Durchsetzung von Regeln zu illegalen Inhalten und Desinformation online

IRIS

Eine Publikation
der Europäischen Audiovisuellen Informationsstelle

Europäische Audiovisuelle Informationsstelle

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

IRIS-6
Durchsetzung von Regeln zu illegalen Inhalten und Desinformation online
Europäische Audiovisuelle Informationsstelle, Straßburg, 2025
ISSN 2079-1062

Verlagsleitung – Pauline Durand-Vialle, Geschäftsführende Direktorin
Redaktionelle Betreuung – Maja Cappello, Leiterin der Abteilung für juristische Informationen
Europäische Audiovisuelle Informationsstelle

Redaktionelles Team – Sophie Valais, Diego de la Vega
Europäische Audiovisuelle Informationsstelle

Verfasser
Irène Bouhadana, Mark D. Cole, Roderick Flynn, William Gilles, Giovanni de Gregorio, Mariette Jones, Mehmet Bedii Kaya, Dariia Opryshko, Roxana Radu, Clara Rauchegger, Sandra Schmitz-Berndt und Krzysztof Wojciechowski

Übersetzung
Erwin Rohwer, Marco Polo Sarl, Anne-Lise Weidmann, Ulrike Welsche

Korrektur
Linda Birne, Aurélie Courtinat, Catherine Koleda, Udo Lücke, Sonja Schmidt

Redaktionsassistentin – Alexandra Ross
Presse und PR – Alison Hindhaugh, alison.hindhaugh@coe.int

Herausgeber
Europäische Audiovisuelle Informationsstelle
76, allée de la Robertsau, 67000 Straßburg, Frankreich
Tel.: +33 (0)3 90 21 60 00
iris.obs@coe.int
www.obs.coe.int

Titellayout – ALTRAN, Frankreich

Bitte zitieren Sie diese Publikation wie folgt:
Cappello M. (Hrsg.), *Durchsetzung von Regeln zu illegalen Inhalten und Desinformation online*, IRIS, Europäische Audiovisuelle Informationsstelle, Straßburg, Dezember 2025

In diesem Dokument/Bericht verwenden wir zur besseren Lesbarkeit und Verständlichkeit geschlechtsspezifische Begriffe. Wo immer möglich, streben wir eine geschlechtsneutrale Formulierung an. Bitte beachten Sie, dass alle Bezeichnungen geschlechtsneutral zu verstehen sind und alle Geschlechter gleichermaßen einschließen.

Durchsetzung von Regeln zu illegalen Inhalten und Desinformation online

Irène Bouhadana, Mark D. Cole, Roderick Flynn, William Gilles, Giovanni de Gregorio, Mariette Jones, Mehmet Bedii Kaya, Dariia Opryshko, Roxana Radu, Clara Rauchegger, Sandra Schmitz-Berndt und Krzysztof Wojciechowski

Europäische Audiovisuelle Informationsstelle

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Vorwort

„Die absolute Freiheit verhöhnt die Gerechtigkeit. Die absolute Gerechtigkeit leugnet die Freiheit. Um fruchtbar zu sein, müssen beide Konzepte sich gegenseitig begrenzen."[1] Albert Camus schrieb diesen Satz in seinem 1951 veröffentlichten Essay *Der Mensch in der Revolte*, nur wenige Jahre nach dem Zweiten Weltkrieg und dem Holocaust. Diese Kritik an revolutionären Bewegungen und ihren Auswüchsen sorgte unter den sogenannten Intellektuellen der damaligen Zeit für große Aufregung.

Rund fünfzig Jahre später brachte das Internet – eine weitere Revolution, die absolute Freiheit predigte – unvermeidlich eine Reihe von Auswüchsen mit sich, für die wir bis heute den Preis zahlen und gegen die wir nach wie vor ankämpfen.

Wie Camus jedoch feststellte, lassen sich absolute Gerechtigkeit und absolute Freiheit nicht gegeneinanderstellen; vielmehr müssen beide Konzepte in einem ausgewogenen Verhältnis zueinanderstehen, damit sie fruchtbar sein können.

Das Konzept der Meinungsfreiheit stößt an seine Grenzen, wenn es um die nationale Sicherheit, die territoriale Unversehrtheit oder die öffentliche Sicherheit, zur Aufrechterhaltung der Ordnung oder zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral, zum Schutz des guten Rufes oder der Rechte anderer, zur Verhinderung der Verbreitung vertraulicher Informationen oder zur Wahrung der Autorität und der Unparteilichkeit der Rechtsprechung geht. Beschränkungen dieser Art müssen jedoch gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig sein.

Dementsprechend können bestimmte Online-Inhalte als rechtswidrig angesehen werden und müssen vom Autor oder Herausgeber – entweder freiwillig oder nach einem Verwaltungs- oder Gerichtsbeschluss – entfernt werden. Auch wenn dies manchmal kompliziert sein mag, handelt es sich dennoch um eine einfache Strafverfolgungsmaßnahme. Schwieriger wird es, wenn es zu entscheiden gilt, welche Inhalte schädlich sind. Wie die Autorinnen und Autoren der vorliegenden Publikation ausführen, umfassen „schädliche Inhalte Material, das möglicherweise nicht rechtswidrig ist, aber dennoch als abträglich für Einzelne oder die Gesellschaft angesehen wird – zum Beispiel Desinformation, Fehlinformationen zum Thema Gesundheit oder Inhalte, die demokratische Prozesse unterminieren." Die Frage ist nun, wie man gegen Inhalte vorgehen kann, die nicht rechtswidrig sind und daher nicht durch Gesetze eingeschränkt werden. *Ja, da liegts*.[2]

Dieser Bericht, der in Zusammenarbeit mit dem Institut für Europäisches Medienrecht (EMR) und Fachleuten auf diesem komplexen Gebiet erstellt wurde, beschäftigt sich sehr umfassend mit der Durchsetzung von Regeln gegen rechtswidrige Inhalte und Desinformation im Internet. Auf der Grundlage des allgemeinen Rechtsrahmens der Europäischen Union und des Europarats und ihrer Plattformregulierung bietet der

---

[1] Camus, A., *L'Homme révolté* [Der Mensch in der Revolt], Gallimard, Folio essais, 1951, p. 363.

[2] Shakespeare, W.„*Ay, there's the rub", Hamlet*. Deutsche Übersetzung von August Wilhelm von Schlegel (1767–1845).

Bericht eine eingehende Analyse nationaler Beispiele aus ganz Europa, die die aktuelle Situation in diesem Bereich veranschaulichen.

Ich möchte allen Autorinnen und Autoren, die zu diesem Bericht beigetragen haben, für ihr engagiertes Mitwirken und ihre ausgezeichnete Arbeit herzlich danken (in der Reihenfolge der Kapitel): Mark D. Cole, Sandra Schmitz-Berndt, Roxana Radu, William Gilles, Irène Bouhadana, Dariia Opryshko, Mehmet Bedii Kaya, Roderick Flynn, Clara Rauchegger, Giovanni de Gregorio, Krzysztof Wojciechowski und Mariette Jones.

Lassen Sie mich – ohne den Schlussfolgerungen dieses interessanten Berichts vorgreifen zu wollen – mit einer persönlichen Überlegung schließen. Die Aufgabe, die Online-Welt zu regulieren, mag bisweilen übermenschlich erscheinen, und es gibt sicherlich noch unendlich viel zu tun, doch lassen Sie uns nicht den Glauben verlieren! Um noch einmal Albert Camus zu zitieren: „Wir nennen Aufgaben übermenschlich, wenn Menschen lange brauchen, um sie zu erledigen, das ist alles."[3]

Ich wünsche Ihnen eine angenehme und anregende Lektüre!

Maja Cappello

IRIS-Koordinatorin

Leiterin der Abteilung für juristische Informationen

Europäische Audiovisuelle Informationsstelle

[3] Camus, A., *L'Été* [Heimkehr nach Tipasa], 1954, Quarto Gallimard, Œuvres, 2013.

Inhaltsverzeichnis

Liste der Abkürzungen und Akronyme

ABl.	Amtsblatt der EU
AEP	*Autoritatea Electorală Permanentă* (Ständige Wahlbehörde, Rumänien)
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AGCOM	*Autorità per le Garanzie nelle Comunicazioni* (Kommunikationsbehörde, Italien)
ANCOM	*Autoritatea Națională pentru Administrare și Reglementare în Comunicații* (Nationale Verwaltungs- und Regulierungsbehörde im Bereich Kommunikation, Rumänien)
APIs	Application Programming Interface (Anwendungsprogrammierschnittstellen)
ARCOM	*Autorité de régulation de la communication audiovisuelle et numérique* (Regulierungsbehörde für audiovisuelle und digitale Kommunikation, Frankreich)
AS	Autonome Systeme
ASA	*Advertising Standard Authority* (Werbeaufsichtsbehörde, Vereinigtes Königreich)
AVMD-RL	Richtlinie über audiovisuelle Mediendienste
BAI	*Broadcasting Authority of Ireland* (Rundfunkbehörde, Irland)
BGH	Bundesgerichtshof (Deutschland)
BKA	Bundeskriminalamt (Deutschland)
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Deutschland)
BTK	*Bilgi Teknolojileri ve İletişim Kurumu* (Behörde für Informations- und Kommunikationstechnologien, Türkiye)
CAP	Committee of Advertising Practice (Ausschuss für Werbepraktiken, Irland)
CM/Rec	Committee of Ministers/Recommendation (Empfehlung des Ministerkomitee des Europarats)
CNA	*Consiliul Național al Audiovizualului* (Nationaler Audiovisueller Rat, Rumänien)
CnaM	*Coimisiún na Meán* (Medienkommission, Irland)
CPS	Core platform service (Zentraler Plattformdienst)

DDG	Digitale-Dienste-Gesetz (Deutschland)
DMA	Digital Markets Act (Gesetz über digitale Märkte)
DNS	Domain-Namen-System
DPI	Deep Packet Inspection
DSA	Digital Services Act (Gesetz über digitale Dienste)
DSB	Datenschutzbehörde
DSC	Digital Service Coordinator (auch Koordinator für digitale Dienste)
DSGVO	Datenschutz-Grundverordnung
DSM-RL	Digital Single Market Directive (Richtlinie über das Urheberrecht im digitalen Binnenmarkt)
EAD	Europäischer Auswärtiger Dienst
EAI	Europäische Audiovisuelle Informationsstelle
EC-RL	ECommerce-Richtlinie
EDMO	Europäische Beobachtungsstelle für digitale Medien
EDSA	Europäischer Datenschutzausschuss
EFCSN	Europäisches Netzwerk für Faktenprüfung
EFTA	Europäische Freihandelsassoziation
EGDD	Europäisches Gremium für digitale Dienste
EGMD	Europäisches Gremium für Mediendienste
EGMR	Europäischer Gerichtshof für Menschenrechte
EMFA	European Media Freedom Act (Europäisches Medienfreiheitfreiheitsgesetz)
EMR	Institut für Europäisches Medienrecht
EMRK	Europäische Menschenrechtskonvention
ERGA	Gruppe europäischer Regulierungsstellen für audiovisuelle Mediendienste
EU	Europäische Union
EU-GRC	EU-Grundrechtecharta
EUDI	Europäische digitale Identität
EuGH	Gerichtshof der Europäischen Union

EUR	Euro
EUV	Vertrag über die Europäische Union
EWR	Europäischer Wirtschaftsraum
FIMI	*Foreign information manipulation and interference* (Manipulation von Informationen und Einmischung aus dem Ausland)FIMI-SAC FIMI-Informationsaustausch- und Analysezentrum
GASP	Gemeinsame Außen- und Sicherheitspolitik
IP	Digitale Netzwerkadressen
IPbpR	Internationaler Pakt über bürgerliche und politische Rechte
IT	Informationstechnologien
IPCR	Integrated Political Crisis Response (Integrierte Regelung für die politische Reaktion auf Krisen)
JMStV	Jugendmedienschutz-Staatsvertrag
JORF	*Journal officiel de la République française* (Amtsblatt der Republik Frankreich)
KAS	*Krajowa Administracja Skarbowa* (Nationale Finanzverwaltung, Polen)
KDD	Koordinator für digitale Dienste
KDD-G	Koordinator-für-Digitale-Dienste-Gesetz (Österreich)
KI	Künstliche Intelligenz
KI-VO	KI-Verordnung
KoPl-G	Bundesgesetz über Maßnahmen zum Schutz der Nutzer auf Kommunikationsplattformen (Österreich)
KRRiT	Krajowa Rada Radiofonii i Telewizji (Nationaler Rundfunk- und Fernsehrat, Polen)
LCEN	*Loi pour la confiance dans l'économie numérique* (Gesetz über das Vertrauen in die digitale Wirtschaft, Frankreich)
MStV	Medienstaatsvertrag (Deutschland)
NaD	Netzwerk gegen Desinformation
NASK	*Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy* (Wissenschaftliches und Akademisches Computernetzwerk – Nationales Forschungsinstitut, Polen)

NetzDG	Netzwerkdurchsetzungsgesetz (Deutschland)
NCU	Nationales Zentrum für das betriebliche und technische Management von Telekommunikationsnetzen (Ukraine)
OSA	*Online Safety Act* (Gesetz über Online-Sicherheit, Vereinigtes Königreich)
OSMR	*Online Safety and Media Regulation Act* (Gesetz für Online-Sicherheit und Medienregulierung, Irland)
PACE	*Parliamentary Assembly of the Council of Europe* (Parlamentarische Versammlung des Europarats)
PERCI	*Plateforme Européenne de Retraits de Contenus illégaux sur Internet* (Europäische Plattform zur Bekämpfung illegaler Online-Inhalte)
PEReN	Pôle d'Expertise de la Régulation Numérique (Kompetenzzentrum für die Regulierung digitaler Plattformen, Frankreich)
RRS	Rapid Response System (Schnellreaktionssystem)
SREN	*Loi visant à sécuriser et à reguler l'espace numérique* (Gesetz zur Sicherung und Regulierung des digitalen Raums, Frankreich)
StGB	Strafgesetzbuch (Deutschland, bzw. Österreich)
TCO	Terroristische Online-Inhalte
TCO-VO	TCO-Verordnung
TerrOIBG	Terroristische-Online-Inhalte-Bekämpfungsgesetz
TTPW-VO	Verordnung über die Transparenz und das Targeting politischer Werbung
TUSMA	*Testo Unico sui Servizi di Media Audiovisivi* (Konsolidiertes Gesetz über audiovisuelle Mediendienste, Italien)
UKE	*Urząd Komunikacji Elektronicznej* (Amt für elektronische Kommunikation, Polen)
UMG	Mediengesetz (Ukraine)
URL	*Uniform Resource Locater*
UŚUDE	*Ustawa o świadczeniu usług drogą elektroniczną* (Gesetz über die Erbringung elektronischer Dienstleistungen, Polen)
VIGINUM	*Service de vigilance et de protection contre les ingérences numériques étrangères* (Dienst zur Überwachung und zum Schutz vor ausländischer digitaler Einmischung, Frankreich)

VLOP	*Very large online platform* (Sehr große Online-Plattform)
VLOPSE	(VLOP und VLOSE)
VLOSE	*Very large online search engine* (Sehr große Online-Suchmaschine)
VoD	*Video-on-Demand*
VPN	Virtuelles privates Netzwerk
VPS	Virtueller privater Server
VSP	Video-Sharing-Platform
VwVG	Verwaltungsvollstreckungsgesetz (Deutschland)
ZMI	Zentrale Meldestelle für strafbare Inhalte im Internet

Zusammenfassung

Dieser IRIS-Bericht bietet eine umfassende Analyse der derzeitigen Durchsetzung der europäischen Vorschriften für rechtswidrige Inhalte und Desinformation im Internet. Zwölf renommierte Autorinnen und Autoren[4] haben als Fachleute auf ihrem jeweiligen Gebiet separate Kapitel beigesteuert, in denen sowohl auf europäischer als auch auf nationaler Ebene untersucht wird, wie unter den rechtlichen Rahmenbedingungen die bestehenden Regeln durchgesetzt werden können.

Der Bericht vermittelt nicht nur den Blickwinkel der Europäischen Union und des Europarats, sondern bietet auch eine Auswahl nationaler Beispiele, die zu verstehen helfen, was heute in Europa unternommen wird, um diese zentrale Frage anzugehen.

Kapitel 1, verfasst von Mark D. Cole und Sandra Schmitz-Berndt, konzentriert sich auf die Frage, inwiefern digitale Plattformen zwar mächtige Ausdrucksmittel sind, aufgrund ihrer Marktmacht, ihrer Reichweite und der fehlenden redaktionellen Kontrolle jedoch auch einzigartige Risiken bergen. Das Kapitel befasst sich darüber hinaus mit den Unterschieden zwischen rechtswidrigen Inhalten und Desinformation im Internet, wobei die rechtlichen Aspekte beider Konzepte, ihre Verbreitung und die Nuancen, die in verschiedenen europäischen Ländern bestehen, untersucht werden.

Kapitel 2 untersucht den Rechtsrahmen für die Regulierung von Inhalten und die im europäischen Rechtsrahmen vorgesehenen Durchsetzungsmaßnahmen. Der erste Abschnitt, verfasst von Sandra Schmitz-Berndt, analysiert die Durchsetzungsmaßnahmen und den Grundrechtsrahmen des Europarats, wobei nicht nur dessen verschiedene Empfehlungen und die Entschließungen der Parlamentarischen Versammlung des Europarats (PACE), sondern auch die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) berücksichtigt werden.

Ausgehend von dem Gedanken, dass das Internet eine wichtige Rolle für die Wahrnehmung des Rechts auf freie Meinungsäußerung spielt, analysiert die Autorin die Haftung von Internetportalen sowie die Pflichten und Verantwortlichkeiten von Internetvermittlern als auch von nicht professionellen Einrichtungen und Erstellern von Hyperlinks in Bezug auf gesetzwidrige Inhalte Dritter. Die Autorin geht zudem auf die verschiedenen Durchsetzungsmaßnahmen im Hinblick auf die Rechtsprechung des Gerichtshofs ein, zum Beispiel die Sperrung des Zugangs zu Websites oder Social-Media-Konten.

[4] In alphabetischer Reihenfolge: Irène Bouhadana, Mark D. Cole, Roderick Flynn, William Gilles, Giovanni de Gregorio, Mariette Jones, Mehmet Bedii Kaya, Dariia Opryshko, Roxana Radu, Clara Rauchegger, Sandra Schmitz-Berndt und Krzysztof Wojciechowski

Im zweiten Abschnitt werden der Regulierungsrahmen für Inhalte und die Durchsetzungsmaßnahmen auf Ebene der Europäischen Union (EU) dargelegt, insbesondere im Primärrecht und im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik (GASP) sowie im Zusammenhang mit ausländischer Informationsmanipulation und Einmischung (FIMI). Das Kapitel stellt zudem weitere von der EU entwickelte Instrumente zur Durchsetzung von Maßnahmen gegen rechtswidrige Inhalte und Desinformation vor.

In **Kapitel 3** untersucht Mark D. Cole die Durchsetzungsmaßnahmen gegen Desinformation auf EU-Ebene und konzentriert sich auf staatlich gelenkte Desinformation als Beispiel dafür, wie Umfang und Qualität von Desinformationskampagnen in der EU zugenommen haben. Der Autor analysiert des Weiteren europäische Initiativen wie den EU-Verhaltenskodex zur Bekämpfung von Desinformation und dessen Beziehung zum Digital Services Act (DSA) und wirft einen Blick auf Instrumente wie Faktenprüfung und die Beteiligung vertrauenswürdiger Hinweisgeber im digitalen Umfeld.

Dieses Kapitel enthält einen Abschnitt von Roxana Radu über Rumänien, in dem der nationale Rahmen für Plattformen, spezifische Vorschriften für Desinformation und der besondere Fall der Annullierung der rumänischen Präsidentschaftswahlen 2024 untersucht werden. Desinformation spielte eine Schlüsselrolle bei der Beeinträchtigung des Wahlprozesses, gestützt auf tieferliegende strukturelle Schwachstellen wie politische Instabilität, wirtschaftliche Unsicherheit und gesellschaftliche Polarisierung. William Gilles und Irène Bouhadana untersuchen das Beispiel Frankreichs, vom nationalen Rechtsrahmen für Plattformen, der durch die verfassungsgerichtliche Rechtsprechung abgesteckt ist, bis zu spezifischen Vorschriften für Desinformation und deren Anwendung bei den jüngsten Wahlen.

Zudem gibt Dariia Opryshko in diesem Kapitel einen Überblick über die Situation in der Ukraine und betrachtet den nationalen Rechtsrahmen für Plattformen und das neue ukrainische Mediengesetz. Sie untersucht die mit diesem Gesetz eingeführten spezifischen Vorschriften zu Desinformation und ihre Anwendung im Falle ausländischer Einmischung durch Desinformation im Kontext des Krieges. In dem Kapitel wird zudem analysiert, wie der Mangel an wirksamen Mechanismen zur Bekämpfung von Einmischung seitens ausländischer Online-Plattformen zum Schutz der nationalen Interessen zu einer weit verbreiteten Sperrung ganzer Websites und Online-Plattformen geführt hat.

In **Kapitel 4** befasst sich Mark D. Cole mit der Zugänglichkeit terroristischer Inhalte und den Maßnahmen, die zu deren Bekämpfung ergriffen werden, aus dem Blickwinkel der Verordnung über terroristische Online-Inhalte (TCO-VO), die unter anderem „Entfernungsanordnungen“ vorsieht und die zuständigen Behörden ermächtigt, solche Anordnungen zu erlassen, mit denen Hostingdiensteanbieter dazu verpflichtet werden, terroristische Inhalte zu entfernen oder den Zugang dazu in allen EU-Mitgliedstaaten zu sperren.

In diesem Kapitel stellt Sandra Schmitz-Berndt zudem den aktuellen deutschen Rechtsrahmen für Plattformen vor und geht dabei auf das inzwischen außer Kraft gesetzte Netzwerkdurchsetzungsgesetz (NetzDG) und dessen Grundsätze ein, die als Inspiration für den DSA dienten. Das NetzDG enthielt bereits eine Liste von Straftatbeständen, die als „gesetzwidrige Inhalte“ galten, und verpflichtete die Anbieter sozialer Netzwerke, ein

wirksames und transparentes Verfahren zur Bearbeitung von Beschwerden über solche gesetzwidrigen Inhalte vorzuhalten. Das Kapitel befasst sich darüber hinaus mit den spezifischen deutschen Vorschriften für terroristische Inhalte.

Mehmet Bedii Kaya bietet einen Einblick in die Situation in Türkiye und gibt einen Überblick über den nationalen Rechtsrahmen in Bezug auf Plattformen aus Sicht der türkischen Mitgliedschaft im Europarat und der Kandidatur zur Europäischen Union. Wie der Autor erläutert, hat Türkiye eine umfassende Regulierungsinfrastruktur entwickelt, die darauf abzielt, die öffentliche Ordnung sowohl im realen als auch im digitalen Raum aufrechtzuerhalten, und einige spezifische Regeln für terroristische Inhalte aufgestellt.

In **Kapitel 5** konzentriert sich Mark D. Cole auf die Bekämpfung von verleumderischen, hasserfüllten und zu Gewalt aufrufenden Äußerungen aus der Durchsetzungsperspektive auf EU-Ebene. Neben dieser Analyse befasst sich Roderick Flynn mit den irischen Rahmenbedingungen für Online-Plattformen und der Rolle der neuen Medienregulierungsbehörde *Coimisiún na Meán* (CnaM). Der Autor analysiert den diesbezüglichen Umsetzungsprozess des DSA sowie neben dem irischen Online-Sicherheitskodex die spezifischen Vorschriften in Bezug auf verleumderische, hasserfüllte und zu Gewalt aufrufende Äußerungen.

Clara Rauchegger stellt die Situation in Österreich vor, insbesondere das österreichische Kommunikationsplattformen-Gesetz und die daraus resultierende Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH) und wie diese die Auslegung des DSA beeinflusst hat. Die Autorin untersucht darüber hinaus die Anwendung des österreichischen Rechtsrahmens in Fällen von Cyber-Belästigung und bildbasiertem sexuellem Missbrauch.

Giovanni de Gregorio erläutert am Beispiel Italiens die nationalen Mechanismen zur Durchsetzung der Bestimmungen des DSA, die besonderen Vorschriften für verleumderische, hasserfüllte und zu Gewalt aufrufende Äußerungen sowie die Rolle des *Codice Penale* (Strafgesetzbuch). Der Autor stellt zudem die bestehenden gerichtlichen Durchsetzungsmechanismen vor und analysiert die anhaltenden Herausforderungen in diesem Bereich.

In **Kapitel 6** wirft Mark D. Cole einen Blick auf andere Arten schädlicher Inhalte, insbesondere auf Inhalte, die nicht notwendigerweise rechtswidrig sind, aber dennoch möglicherweise Zugangsbeschränkungen für bestimmte Gruppen und insbesondere für Minderjährige unterliegen, da die Inhalte für sie schädlich sein können, insbesondere in audiovisuellen Medien.

Krzysztof Wojciechowski erläutert in diesem Kapitel ausführlich den Fall Polens sowie die jüngsten Reformen in Bezug auf schädliche Inhalte und analysiert die Schwierigkeiten, die sich aus legislativer und justizieller Sicht beim Umgang mit diesem komplexen Thema ergeben.

Mariette Jones gibt einen Überblick über die Situation im Vereinigten Königreich, insbesondere im Hinblick auf das im September 2023 in Kraft getretene Online-Sicherheitsgesetz, das private Unternehmen dazu verpflichtet, schädliche Inhalte, die von Dritten erstellt wurden, aktiv zu überwachen, zu bewerten und zu entfernen und Maßnahmen wie strengere Altersverifizierung zu ergreifen, um Kinder vor solchen Inhalten

zu schützen. Darüber hinaus wird in diesem Abschnitt das Thema Online-Glücksspiele angesprochen.

Zum Abschluss liefern Mark D. Cole und Sandra Schmitz-Berndt in **Kapitel 7** eine vergleichende Analyse der in den Länderberichten vorgestellten Fallstudien, in der sie auf die unterschiedliche Strafverfolgungspraxis gegenüber Internetvermittlern in Europa abheben. Obwohl die EU-Gesetzgebung zu einer erheblichen Harmonisierung geführt hat, die für die Mitgliedstaaten unmittelbar verbindlich ist, gibt es in Europa nach wie vor Unterschiede bei der Rechtsdurchsetzung gegenüber Internetvermittlern.

1. Einführung und Überblick

Dr Mark D. Cole, Wissenschaftlicher Direktor des Instituts für Europäisches Medienrecht (EMR) und Professor für Medien- und Telekommunikationsrecht, Universität Luxemburg, und Dr Sandra Schmitz-Berndt, Wissenschaftliche Mitarbeiterin, Institut für Europäisches Medienrecht (EMR)

Im digitalen Zeitalter dient das Internet als „noch nie dagewesene Plattform für die Ausübung des Rechts auf freie Meinungsäußerung“[5] und ist zu einem „unverzichtbaren Instrument für die Teilnahme an Aktivitäten und Diskussionen über politische Fragen und Themen von allgemeinem Interesse“ geworden.[6] Es spielt damit eine wichtige Rolle bei der Verbesserung des Zugangs der Öffentlichkeit zu Nachrichten und erleichtert ganz allgemein die Verbreitung von Informationen in Echtzeit und im globalen Maßstab.[7] Die Evolution des Internets ist insbesondere dadurch gekennzeichnet, dass es sich grundlegend von einem statischen Werkzeug zur Informationssuche zu einem dynamischen, partizipativen Raum gewandelt hat, der den Einzelnen befähigt, Inhalte in einer neuen Größenordnung und mit potenziell globaler Reichweite zu erstellen, zu teilen und zu nutzen.

Die Anfänge des Internets waren vor allem durch Kommunikation in eine Richtung (Web 1.0) gekennzeichnet, bei der Nutzer Informationen aus einer begrenzten Anzahl von Quellen konsumierten. Dies bedeutete auch, dass die Quelle rechtswidriger Inhalte, das heißt der ursprüngliche Verursacher oder zumindest ein Verantwortlicher für eine bestimmte Website, ermittelt und theoretisch zur Rechenschaft gezogen werden konnte. Offensichtlich brachte der „grenzenlose“ Charakter des Internets bereits zu diesem Zeitpunkt Herausforderungen mit sich, die auch heute noch aktuell sind: Identifizierung der Person oder Einrichtung, gegen die Recht durchgesetzt werden soll, Fragen der gerichtlichen Zuständigkeit, Anwendbarkeit nationalen Rechts und schließlich Durchsetzung in grenzüberschreitenden Fällen.[8] Mit dem Aufkommen der Web-2.0-

---

[5] *Delfi AS gegen Estland [GK]*, Beschwerde Nr. 64569/09 (EGMR, 16. Juni 2015), Rn. 110, *Times Newspapers Ltd (Nr. 1 & 2) gegen das Vereinigte Königreich*, Beschwerden Nr. 3002/03 und 23676/03 (EGMR, 10. März 2009), Rn. 27, und *Ahmet Yildirim gegen Türkiye*, Beschwerde Nr. 3111/10 (EGMR, 18. Dezember 2012), Rn. 48.

[6] Sanchez gegen Frankreich [GK], Beschwerde Nr. 45581/15 (EGMR, 15 mai 2023), Rn. 158, mit Verweis auf *Vladimir Kharitonov gegen Russland*, Beschwerde Nr. 10795/14 (EGMR, 23. Juni 2020), Rn. 33, und *Melike gegen Türkiye*, Beschwerde Nr. 35786/19 (EGMR, 15. Juni 2021), Rn. 44.

[7] *Sanchez gegen Frankreich*, a. a. O., Rn. 159; *Delfi AS gegen Estland [GK]*, a. a. O., Rn. 133.

[8] Siehe Reed, C., *Making Laws for Cyberspace*, Oxford University Press, Oxford, 2012, S. 49 ff.; Cole, M. D., Etteldorf, C. und Ullrich, C., *Cross-Border Dissemination of Online Content*, Bd. 81 Schriftenreihe Medienforschung, Nomos, Baden-Baden, 2021, S. 221 ff.; Cole, M.D. und Etteldorf, C., *Future Regulation of Cross-Border Audiovisual Content Dissemination*, Bd. 83 Schriftenreihe Medienforschung, Nomos, Baden-Baden, 2023, S. 85 ff.; Ukrow, J., „Der Rahmen für die Rechtsdurchsetzung gegen Online-Anbieter und ausländische Inhalte-Anbieter“ in Cappello, M. (Hrsg.), *Medienrechtsdurchsetzung ohne Grenzen*, IRIS *Spezial*, Europäische Audiovisuelle Informationsstelle, Straßburg, 2018, S. 9 ff.

Technologien in einer bidirektionalen Kommunikation und der Social-Media-Plattformen Anfang der 2000er Jahre verwandelte sich das Internet mit der Zeit in ein interaktives Umfeld, das es normalen Nutzern ermöglichte, zu Content-Providern, Kommentatoren und Community-Builder zu werden. Diese partizipatorische Wende hat den öffentlichen Diskurs demokratisiert[9] und ermöglicht es verschiedenen Stimmen, zu politischen, kulturellen und sozialen Gesprächen beizutragen, die früher von traditionellen Medien und institutionellen Akteuren beherrscht wurden.[10] Sie hat zudem neue Formen von bürgerschaftlichem Engagement, Beteiligung und Informationsaustausch begünstigt und damit die Rolle des Internets als Eckpfeiler des modernen demokratischen Lebens gestärkt.

Während das Ethos des Web 2.0 auf Offenheit, Partizipation und dezentraler Innovation beruhte, wurde diese partizipative Infrastruktur von einer Handvoll großer Online-Plattformen dominiert. Das Erscheinen von Plattformen als zentralen Akteuren im digitalen Ökosystem hat die Art und Weise, wie Informationen produziert, verbreitet und konsumiert werden, grundlegend verändert, wodurch sie zu mächtigen Torwächtern in der öffentlichen Internet-Sphäre wurden. Sie ermöglichen zwar weiterhin Partizipation, als datengesteuerte Geschäftsmodelle nehmen sie jedoch zunehmend eine algorithmische Kuratierung von Inhalten vor und bestimmen, welche Inhalte gesehen, geteilt oder sogar entfernt werden. Dies bedeutet, dass die Konturen ihres früheren Status als reine passive Vermittler, die Inhalte Dritter hosten, zunehmend verschwimmen und sie mit einigen Funktionen eine aktivere Rolle übernehmen, was heißt, dass Haftungsmodelle, die unter Web 2.0 entstanden sind, auf dem Prüfstand stehen.[11] Die zunehmenden Eingriffe in Inhalte werfen neue Fragen in Bezug auf Transparenz, Rechenschaftspflicht und den Schutz der Grundrechte im digitalen Bereich auf. Angesichts der Macht der Plattformen als Torwächter entstehen neue Durchsetzungsmodelle, die auf die Entfernung rechtswidriger und schädlicher Inhalte und die Sperrung des Zugangs dazu abzielen; einige wie zum Beispiel der Eigentümer von X, Elon Musk, kritisierten diese als „Redezensur".[12]

Genau die Merkmale, die digitale Plattformen zu mächtigen Ausdrucksmitteln machen – Leichtigkeit, Schnelligkeit, Reichweite und Dauerhaftigkeit –, unterscheiden diese bezeichnenderweise auch von traditionellen Medienformen in einer Weise, die einzigartige Risiken schafft, eine Tatsache, die in ihrer Marktmacht, ihrer Reichweite und der fehlenden redaktionellen Kontrolle begründet liegt. Schädliche oder rechtswidrige Inhalte können „wie nie zuvor in Sekundenschnelle weltweit verbreitet werden" und bleiben gegebenenfalls zeitlich unbegrenzt online zugänglich.[13] Dementsprechend ist ein

---

[9] Siehe Rowland, D., Kohl, U. und Charlesworth, A., *Information Technology Law*, Routledge Abingdon, 5. Aufl. 2017, S. 9 ff.

[10] Siehe *Sanchez gegen Frankreich [GK]*, a. a. O., Rn. 159; *Delfi As gegen Estland [GK]*, a. a. O., Rn. 133.

[11] Cole, M. D., Etteldorf, C. und Ullrich, C., *Cross-Border Dissemination of Online Content*, a. a. O., S. 41 ff.

[12] Siehe die Erklärung auf X von Elon Musk vom 12. Juli 2024. Im gleichen Sinne erwägt die derzeitige US-Regierung Sanktionen gegen Beamte der EU oder der Mitgliedstaaten, die für die Umsetzung des DSA verantwortlich sind, siehe Pamuk, H., "*Exclusive: Trump Administration Weighs Sanctions on Officials Implementing EU Tech Law, Sources Say*", Reuters, 26. August 2025. In ähnlicher Weise bezichtigte der US-Vizepräsident J.D. Vance während seiner Rede auf der Münchner Sicherheitskonferenz EU-Politiker, freie Meinungsäußerung zu zensieren, siehe Bose, N. und Chiacu, D., "*In Munich, Vance Accuses European Politicians of Censoring Free Speech*", Reuters, 14. Februar 2025.

[13] Sanchez gegen Frankreich [GK], a. a. O., (Rn. 160, mit Verweis auf *Savva Terentyev gegen Russland*, Beschwerde Nr. 10692/09 (EGMR, 28. August 2018), Rn. 79, und *Savcı Çengel gegen Türkiye*, Beschwerde Nr. 30697/19 (EGMR, 18. Mai 2021), Rn. 35.

verantwortungsvolles und pflichtbewusstes Verhalten von Plattformanbietern wie auch von Anbietern von Vermittlungsdiensten von wesentlicher Bedeutung für ein sicheres, berechenbares und vertrauenswürdiges Online-Umfeld und dafür, dass die Nutzer ihre in den Grundrechtsrahmen garantierten Grundrechte wahrnehmen können, insbesondere das Recht auf Meinungs- und Informationsfreiheit, auf unternehmerische Freiheit, das Recht auf Nichtdiskriminierung und die Erreichung eines hohen Verbraucherschutzniveaus.[14] Allerdings dürfen sich Vorschriften gegen rechtswidrige und schädliche Inhalte nicht allein auf Plattformen konzentrieren, sondern müssen auch das breite Spektrum von Akteuren berücksichtigen, die bei der Erstellung, Verbreitung und Moderation von Inhalten unterschiedliche Rollen wahrnehmen. Die rechtlichen und normativen Rahmenbedingungen hinken der komplexen Herausforderung hinterher, die Grundrechte und die gesellschaftlichen Interessen im Cyberspace zu schützen. Auf globaler Ebene gibt es nur begrenzte Lösungen für die Bekämpfung rechtswidriger Inhalte im Internet.[15] Selbst innerhalb des relativ einheitlichen europäischen Rechtsraums ist die Harmonisierung der Regulierung von Medieninhalten noch unvollständig, doch hat die EU in letzter Zeit mit mehreren digitalen Rechtsakten, die sich direkt oder indirekt mit der Verbreitung rechtswidriger und schädlicher Inhalte befassen, einen bedeutenden Schritt nach vorn getan.

Der vorliegende Bericht konzentriert sich auf die Durchsetzung von Regeln gegen rechtswidrige Inhalte und Desinformation im Internet. Beide Kategorien von Inhalten sind unter anderem für die gesellschaftliche Resilienz und die demokratische Integrität von großer Bedeutung, jedoch unterscheiden sie sich in wichtigen rechtlichen und konzeptionellen Aspekten – insbesondere in Bezug auf die Frage, welche Arten von Äußerungen im Internet rechtmäßig eingeschränkt werden können. Daher ist es notwendig, die Begriffsdefinitionen zu klären.

Als rechtswidrige Inhalte werden in dieser Publikation Materialien bezeichnet, die gegen bestehende gesetzliche Bestimmungen verstoßen. Ihre Rechtswidrigkeit ist durch Gesetz oder Rechtsprechung eindeutig definiert. Was rechtswidrig ist, unterliegt daher in erster Linie nationalem Recht. Dies wiederum verdeutlicht bereits eine der Herausforderungen, nämlich die Beschränkungen bei der Durchsetzung, wenn die Definitionen zwischen den einzelstaatlichen Rechtsvorschriften nicht harmonisiert sind und es darum geht, was als rechtswidrig gilt und wie dieses Problem selbst auf einer supranationalen Ebene wie der EU-Ebene gelöst werden kann. Aufgrund des allgemeinen Verständnisses von „illegal“ wird eben dieser Begriff in der Publikation anstelle des weiter gefassten und weniger genau definierten Terminus „rechtswidrige Inhalte“ verwendet. Einige Gesetze, insbesondere auf nationaler Ebene, sprechen möglicherweise von „rechtswidrigen Inhalten“, so zum Beispiel das (teilweise aufgehobene) deutsche NetzDG.[16] Rechtswidrige Inhalte schließen illegale Inhalte ein, können aber auch Handlungen oder Materialien meinen, die gegen Verwaltungsvorschriften, vertragliche Verpflichtungen oder

[14] Vgl. Erwägungsgrund 3 DSA.

[15] Für einen kurzen Überblick siehe Ukrow, J., „Einleitung und Überblick“ in Cappello, M. (Hrsg.), *Medienrechtsdurchsetzung ohne Grenzen*, IRIS *Spezial, Europäische Audiovisuelle Informationsstelle, Straßburg, 2018*, S. 3 ff.

[16] *Netzwerkdurchsetzungsgesetz* (NetzDG). Das Gesetz wurde durch das Durchführungsgesetz zum DSA teilweise aufgehoben.

Regulierungsstandards verstoßen. Der juristischen Präzision halber wird in den digitalen Gesetzen der EU in den jeweiligen englischen Sprachfassungen standardmäßig der Begriff „illegale Inhalte“ verwendet.[17]

Im Gegensatz dazu umfasst der Begriff „schädliche Inhalte“ Material, das möglicherweise nicht rechtswidrig ist, aber dennoch als abträglich für Einzelne oder die Gesellschaft angesehen wird – zum Beispiel Desinformation, Fehlinformationen zum Thema Gesundheit oder Inhalte, die demokratische Prozesse unterminieren. Der Umgang mit Desinformation in einem rechtlichen, regulatorischen oder politischen Kontext erfordert eine Definition des Begriffs, um sie von anderen Arten von Inhalten zu unterscheiden. Unter Desinformation versteht man im Allgemeinen falsche oder irreführende Informationen, die mit Täuschungsabsicht verbreitet werden. Dementsprechend lässt sie sich von Fehlinformation, das heißt falschen Informationen, die ohne Täuschungsabsicht weitergegeben werden, oder Malinformation, das heißt wahren Informationen, die böswillig oder aus dem Zusammenhang gerissen verwendet werden, differenzieren.[18] Diese Kategorie ist besonders schwierig zu regulieren, da ein Großteil davon nicht unter Rechtswidrigkeit fällt und daher oft unter dem weiter gefassten Begriff der schädlichen Inhalte behandelt wird. Deswegen geht der Rahmen dieses Berichts über rechtswidrige Inhalte hinaus und erfasst Desinformation als separate Kategorie, die nicht notwendigerweise unter den Begriff „rechtswidrig“ fällt und besondere Herausforderungen für die Regulierung mit sich bringt.

Als Reaktion auf das Ausmaß, die Verbreitung und die gesellschaftlichen Auswirkungen von rechtswidrigen Inhalten und Desinformation hat sich eine Reihe von Regulierungs- und Governancemodellen herausgebildet, die der Vielfalt an Internetvermittlern Rechnung tragen sollen, deren Engagement von passiv bis aktiv reicht und die eine Vielzahl von Funktionen und Diensten wahrnehmen. Zu Letzteren gehören soziale Netzwerke, Blogs, Messenger-Dienste, Diskussionsforen und Pinnwände, Plattformen zur Aggregation und zum Rating sozialer Nachrichten sowie Video-Sharing-Plattformen, um nur einige zu nennen. Der Schwerpunkt dieser Publikation liegt auf Plattformen, die als Vermittler Inhalte hosten und verbreiten.

Der erste Teil dieser Publikation befasst sich zunächst mit dem Rechtsrahmen des Europarats und stellt dann die wichtigsten EU-Rechtsinstrumente für Internetvermittler vor. Unter einem Internetvermittler wird im weitesten Sinne eine Einrichtung verstanden, die die Nutzung des Internets erleichtert, indem sie Dienste anbietet, die die Kommunikation, den Zugang zu Inhalten oder die Übertragung von Daten zwischen Nutzern und Datenspeicherung ermöglichen. Gesonderte Definitionen für den Begriff und die erbrachten Dienstleistungen sind in den verschiedenen Rechtsvorschriften enthalten und werden bei Bedarf erläutert. Länderbeispiele, die sich auf verschiedene Phänomene rechtswidriger oder schädlicher Inhalte und die jeweiligen Reaktionen der Länder im Rahmen des EU-Rechts und des nationalen Rechts konzentrieren, sollen einen Überblick über die Unterschiede bei

[17] So auch in der deutschen Sprachfassung der KI-VO oder der TCO-VO, während die offizielle deutsche Sprachfassung des DSA wiederum „illegal“ mit rechtswidrig übersetzt und rechtswidrige Inhalte in Art. 3 lit. h) DSA legaldefiniert.

[18] Für eine Definition von Fehlinformation, Malinformation und Desinformation siehe Wardle, C. und Derakhshan, H., *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*, Bericht des Europarats, DGI(2017)09, S. 20 ff.

der Durchsetzung der Vorschriften geben. In einem weiteren Kapitel werden die verschiedenen Durchsetzungsmodelle verglichen. Vor dem Hintergrund der im ersten Teil dieser Publikation vorgestellten rechtlichen Gegebenheiten sowie einer kurzen Darstellung der nationalen Rechtsrahmen für die Regulierung von Online-Plattformen im Allgemeinen werden in den Länderbeispielen die spezifischen Vorschriften für eine gezielte Bekämpfung der fraglichen rechtswidrigen oder schädlichen Inhalte erläutert und die Anwendung dieser Regelung in einem ausgewählten Kontext beispielhaft beschrieben. Im abschließenden Teil veranschaulicht der Bericht die verbleibenden und anhaltenden Herausforderungen bei der wirksamen Bekämpfung rechtswidriger und schädlicher Online-Inhalte.

2. Der rechtliche Rahmen

2.1 Der Ansatz des Europarats zur Regulierung von Inhalten und Durchsetzungsmaßnahmen

Sandra Schmitz-Berndt, Wissenschaftliche Mitarbeiterin, Institut für Europäisches Medienrecht (EMR)

2.1.1 Durchsetzungsmaßnahmen und der Grundrechtsrahmen im Europarat

Während einerseits „nutzergenerierte, ausdrucksstarke Aktivität im Internet eine noch nie dagewesene Plattform für die Ausübung des Rechts auf freie Meinungsäußerung bietet“,[19] ist andererseits die Durchsetzung von Regeln für spezifische Inhalte wie die Beschränkung des Zugangs zu bestimmten Äußerungen sowie deren Löschung oder strafrechtliche Verfolgung an sich ein Eingriff in das Recht auf freie Meinungsäußerung, wie es in Artikel 10 der Europäischen Menschenrechtskonvention (EMRK) garantiert wird.[20] Die in Artikel 10 Absatz 1 EMRK sowie in vergleichbaren Verfassungsbestimmungen verankerten Kommunikationsfreiheiten – Informationsfreiheit, Meinungsfreiheit und Freiheit der massenmedialen Kommunikation – sind Voraussetzung für eine funktionierende Demokratie. Als Abwehrrechte des Einzelnen gegen den Staat sichern die Kommunikationsfreiheiten die individuelle Selbstbestimmung, indem sie den Kommunikationsprozess gegen staatliche Eingriffe abschirmen. Bei der Beurteilung, ob ein solcher Eingriff vorliegt, ist nach modernem Verständnis jede staatliche Regelung oder Maßnahme zu betrachten, welche die Ausübung eines durch die Grundrechte geschützten Verhaltens einschränkt, behindert oder ganz oder teilweise unmöglich macht. In diesem Sinne kann die Durchsetzung von Regeln, die sich auf die Kommunikation auswirken, für sich einen dem Staat zurechenbaren Eingriff darstellen.[21]

Beim Schutz der Kommunikationsrechte geht es jedoch um mehr als die Abschirmung des Einzelnen gegen willkürliche staatliche Eingriffe. Der Europäische

---

[19] *Delfi As gegen Estland* [GK] Nr. 64569/09 (EGMR, 16. Juni 2015), Rn. 110.

[20] Für einen umfassenden Überblick mit kurzen Zusammenfassungen und schnellem Zugriff auf die Fälle siehe EAI, VERBO-Datenbank, abrufbar unter <https://verbo.obs.coe.int/>; zuvor auch Voorhoof, D. et al. und McGonagle, T. (Ed. Sup.), *Freedom of Expression, the Media and Journalists: Case-Law of the European Court of Human Rights*, IRIS *Themes,* Europäische Audiovisuelle Informationsstelle, Straßburg, 2024. Zum Rahmen für die Rechtsdurchsetzung auf der Ebene nationaler Verfassungsordnungen siehe Ukrow, J., „Der Rahmen für die Rechtsdurchsetzung gegen Online-Anbieter und ausländische Inhalte-Anbieter“ in Cappello, M. (Hrsg.), Medienrechtsdurchsetzung ohne Grenzen*,* IRIS *Spezial,* Europäische Audiovisuelle Informationsstelle, Straßburg 2018.

[21] Mensching, C., „Artikel 10 EMRK“ in Karpenstein, U. und Mayer, F. C. (Hrsg.), *Konvention zum Schutz der Menschenrechte und Grundfreiheiten: EMRK,* C.H.Beck München, 3. Aufl., 2022, Abs. 27 mit weiteren Hinweisen.

Gerichtshof für Menschenrechte (EGMR) hat anerkannt, dass es zusätzliche inhärente positive Verpflichtungen für die wirksame Einhaltung der betreffenden Rechte geben kann. Nach Ansicht des Gerichtshofs hängt die effektive Wahrnehmung des Rechts auf freie Meinungsäußerung demnach nicht allein von der Pflicht eines Staates zur Nichteinmischung ab, sondern kann auch positive Schutzmaßnahmen – selbst in den Beziehungen zwischen Einzelpersonen – erfordern.[22] Je nach den Umständen können auch private Akteure indirekt verpflichtet sein, diese Rechte zu achten, wobei diese Verpflichtung derjenigen von Staaten sehr ähnlich oder sogar gleichwertig ist. Dies ist besonders dann von Bedeutung, wenn private Akteure die grundlegende Infrastruktur für die öffentliche Kommunikation bereitstellen und Funktionen übernehmen, die früher als hoheitliche Aufgaben des Staates angesehen wurden, zum Beispiel die Sicherstellung von Post- und Telekommunikationsdienstleistungen.[23]

Artikel 10 Absatz 2 EMRK sieht die Möglichkeit vor, die Ausübung der in Artikel 10 Absatz 1 genannten Kommunikationsfreiheiten einzuschränken, und nennt die Bedingungen, unter denen solche Einschränkungen auferlegt werden können; er verweist zudem auf eine Reihe explizit aufgeführter legitimer Ziele von Eingriffen durch die Unterzeichnerstaaten der Europäischen Menschenrechtskonvention.

Der EGMR hat wiederholt anerkannt, dass das Internet eine noch nie dagewesene Plattform für die Ausübung der Meinungsfreiheit bietet.[24] Da das Internet gut zugänglich ist und riesige Mengen an Informationen speichern und übermitteln kann, wird ihm eine wichtige Rolle bei der Verbesserung des Zugangs der Öffentlichkeit zu Nachrichten und der Förderung der Informationsverbreitung im Allgemeinen zuerkannt – auch von Inhalten, die von den traditionellen Medien eher ignoriert werden.[25] Zugleich wird das Risiko, dass Inhalt und Kommunikationen im Internet eine Gefahr für die Ausübung und Wahrnehmung der Menschenrechte und Freiheiten darstellen können, insbesondere des Rechts auf Achtung des Privatlebens, höher eingestuft als das Risiko in den Printmedien.[26] Der EGMR hat anerkannt, dass sich das Internet als einzigartig leistungsfähiges Kommunikationsinstrument durch seine Fähigkeit, Informationen weltweit zu speichern und zu übermitteln, von Printmedien unterscheidet und daher maßgeschneiderte Regeln erfordert, die seinen technologischen Besonderheiten Rechnung tragen.[27] Zudem geht der erhebliche Nutzen des Internets, neben anderem bei der Ausübung des Rechts auf freie Meinungsäußerung, mit einer Reihe von Gefahren einher. So können zum Beispiel eindeutig rechtswidrige Äußerungen sofort weltweit verbreitet werden und möglicherweise „dauerhaft online verfügbar bleiben".[28] Der Gerichtshof hat darüber hinaus anerkannt, dass das Schadensrisiko von Inhalten und Kommunikationen im Internet für die Ausübung und

---

[22] *Özgur Gündem gegen Türkiye*, Nr. 23144/93 (EGMR, 16. März 2000), Rn. 43 mit Verweis auf *X und Y gegen die Niederlande*, Nr. 8978/80 (EGMR, 26. März 1985), Rn. 23.

[23] Vgl. BVerfG, Urteil vom 22. Februar 2011, 1 BvR 699/06, Abs. 59.

[24] *Delfi As gegen Estland* [GK], Nr. 64569/09, Rn. 110; *Cengiz und andere gegen Türkiye*, Nr. 48226/10 und 14027/11 (EGMR, 1. Dezember 2015), Rn. 52; *Ahmet Yildirim gegen Türkiye*, Nr. 3111/10 (EGMR, 18. Dezember 2012), Rn. 48; *Times Newspapers Ltd (Nr. 1 & 2) gegen das Vereinigte Königreich*, Nr. 3002/03 und 23676/03 (EGMR, 10. März 2009), Rn. 27.

[25] Ahmet *Yildirim gegen Türkiye*, Nr. 3111/10, Rn. 48; zu Inhalten, die nicht von der traditionellen Presse abgedeckt werden, siehe: *Cengiz und andere gegen Türkiye*, Nr. 48226/10 und 14027/11, Rn. 52.

[26] *Egill Einarsson gegen Island*, Nr. 24703/15 (EGMR, 7. Februar 2018), Rn. 46.

[27] *Redaktion von Pravoye Delo und Shtekel gegen die Ukraine*, Nr. 33014/05 (EGMR, 5. Mai 2011), Rn. 63.

[28] *Delfi As gegen Estland* [GK], Nr. 64569/09, Rn. 110.

Wahrnehmung der Menschenrechte und Freiheiten sicherlich höher ist als das der traditionellen Presse.[29]

Bereits 2003 hat das Ministerkomitee des Europarats eine Erklärung zur Kommunikationsfreiheit im Internet verabschiedet,[30] in der in Grundsatz 6 eine begrenzte Haftung von Diensteanbietern für Internetinhalte festgelegt wurde. Grundsatz 6 sieht vor, dass die Staaten in Fällen, in denen die Funktionen der Diensteanbieter umfassender sind und sie Inhalte speichern, die von Dritten stammen, diese Anbieter mitverantwortlich machen können, wenn sie nicht unverzüglich tätig werden, um Informationen zu entfernen oder den Zugang zu Diensten zu sperren, sobald sie im Sinne des nationalen Rechts Kenntnis von deren Rechtswidrigkeit oder – im Falle von Schadensersatzansprüchen – von Tatsachen oder Umständen erhalten, aus denen die Rechtswidrigkeit der Tätigkeit oder der Informationen hervorgeht. Der Europarat hat damit das im nationalen Recht von EU-Mitgliedstaaten geltende Haftungskonzept nach Artikel 14 der EU-Richtlinie über den elektronischen Geschäftsverkehr übernommen.[31]

In der Folge hat sich der Europarat über viele Jahre hinweg – direkt oder indirekt – in zahlreichen weiteren Grundsatzpapieren einschließlich Empfehlungen und Erklärungen mit der Durchsetzung von Vorschriften zu rechtswidrigen Inhalten und Desinformation im Internet befasst. Diese politischen normsetzenden Texte sind im Gegensatz zu den Übereinkommen des Europarats für Unterzeichner nicht rechtsverbindlich, sondern dienen dazu, die Auslegung der Übereinkommen einschließlich der EMRK zu unterstützen, indem sie allgemeine Grundsätze auf Beispielszenarien oder spezifische Kontexte anwenden und eine differenzierte und abgestufte Reaktion vorsehen.[32]

In der Präambel seiner auf Rechtsstaatlichkeit basierenden Empfehlung CM/Rec(2018)2 zu den Rollen und Verantwortlichkeiten von Internetvermittlern stellt das Ministerkomitee ferner fest, dass „ein breites, vielfältiges und sich rasch entwickelndes Spektrum von Akteuren, die gemeinhin als ‚Internetvermittler' bezeichnet werden, die Interaktionen zwischen natürlichen und juristischen Personen im Internet erleichtern, indem sie eine Vielzahl von Funktionen und Dienstleistungen anbieten und ausführen".[33] „Aufgrund der vielfältigen Rollen, die Vermittler spielen, sollten ihre entsprechenden Pflichten und Verantwortlichkeiten sowie ihr rechtlicher Schutz im Hinblick auf die spezifischen Dienstleistungen und Funktionen, die erbracht bzw. übernommen werden, festgelegt werden."[34] Dementsprechend hat der Europarat angesichts der sich entwickelnden unterschiedlichen Rollen von Online-Akteuren den üblicherweise für Zugangs-, Caching- oder Hostinganbieter verwendeten Begriff „Internetdienstanbieter" zugunsten der umfassenderen Bezeichnung „Internetvermittler" aufgegeben. Im Anhang

[29] *Redaktion von Pravoye Delo und Shtekel gegen die Ukraine*, Nr. 33014/05, Rn. 63.
[30] Europarat, Ministerkomitee, Erklärung zur Kommunikationsfreiheit im Internet (engl.), Decl(28/05/2003).
[31] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, ABl. L 178/1, 17. Juli 2000.
[32] Dieser Ansatz wurde in der Empfehlung CM/Rec(2011) des Europarats für einen neuen Medienbegriff vorgeschlagen. Siehe: CM/Rec(2011)7 – Empfehlung des Ministerkomitees an die Mitgliedstaaten für einen neuen Medienbegriff (engl.).
[33] Europarat, Empfehlung CM/Rec(2018)2 des Ministerkomitees an die Mitgliedstaaten zu den Rollen und Verantwortlichkeiten von Internetvermittlern (engl.), Präambel, Abs. 4
[34] Ebd., Abs. 11.

der Empfehlung CM/Rec(2018)2 sind für den Umgang mit den Verpflichtungen von Staaten und den Verantwortlichkeiten von Internetvermittlern Leitlinien zu den Maßnahmen von Staaten gegenüber Internetvermittlern formuliert. Im Zusammenhang mit der Festlegung der Verpflichtungen von Staaten in Bezug auf den Schutz und die Förderung der Menschenrechte und Grundfreiheiten im digitalen Umfeld müssen bei der Ausarbeitung, Auslegung und Anwendung des Rechtsrahmens die wesentlichen Unterschiede in Bezug auf Größe, Art, Funktion und Organisationsstruktur der Vermittler zu berücksichtigt werden.[35] Das Ministerkomitee erkennt an, dass Plattformanbieter bei der Produktion und Verbreitung von Inhalten unterschiedliche Rollen spielen können, zum Beispiel, indem sie die Inhalte verwalten oder kuratieren oder eine redaktionelle Rolle übernehmen, was einen abgestuften oder differenzierten Ansatz erfordert.[36] Gemäß Empfehlung CM/Rec(2011)7 verlangt dieser Ansatz, dass jeder Akteur, dessen Dienste als Medien oder als Vermittlungs- oder Hilfstätigkeit ausgewiesen sind, sowohl eine angemessene Form (differenziert) als auch einen angemessenen Grad (abgestuft) an Schutz genießt und dass die Verantwortlichkeit abgegrenzt sein sollte.[37]

Die Staaten sollten sicherstellen, dass Rechtsvorschriften, Regelungen und Verfahren in Bezug auf Internetvermittler wirksam umsetzbar und durchsetzbar sind und den Vorgang und den freien Fluss grenzüberschreitender Kommunikation nicht unangemessen einschränken.[38] Im Anhang zu Empfehlung CM/Rec(2018)2 wird klargestellt, dass jede Maßnahme staatlicher Behörden gegenüber Internetvermittlern zur Beschränkung des Zugangs zu Inhalten einschließlich deren Sperrung oder Entfernung oder jede andere Maßnahme, die zu einer Einschränkung des Rechts auf freie Meinungsäußerung führen könnte, den Dreistufentest nach Artikel 10 EMRK bestehen muss. Dies bedeutet, dass jede Anfrage, Aufforderung oder sonstige Handlung staatlicher Behörden gegenüber Internetvermittlern zu dem Zweck, den Zugang zu Inhalten einzuschränken (einschließlich deren Sperrung und Entfernung), gesetzlich vorgeschrieben sein muss, eines der in Artikel 10 EMRK vorgesehenen legitimen Ziele verfolgen, in einer demokratischen Gesellschaft notwendig und dem verfolgten Ziel angemessen sein muss.[39] Dennoch sollten staatliche Behörden im Zusammenhang mit diesen Maßnahmen die Anordnung einer Justizbehörde oder einer anderen unabhängigen Verwaltungsbehörde einholen, deren Entscheidungen einer gerichtlichen Überprüfung unterliegen, bevor sie von Vermittlern verlangen, den Zugang zu Inhalten zu beschränken. Ausgenommen sind dabei Fälle, in denen es sich um von Natur aus rechtswidriges Material wie zum Beispiel Inhalte zu sexuellem Missbrauch von Kindern handelt, oder Fälle, in denen sofortiges Handeln unter den in Artikel 10 EMRK festgelegten Bedingungen gerechtfertigt ist.[40]

---

[35] Anhang zur Empfehlung CM/Rec(2018)2 des Ministerkomitees an die Mitgliedstaaten zu den Rollen und Verantwortlichkeiten von Internetvermittlern (engl.), Abs. 1.1.5

[36] Ebd., Abs. 1.3.9.

