Zwar gibt es bislang noch keine formellen Vorschläge. Bitkom möchte sich dennoch gern im Vorfeld der Konsultation mit den folgenden Eckpunkten konstruktiv in die Diskussion rund um Fragen der Haftung von Diensteanbietern einbringen.

Die geplante Gesetzesnovelle sollte dazu genutzt werden, für die Anbieter digitaler Dienste einen klaren, einheitlichen und aktuellen, innovationsfreundlichen Rechtsrahmen für die Bekämpfung illegaler Inhalte zu schaffen; dabei sind der Schutz und die Befähigung der Nutzer beim Zugriff auf digitale Dienste zentral. Außerdem ist es wichtig, die erforderliche Zusammenarbeit zwischen den Mitgliedstaaten sowie eine angemessene Aufsicht über die Anbieter digitaler Dienste in der EU sicherzustellen. Dienste, die auf dem europäischen Markt aktiv sind, müssen sich an die in der EU geltenden Rechtsvorschriften halten. Dafür ist es von entscheidender Bedeutung, dass alle relevanten Akteure zusammenarbeiten, um einen funktionierenden digitalen Binnenmarkt und einen ausreichenden Schutz für Verbraucher zu gewährleisten.

Gerade deshalb möchten wir auf einige wichtige Punkte hinweisen, die bei einer Revision unbedingt bedacht werden sollten, um die genannten Ziele zu erreichen und gleichzeitig übermäßige Regulierung mit potenziellen Kollateralschäden bzw. unerwünschten Nebeneffekten zu verhindern. Wir plädieren für eine angemessene, auf die zu erreichenden Ziele zugeschnittene Regulierung mit Augenmaß.

Zunächst sollten die jüngsten legislativen Maßnahmen (z.B. die Richtlinie über audiovisuelle Mediendienste, die Platform-to-Business (P2B) Verordnung und die Verordnung

über Marktüberwachung und Konformität von Produkten) beachtet und laufende legislative Prozesse (z.B. die Verordnung zur Verhinderung der Verbreitung terroristischer Inhalte online) antizipiert werden, um Kohärenz sicherzustellen. Wo kein weitergehender Regulierungsbedarf für spezifische Themen/Branchen besteht, sollte der DSA keine Neuregelungen schaffen.

Die E-Commerce Richtlinie ist ein Grundbaustein für den Erfolg des Internets und hat das Entstehen erfolgreicher Dienste entscheidend mit ermöglicht. Ohne das sogenannte Haftungsprivileg und das Verbot einer allgemeinen Überwachungspflicht, welche durch die Richtlinie etabliert wurden, hätte sich die Internetwirtschaft vermutlich nicht so entwickeln können, wie wir es heute sehen; Diensteanbieter stünden vor erheblichen Herausforderungen, die oftmals die Entwicklung neuer Dienste, Plattformen und Geschäftsmodelle erheblich erschweren würden.

Ähnlich wichtig für den Erfolg von Internetdiensten in Europa ist das in der Richtlinie verankerte Herkunftslandprinzip, welches es in der EU niedergelassenen Diensteanbietern ermöglicht, ihre Waren und Dienstleistungen in der gesamten EU anzubieten, ohne jeweils verschiedene, einzelstaatliche Regelungen beachten zu müssen. Dieses Prinzip war und ist maßgeblicher Motor für den wirtschaftlichen Erfolg der europäischen und internationalen Internetwirtschaft, den es zu erhalten gilt.

Heute, wie vor 20 Jahren, sind die Grundregeln der eCD von herausragender Bedeutung für die Funktion der digitalen Wirtschaft. Gleichzeitig hat die gesellschaftliche und wirtschaftliche Bedeutung von Diensten der Informationsgesellschaft aber massiv zugenommen, was teils neue politische Herausforderungen schafft. Im Rahmen konkreter Fallgestaltungen gibt es zudem eine Vielzahl an bereits gesetzlich manifestierter oder aber gesellschaftlich wie wirtschaftlich notwendiger Verantwortung von Diensten der Informationsgesellschaft.