[37] Anhang zur Empfehlung CM/Rec(2011)7 des Ministerkomitees des Europarats an die Mitgliedstaaten für einen neuen Medienbegriff (engl.), Kriterien zur Identifizierung von Medien und Leitlinien für eine abgestufte und differenzierte Reaktion, Abs. 7.

[38] Empfehlung CM/Rec(2018)2 des Ministerkomitees an die Mitgliedstaaten zu den Rollen und Verantwortlichkeiten von Internetvermittlern (engl.), Abs. 1.1.6

[39] Ebd., Abs. 1.3.1.

[40] Ebd., Abs. 1.3.2.

In Empfehlung CM/Rec(2018)2 wird den Staaten zudem geraten, von Vermittlern nicht zu verlangen, dass sie Inhalte überwachen, zu denen sie lediglich Zugang gewähren oder die sie übermitteln oder speichern. Anforderungen an Vermittler oder Koregulierungsinitiativen gleich welcher Art sollten nicht zu einer allgemeinen Überwachungspflicht führen.[41] Empfehlung CM/Rec(2018)2 thematisiert ebenfalls die Verantwortlichkeit für Inhalte Dritter. Demnach sollten Vermittler nicht für Inhalte haftbar gemacht werden, zu denen sie lediglich Zugang gewähren oder die sie übermitteln oder speichern. Eine Mitverantwortung für gespeicherte Inhalte kann jedoch dann in Betracht kommen, wenn Vermittler nicht zügig handeln, um den Zugang zu Inhalten oder Diensten einzuschränken, sobald sie von deren Rechtswidrigkeit Kenntnis erlangen, unter anderem durch Meldeverfahren.[42]

In Empfehlung CM/Rec(2018)2 wird zu Meldeverfahren darauf hingewiesen, dass diese nicht so gestaltet sein sollten, dass sie zur Löschung legaler Inhalte motivieren, zum Beispiel wegen unangemessen kurzer Fristen, und dass sie die erforderlichen Informationen enthalten sollten, damit die Vermittler geeignete Maßnahmen ergreifen können.[43] Vor dem Hintergrund des menschenrechtsbasierten Ansatzes der politischen Maßnahmen des Europarates muss jeder Eingriff von Vermittlern in den freien und offenen Informations- und Ideenfluss auf bestimmte legitime Zwecke beschränkt sein und den Grundsätzen von Transparenz und Rechenschaftspflicht entsprechen sowie Zugang zu einem wirksamen Rechtsbehelf gewährleisten.[44] Dies nimmt Staaten jedoch nicht die Möglichkeit, Vermittler zu verpflichten, die Online-Risiken zu mindern und auf die Verbreitung rechtswidriger Inhalte zu reagieren, indem sie beispielsweise Mechanismen zur Inhaltsmoderation einführen. Nachfolgende Empfehlungen befassten sich mit den Auswirkungen digitaler Technologien auf die Meinungsfreiheit,[45] den Auswirkungen algorithmischer Systeme auf die Menschenrechte[46] und der Bekämpfung von Hassrede.[47] In einem übergreifenden Ansatz thematisiert Empfehlung CM/Rec(2022)11 zu den Grundsätzen der Governance von Medien und Kommunikation[48] die Risiken, die von Plattformen ausgehen, welche rechtswidrige und schädliche Inhalte verbreiten, und bezeichnet risikobasierte und menschenrechtskonforme Inhaltsmoderation ausdrücklich als eine angemessene Reaktion.

Die Empfehlung CM/Rec(2022)13 zu den Auswirkungen digitaler Technologien auf die Meinungsfreiheit[49] ist ein weiterer Vorstoß, sicherzustellen, dass digitale Technologien den in Artikel 10 EMRK verankerten Rechten dienen und sie nicht beschneiden. Im Hinblick auf Rechenschaftspflicht und Rechtsbehelf verlangt diese Empfehlung, dass die Staaten

---

[41] Ebd., Abs. 1.3.5.
[42] Ebd., Abs. 1.3.7.
[43] Ebd.
[44] Ebd., Abs. 2.2 ff
[45] Europarat, Empfehlung CM/Rec(2022)13 des Ministerkomitees an die Mitgliedstaaten zu den Auswirkungen digitaler Technologien auf die Meinungsfreiheit (engl.)
[46] Europarat, Empfehlung CM/Rec(2020)1 des Ministerkomitees an die Mitgliedstaaten zu den Auswirkungen algorithmischer Systeme auf die Menschenrechte (engl.)
[47] Europarat, Empfehlung CM/Rec(2022)16 des Ministerkomitees an die Mitgliedstaaten zur Bekämpfung von Hassrede.
[48] Europarat, Empfehlung CM/Rec(2022)11 des Ministerkomitees an die Mitgliedstaaten zu den Grundsätzen der Governance von Medien und Kommunikation.
[49] Europarat, Empfehlung CM/Rec(2022)13 des Ministerkomitees an die Mitgliedstaaten zu den Auswirkungen digitaler Technologien auf die Meinungsfreiheit (engl.)

wirksame Rechtsbehelfsmechanismen gegen Einschränkungen der Meinungsfreiheit gewährleisten.[50] Wenn Internetvermittler Einschränkungen der Meinungsfreiheit vornehmen, sollten sie den direkt oder indirekt betroffenen Nutzern klare Angaben zu der Regelung machen, nach der ihre Rechte eingeschränkt wurden. Zudem sollten sie zeitnahe und wirksame Rechtsbehelfsmechanismen anbieten.[51]

In Anbetracht der Tatsache, dass diffamierende und andere Arten rechtswidriger Äußerungen „wie nie zuvor weltweit und in Sekundenschnelle verbreitet werden können und manchmal dauerhaft online verfügbar bleiben" und dass die Rechte nach Artikel 10 und 8 EMRK „gleiche Achtung verdienen", „muss die Möglichkeit der Haftbarmachung für diffamierende oder andere Formen unrechtmäßiger Äußerungen grundsätzlich gewahrt bleiben und einen wirksamen Rechtsbehelf für Verletzungen der Persönlichkeitsrechte darstellen".[52] Äußerungen, die mit den von der EMRK proklamierten und garantierten Werten unvereinbar sind, sind aufgrund von Artikel 17 EMRK (der den Missbrauch von Rechten verbietet) nicht durch Artikel 10 geschützt. Obwohl es umfangreiche Rechtsprechung dazu gibt, wie die Abwägung zwischen Artikel 10 und Artikel 8 EMRK vorzunehmen ist, hielt es der Europarat für geboten, die Besonderheiten von Hassrede und insbesondere von Hassrede im Online-Kontext in einer gesonderten Empfehlung zur Bekämpfung von Hassrede zu behandeln.[53] Diese Empfehlung CM/Rec(2022)16 bietet den Staaten Orientierungshilfe für die Umsetzung eines umfassenden und abgestimmten Pakets an rechtlichen und nicht rechtlichen Maßnahmen. Während die allgemeinen Grundsätze, die für Offline-Publikationen gelten, auch online Anwendung finden, richtet Empfehlung CM/Rec(2022)16 besonderes Augenmerk auf das Online-Umfeld, in dem Hassrede heute überwiegend zu finden ist. Angesichts der anhaltenden Viktimisierung, die entsteht, wenn solche Inhalte online bleiben, fordert die Empfehlung die Mitgliedstaaten auf, sich neben strafrechtlichen Ermittlungen auf die Entfernung von Hassrede im Internet zu konzentrieren.[54]

In Anbetracht der Tatsache, dass sich Hassrede im Internet über nationale Grenzen hinweg verbreitet, wird in Empfehlung CM/Rec(2022)16 die Notwendigkeit einer Harmonisierung anerkannt, um Hassrede wirksam zu verhindern und zu bekämpfen.[55] Im Einklang mit Empfehlung CM/Rec(2018)2 muss eine solche Harmonisierung die Rollen und Verantwortlichkeiten aller Beteiligten einschließlich der Internetvermittler umfassen.[56]

In Empfehlung CM/Rec(2022)16 wird gefordert, dass die Verfahren zur Entfernung (einschließlich der Voraussetzungen dafür sowie die den Vermittlern auferlegten Verantwortlichkeiten) transparent, klar und vorhersehbar sein müssen und dass Rechtsbehelfsmechanismen vorgesehen werden.[57] Da Täter wahrscheinlich anonym bleiben, müssen die Staaten ein System vorsehen, das Diensteanbieter verpflichtet,

[50] Ebd., Anhang, Abs. 4.1.
[51] Ebd., Abs. 4.5.
[52] *Delfi As gegen Estland* [GK], Nr. 64569/09, Rn. 110.
[53] Europarat, Empfehlung CM/Rec(2022)16 des Ministerkomitees an die Mitgliedstaaten zur Bekämpfung von Hassrede (engl.).
[54] Ebd., Präambel.
[55] Ebd., Abs. 16.
[56] Ebd., Abs. 17.
[57] Ebd., Abs. 20.

Teilnehmerdaten offenzulegen.[58] Darüber hinaus befasst sich die Empfehlung mit Inhaltsmoderation, die angesichts des Einsatzes von künstlicher Intelligenz (KI) von menschlichen Moderatoren überwacht werden sollte.[59] Neben der Ernennung einer ausreichenden Anzahl geschulter Inhaltsmoderatoren fördert Empfehlung CM/Rec(2022)16 Kooperationsmodelle wie vertrauenswürdige Hinweisgeber und Faktenprüfer sowie Zusammenarbeit mit Organisationen der Zivilgesellschaft, die sich mit Hassrede beschäftigen.[60] Die Empfehlungen wurden ergänzt durch die Leitfäden des Europarats zur Moderation von Inhalten (2021)[61] und zur Bekämpfung der Verbreitung von Falsch- und Desinformationen im Internet durch Faktenprüfung und menschenrechtskonforme Lösungen für die Gestaltung von Plattformen (2023).[62]

Vor kurzem hat die Parlamentarische Versammlung des Europarats (Parliamentary Assembly of the Council of Europe - PACE) in ihrer Entschließung 2590[63] vom Januar 2025 zur Regelung der Moderation von Inhalten in sozialen Medien zum Schutz der Meinungsfreiheit bekräftigt, dass Anbieter sozialer Medien rechtlich verpflichtet sind, rechtswidrige Inhalte zu entfernen, sobald sie von deren Existenz Kenntnis erlangt haben, und dass es „den sozialen Medien obliegt, die Verbreitung schädlicher Inhalte zu bekämpfen".[64] Als Träger von Grundrechten wie dem Recht auf Eigentum und unternehmerische Freiheit sowie dem Recht, Geschäftsbedingungen mit Vertragscharakter (an die die Nutzer nach dem „alles-oder-nichts"-Prinzip gebunden sind) abzufassen, können Social-Media-Unternehmen festlegen, wie Nutzer ihre Dienste nutzen können und welche Inhalte sie posten dürfen. Darüber hinaus können sie interne Richtlinien zur Inhaltsmoderation erstellen, die es ihnen ermöglichen, Inhalte herabzustufen, den Zugang zu ihnen einzuschränken oder sie zu entfernen sowie Benutzerkonten zu sperren oder zu löschen.[65] In Anbetracht ihrer globalen Reichweite und ihrer privaten vertraglichen Macht – dazu gehören Strategien zur Inhaltsmoderation und kommerzielle oder ideologische Entscheidungen über Inhalte – können Anbieter sozialer Medien einen immensen Einfluss auf die öffentliche Meinung haben. In Anerkennung des Machtungleichgewichts und der Notwendigkeit, die Verbreitung schädlicher Inhalte zu bekämpfen, unterstreicht die PACE, dass die Staaten notwendigerweise einen korrigierenden Regulierungsrahmen für Inhaltsmoderation schaffen müssen, der ein Gleichgewicht zwischen der Moderation von Inhalten und dem Schutz der Meinungsfreiheit herstellt.[66] In Entschließung 2590 werden sowohl die Mitgliedstaaten als auch die Anbieter von Social-Media-Plattformen aufgefordert, Systeme zur Inhaltsmoderation einzurichten, die Transparenz, Zugang, Aufsicht und Rechtsbehelfsmechanismen gewährleisten und dafür sorgen, dass

[58] Ebd., Abs. 24.
[59] Ebd., Abs. 33.
[60] Ebd., Abs. 34 ff.
[61] Europarat, Lenkungsausschuss für Medien und Informationsgesellschaft, Leitfaden zur Moderation von Inhalten (engl.), 2021.
[62] Europarat, Lenkungsausschuss für Medien und Informationsgesellschaft, Leitfaden zur Bekämpfung der Verbreitung von Falsch- und Desinformationen im Internet durch Faktenprüfung und menschenrechtskonforme Lösungen für die Gestaltung von Plattformen (engl.), 2024
[63] Europarat, Parlamentarische Versammlung, Regulierung der Moderation von Inhalten bei sozialen Medien zur Sicherung der Meinungsfreiheit (engl.), PACE-Entschließung 2590.
[64] Ebd., Abs. 2.
[65] Ebd., Abs. 3.
[66] Ebd., Abs. 4 ff.

insbesondere bei legalen Inhalten oder Inhalten von öffentlichem Interesse Zurückhaltung geübt wird.[67]

Bei der Moderation von Inhalten, aber auch in anderen Fällen von Inhaltsplatzierung setzen Anbieter zunehmend auf algorithmische Systeme einschließlich KI. Am 17. Mai 2024 verabschiedete der Europarat mit dem Rahmenübereinkommen über künstliche Intelligenz und Menschenrechte, Demokratie und Rechtsstaatlichkeit[68] den ersten Vertrag zum Einsatz von KI, der für die Unterzeichnerstaaten international rechtsverbindlich ist. Die Staaten werden ermutigt, dafür zu sorgen, dass die Rechtsvorschriften für KI-Systeme Transparenz und Rechenschaftspflicht gewährleisten und gleichzeitig die Grundprinzipien der Demokratie wahren sowie eine wirksame Aufsicht und eine durchgängige Überprüfung dieser Systeme vorsehen.[69]

Während alle zuvor erwähnten Empfehlungen Maßnahmen zur Sicherung der Meinungsfreiheit vorsehen, schreibt der Rahmen des Europarats – als Grundrechtsrahmen – keine spezifischen Durchsetzungsmechanismen vor. In den folgenden Abschnitten wird daher die einschlägige Rechtsprechung des EGMR untersucht – unterteilt in thematische Blöcke, die das System der abgestuften Reaktion veranschaulichen.

2.1.2 Internetvermittler und andere Online-Akteure als Adressaten von Durchsetzungsmaßnahmen

Wie bereits oben erwähnt und vom EGMR hervorgehoben, spielt das Internet eine wichtige Rolle „für die Wahrnehmung des Rechts auf freie Meinungsäußerung im Allgemeinen".[70] Natürlich richten sich die Durchsetzungsmaßnahmen in erster Linie gegen die ursprünglichen Verfasser rechtswidriger Inhalte,[71] doch waren auch Internetvermittler als Übermittler von Inhalten schon früh Gegenstand von Durchsetzungsmaßnahmen. Einer der Gründe dafür ist, dass sie leichter zu identifizieren sind und gleichzeitig die Möglichkeit haben, den Zugang zu rechtswidrigen Inhalten zu beschränken oder diese zu löschen. Mit der Diversifizierung der Rollen der Vermittler von eher passiven Durchleitern oder Hostern hin zu aktiven Rollen bei der Produktion und Verbreitung von Inhalten, zum Beispiel durch Verwaltung oder Kuratierung der Inhalte oder eine redaktionelle Rolle, entwickelt sich auch die Rechtsprechung weiter. Der abgestufte Ansatz aus den Empfehlungen des Ministerkomitees spiegelt sich auch in der Rechtsprechung des EGMR wider, der sich mit

[67] Ebd., Abs. 10 ff.
[68] Europarat, Rahmenübereinkommen über künstliche Intelligenz und Menschenrechte, Demokratie und Rechtsstaatlichkeit (engl.), CETS Nr. 225. Einzelheiten zum Status der Unterzeichner und zum Inkrafttreten finden sich hier.
[69] Für einen Überblick über die Leitprinzipien der KI-Regulierung siehe Cole, M. D., "AI Regulation and Governance on a Global Scale": An Overview of International, Regional and National Instruments" in *Journal of AI and Regulation*, 1(1), 2024, S. 126-142; zum Rahmenübereinkommen siehe Gartner, M., "Council of Europe: States Adopt First Binding Framework Treaty on AI" in *Journal of AI and Regulation*, 1(3), 2024, S. 342-349.
[70] *Times Newspapers Ltd (Nr. 1 & 2) gegen das Vereinigte Königreich*, Nr.3002/03 und 23676/03, Rn. 27.
[71] Zur Haftung der ursprünglichen Verfasser eines Kommentars siehe *Delfi As gegen Estland* [GK], Nr. 64569/09, Rn. 147 ff.

Internetvermittlern vor dem Hintergrund ihrer Rechte, Pflichten und Verantwortlichkeiten befasst.

2.1.2.1 Pflichten und Verantwortlichkeiten von Internetvermittlern in Bezug auf rechtswidrige Inhalte Dritter

Die objektive Haftung von Internetportalen für Inhalte, die von Dritten stammen, wird als unvereinbar mit Artikel 10 der EMRK angesehen.[72] Auch bei zivilrechtlichen Maßnahmen kann eine Haftungszurechnung für Kommentare Dritter negative Folgen zum Beispiel für den Kommentarbereich eines Online-Portals haben und eine abschreckende Wirkung auf die freie Meinungsäußerung im Internet ausüben.[73] Diese kann insbesondere für nicht kommerzielle Websites abträglich sein.[74] In Fällen, in denen eine strafrechtliche Verantwortlichkeit besteht – wo Maßnahmen dem Schweregrad des fraglichen Inhalts angepasst und verhältnismäßig sein müssen –, können solche Auswirkungen auf die freie Meinungsäußerung daher als potenziell verstärkt angesehen werden.[75]

In Fällen von rechtswidrigen Nutzerkommentaren Dritter können die Rechte und Interessen anderer und der Gesellschaft als Ganzes die Staaten jedoch dazu berechtigen, Internetvermittler haftbar zu machen, ohne gegen Artikel 10 EMRK zu verstoßen, wenn Internetvermittler keine Maßnahmen ergriffen haben, um eindeutig rechtswidrige Kommentare unverzüglich zu entfernen, selbst wenn es keine Meldung des mutmaßlichen Opfers oder von Dritten gab.

In dem wegweisenden Rechtsstreit *Delfi AS gegen Estland* diskutierte der EGMR erstmals die zivilrechtliche Verantwortung und Sorgfaltspflicht eines professionellen Hostinganbieters für rufschädigende Äußerungen.[76] Obwohl das von Delfi AS betriebene große Online-Nachrichtenportal über ein automatisches Filtersystem und ein Verfahren zur Meldung und Entfernung (*Notice-and-Takedown*) verfügte, stellten estnische Gerichte die Haftung für rechtswidrige Kommentare Dritter fest, die als Reaktion auf einen der eigenen Artikel auf der Website des Portals gepostet wurden.

In Anbetracht des besonderen Charakters des Internets erkannte der EGMR an, dass sich die „Pflichten und Verantwortlichkeiten "eines Online-Nachrichtenportals im Sinne von Artikel 10 EMRK in Bezug auf Inhalte Dritter bis zu einem gewissen Grad von denen eines herkömmlichen Herausgebers unterscheiden können.[77] Obwohl Internet-Nachrichtenportale keine Herausgeber von Inhalten Dritter im herkömmlichen Sinne sind, können sie unter bestimmten Umständen für diese Inhalte verantwortlich gemacht

---

[72] *Magyar Tartalomszolgáltatók Egyesülete und Index.hu Zrt gegen Ungarn*, Nr. 22947/13 (EGMR, 2. Februar 2016), Rn. 91.

[73] *Sanchez gegen Frankreich*, Nr. 45581/15 (EGMR [GK], 15. Mai 2023), Rn. 205 mit Verweis auf *Magyar Tartalomszolgáltatók Egyesülete und Index.hu Zrt gegen Ungarn*, Nr. 22947/13, Rn. 86.

[74] *Magyar Tartalomszolgáltatók Egyesülete und Index.hu Zrt. gegen Ungarn*, Nr. 22947/13, Rn. 86.

[75] *Sanchez gegen Frankreich*, Nr. 45581/15, Rn. 205.

[76] Für einen Kommentar zur Rechtssache siehe Korpisaari, P., "From *Delfi* to *Sanchez* - when can an online communication platform be responsible for third party comments? An analysis of the practice of the ECtHR and some reflections on the Digital Services Act", in *Journal of Media Law,* 14(2), 2022, S. 352-377.

[77] *Delfi As gegen Estland* [GK], Nr. 64569/09, Rn. 113; siehe auch *Orlovskaya Iskra gegen Russland*, Nr. 42911/08 (EGMR, 21. Februar 2017), Rn. 109.

werden.[78] Die unterschiedliche Behandlung von Inhalten Dritter bei Internet-Nachrichtenportalen und traditionellen Herausgebern entspricht internationalen Standards, die zunehmend die Notwendigkeit anerkennen, unterschiedliche Rechtsgrundsätze auf traditionelle Medien und Online-Nachrichtenportale anzuwenden, auf denen Inhalte Dritter in der Regel verbreitet werden, ohne dass der Veröffentlichungsprozess einer redaktionellen Kontrolle unterliegt.[79]

Um zu beurteilen, ob ein Internetportalbetreiber für Inhalte Dritter haftbar gemacht werden kann, hat der EGMR vier Kriterien festgelegt, die sicherstellen sollen, dass eine faire Abwägung der konkurrierenden Interessen – des Rechts auf freie Meinungsäußerung und des Rechts auf Schutz des guten Rufs einer anderen Person oder Einrichtung – stattfindet.[80]

Diese Kriterien, die für die zivil-, straf- und verwaltungsrechtliche Haftung gelten, sind (1) der Kontext der Kommentare, (2) die Haftung der Verfasser der Kommentare, (3) die von den Beschwerdeführern ergriffenen Maßnahmen und das Verhalten der geschädigten Partei sowie (4) die Folgen des innerstaatlichen Verfahrens für die Beschwerdeführer.

Die Prüfung des Kontextes und des Inhalts der streitigen Kommentare ist erforderlich, um die Rechtmäßigkeit der Inhalte Dritter insgesamt festzustellen, das heißt ob die zulässigen Grenzen der Meinungsfreiheit unter Berücksichtigung des unmittelbaren Kontextes und der Besonderheiten des Kommunikationsstils auf bestimmten Internetportalen überschritten wurden.[81] So haben zum Beispiel rassistische und fremdenfeindliche Äußerungen in einem Wahlkampfkontext und in einem unruhigen politischen und gesellschaftlichen Klima größere und schädlichere Auswirkungen.[82]

In der Rechtssache *Delfi AS gegen Estland* erstreckte sich die Beurteilung des Kontextes auf den professionellen und kommerziellen Charakter der Nachrichtenplattform.[83] In Anbetracht der kommerziellen Natur des Bestrebens, eine große Zahl von Kommentaren zu erhalten, stellte der Gerichtshof fest, dass Delfi zu unterscheiden ist von

> *anderen Foren im Internet, wo Kommentare von Dritten verbreitet werden können, wie etwa ein Internet-Diskussionsforum oder eine Pinnwand, auf der die Nutzer ihre Ideen zu beliebigen Themen frei darlegen können, ohne dass die Diskussion durch irgendeinen Input vom Forumsmanager gelenkt wird, oder eine Social-Media-Plattform, wo der Plattformanbieter keinerlei Inhalte anbietet und der Inhalteanbieter eine Privatperson sein kann, welche die Website oder einen Blog als Hobby betreibt.*[84]

Während professionelle Einrichtungen, die soziale Netzwerke schaffen und sie anderen Nutzern zur Verfügung stellen, zwangsläufig bestimmte Verpflichtungen haben, fällt der

---

[78] *Magyar Tartalomszolgáltatók Egyesülete und Index.hu Zrt. gegen Ungarn*, Nr. 22947/13, Rn. 62.
[79] Siehe *Delfi As gegen Estland* [GK], Nr. 64569/09, Rn. 112 ff.
[80] Ebd., Rn. 142 ff.; *Magyar Tartalomszolgáltatók Egyesülete und Index.hu Zrt gegen Ungarn*, Nr. 22947/13, Rn. 61.
[81] *Sanchez gegen Frankreich*, Nr. 45581/15, Rn. 174 ff.; *Magyar Tartalomszolgáltatók Egyesülete und Index.hu Zrt gegen Ungarn*, Nr. 22947/13, Rn. 77.
[82] *Sanchez gegen Frankreich*, Nr. 45581/15, Rn. 176.
[83] *Delfi As gegen Estland* [GK], Nr. 64569/09, Rn. 144.
[84] Ebd., Rn. 116.

Inhaber eines Facebook-Kontos nur dann in die Kategorie der „sonstigen Internetforen, in denen Kommentare Dritter verbreitet werden können", wenn er seine Facebook-Pinnwand zur Verfügung stellt.[85] Dies entbindet den Kontoinhaber oder einen anderen Anbieter jedoch nicht von seinen Pflichten und seiner Verantwortung in Bezug auf Inhalte Dritter, da ein Haftungsausschluss Missbrauch und Zweckentfremdung einschließlich Hassrede und Desinformation erleichtern oder sogar fördern könnte.[86]

Die Haftungszurechnung für Kommentare Dritter hängt von den ergriffenen Maßnahmen und dem Verhalten der geschädigten Partei ab.[87] Die erforderlichen Maßnahmen variieren je nach den verfügbaren Moderations- oder Überprüfungstechniken und müssen sorgfältig geprüft werden, um eine abschreckende Wirkung auf die freie Meinungsäußerung zu vermeiden.[88] In jedem Fall müssen die widerstreitenden Interessen gegeneinander abgewogen werden.[89] Eine zivilrechtliche Haftung eines Internet-Nachrichtenportals für die Weigerung oder das Versäumnis, eindeutig rechtswidrige Inhalte wie in der Rechtssache *Delfi AS gegen Estland* zu entfernen, kann auch ohne Anzeige seitens der geschädigten Partei oder Dritter gerechtfertigt sein,[90] was bedeutet, dass eine gewisse Form der Überwachung erforderlich wäre, insbesondere wenn Inhalte hitzige Diskussionen auslösen können.[91] Der EGMR hält es nämlich für weitgehend unumstritten, dass ein Mindestmaß an nachträglicher Moderation oder automatischer Filterung wünschenswert ist, um eindeutig rechtswidrige Kommentare rasch zu erkennen und zu entfernen, und zwar idealerweise innerhalb einer angemessenen Frist, auch wenn keine Anzeige einer geschädigten Partei vorliegt.[92]

2.1.2.2 Pflichten und Verantwortlichkeiten nicht professioneller Einrichtungen bei rechtswidrigen Inhalten Dritter

Die oben beschriebene Verantwortlichkeit kann entweder bei der Hostingplattform liegen, die als professioneller Anbieter fungiert, oder bei Kontoinhabern, die ihre eigenen Inhalte veröffentlichen und anderen erlauben, diese zu kommentieren.[93] In der Rechtssache *Sanchez gegen Frankreich* prüfte der EGMR, inwieweit die Haftungsregelung für Hostingplattformen auf den Kontoinhaber einer Facebook-Seite angewandt werden kann, wenn Dritte rechtswidrige Kommentare auf dessen Pinnwand posten. In diesem Szenario erkannte der EGMR an, dass eine vorherige Inhaltsmoderation praktisch unmöglich ist –

[85] *Sanchez gegen Frankreich*, Nr. 45581/15, Rn. 180.
[86] Ebd., Rn. 185.
[87] Für einen Überblick darüber, was von Hostingplattformanbietern erwartet werden kann, siehe Korpisaari, P., "From *Delfi* to *Sanchez* - when can an online communication platform be responsible for third party comments? An analysis of the practice of the ECtHR and some reflections on the Digital Services Act", in *Journal of Media Law,* 14(2), 2022, S. 352-377.
[88] Siehe *Sanchez gegen Frankreich*, Nr. 45581/15, Rn. 182.
[89] *Magyar Tartalomszolgáltatók Egyesülete und Index.hu Zrt. gegen Ungarn*, Nr. 22947/13, Rn. 88.
[90] Ebd., Rn. 91 mit Verweis auf *Delfi As gegen Estland* [GK], Nr. 64569/09, Rn. 157. Siehe auch Enarsson, T., "Navigating hate speech and content moderation under the DSA: Insights from ECtHR case law",in *Information & Communications Technology Law*, 33(3), 2024, S. 384-401, 392 ff.
[91] Siehe *Magyar Tartalomszolgáltatók Egyesülete und Index.hu Zrt. gegen Ungarn*, Nr. 22947/13, Rn. 73.
[92] *Sanchez gegen Frankreich*, Nr. 45581/15, Rn. 190.
[93] Ebd.

technisch, aber auch personell, wenn das Konto für nicht kommerzielle Zwecke genutzt wird und sehr beliebt ist.[94]

Eine strafrechtliche Verurteilung nach nationalem Recht wegen Nichtentfernung von Inhalten Dritter, bei der davon ausgegangen wird, dass der Kontoinhaber einer Facebook-Pinnwand die Rolle eines Inhaltsproduzenten übernommen hat, stellt keinen Verstoß gegen Artikel 10 EMRK dar, wenn der Kontoinhaber bestimmte Pflichten und Verantwortlichkeiten nicht beachtet hat. Zu berücksichtigende Sachverhalte sind unter anderem die persönliche Einschätzungsfähigkeit des Kontoinhabers oder allgemeiner gesagt des Vermittlers; so muss sich beispielsweise ein Politiker, der sein Social-Media-Konto für politische Zwecke nutzt und über Erfahrung in öffentlicher Kommunikation verfügt, des erhöhten Risikos bewusst sein, dass überzogene oder unangemessene Äußerungen als Reaktion auf einen Post im Wahlkampf erscheinen und ein größeres Publikum erreichen könnten.[95] Die Änderung der Datenschutzeinstellungen kann eine Risikominderungsmaßnahme sein, um die Sichtbarkeit zu verringern oder einzuschränken, wer eine Antwort auf einen Post einstellen kann. Wenn festgestellt werden kann, dass der Inhaber Kenntnis von den durch einige Kommentare entstandenen Problemen hatte, darf eine minimale Überprüfung erwartet werden.[96] Letzteres gilt insbesondere dann, wenn das Social-Media-Konto täglich aufgerufen wird und bestimmte Nutzer im Anschluss an einen ersten Post in einer Konversation aufeinander reagieren und sich gegenseitig ergänzen und wenn der Inhalt dieser Konversation als rechtswidrig gemeldet wurde.[97] Während in der Rechtssache *Sanchez gegen Frankreich* die strafrechtliche Verurteilung des Inhabers eines Facebook-Kontos wegen der Kommentare Dritter nicht als Verletzung von Artikel 10 EMRK gewertet wurde, ist der Schwellenwert zur Feststellung von „Kenntnis" rechtswidriger Inhalte höchst umstritten, wie die zustimmenden[98] und abweichenden Sondervoten[99] in der Rechtssache *Sanchez gegen Frankreich* zeigen.[100]

Im Einklang mit den Normen des internationalen Rechts kann eine Haftung vermieden werden, wenn rechtswidrige Inhalte „unverzüglich" entfernt werden, sobald der Vermittler von der Rechtswidrigkeit der Inhalte Kenntnis erlangt.[101]

2.1.2.3 Pflichten und Verantwortlichkeiten der Ersteller von Hyperlinks

Ähnlich wie bei der objektiven Haftung von Internetportalen für Inhalte, die von Dritten stammen, ist eine objektive Haftung für Hyperlinks nicht mit Artikel 10 EMRK vereinbar. Hyperlinks unterscheiden sich von herkömmlichen Veröffentlichungshandlungen, da sie die Nutzer lediglich auf Inhalte verweisen, die an anderer Stelle im Internet verfügbar sind, und

[94] Ebd., Rn. 185.
[95] Ebd., Rn. 186 ff.
[96] Ebd., Rn. 194.
[97] Ebd., Rn. 199 ff.
[98] Ebd., zustimmendes Sondervotum von Richter Kūris.
[99] Ebd., abweichendes Sondervotum von Richter Ravarani; abweichendes Sondervotum von Richter Bošnjak; gemeinsames abweichendes Sondervotum der Richter Wojtyczek und Zünd.
[100] Siehe auch Husovec, M. et al., "Grand confusion after *Sanchez v. France*: Seven reasons for concern about Strasbourg jurisprudence on intermediaries", in *Maastricht Journal of European and Comparative Law*, 31(3), 2024, S. 385-411.
[101] *Delfi As gegen Estland* [GK], Nr. 64569/09, Rn, 153.

keine eigenständige Wiedergabehandlung darstellen.[102] Sie sollen es Nutzern ermöglichen, in einem Netz, in dem eine immense Menge an Informationen verfügbar ist, von Material zu Material zu navigieren.[103] Zudem hat die Person, die über einen Hyperlink auf Informationen verweist, keine Kontrolle über den Inhalt, zu dem der Zugang ermöglicht wird und der sich nach der Erstellung des Links ändern kann.[104]

Aufgrund dieser Besonderheiten sind ausreichende und einschlägige Gründe erforderlich, um die Haftung des Erstellers eines Hyperlinks festzustellen, was eine sorgfältige Bewertung der „Pflichten und Verantwortlichkeiten" des Linkerstellers erfordert. Es ist zu prüfen, ob der Ersteller (1) dem streitigen Inhalt beigepflichtet hat, (2) den streitigen Inhalt wiederholt hat (ohne ihm beizupflichten), (3) lediglich einen Hyperlink zu dem streitigen Inhalt gesetzt hat (ohne ihm beizupflichten oder ihn zu wiederholen), (4) gewusst hat oder vernünftigerweise hätte wissen können, dass der streitige Inhalt rufschädigend oder anderweitig rechtswidrig war, und (5) in gutem Glauben gehandelt hat, die journalistische Ethik beachtet und die journalistische Sorgfaltspflicht walten lassen hat, die von einem verantwortungsvollen Journalismus erwartet werden kann..[105]

In diesem Zusammenhang ist anzumerken, dass eine allgemeine Verpflichtung für Journalisten, sich systematisch und formal vom Inhalt eines Zitats zu distanzieren, das andere beleidigen oder provozieren oder deren Ruf schädigen könnte, nicht mit der Rolle der Presse vereinbar ist, Informationen zu aktuellen Ereignissen, Meinungen und Ideen zu liefern.[106]

Die gleiche Argumentation wurde in der Folge auf das Teilen von Inhalten Dritter über Social-Media-Plattformen angewandt, wobei festgestellt wurde, dass das Teilen bestimmter Inhalte ein gängiges Mittel der Kommunikation und sozialen Interaktion ist und zu einer informierten Bürgerschaft beitragen kann.[107] Wenn jedoch Material ohne weitere Einordnung aus dem Zusammenhang gerissen wird und vernünftigerweise als Anstiftung zu Unfriede oder Gewalt aus ethnischen Gründen wahrgenommen werden könnte, kann eine Haftung für die Zugänglichmachung von Inhalten Dritter gerechtfertigt sein.[108]

---

[102] *Magyar Jeti Zrt gegen Ungarn*, Nr. 11257/16 (EGMR, 4. Dezember 2018), Rn. 74. Diese Frage wurde zuvor vom EuGH im Zusammenhang mit dem Begriff „öffentliche Wiedergabe" im Sinne von Art. 3 Abs. 1 der Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft erörtert, siehe C-466/12 *Svensson und andere gegen Retriever Sverige AB* (EuGH, 13. Februar 2014), ECLI:EU:C:2014:76, Rn. 18 ff.

[103] Ebd., Rn. 73.

[104] Ebd., Rn. 75.

[105] Ebd., Rn. 77.

[106] Ebd., Rn. 80 mit Verweis auf *Thoma gegen Luxemburg*, Nr. 38432/97 (EGMR, 29. März 2001), Rn. 64. Eine ähnliche Frage ist derzeit beim EuGH im Rahmen eines Vorabentscheidungsersuchens des Landgerichts Budapest anhängig (C-843/24 *24.hu*).

[107] *Kilin gegen Russland*, Nr. 10271/12 (EGMR, 11. Mai 2021), Rn. 79.

[108] Ebd., Rn. 87 ff.

2.1.3 Das Spektrum der Durchsetzungsmaßnahmen

Während die in den allgemeinen Geschäftsbedingungen von Social-Media-Plattformen enthaltenen Regeln zur Inhaltsmoderation auch die Sperrung oder Löschung eines Nutzerkontos vorsehen können,[109] hat der EGMR in einer Reihe von Urteilen Grenzen für staatliche Durchsetzungsmaßnahmen gesetzt. Die Löschung von Inhalten oder Sperrung des Zugangs zu einem bestimmten rechtswidrigen Inhalt wird den Dreistufentest nach Artikel 10 EMRK wahrscheinlich bestehen, es ist jedoch unwahrscheinlich, dass eine Maßnahme, die über den rechtswidrigen Inhalt als solchen hinausgeht und in rechtmäßige Inhalte eingreift, das Kriterium der Vorhersehbarkeit erfüllt; sie dürfte auch den Verhältnismäßigkeitstest nicht bestehen.

2.1.3.1 Sperrung des Zugangs zu Websites

Der EGMR musste sich bereits mehrfach mit Maßnahmen nationaler Behörden zur Sperrung des Zugangs zu bestimmten Websites befassen. Eine pauschale Sperrung der YouTube-Website führte zu einem unzulässigen Eingriff in das Recht der Nutzer – die nicht direkt Ziel der Maßnahme waren –, Informationen oder Ideen zu empfangen und weiterzugeben; daher waren diese Nutzer berechtigt, dieses Recht vor dem Gerichtshof geltend zu machen.[110] In diesem Fall führte die Art und Weise, wie nationale Gerichtsentscheidungen zu bestimmten Inhalten umgesetzt werden mussten, dazu, dass der Zugang zur gesamten Website gesperrt wurde.[111] Aufgrund der Einzigartigkeit der betreffenden Plattform wurden die potenziellen Auswirkungen der Maßnahme, die große Mengen von Informationen unzugänglich machte, als wesentliche Einschränkung der Rechte der Nutzer mit erheblicher Nebenwirkung angesehen.[112]

Im Gegensatz dazu reichte die bloße Tatsache, dass Nutzer indirekt von einer Sperrung zweier Musiktauschbörsen betroffen waren, nicht aus, um einen „Opferstatus“ gemäß Artikel 34 EMRK geltend zu machen, und begründete somit kein Klagerecht der Nutzer dieses Dienstes vor dem EGMR.[113] Die Sperrung des Zugangs zu einer Website kann auch zur Sperrung einer anderen Website mit derselben IP-Adresse führen; diese Maßnahme schränkt die Rechte von Internetnutzern erheblich ein und dürfte das Kriterium der Vorhersehbarkeit gemäß der EMRK nicht erfüllen.[114]

In Fällen von Vorabbeschränkungen ist ein rechtlicher Rahmen erforderlich, der sowohl eine strenge Kontrolle des Umfangs der Verbote als auch eine wirksame

---

[109] Europarat, Parlamentarische Versammlung, Regulierung der Moderation von Inhalten bei sozialen Medien zur Sicherung der Meinungsfreiheit (engl.), (PACE-Entschließung 2590, Art. 3), 2025.
[110] *Cengiz und andere gegen Türkiye*, Nr.48226/10 und 14027/11, Rn. 52 ff. und *Ahmet Yildirim gegen Türkiye*, Nr. 3111/10, Rn. 49 ff.
[111] *Ahmet Yildirim gegen Türkiye*, No. 3111/10, Rn. 66.
[112] Ebd.; *Cengiz und andere gegen Türkiye*, Nr . 48226/10 und 14027/11, Rn. 64.
[113] *Akdeniz und andere gegen Türkiye*, Nr. 41139/15 und 41146/15 (EGMR, 4. Mai 2021), Rn. 24.
[114] *Vladimir Kharitonov gegen Russland*, Nr. 10795/14 (EGMR, 23. Juni 2020), Rn. 45 ff. Das Hauptproblem bei der Sperrung von IP-Adressen ist, dass viele Adressen von mehreren Inhalteanbietern gemeinsam genutzt werden (gemeinsames Webhosting). Wenn eine bestimmte IP-Adresse gesperrt wird, sind alle Webinhalte unter dieser IP-Adresse nicht mehr zugänglich.

gerichtliche Überprüfung gewährleistet, um jeglichen Machtmissbrauch zu verhindern.[115] Die gerichtliche Überprüfung einer Sperrmaßnahme, die auf einer Abwägung der konkurrierenden Interessen beruht und einen Ausgleich zwischen ihnen erreichen soll, ist ohne einen Rahmen, der präzise und spezifische Regeln für die Anwendung präventiver Einschränkungen der Meinungsfreiheit festlegt, nicht denkbar.[116] In Fällen, in denen es um die Vorabbeschränkung von Veröffentlichungen geht, die zur Teilnahme an einer öffentlichen Veranstaltung aufrufen, muss es möglich sein, eine gerichtliche Überprüfung der Sperrmaßnahme vor dem Datum der betreffenden öffentlichen Veranstaltung zu erwirken, damit die Überprüfung nicht sinnlos wird.[117]

Eine umfassende Sperranordnung für eine Website wird vom EGMR als äußerste Maßnahme angesehen, vergleichbar dem Verbot einer Zeitung oder eines Rundfunksenders.[118] Dementsprechend wurde die ungerechtfertigte vollständige Sperrung von Medien, bei der nicht zwischen rechtswidrigen und rechtmäßigen Inhalten unterschieden wurde, vom EGMR als willkürlich und offenkundig unangemessen betrachtet.[119] Das Gleiche gilt, wenn die Sperrung aufrechterhalten wird, obwohl das als rechtswidrig erachtete Material entfernt wurde.[120]

Überdies muss sichergestellt werden, dass jede Sperrung in einem angemessenen Verhältnis zum verfolgten Ziel steht. Wie bereits erwähnt, müssen Vorschriften zu rechtswidrigen Inhalten und die entsprechenden Durchsetzungsmaßnahmen eng aufeinander zugeschnitten sein. Jede Sperrmaßnahme sollte strikt auf den rechtswidrigen Inhalt abzielen und willkürliche oder übermäßige Auswirkungen vermeiden. Entsprechend lässt sich schlussfolgern, dass pauschale Sperranordnungen wahrscheinlich nicht mit Artikel 10 EMRK vereinbar sind; Behörden müssen prüfen, ob mit weniger einschneidenden Alternativen wie zum Beispiel der Entfernung bestimmter Posts dasselbe Ziel erreicht werden kann, ohne den Zugang zu rechtmäßiger Meinungsäußerung unverhältnismäßig zu beschränken. Dabei sind insbesondere die Auswirkungen auf Dritte und die abschreckende Wirkung auf die Redefreiheit im Internet zu berücksichtigen.

2.1.3.2 Sperrung von Social-Media-Konten

Die Sperrung von Social-Media-Konten wurde in der Rechtssache *Kablis gegen Russland* untersucht, in der ein Social-Media-Konto unter anderem mit der Begründung gesperrt wurde, dass eine solche Maßnahme notwendig war, um Gesetzesverstöße im Bereich der Informationsverbreitung zu verhindern und die öffentliche Ordnung aufrechtzuerhalten. Zunächst stellte der EGMR fest, dass die Möglichkeit, die betroffene Person könnte einfach ein neues Social-Media-Konto einrichten, für die Beurteilung, ob der Eingriff gerechtfertigt

[115] *Kablis gegen Russland*, Nr. 48310/16 und 59663/17 (EGMR 30. April 2019), Rn. 92.
[116] *Ahmet Yildirim gegen Türkiye*, No. 3111/10, Rn. 64.
[117] *Kablis gegen Russland*, Nr.48310/16 und 59663/17, Rn. 85 ff.
[118] *OOO Flavus und andere gegen Russland*, Nr. 12468/15, 23489/15 und 19074/16 (EGMR, 23. Juni 2020), Rn. 37 und *Bulgakov gegen Russland*, Nr. 20159/15 (EGMR, 23. Juni 2020), Rn. 34 mit weiteren Verweisen.
[119] *OOO Flavus und andere gegen Russland*, Nr. 12468/15, 23489/15 und 19074/16, Rn. 34; *Bulgakov gegen Russland*, Nr. 20159/15, Rn. 34.
[120] *Bulgakov gegen Russland*, Nr. 20159/15, Rn. 34 ff.

war, irrelevant ist.[121] Da jeder Eingriff in das Recht auf freie Meinungsäußerung in einer demokratischen Gesellschaft notwendig sein muss, um rechtmäßig zu sein, muss er einer zwingenden gesellschaftlichen Notwendigkeit entsprechen, und die Behörden müssen maßgebliche und ausreichende Gründe für die Einschränkung anführen. Ein solcher Grund könnte zum Beispiel sein, dass das Social-Media-Konto ein Risiko für die öffentliche Sicherheit darstellt oder zu öffentlicher Unruhe oder einer Straftat führen könnte.[122] Ähnlich wie bei der Sperrung einer ganzen Website oder einzelner Seiten müssen die Behörden nach Artikel 10 EMRK unter anderem die Tatsache berücksichtigen, dass durch die Sperrung eines gesamten Social-Media-Kontos große Mengen an Informationen unzugänglich werden. Eine solche Maßnahme schränkt die Rechte der Internetnutzer erheblich ein und hat beträchtliche Nebeneffekte für das Material, das nicht als rechtswidrig eingestuft wurde.[123] Eine sorgfältige Prüfung ist daher unerlässlich, um sicherzustellen, dass eine solche Einschränkung in einem angemessenen Verhältnis zum verfolgten legitimen Ziel steht.

2.2 Der Rechtsrahmen der Europäischen Union zur Regulierung von Inhalten und zu Durchsetzungsmaßnahmen

Dr Mark D. Cole, Wissenschaftlicher Direktor des Instituts für Europäisches Medienrecht (EMR) und Professor für Medien- und Telekommunikationsrecht, Universität Luxemburg

2.2.1 Durchsetzungsmaßnahmen im Lichte des EU-Primärrechts

Nach der Betrachtung der Grenzen, die Artikel 10 EMRK den Durchsetzungsmaßnahmen der EMRK-Vertragsstaaten setzt, müssen auch die besonderen Herausforderungen beleuchtet werden, die sich bei der Durchsetzung im Rahmen des EU-Primärrechts ergeben.[124] Die Grundrechte setzen bereits wesentliche Grenzen für staatliches Handeln; die wirksame Umsetzung der Regulierung von Inhalten – insbesondere im digitalen Umfeld – muss aber auch im Lichte der EU-Verfassungsgrundsätze wie der Kompetenzverteilung,[125] der Binnenmarktfreiheiten, der gemeinsamen Werte und des Grundsatzes der loyalen Zusammenarbeit gemäß Artikel 4 Absatz 3 des Vertrags über die Europäische Union (EU-

[121] *Kablis gegen Russland*, Nr. 48310/16 und 59663/17, Rn. 84.
[122] Ebd., Rn. 88.
[123] Ebd., Rn. 94 mit Verweis auf *Ahmet Yildirim gegen Türkiye*, Nr. 3111/10, Rn 66, und *Cengiz und andere gegen Türkiye*, Nr. 48226/10 und 14027/11, Rn. 64.
[124] Siehe in diesem Zusammenhang auch Ukrow, J., „Der Rahmen für die Rechtsdurchsetzung gegen Online-Anbieter und ausländische Inhalte-Anbieter" in Cappello, M. (Hrsg.), Medienrechtsdurchsetzung ohne Grenzen, IRIS *Spezial,* Europäische Audiovisuelle Informationsstelle, Straßburg 2018.
[125] Siehe Cole, M. D., Ukrow, J. und Etteldorf, C., *On the Allocation of Competences between the European Union and its Member States in the Media Sector*, Nomos, Baden-Baden, 2021.

Vertrag - EUV) bewertet werden.[126] Diese Dimensionen werfen komplexe Fragen dazu auf, wie Durchsetzungsmaßnahmen unter den Mitgliedstaaten koordiniert werden können.

Wenn es um den Binnenmarkt und die Beziehungen zwischen EU-Mitgliedstaaten sowie zu den Institutionen auf EU-Ebene geht, kommen im Wesentlichen zwei Aspekte ins Spiel. Erstens sieht der EU-Rechtsrahmen besondere Regeln für die Streitbeilegung vor. Zweitens werden Interaktionen zwischen den Mitgliedstaaten durch Grundsätze wie dem „Herkunftslandprinzip" bestimmt,[127] das im EU-Recht eine herausragende Rolle spielt und ein Eckpfeiler des Binnenmarktes ist, insbesondere durch die Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH).[128] Nach diesem Grundsatz muss ein in einem Mitgliedstaat niedergelassener Wirtschaftsteilnehmer die Rechtsvorschriften seines Herkunftslandes einhalten, unterliegt aber keinen zusätzlichen rechtlichen Verpflichtungen in dem Mitgliedstaat/den Mitgliedstaaten, in dem/denen seine Waren oder Dienstleistungen angeboten werden oder in Anspruch genommen werden können, das heißt es sollten keine zusätzlichen Anforderungen neben den am Ort der Niederlassung geltenden auferlegt werden. Dieser Ansatz verringert den finanziellen, administrativen und personellen Aufwand und verhindert doppelte Kontrollen oder Anforderungen, die ansonsten die grenzüberschreitende Wirtschaftstätigkeit behindern würden.

Die Verantwortung für die Beurteilung der Rechtmäßigkeit eines Dienstes liegt folglich in erster Linie beim Herkunftsmitgliedstaat. Die Möglichkeit, das Herkunftsland zu wählen, ist in der Niederlassungsfreiheit verankert, die es Unternehmen und Selbstständigen erlaubt, den Ort ihrer Niederlassung innerhalb der EU frei zu wählen. Die eingeschränkte Möglichkeit der Mitgliedstaaten, gegen ausländische Diensteanbieter vorzugehen, gilt jedoch nur im Rahmen des freien Dienstleistungsverkehrs, wenn der Anbieter in einem anderen Mitgliedstaat oder in einem Drittstaat, der Vertragspartei des Abkommens über den Europäischen Wirtschaftsraum (EWR) ist, niedergelassen ist. Anbieter, die nicht in einem EU-/EWR-Mitgliedstaat niedergelassen sind, unterliegen hingegen den allgemeinen Regeln des internationalen öffentlichen Rechts. Darüber hinaus kann Sekundärrecht weitere spezifische Ausnahmemöglichkeiten vom Herkunftslandprinzip vorsehen. Bestimmungsmitgliedstaaten oder solche, in denen ein Dienst eines in einem anderen Mitgliedstaat niedergelassenen Anbieters in Anspruch genommen wird, können ausnahmsweise eingreifen – nämlich dann, wenn eine begründete und verhältnismäßige Beschränkung des freien Dienstleistungsverkehrs gerechtfertigt ist. Dies kann auf expliziten

---

[126] Vertrag über die Europäische Union (konsolidierte Fassung), 15 März 2025.

[127] Für eine allgemeine Diskussion des Herkunftslandprinzips siehe zum Beispiel Cole, M. D., "*The Country of Origin Principle - From State Sovereignty under Public International Law to Inclusion in the Audiovisual Media Services Directive of the European Union*" in Meng, W., Ress, G. und Stein, T. (Hrsg.), *Europäische Integration und Globalisierung - Festschrift zum 60-jährigen Bestehen des Europa-Instituts*, Nomos, Baden-Baden, 2011, S. 113-130; Cole, M. D., Etteldorf, C. und Ullrich, C., *Updating the Rules for Online Content Dissemination*, Bd. 83 Schriftenreihe Medienforschung der LfM NRW, Nomos, Baden-Baden, 2021, S. 143 ff.; Rowland, D., Kohl, U. und Charlesworth, A, *Information Technology Law*, Routledge, Abingdon, 5. Aufl. 2017, S. 268 ff.; Schilling, K., *Binnenmarktkollisionsrecht*, De Gruyter, Berlin, 2006, S. 74 ff.; Garabiol-Furet, M.-D., "*Plaidoyer pour le principe du pays d'origine*" *Revue du Marché commun et de l'Union Européenne*, 2006, S. 82-87.

[128] C-376/22 *Google Ireland gegen KommAustria* [2023] ECLI:EU:C:2023:835; C-665/22 *Amazon Services Europe gegen AGCOM* [2024] ECLI:EU:C:2024:435; Verbundene Rechtssachen C-664/22 und C-666/22 Google Ireland und andere gegen AGCOM [2024] ECLI:EU:C:2024:434; C-663/22 Expedia Inc. gegen AGCOM [2024] ECLI:EU:C:2024:433; Verbundene Rechtssachen C-662/22 und C-667/22 AirBnB und andere gegen AGCOM [2024] ECLI:EU:C:2024:432.

oder impliziten Gründen beruhen, die im EU-Recht anerkannt sind, zum Beispiel Schutz der öffentlichen Ordnung,[129] der öffentlichen Sicherheit oder der Verbraucher. Solche Gründe werden vom EuGH eng ausgelegt.[130]

Wo Sekundärrecht den Anwendungsbereich der Grundfreiheiten konkretisiert, müssen diese harmonisierenden Vorschriften bei der rechtlichen Bewertung Vorrang haben. Zu den wichtigsten Elementen, die im Zusammenhang mit dieser Veröffentlichung von Bedeutung sind, gehören die Richtlinie über audiovisuelle Mediendienste (AVMD-RL)[131] und die Richtlinie über den elektronischen Geschäftsverkehr (EC-RL),[132] die sektorspezifische Vorschriften für die grenzüberschreitende Erbringung von Dienstleistungen im Binnenmarkt enthalten.

2.2.2 Sekundärrecht der Europäischen Union zur Regulierung von Inhalten und zu Durchsetzungsmaßnahmen

2.2.2.1 Regulierung von Medien und VSP: die AVMD-RL und der EMFA

Die AVMD-RL legt den rechtlichen Rahmen fest, nach dem die Mitgliedstaaten in den durch ihre Bestimmungen koordinierten Sachbereichen – insbesondere audiovisuelle kommerzielle Kommunikation, Jugendschutz und Bekämpfung der Anstiftung zu Hass – gegen grenzüberschreitende Anbieter von linearem Fernsehen, Videoabrufdienste und Video-Sharing-Plattformen (VSP) vorgehen können. Da es sich um eine Richtlinie handelt, müssen die Mitgliedstaaten die Bestimmungen in nationales Recht umsetzen. Das bedeutet beispielsweise, dass die Mitgliedstaaten mit geeigneten Mitteln sicherstellen müssen, dass audiovisuelle Mediendienste, die von Mediendiensteanbietern unter ihrer Rechtshoheit

[129] Siehe C-376/22 *Google Ireland gegen KommAustria*.

[130] Siehe die Hervorhebung durch Generalanwalt Szpunar in seinen Schlussanträgen in der Rechtssache *C-376/22, Google Ireland gegen KommAustria* [2023] ECLI:EU:C:2023:467, Abs. 64.

[131] Richtlinie 2010/13/EU des Europäischen Parlaments und des Rates vom 10. März 2010 zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste (AVMD-Richtlinie), ABl. L 95/1, zuletzt geändert durch Richtlinie (EU) 2018/1808 des Europäischen Parlaments und des Rates vom 14. November 2018 zur Änderung der Richtlinie 2010/13/EU zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste (Richtlinie über audiovisuelle Mediendienste) im Hinblick auf sich verändernde Marktgegebenheiten, ABl. L 303 vom 28. November 2018, sowie durch Verordnung (EU) 2024/1083 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Schaffung eines gemeinsamen Rahmens für Mediendienste im Binnenmarkt und zur Änderung der Richtlinie 2010/13/EU (Europäisches Medienfreiheitsgesetz), ABl. L 2024/1083, 17. April 2024.

[132] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, ABl. L 178, 17. Juli 2000.

bereitgestellt werden, keine Aufstachelung zu Gewalt oder Hass[133] oder öffentliche Aufforderung zur Begehung einer terroristischen Straftat enthalten.[134]

Dazu gehört die Verpflichtung aller Anbieter, den Zugang zu jugendgefährdenden Inhalten zu beschränken, das heißt zu Inhalten, die die körperliche, geistige oder sittliche Entwicklung von Minderjährigen beeinträchtigen können, ohne notwendigerweise rechtswidrig zu sein. Zu den in Artikel 6a der AVMD-RL vorgeschlagenen Maßnahmen gehören die Wahl der Sendezeit, Mittel zur Altersverifikation oder andere technische Maßnahmen, die in einem angemessenen Verhältnis zu der potenziellen Schädigung durch die Sendung stehen.

Da ein erheblicher Teil der auf VSP bereitgestellten Inhalte nicht der redaktionellen Verantwortung des VSP-Anbieters unterliegt, sind die Mitgliedstaaten nach Artikel 28b der AVMD-RL verpflichtet, dafür zu sorgen, dass ihrer Rechtshoheit unterliegende VSP-Anbieter die Nutzer vor schädlichen Inhalten abschirmen und geeignete Maßnahmen ergreifen, um die Allgemeinheit vor Sendungen, nutzergenerierten Videos und audiovisuellen kommerziellen Kommunikationen zu schützen, die solche schädlichen Inhalte enthalten.[135] Diese Maßnahmen müssen notwendig, wirksam und verhältnismäßig sein und den notwendigen Schutz der Nutzer gegen die Grundrechte der Plattformanbieter und Nutzer einschließlich des Rechts auf freie Meinungsäußerung abwägen. Zu den Maßnahmen können Mechanismen zur Meldung und Anzeige von Inhalten, Systeme zur Altersverifikation, Instrumente zur elterlichen Kontrolle und transparente Verfahren zur Moderation von Inhalten gehören.[136]

Nationale Regulierungsbehörden oder -stellen verfügen über die Durchsetzungsbefugnisse, um die Einhaltung nach nationalem Recht zu gewährleisten; gleichzeitig unterstützen die Mitgliedstaaten die Nutzung der Koregulierung und die Förderung der Selbstregulierung durch auf nationaler Ebene angenommene Verhaltenskodizes, die unter anderem eine wirksame Durchsetzung einschließlich wirksamer und verhältnismäßiger Sanktionen vorsehen.[137]

Ergänzend zur AVMD-RL wurde mit dem Europäischen Medienfreiheitsgesetz (Europäischer Rechtsakt zur Medienfreiheit – EMFA)[138] ein neues Regelwerk zum Schutz von Medienpluralismus und redaktioneller Unabhängigkeit der Medien in der EU eingeführt.

---

[133] Zum Anwendungsbereich siehe Art. 6 Abs. 1 Buchstabe a) der AVMD-RL.

[134] Gemäß Artikel 5 der Richtlinie (EU) 2017/541 des Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates, ABl. L 88/6 vom 31. März 2017, auf den die Bestimmung der AVMD-RL verweist.

[135] Siehe Erwägungsgrund 47 der Richtlinie (EU) 2018/1808 des Europäischen Parlaments und des Rates vom 14. November 2018 zur Änderung der Richtlinie 2010/13/EU zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste (Richtlinie über audiovisuelle Mediendienste) im Hinblick auf sich verändernde Marktgegebenheiten, ABl. L 303/69, 28. November 2018.

[136] Art. 28b Abs. 3 AVMD-RL.

[137] Art. 4a Abs. 1 AVMD-RL. Darüber hinaus können die Mitgliedstaaten und die Europäische Kommission die Selbstregulierung durch Verhaltenskodizes der Union fördern (Art. 4a Abs. 2 AVMD-RL).

[138] Verordnung (EU) 2024/1083 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Schaffung eines gemeinsamen Rahmens für Mediendienste im Binnenmarkt und zur Änderung der Richtlinie 2010/13/EU (Europäisches Medienfreiheitsgesetz) ABl. L 2024/1083, 17. April 2024.

Darüber hinaus enthält es Vorschriften zu Kooperationsmechanismen für die Zusammenarbeit zwischen den nationalen Medienregulierungsbehörden oder -stellen. Damit wurden die bisherigen, nicht rechtsverbindlichen Kooperationspraktiken der Behörden und Stellen unter dem Dach der Gruppe europäischer Regulierungsstellen für audiovisuelle Mediendienste (ERGA)[139] formalisiert und so der AVMD-RL hinzugefügt. Die AVMD-RL hatte lediglich ein Kooperationsgremium eingerichtet, ohne Verfahrensdetails festzulegen, obwohl die Notwendigkeit einer engen Zusammenarbeit, insbesondere bei der Lösung grenzüberschreitender Fälle, durch die Ausweitung des Anwendungsbereichs der AVMD-RL auf VSP gestiegen war.[140] Mit Artikel 14 EMFA wird somit ein strukturierter Kooperationsrahmen für die einheitliche und wirksame Anwendung des EMFA und die Umsetzung der AVMD-RL eingeführt, der den Dialog und die Verpflichtung zur Rechtfertigung von Maßnahmen seitens der zuständigen Behörde gewährleistet.[141] Darüber hinaus gibt es eine spezielle Bestimmung über Kooperationsersuchen im Hinblick auf die Verpflichtungen von VSP (Artikel 15 EMFA), die den europaweiten Charakter von VSP widerspiegelt: Obwohl die Anbieter ihre Dienste regelmäßig grenzüberschreitend in der EU anbieten, sind sie sowohl nach der EC-RL als auch nach der AVMD-RL „nur“ an die Rechtsprechung ihres Herkunftsmitgliedstaats gebunden.[142]

Die Nachfolgeorganisation der ERGA, das Europäische Gremium für Mediendienste (EGMD), das die ERGA ersetzt, hat unter anderem die Aufgabe, eine koordinierte Durchsetzung in den Mitgliedstaaten zu gewährleisten.[143] Darüber hinaus enthält Artikel 17 EMFA eine Koordinierungsvorschrift für das EGMD zu Maßnahmen in Bezug auf Mediendiensteanbieter mit Sitz außerhalb der EU, die auch Maßnahmen gegen „unseriöse Mediendienste“ umfasst, die eine ernste und schwerwiegende Gefahr für die öffentliche Sicherheit darstellen.[144] Letzteres ist eine direkte Reaktion auf die Schwierigkeiten, die bei dem Versuch aufgetreten waren, eine gemeinsame Antwort auf die Risiken zu finden, die durch die Verbreitung russischer Sender in der EU entstanden waren, nachdem die Russische Föderation den Krieg gegen die Ukraine begonnen hatte. Das EGMD kann nationale Regulierungsmaßnahmen in Bezug auf Mediendienste koordinieren, die sich an Zuschauer in den EU-Mitgliedstaaten richten, wenn diese Dienste zum Beispiel aufgrund einer möglichen Kontrolle durch Regierungen oder Einrichtungen von Drittländern ein ernsthaftes Risiko für die öffentliche Sicherheit oder Verteidigung darstellen. In diesen Fällen kann das EGMD eine Stellungnahme abgeben, um eine einheitlichere und wirksamere Reaktion zu fördern.

---

[139] Gruppe europäischer Regulierungsstellen für audiovisuelle Mediendienste; siehe *Memorandum of Understanding* zwischen den nationalen Regulierungsbehörden, die Mitglieder der Gruppe europäischer Regulierungsstellen für audiovisuelle Mediendienste (ERGA) sind, vom 3. Dezember 2020 sowie Cole, M. D. und Etteldorf, C., "Future Regulation of Cross-Border Audiovisual Content Dissemination", Bd. 84 in *Schriftenreihe Medienforschung der LfM NRW*, Nomos, Baden-Baden, 2023, S. 149 ff. und 176 ff. Die ERGA wurde durch das Europäische Gremium für Mediendienste (EGMD) ersetzt, das gemäß Artikel 8 EMFA eingerichtet wurde.

[140] Erwägungsgrund 43 EMFA.

[141] Siehe Cole, M. D. und Etteldorf, C., *Research for CULT Committee – European Media Freedom Act - Background Analysis*, Europäisches Parlament, Politische Abteilung für Struktur- und Kohäsionspolitik, Brüssel, 2023, S. 50.

[142] Für einen kurzen Überblick über das Verhältnis zwischen der AVMD-RL und der EC-RL siehe Oster, J. und Wagner, E., „*§ 38 Kommunikations- und Medienrecht*“ in Ludwigs, M. (Hrsg.), *Handbuch des EU-Wirtschaftsrechts,* C.H.Beck, 63. überarbeitete Auflage 2025, Rn. 83, München, 2025.

[143] Art. 13 EMFA.

[144] Art. 13 Abs. 1 Buchstabe l) und Art. 17 EMFA sowie Erwägungsgrund 44.

2.2.2.2 Regulierung von Online-Plattformen: der DSA und der DMA

Unter der EC-RL hat sich ein Regulierungssystem mit einer Unterscheidung zwischen aktiven und passiven Vermittlern entwickelt: Die Haftung wurde davon abhängig gemacht, ob der Vermittler neutral blieb (passiv) oder ob seine Mitwirkung über das passive Hosting hinausging und er mit den Inhalten interagierte, zum Beispiel durch Moderation, Kuratierung oder Optimierung der gehosteten Inhalte.[145] Die auf dieser Unterscheidung beruhenden Haftungsausschlüsse, die zuvor in der EC-RL enthalten waren, sind nun in dem Digital Services Act (DSA)[146] übernommen worden, um weiterhin die unterschiedlichen Rollen der Vermittler in Bezug auf Inhalte Dritter widerzuspiegeln, obwohl sich ihre Rollen seit der EC-RL bis zum DSA erheblich verändert haben.[147]

Ziel des DSA ist es, „ein sicheres, berechenbares und vertrauenswürdiges Online-Umfeld [zu schaffen], in dem Innovationen gefördert und die in der EU-Grundrechtecharta[148] verankerten Grundrechte, darunter der Grundsatz des Verbraucherschutzes, wirksam geschützt werden".[149] Dazu gehört eine vollständige Harmonisierung der Vorschriften für Vermittlungsdienste im Binnenmarkt, die sich mit der Verbreitung rechtswidriger Online-Inhalte befassen.[150] Das Konzept der „rechtswidrigen Inhalte" sollte im Großen und Ganzen den bestehenden Regeln für die Offline-Umgebung entsprechen.[151] Daher ist die Definition des DSA für „rechtswidrige Inhalte" weit gefasst und bezieht sich auf „alle Informationen, die als solche oder durch ihre Bezugnahme auf eine Tätigkeit, einschließlich des Verkaufs von Produkten oder der Erbringung von Dienstleistungen, nicht im Einklang mit dem Unionsrecht oder dem Recht eines Mitgliedstaats stehen, ungeachtet des genauen Gegenstands oder der Art der betreffenden Rechtsvorschriften."[152] Dies soll Inhalte abdecken, die nach geltendem Recht entweder an sich rechtswidrig sind, etwa rechtswidrige Hassrede oder terroristische Inhalte und rechtswidrige diskriminierende Inhalte, oder die nach den geltenden Vorschriften rechtswidrig sind, weil sie mit rechtswidrigen Handlungen zusammenhängen.[153]

Erwägungsgrund 12 DSA enthält anschauliche Beispiele für rechtswidrige Inhalte, darunter die Weitergabe von Darstellungen sexuellen Missbrauchs von Kindern, die rechtswidrige Weitergabe privater Bilder ohne Zustimmung, Cyber-Stalking, der Verkauf

---

[145] Siehe Cole, M. D., Etteldorf, C. und Ullrich, C., *Cross-Border Dissemination of Online Content*, Bd. 81 *Schriftenreihe Medienforschung der LfM NRW*, Nomos, Baden-Baden, 2020, S. 176 f.; Rowland, D., Kohl, U. und Charlesworth, A., *Information Technology Law*, Routledge, Abingdon, 5. Aufl. 2017, S. 104 f.; Schmitz, S., *The Struggle in Online Copyright Enforcement*, Nomos, Baden-Baden 2015, S. 574 f.

[146] Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste) Abl. L 277/1, 27. Oktober 2022.

[147] Cole, M. D., Etteldorf, C. und Ullrich, C., *Cross-Border Dissemination of Online Content*, Bd. 81 *Schriftenreihe Medienforschung der LfM NRW*, Nomos, Baden-Baden, 2021, S. 222 f.; Buiten, M. C., *"The Digital Services Act - From Intermediary Liability to Platform Regulation"*, in *JIPITEC*, 12, 2021, S. 361-380; Madiaga, T., *Reform of the EU liability Regime for Online Intermediaries, Background on the forthcoming Digital Services Act*, Wissenschaftlicher Dienst des Europäischen Parlaments, PE 649.404, Brüssel, Mai 2020.

[148] Charta der Grundrechte der Europäischen Union, 2012/C 326/02, ABl C 326/391, 26.10.2012.

[149] Art. 1 Abs. 1 DSA.

[150] Erwägungsgrund 9 DSA.

[151] Erwägungsgrund 12 DSA.

[152] Art. 3 Buchstabe h) DSA.

[153] Erwägungsgrund 12 DSA.

nicht konformer oder gefälschter Produkte, der Verkauf von Produkten oder die Erbringung von Dienstleistungen unter Verstoß gegen das Verbraucherschutzrecht, die nicht genehmigte Verwendung urheberrechtlich geschützten Materials, das rechtswidrige Angebot von Beherbergungsdienstleistungen oder der rechtswidrige Verkauf von lebenden Tieren. Zu diesem Zweck legt der DSA durch harmonisierte Regeln für die Erbringung von Vermittlungsdienstleistungen insbesondere einen Rahmen fest für die bedingte Haftungsbefreiung von Anbietern von Vermittlungsdiensten (Artikel 1 Absatz 2 Buchstabe a) DSA) und – unabhängig von Haftungsfragen – spezifische, auf bestimmte Kategorien von Anbietern von Vermittlungsdiensten zugeschnittene Sorgfaltspflichten (Artikel 1 Absatz 2 Buchstabe b) DSA).

Kapitel II des DSA enthält die Haftungsregeln für Anbieter von Vermittlungsdiensten: reine Durchleitung (Artikel 4 DSA), Caching (Artikel 5 DSA) und Hosting (Artikel 6 DSA).[154] Dienste, die reine Durchleitung und Caching anbieten, haften nicht für übermittelte oder gespeicherte Informationen, wenn sie diese nichtverändern. Hostingdiensteanbieter sind von der Haftung für im Namen von Nutzern gespeicherte Inhalte befreit, es sei denn, sie haben tatsächliche Kenntnis von der rechtswidrigen Tätigkeit oder den rechtswidrigen Inhalten und unterlassen es, „zügig" tätig zu werden, um diese Inhalte zu entfernen oder den Zugang zu ihnen zu sperren.[155] Eine tatsächliche Kenntnis oder ein tatsächliches Bewusstsein kann auf verschiedenen Wegen entstehen, zum Beispiel durch Untersuchungen aus eigener Initiative oder durch Meldungen Dritter, sofern diese ausreichend präzise und hinreichend begründet sind, damit ein aufmerksamer Wirtschaftsteilnehmer die mutmaßlich rechtswidrigen Inhalte angemessen erkennen und bewerten und gegebenenfalls dagegen vorgehen kann.[156] Hostingdiensteanbieter müssen ungeachtet ihrer Größe leicht zugängliche und benutzerfreundliche Melde- und Abhilfeverfahren einrichten, um solche Meldungen zu erleichtern. Abgesehen vom in Artikel 6 Absatz 1 Buchstabe b) DSA geforderten „zügigen" Handeln gibt es keine festen Zeitvorgaben für die Entfernung von Inhalten. Um ein schnelleres Vorgehen gegen rechtswidrige Inhalte zu erreichen, sieht der DSA vor, dass Meldungen von so genannten „vertrauenswürdigen Hinweisgebern",[157] die im Regulierungsrahmen des DSA tätig sind, von den Vermittlern vorrangig behandelt werden müssen.[158] Der Status eines vertrauenswürdigen Hinweisgebers wird vom Koordinator für digitale Dienste (DSC/KDD) des Mitgliedstaates, in dem der Antragsteller für eine solche Funktion niedergelassen ist, und nur an eine begrenzte Anzahl von Einrichtungen vergeben, die besondere Sachkenntnis und Kompetenz bei der Identifizierung rechtswidriger Inhalte nachgewiesen haben.[159] Diese Sachkenntnis kann auch auf einen bestimmten Themenbereich, das „ausgewiesene

[154] Für einen Überblick über die Haftungsregelungen im Rahmen des DSA siehe Capello, M. (Hrsg.), "*Die Entschlüsselung des Gesetzespakets zu digitalen Diensten*", *IRIS Spezial*, Europäische Audiovisuelle Informationsstelle, Straßburg, 2021, S. 13 ff.

[155] Art. 6 DSA.

[156] Siehe Erwägungsgrund 22 und Art. 6 DSA. Zur Voraussetzung der „tatsächlichen Kenntnis" siehe Radtke, T., „Art. 6 DSA" in Gersdorf, H. und Paal B. (Hrsg.), BeckOK Informations- und Medienrecht, C.H.Beck, München, 48. Aufl., 2025, Abs. 27 ff.

[157] Zu vertrauenswürdigen Hinweisgebern siehe van de Kerkhof, J., "Article 22 Digital Services Act: Building Trust with Trusted Flaggers", *Internet Policy Review*, 14(1), 2025. Für einen Überblick siehe auch https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa.

[158] Art. 22 Abs. 1 DSA.

[159] Art. 22 Abs. 2 DSA. Bis zum 25. August 2025 wurden 38 vertrauenswürdige Hinweisgeber benannt.

Fachgebiet“,[160] beschränkt sein, zum Beispiel die Sachkenntnis der HateAid gGmbH in Deutschland auf dem Gebiet der Cybergewalt und rechtswidriger Äußerungen. Im Hinblick auf die Transparenz sind die vertrauenswürdigen Hinweisgeber verpflichtet, leicht verständliche und ausführliche Berichte über die eingereichten Meldungen zu veröffentlichen, unter anderem auch über die Maßnahmen, die vom jeweiligen Anbieter im Anschluss an die Meldung getroffen wurden. [161] Die Europäische Kommission arbeitet derzeit an Leitlinien zu vertrauenswürdigen Hinweisgebern, die den KDD helfen sollen, das Verfahren zur Ernennung vertrauenswürdiger Hinweisgeber zu straffen und auch Orientierungshilfe zu den Umständen zu geben, die zum Entzug des Status führen können.[162]

Während die Verpflichtungen zur Entfernung rechtswidriger Inhalte bei Meldung zur Vermeidung von Haftung alle Vermittler betreffen, gelten einige zusätzliche Sorgfaltspflichten nur für sehr große Online-Plattformen (VLOP) oder sehr große Online-Suchmaschinen (VLOSE), die aufgrund ihrer großen Reichweite eine gesellschaftliche Wirkung haben, die Risiken mit sich bringt. Der operative Schwellenwert wurde auf 45 Millionen monatliche Nutzer festgelegt, ein Wert, der 10 % der EU-Bevölkerung entspricht.[163] Die Verpflichtung zur Durchführung von Risikobewertungen sowie von Risikominderungsmaßnahmen erstreckt sich auf die Verbreitung rechtswidriger Inhalte und die zu erwartenden negativen Auswirkungen auf die Menschenrechte. Die Risiken im Zusammenhang mit der Verbreitung rechtswidriger Inhalte sowie bestimmter schädlicher Inhalte sind gewissenhaft zu melden, zu analysieren und anzugehen.[164] Die Maßnahmen müssen angemessen und wirksam sein und gleichzeitig in einem angemessenen Verhältnis zur wirtschaftlichen Leistungsfähigkeit des Anbieters stehen.[165] Dazu können eine mögliche Einbindung spezifischer Bestimmungen in die Geschäftsbedingungen sowie eventuelle Anpassungen der Systeme zur Moderation von Inhalten und interner Entscheidungsprozesse gehören.[166] Dies bedeutet nicht, dass es eine obligatorische Überwachungspflicht gibt, da laut Artikel 8 DSA keine allgemeine Verpflichtung zur Überwachung oder aktiven Nachforschung besteht. Vielmehr wird im DSA die Moderation von Inhalten als ein Faktor genannt, der das Risiko der Verbreitung rechtswidriger Inhalte beeinflusst.[167]

Gemäß Artikel 3 Buchstabe t) DSA bezeichnet „Moderation von Inhalten“ die – automatisierten oder nicht automatisierten – Tätigkeiten der Anbieter von Vermittlungsdiensten, mit denen rechtswidrige Inhalte oder Informationen, die von Nutzern des Dienstes bereitgestellt werden und mit den allgemeinen Geschäftsbedingungen des Anbieters unvereinbar sind, erkannt, festgestellt und bekämpft werden sollen. Zu diesen Maßnahmen gehört die Beeinflussung der Verfügbarkeit, Anzeige und Zugänglichkeit dieser rechtswidrigen Inhalte, zum Beispiel durch Herabstufung, Demonetisierung, Sperrung des Zugangs zu ihnen oder ihre Entfernung. Eine andere mögliche Reaktion besteht darin, auf

[160] Art. 22 Abs. 1 DSA.
[161] Art. 22 Abs. 3 DSA.
[162] Die Annahme ist vor Ende 2025 geplant.
[163] Art. 33 DSA. Bis zum 25. August 2025 wurden 33 VLOP und zwei VLOSE benannt.
[164] Erwägungsgründe 53 und 55 DSA.
[165] Siehe Erwägungsgrund 86 DSA
[166] Erwägungsgrund 87 DSA.
[167] Art. 34 Abs. 2 Buchstabe b) und Art. 35 Abs. 1 Buchstabe c) DSA.

die Fähigkeit der Nutzer des Dienstes, solche Informationen bereitzustellen, einzuwirken, zum Beispiel durch die Schließung oder Aussetzung des Kontos eines Nutzers. Die detaillierte Ausgestaltung der Moderationsprozesse und -systeme – von Einzelentscheidungen bis zu umfassender Moderation – liegt im Ermessen des ausführenden Unternehmens. Gleichzeitig sieht der DSA jedoch eindeutige Verpflichtungen zur unverzüglichen Entfernung bestimmter Arten von Inhalten vor.

Die Beachtung und Einhaltung von Verhaltenskodizes gemäß Artikel 45 DSA kann eine zulässige Risikominderungsmaßnahme darstellen. Insbesondere sollten Risikominderungsmaßnahmen für bestimmte Arten rechtswidriger Inhalte Gegenstand von Selbst- und Koregulierungsmaßnahmen einschließlich Verhaltenskodizes sein.[168] Die Verhaltenskodizes für erhebliche systemische Risiken waren bereits vor dem DSA als Selbstregulierungsmaßnahmen in Form von Verfahrensregeln vorhanden. Aufbauend auf diesen bereits vorhandenen Verfahrensregeln können diese Kodizes zu Verhaltenskodizes im Rahmen des DSA werden. In Artikel 45 DSA wird dafür eine Reihe von Kriterien festgelegt, darunter die Notwendigkeit, spezifische Zielsetzungen und Leistungsindikatoren zu haben und die Bedürfnisse und Interessen aller Beteiligten angemessen zu berücksichtigen. Die Europäische Kommission und das neu eingerichtete Europäische Gremium für digitale Dienste (EGDD)[169] haben die Aufgabe, zu beurteilen, ob ein Kodex dem Ziel entspricht, zur ordnungsgemäßen Anwendung des DSA beizutragen.[170]

Der DSA legt nicht nur Verpflichtungen für Vermittlungsdienste fest, sondern schafft auch einen umfassenden Rahmen, um deren Einhaltung zu gewährleisten. Die Durchsetzung des DSA umfasst eine Reihe von Untersuchungs- und Sanktionsmaßnahmen, die sowohl den nationalen Behörden als auch der Europäischen Kommission zur Verfügung stehen, je nach Verteilung der Aufsichtsbefugnisse für die verschiedenen Arten von Anbieter.

Zu diesem Zweck sind die Mitgliedstaaten verpflichtet, eine oder mehrere unabhängige zuständige Behörden zu benennen, die für die Aufsicht über die Anbieter und die Durchsetzung des DSA verantwortlich sind. Der DSA verpflichtet die Mitgliedstaaten jedoch nicht, solche zuständigen Behörden damit zu beauftragen, über die Rechtmäßigkeit bestimmter Inhalte zu entscheiden. Die zivil-, straf- und verwaltungsrechtlichen Ansätze, zum Beispiel Aufforderungen zur Entfernung rechtswidriger Inhalte, unterliegen dem nationalen Recht der Mitgliedstaaten.[171] Die Mitgliedstaaten müssen daher Vorschriften für wirksame, verhältnismäßige und abschreckende Sanktionen festlegen, die verhängt werden können, wenn Anbieter von Vermittlungsdiensten, die in ihre Zuständigkeit fallen, gegen den DSA verstoßen .[172] In Anbetracht des grenzüberschreitenden Charakters der betreffenden Dienste und des horizontalen Spektrums an Verpflichtungen muss jeder Mitgliedstaat darüber hinaus einen KDD benennen, der als zentrale Kontaktstelle im Rahmen der Aufsicht und Durchsetzung auf Unionsebene fungiert.[173] Das EGDD dient als

[168] Siehe Erwägungsgrund 104 DSA
[169] Siehe Art. 61 DSA
[170] Art. 45 Abs. 4 DSA.
[171] Siehe zum Beispiel Zurth, P., „Private Rechtsdurchsetzung im Digital Services Act“, *Gewerblicher Rechtsschutz und Urheberrecht*, 125(19), 2023, S. 1329-1408, 1331.
[172] Art. 52 DSA.
[173] Art. 49 Abs. 2 und Erwägungsgrund 110 DSA.

unabhängige Beratergruppe, um eine einheitliche Anwendung des DSA zu gewährleisten und eine effektive Zusammenarbeit zwischen der Europäischen Kommission und den KDD zu unterstützen.[174]

Für die Durchsetzung gegenüber Anbietern von VLOP und VLOSE (zusammen VLOPSE genannt) überträgt der DSA die Zuständigkeit an die Europäische Kommission, die damit zu einer Regulierungsbehörde wird. Gemäß Artikel 65 ff. DSA kann die Europäische Kommission von Amts wegen Untersuchungsbefugnisse ausüben und Verfahren gegen diese Kategorie von Anbietern einleiten. Neben den Untersuchungsbefugnissen kann die Europäische Kommission einen Beschluss wegen Nichteinhaltung erlassen und Geldbußen oder Zwangsgelder verhängen.[175] Ein Verstoß gegen den DSA wird mit einer Geldbuße von bis zu 6 % des weltweit erzielten Gesamtumsatzes der betreffenden VLOPSE geahndet und kann auch zu einer verlängerten Beaufsichtigung führen, um die Einhaltung der Verordnung sicherzustellen.[176] In dringenden Fällen ist es möglich, einstweilige Maßnahmen zu verhängen; bei dauerhaften Zuwiderhandlungen mit schwerwiegenden Folgen für die Nutzer, und bei Straftaten, die eine Bedrohung für das Leben und die Sicherheit einer Person darstellen, kann sogar die vorübergehende Aussetzung des Dienstes beantragt werden.[177]

Die Untersuchungs- und Durchsetzungsbefugnisse der Europäischen Kommission werden durch Transparenzmechanismen ergänzt, um ein angemessenes Maß an Transparenz und Rechenschaftspflicht zu gewährleisten. Alle Vermittlungsdienste sind verpflichtet, einen jährlichen Transparenzbericht über die Moderation von Inhalten zu veröffentlichen, die von ihnen in dem betreffenden Zeitraum durchgeführt wurde .[178] Dazu gehören unter anderem Informationen über die Anzahl der von Behörden der Mitgliedstaaten erhaltenen Anordnungen, ihre Verfahren der Inhaltsmoderation, die Anzahl der entfernten Informationen sowie die Anzahl der von vertrauenswürdigen Hinweisgebern eingereichten Meldungen oder sonstiger Anträge auf Entfernung. In Anbetracht ihrer systemischen Risiken haben Anbieter von VLOPSE erweiterte Berichtspflichten in Bezug auf die personellen Ressourcen und deren Qualifikationen; zudem müssen sie halbjährlich Berichte veröffentlichen.[179] Darüber hinaus hat die Europäische Kommission gemäß Artikel 24 Absatz 5 DSA eine Transparenzdatenbank eingerichtet, in der die verpflichtenden Begründungen[180] gesammelt und öffentlich zugänglich gemacht werden, die VLOPSE angeben müssen, wenn sie Inhalte entfernen oder den Zugang zu ihnen anderweitig beschränken.

Während die Europäische Kommission bisher noch keine Bußgelder im Rahmen des DSA verhängt hat – obwohl mehrere Verfahren laufen, insbesondere in Bezug auf die

[174] Art. 61 DSA.
[175] Art. 73, 74, 76 und 79 DSA.
[176] Art. 74 und 75 DSA.
[177] Art. 82 und Art. 51 Abs. 3 Buchstabe b DSA.
[178] Art. 15 DSA. Siehe auch Etteldorf, C., „Ein wichtiger Meilenstein in der EU: Das Gesetzespaket zu digitalen Diensten“ in Capello, M. (Hrsg.), *Algorithmische Transparenz und Rechenschaftspflicht bei digitalen Diensten*, *IRIS Spezial*, Europäische Audiovisuelle Informationsstelle, Straßburg, 2023, S. 31 und 39.
[179] Art. 42 DSA.
[180] Art. 17 DSA.

Verpflichtungen zum Jugendschutz[181] –, hat sie im Zusammenhang mit dem Gesetz über digitale Märkte (DMA)[182] bereits Durchsetzungsmaßnahmen ergriffen.[183] Ziel des DMA ist die Schaffung eines „bestreitbaren und fairen Marktes"[184] im digitalen Sektor. Es befasst sich in erster Linie mit Wettbewerbsfragen in Bezug auf „zentrale Plattformdienste" (CPS), die von sogenannten „Torwächtern" angeboten werden. Artikel 2 Absatz 2 DMA enthält die Liste von Diensten, die als CPS gelten, darunter Online-Suchmaschinen, Online-Dienste sozialer Netzwerke, Video-Sharing-Plattform-Dienste und Online-Werbedienste, während Kapitel II des DMA die Benennung der Anbieter als Torwächter detailliert beschreibt. Ähnlich dem Konzept der VLOPSE im Rahmen des DSA haben Torwächter einen bedeutenden Einfluss auf den Binnenmarkt und bieten einen (oder mehrere) der ausgewählten CPS an, die gewerblichen Nutzern als wichtiges Zugangstor zu Endnutzern dienen. Die Position des Unternehmens muss entweder gegenwärtig oder in absehbarer Zeit „gefestigt und dauerhaft" sein.[185] Dementsprechend sind Torwächter Unternehmen mit systemischer Relevanz. Die in Artikel 3 Absatz 2 DMA festgelegten numerischen Schwellenwerte sind sehr hoch, aber bisher wurden bereits 23 Dienste von sieben verschiedenen Torwächtern als CPS identifiziert.[186] Das DMA definiert für den Online-Sektor Verhaltensweisen, die als missbräuchlich anzusehen sind, wenn sie von Torwächtern angewendet werden, und führt eine Reihe spezifischer Verpflichtungen und Verbote für Torwächter ein. Dazu gehören Vorschriften über Werbeinformationen einschließlich des Zugangs zu Informationen über die Funktionsweise der Online-Werbewertschöpfungsketten (Artikel 5 Absatz 9 und 10 sowie Artikel 6 Absatz 8 DMA) sowie über das Ranking von Inhalten (Artikel 6 Absatz 5 DMA).

In Bezug auf die Durchsetzung unterscheidet sich das DMA vom Multi-Akteur-Ansatz des DSA durch die zentrale Ansiedlung der Durchsetzung bei der Europäischen Kommission. Sie ist befugt, Marktuntersuchungen einzuleiten[187] und Verfahren zu eröffnen, die zu einem möglichen Erlass von Beschlüssen zur Einhaltung der Verpflichtungen für Torwächter und zur Verhängung von Geldbußen gegen Torwächter einschließlich Geldbußen von bis zu 20 % ihres weltweiten Jahresumsatzes bei wiederholten Zuwiderhandlungen führen.[188]

---

[181] Siehe zum Beispiel Europäische Kommission, Commission Decision Initiating Proceedings pursuant to Article 66(1) of Regulation (EU) 2022/2065 of 18 December 2023 against Twitter International Unlimited. Ein Überblick über die wichtigsten Durchsetzungsmaßnahmen findet sich auf der speziellen Website der Kommission unter https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses.

[182] Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte), ABl. L 265, 27. Oktober 2022.

[183] Am 23. April 2025 verhängte die Kommission gegen Apple eine Geldbuße in Höhe von 500 Millionen EUR und gegen Meta in Höhe von 200 Millionen EUR, siehe Europäische Kommission, „Kommission stellt Verstoß von Apple und Meta gegen das Gesetz über digitale Märkte fest", Pressemitteilung vom 23. April 2025.

[184] Zu Letzterem siehe Cole, M. D., „Der Vorschlag für ein Gesetz über digitale Märkte (DMA): Von Gatekeepern, Fairness und Transparenz im Online-Umfeld" in Capello, M. (Hrsg.), Die Entschlüsselung des Gesetzespakets zu digitalen Diensten, IRIS *Spezial,* Europäische Audiovisuelle Informationsstelle, Straßburg 2021.

[185] Art. 3 DMA.

[186] Auf einer speziellen Website der Kommission sind die benannten Torwächter aufgeführt, siehe https://digital-markets-act.ec.europa.eu/gatekeepers_en.

[187] Art. 16 bis 19 DMA.

[188] Art. 20, 29 und 30 DMA.

2.2.2.3 Regulierung politischer Werbung im Internet: die TTPW-VO

In Anbetracht der potenziellen Reichweite des Internets ist es wenig überraschend, dass es von politischen Parteien und Politikern ausgiebig genutzt wird, um ihre politischen Meinungen zu verbreiten oder „eine politische Botschaft zu vermitteln".[189] In diesem Zusammenhang stellt insbesondere das Mikrotargeting auf der Grundlage von Profiling mithilfe maschinellen Lernens und künstlicher Intelligenz eine erhebliche Bedrohung nicht nur für die persönliche Eigenständigkeit, sondern auch für die Demokratie selbst dar. Letzteres wurde unter anderem durch den Cambridge-Analytica-Skandal aufgedeckt.[190] Mit der Verordnung über die Transparenz und das Targeting politischer Werbung (TTPW-VO)[191] vom April 2024 als regulatorischer Antwort sollen die Bedenken im Zusammenhang mit Informationsmanipulation und ausländischer Einmischung in Wahlen ausgeräumt werden, indem die Vorschriften über die Transparenz und die damit verbundenen Sorgfaltspflichten für die Erbringung politischer Werbedienstleistungen harmonisiert werden. Die TTPW-VO ergänzt unter anderem den DSA, den DMA und die Datenschutz-Grundverordnung (DSGVO), um die Integrität von Wahlen angesichts der schwierigen Herausforderungen bei Regulierung und Durchsetzung im digitalen Zeitalter zu gewährleisten.

Laut der weit gefassten Definition in der TTPW-VO ist politische Werbung eine Botschaft (a) durch oder für einen „politischen Akteur" oder in seinem Namen, es sei denn, sie ist rein privater oder rein kommerzieller Natur, oder (b) die geeignet ist, das Ergebnis einer Wahl oder eines Referendums, eines Rechtsetzungs- oder Regulierungsprozesses oder eines Abstimmungsverhaltens zu beeinflussen. Der Begriff „politischer Akteur" wird in Artikel 2 ebenfalls definiert; er umfasst ein breites Spektrum von Akteuren, darunter politische Parteien, Kandidaten und Organisationen für politische Kampagnen. Kapitel II der TTPW-VO enthält Vorschriften zur Transparenz politischer Werbung einschließlich Transparenzbekanntmachungen und Informationen über den Sponsor, was unter anderem bedeutet, dass jede politische Werbung als solche zu kennzeichnen ist und Informationen über den Sponsor und jede mögliche Einrichtung, die den Sponsor kontrolliert, enthalten muss.[192] Damit verbietet die TTPW-VO bestimmte Arten von Inhalten, die online verbreitet werden, nämlich „nicht gekennzeichnete" politische Werbung. Darüber hinaus verbietet die Verordnung in den drei Monaten vor einer Wahl oder einem Referendum politische Werbung, die von Sponsoren außerhalb der EU stammt.[193] Gemäß den Transparenzverpflichtungen von Artikel 12 der TTPW-VO müssen für die Datenverarbeitung Verantwortliche bei der Verwendung von Verfahren zum Targeting und Amplifizieren politischer Werbung, die sich auf personenbezogene Daten stützen, der Werbung zusätzliche Informationen beifügen, die es dem Einzelnen ermöglichen, die Logik hinter der Technik und die wichtigsten Parameter für ihre Verwendung zu verstehen und zu erkennen, ob Daten Dritter oder zusätzliche Analysemethoden verwendet wurden. Um die

[189] Siehe *Magyar Kétfarkú Kutya Párt gegen Ungarn*, Nr. 201/17 (EGMR, 20. Januar 2020), Rn. 88-89.
[190] Siehe Dowling, M.-E., "Cyber Information Operations: Cambridge Analytica's Challenge to Democratic Legitimacy", *Journal of Cyber Policy*, 7(2), 2022, S. 230-248.
[191] Verordnung (EU) 2024/900 des Europäischen Parlaments und des Rates vom 13. März 2024 über die Transparenz und das Targeting politischer Werbung, ABl. L 2024/900, 20. März 2024.
[192] Art. 11 Abs. 1 TTPW-VO.
[193] Art. 5 Abs. 2 TTPW-VO. „Wahl" oder „Referendum" bezieht sich auf jede Art von Wahlprozessen, die auf Unionsebene oder auf nationaler, regionaler oder lokaler Ebene in einem Mitgliedstaat durchgeführt werden.

Transparenz zu erhöhen, sieht Artikel 13 der TTPW-VO vor, dass die Europäische Kommission ein europäisches Archiv für politische Online-Anzeigen einrichtet, ähnlich den Werbearchiven, die bestimmte Vermittler nach dem DSA unterhalten müssen.

An der Überwachung und Durchsetzung sind verschiedene Akteure beteiligt, darunter auch Datenschutzbehörden, und die Mitgliedstaaten sind verpflichtet, eine oder mehrere zuständige Behörden für die wirksame Anwendung, Überwachung und Durchsetzung der TTPW-VO zu benennen.[194] Diesen Behörden stehen verschiedene Untersuchungs- und Durchsetzungsinstrumente zur Verfügung, darunter die Forderung von Datenzugang sowie die Befugnis, Verwarnungen auszusprechen oder Geldbußen zu verhängen.[195] In Anbetracht des grenzüberschreitenden Charakters bestimmter politischer Online-Werbung legt die TTPW-VO auch Regeln für die gerichtliche Zuständigkeit fest: Bietet ein Diensteanbieter seine Dienste in mehr als einem Mitgliedstaat an, sollte(n) in der Regel die zuständige(n) Behörde(n) des Mitgliedstaats zuständig sein, in dem sich die Hauptniederlassung des Anbieters politischer Werbedienstleistungen befindet.

Bei der Ausübung ihrer Überwachungs- und Durchsetzungsbefugnisse sollten die zuständigen Behörden aller Mitgliedstaaten jedoch bei Bedarf zusammenarbeiten und sich gegenseitig unterstützen und zu diesem Zweck die bestehenden Strukturen einschließlich der nationalen Kooperationsnetze, des Europäischen Kooperationsnetzwerkes für Wahlen,[196] des EGDD und des EGMD (ehemals ERGA) nutzen.[197] Zu diesem Zweck h sind in Artikel 23 der TTPW-VO Regeln für die grenzüberschreitende Zusammenarbeit einschließlich eines grenzüberschreitenden Meldeverfahrens vorgesehen. Zu den Sanktionen gehören Geldbußen in Höhe von bis zu 6 % der Jahreseinnahmen oder des Jahresbudgets des Sponsors oder des Anbieters politischer Werbedienstleistungen, je nachdem, welcher Betrag höher ist, oder 6 % des weltweiten Jahresumsatzes des Sponsors oder des Anbieters politischer Werbedienstleistungen im vorangegangenen Geschäftsjahr. Die Mitgliedstaaten können auch Vorschriften für andere Maßnahmen einschließlich Zwangsgelder festlegen.[198]

2.2.2.4 Regulierung von Inhalten im Zusammenhang mit personenbezogenen Daten: die DSGVO

Die Datenschutz-Grundverordnung (DSGVO)[199] als primärer Rechtsrahmen für die Verarbeitung personenbezogener Daten legt angesichts der rasanten technologischen Entwicklung und der Globalisierung Grundsätze und Regeln für den Schutz natürlicher Personen bei der Verarbeitung dieser Daten fest.[200] Artikel 3 DSGVO erweitert den

[194] Art. 22 Abs. 1-4 TTPW-VO, in denen festgelegt ist, dass unterschiedliche Behörden für verschiedene Überwachungs- und Durchsetzungsaufgaben zuständig sein können.
[195] Art. 22 Abs. 5 TTPW-VO.
[196] Siehe Europäische Kommission, Terms of Reference, European Cooperation Network on Elections.
[197] Art. 22 Abs. 8 TTPW-VO.
[198] Art. 25 und Erwägungsgrund 104 TTPW-VO.
[199] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, [2016] ABl. L 119/1.
[200] Siehe Erwägungsgrund 1 ff. DSGVO.

räumlichen Anwendungsbereich der Verordnung unter anderem auf die Tätigkeiten von für die Verarbeitung Verantwortlichen und Auftragsverarbeitern in der EU, unabhängig davon, ob die Verarbeitung in der EU stattfindet oder nicht, sowie auf für die Verarbeitung Verantwortliche und Auftragsverarbeiter mit Sitz außerhalb der EU, wenn sie einer betroffenen Person in der EU Waren oder Dienstleistungen anbieten. Für diese für die Datenverarbeitung Verantwortlichen und Auftragsverarbeiter sieht die DSGVO Verpflichtungen vor, die von Datenminimierung als Grundsatz bis hin zu Meldepflichten im Falle von Datenschutzverletzungen reichen. Betroffenen Personen stehen zahlreiche Rechte in Bezug auf die Verarbeitung ihrer personenbezogenen Daten zu, so das Recht auf Auskunft darüber, ob ihre personenbezogenen Daten verarbeitet werden (Artikel 15), das Recht auf Berichtigung unrichtiger oder unvollständiger Daten (Artikel 16), das Recht auf Löschung (Artikel 17) oder das Recht auf Widerspruch gegen die Verarbeitung personenbezogener Daten (Artikel 21).

Das Durchsetzungsregime der DSGVO vereint nationale Durchsetzungsmechanismen, grenzüberschreitende Zusammenarbeit und Koordinierungsregeln. Als Teil des administrativen Durchsetzungsregimes sollte jeder Mitgliedstaat unabhängige nationale Aufsichtsbehörden einrichten,[201] welche die in der DSGVO vorgesehenen Kooperationsmechanismen beachten müssen. [202]

Sie sind mit umfassenden Untersuchungs- und Durchsetzungsbefugnissen ausgestattet.[203] Jede Datenschutzbehörde (DSB) ist für die Untersuchung von DSGVO-Beschwerden im Hoheitsgebiet ihres eigenen Mitgliedstaats zuständig. Um eine einheitliche Anwendung der DSGVO zu erreichen, arbeitet sie mit anderen DSB im Rahmen des sogenannten „Kohärenzverfahrens“ zusammen, an dem der Europäische Datenschutzausschuss (EDSA) beteiligt ist.[204] Im Rahmen des DSGVO-Verfahrens der Zusammenarbeit und Kohärenz ist eine federführende Aufsichtsbehörde zuständig, das heißt die DSB der Hauptniederlassung des für die Verarbeitung Verantwortlichen in der EU, wenn es sich um einen grenzüberschreitenden Fall handelt; andere betroffene DSB müssen jedoch informiert werden und können Einspruch gegen einen Entscheidungsvorschlag der federführenden Behörde erheben.[205] Fragen und Herausforderungen, die sich in diesem Durchsetzungssystem, an dem verschiedene Akteure beteiligt sind, stellen, werden in einer neuen Verfahrensverordnung behandelt, die darauf abzielt, die Anforderungen an die Zulässigkeit und die Verfahren für grenzüberschreitende Sachverhalte zu harmonisieren.[206]

---

[201] Art. 51 ff. DSGVO.

[202] Zur Frage, wie die Regelung der DSGVO auf die Herausforderungen im Rahmen der Datenschutzrichtlinie zu antworten versucht, siehe Giurgiu, A. und Larsen, T. A., "Roles and Powers of National Data Protection Authorities: Moving from Directive 95/46/EC to the GDPR: Stronger and More 'European' DPAs as Guardians of Consistency?", in *European Data Protection Law Review*, 2(3), 2016, S. 342 - 352.

[203] Art. 58 DSGVO.

[204] Art. 63 DSGVO.

[205] Für einen Abriss zu den Kooperationsmechanismen nach Artikel 60 DSGVO siehe Hijmans, H., "The DPAs and their Cooperation: How Far Are We in Making Enforcement of Data Protection Law more European?", in *European Data Protection Law Review*, 2(3), 2016, S. 362 - 372.

[206] Verordnung (EU) 2025/2518 des Europäischen Parlaments und des Rates vom 26. November 2025 zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der Verordnung (EU) 2016/679 (2025] ABl. L 2025/2518.Für einen Überblick und eine Bewertung des Kommissionsvorschlags siehe Mustert, L., "The Commission Proposal for a New GDPR Procedural Regulation: Effective and Protected Enforcement Ensured?”, *European Data Protection Law Review*, 9(4), 2023, S. 454 – 464.

Artikel 83 DSGVO ermächtigt die Aufsichtsbehörden, erhebliche Geldbußen von bis zu 20 Millionen EUR oder bis zu 4 % des weltweiten Jahresumsatzes zu verhängen, je nachdem, welcher Betrag höher ist. Die Mitgliedstaaten legen darüber hinaus Regeln für andere Sanktionen bei Nichteinhaltung fest.[207]

Obwohl die DSGVO nicht speziell auf rechtswidrige Inhalte oder Desinformation abzielt, spielt sie indirekt eine wichtige Rolle dabei, wie mit solchen Inhalten umgegangen werden kann, indem sie die Verwendung personenbezogener Daten bei der Moderation von Inhalten, der Profilerstellung und beim Inhaltstargeting regelt. Mit Beschränkungen, wie personenbezogene Daten für Mikrotargeting genutzt werden dürfen, geht die DSGVO beispielsweise gegen einen zentralen Vektor bei der Verbreitung von Desinformationen vor. Die Grundsätze der Datenminimierung und der Zweckbindung schränken die Targeting-Systeme weiter ein. Darüber hinaus müssen DSB gemäß Artikel 17 DSGVO mit dem „Recht auf Vergessenwerden" auf Antrag der betroffenen Person sicherstellen, dass Vermittler Inhalte löschen, wenn die Aufbewahrung dieser Daten gegen die DSGVO, das EU-Recht oder das Recht eines Mitgliedstaats verstößt, dem der für die Verarbeitung Verantwortliche unterliegt. Die betroffene Person hat insbesondere das Recht, dass ihre personenbezogenen Daten gelöscht werden, wenn die Daten nicht mehr erforderlich oder relevant sind.[208]

2.2.2.5 Regulierung der Kommunikationstechnologie: die KI-VO

Die KI-VO[209] ist eine Produktsicherheitsverordnung, die Vorschriften zur Sicherheit der regulierten Technologie einführt; im Gegensatz zu traditionellen Sicherheitsgesetzen schützt die KI-VO jedoch auch die Grundrechte, regelt die Nutzung von KI und enthält ethische Grundsätze. Sie ist daher nicht wie die DSGVO direkt mit der Durchsetzung inhaltsbezogener Vorschriften befasst, kann aber dennoch eine unterstützende Rolle bei der Bewältigung der Risiken von Desinformation und rechtswidrigen Inhalten spielen, insbesondere wenn diese von KI-Systemen erzeugt oder verstärkt werden. Dies ist gerade deshalb der Fall, weil die KI-VO ausdrücklich das Phänomen der sogenannten Deepfakes thematisiert, das heißt durch KI erzeugte oder manipulierte Bild-, Audio- oder Videoinhalte, die wirklichen Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen ähneln und Nutzern fälschlicherweise als echt oder wahrheitsgemäß erscheinen würden.[210] Dementsprechend ergänzt diese Verordnung andere Digitalgesetze, indem es eine weitere Ebene von Verpflichtungen für den Einsatz von KI-Systemen hinzufügt.

Ähnlich wie der DSA sieht die KI-VO als risikobasierte Verordnung Verpflichtungen in Bezug auf Transparenz, Rechenschaftspflicht und Risikominderung vor. Je nach Risikograd eines KI-Systems werden unterschiedliche Verpflichtungen festgelegt. KI-

[207] Art. 84 DSGVO.
[208] C-131/12 *Google Spain SL, Google Inc. gegen AEPD* [2014] ECLI:EU:C:2014:317*;* siehe auch Pouillaude, S., "Harmonising the Enforcement of the Right to Be Forgotten: Navigating New Speech Regulation Challenges in the EU", *European Data Protection Law Review*, 10(2), 2024, S. 162 - 177.
[209] Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 [2024], ABl L 2024/1689.
[210] Art. 3 Abs. 60 KI-Gesetz.

Praktiken, die ein unannehmbares Risiko bergen, sind gemäß Artikel 5 der KI-VO verboten; dazu gehören KI-Systeme, die absichtlich manipulative oder täuschende Techniken einsetzen, um Nutzer zu einer Entscheidung zu veranlassen, die sie andernfalls nicht getroffen hätten. Im Gegensatz dazu sind Hochrisiko-KI-Systeme gemäß Artikel 6 der KI-VO KI-Systeme, die ein erhebliches Risiko für die Gesundheit, die Sicherheit oder die Grundrechte von Personen darstellen; sie unterliegen strengen gesetzlichen Verpflichtungen und einer strengen Aufsicht. Zu den Anforderungen, die an diese Systeme gestellt werden, gehören unter anderem Risikomanagement, technische Dokumentation und das Führen von Aufzeichnungen, Transparenz und menschliche Aufsicht.[211] Die KI-VO enthält spezifische Vorschriften für KI-Systeme mit allgemeinem Verwendungszweck, die systemische Risiken wie tatsächliche oder vernünftigerweise vorhersehbare negative Auswirkungen auf demokratische Prozesse und die Verbreitung rechtswidriger, falscher oder diskriminierender Inhalte bergen.[212] Darüber hinaus werden Anbietern und Anwendern von KI-Systemen mit begrenzten Risiken Transparenzverpflichtungen auferlegt, das heißt Systeme, die zum Beispiel dazu bestimmt sind, direkt mit natürlichen Personen zu interagieren (zum Beispiel Chatbots), oder die manipulierte Audio-, Bild-, Video- oder Textinhalte erzeugen.[213] So müssen beispielsweise KI-Systeme, die zur Erzeugung oder Manipulation von Bild-, Audio- oder Videoinhalten eingesetzt werden, die wirklichen Personen, Objekten, Orten, Einrichtungen oder Ereignissen stark ähneln und fälschlicherweise als echt oder wahrheitsgetreu erscheinen würden, diese sogenannten Deepfakes eindeutig als künstlich erzeugt oder manipuliert kennzeichnen und den künstlichen Ursprung offenlegen.[214] Dadurch wird sichergestellt, dass Nutzern bewusst ist, dass sie synthetische Inhalte betrachten. Inhalte, die nicht gemäß Artikel 50 der KI-VO gekennzeichnet sind, sind rechtswidrig.

Die Durchsetzung und Überwachung der KI-VO folgt dem Neuen Rechtsrahmen der EU für die Produktgesetzgebung,[215] mit dem ein Instrumentarium an Maßnahmen für die Produktgesetzgebung geschaffen wurde. Die Mitgliedstaaten müssen mindestens eine notifizierende Behörde und mindestens eine Marktüberwachungsbehörde einrichten oder benennen, die ihre Befugnisse unabhängig und unparteiisch ausüben.[216] Die Marktüberwachungsbehörden beaufsichtigen die Einhaltung der Vorschriften für KI-Systeme einschließlich der Verbote und Vorschriften für Hochrisiko-KI-Systeme und setzen diese durch, während die notifizierenden Behörden die notifizierten Stellen benennen und beaufsichtigen. Bei diesen Stellen handelt es sich um unabhängige Stellen, die Konformitätsbewertungen vor dem Inverkehrbringen durchführen. In diesem Zusammenhang ist anzumerken, dass bei Hochrisiko-KI-Systemen die Durchsetzung in ein Ex-ante-Konformitätsbewertungssystem eingebettet ist. Ein neues Büro für künstliche Intelligenz[217] auf EU-Ebene sorgt für eine harmonisierte Durchsetzung und Aufsicht, insbesondere in Bezug auf KI-Modelle mit allgemeinem Verwendungszweck.[218] Das Büro für

[211] Art. 8 ff. KI-Gesetz.
[212] Siehe Art. 55 und Erwägungsgrund 110 KI-Gesetz.
[213] Art. 50 KI-Gesetz.
[214] Art. 50 Abs. 4 KI-Gesetz.
[215] Siehe die spezielle Website der Europäischen Kommission.
[216] Art. 70 KI-Gesetz.
[217] Art. 64 KI-Gesetz.
[218] Siehe Art. 88 KI-Gesetz.

künstliche Intelligenz ist demzufolge mit Untersuchungs- und Durchsetzungsbefugnissen ausgestattet.[219] Darüber hinaus wird mit Artikel 65 der KI-VO ein Europäisches Gremium für künstliche Intelligenz eingerichtet, das unter anderem die Aufgabe hat, zur Koordinierung zwischen den zuständigen nationalen Behörden und zur Harmonisierung der Verwaltungspraxis in den Mitgliedstaaten beizutragen.[220] Die KI-VO sieht abgestufte Bußgelder vor. Bei Missachtung des Verbots der genannten KI-Praktiken gemäß Artikel 5 der KI-VOGesetzes werden Geldbußen von bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes fällig, je nachdem, welcher Betrag höher ist. Für falsche, unvollständige oder irreführende Informationen als Antwort auf Auskunftsersuchen notifizierter Stellen oder zuständiger nationaler Behörden können Geldbußen von bis zu 7,5 Mio. EUR oder 1 % des weltweiten Jahresumsatzes verhängt werden, je nachdem, welcher Betrag höher ist.[221]

2.2.2.6 Weitere Ansätze zur Regulierung von Inhalten, die als rechtswidrig gelten

Neben dem oben beschriebenen EU-Sekundärrecht regeln auch sektorspezifische Instrumente Online-Inhalte, die als illegal gelten, und es gibt zunehmend harmonisierte strafrechtliche Bestimmungen.

Für terrorismusbezogene Inhalte sieht die Verordnung über terroristische Inhalte (TCO-VO)[222] Durchsetzungsmechanismen vor und verpflichtet Plattformen, selektiv gegen verbotene Inhalte vorzugehen. Gemäß TCO-VO müssen Hostingdiensteanbieter, die in der EU Dienste anbieten, terroristische Inhalte innerhalb einer Stunde nach Erhalt einer Entfernungsanordnung löschen.[223] Dementsprechend sieht die TCO-VO ein Schnellreaktionsmodell mit direkter Durchsetzung durch die zuständigen nationalen Behörden im Rahmen der TCO-VO vor; diese Behörden sind für die Ausstellung von Entfernungsanordnungen und die Verhängung von Sanktionen zuständig. Die Mitgliedstaaten müssen Regeln für Verwaltungssanktionen bei Zuwiderhandlungen gegen die TCO-VO festlegen und sicherstellen, dass systematische oder anhaltende Nichtbefolgung von Entfernungsanordnungen mit finanziellen Sanktionen von bis zu 4 % des Gesamtjahresumsatzes des Anbieters geahndet wird.[224] Die TCO-VO schreibt darüber hinaus die Zusammenarbeit zwischen den zuständigen nationalen Behörden, den Hostingdiensteanbietern und Europol vor.[225] Die Anwendung der TCO-VO wird von der Europäischen Kommission überwacht, der die Mitgliedstaaten jährlich über die in Übereinstimmung mit der TCO-VO ergriffenen Maßnahmen einschließlich der Anzahl der Entfernungsanordnungen Bericht erstatten müssen.

Weitere EU-Rechtsinstrumente zielen darauf ab, die Rechtswidrigkeit bestimmter Verhaltensweisen im Internet zu harmonisieren, wie zum Beispiel die Richtlinie zur

[219] Siehe Art. 88 ff. KI-Gesetz.
[220] Art. 66 KI-Gesetz.
[221] Art. 99 KI-Gesetz.
[222] Verordnung (EU) 2021/784 des Europäischen Parlaments und des Rates vom 29. April 2021 zur Bekämpfung der Verbreitung terroristischer Online-Inhalte, ABl. L 172/79, 17. Mai 2021
[223] Art. 3 TCO-VO.
[224] Art. 18 TCO-VO.
[225] Art. 14 TCO-VO.

Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt.[226] Diese Richtlinie stellt die Anstiftung zu Gewalt oder Hass im Internet aufgrund des Geschlechts sowie die Weitergabe von Intimbildern ohne Zustimmung unter Strafe, sieht jedoch außer der Förderung von Zusammenarbeit der einschlägigen Vermittler auf Selbstregulierungsebene, zum Beispiel durch die Erstellung von Verhaltenskodizes, keine spezifischen Durchsetzungsmechanismen vor. Die Kriminalisierung von Hassrede wird zudem mit dem Rahmenbeschluss 2008/913/JI des Rates[227] weiter thematisiert, der eine Grundlage für die Kriminalisierung von Hassrede und Hassverbrechen in allen Mitgliedstaaten bildet und rassistische und fremdenfeindliche Inhalte behandelt. Obwohl dieser Rahmenbeschluss als Instrument zwischenstaatlicher Zusammenarbeit nicht direkt anwendbar ist, verpflichtet er die Mitgliedstaaten zur Umsetzung seiner Bestimmungen in nationales Recht und führt damit zu einer Angleichung der Rechtsvorschriften der Mitgliedstaaten. Darüber hinaus zielt der Vorschlag für eine Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern[228] darauf ab, Verpflichtungen zur Risikobewertung und -minderung sowie zur Aufdeckung, Meldung und Entfernung von Material über sexuellen Missbrauch von Kindern einzuführen; eine mögliche Ausweitung dieser Verpflichtungen auf proaktives Durchsuchen durch Online-Plattformen wird kontrovers diskutiert.[229] Mit dem Vorschlag sollen die Schwachstellen einer früheren Richtlinie[230] behoben werden, die zwar die Entfernung des besagten Materials und die Sperrung des Zugangs zu diesem Materia vorschrieb, jedoch keine detaillierteren Regeln für das Verfahren enthielt. Ein zweiter Mechanismus in der Richtlinie bot den Mitgliedstaaten einen Rahmen, Maßnahmen zur Sperrung ausländischer Websites zu ergreifen, auf denen Material über sexuellen Missbrauch von Kindern verbreitet wird. Da die Umsetzung jedoch freiwillig war, führte nur die Hälfte der Mitgliedstaaten spezifische nationale Rechtsvorschriften ein.

2.2.3 Maßnahmen zur Bekämpfung rechtswidriger und schädlicher Inhalte im Rahmen der GASP

Im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik (GASP) der EU hat die Union gezielte Maßnahmen zur Bekämpfung der Verbreitung illegaler und schädlicher Inhalte durch ausländische Akteure ergriffen, insbesondere im Zusammenhang mit

[226] Richtlinie (EU) 2024/1385 des Europäischen Parlaments und des Rates vom 14. Mai 2024 zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt, ABl. L 2024/1385, 24. Mai 2024.
[227] Rahmenbeschluss 2008/913/JI des Rates vom 28. November 2008 zur strafrechtlichen Bekämpfung bestimmter Formen und Ausdrucksweisen von Rassismus und Fremdenfeindlichkeit, ABl. L 328/55, 6. Dezember 2008.
[228] Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern, COM/2022/209 final.
[229] Leiser, M. R. und Murray, A. D., "Rethinking Safety-by-Design and Techno-Solutionism for the Regulation of Child Sexual Abuse Material", in *Technology and Regulation*, 2025, S. 131 - 171.
[230] Richtlinie 2011/93 des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates, ABl. L 335/1, 17. Dezember 2012.

Desinformationskampagnen und Cyberbedrohungen. Diese Maßnahmen werden in der Regel durch Ratsbeschlüsse und -verordnungen erlassen, mit denen restriktive Maßnahmen gegen Personen oder Einrichtungen verhängt werden, die für die Durchführung oder Unterstützung von Operationen ausländischer Informationsmanipulation und Einmischung (Foreign Information Manipulation and Interference - FIMI) verantwortlich sind, welche die Sicherheit, die Demokratie oder die öffentliche Ordnung der EU oder ihrer Mitgliedstaaten bedrohen. Als Reaktion auf den Krieg Russlands gegen die Ukraine hat die EU Maßnahmen ergriffen, die zur Aussetzung der Sendetätigkeit und der Lizenzen mehrerer staatlich kontrollierter russischer Medien geführt haben.[231] Da der Lizenzentzug in der Praxis die Verbreitung von Inhalten in der EU nicht verhindern konnte, verhängte der Rat der EU Sanktionen in Form eines Beschlusses und einer Verordnung, die es den Betreibern untersagten, die Inhalte bestimmter staatlich kontrollierter Medien (namentlich RT und Sputnik) in der EU auszustrahlen oder anderweitig zu deren Ausstrahlung beizutragen, und begründete dies mit deren Rolle bei der Verbreitung von verdrehten Tatsachen und Desinformation.[232] Diese Maßnahmen wurden anschließend auf mehrere andere russische Medien[233] ausgeweitet und vom Gericht der EU als mit den Grundrechten vereinbar bestätigt. Ein Antrag einer niederländischen Koalition von Internet-Diensteanbietern und Medienorganisationen beim EuGH auf Nichtigerklärung der Anordnungen über das Verbot der Verbreitung oder Unterstützung der Verbreitung von Inhalten der sanktionierten Einrichtungen war nicht erfolgreich.[234] Es folgten weitere restriktive Maßnahmen gegen

[231] Siehe den Überblick von Cabrera Blázquez, F. J., „Europäische Kommission: Verbot von Russia Today und Sputnik“, IRIS 2022-3:1/6, Europäische Audiovisuelle Informationsstelle, Straßburg, 2022 und "The Implemenation of EU Sanctions against RT and Sputnik", Europäische Audiovisuelle Informationsstelle, Straßburg, 2022; Cole, M. D. und Etteldorf, C., "Future Regulation of Cross-Border Audiovisual Content Dissemination", Bd. 84 *Schriftenreihe Medienforschung der LfM NRW*, Nomos, Baden-Baden, 2023, S. 217 ff.

[232] Verordnung (EU) 2022/350 des Rates vom 1. März 2022 zur Änderung der Verordnung (EU) Nr. 833/2014 über restriktive Maßnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren, ABl L 65/2, 2. März 2022, und Beschluss (GASP) 2022/351 des Rates vom 1. März 2022 zur Änderung des Beschlusses 2014/512/GASP über restriktive Maßnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren, ABl L 65/1, 2. März 2022.