Mit Blick auf Haftungsfragen unterstützen wir den Plan, auf EU-Ebene eine Konkretisierung und begriffliche Aktualisierung in Bereichen vorzunehmen, in denen die eCD nicht mehr den technischen und marktbedingten Fortschritt widerspiegelt. Auch könnte bewertete werden, ob und inwiefern eine Konkretisierung und Harmonisierung des Notice-and-Take-Down-Verfahrens notwendig ist. Wir warnen jedoch eindrücklich davor, allen Diensten der Informationsgesellschaft eine allgemeine Verpflichtung aufzuerlegen, jegliche Inhalte, die im Internet entstehen, verbreitet und geteilt werden, zu beobachten und zu kontrollieren. Eine solche Verpflichtung würde einen Großteil der Anbieter daran hindern, ihre Dienste überhaupt anzubieten. Vielmehr plädieren wir für einen differenzierten Ansatz, orientiert an der Art der Inhalte und angebotenen Dienste.

Zu den Überlegungen im Einzelnen

1. **Haftungsprivileg beibehalten:** Das sogenannte Haftungsprivileg bzw. das System der abgestuften Haftung, welches die eCD für die verschiedenen Dienste der Informationsgesellschaft festschreibt (Artikel 12-14 eCD), muss dringend erhalten bleiben. Es ist, wie eingangs beschrieben, der Grundbaustein für den Erfolg und Bestand des freien Internets und hat das Entstehen erfolgreicher Dienste entscheidend mit ermöglicht.

2. **Herkunftslandprinzip stärken:** Bitkom spricht sich insbesondere mit Blick auf Haftungsregeln gegen eine Abkehr vom und für eine Stärkung des Herkunftslandprinzips (Artikel 3 (2) eCD) aus, da dieses eine Grundvoraussetzung für die freie Wahl des Niederlassungsortes von Anbietern und den freien Verkehr von digitalen Diensten im Digitalen Binnenmarkt in der Europäischen Union darstellt.

3. **Verbot allgemeiner Überwachungspflichten wahren:** Das Verbot der Auferlegung einer allgemeinen Überwachungspflicht für alle Dienste der Informationsgesellschaft (Artikel 15 eCD) sollte in jedem Fall beibehalten werden, da dieses einen weiteren Grundbaustein der Internetregulierung darstellt und eine wichtige Voraussetzung für das Entstehen und die Fortentwicklung von Plattformen und weiteren Diensten ist. Die Ermöglichung einer derart pauschalen Überwachungspflicht ist nicht die Lösung für die komplexen Herausforderungen, die durch illegale Inhalte entstehen, und bietet enorme Risiken für Kollateralschäden. Wir sind ermutigt durch die Zusagen der Kommission, das Verbot der Implementierung einer „allgemeinen Überwachungspflicht“ aufrechtzuerhalten.

   Wichtig ist auch, dass dieses Verbot nicht ausgehöhlt wird, durch eine Berufung auf die in Erwägungsgrund 47 von dem Verbot ausgenommene Auferlegung von „Überwachungspflicht in spezifischen Fällen“. Entsprechende Entscheidungen des Europäische Gerichtshofes machen deutlich, dass eine spezifische Überwachungspflicht nur solche Fälle umfasst, in denen nicht jeder hochgeladene Inhalt auf unbestimmte Zeit auf das Vorhandensein bestimmter Rechtsverletzungen hin überprüft wird.

4. **Horizontaler, aber trotzdem differenzierter Regulierungsansatz:** Grundsätzlich begrüßen wir, dass der horizontale Regulierungsansatz der E-Commerce Richtlinie, welcher jegliche Dienste der Informationsgesellschaft mit einschließt, weiter entwickelt werden soll. Die zentralen, grundlegenden, allgemeingültigen und damit horizontal anwendbaren Prinzipien der Richtlinie, wie das Haftungsprivileg, das Verbot der allgemeinen Überwachungspflicht und das Herkunftslandprinzip, gilt es, für alle Dienste zu wahren.

Darüber hinaus gilt es jedoch zu berücksichtigen, dass diese Dienste durch sehr unterschiedliche Geschäftsmodelle geprägt sind und es, jenseits der allgemeingültigen Prinzipien, keine „one-size-fits-all Lösungen" im Umgang mit rechtswidrigen Inhalten geben kann. Daher müssen diese Unterschiede bei der Ausgestaltung der Rechte und Pflichten und insbesondere der Bestimmung von zumutbaren Maßnahmen, die durch die Anbieter ergriffen werden können, im Blick behalten werden.