[233] Zum Beispiel: Verordnung (EU) 2022/879 des Rates vom 3. Juni 2022 zur Änderung der Verordnung (EU) Nr. 833/2014 über restriktive Maßnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren, ABl. L 153/53, 3. Juni 2022 und Durchführungsverordnung (EU) 2022/994 des Rates vom 24. Juni 2022 zur Durchführung der Verordnung (EU) 2022/879 zur Änderung der Verordnung (EU) Nr. 833/2014 über restriktive Maßnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren, ABl. LI 167/1, 24. Juni 2022; Verordnung (EU) 2022/2474 des Rates vom 16. Dezember 2022 zur Änderung der Verordnung (EU) Nr. 833/2014 über restriktive Maßnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren, ABl. LI 322/1, 16. Dezember 2022 und Durchführungsverordnung (EU) 2023/180 des Rates vom 27. Januar 2023 zur Durchführung der Verordnung (EU) 2022/2474 zur Änderung der Verordnung (EU) Nr. 833/2014 über restriktive Maßnahmen angesichts der Handlungen Russlands zur Destabilisierung der Lage in der Ukraine, ABl. L 26/1, 30. Januar 2023; Verordnung (EU) 2023/427 des Rates vom 25. Februar 2023 zur Änderung der Verordnung (EU) Nr. 833/2014 über restriktive Maßnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren, ABl. LI 59/6, 25. Februar 2023 und Durchführungsverordnung (EU) 2023/722 des Rates vom 31. März 2023 zur Durchführung der Verordnung (EU) 2023/427 zur Änderung der Verordnung (EU) Nr. 833/2014 über restriktive Maßnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren, ABl. L 94/19, 3. April 2023.

[234] T-307/22 *A2B Connect und andere gegen den Rat* (GK, 26. März 2025) ECLI:EU:T:2025:331. Siehe auch zuvor *T-125/22 RT France gegen den Rat* (GK, 27. Juli 2022) ECLI:EU:T:2022:483.

russische Einrichtungen, die auch auf Einzelpersonen wegen Betreibens einer Desinformationskampagne abzielten.[235]

Diese Maßnahmen, die in der Zuständigkeit der EU für das auswärtige Handeln begründet sind, zeigen die sich entwickelnde Rolle der GASP bei der Bekämpfung ausländischer Informationsbedrohungen und der Ergänzung interner Regulierungsbemühungen im Rahmen von Instrumenten wie dem DSA. Darüber hinaus tragen sie zum Verständnis des sich entwickelnden Rechtsrahmens bei, zum Beispiel der Vorschriften für unseriöse Mediendienste und der beschleunigten Zusammenarbeit im Rahmen des EMFA.[236]

Im Rahmen der zweiten Säule der Gemeinsamen Außen- und Sicherheitspolitik der EU war der Europäische Auswärtige Dienst (EAD) ebenfalls besonders aktiv bei der Bekämpfung von Desinformation. Seit 2015 berichtet der EAD regelmäßig über Desinformation einschließlich Wahlbeeinflussungsversuchen und FIMI-Aktivitäten auf seiner Website zum Sensibilisierungsprojekt „EUvsDisinfo“[237] und in den sozialen Medien auf der Grundlage der Schlussfolgerungen des Europäischen Rates für Außenbeziehungen vom 19. März 2015[238] und anschließend im Rahmen des Aktionsplans gegen Desinformation der Hohen Vertreterin für Außen- und Sicherheitspolitik vom 5. Dezember 2018.[239]

2022 verabschiedete der EAD einen Strategiekompass für Sicherheit und Verteidigung, der die Entwicklung einer FIMI-Toolbox vorsieht, um die Fähigkeit zur Erkennung, Analyse und Reaktion auf die Bedrohung zu stärken und die Fähigkeiten der EU zur strategischen Kommunikation und Desinformationsbekämpfung weiter auszubauen.[240] Die Toolbox behandelt verschiedene Bereiche und skizziert kurz-, mittel- und langfristige Maßnahmen zur Bekämpfung von FIMI. Die Maßnahmen reichen von Gegenmaßnahmen vor einem Vorfall (zum Beispiel Medienkompetenzprogramme), über minimierende Gegenmaßnahmen (zum Beispiel die Entfernung von Online-Inhalten in Abhängigkeit von bestehenden Vorschriften oder Mechanismen) bis hin zu Gegenmaßnahmen nach einem Vorfall einschließlich Informationsaustausch und Anwendung rechtlicher Maßnahmen und Sanktionen.[241] Ähnlich wie im Bereich der Cybersicherheit wird großer Wert auf Informationsaustausch gelegt, um den Grad der Bereitschaft zu erhöhen. Dementsprechend

---

[235] Beschluss (GASP) 2023/1566 des Rates vom 28. Juli 2023 zur Änderung des Beschlusses 2014/145/GASP über restriktive Maßnahmen angesichts von Handlungen, die die territoriale Unversehrtheit, Souveränität und Unabhängigkeit der Ukraine untergraben oder bedrohen, ABl. LI 190/21, 28. Juli 2023; Durchführungsverordnung (EU) 2023/1563 des Rates vom 28. Juli 2023 zur Durchführung der Verordnung (EU) Nr. 269/2014 über restriktive Maßnahmen angesichts von Handlungen, die die territoriale Unversehrtheit, Souveränität und Unabhängigkeit der Ukraine untergraben oder bedrohen, ABl. LI 190/1, 28. Juli 2023.

[236] Siehe in diesem Zusammenhang Eskens, S., "The Role of Regulation on the Transparency and Targeting of Political Advertising and European Media Freedom Act in the EU's Anti-Disinformation Strategy", in *Computer Law & Security Review*, 58, 2025, 106185.

[237] Siehe https://euvsdisinfo.eu/de/.

[238] Europäischer Rat, Tagung des Europäischen Rates (19. und 20. März 2015) - Schlussfolgerungen (engl.), (2015) EUCO 11/15.

[239] Europäische Kommission, Hohe Vertreterin der Union für die Außen- und Sicherheitspolitik, Gemeinsame Mitteilung an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Aktionsplan gegen Desinformation (engl.) (JOIN(2018) 36 final).

[240] EAD, “A Strategic Compass for Security and Defence”, 2022, S. 40.

[241] EAD, "2nd EEAS Report on Foreign Information Manipulation and Interference Threats", Januar 2024, S. 17 ff.

wurde 2023 das FIMI-Informationsaustausch- und Analysezentrum (FIMI-ISAC) als gemeinschaftsbasiertes Netzwerk mit der Zivilgesellschaft und anderen Interessenträgern eingerichtet.[242]

[242] EAD, "EEAS Stratcom's Responses to Foreign Information Manipulation and Interference (FIMI) in 2023", Pressemitteilung vom 28. Juni 2024.

3. Bekämpfung von Desinformation

3.1 Durchsetzung auf EU-Ebene

Dr Mark D. Cole, Wissenschaftlicher Direktor des Instituts für Europäisches Medienrecht (EMR) und Professor für Medien- und Telekommunikationsrecht, Universität Luxemburg

Desinformation kann viele Formen annehmen, und es gibt viele Arten, die gemeinhin als problematisch angesehen werden, unter anderem politische Desinformation,[243] Desinformation im Gesundheitsbereich,[244] Verschwörungstheorien,[245] Deepfakes[246] und manipulierte Medien[247] sowie ausländische Einflussnahme. Auch Betrügereien wie unechte Kapitalanlagemodelle oder soziale und kulturelle Täuschung wie falsche Geschichten, die darauf abzielen, rassische, religiöse oder ethnische Spannungen zu schüren, können unter diesen Oberbegriff fallen, wenn falsche oder irreführende Inhalte verwendet werden, um Menschen mit dem Ziel wirtschaftlichen Gewinns zu übervorteilen oder der Öffentlichkeit Schaden zuzufügen.

Der folgende Abschnitt konzentriert sich auf staatlich gelenkte Desinformation als Beispiel dafür, wie Umfang und Qualität von Desinformationskampagnen in der EU zugenommen haben. Parallel dazu ist eine Verschärfung der Maßnahmen und der Durchsetzung mithilfe verbindlicher gesetzlicher Lösungen zu beobachten.

Auf EU-Ebene wurden seit 2015 vielfältige Initiativen gegen Desinformation ergriffen, als der Europäische Rat nach der rechtswidrigen Annexion der Krim durch Russland 2014 die Notwendigkeit betonte, „gegen die anhaltenden Desinformationskampagnen Russlands vorzugehen".[248] Während sich die ersten politischen Maßnahmen auf sogenannte „hybride Bedrohungen" (das heißt schädliche Aktivitäten staatlicher und nicht staatlicher Akteure, die eine Mischung aus militärischen und nicht

[243] Siehe Europäische Kommission, "Digital Services Act - Application of the Risk Management Framework to Russian Disinformation Campaigns", Amt für Veröffentlichungen der Europäischen Union, Luxemburg, 2023.
[244] Europäische Kommission und Hohe Vertreterin der Union für die Außen- und Sicherheitspolitik, Gemeinsame Mitteilung an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Bekämpfung von Desinformation im Zusammenhang mit COVID-19 – Fakten statt Fiktion 2020.
[245] Siehe die spezielle Website "Identifying Conspiracy Theories" der Europäischen Kommission.
[246] Europol, "Facing Reality? Law Enforcement and the Challenges of Deepfakes", Amt für Veröffentlichungen der Europäischen Union, Luxemburg, 2022, S. 10 ff.
[247] Marwick, A. und Lewis, R. *Media Manipulation and Disinformation Online*, Data & Society Research Institute, 2017; Wardle, C. und Derakhshan, H., "Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making", Bericht des Europarats DGI(2017)09, S. 20 ff. Siehe auch die spezielle Website „Gezielt kommunizieren, Informationsmanipulation und Einflussnahme aus dem Ausland den Kampf ansagen" der Europäischen Kommission.
[248] Europäischer Rat, Schlussfolgerungen der Tagung des Europäischen Rates vom 19. und 20. März 2015 (engl.), 2015.

militärischen Methoden ohne formelle Kriegserklärung einsetzen) konzentrierten,[249] zielten Folgemaßnahmen darauf ab, den Anwendungsbereich dieser Initiativen auf „Desinformation" auszuweiten, verstanden als „nachweislich falsche oder irreführende Informationen, die mit dem Ziel des wirtschaftlichen Gewinns oder der vorsätzlichen Täuschung der Öffentlichkeit konzipiert, vorgelegt und verbreitet werden und öffentlichen Schaden anrichten können."[250] Diese Definition von Desinformation wurde erstmals 2018 in einer Mitteilung der Kommission zur Bekämpfung von Online-Desinformation[251] verwendet, in der die Europäische Kommission die Erarbeitung eines „Verhaltenskodex für den Bereich der Desinformation" für Online-Plattformen und Werbetreibende unterstützte. In dieser Mitteilung wurden mögliche Regulierungsmaßnahmen für den Fall angekündigt, dass sich der Verhaltenskodex als „nicht zufriedenstellend" erweisen sollte.[252] Der EU-Verhaltenskodex zur Bekämpfung von Desinformation wurde schließlich im Oktober 2018 veröffentlicht und unterzeichnet.[253] Es war das erste Mal, dass sich Akteure der Industrie auf freiwilliger Basis auf Selbstregulierungsstandards zur Bekämpfung von Desinformation geeinigt haben und damit von rein politischen zu rechtlichen Maßnahmen übergegangen sind. Auf der Grundlage der Kommissionsmitteilung und als Reaktion auf die Aufforderung des Europäischen Rates, Maßnahmen zum „Schutz der demokratischen Systeme der Union und zur Bekämpfung von Desinformation, auch im Zusammenhang mit den bevorstehenden Europawahlen,"[254] zu ergreifen, haben die Europäische Kommission und die Hohe Vertreterin der Union für Außen- und Sicherheitspolitik eine gemeinsame Mitteilung zu einem Aktionsplan gegen Desinformation veröffentlicht.[255] Eines der Elemente des Aktionsplans gegen Desinformation war die Einrichtung der unabhängigen Europäischen Beobachtungsstelle für digitale Medien (EDMO),[256] die als Drehscheibe für eine grenzübergreifende und multidisziplinäre Gemeinschaft von unabhängigen Faktenprüfern, Wissenschaftlern und anderen relevanten Interessenträgern dient, die untereinander zusammenarbeiten. Zu den Aktivitäten der EDMO gehören die Kartierung von Faktenprüfungsorganisationen und die Unterstützung von Behörden bei der Überwachung

[249] Zum Beispiel die Einrichtung der *East StratCom Task Force* (des Strategischen Kommunikationsteams Ost) 2015 und die gemeinsame Mitteilung für die Abwehr hybrider Bedrohungen (Europäische Kommission und Hohe Vertreterin der Union für Außen- und Sicherheitspolitik, Gemeinsame Mitteilung an das Europäische Parlament und den Rat - Gemeinsamer Rahmen für die Abwehr hybrider Bedrohungen - eine Antwort der Europäischen Union, 2016). Siehe auch Europäisches Parlament, Entschließung vom 23. November 2016 zu dem Thema „Strategische Kommunikation der EU, um gegen sie gerichteter Propaganda von Dritten entgegenzuwirken", 2016.

[250] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Bekämpfung von Desinformation im Internet: ein europäisches Konzept" COM(2018) 236 final, 26. April 2018.

[251] Ebd.

[252] Ebd., Abs. 3.1.1.

[253] Europäische Kommission, Verhaltenskodex zur Bekämpfung von Desinformation, 2018.

[254] Europäischer Rat, Schlussfolgerungen des Europäischen Rates (engl.), Pressemitteilung, 18. Oktober 2018.

[255] Europäische Kommission und Hohe Vertreterin der Union für die Außen- und Sicherheitspolitik, Gemeinsame Mitteilung an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Aktionsplan gegen Desinformation, 2018

[256] Die EDMO wird von einem Konsortium unter der Leitung des Europäischen Hochschulinstituts in Florenz, Italien, geführt und ist völlig unabhängig von öffentlichen Stellen einschließlich der Europäischen Kommission. Für weitere Informationen siehe https://digital-strategy.ec.europa.eu/en/policies/european-digital-media-observatory.

der Maßnahmen, die von Online-Plattformen ergriffen werden, um die Verbreitung und die Auswirkungen von Desinformationen zu begrenzen.

Während sich der Aktionsplan gegen Desinformation auf Desinformation im Allgemeinen konzentrierte, veranlasste die COVID-19-Pandemie die Europäische Kommission und den Hohen Vertreter der Union für Außen- und Sicherheitspolitik, den Schwerpunkt auf spezifische Maßnahmen im Zusammenhang mit pandemiebezogener Desinformation zu verlagern.[257] In Ergänzung zu den spezifischen Maßnahmen gegen Desinformation griff die Europäische Kommission dieses Thema auch in anderen zielgerichteten politischen Instrumenten auf, zum Beispiel im Europäischen Aktionsplan für Demokratie,[258] der Demokratie durch die Förderung freier und fairer Wahlen, die Unterstützung freier und unabhängiger Medien und die Bekämpfung von Desinformation stärken soll.

Bei einer ersten Bewertung der Umsetzung des EU-Verhaltenskodexes zur Bekämpfung von Desinformation im September 2020 wurden mehrere Schwachstellen festgestellt,[259] was in der Folge zur Verabschiedung eines verschärften Verhaltenskodex am 16. Juni 2022 führte.[260] Am 13. Februar 2025 billigten die Europäische Kommission und das Europäische Gremium für digitale Dienste (EGDD)[261] die Integration des freiwilligen verschärften Verhaltenskodex 2022 zur Bekämpfung von Desinformation in den Rahmen des DSA,[262] der dann zum Verhaltenskodex zur Bekämpfung von Desinformation wurde.[263]

Infolgedessen dient letzterer Verhaltenskodex zur Bekämpfung von Desinformation als relevanter Maßstab, um zu prüfen, ob die Anbieter von sehr großen Online-Plattformen (VLOP) und sehr großen Online-Suchmaschinen (VLOSE)[264], gemeinsam als VLOPSE bezeichnet, die Vorschriften des DSA in Bezug auf Desinformationsrisiken einhalten und die Verpflichtungen des Kodex befolgen.[265] Die Verpflichtungen sind nach folgenden Bereichen zusammengefasst: Platzierung von Werbeanzeigen, politische Werbung, Integrität der Nutzer, Stärkung der Nutzer, Stärkung der Forscher-Community, Stärkung der

---

[257] Europäische Kommission und Hoher Vertreter der Union für die Außen- und Sicherheitspolitik, Gemeinsame Mitteilung an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Bekämpfung von Desinformation im Zusammenhang mit COVID-19 – Fakten statt Fiktion, 2020

[258] Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen - Europäischer Aktionsplan für Demokratie, 2020. In diesem Plan wurden auch das Gesetz über digitale Dienste (DSA) und die Verordnung über die Transparenz und das Targeting politischer Werbung (TTPW-VO) angekündigt, auf die auf den folgenden Seiten eingegangen wird.

[259] Europäische Kommission, Arbeitsdokument der Kommissionsdienststellen, Bewertung des Verhaltenskodex zur Bekämpfung von Desinformation - Erfolge und Bereiche für weitere Verbesserungen (engl.), SWD(2020) 180 final.

[260] Europäische Kommission, The Strengthened Code of Practice on Disinformation (Verschärfter Verhaltenskodex zur Bekämpfung von Desinformation) 2022

[261] Siehe Abschnitt 2.2.2.2.

[262] Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste) ABl.. L 277, 27. Oktober 2022.

[263] Europäische Kommission, Verhaltenskodex zur Bekämpfung von Desinformation (engl.), 2025

[264] Zum Begriff der VLOP und VLOSE siehe Abschnitt 2.2.2.2.

[265] Die Integration des Verhaltenskodexes zur Bekämpfung von Desinformation in den DSA-Rahmen trat am 1. Juli 2025 in Kraft.

Faktenchecker-Community, Einrichtung und Unterhaltung eines Transparenzzentrums, Einrichtung einer ständigen Task Force und Überwachung des Kodex. In Bezug auf die Platzierung von Werbeanzeigen umfassen die Verpflichtungen der Unterzeichner neben anderem die Demonetisierung von Desinformationen *(*unter anderem, indem Ad-Tech-Anbieter keine Anzeigen auf Websites platzieren, die dafür bekannt sind, dass sie Desinformationen verbreiten) und die Verhinderung des Missbrauchs von Werbesystemen zur Verbreitung von Desinformationen in Form von Werbebotschaften.[266] Zur Stärkung der Faktenchecker-Community ist zu sagen, dass Faktenprüfung eine wichtige Rolle bei der Bekämpfung der Risiken von Desinformation und rechtswidrigen Inhalten im Rahmen des DSA spielt.[267] Der DSA schreibt Faktenprüfung zwar nicht direkt vor, aber der EU-Verhaltenskodex erkennt Faktenprüfung als eine zentrale Maßnahme zur Risikominderung im Rahmen des Managements systemischer Risiken an und fordert daher eine Verpflichtung zur Zusammenarbeit mit der Faktenprüfergemeinde, auch in Bezug auf Ressourcen und Unterstützung.[268]

Die Integration des Verhaltenskodexes zur Bekämpfung von Desinformation in den DSA-Rahmen kann als eine verschärfte Reaktion auf das bisherige begrenzte Engagement und die daraus resultierende begrenzte Wirksamkeit der Initiativen und Maßnahmen der VLOP und VLOSE gesehen werden.[269]

Wie die Faktenprüfung zu erfolgen hat, wird im EU-Verhaltenskodex selbst nicht näher ausgeführt. Um die Qualität von Faktenprüfung zu fördern und zu verbessern, haben Faktenprüfungsorganisationen das europäische Netzwerk für Faktenprüfung (*European Fact-Checking Standards Network* - EFCSN)[270] gegründet, eine Vereinigung, deren Mitglieder sich zur Einhaltung bestimmter Qualitätsstandards verpflichtet haben, die im Europäischen Normenkodex für unabhängige Faktenprüfungsorganisationen beschrieben sind.[271] Dieser Kodex stellt ein Selbstregulierungsinstrument für Faktenprüfer dar und enthält unter anderem eine Methodik zur Verifizierung der Richtigkeit von in der Öffentlichkeit aufgestellten Behauptungen sowie ethische Standards.

Faktenprüfung ist vom Konzept der „vertrauenswürdigen Hinweisgeber“ zu unterscheiden, das im Rahmen des DSA selbst geregelt ist. Letztere werden von den nationalen Regulierungsbehörden, den Koordinatoren für digitale Dienste (DSC/KDD), benannt und müssen strenge Kriterien in Bezug auf Sachkenntnis, Unabhängigkeit, Transparenz und Genauigkeit erfüllen – sie achten schwerpunktmäßig auf die Einhaltung des geltenden Rechts und nicht nur auf Genauigkeit oder Wahrhaftigkeit; aus diesen Gründen wird ihnen auch ein vorrangiger Status nach dem oben beschriebenen Rahmen für Melde- und Abhilfeverfahren zugewiesen. Im Gegensatz dazu helfen Faktenprüfer den Plattformen, falsche oder irreführende Inhalte zu kennzeichnen, zu kontextualisieren oder herabzustufen, anstatt ihre Entfernung zu fordern. Wie bereits erwähnt, sind

[266] Europäische Kommission, Code of Practice on Disinformation (Verhaltenskodex zur Bekämpfung von Desinformation), 2025, S. 10 ff.
[267] Ebd., S. 37 ff
[268] Ebd.
[269] Vgl. EDMO, *Implementing the EU Code of Practice on Disinformation - An Evaluation of VLOPSE Compliance and Effectiveness (January-June 2024)*, EDMO, Florenz, Juni 2025.
[270] Siehe https://efcsn.com/.
[271] Der Europäische Normenkodex wurde auf der EFCSN-Website (engl.) veröffentlicht.

Faktenprüfungsorganisationen keine formell definierte Kategorie im DSA, spielen aber eine wichtige Rolle bei der Risikominderung.

Die Einbeziehung von Faktenprüfung kann zuweilen zu Spannungen mit dem Geschäftsmodell von Plattformen und mit der Nutzerdynamik führen. Daher sondieren Anbieter sozialer Medien Alternativen wie die von X eingeführten „kollektiven Anmerkungen" („*Community Notes*"),[272] um Desinformation durch gemeinschaftliche Faktenprüfung zu begegnen. Das Programm der kollektiven Anmerkungen ermöglicht es registrierten Nutzern, Kontext oder Korrekturen zu potenziell irreführenden Posts hinzuzufügen, die als Anmerkung zum ursprünglichen Post angezeigt werden. Dieser Mechanismus ist Gegenstand des förmlichen Verfahrens, das die Europäische Kommission am 18. Dezember 2023 gegen X eingeleitet hat und in dem es unter anderem um die Einhaltung der Verpflichtungen im Zusammenhang mit der Bekämpfung der Verbreitung rechtswidriger Inhalte in der EU und die Wirksamkeit von Maßnahmen zur Bekämpfung von Informationsmanipulation auf der Plattform geht.[273] Vorläufige Untersuchungsergebnisse haben Verstöße gegen DSA-Verpflichtungen offengelegt. Die Untersuchung unter anderem der Inhaltsmoderation war im August 2025 allerdings noch nicht abgeschlossen. Im Januar 2025 hat die Europäische Kommission mehrere Auskunftsersuchen an X gerichtet, darunter auch Anfragen nach Zugang zu Anwendungsprogrammierschnittstellen (API), um die komplexe Bewertung systemischer Risiken und deren Minderung voranzutreiben.[274]

Einen gewissen Einblick in die Methoden der Inhaltsmoderation bieten die verpflichtenden Transparenzberichte, die von allen Anbietern von Vermittlungsdiensten zu erstellen sind und in denen auch die Zahl der Anträge auf Entfernung, ihr Ursprung und ihre Bearbeitung offengelegt werden (siehe auch oben). Darüber hinaus liefert die DSA-Transparenzdatenbank empirische Daten zu den Begründungen, die die Anbieter der Kommission vorgelegt haben. Abgesehen von einem Überblick über die Gesamtzahl der vorgelegten Begründungen geben die Daten jedoch lediglich begrenzten Aufschluss über die Art der Verstöße, da die am häufigsten angegebene Kategorie „sonstige Verstöße gegen die Geschäftsbedingungen des Anbieters" ist.[275]

Auf EU-Ebene sind gezielte Maßnahmen gegen Desinformation auch in spezifischen Kontexten zu beobachten, zum Beispiel bei den Wahlen zum Europäischen Parlament 2024, wo eine beispiellose Zusammenarbeit stattfand, um die Reaktionen auf Manipulation von Informationen und Einmischung aus dem Ausland (Foreign Information Manipulation and Interference - FIMI) und Desinformation zu koordinieren.[276] Dazu gehörten die Zusammenarbeit im Rahmen spezifischer Kooperationsstrukturen wie dem Europäischen

---

[272] Siehe https://help.x.com/de/using-x/community-notes.

[273] Europäische Kommission, „Kommission leitet im Rahmen des Gesetzes über digitale Dienste ein förmliches Verfahren gegen X ein", Pressemitteilung, 18. Dezember 2023.

[274] Europäische Kommission, "Commission Addresses Additional Investigatory Measures to X in the Ongoing Proceedings under the Digital Services Act", Pressemitteilung, 17. Januar 2025.

[275] Forschungen haben ergeben, dass mehr als 99,8 % der Fälle auf Zuwiderhandlungen gegen die Nutzungsbedingungen beruhen. Siehe Kaushal, R. et al, *Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database*, in *The 2024 ACM Conference on Fairness, Accountability, and Transparency (FAccT '24), June 03-06, 2024, Rio de Janeiro, Brazil*, ACM, New York, 2024, S. 1121-1132.

[276] Siehe Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Bericht über die Wahlen zum Europäischen Parlament 2024 (engl.), COM(2025) 287 final, 2025.

Kooperationsnetz für Wahlen[277] und mehrere zentrale Maßnahmen, die eingeleitet wurden, um auf die Herausforderungen für die Integrität des Wahlprozesses zu reagieren. Diese Maßnahmen haben auch die Zusammenarbeit zwischen den EU-Institutionen, den Mitgliedstaaten und verschiedenen Einrichtungen wie den Medien, Faktenprüfern und Organisationen der Zivilgesellschaft eingeschlossen.[278] Im April 2024 sorgte die Aktivierung der „Integrierten Regelung für die politische Reaktion auf Krisen" (IPCR)[279] durch die belgische Ratspräsidentschaft für eine schnelle und koordinierte Entscheidungsfindung auf politischer Ebene der EU, insbesondere durch die Unterstützung des Informationsaustauschs zwischen den Mitgliedstaaten und den EU-Institutionen in Bezug auf Desinformation.[280] Ergänzt wurde dies durch die Überwachung und Maßnahmen des Netzwerks der Europäischen Kommission zur Bekämpfung von Desinformation (*Network against Disinformation* – NaD), das als Vorgabe des Aktionsplans gegen Desinformation einen weiteren internen Mechanismus der Kommission zur Bekämpfung von Desinformation darstellt.[281] Aktuelle Informationen über die Verbreitung von Desinformationsnarrativen in der EU wurden von der EDMO zur Verfügung gestellt,[282] während weitere Informationen aus den Berichten der Anbieter von Online-Plattformen über ihre Maßnahmen zum Schutz der Integrität von Wahlprozessen auf der Grundlage ihrer Verpflichtungen gemäß dem Verhaltenskodex zur Bekämpfung von Desinformation und der Meldepflichten im Rahmen des DSA stammten. Insbesondere Artikel 34 Absatz 1 Buchstabe c) DSA verlangt von VLOPSE, dass sie systemische Risiken für Wahlprozesse und den zivilgesellschaftlichen Diskurs einschließlich Desinformationsrisiken bewerten und abmildern. Orientierungshilfen für wahlspezifische Risikominderungsmaßnahmen finden sich auch in Leitlinien für Anbieter von VLOPSE zur Minderung systemischer Risiken für Wahlprozesse.[283] Die KDD im Rahmen des DSA wurden ebenfalls aktiv, hauptsächlich in Form von Koordinierung und Einbindung der Interessenträger in ihren nationalen Kontexten, um die Arbeit der Europäischen Kommission zu ergänzen.[284] Im Zusammenhang mit dem Verhaltenskodex zur Bekämpfung von Desinformation haben die Unterzeichner darüber hinaus ein Schnellreaktionssystem (*Rapid Response System* - RRS) eingerichtet, das es Teilnehmern, die keine Plattformen sind, ermöglicht, schnell Informationen beizusteuern, die sie als potenziell schädlich für die Integrität von Wahlprozessen ansehen,

---

[277] Siehe Europäische Kommission, Terms of Reference, European Cooperation Network on Elections

[278] Siehe ebd., S. 13 ff.

[279] Durchführungsbeschluss (EU) 2018/1993 des Rates vom 11. Dezember 2018 über die integrierte EU-Regelung für die politische Reaktion auf Krisen, ABl. L 320/28, 17. Dezember 2022. Diese Regelung bieten einen flexiblen Krisenmechanismus, der die EU-Ratspräsidentschaft bei der Bewältigung größerer sektorübergreifender Naturkatastrophen oder von Menschen verursachter Katastrophen unterstützt.

[280] Rat der EU, „Einmischung aus dem Ausland: Vorsitz verstärkt Informationsaustausch im Vorfeld der Wahlen zum Europäischen Parlament im Juni 2024", Pressemitteilung, 24. April 2024.

[281] Siehe Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Bericht über die Wahlen zum Europäischen Parlament 2024 (engl.), COM(2025) 287 final, 2025, S. 13

[282] Siehe Desinformationsbulletin zur EU-Wahl unter EU Elections Disinfo Bulletin - EDMO

[283] Europäische Kommission, Mitteilung der Kommission - Leitlinien der Kommission für Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen zur Minderung systemischer Risiken in Wahlprozessen gemäß Artikel 35 Absatz 3 der Verordnung (EU) 2022/2065, [2024] ABl. C 2024/3014.. Zu den Wahlleitlinien siehe auch EGDD, *Report on the European Elections, Digital Services Act and Code of Practice on Disinformation*, Amt für Veröffentlichungen der Europäischen Union, Luxemburg, 2024, S. 11.

[284] EGDD, *Report on the European Elections, Digital Services Act and Code of Practice on Disinformation*, S. 13 ff.

und das so dazu beiträgt, ein vollständiges Bild von Desinformationskampagnen zu erhalten.[285]

Zusammenfassend lässt sich sagen, dass die Selbstregulierungsverpflichtungen und die Verpflichtungen für Anbieter von VLOPSE, die Zusammenarbeit im Rahmen spezifischer Kooperationsstrukturen, der leichtere Informationsaustausch und die verstärkte Informationsbeschaffung, ergänzt durch mehrere Planübungen, nach Ansicht der EU-Institutionen zu einer erhöhten Bereitschaft geführt und die Erkennung von Risiken erleichtert haben.[286] Diese Maßnahmen werden nun zunehmend durch verbindliche Rechtsvorschriften ergänzt, die sich speziell gegen Desinformation richten. Eine solche Rechtsvorschrift ist die neue Verordnung über die Transparenz und das Targeting politischer Werbung (TTPW-VO),[287] die gemeinsame EU-Standards für bestimmte problematische Vorgehensweisen einschließlich Finanzierung von außerhalb der EU bei der Verbreitung politischer Werbung in der EU vorsieht. Darüber hinaus soll die beschleunigte regulatorische Zusammenarbeit im Rahmen des Europäischen Medienfreiheitsgesetzes (Europäischer Rechtsakt zur Medienfreiheit – EMFA) eine schnelle Reaktion auf ausländische Desinformationen durch „unseriöse Mediendienste“ erleichtern, welche die öffentliche Sicherheit eines Mitgliedstaates bedrohen.[288] Es bleibt abzuwarten, inwieweit die Mitgliedstaaten lieber die Option des EMFA wählen, außereuropäische Mediendienste innerhalb der EU durch nationale Maßnahmen der Medienbehörden unter der Koordination des neu eingeführten Europäischen Gremiums für Mediendienste (EGMD) zu blockieren oder durch vom Rat der EU verhängte Sanktionen.

[285] Die beteiligten Akteure haben verschiedene Versuche, Wähler durch Desinformation in die Irre zu führen, zum Beispiel durch falsche Informationen über die Wahlmodalitäten und falsche Informationen über die europäische Politik, entdeckt und offengelegt. Siehe Europäische Kommission, “European Elections: EU Institutions Prepared to Counter Disinformation”, Pressemitteilung, 5. Juni 2024.

[286] Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Bericht über die Wahlen zum Europäischen Parlament 2024 (engl.), COM(2025) 287 final, 6. Juni 2025, S. 15; EGDD, *Report on the European Elections, Digital Services Act and Code of Practice on Disinformation*, 2024, S. 18 ff.

[287] Verordnung (EU) 2024/900 des Europäischen Parlaments und des Rates über die Transparenz und das Targeting politischer Werbung, ABl. L 2024/900, 20. März 2024.

[288] Art. 13 lit. l) und 17 EMFA. Für einen Überblick darüber, wie der EMFA und die TTPW-VO die Strategie der EU gegen „Desinformation“ ergänzen, siehe Eskens, S., "The Role of Regulation on the Transparency and Targeting of Political Advertising and European Media Freedom Act in the EU's Anti-Disinformation Strategy", *Computer Law & Security Review*, 58 - 106185, 2025.

3.2 Das Beispiel Rumänien

Dr *Roxana Radu, Außerordentliche Professorin für digitale Technologien und Public Policy, Blavatnik School of Government, Universität Oxford*

3.2.1 Nationaler Rechtsrahmen für Plattformen

Der Einfluss von Online-Plattformen auf das tägliche Leben der Rumäninnen und Rumänen ist erheblich. Die Abhängigkeit von Facebook, WhatsApp, YouTube und TikTok als primäre Informationsquellen (auch für Nachrichten) ist sehr hoch.[289] In einem Land mit einer der niedrigsten Raten digitaler Kompetenz in Europa[290] erreichte die Verbreitung von Fake News und Desinformationen während der COVID-19-Pandemie[291] einen ersten Höhepunkt und beeinflusste weiterhin die öffentliche Meinung, was in der Annullierung der Präsidentschaftswahlen 2024 gipfelte.

Der rumänische Ansatz bei Online-Plattformen harmonisiert die nationalen Rechtsvorschriften mit den Rechtsakten der Europäischen Union zur Schaffung eines kohärenten digitalen Binnenmarktes. Online-Plattformen müssen sich an nationale Vorschriften wie das *Lege nr. 365/2002 privind comerțul electronic* (Gesetz über den elektronischen Geschäftsverkehr) halten, das grundlegende Regeln für Online-Transaktionen festlegt, sowie an EU-weite Verordnungen wie die DSGVO[292] oder der DSA, die darauf abzielen, die Grundrechte der Nutzer zu schützen, indem sie den Plattformen Verpflichtungen in Bezug auf Transparenz, Rechenschaftspflicht und Compliance auferlegen.

Wie in Kapitel 2 dieser Publikation beschrieben, sieht der DSA Verpflichtungen für Vermittler vor. Für VLOPSE ist die Europäische Kommission die zuständige Behörde, die eng mit den auf nationaler Ebene benannten Koordinatoren für digitale Dienste zusammenarbeitet. In Rumänien fällt diese Rolle der Nationalen Verwaltungs- und Regulierungsbehörde im Bereich Kommunikation (ANCOM) zu.

Die andere zuständige Behörde ist der Nationale Audiovisuelle Rat (CNA), dem es laut der Bewertung der Europäischen Kommission von 2025 weiterhin „an ausreichenden personellen und technologischen Ressourcen fehlt, um sein Mandat zu erfüllen, insbesondere im Hinblick auf die Umsetzung des Gesetzes über digitale Dienste“.[293] Das Mandat des CNA wurde durch die Umsetzung der EU-Richtlinie über audiovisuelle

[289] Reuters Institute for the Study of Journalism, *Digital News Report 2025 – Romania*, 2025.
[290] TRIO Project, *Romania National Report Summary*, März 2023; Issue Monitoring, *Romania's Digital Environment: Navigating the Path to a Tech-Driven Future*, 23. August 2024.
[291] EU DisinfoLab, *Disinformation Landscape in Romania*, September 2023.
[292] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, ABl. L 119, 4. Mai 2016).
[293] Europäische Kommission – Resource Centre on Media Freedom, 2025 Rule of Law Report – Country Chapter: Romania, Juli 2025.

Mediendienste (AVMD-RL)[294] in nationales Recht und die damit verbundenen Änderungen des *Lege nr. 504/2002 Legea audiovizualului* (Audiovisuelles Gesetz Nr. 504/2022) und der *Ordonata Guvernului nr. 39/2005 privind cinematografia* (Verordnung über Kinematographie Nr. 39/2005) erweitert. Diese Änderungen verpflichten Streaming-Plattformen (Video-on-Demand-Anbieter), nach definierten Vorgaben einen Teil ihrer lokalen Einnahmen entweder in Form von Abgaben oder durch Investitionen in die nationale Filmindustrie beizusteuern.[295]

Abgesehen von der Angleichung der Rechtsvorschriften an EU-Recht gab es nur sehr wenige Initiativen, die sich auf die Sensibilisierung der Öffentlichkeit und hochwertige Online-Inhalte konzentrierten. Programme zur Förderung der digitalen Kompetenz, unabhängige Faktenprüfung und Finanzierung von öffentlicher Forschung und Lokaljournalismus waren keine vorrangigen Aufgaben in Rumänien. Die gesellschaftliche Resilienz gegenüber Desinformation ist in Rumänien nach wie vor unterentwickelt, und es gab keine ernsthaften Bemühungen, um sowohl das Angebot an Desinformationen als auch die Nachfrage einzudämmen.[296]

3.2.2 Spezifische Vorschriften zu Desinformation

Der Anstieg an Online-Desinformationen wurde besonders während der COVID-19-Pandemie offenkundig, als der Präsidialerlass, mit dem der Ausnahmezustand ausgerufen wurde, die Regierung ermächtigte, alle für notwendig erachteten Maßnahmen zu ergreifen, um die Verbreitung von Falschinformationen einzudämmen – einschließlich der Befugnis, Quellen von Fake News über die ANCOM (die nationale Behörde für Kommunikationsmanagement und -regulierung) zu schließen.[297] Die Anfälligkeit der rumänischen Bevölkerung für die COVID-19-„Infodemie“[298] gehörte zu den höchsten in Europa, wie der weit verbreitete Glaube an Verschwörungstheorien und niedrige Impfraten belegten.[299] Vor diesem Hintergrund verabschiedete der rumänische Senat Beschluss Nr. 24 zur Mitteilung der Europäischen Kommission zur Bekämpfung von Desinformation im

[294] Richtlinie (EU) 2018/1808 des Europäischen Parlaments und des Rates vom 14. November 2018 zur Änderung der Richtlinie 2010/13/EU zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste (Richtlinie über audiovisuelle Mediendienste), ABl. L 303, 28. November 2018.

[295] Cristian, D., "Romania Imposes Financial Contributions on Streaming Platforms to Support National Film Fund", *Business Review*, 17. Oktober 2022.

[296] Cercelescu, M., *Dezinformarea în epoca post-adevăr. Avem, în România, legislație sau alte măsuri pentru combaterea dezinformării?*, JURIDICE.ro, 1. März 2019; Munteanu, D., *Barometrul rezilienței societale la dezinformare*, Centrul Euro-Atlantic pentru Reziliență (E-ARC), Bukarest, 2022.

[297] *Decree on the Establishment of the State of Emergency in the Territory of Romania*, Staatsanzeiger Rumäniens, Teil I, Nr. 212/16, März 2020.

[298] Radu, R., “Fighting the ‘Infodemic’: Legal Responses to COVID-19 Disinformation”, *Social Media + Society*, 6(3), 2020.

[299] Mosila, A., “The Challenge of Populism and Disinformation on the Pandemic Response in Romania”, *EuropeNow Journal*, 20. November 2023.; Cucu, C., “Disinformation Landscape in Romania”, EU DisinfoLab, September 2023.

Zusammenhang mit COVID-19 – Fakten statt Fiktion.[300/301] Ihre Empfehlungen haben jedoch nicht zu konkreten Maßnahmen geführt, um die Resilienz gegenüber Desinformation zu erhöhen. Ein Bericht des *Euro-Atlantic Resilience Centre* von 2022 stellte fest, dass die rechtlichen und institutionellen Instrumente Rumäniens „unzureichend für die derzeitige Phase der technologischen Entwicklung geeignet [waren …]. Rechtsvorschriften und zuständige Institutionen erfassten nicht das gesamte Spektrum der Bedrohungen und ermöglichten keine rasche und effiziente Gegenmaßnahme."[302]

Im nationalen Kontext umfasst die Bekämpfung von Desinformation 1) umfassendere, allgemein geltende rechtliche Schutzmaßnahmen, 2) gezieltere, strategische Bemühungen zur Bewältigung der neuen Herausforderungen und 3) die Umsetzung umfassenderer EU-Initiativen. Auf grundlegender Ebene bieten die bestehenden Bestimmungen im Strafgesetzbuch und die verfassungsrechtlichen Garantien ein breites Spektrum an Schutz gegen die Verbreitung falscher oder irreführender Informationen. Artikel 404 des (aktualisierten) Strafgesetzbuchs stellt die wissentliche Verbreitung falscher Informationen, die die nationale Sicherheit gefährden, unter Strafe und sieht ein bis fünf Jahre Gefängnis hierfür vor.[303] In der Praxis ist es jedoch schwierig, diese Bestimmung auf hochkomplexe Formen von Desinformation anzuwenden. Erstens handelt es sich bei Desinformation nicht immer um fabrizierte Inhalte – sie kann auf echten Inhalten, die manipuliert oder aus dem Zusammenhang gerissen wurden, betrügerischen Inhalten oder falschen Zusammenhängen beruhen.[304] Zweitens sind Menschen selbst oft anfällig für solche Inhalte und teilen sie gegebenenfalls weiter, ohne sich der möglichen Auswirkungen auf die nationale Sicherheit bewusst zu sein.[305] Etwa ein Viertel der rumänischen Nutzer von Online-Plattformen gibt an, Nachrichten über soziale Medien, Messenger-Dienste oder E-Mail zu teilen.[306]

Die rumänische Verfassung enthält Bestimmungen zur freien Meinungsäußerung und zum Recht auf Information, die Verleger, Produzenten, Autoren oder Rundfunkveranstalter für veröffentlichte Inhalte haftbar machen und Massenmedien verpflichten, die Öffentlichkeit korrekt zu informieren. Moderne Desinformation stellt diesen Rahmen jedoch in Frage: Schaden ist häufig diffus und betrifft eher die breite Öffentlichkeit als identifizierbare Einzelpersonen, verbreitet über undurchsichtige

---

[300] Europäische Kommission und Hoher Vertreter der Union für die Außen- und Sicherheitspolitik, Gemeinsame Mitteilung an das Europäische Parlament, den Europäischen Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Bekämpfung von Desinformation im Zusammenhang mit COVID-19 – Fakten statt Fiktion (2020).

[301] Rumänischer Senat**,** *Hotărâre nr. 24 din 8 martie 2021referitoare la Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor - Combaterea dezinformării în legătură cu COVID-19 - Asigurarea unei informări corecte - JOIN(2020) 8 final* (Beschluss Nr. 24 vom 8. März 2021 betreffend die Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Bekämpfung von Desinformation im Zusammenhang mit COVID-19 – Fakten statt Fiktion), 25. März 2021.

[302] Munteanu, D., *Barometrul rezilienței societale la dezinformare*,Centrul Euro-Atlantic pentru Reziliență (E-ARC), Bukarest, 2022.

[303] *Codul Penal din 17 Iulie 2009* (Strafgesetzbuch, Gesetz Nr. 286/2009), aktualisiert am 5. Februar 2017.

[304] Büro des Hohen Kommissars der Vereinten Nationen für Menschenrechte (OHCHR)**,** Bericht über Desinformation (engl.), A/HRC/47/25, 2021.

[305] Munteanu, D., *Barometrul rezilienței societale la dezinformare*, Centrul Euro-Atlantic pentru Reziliență (E-ARC), Bukarest, 2022.

[306] Reuters Institute for the Study of Journalism, *Digital News Report 2025 – Romania*, 2025.

Netzwerke, die ständig ihre Form ändern. In Anbetracht der Dimensionen des Problems hat Rumänien einen Anti-Desinformationsplan in seine Nationale Verteidigungsstrategie für 2020-2024 aufgenommen. Der Zeitplan für seine Umsetzung (seit 2021) ist jedoch nach wie vor Verschlusssache.[307] Im Rahmen der gezielten Bemühungen hat sich das Verteidigungsministerium öffentlich zur Bekämpfung von Desinformation über die Plattform InfoRadar geäußert, die Falschinformationen und Desinformationskampagnen zu Themen, die für die Armee von Interesse sind, überwacht und Bürgerinnen und Bürgern die Möglichkeit bietet, entsprechende Fälle über ein Kontaktformular zu melden. Das Ministerium für Digitalisierung hat außerdem eine Kontaktstelle für die Meldung wahlbezogener Deepfakes eingerichtet, da der Gesetzentwurf, der vorsieht, dass Deepfake-Inhalte mit Warnhinweisen versehen werden müssen, noch nicht endgültig verabschiedet wurde.[308]

Rumänien beteiligt sich darüber hinaus an dem erweiterten EU-Rahmen, der sich mit Desinformation und demokratischen Prozessen befasst. Nach der *Ordonanţă de Urgenţă nr. 6/2019* (Dringlichkeitsverordnung Nr. 6/2019) wurde die Ständige Wahlbehörde (AEP) als zentrale Kontaktstelle für alle Cybersicherheitsvorfälle und Desinformationskampagnen im Zusammenhang mit den Wahlen zum Europäischen Parlament benannt. 2024 veröffentlichte die AEP einen Leitfaden zur Verhinderung und Bekämpfung von Desinformation unter den Wählerinnen und Wählern. Darin wird erklärt, wie Desinformation funktioniert, es werden Instrumente zur Identifizierung und Analyse falscher Inhalte bereitgestellt und Empfehlungen für Journalisten, Content-Creator und Wahlbewerber gegeben.[309] Trotz dieser Bemühungen hielt sich die Durchsetzung der Vorschriften in Grenzen, bis der CNA und die ANCOM die Europäische Kommission offiziell auf erhebliche Unregelmäßigkeiten bei TikToks Handhabung politischer Inhalte während der Präsidentschaftswahlen im November 2024 aufmerksam machten.[310] Dies hatte die Einleitung einer offiziellen Untersuchung durch die Europäische Kommission im Rahmen des DSA am 17. Dezember 2024 zur Folge.[311]

3.2.3 Annullierung der Präsidentschaftswahlen in Rumänien 2024

Der Online-Raum wurde zum Schlachtfeld für die Integrität von Wahlen, lange bevor die Wählerinnen und Wähler am 24. November 2024 für die Präsidentschaftswahlen an die

---

[307] Stanoiu, I., "*Serviciile de informații, Administrația Prezidențială și guvernul au scris și țin la secret planul național anti-dezinformare, care a eșuat*,", *Context.ro*, 5. Februar 2025.

[308] *Legislativvorschlag L295/2023, Propunere legislativă privind interzicerea utilizării malițioase a tehnologiei și limitarea fenomenului Deepfake* (Vorschlag zum Verbot der böswilligen Nutzung von Technologie und zur Begrenzung des Deepfake-Phänomens).

[309] Ständige Wahlbehörde (AEP), *Ghid de prevenire și combatere a acțiunilor de dezinformare a alegătorilor*, März 2024.

[310] Digital Policy Alert, "Romania: Announced NAC and ANCOM Referral to the European Commission for an Investigation into TikTok for Alleged Failure to Address Disinformation and Electoral Manipulation Amplification under DSA", *Digital Policy Alert*, 26. November 2024.

[311] Europäische Kommission, „Kommission leitet förmliches Verfahren nach dem Gesetz über digitale Dienste gegen TikTok wegen Risiken im Zusammenhang mit Wahlen ein", Pressemitteilung, 17. Dezember 2024.

Urnen gingen. Desinformation spielte eine Schlüsselrolle bei der Beeinträchtigung des Wahlprozesses, gestützt auf tieferliegende strukturelle Schwachstellen wie politische Instabilität, wirtschaftliche Unsicherheit und gesellschaftliche Polarisierung. Bereits lange vorhandene sozioökonomische und politische Bruchlinien traten im Online-Diskurs deutlich zutage.[312] Bei den Präsidentschaftswahlen erreichte Călin Georgescu, ein Kandidat mit einer pro-russischen Agenda, im ersten Wahlgang unerwartet den ersten Platz, obwohl er in den Umfragen vor der Wahl nur 6 % Unterstützung hatte. Begünstigt wurde dieser plötzliche Anstieg durch eine undurchsichtige Wahlkampffinanzierung,[313] den Einsatz digitaler Influencer und das Empfehlungssystem von TikTok,[314] einer Plattform mit 9 Millionen rumänischen Nutzern. Als Reaktion auf glaubwürdige Berichte über ausländische Einmischung und Unregelmäßigkeiten bei den Wahlen[315] kam das Verfassungsgericht zu dem Schluss, dass die Integrität des gesamten Wahlprozesses beeinträchtigt worden war. Sie erklärte schließlich die Ergebnisse für ungültig und ordnete eine Wiederholung der Wahlen an.[316] Georgescu wurde in der Folge von einer erneuten Kandidatur ausgeschlossen.[317]

Die Annullierung der Wahl zeigte, dass alle nationalen Maßnahmen zum Schutz der Wahlprozesse in der Praxis versagt hatten. Auf europäischer Ebene wurden die in den Leitlinien der Kommission 2024 festgelegten Standards zur Minderung systemischer Risiken für Wahlprozesse[318] nicht eingehalten. Große Plattformen trafen unzureichende Maßnahmen, um Bedrohungen in Echtzeit zu begegnen, was Fragen nach ihrer Verantwortlichkeit aufwarf. In Rumänien setzte TikTok sein eigenes Verbot politischer Werbung[319] nicht durch und ließ zu, dass Konten und wahlbezogene Inhalte aggressiv beworben wurden. Trotz wiederholter Benachrichtigungen von nationalen Behörden über Unregelmäßigkeiten bei den Wahlen[320] blieb die Plattform untätig.

Der Fall der Annullierung der rumänischen Wahl zeigt auch den evolutionären Charakter von Desinformation, mit fließenden Übergängen zwischen Influencern, Monetisierungstools und algorithmischer Unterstützung von Wahlinhalten.[321] Angesichts der geringen digitalen Kompetenz, der politischen und wirtschaftlichen Instabilität und der weit verbreiteten Unzufriedenheit der Wählerinnen und Wähler war das Land nicht darauf vorbereitet, Desinformationen adäquat entgegenzutreten. Die Trägheit des Gesetzgebers und die begrenzten institutionellen Kapazitäten verschärften das Problem noch weiter und

---

[312] Radu, R., "TikTok, Telegram, and Trust: Urgent Lessons from Romania's Election", *TechPolicy Press*, 25. Juni 2025.
[313] Rumänische Präsidialverwaltung, Dokument CSAT SRI I, 4. Dezember 2024.
[314] EDMO (Europäische Beobachtungsstelle für digitale Medien), Analysis of the 2024 Romanian Presidential Elections:The Role of Social Media and Emerging Political Trends, 26. November 2024.
[315] Rumänische Präsidialverwaltung, Dokument CSAT SRI I, 4. Dezember 2024.
[316] Rumänisches Verfassungsgericht, Presseerklärung (rum.), 6. Dezember 2024.
[317] Rainsford, S. und Gozzi, L., "Final ruling bars far-right Georgescu from Romanian vote", *BBC News*, 11. März 2025.
[318] Mitteilung der Kommission - Leitlinien der Kommission für Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen zur Minderung systemischer Risiken in Wahlprozessen gemäß Artikel 35 Absatz 3 der Verordnung (EU) 2022/2065 (C/2024/3014), 26. April 2024.
[319] TikTok, TikTok-Werberichtlinien - Politik, Regierungsbehörden und Wahlen, zuletzt aktualisiert im Juli 2025.
[320] DIGI24, "*ANCOM: TikTok nu a acționat la solicitarea AEP ce semnala diverse nereguli legate de conținutul ilegal distribuit*" *Digi24*, 26 November 2024.
[321] Ings, R, "The TikTokers accused of triggering an election scandal", *BBC News*, 30. April 2025.

schufen Bedingungen, die eine unkontrollierte Verbreitung irreführender Informationen ermöglichten. Die oben erwähnte Untersuchung der Richtlinien von TikTok in Bezug auf politische Werbung, bezahlte politische Inhalte und die Rolle seiner Empfehlungssysteme bei der Amplifizierung solchen Materials, die von der Europäischen Kommission im Dezember 2024 eingeleitet wurde, ist noch nicht abgeschlossen.[322] Die Beweisaufnahme geht nur langsam voran, was zum Teil daran liegt, dass der DSA keine Fristen für den Abschluss förmlicher Verfahren setzt. Nur die Europäische Kommission kann die Einhaltung der Vorschriften durch VLOP beurteilen und stützt sich dabei auf die Zusammenarbeit mit der irischen Medienregulierungsbehörde *Coimisiún na Meán*, da TikTok seinen EU-Hauptsitz in Irland hat.

Auf nationaler Ebene gab es zwei gesetzgeberische Reaktionen. Am 16. Januar 2025 erließ die rumänische Regierung die Dringlichkeitsverordnung Nr. 1/2025,[323] mit der die Vorschriften für politische Werbung ohne Konsultation der Interessenträger geändert wurden.[324] Die Verordnung schreibt vor, dass alle Wahlinhalte, auch von Privatpersonen, ordnungsgemäß zu kennzeichnen sind. Im März 2025 wurde ein Gesetzentwurf zur Eindämmung von Desinformation und schädlichen Inhalten im Internet vorgelegt und im Juni 2025 vom rumänischen Senat verabschiedet.[325] Der Gesetzentwurf sieht strengere Regeln für VLOP vor als der DSA. In seiner jetzigen Form – die in den kommenden Monaten von der Abgeordnetenkammer beraten werden soll – verpflichtet er Plattformen, die Verbreitung potenziell schädlicher Inhalte auf höchstens 150 Nutzer zu beschränken, Werbung dafür zu verbieten und rechtswidrige Inhalte innerhalb von 15 Minuten nach ihrer Veröffentlichung zu entfernen, wenn sie von automatisierten Systemen als rechtswidrig eingestuft wurden. Er verbietet zudem bezahlte Werbung für Inhalte, die zu Hass, Gewalt oder Desinformation zu Themen von nationalem Interesse aufrufen. Wird nicht wirksam gehandelt – gemessen an einem Schwellenwert von 30 % der validierten Nutzermeldungen –, verhängt die ANCOM Geldbußen in Höhe von 1 % des Umsatzes. Mit dem Gesetz soll zwar der Schutz der Öffentlichkeit gestärkt werden, Experten warnen jedoch, dass die weit gefasste Definition schädlicher Inhalte, der starke Einsatz künstlicher Intelligenz (KI) und die beschleunigten Fristen Anlass zu Bedenken hinsichtlich der Durchführbarkeit und der Risiken für die Meinungsfreiheit geben.[326] Das Gesetz stellt eine erhebliche Ausweitung über die durch den DSA auferlegten Verpflichtungen hinaus dar und kann im Fall der Annahme einen Präzedenzfall schaffen.

---

[322] Europäische Kommission, „Kommission leitet förmliches Verfahren nach dem Gesetz über digitale Dienste gegen TikTok wegen Risiken im Zusammenhang mit Wahlen ein“, Pressemitteilung, 17. Dezember 2024.
[323] Emergency Ordinance No. 1/2025 on certain measures for the organisation and conduct of the 2025 elections for the President of Romania and the 2025 local by-elections, 17. Januar 2025.
[324] Funky Citizens, “Romania’s Elections Overview, 22 April 2025”, *Europäische Beobachtungsstelle für digitale Medien*, 22. April 2025.
[325] Mocanu, R., "*A fost adoptata de Senat legal impotrivata manipularii online propusa de USR*", *MediaFax*, 16. Juni 2025.
[326] CMS LawNow, “Romania proposes stricter rules against harmful content on social media”, *CMS LawNow*, 10. März 2025.

3.3 Das Beispiel Frankreich

Dr William Gilles, außerordentlicher Professor, Universität Paris 1 Panthéon Sorbonne, und Dr Irène Bouhadana, außerordentliche Professorin, Universität Paris 1 Panthéon Sorbonne

3.3.1 Nationaler Rechtsrahmen für Plattformen

Das nationale Recht in Frankreich zur Regelung von Plattformen wird in erster Linie durch die Verfassungsrechtsprechung bestimmt, welche die Verfahren definiert, nach denen der französische Gesetzgeber Maßnahmen in Bezug auf solche Plattformen ergreifen kann. So entschied der Verfassungsrat in seinem Beschluss zum Gesetz zur Förderung der Verbreitung und des Schutzes kreativer Werke im Internet (bekannt als Hadopi 1),[327] dass die Kommunikations- und Meinungsfreiheit, wie sie in Artikel 11 der Erklärung der Menschen- und Bürgerrechte vom 26. August 1789[328] vorgesehen ist, „die Freiheit des Zugangs" zu „öffentlichen Online-Kommunikationsdiensten" und damit zum Internet beinhaltet.[329]

In seinem Beschluss von 2020 zum Gesetz zur Bekämpfung von Hassinhalten im Internet (bekannt als Avia-Gesetz)[330] bekräftigte der Verfassungsrat diese Rechtsprechung und stellte fest, dass die Kommunikations- und Meinungsfreiheit auch die Freiheit einschließt, sich selbst zu äußern.[331] Er entschied daher:

> *In Anbetracht des derzeitigen Stands der Kommunikationstechnologie und der allgemeinen Entwicklung öffentlicher Online-Kommunikationsdienste sowie der Bedeutung dieser Dienste für die Teilnahme am demokratischen Leben und die Äußerung von Ideen und Meinungen beinhaltet dieses Recht die Freiheit, auf diese Dienste zuzugreifen und sich dort zu äußern.*

Er fügte hinzu, dass der französische Gesetzgeber einen Rechtsrahmen erlassen kann, der darauf abzielt, Missbräuchen der Meinungs- und Kommunikationsfreiheit, die die öffentliche Ordnung und die Rechte Dritter beeinträchtigen, ein Ende zu setzen; dafür hat er zum ersten Mal die Verbreitung pornografischer Bilder, auf denen Minderjährige abgebildet sind, und die Aufstachelung zu terroristischen Handlungen oder deren Verherrlichung dieser Kategorie von Missbräuchen zugeordnet.

Mit dem Beschluss des Verfassungsrats von 2020 wurden jedoch mehrere Bestimmungen des Avia-Gesetzes mit der Begründung aufgehoben, dass die Eingriffe in die Meinungs- und Kommunikationsfreiheit im Hinblick auf das verfolgte Ziel nicht angemessen, notwendig oder verhältnismäßig waren. Die für ungültig erklärten

---

[327] *Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet*, *Journal officiel de la République française* (JORF) Nr. 0135 vom 13. Juni 2009 (Hadopi).
[328] *La déclaration des droits de l'homme et du citoyen* – Offizielle deutsche Übersetzung.
[329] *Conseil Constitutionnel*, Beschluss Nr. 2009-580 vom 10. Juni 2009 (engl.).
[330] *Loi n° 2020-766 visant à lutter contre les contenus haineux sur internet*, JORF Nr. 0156 vom 25. Juni 2020 (Avia-Gesetz).
[331] *Conseil Constitutionnel*, Beschluss Nr. 2020-801 DC vom 18. Juni 2020 (franz.).