5. **Technische Architektur der Dienste berücksichtigen:** Das aktuelle Regime der E-Commerce Richtlinie unterscheidet bei Diensten der Informationsgesellschaft zwischen „Reinen Durchleitern", deren Dienst darin besteht, „von einem Nutzer eingegebene Informationen in einem Kommunikationsnetz zu übermitteln oder Zugang zu einem Kommunikationsnetz zu vermitteln" (Artikel 12 eCD), Diensten die „Caching" betreiben, also eine „automatische, zeitlich begrenzte Zwischenspeicherung", von Informationen, „die dem alleinigen Zweck dient, die Übermittlung der Information an andere Nutzer auf deren Anfrage effizienter zu gestalten" (Artikel 13 eCD), und „Hosting Providern", deren Dienst in der „Speicherung von durch einen Nutzer eingegebenen Informationen" besteht (Artikel 14 eCD). Jeder dieser Anbieter kann von dem Haftungsprivileg profitieren, allerdings unter unterschiedlichen Bedingungen. Dieser horizontale aber trotzdem differenzierte Ansatz ist wichtig, da er die unterschiedliche technische Architektur der Dienste berücksichtigt und damit den tatsächlichen Einblick bzw. die tatsächlichen Möglichkeiten des jeweiligen Anbieters im Umgang mit rechtswidrigen Inhalten. Internet Access Provider bspw. haben weder Kenntnis noch Kontrolle über die Informationen, die über Ihr Kommunikationsnetz vermittelt werden, auch weil Regulierung zur Netzneutralität dies untersagt.

Unter Umständen ist es angebracht, die bestehenden Angebotskategorien der eCD (Host-Provider, Access-Provider, Caching-Provider) um weitere Kategorien mit spezifischen Regelungen zu ergänzen oder zu unterteilen, ebenfalls unter Berücksichtigung der technischen Architektur der Diensteanbieter. Clouddienste beispielsweise agieren eher passiv und haben meist weder Kenntnis von noch Kontrolle über die Inhalte, die auf ihrer Plattform gespeichert werden. Diese Dienste sind daher angesichts ihrer technischen Architektur und der vertraglichen Beziehungen, die sie mit ihren Nutzern unterhalten, in ihren Möglichkeiten, illegale Inhalte, die von ihren Nutzern hochgeladen werden, zu bekämpfen, stärker eingeschränkt. Von diesen passiv agierenden Diensten die gleichen Anstrengungen zur Verwaltung von Inhalten zu erwarten, wie sie von öffentlich zugänglichen Diensten zur gemeinsamen Nutzung von Inhalten verlangt werden, widerspricht ihrem technischen und operationellen Charakter und würde zu ungerechtfertigten Datenschutz-, Sicherheits- und kommerziellen Überschneidungen führen. Als Kriterium der Unterscheidung zwischen Diensten könnte daher ebenfalls hinzugezogen werden, ob ein Dienst das Teilen von Inhalten mit der Öffentlichkeit erlaubt.

6. **Berücksichtigung unterschiedlicher Sektoren und Inhalte**: Auch innerhalb der Kategorie der Hosting Provider sind Diensteanbieter in verschiedensten Sektoren betroffen – von sozialen Netzwerken über Anbieter von Kurzzeitvermietung bis zu Online-Marktplätzen. Außerdem steht eine Vielzahl unterschiedlicher Inhalte im Fokus – von audiovisuellen Medien oder user-generated-content über Angebote von Ferienhäusern bis zum Angebot von physischen Gütern. Ein differenzierter Ansatz bei der Ausgestaltung der Rechte und Pflichten der Diensteanbieter und insbesondere der Bestimmung von zumutbaren Maßnahmen, die durch die Anbieter ergriffen werden können, sollte auch den unterschiedlichen Arten von Inhalten und möglichen Maßnahmen zum Umgang mit diesen Inhalten Rechnung tragen. Zentral ist bei der Differenzierung der Inhalte auch das jeweilige Gefährdungspotenzial.

7. **Verhältnismäßigkeit & Schwellenwerte:** In der öffentlichen Debatte geht es meist um Dienste mit einer großen Marktpräsenz und Reichweite. Bestimmte Regulierung an Schwellenwerte, wie z.B. Nutzerzahlen, zu knüpfen spiegelt grundsätzlich den Gedanken der Verhältnismäßigkeit wider – dass kleine Unternehmen nicht die gleichen Verpflichtungen auferlegt werden sollten wie großen, die mehr Ressourcen zur Verfügung haben – und den Umstand, dass Dienste mit hohen Nutzerzahlen eine größere gesellschaftliche und wirtschaftliche Relevanz haben. Auch wenn dieser Gedanke der Verhältnismäßigkeit grundsätzlich richtig ist, ist es häufig sehr schwierig und auch den Gegebenheiten des Marktes ggf. nicht durchgängig angemessen, Regulierung an konkrete Schwellenwerte zu knüpfen. Mit Schwellenwerten, also einem strikt quantitativen Ansatz, verknüpft ist immer eine Gefahr der rechtlichen Ungenauigkeit bis hin zur Umgehung. Überdies können abhängig von der Regelung Wettbewerbsverzerrungen die Folge sein, wenn Mitbewerber in verschiedenem Maße regulatorischer Intervention ausgesetzt sind. Bei manchen Regelungen ist eine pauschale Begrenzung auf z.B. große Marktspieler sicher nicht angemessen, z.B. bei Notice-and-Take-Down. Hier würde dem Ziel der Entfernung illegaler Inhalte zuwider laufen, wenn lediglich große Unternehmen dem nachkommen würden.

8. **Kleine Unternehmen schützen:** Unabhängig von potentiellen Regeln auf der Grundlage des Marktstatus sollte die Regulierung für Unternehmen, insbesondere kleinere Unternehmen, keine übermäßige Belastung darstellen. Die Regierungen sollten mehr Ressourcen zur Unterstützung von Kleinst- und Kleinunternehmen mit geringen Ressourcen bereitstellen. Für Startups und kleinere Anbieter kann es eine Herausforderung sein, erhebliche Investitionen in die Entwicklung neuer Technologien zu tätigen, um die Sicherheit ihrer Benutzer zu gewährleisten.

9. **Notice-and-Take-Down Verfahren:** Innerhalb des bestehenden Regimes ist eine Verbesserung des Notice-and-Take-Down Verfahrens auf europäischer Ebene dort notwendig, wo Defizite festgestellt werden. Diese Verfahren müssen einen soliden Satz von Grundrechtsgarantien enthalten und bestehende Rechtsunsicherheiten beseitigen. Für das Notice-and-Take-Down Verfahren sind Leitlinien dazu erforderlich, welche Bedingungen eine Mitteilung erfüllen muss, um gültig zu sein, sowie was notwendig ist, um unzulässige Mitteilungen, Fehler und Missbrauch zu verhindern. Für alle Rechtsbehelfs- und Anti-Missbrauchsmechanismen sind Informationen entscheidend für die Identifizierung. Je konkreter die Voraussetzungen für eine Mitteilung sind, umso besser, fehlerfreier und schneller kann eine Bearbeitung und Reaktion erfolgen.

   Zudem könnte einheitlich geregelt werden, was im strittigen Fall eines take-down zu tun ist. Wichtig ist hierbei zu beachten und anzuerkennen, dass verschiedene Anbieter aufgrund der unterschiedlichen Dienste und Inhalte unterschiedlichen Herausforderungen gegenüberstehen, die unterschiedlich durch Notice-and-Take-Down beantwortet werden können. So haben die Anbieter auch unterschiedliche Anforderungen an ein Notice-and-Take-Down-Verfahren. Notice-and-Take-Down Verfahren müssen in jedem Fall die Besonderheiten der jeweiligen Sektoren berücksichtigen und sich stets am Prinzip der Verhältnismäßigkeit orientieren und gegebenenfalls unterschiedlich ausgestaltet sein. Alternativ wäre ein Counternotice-Verfahren entsprechend der Regelungen im DMCA anzudenken. Leider kann es auch zu missbräuchlicher und geschäftsgefährdender Inanspruchnahme des Notice-and-Take-Down Verfahrens kommen. Dies muss Berücksichtigung finden, z.B. durch explizite Regelungen zum Umgang mit (wiederholt) missbräuchlichen Mitteilungen.

10. **Flexibilität statt starren Fristen:** Grundsätzlich warnen wir davor, zu starren Fristen für das Entfernen von Inhalten zu greifen. Der Begriff „unverzüglich“, wie er aktuell in der e-Commerce Richtlinie zu finden ist, bietet die nötige Flexibilität, welche die unterschiedlichen Arten von rechtswidrigen Inhalten sowie von Diensten verlangen, und stellt trotzdem die Dringlichkeit der Bearbeitung dar.