Bestimmungen hätten es der zuständigen Verwaltungsbehörde ermöglicht, von Hostinganbietern oder Herausgebern eines Online-Kommunikationsdienstes zu verlangen, Inhalte zu entfernen, die Kinderpornografie darstellen oder zu terroristischen Handlungen auffordern oder diese verherrlichen, und, falls solche Inhalte nicht innerhalb von 24 Stunden entfernt werden, die Zugangsanbieter anzuweisen, den Zugang zu solchen Inhalten unverzüglich zu sperren. Der Verfassungsrat vertrat jedoch erstens die Auffassung, die Rechtswidrigkeit eines solchen Inhalts würde somit nicht von seiner eindeutigen Aussage, sondern allein von der Einschätzung der Verwaltung abhängen. Zweitens hätte ein Rechtsbehelf gegen eine Aufforderung zur Entfernung keine aufschiebende Wirkung: Der Herausgeber oder der Hostinganbieter hätte lediglich eine Stunde Zeit, um den Zugang zu den Inhalten zu sperren; dies wäre eine zu kurze Frist, als dass er vor der Entfernung der beanstandeten Inhalte ein Gerichtsurteil erwirken könne, während ihm eine Geldstrafe von EUR 250 000 und eine einjährige Haftstrafe drohe, wenn er die Inhalte nicht innerhalb dieser Frist entferne. Ebenso strich der Verfassungsrat die Bestimmungen des Gesetzes, nach denen Betreiber von Online-Plattformen zur Vermeidung strafrechtlicher Sanktionen verpflichtet waren, binnen 24 Stunden „Inhalte, die aufgrund ihres hasserfüllten oder sexuellen Charakters offenkundig rechtswidrig sind“, zu entfernen und unzugänglich zu machen.

Die übrigen Bestimmungen des Gesetzes, das nach der Überprüfung durch den Verfassungsrat zum oben erwähnten Avia-Gesetz wurde, zielten auf die Bekämpfung von Hassinhalten im Internet ab. Mit diesem Gesetz wurde das Bildungsgesetz (*Code de l'éducation)*[332] geändert, um die Schulung von Schülern und Lehrern im Umgang mit digitalen Werkzeugen und Ressourcen mit dem Ziel zu stärken, die Verbreitung von Hassinhalten im Internet zu verhindern und digitale Bürgerschaft zu fördern. Mit dem Avia-Gesetz wurde auch die Beobachtungsstelle für Hass im Internet[333] geschaffen, die der französischen Regulierungsbehörde für audiovisuelle und digitale Kommunikation (ARCOM)[334] untersteht, einer unabhängigen französischen Behörde, die für die Gewährleistung der Kommunikationsfreiheit verantwortlich ist. Diese Beobachtungsstelle ist seit 2020 tätig und hat die Aufgabe, Hassinhalte im Internet zu überwachen und zu analysieren. Sie umfasst die vier Bereiche Verwaltungen, Forscher, Verbände und Betreiber, wobei zu letzterem Dailymotion, Facebook, Google, LinkedIn, Microsoft, Qwant, Snapchat, TikTok, Twitch, X (früher Twitter), Wikimedia Frankreich und Yubo gehören. Schließlich änderte das Avia-Gesetz das Gesetz über das Vertrauen in die digitale Wirtschaft *(Loi pour la confiance dans l'économie numérique* - LCEN-Gesetz),[335] welches die französische Referenzvorschrift zum Rechtsrahmen für Internet-Akteure darstellt. Dieser Rechtstext wurde durch das Gesetz zur Sicherung und Regulierung des digitalen Raums (*Loi visant à sécuriser et à reguler l'espace numérique* - SREN-Gesetz)[336] geändert, um insbesondere das französische Recht nach der Verabschiedung des DMA und des DSA an EU-Recht anzupassen. Es wurde vor kurzem durch das Gesetz zur Befreiung Frankreichs aus der Falle

[332] *Code de l'éducation*.
[333] Siehe ARCOM, *"Observatoire de la haine en ligne : analyser pour mieux lutter"*.
[334] *Autorité de régulation de la communication audiovisuelle et numérique*.
[335] *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, JORF Nr. 0143 vom 22. Juni 2004.
[336] *Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique*, JORF Nr. 0117 vom 22. Mai 2024.

des Drogenhandels (*Loi visant à sortir la France du piège du narcotrafic*)[337] geändert, um diese Problemstellungen zu berücksichtigen. Gleichzeitig wurde klargestellt, dass der Hauptzweck dieser Rechtsvorschriften nicht in der Regulierung von Plattformen besteht.

In Bezug auf Plattformregulierung wurde per Dekret Nr. 2020-1102 vom 31. August 2020[338] schließlich innerhalb der Generaldirektion für Unternehmen, welche den Ministerien für Wirtschaft, Kultur sowie digitale Angelegenheiten untersteht, mit dem Kompetenzzentrum für die Regulierung digitaler Plattformen (*Pôle d'Expertise de la Régulation Numérique* - PEReN) ein nationaler Dienst eingerichtet, dessen Aufgabe es ist, den für die Regulierung digitaler Plattformen zuständigen staatlichen Stellen und unabhängigen Behörden Fachwissen und technische Unterstützung bereitzustellen. Dekret Nr. 2022-603 vom 21. April 2022,[339] geändert durch Dekret Nr. 2025-385 vom 28. April 2025,[340] legt fest, welche unabhängigen Verwaltungs- und Staatsbehörden berechtigt sind, das PEReN zu befassen: die Wettbewerbsbehörde (ADLC), die Finanzmarktaufsicht (AMF), die Nationale Glücksspielbehörde (ANJ), die Regulierungsbehörde für elektronische Kommunikation, Postdienste und Pressevertrieb (ARCEP), ARCOM, die Verkehrsregulierungsbehörde (ART), die Energieregulierungskommission (CRE), die Nationale Kommission für Informationstechnologie und bürgerliche Freiheiten (CNIL) und der Ombudsmann.

3.3.2 Spezifische Vorschriften zu Desinformation

Das Aufkommen der Datengesellschaft und die Entwicklung von Plattformen haben die Risiken der neuen Technologien in Bezug auf die Verbreitung von Fake News aufgezeigt; Frankreich ist in diesem neuen Kontext keine Ausnahme. Besonders deutlich wurde dies bei den französischen Präsidentschaftswahlen 2017, während derer Versuche ausländischer Einmischung die ordnungsgemäße Durchführung der Wahlen gefährdete. Vor diesem Hintergrund verabschiedete der französische Gesetzgeber mit Gesetz Nr. 2018-1202 zur Bekämpfung von Informationsmanipulation *(Loi n° 2018-1202 relative à la lutte contre la manipulation de l'information*) erstmals eine Rechtsvorschrift über Falschinformationen, die speziell auf die Bekämpfung von Falschinformationen bei Wahlen ausgerichtet war.[341] Dieser Rechtsrahmen wurde später abgeändert, insbesondere durch das SREN-Gesetz, das den DSA mit direkter Anwendung in französisches Recht umsetzt und ARCOM als

[337] *Loi n° 2025-532 du 13 juin 2025 visant à sortier la France du piège du narcotrafic*, JORF Nr. 0137 vom 14. Juni 2025.
[338] *Décret n° 2020-1102 du 31 août 2020 portant création d'un service à compétence dénominé "Pôle d'expertise de la régulation numérique*", JORF Nr. 0214 vom 2. September 2020.
[339] *Décret n° 2022-603 du 21 avril 2022 fixant la liste des autorités administratives et publiques indépendantes pouvant recourir à l'appui du pôle d'expertise de la régulation numérique et relatif aux méthodes de collecte de données mises en œuvre par ce service dans le cadre de ses activités d'expérimentation*, JORF Nr. 0095 vom 23. April 2022.
[340] *Décret n° 2025-385 du 28 avril 2025 complétant le décret n° 2022-603 du 21 avril 2022 fixant la liste des autorités administratives et publiques indépendantes pouvant recourir à l'appui du pôle d'expertise de la régulation numérique et relatif aux méthodes de collecte de données mises en œuvre par ce service dans le cadre de ses activités d'expérimentation*, JORF Nr. 0102 vom 30. April 2025.
[341] *Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information*, JORF Nr. 0297 vom 23. Dezember 2018.

Koordinator für digitale Dienste benennt. Der derzeit geltende Rechtsrahmen zur Eindämmung der Verbreitung von Falschinformationen stellt sich somit wie folgt dar.

Erstens wurde das französische Wahlgesetz[342] geändert, um eine größere Integrität der französischen Wahlen zu gewährleisten und das Risiko ausländischer Einmischung in diesem Bereich zu begrenzen. In seiner neuesten Fassung verpflichtet Artikel L163-1 des Wahlgesetzes sehr große Online-Plattformen und -Suchmaschinen, wie sie im DSA definiert sind, zu Transparenz, wenn sie Informationen über Debatten von allgemeinem Interesse verbreiten. So müssen sie in den drei Monaten vor den Wahlen und bis zum Wahlausgang in dem in Artikel 39 des DSA vorgesehenen Umfang faire, klare und transparente Angaben nicht nur über die Sponsoren der Förderung von Inhalten im Zusammenhang mit diesen Debatten von allgemeinem Interesse, sondern auch über die Art und Weise der Verwendung personenbezogener Daten in diesem Kontext machen. In diesem Rahmen müssen sie im Falle einer Vergütung zudem Beträge von über EUR 100 (ohne Steuern) ausweisen, die sie pro Informationsinhalt, der im Rahmen der Debatte von allgemeinem Interesse verbreitet wird, erhalten haben. Diese Bestimmungen sind Teil der Verpflichtung von Online-Plattformen, bei der Bekämpfung der Verbreitung von Falschinformationen mitzuarbeiten. Sie ergänzen die allgemeinen Verpflichtungen von Plattformen nach dem DSA, auch außerhalb von Wahlen, wie etwa in Bezug auf die Transparenz ihrer Empfehlungssysteme.

Artikel L163-2 des Wahlgesetzes sieht seinerseits die Möglichkeit vor, dass ein Kandidat, die Staatsanwaltschaft, eine Partei oder jede klageinteressierte Person während desselben Wahlzeitraums in einem Schnellverfahren einen Richter anrufen kann, wenn vorsätzlich, künstlich oder automatisiert und massenhaft Informationen online verbreitet werden, die unrichtige oder irreführende Tatsachen behaupten oder unterstellen, die geeignet sind, die Integrität der Wahlen zu beeinträchtigen. Der Richter hat dann 48 Stunden Zeit, eine Entscheidung zu treffen, ebenso ein Berufungsrichter. Damit soll eine schnelle Reaktion auf die Verbreitung falscher Informationen, die das Wahlergebnis beeinflussen könnten, gewährleistet werden.

Generell wollte der Gesetzgeber eine erzieherische Komponente in den Kampf gegen Desinformation einbringen und änderte zu diesem Zweck das Bildungsgesetz,[343] um Grundschüler (Artikel L312-5) und Schüler der Mittelstufe (Artikel L332-5) sowie Lehrer, die für die Vermittlung entsprechenden Unterrichts zuständig sind (Artikel L721-2) in der kritischen Analyse und Verifizierung der Zuverlässigkeit der in den Medien verbreiteten Informationen zu schulen. Hörfunk- und audiovisuelle Medien sowie VSP-Anbieter sind verpflichtet, durch entsprechende Maßnahmen zur Erreichung dieses Bildungsziels beizutragen (Artikel 28, 43-11 und 60 des Gesetzes Nr. 86-1067 vom 30. September 1986 über die Kommunikationsfreiheit (*Loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication*), bekannt als Léotard-Gesetz).[344]

Darüber hinaus erteilt das Léotard-Gesetz der ARCOM Befugnisse zur Bekämpfung der Verbreitung von Falschinformationen. In Artikel 17-2 dieses Gesetzes wird ihre Rolle in diesem Bereich bekräftigt, wenn eine solche Verbreitung die öffentliche Ordnung stören oder die Integrität von Wahlen beeinträchtigen kann.

---

[342] *Code électoral*.
[343] *Code de l'éducation*.
[344] *Loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication*, JORF vom 1. Oktober 1986.

Das Léotard-Gesetz ermöglicht es der ARCOM auch, gegen audiovisuelle Kommunikationsdienste vorzugehen, die eine Vereinbarung mit ihr unterzeichnet haben und die von einem ausländischen Staat kontrolliert oder beeinflusst werden und die absichtlich Falschinformationen verbreiten. Wenn diese Informationen geeignet sind, die Integrität der Wahlen in den drei vorausgehenden Monaten bis zum Wahltag zu beeinträchtigen (Artikel 33-1-1), kann die ARCOM entsprechende Ausstrahlungen als Präventivmaßnahme oder zur Beendigung der daraus resultierenden Störung aussetzen oder einstellen. Wenn Falschinformationen geeignet sind, die grundlegenden Interessen der Nation zu schädigen und beispielsweise das ordnungsgemäße Funktionieren der Institutionen zu behindern, kann die ARCOM diese Vereinbarung nach förmlicher Ankündigung einseitig kündigen (Artikel 42-6). Stellt sie einen Verstoß gegen die im Léotard-Gesetz vorgesehenen Verpflichtungen fest, zu denen auch die oben genannten Beispiele gehören, kann der Präsident der ARCOM auch den Staatsrat mit einem Eilverfahren befassen, um eine Anordnung zur sofortigen Durchsetzung von Maßnahmen zur Einhaltung der Vorschriften, zur Beendigung der Unregelmäßigkeit oder zur Beseitigung ihrer Auswirkungen zu erwirken (Artikel 42-10). Generell kann die ARCOM eine Angelegenheit der Staatsanwaltschaft übergeben, wenn sie einen Verstoß gegen das Léotard-Gesetz feststellt.

Gemäß Artikel 58 des Léotard-Gesetzes ist die ARCOM darüber hinaus dafür verantwortlich, dass die Betreiber von Online-Plattformen ihren Verpflichtungen aus dem LCEN-Gesetz nachkommen. Zur Bekämpfung von Informationsmanipulation, die die öffentliche Ordnung stören oder die Integrität von Wahlen beeinträchtigen könnte, richtet die ARCOM Empfehlungen zu diesem Thema an die Anbieter großer Online-Plattformen, die großen Suchmaschinen und die Anbieter großer VSP-Dienste und veröffentlicht regelmäßig einen Bericht über die von ihnen getroffenen Maßnahmen. Schließlich liegt es in der Verantwortung der ARCOM, dass Online-Plattformen die Vorschriften zur Bekämpfung von Hassinhalten einhalten (Artikel 62).

Außerhalb dieses Kontextes hat der französische Gesetzgeber keine spezifischen rechtlichen Regelungen für andere Fälle der Verbreitung von Falschinformationen erlassen. In Bezug auf die Verbreitung von Informationen im Internet ist zu beachten, dass der französische Gesetzgeber den Grundsatz der Freiheit der elektronischen öffentlichen Wiedergabe bekräftigt hat, wobei etwaige Einschränkungen unter die im Léotard-Gesetz vorgesehenen Ausnahmen fallen. Neben den genannten Einschränkungen ist es jedoch möglich, unter Berufung auf mehrere in Artikel 1 des Léotard-Gesetzes vorgesehene Szenarien und insbesondere auf die Notwendigkeit, die Menschenwürde, die Freiheit, den Gedanken- und Meinungspluralismus und die öffentliche Ordnung zu wahren oder aber Kinder und Jugendliche zu schützen, wenn diese zur Zielscheibe werden, Rechtsbeschwerde gegen Fehlinformationen einzulegen.

Darüber hinaus können mehrere Bestimmungen des Gesetzes vom 29. Juli 1881 über die Pressefreiheit (*Loi du 29 juillet 1881 sur la liberté de la presse*[345]), wenngleich sie nicht speziell auf Falschinformationen abzielen, dennoch angewandt werden, um deren Folgen zu sanktionieren. In strafrechtlicher Hinsicht könnte Desinformation nach mehreren

[345] *Loi du 29 juillet 1881 sur la liberté de la presse*.

in diesem Gesetz vorgesehenen Tatbeständen geahndet werden. Drei Sachlagen vermitteln in diesem Zusammenhang ein besonders anschauliches Bild.

Zum einen können Falschinformationen zu Straftaten und Vergehen anstiften, die gemäß Artikel 24 und 24*bis* des Gesetzes über die Pressefreiheit mit bis zu fünf Jahren Haft und einer Geldstrafe von EUR 45 000 geahndet werden. Mit anderen Worten läge hier eine Situation vor, in der die Begehung einer Straftat oder eines Vergehens direkt durch Falschinformationen provoziert wurde. So hatte der Kassationsgerichtshof in einem Urteil vom 15. Oktober 2019[346] über stigmatisierende Aussagen zu entscheiden, die sich auf die vermeintliche Herkunft oder Religion von Personen bezogen und die Religionszugehörigkeit mit einer Krankheit gleichsetzten. Diese Falschinformationen, die über Twitter und Facebook verbreitet worden waren, wurden als rassistische Beleidigungen und Aufstachelung zu Diskriminierung, Hass oder Gewalt eingestuft, was die Verurteilung ihres Verfassers nach Artikel 24 und 27 des genannten Gesetzes rechtfertigte, da diese „Kommentare die Öffentlichkeit explizit oder implizit dazu aufforderten, bestimmte Personengruppen aufgrund ihrer Rasse oder Religion zu diskriminieren“, so die Richter.

Zum anderen können Falschinformationen auch als Straftat gegen Personen nach Artikel 29 des Gesetzes über die Pressefreiheit geahndet werden, wenn sie Beleidigungen, das heißt verächtliche oder beschimpfende Äußerungen (Strafen zwischen EUR 12 000 und 75 000) oder eine Verleumdung darstellen. Letzteres erwüchse aus Desinformationen, die darauf abzielen, eine Tatsache zu behaupten oder zu unterstellen, die die Ehre oder das Ansehen einer Person oder der Körperschaft, der sie angehört, schädigt. Dem Täter droht dann eine Geldstrafe, die je nach den Umständen zwischen EUR 12 000 und 45 000 liegen kann. Die schwersten Strafen gelten dabei insbesondere für Verleumdungen von Gerichten, öffentlichen Verwaltungen, Beamten, Bürgern, die eine öffentliche Funktion oder ein öffentliches Amt ausüben, sowie des Präsidenten der Republik oder für Verleumdungen aufgrund der Herkunft, Zugehörigkeit oder Nichtzugehörigkeit dieser Person zu einer bestimmten ethnischen Gruppe, Nation, Rasse oder Religion. In Frankreich wurden beispielsweise vor kurzem Falschinformationen im Internet verbreitet, die viral gingen und in denen behauptet wurde, Brigitte Macron, die Ehefrau des französischen Staatspräsidenten, sei eine Transgender-Frau, die sich zu diesem Zweck mehreren chirurgischen Eingriffen unterzogen habe. Am 12. September 2024 wurden die Verfasserinnen dieser Falschinformationen vom Pariser Gericht zunächst wegen Verleumdung verurteilt, am 10. Juli 2025 jedoch vom Pariser Berufungsgericht freigesprochen, da sie „guten Glaubens“ gehandelt hätten. Das Verfahren ist derzeit noch anhängig, da Rechtsmittel beim Kassationsgerichtshof eingelegt wurden.[347]

Schließlich sieht Artikel 27 des Gesetzes über die Pressefreiheit eine Geldstrafe in Höhe von EUR 45 000 für jede Person vor, die falsche Nachrichten über Dritte veröffentlicht, verbreitet oder vervielfältigt, wobei dieser Betrag auf EUR 135 000 steigen kann, wenn die Disziplin oder die Moral der Streitkräfte sowie Kriegsanstrengungen des Landes betroffen sind. Allerdings handelt es sich hier um einen Sonderfall, da die Veröffentlichung, Verbreitung oder Vervielfältigung bösgläubig erfolgt sein muss und eine Störung der

[346] *Court de Cassation*, *Décision n° 18-85.365* (nicht in den amtlichen Entscheidungssammlungen veröffentlicht).
[347] Le Monde mit AFP, "Brigitte Macron Takes Gender Libel Case to France's Highest Appeals Court", *Le Monde*, 14. Juli 2025.

öffentlichen Ordnung verursacht oder riskiert haben muss, um als solche eingestuft zu werden. Dieses letzte Szenario verdeutlicht die Notwendigkeit, den Unterschied zwischen den Begriffen Falschinformationen und „Fake News" zu klären. Bei der Prüfung des Gesetzentwurfs über die Verbreitung von Falschinformationen – der später als Gesetz Nr. 2018-1202 vom 22. Dezember 2018 zur Bekämpfung von Informationsmanipulation[348] verabschiedet wurde – hielt es der Staatsrat in einem Gutachten vom 4. Mai 2018 für angebracht, die Unterscheidung zwischen den Begriffen Falschinformationen und „Fake News" zu klären, die im französischen Recht bereits durch das Gesetz über die Pressefreiheit sowie im Wahlgesetz bestand.[349] Er weist darauf hin, dass sich nach der Rechtsprechung des Kassationsgerichtshofs „Fake News" auf „eine eindeutige und detaillierte Tatsache bezieht, die noch nicht veröffentlicht wurde und deren Unwahrheit objektiv festgestellt wurde", während Falschinformationen weiter gefasst sind, da dieser Begriff nicht die Bedingung „keine vorherige Veröffentlichung der streitigen Informationen" beinhaltet. Darüber hinaus empfahl der Staatsrat, den Begriff Falschinformationen auf Informationen zu beschränken, die „in der bewussten Absicht, Schaden zu verursachen", verbreitet werden.

3.3.3 Anwendung im Falle von Wahlen

Der geopolitische Kontext der letzten Jahre und die zunehmende ausländische Einmischung haben deutlich gemacht, dass sich der Kampf gegen Falschinformationen nicht allein auf das bereits erwähnte Gesetz Nr. 2018-1202 zur Bekämpfung von Informationsmanipulation stützen kann. Somit sah sich der Gesetzgeber 2024 dazu veranlasst, neue Maßnahmen zu ergreifen, um dieses Ziel durch den Einsatz von Algorithmen zu erreichen. Grundlage war die algorithmische Verarbeitung, die versuchsweise durch das Geheimdienstgesetz[350] zur Aufdeckung terroristischer Bedrohungen eingeführt wurde. Diese in Artikel L851-3 des Gesetzes über die innere Sicherheit[351] eingeführte Maßnahme wurde zweimal verlängert, bevor sie durch das Gesetz über die Verhinderung terroristischer Handlungen und den Geheimdienst[352] festgeschrieben wurde. Mit dem Gesetz zur Verhinderung ausländischer Einmischung in Frankreich[353] soll diese Maßnahme ausgeweitet werden, indem der Einsatz solcher algorithmischer Verarbeitung ermöglicht wird, um auf der Grundlage von Verbindungsdaten und den Adressen der abgerufenen Internetinhalte jegliche tatsächliche oder versuchte ausländische Einmischung zu identifizieren. Im Gegenzug sind Verfahrensgarantien festgelegt, indem eine Genehmigung des Premierministers verlangt wird, die den Grundsatz der Verhältnismäßigkeit wahrt und die genehmigte Verarbeitung genau definiert. Außerdem muss die Regierung dem Parlament einen Bericht über die Umsetzung dieser gesetzlichen Bestimmung vorlegen.

---

[348] Op. cit.
[349] Conseil d'État, *Lutte contre les fausses informations, avis consultatif*, 4. Mai 2018.
[350] *Loi n° 2015-912 du 24 juillet 2015 relative au renseignement*, JORF Nr. 0171 vom 26. Juli 2015.
[351] *Code de la sécurité intérieure*.
[352] *Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement*, JORF Nr. 0176 vom 31. Juli 2021.
[353] *Loi n° 2024-850 du 25 juillet 2024 visant à prévenir les ingérences étrangères en France*, JORF Nr. 0177 vom 26. Juli 2024.

Zusätzlich zu diesem rechtlichen Rahmen ist Frankreich auch auf operativer Ebene aktiv geworden und hat einen Dienst zur Überwachung und zum Schutz vor ausländischer digitaler Einmischung (VIGINUM) eingerichtet. Dieser Dienst mit nationaler Zuständigkeit wurde per Dekret Nr. 2021-922 vom 13. Juli 2021[354] geschaffen und ist dem Generalsekretariat für Verteidigung und nationale Sicherheit (SGDSN) angegliedert. Die Aufgabe von VIGINUM besteht darin, ausländische digitale Einmischung, die öffentlich auf Online-Plattformen verbreitet wird, aufzuspüren und zu kennzeichnen, insbesondere in Wahlkampfzeiten, wenn sie die Art und Weise, wie die Bürger informiert werden, verändern kann. Bei den Informationsbedrohungen, die besonders im Fokus stehen, geht es um Vorgänge, die direkt oder indirekt mit einem ausländischen Staat oder einer ausländischen nichtstaatlichen Organisation in Verbindung stehen und die darin bestehen, absichtlich Falschinformationen in großem Umfang durch künstliche oder automatisierte Prozesse über einen öffentlichen Online-Kommunikationsdienst zu verbreiten. Der Begriff Falschinformationen bezieht sich in diesem Zusammenhang auf die Beschreibung solcher Vorgänge in Artikel R*1132-3 des Verteidigungsgesetzes[355], nämlich auf „Behauptungen oder Unterstellungen von Tatsachen, die offenkundig unrichtig oder irreführend und geeignet sind, den grundlegenden Interessen der Nation zu schaden“. Schließlich unterstützt VIGINUM mehrere französische Institutionen: Unterstützung des SGDSN bei der Koordinierung und Leitung ressortübergreifender Bemühungen zur Bekämpfung von Fake News, Beiträge zu den europäischen und internationalen Bemühungen in diesem Bereich und Bereitstellung von Informationen für die ARCOM und die Nationale Kommission für die Kontrolle von Wahlkampagnen in ihrer jeweiligen Rolle bei der Bekämpfung dieser Bedrohungen.

3.4 Das Beispiel Ukraine

Dr *Dariia Opryschko, NGO Human Rights Platform*

3.4.1 Nationaler Rechtsrahmen für Plattformen

In der Ukraine wurden Fragen im Zusammenhang mit Online-Plattformen und der Veröffentlichung von Inhalten lange Zeit durch allgemeine Bestimmungen in verschiedenen Gesetzesvorschriften geregelt. Die ukrainische Gesetzgebung erlaubte die Sperrung von Inhalten in Fällen, in denen sie sexuellen Missbrauch von Kindern darstellten oder gegen Urheberrechte und verwandte Schutzrechte verstießen.[356]

---

[354] *Décret n° 2021-922 du 13 juillet 2021 portant création, auprès du secrétaire général de la défense et de la sécurité nationale, d'un service à compétence nationale dénominé "service de vigilance et de protection contre les ingérences numériques étrangères"*, JORF Nr. 0162 vom 14. Juli 2021.

[355] *Code de la défense*.

[356] Opryshko, D., "Report on Ukraine" *in* Schweizerisches Institut für Rechtsvergleichung (Hrsg.), *Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content*, Lausanne, 2015; Opryshko, D., *Follow-up to the Comparative Study on "Blocking, Filtering and Take-Down of Illegal Internet Content", Report on Ukraine*, 2019.

Die ersten spezifischen Bestimmungen zur Regulierung von Online-Plattformen in der Ukraine wurden mit dem ukrainischen Mediengesetz (UMG)[357] eingeführt. Das am 13. Dezember 2022 verabschiedete Gesetz trat am 31. März 2023 in Kraft. Das UMG unterscheidet zwischen Video-Sharing-Plattformen (VSP) und Plattformen für gemeinsamen Informationszugang[358] (Online-Plattformen), regelt aber nur erstere und auch nur solche, die unter die Rechtshoheit der Ukraine fallen. Das bedeutet, dass die bei Ukrainerinnen und Ukrainern beliebtesten Online-Plattformen wie Telegram, Facebook, Instagram, YouTube, Netflix, TikTok usw. nicht verpflichtet sind, das UMG einzuhalten.

Laut UMG[359] sind VSP verpflichtet, die Anforderungen zur Transparenz des Medieneigentums einzuhalten,[360] in ihren Nutzungsbedingungen Verbote der Verbreitung von Informationen vorzusehen, die gegen die Anforderungen des UMG (einschließlich während bewaffneter Angriffe und in der Zeit nach Konflikten[361])[362] sowie gegen die Gesetzgebung zum Urheberrecht und zu verwandten Schutzrechten verstoßen, ihre Nutzungsbedingungen zu veröffentlichen und den Nutzer damit vertraut zu machen und in ihren Nutzungsbedingungen ein Verfahren vorzusehen, mit dem das Recht wahrgenommen werden kann, auf fehlerhafte Informationen zu erwidern oder sie anzufechten. Sie sind außerdem verpflichtet sicherzustellen, dass das Alter eines Nutzers verifiziert wird, bevor Zugang zu Informationen gewährt wird, die der körperlichen, geistigen oder sittlichen Entwicklung von Kindern schaden können; darüber hinaus müssen sie die Möglichkeit gewährleisten, ein System der elterlichen Kontrolle zu nutzen, um Kinder vor solchen Informationen zu schützen; sie müssen transparente und verständliche Beschwerdemechanismen umsetzen, insbesondere im Zusammenhang mit der Verbreitung rechtswidriger Inhalte, Mechanismen für deren wirksame Prüfung und für die Unterrichtung der Beschwerdeführer über die Ergebnisse einer solchen Beschwerdeprüfung sowie einen transparenten, einfachen und wirksamen Mechanismus für die Einlegung von Rechtsmitteln gegen Maßnahmen gewährleisten, die von VSP-Anbietern im Zusammenhang mit der Prüfung solcher Nutzerbeschwerden ergriffen werden; wirksame Maßnahmen und Instrumente zur Förderung der Medienkompetenz und Sensibilisierung der Nutzer für solche Maßnahmen umsetzen usw.[363] Verstößt eine VSP gegen ihre Verpflichtungen aus

[357] Gesetz der Ukraine über die Medien, Nr. 2849-IX (ukr.), 13. Dezember 2022.
[358] Dazu können Plattformen wie Telegram, Facebook, X usw. gehören.
[359] Die Verpflichtungen im Gesetz orientieren sich an den entsprechenden Bestimmungen in der AVMD-RL, insbesondere an Artikel 28b und weiteren Artikeln.
[360] Art. 25, 26 und 120 UMG. Diese Anforderungen zielen darauf ab, jegliche Verbindungen mit dem Aggressorstaat, sei es durch Eigentum oder Finanzierung, zu verhindern. Für weitere Informationen siehe Opryshko, D., "Regulation of Media in the Context of Armed Aggression" *in* Batura, O., Holznagel, B. und Kalbhenn, J.C. (Hrsg.), *Disinformation in Europe. Challenges, Legal Instruments & Policy Recommendations*, Nomos, 2024, S. 254-257.
[361] Die in Kapitel IX UMG vorgesehenen Sonderbestimmungen gelten nur für einen Aggressorstaat, der vom Parlament der Ukraine offiziell als solcher anerkannt wurde. Die Anwendung dieser Bestimmungen ist zeitlich begrenzt – bis zum Widerruf dieses Status und für fünf Jahre nach einem solchen Widerruf. Stand August 2025 wendet die Ukraine den Status eines „Aggressorstaats" nur auf Russland an (seit 2015), nachdem es einen Teil des ukrainischen Hoheitsgebiets rechtswidrig besetzt hat.
[362] Zu diesen Einschränkungen gehören 14 allgemeine Kategorien (Artikel 36 UMG), Informationen, welche die körperliche, geistige oder sittliche Entwicklung von Kindern beeinträchtigen können (Artikel 42 UMG) und vier besondere Arten von Inhalten, deren Verbreitung verboten ist, solange die Bestimmungen des Kapitels IX in Kraft sind (Artikel 119 UMG).
[363] Art. 23 Abs. 1 UMG.

dem UMG, kann der Nationale Rundfunkrat der Ukraine (Nationalrat) entsprechende Geldstrafen verhängen.[364]

Die Nutzer von VSP können gegen rechtswidrige Entscheidungen, Handlungen und Untätigkeit von VSP beim Nationalrat und/oder vor Gericht Einspruch erheben.[365] Die VSP-Anbieter haben wiederum das Recht, eine Koregulierungsstelle einzurichten.[366]

Die ukrainischen Rechtsvorschriften sehen für die Interaktion mit Online-Plattformen, die nicht der Rechtshoheit der Ukraine unterliegen, nur „nicht zwingende" Mechanismen vor. In diesem Zusammenhang ermächtigt das UMG die Medienregulierungsbehörde und andere staatliche Stellen, Maßnahmen zur Zusammenarbeit mit solchen Plattformen zu ergreifen, unter anderem durch den Abschluss entsprechender Vereinbarungen oder Memoranden.[367] Obwohl die Verhandlungen mit einigen Unternehmen wie Meta und Google seit etwa einem Jahr laufen, wurden bislang keine Memoranden unterzeichnet oder Vereinbarungen getroffen.[368] Bis Ende 2024 gab es immer noch keine wirksamen rechtlichen Mechanismen, um auf Online-Plattformen einzuwirken, die nicht der ukrainischen Rechtsprechung unterliegen, aber innerhalb der Ukraine tätig sind.[369] Stand August 2025 gab es in dieser Hinsicht keine wesentlichen Änderungen.

Dies stellt eine Herausforderung für die Ukraine dar, insbesondere angesichts der systematischen, groß angelegten und gezielten Informationsangriffe Russlands auf das Land und seine Bevölkerung. Die Situation wird durch den stetigen Anstieg des

[364] Art. 114 und Art. 116 Abs. 19 UMG. Bei schwerwiegenden Verstößen müssen VSP-Anbieter mit einer Geldbuße zwischen dem 5- und 25-Fachen des zum Zeitpunkt des Verstoßes geltenden Mindestlohns rechnen. Bei der Festsetzung der Geldbuße muss der Nationalrat die für die Erbringung des Dienstes verwendete Technologie, das Gebiet, in dem der Dienst erbracht wird, die Reichweite des Dienstes und andere Umstände berücksichtigen, die sich auf den Grad der öffentlichen Gefahr auswirken, die von der begangenen Verletzung ausgeht. Stand August 2025 beläuft sich die ungefähre Höhe der Geldbuße auf 870 EUR bis 4.350 EUR.

[365] Art. 23 Abs. 3 UMG.

[366] Laut UMG werden von den Vertretern der Medienbranche Koregulierungsstellen eingerichtet, die gemeinsam mit dem Nationalrat berechtigt sind, Kodizes (Regeln) für die Erstellung und Verbreitung bestimmter Informationen, Kriterien für verbotene Informationen (unter anderem Hassrede, Diskriminierung, Aufstachelung zu Terrorismus, Kinderpornografie), Kriterien für die Einstufung von Personen als Rechtsträger im Bereich der Online-Medien, Kriterien für die Einstufung von Werbung als schädlich usw. zu entwickeln. Dieser Mechanismus sieht vor, dass sich Rechtsträger im Medienbereich freiwillig zur Einhaltung der jeweiligen Kodizes (Regeln) verpflichten, während der Nationalrat anerkennt, dass diese Anforderungen ausreichen, um das öffentliche Interesse zu gewährleisten (Art. 36 Abs.2, Art. 90 Abs. 1 Ziff. 23, 24, 26, 51 und Abs. 2, Art. 92 UMG).

[367] Art. 2 Abs. 15, Art. 90 Abs. 1 Ziff. 13 und 14, Art. 91 Abs. 1 Ziff. 3, 11, 13, Art. 99 Abs, 3, Art. 124 Abs. 5 UMG.

[368] Opryshko, D., "Monitoring Media Pluralism in the European Union: Preliminary Study to the Implementation of the Media Pluralism Monitor 2025 in Ukraine", EUI, RSC, Forschungsprojektbericht, Zentrum für Medienpluralismus und Medienfreiheit (CMPF), 2025, S.13; „Nationaler Rundfunkrat der Ukraine, Regulierung von Plattformen und wer finanziert Unternehmen, die Medien registrieren: Nationalrat trifft sich mit amerikanischer Handelskammer" (ukr.), Pressemitteilung, 15. April 2025, abrufbar unter: https://webportal.nrada.gov.ua/regulyuvannya-platform-ta-hto-finansuye-kompaniyi-yaki-reyestruyut-media-natsionalna-rada-provela-zustrich-z-amerykanskoyu-torgovelnoyu-palatoyu/.

[369] Opryshko, D., "Monitoring Media Pluralism in the European Union: Preliminary Study to the Implementation of the Media Pluralism Monitor 2025 in Ukraine", EUI, RSC, Forschungsprojektbericht, Zentrum für Medienpluralismus und Medienfreiheit (CMPF), 2025.

Informations- und Nachrichtenkonsums über soziale Plattformen noch besorgniserregender.[370]

In diesem Zusammenhang ist anzumerken, dass Telegram nach dem Beginn der umfassenden russischen Invasion im Februar 2022 zur beliebtesten Online-Plattform in der Ukraine wurde. Der Grund dafür war, dass die Plattform einen sehr einfachen Zugang zu Informationen ermöglichte und Kanäle enthielt, die die Menschen über die Richtung von Drohnen und Raketen informierten, die auf die Ukraine abgeschossen wurden, usw. Darüber hinaus richteten viele Regierungsbeamte, auch auf höchster Ebene, eigene Kanäle auf der Telegram-Plattform ein, um mit den ukrainischen Bürgerinnen und Bürgern zu kommunizieren.[371] Telegram behauptete seinen Status als führende Online-Plattform in der Ukraine zumindest bis Ende 2024.[372]

Gleichzeitig wird diese Online-Plattform aktiv im Rahmen feindlicher russischer Informationsaktionen genutzt, und zwar für Cyberangriffe, zur Verbreitung von Phishing-Nachrichten und Schadsoftware, zur Geolokalisierung von Nutzern und zur Korrektur von Raketenangriffen,[373] zur Rekrutierung von Bürgerinnen und Bürgern (einschließlich Minderjähriger) für die Begehung von Straftaten gegen die Ukraine (zum Beispiel Sprengung militärischer Kommandostellen, die für die Umsetzung der ukrainischen Rechtsvorschriften zur Wehrpflicht, zum Wehrdienst und zur Mobilisationsvorbereitung zuständig sind, und Beschädigung oder Zerstörung des Eigentums (zum Beispiel Autos) von Militärangehörigen usw.) genutzt.[374]

Dies war der Anstoß für die Ausarbeitung mehrerer Gesetzesentwürfe zur Regulierung von Online-Plattformen, darunter der Entwurf eines Gesetzes zur Änderung bestimmter Gesetze der Ukraine über die Regulierung der Tätigkeit von Plattformen für gemeinsamen Informationszugang, über die Masseninformationen verbreitet werden.[375]

Laut der Begründung soll dieser Gesetzesentwurf den staatlichen Behörden die Mittel an die Hand geben, um wirksam auf Bedrohungen der nationalen Sicherheit zu reagieren, die von Online-Plattformen, insbesondere Telegram, ausgehen.[376]

---

[370] Ebd., S. 6.

[371] Horbyk, R., Dutsyk, D. und Shalaysky, S., "Die Effektivität der Bekämpfung russischer Desinformation in der Ukraine im Kontext eines umfassenden Kriegs. Ein analytischer Bericht“ (ukr.) NGO "Ukrainisches Institut für Medien und Kommunikation", 2023, S. 7 und 50.

[372] InMind, „Ukrainische Medien, Einstellung und Vertrauen im Jahr 2024“ (ukr.), November 2024, S. 4 und 28.

[373] Der Nationale Sicherheits- und Verteidigungsrat der Ukraine hat beschlossen, die Nutzung von Telegram in staatlichen Behörden, militärischen Formationen und kritischen Infrastruktureinrichtungen zu beschränken, siehe https://www.rnbo.gov.ua/ua/Diialnist/6994.html.

[374] Regionale Militärverwaltung Charkiw, „Cyberpolizei warnt: Die Anwerbung von Jugendlichen im Internet für Sabotageakte hat zugenommen“ (ukr.), 19. Februar 2025; Innenministerium der Ukraine, „Feind rekrutiert Jugendliche für Sabotageakte: Cyberpolizei warnt vor Gefahren im Internet" (ukr.), 12. März 2025; Patoka, M., "Der SBU hat offengelegt, wie viele Minderjährige wegen Kollaboration mit der Russischen Föderation festgenommen wurden“ (ukr.), 30. Juni 2025.

[375] Gesetz zur Änderung bestimmter Gesetze der Ukraine über die Regelung der Tätigkeit von Plattformen für gemeinsamen Informationszugang, über die Masseninformationen verbreitet werden, Nr. 11115, 25. März 2024 (Gesetzentwurf).

[376] Erläuterung zum Gesetzentwurf der Ukraine über die Änderung bestimmter Gesetze der Ukraine zur Regelung der Tätigkeit von Plattformen für gemeinsamen Informationszugang, über die Masseninformationen verbreitet werden, Nr. 11115 vom 25. März 2024, verfügbar unter: https://itd.rada.gov.ua/billinfo/Bills/Card/43884.

Die Urheber des Entwurfs wollten Elemente des DSA-Ansatzes zur Regulierung von Online-Plattformen in die ukrainische Gesetzgebung übernehmen. So schlugen sie beispielsweise vor, dass Plattformen, die nicht unter die Rechtshoheit der Ukraine oder eines EU-Mitgliedstaates fallen, verpflichtet werden sollten, einen bevollmächtigten Vertreter in der Ukraine zu benennen, um die Kommunikation mit dem Nationalrat, anderen staatlichen Behörden und lokalen Selbstverwaltungsorganen zu erleichtern.

Die vorgeschlagenen Änderungen des Entwurfs bieten jedoch keine ausreichende Rechtssicherheit. Sie erklären nicht, warum Online-Plattformen, die Masseninformationen verbreiten, anders behandelt werden sollten als andere Online-Plattformen, da beide Arten von Plattformen die Möglichkeit bieten, Nutzerinformationen zu speichern und an eine unbegrenzte Zahl von Adressaten weiterzugeben. Aus dem Entwurf geht nicht hervor, ob die vorgeschlagenen Bestimmungen nur für Plattformen gelten, die ihre Aktivitäten auf die Ukraine und ihre Bevölkerung ausrichten. Darüber hinaus ist unklar, auf welcher Grundlage Plattformen, die der Rechtshoheit eines oder mehrerer EU-Mitgliedstaaten unterliegen, mit den ukrainischen Behörden zu Benachrichtigungen, Forderungen, Entscheidungen, Anträgen, Briefen oder anderen Dokumenten kommunizieren sollten, die ihnen von den zuständigen ukrainischen Stellen zugestellt werden.

Dieser Entwurf klassifiziert Anbieter von Online-Plattformen, über die Masseninformationen verbreitet werden, als Rechtsträger im Medienbereich, klärt aber im Gegensatz zum EMFA und zum DSA nicht die Frage der redaktionellen Verantwortung in diesem Zusammenhang.[377] Er sieht neben anderem auch keine gerichtlichen Mechanismen in Fällen vor, in denen es um Zugangsbeschränkungen auf der Grundlage von Anträgen der Medienregulierungsbehörde zu Inhalten geht, deren Verbreitung gegen die Anforderungen des UMG verstößt.

Im August 2025 befand sich der Entwurf noch zur Beratung im Parlamentsausschuss für humanitäre Hilfe und Informationspolitik. Bisher ist er noch nicht der *Werchowna Rada* (ukrainisches Parlament) zur ersten Lesung vorgelegt worden.

Im September 2024 empfahl das Nationale Koordinationszentrum für Cybersicherheit des Nationalen Sicherheits- und Verteidigungsrates der Ukraine, die Installation und die Nutzung von Telegram auf den dienstlichen Geräten von Mitarbeitern staatlicher Behörden zu verbieten. Dieses Verbot gilt auch für Militärangehörige, Mitarbeiter des Sicherheits- und Verteidigungssektors sowie Unternehmen, die kritische Infrastrukturen betreiben (mit Ausnahme von Personen, für die die Nutzung dieses Messengers Teil ihrer dienstlichen Pflichten ist).[378] Diese Empfehlungen wurden von einer Reihe von Behörden, staatlichen Universitäten und anderen Einrichtungen umgesetzt.

---

[377] Nach dem EMFA könnten Anbieter sehr großer VSP als VSP-Anbieter, als VLOP-Anbieter, aber auch als Mediendiensteanbieter eingestuft werden, wenn sie die redaktionelle Kontrolle über einen Teil oder mehrere Teile ihrer Dienste ausüben (Erwägungsgrund 11). Die im DSA vorgesehenen Haftungsbefreiungen sollten unter anderem nicht für Informationen gelten, die unter der redaktionellen Verantwortung des Anbieters des Vermittlungsdienstes selbst erstellt wurden (Erwägungsgrund 18).

[378] Nationaler Sicherheits- und Verteidigungsrat, "The NCCC Has Decided to Restrict the Use of Telegram in Government Agencies, Military Formations, and Critical Infrastructure Facilities", Pressemitteilung, 20. September 2024.

Im Zusammenhang mit dieser Empfehlung kündigte der Nationalrat zudem die Einführung einer Sonderregelung für den Zugang zu Telegram an. Den Mitarbeitern der Medienregulierungsbehörde wurde die Nutzung von Telegram auf ihren Arbeitsgeräten untersagt (zum Schutz von Verschlusssachen). Gleichzeitig wurde ein separates Netzwerksegment (getrennt vom internen Netzwerk des Nationalrats, aber verbunden mit dem externen Internet) geschaffen, um die Aktivitäten von Medien auf dieser Online-Plattform zu analysieren.[379]

3.4.2 Spezifische Vorschriften zu Desinformation

In einer Reihe von strategischen Dokumenten der Ukraine werden die Bekämpfung von Desinformation und speziellen Informationsaktionen sowie die Verbesserung der Medienkompetenz der Bevölkerung als Ziele definiert.[380]

2022 führte die umfassende russische Invasion zur Verhängung des Kriegsrechts[381] über das gesamte Gebiet der Ukraine und zur Einschränkung des Rechts auf freie Meinungsäußerung[382] sowie zur Abweichung der Ukraine von ihren Verpflichtungen gemäß Artikel 19 des Internationalen Pakts über bürgerliche und politische Rechte (IPbpR)[383] und Artikel 10 der EMRK.[384] Obwohl offiziell keine Zensur eingeführt wurde, wurde die ukrainische Gesetzgebung geändert, womit neue Vorschriften zur Bekämpfung des russischen Informationseinflusses vorgesehen wurden.

---

[379] Nationaler Rundfunkrat der Ukraine, "Der Nationalrat hat ein spezielles Verfahren für den Zugang zu Telegram eingeführt", Pressemitteilung, 9. Oktober 2024,

[380] Diese Ziele wurden als Prioritäten der staatlichen Politik im Informationsbereich der Ukraine unter anderem in der Doktrin der Informationssicherheit der Ukraine (2017-2021) (ukr.) und als strategische Ziele in der Strategie der Informationssicherheit (2021) (ukr.) mit geplanter Umsetzungsfrist bis 2025 definiert. Siehe auch die Strategie des Ministeriums für Kultur und Informationspolitik der Ukraine zur Entwicklung der Medienkompetenz für den Zeitraum bis 2026, abrufbar hier (ukr.).

[381] Das Kriegsrecht ist eine besondere rechtliche Regelung, die in der Ukraine oder in bestimmten Gebieten im Fall einer bewaffneten Aggression oder der Gefahr einer Aggression oder einer Bedrohung der Unabhängigkeit des ukrainischen Staates und seiner territorialen Integrität verhängt wird; es sieht die Erteilung von Befugnissen an die zuständigen staatlichen Behörden, das Kommando der Streitkräfte, die Militärverwaltungen und die lokalen Regierungen vor, die notwendig sind, um die Bedrohung abzuwenden, den bewaffneten Angreifer abzuwehren und die nationale Sicherheit zu gewährleisten, die Bedrohung der Unabhängigkeit des Staates und der territorialen Integrität der Ukraine abzuwehren sowie eine vorübergehende bedrohungsbedingte Einschränkung der verfassungsmäßigen Rechte und Freiheiten von Personen und Bürgern und der Rechte und legitimen Interessen von juristischen Personen vorzunehmen, wobei die Dauer dieser Einschränkungen festgelegt wird (Artikel 1 des Gesetzes der Ukraine über die rechtliche Regelung des Kriegsrechts vom 12. Mai 2015 (ukr.), Nr. 389-VIII).

[382] Opryshko ,D., "Freedom of Expression during Military Conflict" in ORF (Hrsg.), *Public Value Texte 25 – Why Independence Matters,* ORF, Wien, 2022, S. 45-53, 46.

[383] Internationaler Pakt über bürgerliche und politische Rechte (engl.), (verabschiedet am 16. Dezember 1966) 999 UNTS 171.

[384] Opryshko, D., "Monitoring Media Pluralism in the Digital Era: Application of the Media Pluralism Monitor in the European Union, Albania, Montenegro, the Republic of North Macedonia, Serbia and Turkey in the Year 2022. Preliminary Study to the Implementation of the Media Pluralism Monitor: Ukraine", EUI, RSC, Zentrum für Medienpluralismus und Medienfreiheit, 2023, S. 7-8.

Dazu gehörten beispielsweise die Einführung strafrechtlicher Verantwortung für die Rechtfertigung, Anerkennung der Legitimität oder Leugnung der bewaffneten Aggression der Russischen Föderation gegen die Ukraine oder die Verherrlichung ihrer Teilnehmer,[385] die vorübergehende Sperrung von audiovisuellen Abrufmediendiensten und von Diensten der Anbieter audiovisueller Dienste des Aggressorstaates auf dem Gebiet der Ukraine[386] sowie die Einführung von Verpflichtungen für VSP, vorübergehende Verbote der Verbreitung von vier speziellen Arten von Inhalten in ihre Nutzungsbedingungen aufzunehmen.[387]

Zu Letzteren gehören (1) Informationen, die die bewaffnete Aggression gegen die Ukraine als internen Konflikt, Zivilkonflikt oder Bürgerkrieg darstellen, und (2) nicht vertrauenswürdiges Material über die bewaffnete Aggression und die Handlungen des Aggressorstaates (Besatzungsstaates), seiner Beamten, Personen und Organisationen, die vom Aggressorstaat (Besatzungsstaat) kontrolliert werden, wenn die Verbreitung dieses Materials zu Feindseligkeit oder Hass aufstachelt.[388] Dies erklärt sich aus der Tatsache, dass Russland systematisch Desinformationsnarrative wie „interner Konflikt/Zivilkonflikt/Bürgerkrieg“ oder „Durchführung einer Spezialoperation zur Entnazifizierung/Entsatanisierung“ verwendet, um seine rechtswidrigen Aktionen zu rechtfertigen und die ukrainische Gesellschaft zu spalten und zu schwächen.[389]

Um die verstärkende Wirkung von Desinformationsnarrativen, die von russischen Künstlern und Musikern unterstützt werden,[390] zu verringern, verbietet das ukrainische Gesetz darüber hinaus die Verbreitung von (3) Sendungen und Material (mit Ausnahme von Informationen und analytischen Inhalten), bei denen einer der Teilnehmer eine Person ist, die auf der Liste der Personen steht, die eine Bedrohung für die nationale Sicherheit darstellen[391] und (4) Musiktonträger, Bildaufzeichnungen und Musikclips, die von Sängern dargeboten werden, die Bürger des Aggressorstaates sind (mit einigen Ausnahmen) und die die russische Aggression gegen die Ukraine nicht verurteilt haben und daher auf der entsprechenden Liste stehen.[392]

---

[385] Siehe Gesetz der Ukraine über die Änderung bestimmter Rechtsakte der Ukraine zur Verschärfung der strafrechtlichen Verantwortung für die Herstellung und Verbreitung verbotener Informationsprodukte vom 3. März 2022 (ukr.).

[386] Art. 123 UMG. Stand August 2025 sind 49 Dienste in die Liste der audiovisuellen Abrufmediendienste und der Dienste von Anbietern audiovisueller Dienste des Aggressorstaates aufgenommen worden. Die entsprechende Liste ist hier (ukr.) abrufbar.

[387] Während die Bestimmungen des Kapitels IX des UMG wie oben erwähnt in Kraft sind, gelten die in diesem Kapitel vorgesehenen Sonderbestimmungen nur für einen Aggressorstaat, der vom Parlament der Ukraine offiziell als solcher anerkannt wurde. Die Anwendung der Bestimmungen ist zeitlich begrenzt – bis zur Aufhebung des Status eines Aggressorstaates und für fünf Jahre nach einer solchen Aufhebung.

[388] Art. 112 Abs 4 Ziff. 7 und 8, Art. 119 Abs. 1 Ziff. 1 und 2 UMG.

[389] Opryshko, D., “Regulation of Media in the Context of Armed Aggression” in Batura O., Holznagel B. and Kalbhenn J.C. (Hrsg.), *Disinformation in Europe. Challenges, Legal Instruments & Policy Recommendations*. Nomos, 2024, S. 251-252.

[390] Ebd., S. 252-254; Batura, O. und Opryshko, D., *„Kunstfreiheit und Propaganda aus Sicht des Völkerrechts“*, in Crückeberg J. et al. (Hrsg.), *Handbuch Kulturpolitik*, Springer VS, Wiesbaden, 2023.

[391] Auf dieser Liste stehen unter anderem berühmte Theater- und Filmschauspieler, Regisseure, Produzenten, Komponisten, Sänger, Fernsehmoderatoren usw., die den Krieg Russlands gegen die Ukraine öffentlich unterstützen. Die Liste ist hier (ukr.) verfügbar.

[392] Art. 119 Abs. 1 Ziff. 3 und 4 UMG.

3.4.3 Anwendung im Fall ausländischer Einmischung durch Desinformation in Kriegszeiten

Die Bestimmungen des UMG, die für die der ukrainischen Rechtsprechung unterliegenden VSP gelten, wurden bislang nicht angewandt. Der Grund dafür ist, dass solche Plattformen in der Ukraine erst seit 2025 registriert sind. Stand August 2025 gibt es lediglich zwei VSP, die unter ukrainische Rechtshoheit fallen.[393]

Es ist zu beachten, dass das UMG unterschiedliche Regulierungsansätze für Online-Plattformen und Medien festlegt, die ihre Konten auf diesen Plattformen als Online-Medien registriert haben. Letztere müssen die Anforderungen der ukrainischen Gesetzgebung einschließlich der Vorschriften über Transparenz der Eigentumsverhältnisse erfüllen und können für Verstöße gegen das UMG haftbar gemacht werden. Sehr viel problematischer ist nach wie vor die Bekämpfung von Desinformation, Fehlinformation und Propaganda auf anonymen Konten und Kanälen. Solche Kanäle haben häufig eine große Zahl von Followern (in absoluten Zahlen bis zu einem Drittel der ukrainischen Bevölkerung)[394] und damit einen starken Einfluss auf die Gesellschaft. Die Ukraine kann jedoch ihre Rechtsvorschriften nicht auf sie anwenden, da sie über die zuvor erwähnten Online-Plattformen keine Rechtshoheit hat.

Die Tatsache, dass dem Staat wirksame Mechanismen zur Einflussnahme auf ausländische Online-Plattformen fehlen, um seine nationalen Interessen zu schützen, hat zu einer weit verbreiteten Sperrung ganzer Websites und Online-Plattformen geführt. Solche Sperrungen erfolgen hauptsächlich auf der Grundlage des ukrainischen Sanktionsgesetzes und im Zusammenhang mit der umfassenden russischen Invasion in der Ukraine; sie werden auch auf Anweisung des Nationalen Zentrums für das betriebliche und technische Management von Telekommunikationsnetzen (NCU) vorgenommen. Beide Mechanismen werden von Menschenrechtsanwälten, Experten und Branchenverbänden ständig kritisiert, unter anderem wegen ihrer mangelnden Transparenz und Vorhersehbarkeit.[395]

Die ersten Sperrungen von Webressourcen nach dem ukrainischen Sanktionsgesetz erfolgten ab 2017 und betrafen unter anderem russische Online-Plattformen wie VKontakte, Odnoklassniki, den E-Mail-Dienst Mail.ru sowie die Suchmaschine und das Internetportal von Yandex.[396] Als Rechtsgrundlage für solche Sperrungen wurde Artikel 4

---

[393] Liste der Rechtsträger im Medienbereich vom 1. August 2025, S. 6208, 6455, verfügbar hier (ukr.).

[394] Rodak, K., "Trukha: true colours revealed. Who really stands behind the largest network of anonymous Telegram channels in Ukraine and how much it costs", 5. September 2023; Sklyarevs'ka, G., NGL.media:" Trukha ist im Besitz von Volodymyr Lytvyn und verdient monatlich Hunderttausende von Dollar mit Werbung“ (ukr.); Opryshko D., "Media Ownership Transparency as a Shield against Foreign Interference: the Ukrainian Experience", EMFA Observatory, EUI, 26. März 2025.

[395] Opryshko, D., “Monitoring Media Pluralism in the European Union: Preliminary Study to the Implementation of the Media Pluralism Monitor 2025 in Ukraine", EUI, RSC, Forschungsprojektbericht, Zentrum für Medienpluralismus und Medienfreiheit (CMPF), 2025, S. 15-17.

[396] Erlass des Präsidenten der Ukraine zum Beschluss des Nationalen Sicherheits- und Verteidigungsrates der Ukraine vom 28. April 2017 über die Anwendung persönlicher wirtschaftlicher Sondermaßnahmen und anderer restriktiver Maßnahmen (Sanktionen), 15. Mai 2017 Nr. 133, verfügbar hier (ukr.). Beschlüsse zur Sperrung von Online-Ressourcen gemäß dem ukrainischen Sanktionsgesetz werden vom Nationalen Sicherheits- und

Absatz 1 Ziff. 25 des ukrainischen Sanktionsgesetzes herangezogen, nämlich „andere Sanktionen, die mit den in diesem Gesetz festgelegten Grundsätzen für ihre Anwendung übereinstimmen". Diese Art der Sperrung von Webressourcen wurde kritisiert, weil sie nicht dem Grundsatz entsprechen, dass solche Maßnahmen „gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig sind", wie in Artikel 10 Absatz 2 EMRK gefordert. Im Hinblick auf die Einschränkung der Verbreitung schädlicher Inhalte halten Experten eine solche Sperrung jedoch für eine verhältnismäßige Maßnahme zum Schutz der nationalen Sicherheit, personenbezogener Daten, des Urheberrechts und verwandter Schutzrechte sowie zur Bekämpfung raubkopierter Inhalte und nicht für einen Verstoß gegen das Recht auf freie Meinungsäußerung.[397]

Ein weiterer bereits erwähnter Mechanismus zur Sperrung von Webressourcen einschließlich der Sperrung des Zugangs zu digitalen Netzwerkadressen (IP) und autonomen Systemen (AS), der während des Kriegsrechts in der Ukraine angewandt wird, sind entsprechende Anordnungen des NCU.[398] Die Nichteinhaltung von NCU-Anordnungen kann zum Ausschluss von elektronischen Kommunikationsnetzen und Diensteanbietern aus dem entsprechenden Register führen, wodurch ihre Tätigkeit für ein Jahr ausgesetzt wird.[399]

Die Beschränkung des Zugangs zu IP-Adressen und AS hat nicht nur erhebliche Auswirkungen auf diejenigen, die schädliche Inhalte verbreiten, sondern auch auf andere Ressourcen, die keinen Beschränkungen unterworfen sind.[400] Dies führt dazu, dass es unmöglich ist, auf eine große Anzahl von Webressourcen zuzugreifen, die unter einer digitalen Adresse neben feindlichen Propagandaressourcen zu finden sind und nicht mit dem russischen Krieg gegen die Ukraine oder russischer Propaganda in Zusammenhang stehen. Experten betonen, dass die Praxis der AS-Sperrung einzigartig ist und nirgendwo sonst auf der Welt angewendet wird.[401] Die Sperrung von Webressourcen auf der Grundlage von Anordnungen des NCU ist nicht ausreichend transparent und vorhersehbar und bietet keinen Schutz vor willkürlichen Sperrungen[402]. Daher wurde kritisiert, dass sie nicht den europäischen Standards im Bereich der Meinungsfreiheit entspricht.