11. **Anreize für proaktive Maßnahmen setzen:** Insbesondere Hosting Provider sollten dazu ermutigt werden, proaktive freiwillige Maßnahmen zu ergreifen, um illegale und potenziell schädliche Inhalte von ihren Plattformen zu entfernen. Es sollte also klargestellt werden, dass diese Bemühungen das Fortgelten des Haftungsprivilegs unangetastet lassen. Proaktive Maßnahmen können in der Tat dazu führen, dass der Anbieter Kenntnis über illegale Aktivitäten oder illegale Informationen erlangt. In solchen Fällen hat der Hosting-Provider jedoch die Möglichkeit zu handeln und die fraglichen Informationen zu entfernen oder den Zugang zu ihnen zu sperren, sobald er von ihnen Kenntnis erlangt hat. Wenn der Hosting-Provider dies tut, profitiert er weiterhin von der Haf-

tungsbefreiung. Dies entspricht der Mitteilung der EU Kommission von 2017 zum Umgang mit illegalen Online-Inhalten[1] (S. 12-14).

Es sollte zusätzlich klargestellt werden, dass proaktive Maßnahmen nicht dazu führen, dass der Hosting Provider automatisch Kenntnis über alle von ihm gespeicherten Informationen hat. Deshalb ist es wichtig, rechtliche Klarheit über den Wissensstandard im Rahmen des Haftungsschutzregimes zu schaffen. Klarzustellen wäre in diesem Kontext Folgendes:
a) wenn ein Diensteanbieter freiwillig einige Inhalte überprüft hat, um sicherzustellen, dass sie nicht gegen ein oder mehrere Gesetze verstoßen, wird davon ausgegangen, dass dieser Anbieter keine Kenntnis von der Rechtswidrigkeit anderer Inhalte auf seiner Plattform hat, die er nicht für solche Zwecke überprüft hat; und
b) wenn ein Diensteanbieter freiwillig Inhalte auf seiner Plattform überprüft hat, um Inhalte zu entfernen, die gegen ein bestimmtes Gesetz verstoßen, wird davon ausgegangen, dass dieser Anbieter keine Kenntnis von allen anderen möglichen Rechtsverstößen hat, die derselbe Inhalt ebenfalls erfüllen könnte, die aber nicht Teil der Überprüfung waren.

Ohne eine solche Klarheit könnte das Risiko, dass einem Dienstanbieter, der in gutem Glauben proaktive Maßnahmen ergreift, Kenntnis aller Inhalte seines Dienstes unterstellt wird, als Abschreckung dafür wirken, solche verantwortungsvollen Schritte zu unternehmen. Darüber hinaus sind auch Regelungen denkbar, die positive Anreize zur Einführung solcher freiwilliger Maßnahmen setzen – z.B. im Wege einer erleichterten Beweislastverteilung für entsprechende Anbieter.

12. **Verantwortung | Haftung:** Wichtig ist die Unterscheidung zwischen der Übernahme freiwilliger Verantwortung und rechtlicher Haftung. Unter Beibehaltung des allgemeinen Haftungsprivilegs sollten Möglichkeiten der Verantwortungsübernahme, abhängig von der Art des Diensteanbieters und des Inhalts, diskutiert werden.

13. **Grundrechte schützen:** Im Rahmen einer Regulierung von Diensteanbietern sind stets die fundamentalen Grundrechte zu beachten und durch entsprechende Schutzvorkehrungen zu sichern. Im Bereich der Anbieter von Medien und sozialen Netzwerken ist hier die Meinungsfreiheit hervorzuheben, im Bereich der Anbieter im Online-Handel ist es der freie Warenverkehr.

14. **Kundenschutzbestimmungen & Transparenz:** Die Kundenschutzbestimmungen, wie z.B. Transparenz, sind ein wichtiger Faktor des Vertrauens. Hier wurde auf EU-Ebene in den letzten Jahren bereits eine ganze Reihe von Verbraucherschutzvorschriften einge-

[1] https://ec.europa.eu/transparency/regdoc/rep/1/2017/DE/COM-2017-555-F1-DE-MAIN-PART-1.PDF

führt, zuletzt z.B. die sog. Modernisierungs-Richtlinie. Bestimmungen in der eCD werden inzwischen durch neue Gesetze überlagert. Fraglich ist daher, ob die anstehende Novelle den richtigen Rahmen für Verbraucherschutz darstellt.