Verteidigungsrat der Ukraine verabschiedet und per Präsidialerlass in Kraft gesetzt (Art. 5 Abs. 2 und 3 des ukrainischen Sanktionsgesetzes).

[397] Opryshko, D., "Monitoring Media Pluralism in the European Union: Preliminary Study to the Implementation of the Media Pluralism Monitor 2025 in Ukraine", EUI, RSC, Forschungsprojektbericht, Zentrum für Medienpluralismus und Medienfreiheit (CMPF), 2025, S. 15-20.

[398] Art. 32 Abs. 8 des Gesetzes der Ukraine über elektronische Kommunikation (ukr.).

[399] Siehe zum Beispiel den Beschluss der Nationalen Kommission für staatliche Regulierung im Bereich der elektronischen Kommunikation, des Funkfrequenzspektrums und der Erbringung von Postdiensten (NKEK) vom 30. März 2022, Nr. 26, zum Ausschluss der Gesellschaft mit beschränkter Haftung NETASSIST aus dem Register der Betreiber und Anbieter von Telekommunikationsdiensten mit Änderungen durch den Beschluss der NKEK vom 1. Juni 2022, Nr. 59 (ukr.).

[400] Belovolchenko, A., "Es ist unmöglich, etwas im Internet zuverlässig zu blockieren. Wie russische Ressourcen in der Ukraine blockiert werden und warum es legale Seiten betrifft" (ukr.) DOU.ua, 13. Januar 2023.

[401] Opryshko, D., "Monitoring Media Pluralism in the European Union: Preliminary Study to the Implementation of the Media Pluralism Monitor 2025 in Ukraine", EUI, RSC, Forschungsprojektbericht, Zentrum für Medienpluralismus und Medienfreiheit (CMPF), 2025, S. 16-17.

[402] Ebd., S. 17.

4. Bekämpfung terroristischer Inhalte

4.1 Durchsetzung auf EU-Ebene

Dr Mark D. Cole, Wissenschaftlicher Direktor, Institut für Europäisches Medienrecht (EMR) und Professor für Medien- und Telekommunikationsrecht, Universität Luxemburg

Die Verbreitung terroristischer Inhalte im Internet hat im Laufe der Jahre zugenommen, weil Terroristen ihre Botschaften auf breiter Front über Plattformen verbreiten, auf denen hochgeladene Inhalte Dritter gehostet werden.[403] Schon in der AVMD-RL wird betont, dass die Öffentlichkeit vor Aufstachelung zum Terrorismus geschützt werden muss.[404] Daher verpflichtet die AVMD-RL die Mitgliedstaaten, mit geeigneten Mitteln sicherzustellen, dass die Dienste der ihrer Rechtshoheit unterworfenen Anbieter audiovisueller Mediendienste keine öffentliche Aufforderung zur Begehung einer terroristischen Straftat enthalten.[405] Gleichsam müssen auch Anbieter von Video-Sharing-Plattformen (VSP) geeignete Maßnahmen ergreifen, um solche Inhalte auf ihren Plattformen zu vermeiden.[406] Zu diesen Maßnahmen gehören Mechanismen zur Meldung und Anzeige von Inhalten, Systeme zur Altersüberprüfung, Tools zur Kontrolle durch Eltern und transparente Verfahren zur Moderation von Inhalten.[407]

Die Zugänglichkeit terroristischer Online-Inhalte hat entscheidend zur Radikalisierung einzelner Personen beigetragen.[408] So war die Verordnung über terroristische Online-Inhalte (TCO-VO)[409] eine direkte Reaktion auf die Grenzen der

[403] Europol, „European Union Terrorism Situation and Trend Report 2023“, Publications Office of the European Union, Luxembourg, 2023, und Europol, „European Union Terrorism Situation and Trend Report 2022“, Publications Office of the European Union, Luxembourg, 2022.

[404] Siehe Erwägungsgrund 18 AVMD-RL zur Erläuterung der Einführung einer speziellen Bestimmung zum Verbot der Verbreitung terroristischer Inhalte in Artikel 6 AVMD-RL.

[405] Artikel 6 der Richtlinie (EU) 2018/1808 des Europäischen Parlaments und des Rates vom 14. November 2018 zur Änderung der Richtlinie 2010/13/EU zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste (Richtlinie über audiovisuelle Mediendienste) im Hinblick auf sich verändernde Marktgegebenheiten, ABl. L 303/69, 28. November 2018.

[406] Artikel 28b Absatz 1 Buchstabe c AVMD-RL.

[407] Artikel 28b Absatz 3 AVMD-RL.

[408] Europäische Kommission, „Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Verhinderung der Verbreitung terroristischer Online-Inhalte“, COM(2018) 640 final, 2018 (Begründung); Europäische Kommission, „Bericht der Kommission an das Europäische Parlament und den Rat über die Durchführung der Verordnung (EU) 2021/784 zur Bekämpfung der Verbreitung terroristischer Online-Inhalte“, COM(2024) 64 final, 2024.

[409] Verordnung (EU) 2021/784 des Europäischen Parlaments und des Rates vom 29. April 2021 zur Bekämpfung der Verbreitung terroristischer Online-Inhalte, ABl. L 172/79 17. Mai 2021. Für einen Überblick siehe Voigt P., Eschborn E., Bastians H., *Weitreichende neue Pflichten für Host-Provider, Kurzanalyse der Verordnung zur Bekämpfung der Verbreitung terroristischer Online-Inhalte*, MMR 727, 2022.

freiwilligen Vereinbarungen im Rahmen des EU-Internetforums,[410] einer von der Europäischen Kommission im Dezember 2015 ins Leben gerufenen Multi-Stakeholder-Initiative. Obwohl das Echo zum EU-Internetforum im Hinblick auf die Verbesserung der Kooperation zwischen der Branche, Europol und den nationalen Behörden positiv Echo war, haben sich dort nicht allzu viele Hostingdiensteanbieter engagiert. Auch „Umfang und Tempo der Fortschritte" bei den Hostingdiensteanbietern wurden als nicht ausreichend angesehen, um das Problem der Zugänglichkeit terroristischer Online-Inhalte wirksam anzugehen.[411] Der Konsens über die Notwendigkeit eines stärkeren Vorgehens der EU gegen terroristische Online-Inhalte mündete 2018 in eine Empfehlung der Kommission.[412] Diese stützte sich auf die Mitteilung der Kommission aus dem Jahr 2017 über die Bekämpfung illegaler Online-Inhalte[413] und die Aktivitäten des EU-Internetforums, in denen wichtige Maßnahmen skizziert wurden, darunter auch Melde- und Abhilfeverfahren. Die vorgeschlagenen Maßnahmen wurden später in die TCO-VO aufgenommen, die harmonisierte Regeln für die Entfernung terroristischer Inhalte enthält und im Juni 2022 in Kraft trat.[414]

Die TCO-VO stützt sich auf die Definitionen terroristischer Straftaten in der Richtlinie 2017/541 zur Terrorismusbekämpfung[415] und legt zudem fest, für welches Material die Definition terroristischer Online-Inhalte gelten soll.[416] In diesem Sinne umfasst der weit gefasste Begriff „terroristische Inhalte" nicht nur Inhalte, die zur Begehung einer terroristischen Handlung anstiften, sondern auch Materialien, die sich auf die Anwerbung, die Ausbildung oder die Erteilung von Anweisungen beziehen, zur Beteiligung an einer terroristischen Vereinigung ermutigen oder die Gefahr bergen, dass eine Person zur Begehung einer terroristischen Handlung ermutigt wird.[417] Die Richtlinie 2017/541 enthält eine Liste vorsätzlicher Handlungen, die nach nationalem Recht als Straftaten definiert sind

---

[410] Europäische Kommission, „EU-Internetforum: Regierungen, Europol und Technologieunternehmen suchen gemeinsam Wege zur Bekämpfung von Anstiftung zu Terrorismus und Hassreden in Online-Medien", Pressemitteilung, 3. Dezember 2015.

[411] Europäische Kommission, „Bericht der Kommission an das Europäische Parlament und den Rat über die Durchführung der Verordnung (EU) 2021/784 zur Bekämpfung der Verbreitung terroristischer Online-Inhalte", op. cit.

[412] Empfehlung (EU) 2018/334 der Kommission vom 1. März 2018 für wirksame Maßnahmen im Umgang mit illegalen Online-Inhalten, ABl. L 63/50, 2018.

[413] Europäische Kommission, „Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Umgang mit illegalen Online-Inhalten, Mehr Verantwortung für Online-Plattformen", COM(2017) 555 final, 2017.

[414] Zu dem Vorschlag für eine TCO-VO siehe Cole M.D., Etteldorf C., Ullrich C., *Cross-Border Dissemination of Online Content*, Bd. 81, *Schriftenreihe Medienforschung*, Nomos, Baden-Baden, 2021, S. 149 ff. Für weitere Einzelheiten zur finalen TCO-VO siehe Albus V.H., „Eyes Shut, Fingers Crossed: the EU's Governance of Terrorist Content Online under Regulation 2021/784" in Gsenger R., Sekwenz M-T. (Hrsg.), *Digital Decade: How the EU Shapes Digitalisation Research*, Nomos, Baden-Baden, 2025, S. 209 ff.

[415] Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates sowie zur Änderung des Beschlusses 2005/671/JI des Rates, ABl. L 88/6 vom 31. März 2017.

[416] In Artikel 3 der Richtlinie 2017/541 zur Terrorismusbekämpfung sind eine Reihe von Straftaten aufgeführt, die nach nationalem Recht als terroristische Straftaten eingestuft werden sollten, wenn sie mit dem Ziel begangen werden, eine Bevölkerung auf schwerwiegende Weise einzuschüchtern, öffentliche Stellen oder eine internationale Organisation rechtswidrig zu einem Tun oder Unterlassen zu zwingen oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Landes oder einer internationalen Organisation ernsthaft zu destabilisieren oder zu zerstören.

[417] Artikel 2 Absatz 7 TCO-VO.

und rechtlich als terroristische Straftaten gelten, wie etwa Angriffe auf das Leben einer Person, die zum Tod führen können, Entführungen oder Geiselnahmen. Artikel 21 enthält außerdem eine Reihe von Maßnahmen, die gegen Online-Inhalte zu ergreifen sind, die eine öffentliche Aufforderung zur Begehung einer terroristischen Straftat darstellen.

Artikel 3 der TCO-VO führt mit Geltung für alle Hostingdiensteanbieter, die Dienstleistungen in der EU anbieten,[418] „Entfernungsanordnungen" ein und ermächtigt die zuständigen Behörden, solche Anordnungen zu erlassen, mit der die Hostingdiensteanbieter verpflichtet werden, in allen Mitgliedstaaten terroristische Inhalte zu entfernen oder den Zugang zu terroristischen Inhalten zu sperren. Je nachdem, welche Behörde als zuständig benannt wird, können Entfernungsanordnungen in Form einer behördlichen oder gerichtlichen Entscheidung ergehen. Die TCO-VO soll die Reaktionsgeschwindigkeit erhöhen und die Sperrung oder Entfernung von Inhalten an der Quelle gewährleisten. Daher muss die Anordnung, terroristische Inhalte zu entfernen oder zu sperren, so schnell wie möglich, in jedem Fall aber innerhalb einer Stunde nach Erhalt ausgeführt werden.[419]

Um eine zügige Bearbeitung der Anordnungen zu gewährleisten, müssen die zuständigen Behörden das Formular in Anhang I der TCO-VO verwenden, und gemäß Artikel 15 der TCO-VO haben Hostingdiensteanbieter eine Kontaktstelle zu benennen oder einzurichten, die den Erhalt von Entfernungsanordnungen auf elektronischem Weg ermöglicht. Hostingdiensteanbieter, deren Hauptniederlassung sich nicht in der EU befindet, müssen für die Entgegennahme, Einhaltung und Durchsetzung von Entfernungsanordnungen und Entscheidungen einen gesetzlichen Vertreter in der EU benennen. Vor dem Erlass einer Entfernungsanordnung sollten die zuständigen Behörden Informationen austauschen und sich untereinander sowie gegebenenfalls mit Europol abstimmen und zusammenarbeiten, um Doppelarbeit und die Störung von Ermittlungen zu vermeiden.[420] Nicht in der TCO-VO geregelt sind Löschersuchen – ein Mechanismus, mit dem Hostingdiensteanbieter auf Informationen aufmerksam gemacht werden, die als terroristische Inhalte gelten könnten, damit sie die Vereinbarkeit dieser Inhalte mit ihren Nutzungsbedingungen freiwillig prüfen können.[421] Sie sind jedoch nach wie vor eine wirksame und schnelle Möglichkeit, um Hostingdiensteanbieter auf terroristische Inhalte hinzuweisen, die über ihre Dienste verfügbar sind, und sie so in die Lage zu versetzen, freiwillig zu reagieren.[422]

Für grenzüberschreitende Entfernungsanordnungen innerhalb der EU führt die TCO-VO ein neues Verfahren ein, das unter anderem vorsieht, dass der Mitgliedstaat, in dem die Anordnung erlassen wurde, eine Kopie der Anordnung an die für die Hauptniederlassung

---

[418] Artikel 1 Absatz 2 TCO-VO.
[419] Artikel 3 Absatz 3 TCO-VO.
[420] Artikel 14 TCO-VO. Um Doppelarbeit zu vermeiden, werden die Mitgliedstaaten aufgefordert, die speziell dafür von Europol entwickelten Werkzeuge zu nutzen, etwa die von der EU Internet Rerferral Unit entwickelte *Plateforme Européenne de Retraits des Contenus illégaux sur Internet* (PERCI) (siehe Europol, „PERCI TCO Regulation Presentation" (7. November 2022)). PERCI soll die Übermittlung von Entfernungsanordnungen und Löschersuchen zentralisieren, koordinieren und erleichtern; dies hilft den zuständigen Behörden der Mitgliedstaaten, entsprechende Entfernungsanordnungen oder Löschersuchen vorzubereiten und an die entsprechenden Kontaktstellen zu übermitteln.
[421] Siehe Erwägungsgrund 40 TCO-VO.
[422] Ebd.

des Hostingdiensteanbieters zuständige Behörde[423] übermittelt, damit diese die Anordnung überprüfen kann. Die empfangende Behörde sollte zwar davon ausgehen können, dass die in einem anderen Mitgliedstaat erlassene Entfernungsanordnung rechtmäßig ist, hat aber die Möglichkeit, selbst zu überprüfen, ob sie gemäß den Bestimmungen der TCO-VO erlassen wurde und nicht anderweitig gegen die in der EU-Grundrechtecharta (EU-GRC) verankerten Standards verstößt.[424]

Darüber hinaus sieht die TCO-VO vor, dass Hostingdiensteanbieter im Rahmen zusätzlicher Sorgfaltspflichten sogenannte „spezifische Maßnahmen" ergreifen müssen, wenn festgestellt wurde, dass sie zuvor terroristischen Inhalten ausgesetzt waren.[425] Zu den spezifischen Maßnahmen gehören die Identifizierung und präventive Entfernung terroristischer Inhalte.[426] Allerdings sind Hostingdiensteanbieter nicht verpflichtet, zur Identifizierung oder Entfernung von Inhalten automatisierte Verfahren einzusetzen. Eine solche Verpflichtung würde auch gegen das in Artikel 8 des DSA und auch schon in der EC-RL[427] festgeschriebene Verbot verstoßen, Vermittlern allgemeine Überwachungspflichten aufzuerlegen.

Die Europäische Kommission hat die Aufgabe, die Umsetzung der TCO-VO genau zu überwachen.[428] Um das Bewusstsein für die im Rahmen der TCO-VO ergriffenen Maßnahmen zu schärfen, muss ein Hostingdiensteanbieter, der Maßnahmen gegen die Verbreitung terroristischer Inhalte ergriffen hat oder im Rahmen der TCO-VO zur Ergreifung von Maßnahmen aufgefordert wird, Transparenzberichte über diese Maßnahmen öffentlich zugänglich machen.[429] Da die TCO-VO keine zivilrechtliche Haftung für gehostete Inhalte vorsieht, stützt sie sich auf ein System von Sanktionen. Artikel 18 der TCO-VO verpflichtet die Mitgliedstaaten, Sanktionsvorschriften zu erlassen; bei einem systematischen oder fortwährenden Verstoß gegen die Entfernungsverpflichtungen sind finanzielle Sanktionen in Höhe von bis zu 4 % vom weltweiten Jahresumsatz des Hostingdiensteanbieters zu verhängen.[430]

Trotz des sehr begrenzten Anwendungsbereichs, sowohl hinsichtlich der Art der betroffenen Inhalte als auch hinsichtlich der Tatsache, dass es lediglich um die Adressen von Hostingdiensteanbietern geht, kommt der Bericht über die Umsetzung der TCO-VO zu dem Schluss, dass diese sich positiv auf die Eindämmung der Verbreitung terroristischer Online-Inhalte ausgewirkt hat.[431] Aus dem Bericht geht jedoch auch hervor, dass die Europäische Kommission nur Informationen über 349 Entfernungsanordnungen erhalten

[423] Eine Liste der zuständigen nationalen Behörden und Kontaktstellen ist auf einer speziellen Website der Europäischen Kommission zu finden.
[424] Artikel 4 TCO-VO.
[425] Siehe Artikel 5 Absatz 4 TCO-VO.
[426] Artikel 5 TCO-VO.
[427] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (Richtlinie über den elektronischen Geschäftsverkehr).
[428] Artikel 21 TCO-VO.
[429] Artikel 7 Absatz 2 TCO-VO.
[430] Artikel 18 Absatz 3 TCO-VO.
[431] Europäische Kommission, „Bericht der Kommission an das Europäische Parlament und den Rat über die Durchführung der Verordnung (EU) 2021/784 zur Bekämpfung der Verbreitung terroristischer Online-Inhalte", op. cit.

hat, die von den zuständigen Behörden[432] von sechs Mitgliedstaaten (Spanien, Rumänien, Frankreich, Deutschland, Tschechien und Österreich) zwischen Juni 2022 und 31. Dezember 2023 erlassen wurden.[433] Die Einführung der von Europol entwickelten technischen Plattform PERCI am 3. Juli 2023, als neuem Kommunikationskanal zur Bekämpfung illegaler Online-Inhalte, führte zu einer Zunahme der Löschersuchen, und bis Ende 2023 wurden mehr als 14 000 Löschersuchen bearbeitet.[434] Eine Herausforderung stellt nach wie vor die Übermittlung von Takedown-Ersuchen – jetzt in Form von Entfernungsanordnungen – dar, wenn Hostingdiensteanbieter ihren Sitz in einem Drittland haben und keinen gesetzlichen Vertreter in der EU benannt haben.[435]

Parallel zur TCO-VO und der Überwachung ihrer Umsetzung hat die Europäische Kommission ihre Arbeit mit den Mitgliedstaaten, Europol und der Industrie, die auf freiwilliger Basis teilnahm, fortgesetzt, unter anderem im Rahmen des EU-Internetforums. So wurde beispielsweise 2024 eine Planübung im Rahmen des EU-Krisenprotokolls durchgeführt – eines freiwilligen Mechanismus, der es EU-Mitgliedstaaten und Online-Plattformen ermöglicht, bei einem Terroranschlag schnell und koordiniert auf die Verbreitung terroristischer Online-Inhalte zu reagieren.[436] Darüber hinaus hat Europol an der Entwicklung einer „Hash-Datenbank" für bekannte terroristische Inhalte mitgewirkt, mit der als schädlich identifizierte Inhalte elektronisch gekennzeichnet werden, sodass deren erneutes Auftauchen verhindert wird.[437]

Es ist zu beachten, dass der DSA unbeschadet der Bestimmungen der TCO-VO gilt, die Haftungsregelung der TCO-VO also Vorrang vor den entsprechenden Bestimmungen des DSA hat, etwa bei der Vollstreckung einer Entfernungsanordnung.[438] Gemäß Artikel 16 Absätze 5 und 6 des DSA müssen VLOPSEs Personen oder Einrichtungen unverzüglich über Entscheidungen zur Inhaltsmoderation informieren und dabei auf mögliche Rechtsbehelfe hinweisen. Sie müssen also den betroffenen Personen oder Einrichtungen auch mitteilen, wenn sie aufgrund eines Löschersuchens oder einer Entfernungsanordnung tätig werden.

Es ist anzumerken, dass der DSA zwar ein breiteres Spektrum an Diensten abdeckt als die TCO-VO, VLOPSEs jedoch hinsichtlich von Maßnahmen gegen die Verbreitung terroristischer Inhalte von besonderem Interesse sind. Aufgrund der mit VLOPSEs verbundenen systemischen Risiken müssen die Anbieter dieser Dienste gemäß DSA unter anderem eine Risikobewertung in Bezug auf die Verbreitung illegaler – also auch terroristischer – Inhalte und die zu erwartenden negativen Auswirkungen auf die Menschenrechte durchführen. Die Risiken, die mit der Verbreitung illegaler Inhalte

[432] Eine Liste der zuständigen nationalen Behörden und Kontaktstellen ist auf einer speziellen Website der Europäischen Kommission zu finden.
[433] Europäische Kommission, „Bericht der Kommission an das Europäische Parlament und den Rat über die Durchführung der Verordnung (EU) 2021/784 zur Bekämpfung der Verbreitung terroristischer Online-Inhalte", op. cit.
[434] Ebd.
[435] Ebd.
[436] Europol, „Tabletop Exercise Hosted by Europol to Disrupt Terrorist Content Online", Pressemitteilung, 7. März 2024.
[437] Europäische Kommission, „Eine Agenda für Terrorismusbekämpfung für die EU und ein stärkeres Mandat für Europol: Fragen und Antworten",Pressemitteilung, 9. Dezember 2020.
[438] Artikel 2 Absatz 4 DSA.

verbunden sind, müssen sorgfältig gemeldet, analysiert und angegangen werden.[439] Da die VLOPSEs sehr verschieden sind, fällt die Exposition gegenüber terroristischen Inhalten ganz unterschiedlich aus.

Sobald ein systemisches Risiko der Verbreitung von und Exposition gegenüber terroristischen Inhalten festgestellt wird, erfordern die Risikominderungsmaßnahmen, dass die betreffende VLOPSE sich mit verschiedenen Akteuren abstimmt und austauscht. Alle Maßnahmen, die VLOPSEs in Bezug auf terroristische Inhalte ergreifen, sollten die festgestellten spezifischen Systemrisiken angemessen und wirksam mindern.[440]

Im Gegensatz dazu ist ein Hostingdiensteanbieter gemäß TCO-VO nur dann verpflichtet, „spezifische Maßnahmen" – auch solche zur Verringerung seiner Exposition gegenüber terroristischen Inhalten – zu ergreifen, wenn diese Exposition gegenüber terroristischen Inhalten von der für ihn zuständigen Behörde förmlich festgestellt wurde. Die Entscheidung der zuständigen Behörde muss sich auf objektive Faktoren stützen, etwa auf den Erhalt von mindestens zwei Entfernungsanordnungen innerhalb eines Jahres.[441] Diese Form der Risikominderung ist also reaktiv, während der DSA von den VLOPSEs verlangt, dass sie proaktiv tätig werden, indem sie eine präventive Risikobewertung durchführen. Während Einzelheiten für andere Risikobereiche in Verhaltenskodizes geregelt sind, sieht die TCO-VO bereits selbst Risikominderungsmaßnahmen in Form von Löschersuchen, Entfernungsanordnungen und „spezifischen Maßnahmen" vor, sobald ein Hostingdiensteanbieter terroristischen Inhalten ausgesetzt war.[442]

Darüber hinaus verpflichtet Artikel 18 des DSA Hostingdiensteanbieter, die Kenntnis von Informationen erhalten, die den Verdacht begründen, dass eine Straftat, die eine Gefahr für das Leben oder die Sicherheit einer Person oder von Personen darstellt, begangen wurde, begangen wird oder begangen werden könnte, unverzüglich die Strafverfolgungs- oder Justizbehörden zu informieren und ihnen einschlägige Informationen zur Verfügung zu stellen. Die Straftaten werden zwar nicht konkret genannt, aber in Erwägungsgrund 56 des DSA wird darauf hingewiesen, dass darunter Straftaten im Sinne der Richtlinie 2017/541 zur Terrorismusbekämpfung fallen sollten, also etwa die Aufstachelung zum Terrorismus.

Die Europäische Kommission hat unter Berufung auf ihre Untersuchungs- und Durchsetzungsbefugnisse im Rahmen des DSA bereits förmliche Verfahren gegen VLOPs eingeleitet, etwa gegen X wegen unzureichender Bewertung des Risikos der Verbreitung terroristischer Inhalte (insbesondere im Zusammenhang mit den Terroranschlägen der Hamas gegen Israel),[443] auf Grundlage der Konzeption und dem Betrieb des Dienstes.[444] In Zukunft wird sich aufgrund der Transparenz- und Berichtspflichten im Rahmen der TCO-VO und des DSA besser beurteilen lassen, inwieweit Vermittler terroristischen Inhalten

[439] Erwägungsgründe 53 und 55 DSA.
[440] Siehe Erwägungsgrund 86 DSA.
[441] Artikel 5 Absatz 4 TCO-VO.
[442] Artikel 3 bis 5 TCO-VO und Erwägungsgrund 40 TCO-VO.
[443] Europäische Kommission, „Kommission leitet im Rahmen des Gesetzes über digitale Dienste ein förmliches Verfahren gegen X ein", Pressemitteilung, 18. Dezember 2023.
[444] Commission Decision initiating proceedings pursuant to Article 66(1) of Regulation (EU) 2022/2065, COM(2023) 9137 final, 2023.

ausgesetzt sind und welche Maßnahmen sie ergreifen, um die Verbreitung solcher Inhalte zu verhindern.

4.2 Beispiel Deutschland

Dr Sandra Schmitz-Berndt, Wissenschaftliche Mitarbeiterin, Institut für Europäisches Medienrecht (EMR)

4.2.1 Nationaler Rechtsrahmen für Plattformen

Nach der Annahme des DSA wurde die Plattformregulierung in Deutschland mehrfach geändert, unter anderem durch die Verabschiedung des Digitale-Dienste-Gesetzes (DDG)[445] zur Umsetzung des DSA. Das DDG gilt, soweit darin nichts anderes bestimmt ist, für alle digitalen Dienste im Sinne von Artikel 1 Absatz 2 Buchstabe b des DSA. Das DDG ähnelt auch im Aufbau dem DSA und vereint die bereits bestehenden Regelungen für Vermittler in einem einzigen Rechtsakt, einschließlich der relevanten Elemente der nationalen Umsetzung der AVMD-RL und der Haftungsausschlüsse für Vermittler. Es ergänzt den DSA mit der Zuweisung von Zuständigkeiten, darunter die Benennung des Bundeskriminalamts (BKA)[446] als zuständige Behörde für Verdachtsmeldungen zu Straftaten nach Artikel 18 des DSA.[447] Die zuständige Behörde für die Aufsicht über die Anbieter von Vermittlungsdiensten und die Durchsetzung des DSA ist die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA), die als Koordinator für digitale Dienste (KDD) für Deutschland fungiert. Der KDD handelt bei der Wahrnehmung der ihm übertragenen Aufgaben und Befugnisse völlig unabhängig. Das DDG regelt auch, welche Sanktionen bei Verstößen gegen den DSA verhängt werden können.

Obwohl sich der nationale Rechtsrahmen mit der Annahme des DSA erheblich geändert hat, lohnt sich ein Blick auf die bis dahin bestehende Rechtslage, insbesondere auf das Netzwerkdurchsetzungsgesetz (NetzDG),[448] das sowohl innerhalb als auch außerhalb Deutschlands große Aufmerksamkeit erregt hat[449] und als Maßnahme gilt, die den DSA und auch schon die TCO-VO inspiriert hat.[450] Das NetzDG enthielt eine Liste von Straftatbeständen, die „rechtswidrige Inhalte" darstellen, und verpflichtete die Anbieter

---

[445] Bundesgesetzblatt (BGBl), 2024 I Nr. 149.

[446] Das BKA ist die Zentralstelle der deutschen Kriminalpolizei.

[447] Siehe § 13 DDG.

[448] Netzwerkdurchsetzungsgesetz (NetzDG) vom 1. September 2017, BGBl. I, S. 3352.
Für einen Überblick über die ursprüngliche Fassung des NetzDG siehe Schmitz S., Berndt C., *The German Act on Improving Law Enforcement on Social Networks (NetzDG): A Blunt Sword?*, 2018.

[449] Zu der kontroversen Debatte siehe Schulz W., „Regulating Intermediaries to Protect Privacy Online – the Case of the German NetzDG" in Schulz W. , Kettemann M.C., Heldt A.P. (Hrsg.), *Probleme und Potenziale des NetzDG – ein Reader mit fünf HBI-Expertisen*, *Arbeitspapiere des Hans-Bredow-Instituts*, 48, 2019, S. 13 ff.

[450] Holznagel, D., „*Chapter II des Vorschlags der EU-Kommission für einen Digital Services Act – Versteckte Weichenstellungen und ausstehende Reparaturen bei den Regelungen zu Privilegierung, Haftung & Herkunftslandprinzip für Provider und Online-Plattformen*", *Computer und Recht,* 2021, S. 123–132; Kahl J., Liepert S., „Digital Services Act: *Was sich gegenüber dem NetzDG ändert*", heise online (9. Dezember 2022).

sozialer Netzwerke, ein wirksames und transparentes Verfahren für den Umgang mit Beschwerden über solche rechtswidrigen Inhalte zur Verfügung zu stellen.[451] Nach diesem Verfahren war ein Anbieter verpflichtet, offensichtlich rechtswidrige Inhalte in der Regel innerhalb von 24 Stunden zu entfernen.[452] Zudem musste der Anbieter ein wirksames und transparentes Verfahren zur Verfügung stellen, nach dem sowohl der Beschwerdeführer als auch der Nutzer, dessen Inhalt gemeldet wurde, eine Überprüfung der Entscheidung zur Entfernung des Inhalts beantragen kann. Darüber hinaus waren die in den Anwendungsbereich des NetzDG fallenden sozialen Netzwerke verpflichtet, „rechtswidrige Inhalte", die einen der in § 3a des NetzDG genannten Straftatbestände erfüllen, an das BKA zu melden, das dafür eine Zentrale Meldestelle für strafbare Inhalte im Internet (ZMI BKA) eingerichtet hatte. Zu diesen Straftaten gehörten die Verbreitung von Propagandamitteln terroristischer Vereinigungen, die Verwendung von Symbolen terroristischer Vereinigungen und die Bildung terroristischer Vereinigungen. Darüber hinaus wurde eine halbjährliche Berichtspflicht eingeführt, um einen Einblick in das Beschwerdemanagement zu erhalten; hinzu kam eine Berichtspflicht über die Bemühungen zur Unterbindung „strafbarer Handlungen", einen Kennzeichnungsmechanismus, die Umsetzung der Inhaltsmoderation und Einzelheiten zu den Entscheidungsprozessen.[453] Die Informationen über die Moderationspraktiken betrafen auch die beruflichen Qualifikationen der menschlichen Moderatoren, einschließlich ihrer sprachlichen Kompetenz, eine Anforderung, die nun auch im DSA enthalten ist. Mit dem Inkrafttreten des DSA im Jahr 2024 wurden große Teile des NetzDG aufgehoben, wobei nur die Verpflichtung zur Benennung eines Zustellungsbevollmächtigten bestehen blieb,[454] während die Verpflichtungen der Anbieter nun, wie oben erwähnt, in das DDG integriert sind.

Zur Haftung von Plattformanbietern für Inhalte Dritter gibt es eine umfangreiche Rechtsprechung deutscher Gerichte bis hin zum Bundesgerichtshof (BGH),[455] die sich vor allem mit der Anwendbarkeit des Haftungsausschlusses der früher geltenden deutschen Umsetzung von Artikel 14 der EC-RL (nun durch Artikel 6 des DSA ersetzt), dem Umfang von Takedown-and-Staydown-Pflichten sowie der Störerhaftung befasst. Bei Letzterer handelt es sich um eine aus dem Sachenrecht abgeleitete verschuldensunabhängige Haftung, die Eigentümer berechtigt, die Beseitigung und Unterlassung von Eigentumsstörungen zu verlangen, auch wenn diese nicht unmittelbar durch die vom Eigentümer angesprochene Person verursacht wurden.[456] Sobald ein Plattformbetreiber auf

[451] §§ 1 und 3 NetzDG.
[452] § 1 II NetzDG.
[453] § 2 NetzDG.
[454] § 5 NetzDG.
[455] Der BGH ist das oberste Gericht Deutschlands für Zivil- und Strafsachen.
[456] § 1004 des Bürgerlichen Gesetzbuchs (BGB); vgl. BGH, Internet-Versteigerung (11. März 2004), I ZR 304/01 36; BGH, Internet-Versteigerung II (19. April 2007), I ZR 35/04; BGH, Internet-Versteigerung III (30. April 2008), I ZR 73/05. Im Rahmen der Störerhaftung haftet eine Person (indirekt) für die Ermöglichung oder Erleichterung der rechtswidrigen Handlung einer anderen Person, auch wenn sie die rechtswidrige Handlung nicht selbst begangen hat; um die Haftung zu begründen, reicht es aus, dass die Person bei der Verursachung oder Ermöglichung der Rechtsverletzung eine Rolle gespielt hat. Somit könnte der Anbieter einer Auktionswebsite nach der oben genannten Rechtsprechung dafür haften, dass er zu einer Rechtsverletzung beigetragen hat, indem er beispielsweise die Plattform zur Verfügung stellt, die rechtswidrige Angebote ermöglicht hat, obwohl er von der rechtswidrigen Tätigkeit wusste oder hätte wissen müssen, und nichts unternommen hat, obwohl er die technischen Möglichkeiten hatte, die Rechtsverletzung zu stoppen oder zu verhindern.

eine Rechtsverletzung hingewiesen wird, muss er dem Geschädigten nicht nur Unterlassung zusichern, sondern auch Präventivmaßnahmen sicherstellen.

Im digitalen Bereich wird die nationale Gesetzgebung zunehmend durch EU-Rechtsakte ersetzt und ergänzt. Neben dem DSA mit seinen Haftungsregelungen und Vorschriften zur Minderung systemischer Risiken enthalten daher unter anderem auch die DSGVO, der DMA oder die TCO-VO direkt anwendbare Regeln für Plattformen, die in Deutschland wie auch in allen anderen Mitgliedsstaaten Dienste anbieten.

4.2.2 Spezifische Regeln zu terroristischen Inhalten

Das Strafgesetzbuch (StGB) enthält eine Reihe von Straftatbeständen im Zusammenhang mit Terrorismus, darunter das Verbreiten von Propagandamitteln terroristischer Organisationen,[457] das Verwenden von Kennzeichen terroristischer Organisationen,[458] die Unterstützung terroristischer Vereinigungen,[459] die öffentliche Aufforderung zu Straftaten, einschließlich terroristischer Handlungen,[460] und die Billigung terroristischer Handlungen.[461/462]

Wenn Inhalte online verbreitet werden, stößt die Durchsetzung des nationalen Strafrechts jedoch häufig an ihre Grenzen. Diese Grenzen sind entweder faktischer Art (z. B. wenn der tatsächliche Täter nicht ermittelt werden kann), justizieller Art (z. B. bei fehlendem territorialem Bezug) oder praktischer Art (z. B. weil nationales Strafrecht schwer gegen ausländische Akteure durchzusetzen ist).[463] Herausforderungen ergeben sich auch dann, wenn ein bestimmtes Verhalten wie etwa Holocaustleugnung nach deutschem Recht eine Straftat darstellt,[464] in anderen Staaten aber als legal gilt. Um sicherzustellen, dass terroristische Inhalte auf großen Social-Media-Plattformen zügig entfernt werden, hat das NetzDG die Holocaustleugnung in eine eigene Kategorie eingeordnet und die beschriebene Takedown-Regelung eingeführt (siehe 4.2.1.). Die TCO-VO verfolgt einen ähnlichen Ansatz wie das NetzDG, wobei es in erster Linie auf Hostingdiensteanbieter abzielt, die ihre Dienste innerhalb der EU anbieten.

Mit der Verabschiedung der TCO-VO und des DSA wurden neue Konformitätsebenen eingezogen, und die Takedown-and-Staydown-Pflichten fallen nun direkt unter das geltende harmonisierte EU-Recht. Allerdings waren einige Umsetzungsmaßnahmen nach nationalem Recht erforderlich, vor allem in Bezug auf die zuständigen Behörden und die Durchsetzung auf nationaler Ebene.

---

[457] Strafgesetzbuch, § 86.
[458] Ebd., § 86a.
[459] Ebd., §§ 129a-b.
[460] Ebd. § 111.
[461] Ebd.§ 140.
[462] Diese Straftaten standen alle auf der Liste der strafbaren Inhalte, die nach dem NetzDG unverzüglich entfernt werden mussten.
[463] Siehe Ukrow J., „Einleitung und Überblick“ in Cappello M. (Hrsg.), *Medienrechtsdurchsetzung ohne Grenzen, IRIS Spezial*, Europäische Audiovisuelle Informationsstelle, Straßburg, 2018, S. 3 ff.
[464] Zu § 130 StGB siehe Heger M., „§ 130 StGB“ in Lackner K., Kühl K. (Hrsg.), Strafgesetzbuch, C.H. Beck, München, 31. Aufl. 2025, Rn. 8 ff.

Deutschland benannte das BKA als zuständige Behörde für den Erlass von Entfernungsanordnungen gemäß Artikel 3 der TCO-VO und für die Prüfung der Entfernungsanordnungen von Behörden anderer EU-Mitgliedstaaten an deutsche Hostingdiensteanbieter. Darüber hinaus ist die BNetzA die zuständige Behörde für die Überwachung technischer Sicherheitsvorkehrungen und die Verhängung von Sanktionen. Die BNetzA beaufsichtigt daher die Umsetzung von spezifischen Maßnahmen wie der Inhaltsmoderation gemäß Artikel 5 der TCO-VO für in Deutschland niedergelassene Hostingdiensteanbieter und entscheidet auch gemäß Artikel 5 Absatz 4 der TCO-VO, ob ein Hostingdiensteanbieter als terroristischen Online-Inhalten ausgesetzt gelten kann.[465] Zudem ist die BNetzA für alle Bußgeldverfahren im Rahmen der TCO-VO zuständig. Das BKA ist als Kontaktstelle gemäß Artikel 12 Absatz 2 der TCO-VO zuständig für die Entgegennahme von Meldungen gemäß Artikel 14 Absatz 5 der TCO-VO über Inhalte, die zu einer unmittelbaren Bedrohung von Leben führen. Sowohl das BKA als auch die BNetzA müssen unter anderem Informations- und Transparenzberichte gemäß Artikel 8 der TCO-VO veröffentlichen.[466] Zur Durchsetzung der oben genannten Anordnungen gemäß Artikel 3 Absatz 1 und Artikel 5 Absatz 6 der TCO-VO kann nach dem Verwaltungsvollstreckungsgesetz (VwVG) ein Zwangsgeld von bis zu EUR 5 Millionen verhängt werden.[467] Darüber hinaus enthält § 6 des Terroristische-Online-Inhalte-Bekämpfungsgesetzes (TerrOIBG)[468] detaillierte Bußgeldvorschriften, die Bußgelder für natürliche Personen von bis zu EUR 5 Millionen und für juristische Personen von bis zu 4 % des weltweiten Jahresumsatzes vorsehen.

Neben diesen rechtlichen Rahmenbedingungen hat die ZMI BKA, die als zentrale Meldestelle für Verdachtsmeldungen zu Straftaten im Rahmen des NetzDG eingerichtet wurde und diese Aufgabe für Straftaten mit Bedrohung von Menschenleben im Rahmen des DSA fortführt, auch eine freiwillige Kooperation mit Interessenträgern zur Bekämpfung von Hasskriminalität eingerichtet. Auch wenn deren Schwerpunkt auf Hasskriminalität liegt, beschränkt sich ihr Tätigkeitsbereich nicht auf Hass und Hetze. Die Nutzer können diesen Interessenträgern hetzerische oder extremistische Inhalte melden, und diese bewerten den Inhalt dann. Wenn er strafrechtlich relevant ist, leiten sie die Meldung an die ZMI BKA zur weiteren zusammenfassenden Beurteilung und zur Identifizierung des potenziellen Täters weiter. Der Status eines Kooperationspartners als vertrauenswürdiger Hinweisgeber (Trusted Flagger) im Rahmen des DSA hat auf die Beurteilung keinen Einfluss; Hostingdiensteanbieter sind lediglich verpflichtet, Meldungen vertrauenswürdiger Hinweisgeber vorrangig zu bearbeiten. Kooperationspartner sind bisher das Land Hessen,[469] eine Stiftung,[470] die Medienaufsichtsbehörden der Länder und Staatsanwaltschaften.[471] Diese Meldewege sind als niedrigschwelliges Angebot gedacht, das die Möglichkeit einer Anzeige bei einer Strafverfolgungsbehörde ergänzt. Relevant ist die Arbeit der ZMI BKA im

[465] Dies ist im Durchführungsgesetz geregelt, dem *Terroristische-Online-Inhalte-Bekämpfungs-Gesetz* (TerrOIBG).
[466] Ebd., § 4.
[467] Ebd., § 5.
[468] Gesetz zur Durchführung der TCO-Verordnung, TerrOIBG.
[469] Das die *Meldestelle HessenGegenHetze* für *Hate Speech* und Extremismus betreibt.
[470] Die Jugendstiftung beim Demokratiezentrum Baden-Württemberg betreibt REspect!, ein Meldeportal für Hass und Hetze.
[471] So betreibt beispielsweise die Staatsanwaltschaft Göttingen als Zentralstelle zur Bekämpfung von Hasskriminalität im Internet in Niedersachsen ein Meldetool auf einer eigenen Website.

Zusammenhang mit terroristischen Online-Inhalten aufgrund der Tatsache, dass die ZMI BKA mit den Medienaufsichtsbehörden zusammenarbeiten muss, um Verfahren zur Entfernung illegaler Inhalte einzuleiten. Diese Behörden sind nach dem deutschen Jugendmedienschutz-Staatsvertrag (JMStV) für die Entfernung eines Katalogs[472] rechtswidriger Inhalte zuständig, wozu auch terroristische Straftaten gehören, einschließlich der Schilderung grausamer oder sonst unmenschlicher Gewalttätigkeiten gegen Menschen in einer Art, die eine Verherrlichung oder Verharmlosung solcher Gewalttätigkeiten ausdrückt.[473] Die Durchsetzungsbefugnisse erstrecken sich auf Bußgelder und weitere Zwangsmaßnahmen im Verwaltungsrecht.

Die Medienaufsichtsbehörden haben zudem Durchsetzungsbefugnisse zur Bekämpfung strafrechtlich relevanter Inhalte nach dem deutschen Medienstaatsvertrag (MStV), der auch für Internetvermittler gilt. Die Durchsetzungsbefugnisse erstrecken sich auch auf Zugangsanbieter, wenn der Inhaltsanbieter oder der Hostingdienstanbieter einer ersten Anordnung zur Entfernung der betreffenden rechtswidrigen Inhalte nicht nachkommt. Insbesondere hat eine Medienaufsichtsbehörde als Ultima Ratio eine Sperrungsverfügung gegen große deutsche Zugangsanbieter erlassen, um den Zugang zu Pornografie-Plattformen zu sperren.[474]

4.2.3 Anwendung nach dem Terroranschlag der Hamas in Israel im Oktober 2023

Nach dem terroristischen Angriff der Hamas in Israel am 7. Oktober 2023 waren Internetnutzer in einem noch nie dagewesenen Ausmaß terroristischem Material ausgesetzt. Während des Angriffs nutzte die Hamas gezielt Internettechnologien, unter anderem indem sie ihre Gräueltaten mit Hilfe von Mobiltelefonen und Bodycams live auf Plattformen wie Telegram und Facebook streamte.[475] Die Inhalte wurden auch in Echtzeit bearbeitet und über Social-Media-Plattformen verbreitet.[476] In der Folge waren Social-Media-Plattformen zudem hetzerischen Narrativen ausgesetzt, die mit Hashtags wie #freepalestine geframt wurden. Anders als in den meisten anderen EU-Mitgliedstaaten haben die Regulierungsbehörden in Deutschland schnell reagiert und die TCO-VO aktiv genutzt. Gründe für die zügige Nutzung der Möglichkeiten der TCO-VO sind zum einen die historische und rechtliche Sensibilität Deutschlands gegenüber Antisemitismus und Terrorismus; zum anderen hatten die Behörden bereits eine gewisse Erfahrung mit der

[472] Siehe § 4 JMStV und Ukrow J., „§ 4 JMStV" in Cole M.D., Oster J., Wagner E.E. (Hrsg.), *Medienstaatsvertrag, Jugendmedienschutz-Staatsvertrag (HK-MstV)*, C.F. Müller, Heidelberg, 104. ergänzte Aufl., September 2025.
[473] Siehe § 20 JMStV. Der JMStV enthält in § 5b auch eine Verpflichtung für VSP-Anbieter, ein Meldeverfahren für rechtswidrige Inhalte einzurichten. Diese Verpflichtung ist als unionsrechtswidrig kritisiert worden, weil sie die vollharmonisierende Wirkung des DSA missachtet, und hat bisher keine praktische Bedeutung, vgl. Liesching M., „§ 5b JMStV" in Liesching M. (Hrsg.), *BeckOK Jugendschutzrecht*, C.H. Beck, München, 5. Aufl. 2025, Rn. 2.
[474] Siehe Schmitz-Berndt S., „Verwaltungsgericht Berlin lehnt im Eilverfahren Antrag auf vorläufigen Rechtsschutz von Pornoplattformen gegen Sperrverfügung der zuständigen Landesmedienanstalt ab", *IRIS* 2025-6:1/18, Europäische Audiovisuelle Informationsstelle, 2025.
[475] Cortellessa E., „The Oct. 7 Massacre Revealed a New Hamas Social Media Strategy", *TIME*, 31. Oktober 2023.
[476] Loucaides D., „How Telegram Became a Terrifying Weapon in the Israel-Hamas War", *WIRED*, 31. Oktober 2023.

zentralen Meldestelle ZMI BKA, die schon im Rahmen des NetzDG die gleiche Funktion hatte wie jetzt unter Artikel 18 des DSA, nämlich als zuständige Behörde für die Entgegennahme von Verdachtsmeldungen zu Straftaten. Am Beispiel des Hamas-Angriffs und seiner Nachwirkungen mit einer erheblichen Zunahme von rechtswidrigen Inhalten, Desinformation und Hetze in den sozialen Medien[477] lässt sich zeigen, wie die Takedown-Regelung der TCO-VO in der Praxis funktioniert.

Wie bereits ausgeführt, haben die zuständigen Behörden von sechs Mitgliedstaaten auf der Grundlage der TCO-VO von Juni 2022 bis 31. Dezember 2023 insgesamt 349 Entfernungsanordnungen ausgestellt. Die meisten – 249 – davon kamen aus Deutschland.[478] Alle diese Anordnungen waren an Hostingdiensteanbieter außerhalb Deutschlands gerichtet und wurden umgesetzt. Umgekehrt haben die zuständigen Behörden anderer Mitgliedstaaten nur zwei Entfernungsanordnungen gegen deutsche Hostingdiensteanbieter erlassen. Beim Erlass von Anordnungen und bei der Prüfung grenzüberschreitender Anträge kann das BKA mit den Landesmedienanstalten zusammenarbeiten. Hierbei ist regelmäßig die Landesanstalt für Medien Nordrhein-Westfalen als Vertreterin aller Landesmedienanstalten beteiligt.

Die meisten Anordnungen betrafen mit Stand 21. November 2023 den Angriff der Hamas auf Israel im Oktober 2023 und waren an Telegram gerichtet.[479] Zwischen dem 7. Oktober und dem 21. November 2023 erließ das BKA gegen Telegram und X 153 Entfernungsanordnungen wegen Propaganda der Hamas und des Palästinensischen Islamischen Dschihad.[480] Insgesamt scheint diese Zahl nicht sehr hoch zu sein, weil das BKA vor dem Erlass einer Entfernungsanordnung regelmäßig das Instrument des „Löschersuchens" nutzt, das eine Aufforderung an die Hostingdiensteanbieter darstellt, freiwillig zu reagieren.

Im Jahr 2023 übermittelte das BKA 7240 Löschersuchen, von denen 5762 dazu führten, dass die betreffenden Inhalte entfernt oder gesperrt wurden. Da diese Löschersuchen nicht bindend sind, besteht keine Verpflichtung, sie innerhalb eines bestimmten Zeitraums zu bearbeiten. Das BKA prüft jedoch nach zwei Arbeitstagen, ob die Inhalte entfernt oder deaktiviert wurden.[481] Diese Frist erfüllt das Erfordernis des „zügigen" Tätigwerdens im Rahmen des Haftungsausschlusses für Hostingdiensteanbieter nach Artikel 6 Absatz 1 des DSA. Reagiert ein Hostingdiensteanbieter nicht innerhalb dieser Frist, erlässt das BKA nötigenfalls eine Entfernungsanordnung. Entfernungsanordnungen können auch direkt erlassen werden, also ohne Ersuchen um freiwillige Entfernung. Tatsächlich hat das BKA als Reaktion auf die oben erwähnten Inhalte der Hamas und des Palästinensischen Islamischen Dschihad im Oktober 2023 zunächst Löschersuchen verschickt und anschließend, weil darauf nicht reagiert wurde, Entfernungsanordnungen erlassen.

Die BNetzA stufte 2023 den ersten deutschen Hostingdiensteanbieter als terroristischen Inhalten ausgesetzt ein und forderte ihn nach Artikel 5 der TCO-VO auf, die

---

[477] Bundesministerium des Innern, „*Wellen des Hasses stoppen*", Pressemitteilung, 13. Februar 2024.
[478] BKA, *Umsetzung der TCO-Verordnung im Bundeskriminalamt, Transparenzbericht für das Jahr 2023*, 2024.
[479] Siehe Deutscher Bundestag, „*Antwort der Bundesregierung auf die kleine Anfrage der Fraktion der CDU/CSU – Drucksache 20/9299 – Social-Media-Terrorismus*", 2023, BT-Drs. 20/9688.
[480] Entfernungsanordnungen wurden gegen X (10 Fälle) und Telegram (143 Fälle) erlassen, siehe ebd.
[481] BNetzA, „Transparenzbericht nach Art. 8 TCO-VO und § 4 TerrOIBG sowie Monitoringbericht nach Art. 21 Abs. 1 TCO-VO und § 3 TerrOIBG", 2024, S. 7.

erforderlichen Maßnahmen zu ergreifen, um sicherzustellen, dass über seine Dienste keine terroristischen Inhalte öffentlich verbreitet werden.[482] Der Einstufung waren eine Vielzahl von Löschersuchen des BKA und zwei Entfernungsanordnungen vorausgegangen.[483] Der Anbieter verstärkte daraufhin seine technischen und organisatorischen Maßnahmen gegen die Verbreitung terroristischer Online-Inhalte.

Nach Ansicht von BNetzA und BKA sind die ergriffenen Maßnahmen grundsätzlich geeignet, um die Verbreitung terroristischer Online-Inhalte auf der Plattform des betroffenen Hostingdiensteanbieters einzudämmen, und die Effektivität der Maßnahmen konnte im Berichtszeitraum 2024 deutlich erhöht werden. Die Eigenständigkeit des Hostingdiensteanbieters bei der Identifizierung terroristischer Online-Inhalte sowie der Wirksamkeit seiner Maßnahmen wird derzeit evaluiert. Eine Umfrage unter Hostingdiensteanbietern ergab eine Reihe unterschiedlicher Maßnahmen, die ergriffen wurden: organisatorische Maßnahmen (z. B. bei den Nutzungsbedingungen), technische Maßnahmen (z. B. automatische Erkennung extremistischer Emoji-Kombinationen, Restriktionen für Benutzernamen, URLs und gesperrte Accounts) sowie manuelle Maßnahmen (z. B. Moderationsteams, Prüfung von Trends und Umgehungstaktiken).[484] Im Jahr 2023 wurden von dem als terroristischen Inhalten ausgesetzt eingestuften Hostingdiensteanbieter insgesamt 15 766 Inhalte aufgrund spezifischer Maßnahmen nach Artikel 5 der TCO-VO entfernt.[485] In 100 Fällen reichten Nutzerinnen und Nutzer gegen die Entfernung ihrer Inhalte Beschwerde ein, was in neun Fällen zur Wiederherstellung der Inhalte führte.[486]

Im Jahr 2023 gingen bei Hostingdiensteanbietern 139 Anträge zuständiger Behörden auf Zugang zu Nutzerdaten im Zusammenhang mit terroristischen Inhalten oder Aktivitäten ein,[487] im Jahr 2024 dagegen nur vier.[488] Dies unterstreicht die Notwendigkeit eines Mechanismus für eine rasche Entfernung parallel zu strafrechtlichen Ermittlungen, insbesondere angesichts der Zunahme der Löschersuchen und Entfernungsanordnungen. Im Jahr 2024 erließ das BKA 482 Entfernungsanordnungen und erreichte eine Umsetzungsquote von 95,9 %.[489] Zudem prüfte das BKA elf Entfernungsanordnungen ausländischer Stellen, von denen keine beanstandet wurde, und übermittelte 17 045 Löschersuchen an Hostingdiensteanbieter (wovon 87,4 % zur Entfernung oder Sperrung der Inhalte führten).[490]

Neben dem Rahmen der TCO-VO stützt sich die ZMI BKA auf ihr Verfahren zur freiwilligen Kooperation mit Online-Meldeportalen für Hetze. Vom 7. Oktober bis zum

---

[482] Ebd.
[483] Ebd., S. 7.
[484] BNetzA, „Transparenzbericht nach Art. 8 TCO-VO und § 4 TerrOIBG sowie Monitoringbericht nach Art. 21 Abs. 1 TCO-VO und § 3 TerrOIBG“, 2025, S. 8 ff.
[485] BNetzA, „Transparenzbericht nach Art. 8 TCO-VO und § 4 TerrOIBG sowie Monitoringbericht nach Art. 21 Abs. 1 TCO-VO und § 3 TerrOIBG“, 2024, S. 8.
[486] Ebd.
[487] Ebd.
[488] BNetzA, „Transparenzbericht nach Art. 8 TCO-VO und § 4 TerrOIBG sowie Monitoringbericht nach Art. 21 Abs. 1 TCO-VO und § 3 TerrOIBG“, 2025, S. 9.
[489] BKA, „Transparenzbericht 2024 zur Bekämpfung terroristischer Online-Inhalte veröffentlicht“, Pressemitteilung, 2025.
[490] Ebd., S. 1.

20. November 2023 gingen beim BKA aus dieser Quelle beispielsweise insgesamt 139 Meldungen ein, die als Volksverhetzung (§ 130 StGB) strafrechtlich relevant sind und einen Bezug zum Nahostkonflikt aufweisen.[491]

Auch Plattformanbieter haben dem BKA nach Artikel 18 des DSA Inhalte gemeldet. Von Oktober 2023 bis Dezember 2023 wurden nur 16 Meldungen abgegeben, was hauptsächlich darauf zurückzuführen ist, dass die Verpflichtungen damals nur für benannte VLOPSEs galten, für andere Vermittler dagegen erst seit dem 17. Februar 2024. Von den 1773 Meldungen im Jahr 2024 waren 1244 strafrechtlich relevant, wobei nur neun Meldungen speziell den Terrorismus betrafen.[492]

Die genaue Zahl der Entfernungsanordnungen, Löschersuchen und sonstigen Meldungen sowie der effektiven Takedowns im Zusammenhang mit dem Angriff der Hamas lässt sich nur schwer ermitteln. Im Februar 2024 erklärte die Bundesinnenministerin, im Zeitraum vom 7. Oktober 2023 bis zum 6. Februar 2024 habe sich die Gesamtzahl der Löschersuchen wegen terroristischer Inhalte im Zusammenhang mit dem Hamas-Anschlag auf über 3500 belaufen.[493] Daraufhin seien 290 Entfernungsanordnungen erlassen worden.[494]

Die obigen Zahlen sind signifikant und deuten darauf hin, dass die Zunahme terroristischer Inhalte mit einem Anstieg der Takedown-Maßnahmen einherging. Die rasche Reaktion ist vor allem darauf zurückzuführen, dass die entsprechende Infrastruktur und der institutionelle Rahmen schon vor dem Inkrafttreten der TCO-VO vorhanden waren und die jeweiligen Akteure bereits Erfahrung hatten. Auch die strengen Vorgaben des inzwischen aufgehobenen NetzDG könnten dazu beigetragen haben, die Anbieter für eine zügige Reaktion auf Takedown-Ersuchen zu sensibilisieren.

4.3 Beispiel Türkiye

Dr Mehmet Bedii Kaya, Außerordentlicher Professor für IT-Recht, Bilgi-Universität Istanbul

4.3.1 Nationaler Rechtsrahmen für Plattformen

Die Republik Türkiye ist Mitglied des Europarats und der Organisation für Sicherheit und Zusammenarbeit in Europa sowie Beitrittskandidat zur EU. Die Internetdurchdringung der Bevölkerung ist in dem Land bemerkenswert hoch. Nach Angaben des türkischen

[491] Siehe Deutscher Bundestag, „*Antwort der Bundesregierung auf die kleine Anfrage der Fraktion der CDU/CSU – Drucksache 20/9299 – Social-Media-Terrorismus*“, 2023, BT-Drs. 20/9688, S. 5.
[492] Von den strafrechtlich relevanten Inhalten bezogen sich 1046 auf Sexualdelikte zum Nachteil von Kindern und Jugendlichen. Das als nicht strafrechtlich relevant eingestufte Material betraf hauptsächlich Suizidankündigungen, die zwar keinen Straftatbestand, aber eine ernsthafte Bedrohung für das Leben darstellen. Siehe Bundesregierung, *Bericht der Bundesregierung gemäß § 13 Satz 2 des Digitale-Dienste-Gesetzes*vom 27. August 2025.
[493] *Bundesministerium des Inneren*, „*Wellen des Hasses stoppen*“, op. cit.
[494] Ebd.

Statistikinstituts hat die Internetnutzung zwischen 2004 und 2024 von 27 % auf etwa 97 % zugenommen, was einer 3,6-fachen Steigerung innerhalb von zwei Jahrzehnten entspricht. Aktuelle Nutzungsmuster zeigen, dass WhatsApp, Instagram und YouTube die am häufigsten genutzten Social-Media-Plattformen sind. Dabei dominiert YouTube mit einem Anteil von 46,1 % am gesamten Datenverbrauch, gefolgt von Instagram mit 13 % und Netflix mit 5,9 %.[495] Diese Zahlen unterstreichen einen Trend im Nutzerverhalten, der stark auf videobasierte Inhalte ausgerichtet ist, wobei Social-Media-Plattformen einen erheblichen Anteil am gesamten Internetverkehr in Türkiye ausmachen.

In der Verfassung der Republik Türkiye sind die wichtigsten bürgerlichen Freiheiten verankert, darunter das Recht auf freie Meinungsäußerung, die Pressefreiheit und der Schutz der körperlichen und geistigen Unversehrtheit des Einzelnen. Während sich der nationale Rechtsrahmen vieler Länder an den Standards der EU orientiert, passt Türkiye als Nichtmitglied diese Normen an die nationalen Prioritäten und den soziopolitischen Kontext an. Die Verfassung enthält keine spezifischen Bestimmungen zur Technologie. Mit einer wichtigen Änderung im Jahr 2010 wurde jedoch eine Bestimmung zum Schutz personenbezogener Daten eingeführt. In Artikel 20 Absatz 3 der Verfassung wird das Recht auf den Schutz personenbezogener Daten ausdrücklich anerkannt.