Einige Diensteanbieter liefern daneben bereits Informationen, die über rechtliche Anforderungen hinausgehen. Unabhängig von ihrer Größe haben die Diensteanbieter ein starkes Interesse an dem Vertrauen ihrer Nutzer. Dort, wo dennoch Transparenz-Defizite auftreten, können weitere Kundenschutzvorschriften wie z.B. Transparenzverpflichtungen durchaus sinnvoll sein. Mit Blick auf mögliche neue Transparenzregeln für das Ranking auf Internetangeboten ist es wichtig zu verstehen, dass dieses von einer Vielzahl von Faktoren und Filtern beeinflusst wird. Außerdem sollte jede Transparenzverpflichtung Schutzmaßnahmen gegen die Weitergabe von Geschäftsgeheimnissen beinhalten. Keinesfalls sollten allgemeine Regelungen erwogen werden, die eine Offenlegung konkreter Algorithmen verpflichtend machen, da sie in vielen Fällen einen Kern des Geschäftsmodells eines Anbieters darstellen. Das Aufdecken zu vieler Informationen über die Funktionsweise von Algorithmen kann auch dazu führen, dass sie von betrügerischen Akteuren (Hackern, Spammern usw.) kompromittiert werden, was letztendlich zum Schaden für den Verbraucher führen kann. Vielmehr sollte allenfalls die Veröffentlichung generischer, nicht detaillierter, Informationen erforderlich sein. Dies wird in den entsprechenden Regelungen in der Modernisierungs-Richtlinie sowie der P2B Verordnung bereits entsprechend klargestellt.

Während bei einigen Diensteanbietern eine Überprüfung der Unternehmensidentität der Akteure auf der jeweiligen Plattform nützlich sein könnte, um schädliche Online-Akteure abzuschrecken und die Strafverfolgung zu unterstützen, muss die Einführung solcher Verpflichtungen verhältnismäßig sein und angemessene Schutzmaßnahmen zum Schutz der Privatsphäre der Nutzer im Rahmen legitimer und rechtmäßiger Aktivitäten beinhalten. Die Überprüfung muss sich auf Daten beschränken, die wirklich erforderlich sind und ausreichen, um den Zweck zu erfüllen.

15. **Schädliche vs. Illegale Inhalte**: Inhalte (insb. user generated content) auf Medienplattformen, die als „rechtmäßig, aber schädlich“ eingestuft werden, bspw. Falschnachrichten, können häufig besser durch Selbstregulierung als durch strikte regulatorische Vorgaben angegangen werden. Dies ist ein effizienteres Instrument in diesem Bereich, da durch größere Flexibilität und schnellere Anpassung die sich ständig ändernden schädlichen Inhalte besser berücksichtigt werden können. Vor allem aber ist der nötige rechtliche Rahmen zum Umgang mit diesen Inhalten ein ganz anderer als der bei illegalen Inhalten und es besteht ein stärkerer Zusammenhang zur Einschränkung von Persönlichkeitsrechten. Selbst die Bewertung, ob ein Inhalt rechtswidrig ist oder nicht, ist häufig sehr schwierig zu treffen. Ob ein Inhalt „schädlich“ ist, lässt sich oft noch weniger an-

hand klar definierter Kriterien entscheiden, da dies noch stärker vom jeweiligen Kontext/Nutzerkreis abhängt. Regelungen zu schädlichen Medieninhalten sollten nicht Gegenstand des Digital Services Acts sein und besser im Democracy Act adressiert werden. Gleichwohl muss es Anbietern weiterhin möglich sein, auf ihren Angeboten unerwünschte Inhalte nach eigenen (transparenten) Regeln zu moderieren.

16. **Rechtsdurchsetzung verbessern:** Die Verbesserung der Rechtsdurchsetzung ist ein zentraler Faktor und ist ein komplementärer Baustein zur Diskussion über die Einführung aktualisierter Verpflichtungen. Eine wichtige Rolle spielt hier eine angemessene, effiziente Aufsicht sowie die Durchsetzung der bestehenden Verpflichtungen. Hier ist auch eine bessere Kooperation zwischen nationalen Aufsichtsbehörden notwendig und eine Förderung dieser wünschenswert, um eine unterschiedliche Anwendung und Durchsetzung der EU-weit einheitlich gestalteten Vorschriften zu vermeiden und Konsistenz sicherzustellen. Außerdem würde das Instrument der Verordnung im Gegensatz zu dem der Richtlinie eine bessere Harmonisierung bieten können.