Türkiye hat eine umfassende Regulierungsinfrastruktur entwickelt, die darauf abzielt, im physischen wie auch im digitalen Bereich die öffentliche Ordnung zu wahren. Im Laufe der Zeit haben sich Umfang und Intensität dieser Regulierungsmaßnahmen ausgeweitet, was einen Trend zu immer strengeren Kontrollen widerspiegelt.

Das wichtigste Rechtsinstrument, das die Internetaktivitäten in Türkiye regelt, ist das Gesetz Nr. 5651 *İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun* (*Gesetz über die Regulierung von Sendungen über das Internet und die Verhinderung von Straftaten, die durch solche Sendungen begangen werden* – Internetgesetz).[496]

Das Internetgesetz regelt im Wesentlichen drei Bereiche:[497]

1) die rechtlichen, strafrechtlichen und administrativen Verantwortlichkeiten der wichtigsten Internetakteure, darunter Inhaltsanbieter, Hostinganbieter, Internetdiensteanbieter, öffentliche Internetanbieter und Anbieter sozialer Netzwerke;[498]
2) die Verfahren zur Beschränkung des Zugangs bei bestimmten Straftaten, insbesondere in Notfällen;

[495] Zu allen Zahlen siehe Bilgi Teknolojileri ve İletişim Kurumu (türkische Behörde für Informations- und Kommunikationstechnologien), „*Türkiye Elektronik Haberleşme Sektörü, Üç Auylik Pazar Verileri Raporu*“ (Elektronische Kommunikation, vierteljährlicher Marktdatenbericht), 2025, S. 54-56.

[496] *5651 İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun*, ABl. 23. Mai 2007/26530. Eine vollständige englische Übersetzung des türkischen Internetgesetzes findet sich hier.

[497] Die Bestimmungen zum Schutz der Persönlichkeitsrechte wurden vom türkischen Verfassungsgericht für nichtig erklärt. Neue Vorschriften, die diese Bestimmungen ersetzen sollen, sind noch nicht erlassen worden.

[498] Für einen umfassenden Überblick über das türkische Internetgesetz siehe Kaya, M.B., „The regulation of Internet intermediaries under Turkish law: Is there a delicate balance between rights and obligations?“, *Computer Law & Security Review* 32, 2016, S. 759 ff.

3) die Einführung von Internet-Filtermechanismen und Überwachungspraktiken.

Seit seiner ursprünglichen Verabschiedung wurde das Internetgesetz mehrfach geändert, insbesondere 2014, 2020 und 2022, um den sich verändernden politischen Prioritäten und technologischen Entwicklungen Rechnung zu tragen. Neben den Gesetzesreformen haben auch gerichtliche Auslegungen, insbesondere die Urteile des türkischen Verfassungsgerichts zu Plattformen wie Twitter und YouTube, wesentlich dazu beigetragen, dass sich das Verständnis und die Anwendung des Gesetzes weiterentwickeln.[499]

Anfangs diente das Internetgesetz als wichtigstes Instrument der Internetregulierung in Türkiye, doch die Gesetzeslandschaft hat sich seither so entwickelt, dass zahlreiche Institutionen im Rahmen ihres jeweiligen gesetzlichen Mandats Befugnisse erhalten haben. Daher kann nun eine Vielzahl öffentlicher Stellen rechtswidrige Online-Inhalte ermitteln, entfernen und sperren. Diese Dezentralisierung hat zu einem fragmentierten rechtlichen und institutionellen Rahmen geführt. Trotz der Zunahme ergänzender gesetzlicher Bestimmungen, die sich mit internetbezogenen Fragen befassen, bleibt das Internetgesetz das grundlegende Gesetz zur Regelung von Online-Inhalten und der Verantwortlichkeiten digitaler Vermittler.

Wie bereits erwähnt, regelt das Internetgesetz in erster Linie bestimmte Kategorien von Akteuren, darunter Inhaltsanbieter, Hostinganbieter, Internetdiensteanbieter, öffentliche Internetzugangsanbieter und Anbieter sozialer Netzwerke. Unter diesen nehmen Hostinganbieter eine zentrale Rolle ein. Gemäß Artikel 2 Absatz 1 Buchstabe m des Internetgesetzes sind Hostinganbieter definiert als „natürliche oder juristische Personen, die Systeme anbieten, die Dienste und Inhalte hosten".

Die für Hostinganbieter geltenden Rechtsvorschriften umfassen ein breites Spektrum von Plattformen mit unterschiedlichen Funktionen, Betriebsmodellen und technischen Architekturen. Dazu gehören herkömmliche Webhostingdienste wie Shared Hosting, Cloud-basiertes Hosting, virtuelle private Server (VPS), dedizierte Server, Colocation-Dienste und virtuelle private Netzwerke (VPN) sowie Plattformen, die Datei-, Bild-, Video-, Blog- und E-Mail-Hosting anbieten. Der Kreis erstreckt sich auch auf soziale Netzwerke, Suchmaschinen, Online-Auktionsplattformen, digitale Marktplätze und andere Online-Plattformanbieter.[500]

Das Internetgesetz reicht nicht aus, um die vielfältigen Hostinganbieter mit ihren ganz unterschiedlichen Betriebsmodellen angemessen zu regulieren. Insbesondere sieht es vor, dass Hostinganbieter je nach Art ihrer Dienste klassifiziert und hinsichtlich ihrer Rechte und Pflichten auf Basis von Grundsätzen und Verfahren, die im Sekundärrecht festzulegen sind, differenziert werden können. Diese Bestimmung wurde 2014 in das Internetgesetz aufgenommen,[501] doch bis heute wurde keine solche Klassifizierung in einschlägiges Sekundärrecht umgesetzt. Daher gilt derzeit für alle Online-Plattformen eine einzige Rechtsvorschrift.

---

[499] Verfassungsgericht der Republik Türkiye, *Fall Twitter*, Einzelantrag Nr. 2014/3986, 2. April 2014; *Fall YouTube*, Einzelantrag Nr. 2014/4705, 29. Mai 2014; siehe auch *Fall Internetrecht*, Entscheidungsaufruf Nr. 2014/87, Entscheidung Nr. 2015/112, 8. Dezember 2015.

[500] Siehe, Işık A., İnternet Aktörleri ve Egemenliğin Değişen Boyutları, On İki Levha Publishing, 2023.

[501] Änderung durch Gesetz Nr. 6518, ABl. 19. Februar 2014/28918.

Nach Artikel 5 des Internetgesetzes ist es nicht Aufgabe von Hostinganbietern, die von ihnen gehosteten Inhalte zu überwachen oder festzustellen, ob rechtswidrige Handlungen vorliegen. Ihre Haftung beschränkt sich darauf, rechtswidrige Inhalte nach einer entsprechenden Meldung gemäß dem Notice-and-Takedown-Mechanismus des Internetgesetzes zu entfernen. Sie sind verpflichtet, rechtswidrige Inhalte unverzüglich aus der öffentlichen Verfügbarkeit zu entfernen.

Die zentrale Frage, die es zu klären gilt, ist der Umfang dieser Entfernungspflicht. Insbesondere geht es darum, ob die Inhalte dauerhaft von den Servern gelöscht werden müssen oder ob es ausreicht, den Zugang für Nutzer innerhalb Türkiyes (oder den von Türkiye ausgehenden Datenverkehr) zu sperren. Diese Unklarheit ist einer der umstrittensten Aspekte des Internetgesetzes. Artikel 2 dieses Gesetzes definiert die Entfernung von Inhalten als „das Entfernen von Inhalten von den Servern oder von den gehosteten Inhalten durch Inhalts- oder Hostinganbieter". Demnach kann ein Anbieter, der technische Maßnahmen wie Geoblocking oder länderspezifische Inhaltsbeschränkungen einsetzt, nach den Bestimmungen des Internetgesetzes dennoch haftbar gemacht werden.

Das Internetgesetz sieht zudem eine breite Palette von gerichtlichen und administrativen Sanktionen für Hostinganbieter vor, die gerichtlichen Anordnungen oder Verwaltungsanweisungen nicht nachkommen oder mit den zuständigen Behörden unzureichend zusammenarbeiten.

Im Internetgesetz sind neben den Hostinganbietern nur die Anbieter sozialer Netzwerke ausdrücklich als Kategorie von Online-Plattformen definiert.[502] Diese Bezeichnung wurde im Jahr 2022 eingeführt, wobei die Gesetzesänderung vor allem vom deutschen NetzDG inspiriert war.[503]

Artikel 2 Absatz 1 Buchstabe s des Internetgesetzes definiert Anbieter sozialer Netzwerke als „natürliche oder juristische Personen, die es Nutzern ermöglichen, Text-, Bild-, Audio-, ortsbezogene oder ähnliche Daten zum Zweck der sozialen Interaktion zu erstellen, anzusehen oder zu teilen." Anbieter sozialer Netzwerke werden als eine eigene Unterkategorie von Hostinganbietern betrachtet. Wichtig ist, dass die Anwendung spezieller Bestimmungen für Anbieter sozialer Netzwerke diese nicht von den Verpflichtungen und Verantwortlichkeiten befreit, die sie als Hostinganbieter nach dem Internetgesetz haben.

Gemäß Zusatzartikel 4 des Internetgesetzes müssen ausländische Anbieter sozialer Netzwerke, die täglich mehr als eine Million Besuche aus Türkiye erhalten, mindestens einen gesetzlichen Vertreter im Land benennen. Sowohl ausländische als auch inländische Anbieter, die diesen Schwellenwert überschreiten, müssen innerhalb von 48 Stunden auf Notice-and-Takedown-Ersuchen reagieren, und jede Weigerung muss mit einer begründeten Erklärung versehen sein.

Darüber hinaus sind diese Anbieter gemäß Zusatzartikel 4 verpflichtet, halbjährliche Berichte in türkischer Sprache vorzulegen, die statistische und kategorische

[502] Änderung durch Gesetz Nr. 7253, ABl. 31. Juli 2020/31202.
[503] Für einen umfassenden Überblick über die Regulierung sozialer Medien siehe Kaya M.B., Akıncı M.F., „Social Media Regulation" in Eroğlu M., Finger M., Köksal E. (Hrsg.), *The Economics and Regulation of Digitalisation: The Case of Türkiye*, Routledge, Abingdon, 2024. Siehe auch oben unter 4.2.1f zum *NetzDG*.

Daten über die Umsetzung von Entscheidungen zur Entfernung und Sperrung von Inhalten enthalten. Die Nichteinhaltung dieser Verpflichtungen kann zu Bußgeldern führen, wobei die Strafen für ausländische Anbieter bis zu einer Million türkische Lira betragen können.

Das wichtigste Instrument, das im Rahmen des Internetgesetzes zur Bekämpfung rechtswidriger Online-Inhalte eingesetzt wird, ist die Entscheidung, solche Inhalte zu sperren und zu entfernen. Die wichtigste Methode, um gegen Rechtsverletzungen im Internet vorzugehen, ist die Entfernung von Inhalten, die durch Gerichtsbeschlüsse oder unter bestimmten Bedingungen durch Verwaltungsbehörden als illegal eingestuft wurden. Wird der Inhalt nicht entfernt, wird die konkrete URL, unter der sich das rechtswidrige Material befindet, gesperrt; ist dies technisch nicht machbar, kann der Zugriff auf die gesamte Website eingeschränkt werden.

Das Internetgesetz gibt einen allgemeinen Rahmen für das Vorgehen gegen verschiedene Formen rechtswidriger Inhalte vor. Dazu gehören:

1) Artikel 8 – Bekämpfung spezifischer Straftaten;
2) Artikel 8/A – Ermöglichung von Zugangsbeschränkungen in Notsituationen.

Eine zentrale Rolle bei der Verwaltung der türkischen Kommunikationsinfrastruktur und bei der Vollstreckung von Entscheidungen über Zugangssperren gemäß dem Internetgesetz spielt die Behörde für Informations- und Kommunikationstechnologien (BTK).

Artikel 8 des Internetgesetzes sieht ein spezielles Verfahren zur Verhängung von Zugangsbeschränkungen für Websites mit rechtswidrigen Inhalten vor.[504] Diese Bestimmung lässt derartige Beschränkungen nicht für alle Straftaten zu, sondern gilt nur für bestimmte Straftaten, die in einer Liste aufgeführt sind. Mit anderen Worten: Der Zugang zu einer Website kann nicht gesperrt werden, wenn die Straftat nicht ausdrücklich im Gesetz genannt ist. Zu diesen in Artikel 8 genannten Straftaten gehören die folgenden:

1) Ermutigung zum Suizid
2) sexueller Missbrauch von Kindern
3) Begünstigung des Konsums von Drogen oder Stimulanzien
4) Lieferung gesundheitsgefährdender Substanzen
5) Obszönität
6) Prostitution
7) Bereitstellung von Raum und Einrichtungen für Glücksspiele
8) Verbrechen im Sinne des Gesetzes Nr. 5816 Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun (Gesetz über strafbare Handlungen gegen Atatürk)
9) illegale Wetten
10) Verbrechen gemäß Artikel 27 Absatz 1 und 2 des Gesetzes Nr. 2937 Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu (Gesetz über staatliche Nachrichtendienste und die nationale Nachrichtendienstorganisation).

[504] Siehe auch Keser L., „Berichte aus der Praxis in ausgewählten Staaten – Türkei“ in Cappello M. (Hrsg.), *Medienrechtsdurchsetzung ohne Grenzen, IRIS Spezial*, Europäische Audiovisuelle Informationsstelle, Straßburg, 2018, S. 92.

Entscheidungen über Zugangssperren können in der Ermittlungsphase von der Staatsanwaltschaft und in der Strafverfolgungsphase vom Gericht erlassen werden. Zu beachten ist, dass Terrorismus und terroristische Straftaten nicht zu den in Artikel 8 des Internetgesetzes aufgeführten Verbrechen gehören.

Im Jahr 2015 wurde das Internetgesetz reformiert, wobei in Artikel 8/A eine stark umstrittene Bestimmung eingeführt wurde.[505]

In Angelegenheiten, die den Schutz von Leben und Eigentum, die nationale Sicherheit, die öffentliche Ordnung, die Verbrechensverhütung oder die öffentliche Gesundheit betreffen, kann ein Richter die Entscheidung erlassen, einen Online-Inhalt zu sperren oder zu entfernen. In dringenden Fällen kann dieses Recht auch durch den Präsidenten der Republik oder die zuständigen Ministerien ausgeübt werden. In solchen Fällen muss die endgültige Entscheidung, einen Inhalt zu sperren oder zu entfernen, vom Präsidenten der BTK getroffen werden.

Nach Artikel 8/A des Internetgesetzes sind Hostinganbieter und Anbieter sozialer Netzwerke verpflichtet, die Maßnahme innerhalb von vier Stunden nach der offiziellen Mitteilung umzusetzen, sobald die Entscheidung, einen Inhalt zu sperren oder zu entfernen, aus einem der in der Bestimmung genannten Gründe ergangen ist.

Obwohl der Eingriff in die Verfügbarkeit von Internetinhalten in erster Linie auf richterlichen Anordnungen beruht, können Zugangsbeschränkungen auch durch eine Entscheidung des Präsidenten oder der zuständigen Minister verhängt werden. Wenn eine solche Entscheidung auf Ersuchen des Präsidenten der Republik oder der zuständigen Ministerien getroffen wird, muss der Präsident der BTK die Entscheidung gemäß Artikel 8/A innerhalb von 24 Stunden dem Friedens-Strafgericht zur gerichtlichen Genehmigung vorlegen. Der Richter muss innerhalb von 48 Stunden einen Beschluss fassen, andernfalls wird die Entscheidung automatisch aufgehoben.

Verwaltungsmaßnahmen zur Beschränkung des Zugangs zu Internetinhalten sind in Türkiye weit verbreitet. Vor allem Artikel 8/A hat sich zu einer allgemeinen Rechtsgrundlage für die Regulierung von Online-Inhalten entwickelt. Diese Bestimmung wird zunehmend als breiter Sperrmechanismus genutzt. Im Laufe der Zeit wurden schon verschiedene Social-Media-Plattformen wie X, Wattpad, TikTok und Instagram auf Basis dieses Artikels gesperrt.[506]

Nach dem Internetgesetz werden Sperrentscheidungen umgesetzt, indem bestimmte Elemente der rechtsverletzenden Inhalte ins Visier genommen werden, etwa die Veröffentlichung, ein Abschnitt einer Veröffentlichung oder die URL-Adresse. Wenn es jedoch technisch nicht möglich ist, den Zugang nur zu den rechtswidrigen Inhalten oder den damit verbundenen Komponenten zu beschränken, können die Behörden die gesamte Website sperren.

---

[505] Siehe ebd., S. 93.

[506] Siehe auch Michaelson R., „The Internet's Sewer: Why Turkey Blocked Its most popular Social Site“, *The Guardian,* 1. März 2023; „Ekşi Sözlük'e 'milli güvenlik ve kamu düzeninin korunması' gerekçesiyle yine erişim engeli getirildi“ (Anordnung der Sperrung von Ekşi Sözlük zum „Schutz der nationalen Sicherheit und der öffentlichen Ordnung“), *BBC*, 14. Dezember 2023.

Da Websites ihren Datenverkehr mittlerweile meist verschlüsseln, ist die URL-basierte Sperrung praktisch unwirksam geworden. Daher wird in der Regel der Zugriff auf die gesamte Website eingeschränkt, wenn ein Diensteanbieter die betreffenden Inhalte nicht entfernt. Dieser Ansatz ist zu einer langjährigen Regulierungspraxis geworden, infolgedessen in der Vergangenheit der Zugang zu ganzen Plattformen wie Google Sites, YouTube und Wikipedia gesperrt wurde. Diese Methode der pauschalen Sperrung war bereits Gegenstand mehrerer Urteile des Europäischen Gerichtshofs für Menschenrechte gegen Türkiye.[507]

Türkiye verfolgt die Strategie, Online-Inhalte vor allem durch IP- und DNS-basierte Beschränkungsmethoden zu kontrollieren. Zur Unterstützung dieses Ansatzes wurde die Internet-Infrastruktur des Landes stark aufgerüstet, um den Zugang zu Inhalten zu verhindern, die von den zuständigen Behörden als rechtswidrig eingestuft werden. An allen Zugangspunkten landesweit wird ein umfassendes hochmodernes DPI-System (Deep Packet Inspection) eingesetzt. Allerdings hat der Vormarsch von Verschlüsselungstechnologien, insbesondere der weit verbreitete Einsatz von verschlüsseltem Datenverkehr, die Wirksamkeit solcher Inspektionssysteme beeinträchtigt. Infolge dieser technologischen Einschränkungen war Türkiye gezwungen, sein Modell der „Internetzensur“ zu überdenken. Diese Verschiebung fiel mit einem großen Wandel in der Internet-Governance zusammen, der durch die rasante Ausbreitung der sozialen Medien vorangetrieben wurde, die heute sowohl im sozialen als auch im wirtschaftlichen Bereich eine zentrale Rolle spielen.

Der neue Regulierungsansatz Türkiyes zielt darauf ab, die Verwaltung von Inhalten auf Social-Media-Plattformen an ihrem Ursprung anzugehen. Dabei geht es nicht nur darum, den Zugang zu beschränken, sondern vor allem darum, dass rechtswidrige oder schädliche Inhalte direkt an der Quelle vollständig entfernt werden. Im Einklang mit diesem Wandel schreibt die überarbeitete Gesetzgebung vor, dass Social-Media-Unternehmen einen lokalen Vertreter ernennen müssen, um die direkte Zusammenarbeit mit den türkischen Behörden zu erleichtern. Diese Plattformen müssen außerdem umgehend auf Nutzeranfragen reagieren, Transparenzberichte über ihre Aktivitäten zur Moderation von Inhalten vorlegen, personenbezogene Daten innerhalb der türkischen Grenzen aufbewahren, ihre Fähigkeit zur Bekämpfung krimineller Aktivitäten verbessern und proaktive Maßnahmen zum Schutz von Minderjährigen und jungen Nutzern ergreifen. Die überarbeiteten Vorschriften für soziale Medien, d. h. der 2022 eingeführte Zusatzartikel 4 des Internetgesetzes, haben eine einzigartige, auf die politischen Ziele Türkiyes zugeschnittene Rechenschaftsstruktur geschaffen. Um eine wirksame Durchsetzung dieser Bestimmungen zu gewährleisten, wurde das Internetgesetz um neue Sanktionsmechanismen ergänzt. Social-Media-Plattformen, die ihren rechtlichen Verpflichtungen nicht nachkommen, müssen mit Sanktionen wie Werbeverboten, Bandbreitenreduzierungen, zivilrechtliche Mithaftung für rechtswidrige Inhalte und erhebliche Bußgelder rechnen.

[507] Siehe *Ahmet Yildirim gegen Türkiye*, Beschwerde Nr. 3111/10 (EGMR, 18. Dezember 2012); *Cengiz und Andere gegen Türkiye*, Beschwerde Nr. 48226/10 und 14027/11 (EGMR, 1. Dezember 2015).

4.3.2 Spezifische Regeln zu terroristischen Inhalten

Türkiye engagiert sich seit Langem im Kampf gegen den Terrorismus und hat im Laufe der Jahre zahlreiche Terroranschläge erlebt. Dieser Kampf wird mit operativen Maßnahmen wie auch mit Rechtsinstrumenten geführt. Als Reaktion auf die rechtlichen Dimensionen des Terrorismus wurde 1991 ein spezielles Gesetz mit dem Titel *Terörle Mücadele Kanunu (Antiterrorgesetz)* erlassen, um den erforderlichen Rechtsrahmen für das Vorgehen gegen solche Bedrohungen zu schaffen.[508]

Dieses Gesetz bietet einen umfassenden Rahmen, indem es Terrorismus definiert, die für terroristische Handlungen verantwortlichen Personen benennt, die in terroristischer Absicht begangenen Straftaten umreißt, terroristische Organisationen charakterisiert und verschiedene Verfahren und Strafen für entsprechende Straftaten festlegt.

Im Antiterrorgesetz wird Terrorismus wie folgt definiert:

> *Terrorismus ist jede Handlung, die von einer oder mehreren Personen, die einer Organisation angehören, mit dem Ziel begangen wird, die in der Verfassung festgelegten Merkmale der Republik, ihr politisches, rechtliches, soziales, weltliches und wirtschaftliches System zu verändern, die unteilbare Einheit des Staates mit seinem Gebiet und Volk zu beschädigen, die Existenz des türkischen Staates und der türkischen Republik zu gefährden, die Staatsgewalt zu schwächen, zu zerstören oder an sich zu reißen, die Grundrechte und -freiheiten zu beseitigen oder die innere und äußere Sicherheit des Staates, die öffentliche Ordnung oder die allgemeine Gesundheit durch Druck, Zwang und Gewalt, Terror, Einschüchterung, Unterdrückung oder Bedrohung zu beeinträchtigen.*

Terrorismus im Sinne des Antiterrorgesetzes kann von Einzelpersonen oder Gruppen verübt werden.

Als terroristische Verbrechen werden Straftaten eingestuft, die im Zusammenhang mit den Aktivitäten einer terroristischen Organisation begangen werden. Wenn eine Handlung als terroristische Straftat eingestuft wird, unterliegt sie nach dem geltenden Rechtsrahmen verschärften Strafen und besonderen Verfahrensregeln.

Seit seinem Inkrafttreten steht dieses Gesetz im Mittelpunkt rechtlicher und politischer Debatten. Kritiker machen geltend, dass es unverhältnismäßige Einschränkungen der Grundrechte und -freiheiten vorsieht. Im Laufe der Zeit wurden sein Anwendungsbereich und seine Bestimmungen stark verändert.

4.3.3 Anwendung im Hinblick auf die Sperrung des Zugangs zu terroristischen Inhalten

Da digitale Technologien bei der Verabschiedung des Antiterrorgesetzes noch wenig verbreitet waren, werden das Internet und damit zusammenhängende Technologiebereiche

[508] Eine vollständige englische Übersetzung des türkischen Antiterrorgesetzes findet sich hier.

darin verständlicherweise nicht ausdrücklich erwähnt. Dennoch haben seine grundlegenden Definitionen auch nachfolgende Rechtsrahmen zur Regulierung der digitalen Sphäre beeinflusst und geprägt.

Im Gegensatz zu Artikel 8 des Internetgesetzes, der die Sperrung und Entfernung von Inhalten nur bei bestimmten Straftaten zulässt, erlaubt Artikel 8/A die Sperrung und Entfernung von Inhalten bei jeder Straftat oder Verletzung der öffentlichen Ordnung. Insbesondere Terrorismus und terrorismusbezogene Straftaten können in den Anwendungsbereich von Artikel 8/A des Internetgesetzes fallen, weil die weit gefassten Begriffe der nationalen Sicherheit, der öffentlichen Ordnung und der Verbrechensverhütung bei der Internetregulierung einen erheblichen Ermessensspielraum zulassen.

Die BTK führt keine statistischen Aufzeichnungen über Websites, die wegen Terrorismus gesperrt werden, und gibt auch keine umfassenden Daten dazu an die Öffentlichkeit weiter. Aus verschiedenen Presseerklärungen geht jedoch hervor, dass terrorismusbezogene Inhalte gemäß Artikel 8/A des Internetgesetzes gesperrt worden sind.[509]

Hierbei ist zu beachten, dass Terrorismusbekämpfung nach wie vor eine der vordringlichsten Prioritäten Türkiyes ist und das Land aktiv gegen terroristische Inhalte im Internet vorgeht. Obwohl das Internetgesetz als wichtigster Rechtsrahmen Türkiyes für die Regulierung des Internets terroristische Inhalte nicht ausdrücklich erwähnt, werden die Durchsetzungsbemühungen in diesem Bereich fortgesetzt. Artikel 8/A des Gesetzes ist eine weit gefasste Bestimmung, die Eingriffe und Zugangssperren für ein breites Spektrum rechtswidriger Inhalte ermöglicht.

Daher könnte man argumentieren, dass Artikel 8/A des Internetgesetzes als Pauschalregelung für die Kontrolle beliebiger Online-Inhalte dient. In der Praxis bedeutet dies, dass für die Entfernung aller terroristischen Inhalte von allen Plattformen, einschließlich der sozialen Medien, der sehr kurze Zeitrahmen von vier Stunden gilt.

[509] Siehe „6 bin 500 habere engel 5 bin habere sansür!“ (6500 Elemente gesperrt, 5000 entfernt!), *Cumhuriyet*, 16. Oktober 2023; Uludag A., „AYM kararına rağmen engellenen içeriklerin sayısı artıyor“ (Trotz der Entscheidung des Verfassungsgerichts steigt die Zahl der gesperrten Inhalte), *Deutsche Welle*, 4. August 2023.

5. Bekämpfung von diffamierenden, hetzerischen und zu Gewalt aufstachelnden Äußerungen

5.1 Durchsetzung auf EU-Ebene

Dr Mark D. Cole, Wissenschaftlicher Direktor, Institut für Europäisches Medienrecht (EMR) und Professor für Medien- und Telekommunikationsrecht, Universität Luxemburg

Mehrere Faktoren, darunter eine Abfolge wirtschaftlicher und sozialer Krisen, die COVID-19-Pandemie, Herausforderungen im Zusammenhang mit der Migration und die zunehmende Digitalisierung, haben dazu beigetragen, dass sich diffamierende, hetzerische und zu Gewalt aufstachelnde Äußerungen im Internet häufen.[510] Der jüngste Regulierungsansatz der EU zur Bekämpfung solcher Äußerungen entwickelt sich ständig weiter.

Zur Erleichterung eines harmonisierten Durchsetzungskonzepts ähnlich dem für terroristische Inhalte (siehe Kapitel 4.1) hat die EU eine Angleichung der Regeln darüber angeregt, was in ihren Mitgliedstaaten als kriminelle und damit rechtswidrige Äußerung zu betrachten ist. So wird beispielsweise rechtswidrige Hetze in einem Rahmenbeschluss zur strafrechtlichen Bekämpfung bestimmter Formen und Ausdrucksweisen von Rassismus und Fremdenfeindlichkeit[511] als öffentliche Aufstachelung zu Gewalt oder Hass aufgrund bestimmter Merkmale wie Rasse, Hautfarbe, Religion, Abstammung oder nationale oder ethnische Herkunft definiert.[512] Dieser Rahmenbeschluss zur Bekämpfung von Rassismus und Fremdenfeindlichkeit bezieht sich zwar nur auf rassistische und fremdenfeindliche Äußerungen, aber die meisten Mitgliedstaaten haben ihre nationalen Gesetze ausgeweitet, um Hetze aus anderen Gründen, wie etwa sexuelle Orientierung, Geschlechtsidentität und Behinderung, zu sanktionieren. Dieser Ansatz spiegelt sich auch in der konsolidierten AVMD-RL wider, die in Artikel 6 allgemein und in Artikel 9 Absatz 1 Buchstabe c Ziffer ii für kommerzielle Kommunikation eine umfangreichere Liste von Gründen für verbotene Diskriminierung nennt, die Geschlecht, Rasse oder ethnische Herkunft, Staatsangehörigkeit, Religion oder Glauben, Behinderung, Alter und sexuelle Ausrichtung umfasst und damit

[510] Siehe Faloppa F. et al., *Study on Preventing and Combating Hate Speech in Times of Crisis*, Europarat, CDADI, Straßburg, November 2023.

[511] Rahmenbeschluss 2008/913/JI des Rates vom 28. November 2008 zur strafrechtlichen Bekämpfung bestimmter Formen und Ausdrucksweisen von Rassismus und Fremdenfeindlichkeit, ABl. L 328/55, 6. Dezember 2008.

[512] Zudem hat die EU mehrere Richtlinien verabschiedet, die Diskriminierung aus verschiedenen Gründen verbieten, etwa aufgrund von Rasse und ethnischer Herkunft. Da dies den Rahmen des vorliegenden IRIS-Berichts sprengen würde, wird auf diese Richtlinien hier nicht eingegangen.

Artikel 21 der EU-Grundrechtecharta (EU-GRC) ähnelt, auf den in Artikel 6 Absatz 1 ausdrücklich verwiesen wird.[513]

Angesichts der Zersplitterung des materiellen Rechts auf der einen Seite und der starken Zunahme von Hetze und Hasskriminalität in Europa auf der anderen Seite[514] hat die Europäische Kommission im Jahr 2021 eine Mitteilung angenommen, in der die Notwendigkeit eines Ratsbeschlusses betont wird, der die derzeitige Liste der „EU-Straftatbestände" gemäß Artikel 83 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV)[515] auf Hetze und Hasskriminalität ausweitet.[516] Da eine solche Ausweitung der Liste jedoch noch nicht förmlich abgeschlossen ist, haben das Europäische Parlament und der Rat keine Rechtsgrundlage, um sekundäre Rechtsvorschriften mit Mindestbestimmungen für die Definition von Straftaten im Zusammenhang mit Hetze und entsprechende Sanktionen zu erlassen.[517] Ungeachtet dieser Grenzen stellt die Richtlinie zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt[518] Hetze gegen Frauen zusammen mit anderen Formen geschlechtsspezifischer Cybergewalt unter Strafe, weil Gewalt gegen Frauen den zentralen EU-Wert der

[513] Da die Bestimmungen der EU-GRC in gleicher Weise wie die EMRK ausgelegt werden sollten, stellt die Rechtsprechung des EGMR zu Artikel 17 der EMRK die Mindestschwelle der europäischen Menschenrechte für strafbare Hetze klar. Dies wurde in Absatz 11 der Empfehlung CM/Rec/(2022)16 des Ministerkomitees des Europarats zur Bekämpfung von Hassrede herausgearbeitet, der Folgendes umfasst: a. öffentlicher Aufruf, zur Begehung von Völkermord, Verbrechen gegen die Menschlichkeit oder Kriegsverbrechen; b. öffentlicher Aufruf zu Hass, Gewalt oder Diskriminierung; c. rassistische, fremdenfeindliche, sexistische und LGBTI-feindliche Drohungen; d. rassistische, fremdenfeindliche, sexistische und LGBTI-feindliche öffentliche Beleidigungen unter Bedingungen wie jene, die für Beleidigungen im Internet im Zusatzprotokoll zum Übereinkommen über Computerkriminalität betreffend die Kriminalisierung mittels Computersysteme begangener Handlungen rassistischer und fremdenfeindlicher Art (SEV Nr. 189) aufgeführt sind; e. die öffentliche Leugnung, Verharmlosung und Billigung von Völkermord, Verbrechen gegen die Menschlichkeit oder Kriegsverbrechen; und f. die vorsätzliche Verbreitung von Material, das solche Äußerungen von Hassrede (wie oben unter a-e aufgeführt) enthält, einschließlich Ideen, die auf rassischer Überlegenheit oder Hass basieren.

[514] Zu Letzterem siehe die Jahresberichte 2019 und 2020 der Europäischen Kommission gegen Rassismus und Intoleranz (ECRI): ECRI, „Annual Report of ECRI's Activities Covering the Period from 1 January to 31 December 2019", Straßburg, März 2020, und ECRI, „Annual Report on ECRI's Activities Covering the Period from 1 January to 31 December 2020", Straßburg, März 2021. Siehe auch die von der Fachabteilung Bürgerrechte und konstitutionelle Angelegenheiten des Europäischen Parlaments in Auftrag gegebene Studie „Hate speech and hate crime in the EU and the evaluation of online content regulation approaches", Juli 2020.

[515] Die in Artikel 83 Absatz 1 des AEUV aufgeführten Kriminalitätsbereiche sind: Terrorismus, Menschenhandel und sexuelle Ausbeutung von Frauen und Kindern, illegaler Drogenhandel, illegaler Waffenhandel, Geldwäsche, Korruption, Fälschung von Zahlungsmitteln, Computerkriminalität und organisierte Kriminalität.

[516] Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament und den Rat, Ein inklusiveres und besser schützendes Europa: Erweiterung der Liste der EU-Straftatbestände um Hetze und Hasskriminalität, COM(2021) 777 final, 2021.

[517] Gemäß Artikel 83 Absatz 1 des AEUV können das Europäische Parlament und der Rat gemäß dem ordentlichen Gesetzgebungsverfahren durch Richtlinien Mindestvorschriften zur Festlegung von Straftaten und Strafen in Bereichen besonders schwerer Kriminalität festlegen, die aufgrund der Art oder der Auswirkungen der Straftaten oder aufgrund einer besonderen Notwendigkeit, sie auf einer gemeinsamen Grundlage zu bekämpfen, eine grenzüberschreitende Dimension haben. Zum Stand der Vorschläge zur Erweiterung der Liste der EU-Straftatbestände auf alle Formen von Hasskriminalität und Hetze siehe die spezielle Website des Europäischen Parlaments zum Gesetzgebungsfahrplan unter https://www.europarl.europa.eu/legislative-train/theme-protecting-our-democracy-upholding-our-values/file-hate-crimes-and-hate-speech.

[518] Richtlinie (EU) 2024/1385 des Europäischen Parlaments und des Rates vom 14. Mai 2024 zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt, ABl. L 2024/1385, 24. Mai 2024.

Gleichstellung von Frauen und Männern gefährdet, wobei sie sich auf Artikel 82 Absatz 2 und Artikel 83 Absatz 1 des AEUV als Rechtsgrundlage stützt.

In der Zwischenzeit sind im Primärrecht, Sekundärrecht und Soft Law der EU Strategien entwickelt worden, um Hetze zu bekämpfen, indem Schlüsselelemente ihrer Konzeptualisierung geklärt werden.[519] Der Arbeit zur Bekämpfung von Hetze im Internet kommt zugute, dass diese als Verstoß gegen zentrale Werte der EU betrachtet wird, die in Artikel 2 des Vertrags über die Europäische Union (EUV) verankert sind.[520] Angesichts der zahlreichen Initiativen und Sensibilisierungskampagnen gegen Hass im Online- und Offline-Bereich[521] liegt der Schwerpunkt dieses Kapitels auf der Verbreitung entsprechender Inhalte auf Online-Plattformen. Von Online-Plattformen gehen besondere Risiken aus, weil ihre algorithmischen Systeme die Verbreitung bestimmter Arten von Äußerungen verstärken, sodass es zu schwerwiegenden negativen Auswirkungen auf mögliche Opfer kommen kann.

Auch bei diffamierenden Äußerungen ist ein Effekt zu beobachten, wie er im Zusammenhang mit Hetze beschrieben wurde, denn durch die schnelle Verbreitung und Replikation solcher Inhalte im Internet sind die Opfer fortwährend von Beleidigungen und potenziellen weiteren Schäden betroffen. Im Gegensatz zur Hetze, die nach Artikel 10 der EMRK[522] oder Artikel 11 der EU-GRC eingeschränkt werden kann, ist die Lage bei diffamierenden Äußerungen jedoch nicht so klar. Diffamierung ist nicht immer eindeutig rechtswidrig, und auch beleidigende Äußerungen können noch im Rahmen der EMRK und der EU-GRC geschützt sein.[523] Ob diffamierende Äußerungen den Grad der Rechtswidrigkeit erreichen oder nicht, wird durch innerstaatliches Recht bestimmt. Die Anwendung der Standards erfordert grundsätzlich eine Bewertung der sachlichen Richtigkeit, eine Berücksichtigung des Kontexts, ein öffentliches Interesse und eine Absicht. Ähnliche Herausforderungen bestehen bei Äußerungen, die zu Gewalt aufstacheln.

Obwohl die Einstufung konkreter Äußerungen schwierig ist, führt der DSA auf EU-Ebene für Online-Plattformen einen Rahmen mit abgestuften Verantwortlichkeiten ein. Darin werden Insbesondere VLOPSEs verpflichtet, die mit der Verbreitung rechtswidriger

---

[519] Siehe Nave E., Lane L., „Countering Online Hate Speech: How Does Human Rights Due Diligence Impact Terms of Service“, *Computer Law & Security Review* 51, 2023, 105884. Als politische Maßnahme hat die Europäische Kommission 2016 eine Hochrangige Gruppe zur Bekämpfung von Hetze und Hasskriminalität eingesetzt, die unter anderem Leitlinien für die Zusammenarbeit zwischen Strafverfolgungsbehörden und Organisationen der Zivilgesellschaft veröffentlicht hat und den Austausch bewährter Praktiken erleichtern soll (siehe Europäische Kommission, *Informal Commission Expert Group „High Level Group on Combating Hate Speech and Hate Crime“, Terms of Reference*, 2016).

[520] Siehe Europäische Kommission, Gemeinsame Mitteilung an das Europäische Parlament und den Rat, „Kein Platz für Hass: ein Europa, das geeint gegen Hass steht“, JOIN(2023) 51 final, 2023 (als Antwort auf die Online-Reaktionen auf den Hamas-Angriff auf Israel vom 7. Oktober 2023).

[521] Einen Überblick über die Arbeitsabläufe und Ressourcen auf EU-Ebene findet sich auf der Website der Kommission „Combating Hate Speech and Hate Crime“ (Bekämpfung von Hetze und Hasskriminalität): https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/combating-hate-speech-and-hate-crime_en.

[522] Entweder wegen Rechtsmissbrauchs (Artikel 17 EMRK) oder wegen Zerstörung der Grundwerte der EMRK (wobei Einschränkungen gemäß Artikel 10 Absatz 2 EMRK als notwendig erachtet werden). Für einen kurzen Überblick über die Rechtsprechung des EGMR zum Theme Hetze siehe EGMR, Presseabteilung, „Factsheet – Hate Speech“, 23. November 2023.

[523] *Handyside gegen Vereinigtes Königreich*, Beschwerde Nr. 5493/72 (EGMR, 7. Dezember 1976).

Inhalte verbundenen Risiken im Rahmen ihrer spezifischen Verpflichtungen aus Kapitel III Abschnitt 5 des DSA anzugehen und zu mindern. Diese zusätzliche Verpflichtung besteht neben der allgemeinen Anforderung, dass alle Hostingdiensteanbieter einen Melde- und Abhilfemechanismus einrichten und rechtswidrige Inhalte, von denen sie Kenntnis haben, unverzüglich entfernen müssen. Außerdem müssen sie die Funktionsweise ihrer Algorithmen und Empfehlungssysteme transparent machen und der Gefahr entgegenwirken, dass solche Systeme als Verstärker für rechtswidrige Inhalte fungieren.

In Bezug auf Hassreden sind diese Verpflichtungen, auch jene zum raschen Handeln, im Verhaltenskodex für die Bekämpfung illegaler Hassreden im Internet[524] verankert, der sich mit illegalen Hassreden im Sinne des oben genannten Rahmenbeschlusses befasst. Dieser 2016 formulierte Verhaltenskodex war zunächst eine freiwillige Vereinbarung zwischen der Europäischen Kommission und ursprünglich Facebook, Microsoft, Twitter und YouTube. Später kamen weitere Plattformanbieter hinzu.[525] Der Verhaltenskodex für die Bekämpfung illegaler Hassreden im Internet zielt darauf ab, der Verbreitung illegaler Hassreden im Internet im Einklang mit EU- und nationalem Recht entgegenzuwirken, unter anderem durch Beschleunigung der Überprüfung und Entfernung illegaler Hassreden, meist mit einer Reaktionszeit von 24 Stunden ab Meldung, und durch Förderung der Transparenz und Kooperation zwischen Plattformen und EU-Behörden. Am 20. Januar 2025 wurde der Verhaltenskodex überarbeitet und als „Verhaltenskodex für die Bekämpfung illegaler Hassreden im Internet +“ in die Koregulierungsarchitektur des DSA integriert.[526] Im Mittelpunkt des Verhaltenskodex für die Bekämpfung illegaler Hassreden im Internet + steht die Prävention und Antizipation von Bedrohungen. Ziel ist, den Umgang der Plattformen mit rechtswidrigen Äußerungen im Rahmen des EU-Rechts und der nationalen Gesetze zu verbessern und die wirksame Durchsetzung des DSA zu unterstützen. Die Einhaltung des Verhaltenskodex für die Bekämpfung illegaler Hassreden im Internet + kann für Unterzeichner, die als VLOPSE einzustufen sind, eine wirksame Maßnahme zur Risikominderung darstellen.

Vor der Eingliederung des Verhaltenskodex in den DSA hat die Europäische Kommission ein förmliches Verfahren gegen X nach Artikel 66 Absatz 1 des DSA eingeleitet (siehe oben, Kapitel 4.1). In diesem Verfahren wurde ein Verstoß gegen die Artikel 34 und 35 des DSA in Bezug auf die Risikobewertung und -minderung geltend gemacht, da die Bewertung des Anbieters von X hinsichtlich der Gestaltung und Funktionsweise seines Systems „Freedom of Speech Not Freedom of Reach“ in der EU inadäquat gewesen sei.[527] Insbesondere reduzierte X im Jahr 2023 sein Personal für die Moderation von Inhalten,[528] zog sich aus dem Verhaltenskodex zur Bekämpfung von Desinformation zurück[529] und löste

[524] Verhaltenskodex für die Bekämpfung illegaler Hassreden im Internet, 30. Juni 2016.
[525] Siehe die spezielle Website der Kommission zu diesem Verhaltenskodex.
[526] Code of Conduct on Countering Illegal Hate Speech Online +, 20. Januar 2025. Der Kodex besteht aus fünf Verpflichtungen und zwei Anhängen. Die Verpflichtungen betreffen unter anderem die Überprüfung der meisten Meldungen von Hassreden binnen 24 Stunden gemäß Artikel 16 und 22 des DSA durch sogenannte „Berichterstatter“ mit Kenntnissen im Bereich rechtswidriger Hassreden.
[527] Entscheidung der Kommission vom 18. Dezember 2023 zur Einleitung eines Verfahrens gemäß Artikel 66 Absatz 1 der Verordnung (EU) 2022/2065, COM(2023) 9137 final, Rn. 9, 2023.
[528] Reuters, „Twitter further Cuts Staff Overseeing Global Content Moderation, Bloomberg Reports“, *Reuters*, 7. Januar 2023.
[529] Siehe Beitrag von Thierry Breton auf X, „Twitter leaves EU voluntary Code of Practice against disinformation“, 26. Mai 2023.

seine Beratungsgruppe auf, die sich um Hetze kümmern sollte.[530] Insbesondere war die Europäische Kommission der Ansicht, dass

> *die regionalen und sprachlichen Aspekte der Politik von X in Bezug auf „gewalttätige und hetzerische Organisationen", „gewalttätige Äußerungen", „hetzerische Inhalte" und „sensible Medien" in der Europäischen Union sowie die von TIUC und X Holdings Corp. für die Umsetzung dieser Politik eingesetzten Ressourcen für die Inhaltsmoderation und andere Systeme unzureichend erscheinen, um das Risiko der Verbreitung rechtswidriger Inhalte konsequent und wirksam zu mindern.*[531]

Eine nachträgliche Analyse der im November 2023 an die DSA-Transparenzdatenbank übermittelten Daten ergab, dass die Inhaltsmoderation von X im Vergleich zu anderen Social-Media-Plattformen tatsächlich begrenzt ist.[532] Im Januar 2025 erließ die Europäische Kommission im Rahmen der laufenden Untersuchung eine Aufbewahrungsanordnung, in der sie X aufforderte, weitere Informationen im Wege technischer Untersuchungsmaßnahmen zum Empfehlungssystem der Plattform bereitzustellen.[533] Die Europäische Kommission beantragte den Zugriff auf bestimmte kommerzielle Anwendungsprogrammierschnittstellen (APIs), insbesondere die technischen Schnittstellen zu den Inhalten auf X, die eine direkte Überprüfung der Inhaltsmoderation und der Viralität von Accounts ermöglichen. Die Dauer der Untersuchung zeigt, wie komplex die Bewertung systemischer Risiken und ihrer Minderung aus Sicht der Aufsichtsbehörde ist. Mit Stand September 2025 ist die Untersuchung der Europäischen Kommission gegen X wegen seiner Inhaltsmoderationspraktiken und Transparenzpflichten noch immer nicht abgeschlossen. Wenn die Kommission feststellt, dass X seinen Verpflichtungen aus dem DSA nicht nachgekommen ist, kann sie Sanktionen verhängen (siehe Kapitel 2.2.2.2).

Bei den Melde- und Abhilfeanforderungen im DSA dürften die Herausforderungen, die sich schon bei der ECRL gezeigt haben, wohl bestehen bleiben, wie etwa die Frage des Takedown und Staydown bei wiederholten Verstößen der gleichen Art. Ähnlich wie die EC-RL sieht der DSA keine allgemeine Überwachungspflicht für Hostingdiensteanbieter vor. Parteien, die geltend machen können, dass ihre Rechte durch die von den Anbietern bereitgestellten Inhalte verletzt wurden, haben jedoch ein starkes Interesse daran, die rechtswidrige Handlung zu beenden und zu verhindern, dass die rechtswidrige Verbreitung der Inhalte fortgesetzt oder wiederholt wird. Deshalb können sie eine einstweilige Verfügung beantragen, die sicherstellen soll, dass die betreffenden Inhalte von den Anbietern zügig und dauerhaft entfernt werden und auch nicht wieder auftauchen.[534] Eine

---

[530] Associated Press, „Musk's Twitter Has Dissolved its Trust and Safety Council", *npr*, 12. Dezember 2022.

[531] Ebd., Rn. 10. TIUC ist die Twitter International Unlimited Company, die Hauptniederlassung des Anbieters von X in der EU. X Holdings Corp. ist das Unternehmen, das die Gruppe juristischer Personen kontrolliert, zu der TIUC gehört.

[532] Kaushal R. et al., „Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database", FAccT '24: Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency, S. 1121–1132.

[533] Europäische Kommission, „Kommission richtet zusätzliche Ermittlungsmaßnahmen an X in laufenden Verfahren nach dem Gesetz über digitale Dienste", Pressemitteilung, 17. Januar 2025.

[534] Siehe mit Blick auf Rechte an geistigem Eigentum: C-324/09 *L'Oréal SA u. a. gegen eBay International u. a.* (GHEU, 12. Juli 2011, ECLI:EU:C:2011:474) und C-70/10 *Scarlet Extended SA gegen SABAM* (GHdEU, 24. November 2011, ECLI:EU:C:2011:771).

solche dauerhafte Entfernung erfordert ein Eingreifen des Hostingdiensteanbieters, etwa durch Inhaltsmoderation oder Filterung.[535]

Die Frage spezifischer Filterverpflichtungen wurde auch im Bereich des Urheberrechts und der verwandten Schutzrechte intensiv diskutiert, insbesondere im Hinblick auf Artikel 17 der Richtlinie über das Urheberrecht im digitalen Binnenmarkt (DSM-RL),[536/537] doch bei diffamierenden oder verleumderischen Inhalten wirft der Gedanke des Takedown und Staydown noch mehr Fragen auf: Hier lässt sich die Rechtswidrigkeit von Inhalten nicht unbedingt an der Verwendung bestimmter Wörter oder Wendungen (z. B. solcher, die als beleidigend angesehen werden) festmachen, sondern daran, dass eine Äußerung insgesamt als diffamierend angesehen werden kann.[538] Um einen wirksamen Schutz der Rechte Betroffener zu gewährleisten, müsste sich eine gerichtliche Verfügung nicht nur auf den Wortlaut des als rechtswidrig eingestuften Inhalts erstrecken, sondern auch auf Informationen, „deren Inhalt wegen der verwendeten Worte oder ihrer Kombination […] zwar leicht unterschiedlich formuliert ist, aber im Wesentlichen die gleiche Aussage vermittelt", wie es der Gerichtshof der Europäischen Union (EuGH) in einem von einem österreichischen Gericht vorgelegten Fall formuliert hat.[539] Das Konzept der „sinngleichen Informationen" wurde vom EuGH für eine Verfügung eines innerstaatlichen Gerichts als zulässig angesehen, solange es nicht eine autonome Beurteilung durch den Anbieter und eine generelle Verpflichtung zur Sperrung solcher Informationen erfordert.[540] In dieser Schlussfolgerung wird anerkannt, dass die Anbieter – aufgrund der Menge der gespeicherten Informationen – in der Regel automatisierte Suchwerkzeuge und -techniken zur Moderation und Filterung von Inhalten verwenden,[541] sodass es sich nicht um eine Vorabprüfung aller eingestellten Beiträge handelt.

---

[535] Siehe Enarsson T., „Navigating Hate Speech and Content Moderation under the DSA: Insights from ECtHR case law", *Information & Communications Technology Law* 33(3), 2024, S. 384-401.

[536] Richtlinie (EU) 2019/790 des Europäischen Parlaments und des Rates vom 17. April 2019 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG, ABl. L 130/92, 17. Mai 2019.

[537] Siehe z. B. Geiger C., Jütte BJ., „Platform Liability under Article 17 of the Copyright in the Digital Single Market Directive, Automated Filtering and Fundamental Rights: An Impossible Match", *GRUR International* 70(6), 2021, S. 517-543; Rauer N., Bibi A., „Grundrechtskonformität des Art. 17 DSM-RL – Ende gut alles gut?", *Zeitschrift für Urheber- und Medienrecht*, 2022, S. 585-672.

[538] *C-18/18 Glawischnig-Piesczek gegen Facebook* (GHdEU, 3. Oktober 2019) ECLI:EU:C:2019:821, Rn. 40.

[539] Ebd., Rn. 41.

[540] Ebd., Rn. 46 ff.

[541] Siehe ebd., Rn. 46. Für einen Kommentar hierzu siehe Rojszczak M., „Online Content Filtering in EU Law – A Coherent Framework or Jigsaw Puzzle?", *Computer Law & Security Review* 47, 2022, 105739.

5.2 Beispiel Irland

Dr Roderick Flynn, Außerordentlicher Professor, Lehrstuhl für Kommunikationswissenschaften, School of Communications, Dublin City University

5.2.1 Nationaler Rechtsrahmen für Plattformen

Die Verabschiedung der jüngsten (2018) Version der AVMD-RL und des DSA im Jahr 2022 sowie die Anforderung, beide in irisches Recht umzusetzen oder zu integrieren, führten zu einer Reihe umfangreicher Ergänzungen des irischen Rundfunkgesetzes von 2009.[542] Diese Ergänzungen betreffen die Regulierung von hetzerischen und zu Gewalt aufstachelnden Äußerungen im Internet, obwohl sie relativ wenig mit Diffamierung zu tun haben. Letztere unterliegt weiterhin dem Diffamierungsgesetz von 2009[543].

Ein unmittelbares Ergebnis der Umsetzung und Integration der AVMD-RL und des DSA war die Schaffung einer neuen Medienregulierungsbehörde, der Coimisiún na Meán (CnaM). Die CnaM löste die Broadcasting Authority of Ireland (BAI) ab, deren Regulierungsauftrag sich weitgehend auf Hörfunk- und Fernsehveranstalter sowie Abrufdienste beschränkte. Die mit der AVMD-RL und der DSA vorangetriebene starke Ausweitung der Regulierung auf Online-Inhalte erforderte neue Regulierungsstrukturen, die mit der Gründung der CnaM am 15. März 2023 ihren institutionellen Ausdruck fanden. Alle Funktionen, die zuvor bei der BAI angesiedelt waren, wurden auf die CnaM übertragen, ebenso wie die zusätzlichen regulatorischen Verpflichtungen, die sich aus der AVMD-RL und dem DSA ergeben. Im Zuge ihrer Neugründung bezog die Regulierungsbehörde einen neuen Hauptsitz, da diese voraussichtlich mit einer Zunahme der Mitarbeiterzahl von weniger als 50 auf mehr als 350 einhergehen wird. Die CnaM hat nun als verantwortliche Stelle dafür zu sorgen, dass Online-Plattformen Mechanismen einsetzen, die ihre Nutzer wirksam vor schädlichen Inhalten schützen, darunter auch hetzerische und zu Gewalt aufstachelnde Äußerungen.

Die Aufnahme der Bestimmungen der AVMD-RL und des DSA in das irische Recht wurde im Wesentlichen durch zwei innerstaatliche Rechtsvorschriften erreicht: das Gesetz für Online-Sicherheit und Medienregulierung (OSMR) von 2022[544] und das irische Gesetz über digitale Dienste von 2024.[545] Die Texte beider Gesetze wurden dem bestehenden Rundfunkgesetz von 2009 hinzugefügt. Bisher wurde noch keine offizielle Konsolidierung der Rechtsvorschriften veröffentlicht, aber die Irish Law Society unterhält eine Online-Version, die alle nachträglichen Ergänzungen des ursprünglichen Rundfunkgesetzes von 2009 enthält.[546]

Trotz der Verabschiedung des OSMR-Gesetzes war Irland bei der Umsetzung einiger Elemente der AVMD-RL (darunter jene zu Video-Sharing-Plattformen (VSPs)) in nationales

[542] Broadcasting Act 2009.
[543] Defamation Act 2009.
[544] Online Safety and Media Regulation Act 2022.
[545] Digital Services Act 2024.
[546] Siehe Law Reform Commission, Broadcasting Act 2009 (zuletzt aktualisiert am 1. Juni 2025).

Recht langsam. Im Februar 2024 verhängte der EuGH gegen Irland ein Bußgeld in Höhe von EUR 2 500 000, weil es die AVMD-RL nicht vollständig umgesetzt hatte.[547] Der EuGH stellte fest, dass das OSMR zwar Bestimmungen enthielt, die die (obligatorische) Annahme von Kodizes für VSPs vorsahen, diese Kodizes aber bis Anfang 2024 nicht ausgearbeitet worden waren. Dies wurde schließlich im Oktober 2024 in Angriff genommen, als die CnaM den Kodex für Online-Sicherheit veröffentlichte.[548] Auf diesen wird im Folgenden noch näher eingegangen, doch im Wesentlichen beschreibt er, was unter schädlichen Inhalten zu verstehen ist, und nennt insbesondere die Aufstachelung zu Gewalt oder Hass gegen eine Gruppe oder ein Mitglied einer Gruppe von Personen aus einem der in Artikel 21 der EU-GRC genannten Gründe wie Geschlecht, politische Zugehörigkeit, Behinderung, Zugehörigkeit zu einer ethnischen Minderheit, Religion und Rasse. Zudem legt er die Pflichten von VSP-Diensteanbietern in Bezug auf die von ihnen gehosteten Inhalte fest. Danach müssen solche Plattformanbieter „in den Geschäftsbedingungen und den damit verbundenen Verpflichtungen des Dienstes Beschränkungen vorsehen, die es den Nutzern untersagen:

- eingeschränkte Videoinhalte im Sinne dieses Kodex hochzuladen oder zu teilen und
- eingeschränkte, nicht [von dem Video] trennbare nutzergenerierte Inhalte im Sinne dieses Kodex hochzuladen oder zu teilen".[549]

Der Kodex für Online-Sicherheit sieht zudem vor, dass der Plattformanbieter das Konto eines Nutzers sperrt, wenn dieser häufig gegen diese Geschäftsbedingungen verstoßen hat.[550] Gemäß dem Kodex hat die CnaM die Aufgabe, VSP-Dienste zu identifizieren, die der Rechtshoheit Irlands unterliegen, und diese als solche zu benennen, was zum ersten Mal im Dezember 2023 geschah und die meisten der großen in Europa aktiven VSP-Dienste betraf.[551]

Reddit und Tumblr legten gegen diese Nennung 2024 Einspruch beim irischen High Court ein. Reddit argumentierte, dass es als US-Körperschaft nicht der Rechtshoheit des irischen Staates unterliegen sollte, während Tumblr vortrug, dass der Umfang der Videoinhalte auf seiner Plattform relativ gering sei und daher die Schwelle für die Einstufung als VSP nicht erreiche. Der High Court wies beide Einsprüche im Juni 2024 eindeutig ab und stellte fest, dass die CnaM beide Dienste korrekt eingestuft hatte.[552] Im Mai 2025 widerrief die CnaM jedoch die Einstufung von Reddit, weil dessen Muttergesellschaft ihren europäischen Hauptsitz in die Niederlande verlegt hatte.[553]

---

[547] Collins S., „Ireland fined €2.5m by EU courts for delays to online safety law", *Irish Independent*, 29. Februar 2024.
[548] Coimisiún na Meán, Online Safety Code, Oktober 2024.
[549] Ebd., Abschnitt 12.1.
[550] Ebd. Abschnitt 12.6.
[551] Da eine beträchtliche Anzahl von Plattformen und Technologieunternehmen ihren europäischen Hauptsitz in Irland haben, stellte die CnaM im Dezember 2023 bei zehn VSP-Diensten fest, dass sie dem – damals noch nicht veröffentlichten – Kodex für Online-Sicherheit unterliegen. Es handelte sich um Facebook, Instagram, YouTube, Udemy, TikTok, LinkedIn, X/Twitter, Pinterest, Tumblr und Reddit.
[552] O'Faolain A., „High Court dismisses Reddit and Tumblr challenges over new online safety code", *Irish Times*, 20. Juni 2024.
[553] Coimisiún na Meán, Revocation of Designation Notice, 22. Mai 2025.

5.2.2 Besondere Regeln für diffamierende, hetzerische und zu Gewalt aufstachelnde Äußerungen

Auf Diffamierung wird in diesem Bericht nur kurz eingegangen, weil der Kodex für Online-Sicherheit Verleumdung oder Diffamierung nicht direkt erwähnt. Das soll nicht heißen, dass hetzerische oder zu Gewalt aufstachelnde Äußerungen nicht auch eine Diffamierung darstellen können. In der Praxis wird Online-Diffamierung jedoch rechtlich genauso behandelt wie Diffamierung in Print- oder Rundfunkinhalten. Online-Diffamierung als solche unterliegt den Bestimmungen des Diffamierungsgesetzes von 2009. Es wurde jedoch angemerkt, dass Online-Diffamierung besondere Herausforderungen mit sich bringt, nicht zuletzt bei der Identifizierung der für die Veröffentlichung von diffamierendem Material über eine Online-Plattform verantwortlichen Person. In diesem Zusammenhang ist auf die Bestimmungen des Diffamierungsgesetzes von 2024 hinzuweisen, das vom Unterhaus des irischen Parlaments verabschiedet wurde und derzeit (Oktober 2025) im Oberhaus auf der Ausschussebene geprüft wird.[554] In Anbetracht der potenziellen Schwierigkeit, Personen zu identifizieren, die diffamierende Äußerungen online veröffentlichen, wird in Teil 9 Abschnitt 22 des Gesetzentwurfs vorgeschlagen, das Diffamierungsgesetz von 2009 dahingehend zu ändern, dass Einzelpersonen eine Anordnung des Bezirksgerichts beantragen können, wonach die betreffende Online-Plattform (der „Informationsdiensteanbieter“) die Identität der Person offenlegen muss, die das diffamierende Material veröffentlicht hat. Wer eine solche Offenlegung beantragt, muss zur Zufriedenheit des Bezirksgerichts nachweisen, dass eine Diffamierung stattgefunden hat und dass ein Prozess dagegen Erfolg haben dürfte.[555]

Bei rechtswidrigen und schädlichen Inhalten muss die CnaM gemäß Abschnitt 7(2)(d) des Rundfunkgesetzes von 2009 (in seiner geänderten Fassung) dafür sorgen, dass ihre Regulierungsmaßnahmen „Programmmaterial, nutzergenerierten Inhalten und anderen Inhalten, die schädlich oder rechtswidrig sind, entgegenwirken“. Nach Abschnitt 139K(3) des Rundfunkgesetzes ist die CnaM ausdrücklich verpflichtet, wie oben erwähnt, einen Kodex für Online-Sicherheit zu erstellen, der für Anbieter von VSP-Diensten gilt.

Abschnitt 139A des Rundfunkgesetzes von 2009 (in seiner geänderten Fassung) legt fest, um welche Kategorien schädlicher Online-Inhalte es in dem Kodex geht. Abschnitt 139A(2)(a) verweist auf eine Liste mit „deliktsspezifischen Kategorien von Online-Inhalten“ in Anhang 3. Abschnitt 4 von Anhang 3 definiert hetzerische und zu Gewalt aufstachelnde Äußerungen als „Online-Inhalte, mit denen eine Person schriftliches Material oder eine Aufzeichnung von visuellen Bildern oder Tönen veröffentlicht oder verbreitet, die gegen Abschnitt 2(1) des Gesetzes über das Verbot der Aufstachelung zum Hass von 1989 verstoßen (Material, Bilder oder Töne, die eine Drohung, Beschimpfung oder Beleidigung

[554] House of the Oireachtas, Defamation (Amendment) Bill 2024, Bill 67 of 2024.

[555] Nebenbei sei darauf hingewiesen, dass im März 2022 vier irische Abgeordnete einen Gesetzentwurf („Responsibility of Social Media Platforms (Defamation Amendment) Bill“) eingebracht haben, der es ermöglicht hätte, Social-Media-Plattformen wegen Diffamierung zu verurteilen, wenn dort diffamierende Äußerungen getätigt werden und die Plattform nicht angeben kann, von wem die Äußerungen stammen. Da es sich bei dem Gesetzentwurf jedoch um eine Privatinitiative der vier Abgeordneten handelte, fand er nicht die Unterstützung der Regierung und ging nicht durch das Parlament.

darstellen und dazu bestimmt oder unter Berücksichtigung aller Umstände geeignet sind, Hass zu schüren)". Nach Abschnitt 5 von Anhang 3 zählen zu den schädlichen Inhalten auch Sendungen, die „gegen Abschnitt 3(1) des Gesetzes über das Verbot der Aufstachelung zum Hass von 1989 verstoßen (Bilder oder Töne, die eine Drohung, Beschimpfung oder Beleidigung darstellen und deren Ausstrahlung dazu bestimmt oder unter Berücksichtigung aller Umstände geeignet ist, Hass zu schüren)".

Die Berufung auf das Gesetz über das Verbot der Aufstachelung zum Hass von 1989[556] ist potenziell problematisch, weil dieses Gesetz, wie weiter unten erörtert, als fehlerhaft gilt. Es verbietet die Aufstachelung zum Hass gegen eine Gruppe von Personen aufgrund ihrer „Rasse, Hautfarbe, Nationalität, Religion, ethnischen oder nationalen Herkunft, Zugehörigkeit zur Bevölkerungsgruppe der Fahrenden oder sexuellen Orientierung".

Obwohl das Gesetz über das Verbot der Aufstachelung zum Hass von 1989 die Aufstachelung zum Hass unter Strafe stellt, gilt es in erster Linie als Maßnahme gegen Hetze. Aufstachelung umfasst die Veröffentlichung, Ausstrahlung und Vorbereitung von Materialien, und die Anwendung des Gesetzes von 1989 ist nicht auf Offline-Verhalten beschränkt, sondern erstreckt sich auch auf das Verwenden von Wörtern, das Zeigen von Verhaltensweisen und das Ausstellen von Materialien an „jedem anderen Ort als innerhalb einer Privatwohnung".[557]

Das Gesetz über das Verbot der Aufstachelung zum Hass aus dem Jahr 1989 gilt jedoch als fehlerhaft: In einem Bericht der Rechtsreformkommission von 2016 über schädliche Kommunikation und digitale Sicherheit heißt es, dass „das Gesetz von 1989 stark wegen seiner offenbar mangelnden Wirksamkeit kritisiert wurde, die sich in der begrenzten Anzahl von Anklagen zeigt, die auf Basis dieses Gesetzes erhoben wurden".[558] Auch der UN-Ausschuss für die Beseitigung der Rassendiskriminierung hat in seinen Bemerkungen zu Irland die Befürchtung geäußert, dass das Gesetz von 1989 über das Verbot der Aufstachelung zum Hass bei der Bekämpfung rassistischer Hetze, insbesondere im Internet, unwirksam war.[559] Einige Wissenschaftler haben das Gesetz über das Verbot der Aufstachelung zum Hass von 1989 als „für die Bekämpfung von Hasskriminalität offenkundig ungeeignet" bezeichnet und eine Reform gefordert, die insbesondere den Kontext der Cyber-Hasskriminalität berücksichtigt.[560]

Um diese Mängel zu beheben, ersetzte die damalige Regierung im Jahr 2021 das Gesetz über das Verbot der Aufstachelung zum Hass von 1989 durch ein Gesetz, das neue und verschärfte Straftatbestände vorsah, darunter auch einen neuen Straftatbestand der Aufstachelung. Im April 2021 wurde das allgemeine Konzept eines Gesetzentwurfs veröffentlicht, der vorsieht, dass Hasskriminalität aufgrund der Hautfarbe, der sexuellen Orientierung oder des Geschlechts, einschließlich des Geschlechtsausdrucks oder der Geschlechtsidentität, unter Strafe gestellt wird. Weitere neue „geschützte Merkmale" sind

---

[556] Prohibition of Incitement to Hatred Act 1989.
[557] Ebd., Abschnitt 2.(1)(b)(i).
[558] Law Reform Commission, „Harmful Communications and Digital Safety", Bericht LRC 116-2016, Dublin 2016.
[559] Committee on the Elimination of Racial Discrimination, „Concluding observations on the combined fifth to ninth reports of Ireland", UN, CERD/C/IRL/CO/5-9, Genf, 23. Januar 2020.
[560] Haynes A., Schweppes J., „Lifecycle of a hate Crime: Country Report for Ireland", Irish Council for Civil Liberties, Dublin, 2017.

die Rasse, die Nationalität, die Religion, die ethnische und nationale Herkunft sowie eine etwaige Behinderung des Opfers.[561] Eine überarbeitete Fassung des Gesetzentwurfs wurde im Oktober 2022 als Criminal Justice (Incitement to Violence or Hatred and Hate Offences) Bill veröffentlicht.[562]

Das neue Gesetz sollte jede vorsätzliche oder fahrlässige Kommunikation oder Verhaltensweise unter Strafe stellen, das geeignet ist, zu Gewalt oder Hass gegen eine oder mehrere Personen aufzustacheln, weil sie mit einem der obigen geschützten Merkmale in Verbindung gebracht werden. Zudem sollte es strafverschärfend wirken, wenn bestimmte Straftaten aus Hass gegen ein geschütztes Merkmal begangen wurden.

Trotz einiger Debatten über den Vorschlag wurde das neue Gesetz 2023 vom Unterhaus des Parlaments verabschiedet.[563] Nach Kritik von Hinterbänklern und einigen Senatoren kam der Vorschlag jedoch im Oberhaus ins Stocken. Im Oktober 2024, als die Legislaturperiode des Parlaments zu Ende ging (im November 2024 standen Parlamentswahlen an), entschied die damalige Justizministerin, dass es am pragmatischsten sei, jegliche Verweise auf die Aufstachelung zu Gewalt oder Hass (sowie auf den EU-Rahmenbeschluss zur Bekämpfung von Rassismus und Fremdenfeindlichkeit) aus dem Gesetzentwurf zu streichen.[564] Daher ist die Grundlage für die Definition von hetzerischen und zu Gewalt aufstachelnden Äußerungen nach wie vor das Gesetz von 1989.

5.2.3 Der Kodex für Online-Sicherheit in der Praxis

Bei der Vorstellung des irischen Rahmenwerks für Online-Sicherheit betont die CnaM, dass sie als irische Medienaufsichtsbehörde Inhalte nicht sofort aus dem Internet entfernen kann. Vielmehr hat sie dafür zu sorgen, dass die in ihre Zuständigkeit fallenden Online-Plattformen (und Fernsehveranstalter) Maßnahmen ergreifen, damit keine rechtswidrigen oder schädlichen Inhalte gezeigt werden. Die Hauptverantwortung für den Umgang mit schädlichen Inhalten (einschließlich Hetze und Aufstachelung zu Gewalt) liegt also bei den Plattformen selbst. Die CnaM weist darauf hin, dass die Plattformen rechtlich verpflichtet sind, ihre eigenen Regeln für Inhalte durchzusetzen und Mechanismen bereitzustellen, mit denen Nutzer Inhalte melden können, die gegen diese Regeln verstoßen.

Daher besteht die Aufgabe der CnaM darin, einzugreifen, wenn diese Meldemechanismen nicht wie vorgesehen funktionieren. Die CnaM weist die Nutzer darauf hin, dass diese sie informieren sollten, wenn sie Schwierigkeiten haben, eine Meldung an

[561] Department of Justice, Home Affairs and Migration, „New Bill to tackle hate crime and hate speech includes clear provision to protect freedom of expression“, Pressemitteilung, 27. Oktober 2022.
[562] Irish Council for Civil Liberties, „Better engagement with affected communities paramount as hate crime and extreme hate speech legislation advances at the Oireachtas“, Pressemitteilung, 27. Oktober 2022 (Dublin: ICCL).
[563] Public Interest Law Alliance, „New Bill to tackle hate crime and hate speech is currently before the Seanad“, Pressemitteilung, 17. Mai 2023.
[564] Rahmenbeschluss 2008/913/JI des Rates vom 28. November 2008 zur strafrechtlichen Bekämpfung bestimmter Formen und Ausdrucksweisen von Rassismus und Fremdenfeindlichkeit, ABl. L 328/55, 6. Dezember 2008.

eine Plattform abzusetzen, oder wenn sie der Meinung sind, dass eine Plattform im Umgang mit einer Meldung nicht korrekt vorgegangen ist.

Für den Fall, dass Nutzer einer Plattform rechtswidrige Inhalte melden und keine zeitnahe Antwort erhalten und/oder der Inhalt nicht entfernt wird, weist die CnaM darauf hin, dass sie dies melden können. Allerdings weist sie auch darauf hin, dass ihre Befugnisse danach begrenzt sind: „Unsere Beratungsstelle dankt Ihnen für Ihre Meldung, berät Sie und nimmt Ihre Bedenken auf. Wir können diesen Inhalt aber nicht für Sie entfernen."

Im besten Fall leitet die CnaM die Meldung dann an ihr Plattformaufsichtsteam weiter, „das darauf hinwirken wird, dass die Plattformen ihre Systeme verbessern". In dringenderen Fällen – bei direkten Online-Bedrohungen der physischen Sicherheit einer Person – rät die CnaM den Nutzern, sich direkt an die irische Polizei zu wenden. Auch hier betont die CnaM, dass sich ihre Aufgabe darauf beschränkt, auf Plattformen systemische Risiken zu untersuchen und nicht konkrete Vorfälle.

Hierzu verlangt Artikel 34 des DSA, wenn auch nicht in direktem Zusammenhang mit Artikel 28b der AVMD-RL, dass die benannten VLOPs und VLOSEs „alle systemischen Risiken […], die sich aus der Konzeption oder dem Betrieb ihrer Dienste und seinen [sic!] damit verbundenen Systemen, einschließlich algorithmischer Systeme, oder der Nutzung ihrer Dienste ergeben", ermitteln, analysieren und sorgfältig bewerten.

Alle zehn VLOPs und VLOSEs mit Hauptsitz in Irland haben der Europäischen Kommission eine Bewertung der systemischen Risiken nach Artikel 34 des DSA vorgelegt.[565] Dazu gehört jeweils auch ein Abschnitt zum Thema Hetze. In den ersten vorgelegten Bewertungen weisen alle zehn in Irland ansässigen Plattformen auf das inhärente Risiko hin, dass ihre Plattformen für Hetze genutzt werden könnten, erklären jedoch, dass das tatsächliche Risiko aufgrund ihrer internen Maßnahmen zur Risikominderung gering sei. Allerdings liegt es auch nicht im Interesse einer Plattform, sich selbst als ein erhebliches Risiko in Bezug auf rechtswidrige Äußerungen darzustellen.

Da das Rahmenwerk für Online-Sicherheit und der zugehörige Kodex erst vor Kurzem eingeführt wurden, ist es für eine objektive Bewertung ihrer Wirksamkeit vielleicht noch zu früh. Bemerkenswert ist, dass sich die CnaM im Juni 2025 gezwungen sah, ein gesetzliches Informationsschreiben an die Plattform X zu richten, weil X ihr nicht genügend Informationen zur Verfügung gestellt hatte, um feststellen zu können, ob X ausreichende Maßnahmen ergreift, um die Kinderschutzbestimmungen des Kodex einzuhalten.[566] X hatte schon im Dezember 2024 gegen die Regeln geklagt, die ihm im Rahmen des Kodex für Online-Sicherheit auferlegt worden waren, weil diese eine „regulatorische Übertreibung"[567] darstellten und über das nach Artikel 28b der AVMD-RL erforderliche Maß hinausgingen. Diese Klage wurde vom irischen High Court im Juli 2025 abgewiesen, und im selben Monat

[565] Tremau Digital Services Act Database. Abrufbar unter: https://tremau.com/resources/dsa-database/, 31. Oktober 2025. Siehe auch: DSA: Risk Assessment & Audit Database.
[566] Coimisiún na Meán, „Coimisiún na Meán issues statutory information notice to X", Pressemitteilung, 17. Juni 2025.
[567] Siehe Gallagher, F., „X Loses High Court Challenge Brought against Coimisiún na Meán Safety Code", *The Irish Times*, 29. Juli 2025.

führte X neue Maßnahmen zur Altersfeststellung ein, um die Bedenken von CnaM hinsichtlich der Sicherheit von Kindern auszuräumen.[568]

Erwähnenswert sind auch die Schlussfolgerungen einer von der CnaM im September 2025 veröffentlichten Studie zu den Online-Erfahrungen der Kandidaten für die irischen Kommunal- und Parlamentswahlen von 2024.[569] Der Kodex für Online-Sicherheit wurde erst nach der Kommunalwahl im Juni 2024 veröffentlicht, trat aber vor der Parlamentswahl im November 2024 in Kraft. Die Studie ergab, dass 48 % der Kandidaten für die Kommunalwahl entweder Beleidigungen, Beschimpfungen oder Hetze im Internet, Gewalt oder Einschüchterung im Internet oder aber Nachahmungen der eigenen Person erlebt haben.[570] Bei der der Parlamentswahl im November 2024 stieg dieser Anteil auf 59 %. Außerdem ergab die Studie, dass bei der Kommunalwahl 24 % und bei der Parlamentswahl 21 % der Kandidaten, die „soziale Medien nutzten und einschlägiges Online-Verhalten erlebten, im Wahlkampf online damit bedroht wurden, *sie zu töten oder ihnen schweren Schaden zuzufügen*“[571] (Hervorhebung hinzugefügt).

Darüber hinaus hatten bei der Kommunalwahl 58 % und bei der Parlamentswahl 69 % der Kandidaten für allgemeine Wahlen, die solches Verhalten erlebt hatten, dies den entsprechenden Online-Plattformen nicht gemeldet.[572] Viele hatten nicht gewusst, wie man eine Meldung macht, oder die Meldefunktion auf der betreffenden Plattform nicht gefunden, oder das Ausmaß der hetzerischen oder gewalttätigen Inhalte war zu groß gewesen, um alle Fälle zu melden. Bei Weitem am häufigsten (bei der Kommunalwahl von 59 % und bei der Parlamentswahl von 72 % der Kandidaten) wurde als Grund jedoch die Annahme genannt, dass die Meldung nicht effektiv bearbeitet würde.[573] Eine „Annahme“ ist zwar kein zwingender Grund für die Schlussfolgerung, dass das irische Rahmenwerk für Online-Sicherheit ineffektiv ist, aber die Ergebnisse dieser Studie können als besorgniserregend gelten.

[568] *X Internet UnLtd Company v. Coimisiún na Meán* [2025] IEHC 442.
[569] Coimisiún na Meán, „On the digital campaign trail: Election candidates' online experiences in the 2024 elections“, (Dublin: CnaM).
[570] Ebd., S. 5.
[571] Ebd., S. 6.
[572] Ebd., S. 81.
[573] Ebd., S. 86.

5.3 Das Beispiel Österreich

Dr Clara Rauchegger, Universität Innsbruck

5.3.1 Nationaler Rechtsrahmen für Plattformen

5.3.1.1 Das österreichische Kommunikationsplattformen-Gesetz

2020 verabschiedete der österreichische Gesetzgeber ein gesetzliches Maßnahmenpaket zur Bekämpfung von Hassreden im Internet, Verleumdung, Cybermobbing und anderen rechtswidrigen Verhaltensweisen auf Online-Plattformen. Das gemeinsame Ziel dieser Maßnahmen war der Kampf gegen „Hass im Internet".[574] Das Hass-im-Netz-Bekämpfungsgesetz trat im Januar 2021 in Kraft.

Ein zentraler Bestandteil dieses gesetzliches Maßnahmenpakets war das neu verabschiedete Bundesgesetz über Maßnahmen zum Schutz der Nutzer auf Kommunikationsplattformen (Kommunikationsplattformen-Gesetz – KoPl-G).[575] Nach dem Vorbild des deutschen Netzwerkdurchsetzungsgesetzes (NetzDG)[576] wurde damit eine Reihe von Verpflichtungen für große Online-Plattformen eingeführt. Sie mussten ein Meldesystem bereitstellen, damit Nutzer auf rechtswidrige Inhalte hinweisen konnten, und offensichtlich rechtswidrige Inhalte binnen 24 Stunden und Inhalte, bei denen eine detaillierte Prüfung zur Feststellung ihrer Rechtswidrigkeit erforderlich ist, binnen sieben Tagen entfernen oder sperren.[577] Darüber hinaus waren Plattformen verpflichtet, Transparenzberichte[578] zu veröffentlichen und einen verantwortlichen Beauftragten in Österreich zu benennen.[579]

[574] Bundesgesetz, mit dem das Kommunikationsplattformen-Gesetz, das E-Commerce-Gesetz, das Mediengesetz, das Strafgesetzbuch, die Strafprozessordnung, das Einführungsgesetz zu den Strafgesetzen, das Allgemeine Bürgerliche Gesetzbuch und die Zivilprozessordnung geändert werden (Hass-im-Netz-Bekämpfungsgesetz), BGBl. I Nr. 151/2020.

[575] Bundesgesetz über Maßnahmen zum Schutz der Nutzer auf Kommunikationsplattformen (Kommunikationsplattformen-Gesetz – KoPl-G), BGBl. I Nr. 151/2020.

[576] Netzwerkdurchsetzungsgesetz (NetzDG) vom 1. September 2017, BGBl. I, S. 3352. Für einen Überblick über die ursprüngliche Fassung des NetzDG siehe Schmitz, S. und Berndt, C., *The German Act on Improving Law Enforcement on Social Networks (NetzDG):A Blunt Sword?*, 2018.

[577] § 3 KoPl-G.

[578] § 4 KoPl-G.

[579] § 5 KoPl-G.

5.3.1.2 Das EuGH-Urteil zur Ungültigkeit des Kommunikationsplattformen-Gesetzes

Das KoPl-G wurde vom EuGH in seinem Urteil in der Rechtssache *Google Ireland gegen KommAustria*[580] für unvereinbar mit der EC-RL[581] erklärt. Konkret stellte der EuGH einen Verstoß gegen das in dieser Richtlinie verankerte Herkunftslandprinzip fest.

Nach dem Herkunftslandprinzip müssen Anbieter von Diensten der Informationsgesellschaft in der Regel nur die nationalen Rechtsvorschriften ihres Herkunftslandes einhalten, das heißt des Mitgliedstaates, in dem sie niedergelassen sind.[582] Die Bestimmungsländer, das heißt die Mitgliedstaaten, in denen die Dienste angeboten werden, können den in einem anderen Mitgliedstaat niedergelassenen Diensteanbietern nicht ihre eigenen rechtlichen Vorschriften auferlegen.[583] Das Herkunftslandprinzip erstreckt sich auf den „koordinierten Bereich", das heißt auf alle „für die Anbieter von Diensten der Informationsgesellschaft und die Dienste der Informationsgesellschaft in den Rechtssystemen der Mitgliedstaaten festgelegten Anforderungen, ungeachtet der Frage, ob sie allgemeiner Art oder speziell für sie bestimmt sind."[584]

Als die EC-RL 2000 erlassen wurde, schien es unrealistisch, dass die EU die einschlägigen Rechtsvorschriften für Dienste der Informationsgesellschaft umfassend harmonisieren würde.[585] Gleichzeitig wollte die EU aber die Entwicklung von Diensten der Informationsgesellschaft unterstützen, um Innovation und Wirtschaftswachstum zu fördern und „die Wettbewerbsfähigkeit der europäischen Industrie [zu] stärken".[586] In Ermangelung harmonisierter Rechtsvorschriften in den betreffenden Bereichen sollte das Herkunftslandprinzip die Hemmnisse beseitigen, die „in Unterschieden der innerstaatlichen Rechtsvorschriften sowie in der Rechtsunsicherheit hinsichtlich der auf Dienste der Informationsgesellschaft jeweils anzuwendenden nationalen Regelungen" bestehen.[587] Der Gedanke dahinter ist, Hindernisse durch die Vorschrift zu beseitigen, dass „die Dienste der Informationsgesellschaft grundsätzlich dem Rechtssystem desjenigen Mitgliedstaats unterworfen werden [sollten], in dem der Anbieter niedergelassen ist".[588] Sie werden „nur durch Vorschriften des Mitgliedstaats geregelt [...], in dessen Hoheitsgebiet die Anbieter dieser Dienste niedergelassen sind."[589] Die EC-RL lässt unter bestimmten Bedingungen Abweichungen von diesem Prinzip zu.[590] Insbesondere kann der freie Verkehr von Diensten der Informationsgesellschaft eingeschränkt werden, wenn dies aus Gründen der öffentlichen Ordnung, der öffentlichen Gesundheit, der öffentlichen Sicherheit oder des

[580] C-376/22 *Google Ireland gegen KommAustria* (EuGH, 9. November 2023) ECLI:EU:C:2023:835.
[581] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, ABl. L 178, 17. Juli 2000.
[582] Art. 3 Abs. 1 EC-RL.
[583] Art. 3 Abs. 2 EC-RL.
[584] Definition des Begriffs „koordinierter Bereich" in Art. 2 lit. h) EC-RL.
[585] Raue, B., "*Case Note on CJEU, Google Ireland and Others, C-376/22*", Neue Juristische Wochenschrift, 2024, S. 201-205, 204.
[586] Erwägungsgrund 2 der EC-RL.
[587] Erwägungsgrund 5 der EC-RL.
[588] Erwägungsgrund 22 der EC-RL.
[589] C-376/22 *Google Irland gegen KommAustria* (EuGH, 9. November 2023), Rn. 42. ECLI:EU:C:2023:835.
[590] Art. 3 Abs. 4 EC-RL.

Verbraucherschutzes erforderlich ist.[591] Eine zentrale wesentliche Voraussetzung für diese Abweichung ist, dass die Maßnahme „einen bestimmten Dienst der Informationsgesellschaft" betreffen muss.[592] Die zentrale Frage in der Rechtssache *Google Ireland gegen KommAustria* war, ob generell-abstrakte Maßnahmen, die allgemein für bestimmte Kategorien von Diensten der Informationsgesellschaft gelten, als Maßnahmen, die „einen bestimmten Dienst der Informationsgesellschaft betreffen", ausgelegt werden und daher als zulässige Abweichungen vom Herkunftslandprinzip gerechtfertigt sein können.[593] Der EuGH erklärte in seinem Urteil, dass dies nicht der Fall sei. Die Möglichkeit, vom Herkunftslandprinzip abzuweichen, erstrecke sich nicht auf generell-abstrakte Maßnahmen, wie sie das KoPl-G vorsehe. Letzteres wurde daher nach Ansicht des Gerichts unter Verstoß gegen die EC-RL erlassen.

Der EuGH nahm eine wörtliche, systematische und teleologische Auslegung vor, um zu diesem Schluss zu gelangen. Hinsichtlich des Wortlauts betonte der EuGH, dass sich die Abweichungsbestimmung auf einen „bestimmten Dienst der Informationsgesellschaft" beziehe. Die Verwendung des Singulars und des Adjektivs „bestimmt" deute darauf hin, dass sich die Abweichung nicht auf generell-abstrakte Maßnahmen erstrecke, die allgemein auf eine Kategorie von Diensten der Informationsgesellschaft abzielen.[594] Bei seiner systematischen Auslegung stützte sich der EuGH auf die Verfahrensbedingungen, die die Mitgliedstaaten einhalten müssen, wenn sie vom Herkunftslandprinzip abweichen wollen.[595] In teleologischer Hinsicht betonte der EuGH, dass die EC-RL darauf abziele, die Freiheit der Dienste der Informationsgesellschaft zu gewährleisten, ein Ziel, das durch die Grundsätze der Aufsicht im Herkunftsmitgliedstaat und der gegenseitigen Anerkennung verfolgt werde.[596] Diese Grundsätze würden in Frage gestellt, wenn es den Mitgliedstaaten gestattet wäre, generell-abstrakte Maßnahmen zu ergreifen, die auf eine Kategorie von Diensten der Informationsgesellschaft innerhalb des koordinierten Bereichs abzielen.[597] Insgesamt entschied sich der EuGH für eine binnenmarktfreundliche Auslegung des Herkunftslandprinzips.[598] Er stärkte dieses Prinzip und schränkte die Freiheit der Mitgliedsstaaten ein, Rechtsvorschriften wie das KoPl-G oder das deutsche NetzDG zu erlassen.[599/600] Wie ein Kommentator anmerkte, setzte der EuGH ein deutliches Ausrufezeichen hinter das Herkunftslandprinzip.[601]

---

[591] Art. 3 Abs. 4 lit. a) (i) EC-RL.
[592] Art. 3 Abs. 4 lit. a) (ii) EC-RL.
[593] Siehe C-376/22 *Google Ireland gegen KommAustria*, op. cit., Rn. 25.
[594] Ebd., Rn. 27.
[595] Art. 3 Abs. 4 lit. b) EC-RL; ebd. [35-38].
[596] Siehe C-376/22 *Google Ireland gegen KommAustria*, op. cit., Rn. 39-59.
[597] Ebd., Rn. 60.
[598] Knoke, L., Krüger, H. und Sachs, C., „EuGH stärkt Herkunftslandprinzip: Zugleich Besprechung von EuGH Urt. v. 9.11.2023 - C-376/22, EuZW 2024, 137 - Google Ireland u.a.", Europäische Zeitschrift für Wirtschaftsrecht, 2024, S. 957-961, 958.
[599] Zum deutschen NetzDG siehe auch Kapitel 4.2.1.
[600] Liesching, M., „Das Herkunftslandprinzip limitiert Alleingänge nationaler Gesetzgeber: Anmerkung zu EuGH, Urteil vom 9.11.2023 - C-376/22", Zeitschrift für Urheber- und Medienrecht, 2024, S. 205-207, 207; Wimmer, N. und Teetzmann, C. „Anmerkung zu Google Ireland und andere, C-376/22", MMR – Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT, 2024, S. 157-162, 162.
[601] Mantz, R., „Herkunftslandprinzip versus NetzDG - Wie geht es weiter mit den Pflichten von Diensteanbietern?" Zugleich Besprechung von EuGH "Google Ireland u.a.", Gewerblicher Rechtsschutz und Urheberrecht, 2024, S. 34-37, 37.

5.3.1.3 Relevanz des Urteils für die Auslegung des DSA

Nach den Feststellungen des EuGH wurde das KoPl-G 2024 durch das DSA-Begleitgesetz (DSA-BegleitG) aufgehoben.[602] Mit diesem Gesetz wurde darüber hinaus eine Reihe von Änderungen zu bestehenden österreichischen Rechtsvorschriften vorgenommen und ein neues Koordinator-für-Digitale-Dienste-Gesetz (KDD-G) geschaffen.[603]

Gemäß Artikel 49 DSA müssen die Mitgliedstaaten einen nationalen Koordinator für digitale Dienste (Digital Services Coordinator – DSC/KDD) benennen. In Österreich wurde die Kommunikationsbehörde Austria (KommAustria) als nationaler KDD benannt.[604] KommAustria[605] ist das Regulierungs- und Aufsichtsorgan für Rundfunk und elektronische audiovisuelle Medien und wäre auch für die Durchsetzung des KoPl-G zuständig gewesen, das wie oben beschrieben vom EuGH für nichtig erklärt wurde. Sie wird bei den Aufgaben, die sich aus dem DSA ergeben, von einer Geschäftsstelle der Regulierungsbehörde unterstützt, die als privates Unternehmen organisiert ist, das sich vollständig im Besitz des Staates befindet.[606]

Darüber hinaus enthält das KDD-G eine lange Liste von Verwaltungsübertretungen, die Anbieter von Vermittlungsdiensten begehen, wenn sie gegen Bestimmungen des DSA verstoßen.[607] Diese Verwaltungsübertretungen werden von KommAustria mit einer Geldstrafe von bis zu 1 % (bei Nichtbereitstellung von Informationen oder Nichtduldung einer Nachprüfung) bzw. bis zu 6 % (bei allen anderen Übertretungen) des weltweiten Jahresumsatzes des Anbieters im vorangegangenen Geschäftsjahr geahndet.[608] Liegen die Voraussetzungen gemäß Artikel 51 Absatz 3 lit. b DSA vor, hat KommAustria beim Bundesverwaltungsgericht einen Antrag auf Anordnung einer vorübergehenden Einschränkung des Zugangs zu dem betroffenen Dienst oder, soweit dies technisch nicht möglich ist, zur Online-Schnittstelle zu stellen.[609]

5.3.2 Der Spielraum für die Regulierung rechtswidriger Online-Inhalte nach dem EuGH-Urteil in der Rechtssache *Google Ireland gegen KommAustria*

Das EuGH-Urteil in der Rechtssache *Google Ireland gegen KommAustria* bleibt im Rahmen des DSA aktuell, „da diese Verordnung weder das Herkunftslandprinzip noch die Möglichkeit aufhebt, [...] von diesem Prinzip abzuweichen."[610] Gemäß Artikel 2 Absatz 3 DSA

---

[602] Art. 10 Abs. 1 Koordinator-für-digitale-Dienste-G, BGBl. I, Nr. 182/2023.
[603] Für einen Überblick siehe Wittmann, H., „Das DSA-Begleitgesetz: Neue Instrumente zur Bekämpfung von ‚Hass-im-Netz'", Medien und Recht, 2023, S. 298-301.
[604] § 2 Ziff. (1) *Koordinator-für-digitale-Dienste-G*, BGBl. I, Nr. 182/2023.
[605] Siehe Die Kommunikationsbehörde Austria (KommAustria) | RTR.
[606] § 2 Ziff. (2) Koordinator-für-digitale-Dienste-G; RTR-Medien | RTR.
[607] § 5 Koordinator-für-digitale-Dienste-G.
[608] § 6 Koordinator-für-digitale-Dienste-G.
[609] § 4 Koordinator-für-digitale-Dienste-G.
[610] *Google Ireland gegen KommAustria*, Schlussanträge des Generalanwalts Szpunar vom 8. Juni 2023, ECLI:EU:C:2023:467, Rn. 8; Liesching, M., op. cit., S. 205-207.

berührt diese Verordnung nicht die Anwendung der EC-RL, die weiterhin in Kraft bleibt. Folglich gilt weiterhin das Herkunftslandprinzip.[611]

Darüber hinaus wird in Erwägungsgrund 9 des DSA darauf hingewiesen, dass die Mitgliedstaaten Vermittlungsdienste unter zwei Bedingungen regulieren können. Erstens müssen die nationalen Maßnahmen außerhalb des Anwendungsbereichs des DSA liegen. Zweitens müssen sie, wenn sie nicht in den Anwendungsbereich des DSA fallen, immer noch mit dem Herkunftslandprinzip der EC-RL in Einklang stehen. Dies bedeutet, dass eine nationale Regelung, die sich auf Anbieter aus anderen Mitgliedstaaten erstreckt und nicht in den Anwendungsbereich des DSA, aber in den koordinierten Bereich der EC-RL fällt, nur dann zulässig ist, wenn sie als zulässige Abweichung vom Herkunftslandprinzip gerechtfertigt ist (und nicht durch andere EU-Rechtsvorschriften harmonisiert ist).

Das Urteil in der Rechtssache *Google Ireland gegen KommAustria* wird darüber hinaus für die Auslegung des DSA von Bedeutung sein, der ebenfalls den Grundsatz der Aufsicht im Herkunftsmitgliedstaat befürwortet.[612] Nach Artikel 56 Absatz 1 DSA ist in der Regel der Mitgliedstaat, in dem sich die Hauptniederlassung des Anbieters von Vermittlungsdiensten befindet, exklusiv für die Überwachung und Durchsetzung des DSA zuständig. Wie die EC-RL sieht auch der DSA in abweichenden nationalen Rechtsvorschriften zu Vermittlungsdiensten eine Bedrohung für den freien Verkehr dieser Dienste.[613]

In seinem Anwendungsbereich harmonisiert der DSA die für Vermittlungsdienste im Binnenmarkt geltenden Vorschriften vollständig (Erwägungsgrund 9 des DSA). Es ist also nicht mehr der Herkunftsmitgliedstaat, der diese Regeln festlegt; dies hat bereits die EU getan.[614] Insbesondere legt der DSA gemäß Artikel 1 Absatz 2 einen Rahmen für die bedingte Haftungsbefreiung von Anbietern von Vermittlungsdiensten, besondere Sorgfaltspflichten für bestimmte Kategorien von Anbietern von Vermittlungsdiensten sowie Vorschriften für die Durchführung und Durchsetzung des DSA fest. Umgekehrt steht es den Mitgliedstaaten frei, Angelegenheiten zu regeln, die nicht unter den DSA fallen. Der DSA greift keiner nationalen Gesetzgebung zu rechtswidrigen Online-Inhalten vor.[615] Insbesondere definiert der DSA nicht, was online rechtswidrig ist, sondern überlässt dies den Mitgliedsstaaten.[616] Darüber hinaus sind nationale Vorschriften für rechtswidrige Online-Inhalte zulässig, wenn sie andere legitime Ziele des öffentlichen Interesses als die des DSA verfolgen oder wenn sie EU-Sekundärrecht umsetzen, das vom DSA unberührt bleibt.[617]

[611] Mischensky, L. und Denk, S., „Digital Services Act und das Herkunftslandprinzip der E-Commerce-Richtlinie“, Ecolex, 2024(3), S.226 ff, 227.
[612] Siehe Schroeder, W. und Reider, L., „Der rechtliche Kampf gegen Hass im Netz – Nationale Spielräume unter dem DSA“, Österreichische Jurist:innenzeitung, 2024(8), S. 465 ff., 467.
[613] Siehe Erwägungen 2, 4 und 9 DSA.
[614] Mischensky, L. und Denk, S., op. cit., S. 226 ff., 227.
[615] Schroeder, W. und Reider, L., op. cit., S. 465 ff., 467.
[616] Ebd., S. 468.
[617] Ebd., S. 467. Siehe Erwägungsgrund 9 des DSA (letzter Satz); Art. 2 Abs. 4 DSA.

5.3.3 Anwendung im Hinblick auf Cyber-Belästigung und bildbasierten sexuellen Missbrauch

Das gesetzliche Maßnahmenpaket zur Bekämpfung von Hass im Internet enthielt auch Abänderungen einer Reihe bestehender Gesetze, darunter mehrere Abänderungen des österreichischen Strafgesetzbuchs (StGB). Abgesehen vom KoPl-G bleibt die Gesetzgebung zu Hass im Internet weitgehend in Kraft.

Zu den neu eingeführten Straftatbeständen gehört jetzt fortdauernde Cyber-Belästigung.[618] Cyber-Belästigung kann entweder eine Verletzung der Ehre des Opfers oder die Verbreitung von Tatsachen oder Bildaufnahmen aus dem höchstpersönlichen Lebensbereich des Opfers ohne dessen Zustimmung sein. Sie ist strafbar, wenn sie geeignet ist, die Lebensführung des Opfers unzumutbar zu beeinträchtigen, und für eine größere Zahl von Personen über einen längeren Zeitraum wahrnehmbar ist. Die Strafe für fortdauernde Cyber-Belästigung ist Freiheitsentzug bis zu einem Jahr oder eine Geldstrafe. Die Straftat wird mit Freiheitsentzug bis zu drei Jahren geahndet, wenn sie zum Selbstmord oder versuchten Selbstmord des Opfers führt oder wenn sie fortgesetzt über einen Zeitraum von mehr als einem Jahr begangen wird oder für das Opfer länger als ein Jahr wahrnehmbar bleibt.

Eine weitere wichtige Änderung des StGB war die Einführung des Straftatbestands der unbefugten Bildaufnahmen (*Upskirting*).[619] *Upskirting* (oder *Downblousing*) bezeichnet das Fotografieren oder Aufnehmen des Schambereichs einer Person ohne deren Einwilligung, in der Regel indem eine Kamera unter den Rock oder das Kleid gerichtet wird. Dies wird nun mit Freiheitsentzug bis zu sechs Monaten oder einer Geldstrafe geahndet, unabhängig davon, ob die Bildaufnahmen letztlich veröffentlicht wurden oder nicht.

Darüber hinaus ist die Aufstachelung zu Gewalt und Hass nun auch dann strafbar, wenn sie sich nicht gegen eine ganze Bevölkerungsgruppe, sondern gegen eine einzelne Person richtet, die dieser Gruppe angehört.[620] In jüngerer Zeit wurde – nicht durch das Hass-im-Netz-Bekämpfungsgesetz, sondern durch eine separate Gesetzesinitiative von 2025 – ein neuer Straftatbestand in das StGB aufgenommen:[621] Die unaufgeforderte Zusendung von Bildern, auf denen entblößte menschliche Genitalien zu sehen sind, ist nun strafbar und wird mit Freiheitsentzug bis zu sechs Monaten oder einer Geldstrafe belegt.

Neben den Abänderungen des StGB wurden auch andere Rechtsbereiche überarbeitet, um die Bekämpfung von Hass im Internet zu verbessern, insbesondere durch Änderungen im Zivil- und Strafprozessrecht.

Eine Abänderung der Zivilprozessordnung (ZPO) zielt darauf ab, dass Online-Inhalte, die eine Person in ihrer Menschenwürde verletzen, schnell entfernt werden.[622] Ist der geltend gemachte Anspruch hinreichend begründet, hat das zuständige Gericht auf Antrag

[618] 107c StGB; Artikel 8 des Hass-im-Netz-Bekämpfungsgesetzes, BGBl. I Nr. 151/2020.
[619] 120a StGB; Artikel 8 des Hass-im-Netz-Bekämpfungsgesetzes, op. cit.
[620] 283 StGB; Artikel 8 des Hass-im-Netz-Bekämpfungsgesetzes, op. cit.
[621] § 218 Abs. 1b StGB, gemäß BGBL. I Nr. 45/2025.
[622] § 549 ZPO, gemäß Artikel 3 des Hass-im-Netz-Bekämpfungsgesetzes, op. cit.

des Klägers ohne vorherige mündliche Verhandlung und ohne Anhörung des Beklagten einen Unterlassungsauftrag zu erlassen.

Darüber hinaus wurden mehrere Abänderungen an der Strafprozessordnung (StPO) vorgenommen. Die erste betrifft die Ausforschung der beschuldigten Person. Beleidigung und üble Nachrede sind in Österreich Privatanklagedelikte, was bedeutet, dass die Opfer in der Regel die Täter selbst ausforschen müssen, was häufig mit erheblichen Kosten verbunden ist. Das neue Verfahren erleichtert die Angelegenheit für die Opfer.[623] Zudem tragen die Opfer nicht mehr das Kostenrisiko im Falle eines Freispruchs des Beklagten.[624] Auch erhalten Opfer mehr psychosoziale und rechtliche Unterstützung während des Verfahrens.[625]

5.4 Das Beispiel Italien

Dr Giovanni de Gregorio, Professor für Recht und Technologie, Católica Global School of Law und Católica Lisbon School of Law

5.4.1 Nationaler Rechtsrahmen für Plattformen

Italiens Vorschriften für Online-Inhalte sind vom wachsenden Bewusstsein für die Gefahren von rechtswidrigen Inhalten und Desinformation beeinflusst. Der italienische Rechtsrahmen steht im Einklang mit dem europäischen Recht, insbesondere mit Blick auf den DSA, doch die Durchsetzung der Vorschriften erfolgt in erster Linie durch nationale Mechanismen. Dazu gehören sowohl Verwaltungs- als auch Justizbehörden, die bei der Bekämpfung rechtswidriger und schädlicher Inhalte wie Hetze und Desinformation eine Schlüsselrolle spielen. Im Mittelpunkt dieses Systems stehen nicht nur Gerichte, sondern auch Verwaltungsbehörden wie die Autorità per le Garanzie nelle Comunicazioni (AGCOM) und andere Regulierungsbehörden, die in bestimmten Fällen in Bereichen wie Datenschutz oder KI-Systeme tätig werden können.

Der DSA hat den Flickenteppich an Haftungsregeln für Vermittler ersetzt, den die Mitgliedstaaten im Rahmen der EC-RL entwickelt hatten.[626] In Italien führte die Einführung des DSA zur Teilaufhebung des Gesetzesdekrets,[627] das die frühere „Safe-Harbour-Regelung" der EU mit den Haftungsprivilegien im Rahmen der EC-RL kodifiziert hatte. Nach der neuen DSA-Regelung sind die Verpflichtungen für Online-Vermittler in Italien, die von

[623] § 71 StPO 1975; Artikel 10 des Hass-im-Netz-Bekämpfungsgesetzes, op. cit.
[624] § 390 Abs. 1a StPO 1975; Artikel 10 des Hass-im-Netz-Bekämpfungsgesetzes, op. cit.
[625] § 66b StPO 1975; Artikel 10 des Hass-im-Netz-Bekämpfungsgesetzes, op. cit.
[626] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, ABl. L 178, 17. Juli 2000.
[627] *Decreto legislativo 9 aprile 2003, n. 70, Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio ellettronico* (Gesetzesdekret Nr. 70/2003).

Melde- und Abhilfeverfahren für rechtswidrige Inhalte bis hin zu verstärkten Transparenz- und Rechenschaftsmaßnahmen für VLOPs reichen, direkt anwendbar, ähnlich wie andere Regulierungsinstrumente, etwa die Verordnung über terroristische Online-Inhalte (TCO-VO),[628] die Verordnung über politische Werbung (TTPW-VO),[629] und der European Media Freedom Act (EMFA).[630]

Darüber hinaus hat Italien sein innerstaatliches Medienrecht durch den Testo Unico sui Servizi di Media Audiovisivi (Konsolidiertes Gesetz über audiovisuelle Mediendienste – TUSMA) reformiert.[631] Der TUSMA setzt die überarbeitete AVMD-RL um und erweitert die regulatorischen Verpflichtungen auf „fornitori di Servizi di piattaforma per la condivisione di video" (Anbieter von VSP-Diensten), die mit YouTube vergleichbare Dienste umfassen. Diese Dienste unterliegen nun inhaltlichen Standards, einschließlich Vorschriften über Hetze, Jugendschutz und Aufstachelung zu Gewalt. Diese Plattformen müssen Maßnahmen ergreifen, um die Verbreitung von Hass und öffentlichkeitsgefährdenden Inhalten einzuschränken, etwa durch Kennzeichnungs- und Anzeigesysteme, transparente Nutzungsbedingungen oder Tools zur Kontrolle durch Eltern.

5.4.2 Besondere Regeln für diffamierende, hetzerische und zu Gewalt aufstachelnde Äußerungen

Die Vorschriften über Hetze und Desinformation sind nicht nur mit der Plattformregulierung verbunden, sondern auch mit dem Straf- und Zivilrecht. Nach dem italienischen Strafgesetzbuch (*Codice Penale*)[632] ist Diffamierung die Schädigung des Rufs einer anderen Person durch Kommunikation mit mehreren Personen,[633] wobei ein schwerer Fall mit verschärften Strafen vorliegt, wenn die Tat durch die Presse oder ein anderes Mittel der Publizität begangen wird. Nach ständiger Rechtsprechung der italienischen Gerichte stellt das Internet, einschließlich sozialer Netzwerke, ein solches Mittel dar, sodass Online-Diffamierung als schwerwiegende Form der Diffamierung gilt.[634] Die Strafen reichen von Geldstrafen bis hin zu Freiheitsentzug von bis zu drei Jahren, wobei Freiheitsstrafen zunehmend durch Geldstrafen ersetzt werden. Das Strafgesetzbuch regelt ferner auch die

---

[628] Verordnung (EU) 2021/784 des Europäischen Parlaments und des Rates vom 29. April 2021 zur Bekämpfung der Verbreitung terroristischer Online-Inhalte, ABl. L 172/79, 17. Mai 2021.
[629] Verordnung (EU) 2024/900 des Europäischen Parlaments und des Rates vom 13. März 2024 über die Transparenz und das Targeting politischer Werbung, ABl. L 2024/900, 20. März 2024.
[630] Verordnung (EU) 2024/1083 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Schaffung eines gemeinsamen Rahmens für Mediendienste im Binnenmarkt und zur Änderung der Richtlinie 2010/13/EU (Europäisches Medienfreiheitsgesetz), ABl. L 2024/1083, 17. April 2024.
[631] *Decreto legislativo 8 novembre 2021, n. 208, attuazione della direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri, concernente il testo unico per la fornitura di servizi di media audiovisivi in considerazione dell'evoluzione delle realtà del mercato* (Gesetzesdekret Nr. 208/2021 – TUSMA).
[632] Codice Penale (Strafgesetzbuch, verabschiedet durch den Königlichen Erlass Nr. 1398/1930, geändert durch das Gesetzesdekret Nr. 63/2018).
[633] Artikel 595 des italienischen Strafgesetzbuchs.
[634] Siehe z. B. Oberster Gerichtshof Italiens, Urteil 3453/2023; Oberster Gerichtshof Italiens, Urteil 45680/2022.

Anstiftung zu und Rechtfertigung von Straftaten.[635] Es behandelt die öffentliche Aufforderung zur Begehung von Straftaten und die Verherrlichung von kriminellem Verhalten.

Die Bestimmungen zu diskriminierenden Äußerungen ergaben sich aus der Weiterentwicklung des italienischen Strafgesetzbuchs, dem sogenannten Mancino-Gesetz,[636] das die früheren Rechtsvorschriften gegen Faschismus und Rassismus ergänzt. Artikel 604-bis des Strafgesetzbuchs ahndet Propaganda, die auf Überlegenheit oder Hass rassischer, ethnischer, nationaler oder religiöser Gruppen basiert, sowie die Aufstachelung zu Diskriminierung oder Gewalt gegen solche Gruppen. Artikel 604-ter sieht einen erschwerenden Umstand vor, der das Strafmaß erhöht, wenn gewöhnliche Straftaten in diskriminierender Absicht begangen werden. Diese Bestimmungen stehen in erster Linie im Zusammenhang mit den internationalen Menschenrechtsnormen und den EU-Antidiskriminierungsvorschriften zur Bekämpfung rassistischer und fremdenfeindlicher Hetze im Internet. Weitere einschlägige Rechtsbeispiele finden sich im Gesetzesdekret 215/2003[637] zur Umsetzung der Richtlinie 2000/43/EG[638] zur Anwendung des Gleichbehandlungsgrundsatzes ohne Unterschied der Rasse oder der ethnischen Herkunft sowie im Gesetz Nr. 115/2016 gegen Völkermord und Verbrechen gegen die Menschlichkeit.[639]

Desinformation ist in Italien jedoch nicht speziell geregelt. Versuche, Rechtsvorschriften zur Bekämpfung von Online-Desinformation einzuführen, einschließlich eines Gesetzentwurfs zur Kriminalisierung von Desinformation,[640] sind bisher gescheitert. Während die Bekämpfung von Hetze im Strafrecht mehr Rechtsgrundlagen findet und durch EU- und andere nationale Rechtsrahmen gestärkt wird, wird Desinformation nur indirekt durch die Regulierung von Plattformen, medienrechtliche Verpflichtungen oder in Fällen, in denen sie sich mit bestehenden Straftatbeständen wie Diffamierung oder Aufstachelung zum Hass überschneidet, behandelt.

[635] Artikel 414 des italienischen Strafgesetzbuchs.
[636] Artikel 604-bis und 604-ter des italienischen Strafgesetzbuchs.
[637] *Decreto Legislativo 9 luglio 2003, n. 215, Attuazione della direttiva 2000/43/CE per la parità di trattamento tra le persone indipendentemente dalla razza e dall'origine etnica* (Gesetzesdekret Nr. 215/2003).
[638] Richtlinie 2000/43/EG des Rates vom 29. Juni 2000 zur Anwendung des Gleichbehandlungsgrundsatzes ohne Unterschied der Rasse oder der ethnischen Herkunft, 2000, ABl. L 180/22.
[639] *Legge 16 giugno 2016, n. 115, modifica all'articolo 3 della legge 13 ottobre 1975, n. 654, in materia di contrasto e repressione dei crimini di genocidio, crimini contro l'umanità e crimini di guerra, come definiti dagli articoli 6, 7 e 8 dello statuto della Corte penale internazionale* (Gesetz Nr. 115/2016).
[640] Gesetzentwurf 2688.

5.4.3 Anwendung im Hinblick auf diffamierende, hetzerische und zu Gewalt aufstachelnde Äußerungen

5.4.3.1 Administrative Durchsetzung und die Rolle der AGCOM

Für die administrative Durchsetzung der Inhaltsvorschriften ist in Italien die AGCOM zuständig. Ihr traditionelles Mandat, das die Regulierung von Telekommunikation und Rundfunk sowie die Gewährleistung von Pluralismus, Wettbewerb und Jugendschutz umfasst,[641] hat sich im Laufe der Zeit auf Online-Umgebungen ausgeweitet, von der Herausgabe unverbindlicher Verhaltenskodizes und der Einrichtung von Beobachtungsstellen und Überwachungssystemen bis hin zur Ernennung von Italiens Koordinator für digitale Dienste (KDD) gemäß dem DSA. Diese Schritte haben dazu beigetragen, dass sich die AGCOM von einem „Kommunikationswächter" zum wichtigsten institutionellen Akteur für die Regulierung von Online-Inhalten in Italien entwickelt hat.

Die Zuständigkeit der AGCOM in Italien ist auf ihr nationales Mandat beschränkt. Die ausschließliche Zuständigkeit für sehr große Plattformen in Bezug auf systemische Risiken liegt zwar bei der Europäischen Kommission, doch die AGCOM trägt dazu bei, die Einhaltung der Vorschriften zu überwachen und die Durchsetzung der Nutzerrechte auf nationaler Ebene zu gewährleisten. Zudem beteiligt sie sich auch am Europäischen Gremium für digitale Dienste, in dem die nationalen Behörden Informationen austauschen und gemeinsame Positionen entwickeln. Zu den Aufgaben der AGCOM gehört unter anderem, Verstöße gegen den DSA zu untersuchen, außergerichtliche Streitbeilegungsverfahren zu zertifizieren und sich mit anderen nationalen und europäischen Regulierungsbehörden abzustimmen.

Schon vor der Verabschiedung des DSA hat die AGCOM eine aktive Rolle gespielt. Die Behörde hat ein Regelwerk über den Schutz der Menschenwürde, den Grundsatz der Nichtdiskriminierung und den Kampf gegen Hetze verabschiedet[642] und damit Standards für alle Medien zur Verhinderung diskriminierender und beleidigender Inhalte festgelegt und mit Blick auf VSP-Anbieter Verhaltenskodizes gefördert sowie Formen der Koregulierung und Mechanismen für die Beaufsichtigung und Überwachung von Aktivitäten definiert. Dieses Instrument wurde dann durch ein weiteres Regelwerk[643] ergänzt, das auf den Schutz der individuellen Grundrechte ausgerichtet ist. Mit diesem Regelwerk wurden die Befugnisse der AGCOM auf den Kampf gegen Hetze ausgeweitet. Insbesondere werden darin verbindliche Kriterien festgelegt, an denen sich die Anbieter von audiovisuellen Mediendiensten, einschließlich Video-Sharing-Diensten, orientieren müssen, um die Aufstachelung zu Gewalt und Hass zu verhindern. Darüber hinaus führt das Regelwerk einen konkreten Sanktionsmechanismus ein, der es der AGCOM erlaubt, Bußgelder zu verhängen, wann immer sie eine Verletzung des Verbots der Aufstachelung zu Gewalt oder Hass gegen

[641] *Legge 31 luglio 1997, n. 249, Istituzione dell'Autorità per le garanzie nelle comunicazioni e norme sui sistemi delle telecomunicazioni e radiotelevisivo* (Gesetz Nr. 249/1997).
[642] AGCOM, Delibera 157/19/CONS.
[643] AGCOM, Delibera 37/23/CONS.

eine Person oder Personengruppe aus den in Artikel 21 der EU-GRC aufgeführten Gründen oder unter Verstoß gegen Artikel 604-bis des italienischen Strafgesetzbuchs feststellt.

Ein komplexeres Problem ist die Desinformation. Da das italienische Recht hier nur begrenzte Ansatzpunkte bietet, wird gegen Desinformation über verschiedene Ansätze indirekt vorgegangen, etwa über das Diffamierungs- und Verbraucherrecht, den Verbraucherschutz, die Durchsetzung von Urheberrechten oder Verwaltungsmaßnahmen. Der Ansatz der AGCOM besteht darin, die Medienkompetenz, die Transparenz politischer Werbung und die Kooperation mit Plattformen zu fördern, anstatt sich auf das Strafrecht zu stützen. So lässt sich dieser Rechtsrahmen auch auf Situationen anwenden, in denen sich in Bezug auf denselben Inhalt Desinformation und Hetze überschneiden. Tatsächlich nutzen Desinformationskampagnen oft Vorurteile oder diskriminierende Narrative aus, verstärken Stereotypen oder schüren die Feindseligkeit gegenüber bestimmten Gruppen.

Zudem setzt die AGCOM auch auf eine sanfte Durchsetzung durch Berichte, Leitlinien und Multi-Stakeholder-Foren. Seit 2017 koordiniert sie den Tavolo per il pluralismo e la correttezza dell'informazione sulle piattaforme digitali, eine Plattform, die Institutionen, Medien, Plattformen und die Zivilgesellschaft im Kampf gegen Desinformation zusammenbringt. Im Rahmen dieser Aktivitäten hat die AGCOM eine Untersuchung digitaler Plattformen sowie des Informationssystems durchgeführt und in ihren Berichten darüber die Verbreitung von Desinformation dargestellt und die Wahrnehmungen und Verhaltensweisen der Nutzer analysiert.[644] Darüber hinaus hat die AGCOM Leitlinien zur Gewährleistung eines gleichberechtigten Zugangs zu Online-Plattformen in Wahlkämpfen verabschiedet,[645] die im Rahmen ihres technischen Runden Tisches entwickelt wurden und den Einsatz von Tools zur Faktenprüfung sowie von Arbeitsgruppen zur Überwachung, Klassifizierung und Medienkompetenz förderten.

5.4.3.2 Gerichtliche Durchsetzung und Rolle der Gerichte

Bei der Durchsetzung der Vorschriften in Streitfällen über rechtswidrige Online-Inhalte spielen die Gerichte eine entscheidende Rolle. Italienische Gerichte werden regelmäßig mit Fällen von Diffamierung und Hetze auf Plattformen, insbesondere sozialen Medien, befasst. In Anbetracht der mit dem DSA eingeführten Möglichkeit für Nutzer, Entschädigungen zu fordern, dürfte diese Rolle sogar noch an Bedeutung gewinnen.[646] Neben der strafrechtlichen Haftung können die Opfer auch zivilrechtliche Ansprüche geltend machen, etwa auf Schadenersatz aus Delikthaftung,[647] oder einstweilige Verfügungen beantragen. Die Gerichte können ihnen Schadenersatz zusprechen und Abhilfemaßnahmen anordnen, etwa die Entfernung des diffamierenden Inhalts.

Die Gerichte wenden weiterhin dasselbe System der Vermittlerhaftung auf Basis der Haftungsbeschränkungen aus dem DSA an, etwa im Falle der Verantwortung von sozialen

[644] AGCOM, Delibera 309/16/CONS; Delibera 79/20/CONS.
[645] AGCOM, *Linee guida per la parità di accesso alle piattaforme online durante la campagna elettorale per le elezioni politiche 2018* (Leitlinien für den gleichberechtigten Zugang zu Online-Plattformen während des Wahlkampfs 2018).
[646] Artikel 54 DSA.
[647] Artikel 2043 des italienischen Zivilgesetzbuchs.

Medien und auch von Bloggern für Inhalte Dritter.[648] In diesem Zusammenhang hat sich der Oberste Gerichtshof Italiens auf die Unterscheidung zwischen passiven und aktiven Anbietern konzentriert[649] und bekräftigt, dass Anbieter von Online-Inhalten für diffamierendes Material haften, wenn sie dieses nicht unverzüglich entfernen, nachdem sie darauf hingewiesen wurden.

Allerdings haben Gerichte ähnliche Fälle von Online-Hetze unterschiedlich behandelt, etwa in den abweichenden Urteilen über die Entfernung der rechtsextremen Parteien CasaPound und Forza Nuova durch Facebook im Jahr 2019.[650] CasaPound erwirkte zunächst in Rom eine einstweilige Verfügung, wonach Facebook die Seite der Partei wiederherstellen musste, wobei das Gericht argumentierte, die Entfernung einer ansonsten legalen politischen Partei von der Plattform verstoße gegen die verfassungsmäßigen Rechte auf Meinungsäußerung und politische Beteiligung, während die Klage von Forza Nuova im Jahr 2020 von vornherein abgewiesen wurde, weil das Gericht feststellte, dass deren rassistische und faschistische Inhalte eindeutig gegen die Nutzungsbedingungen von Facebook verstießen und die Verbreitung von Hass kein Recht sei. Im Hauptverfahren im Jahr 2022 stellte das Gericht jedoch fest, dass der hetzerische Inhalt von CasaPound nicht unter den Schutz der Meinungsfreiheit fällt und die Deaktivierung der Konten durch Facebook daher rechtmäßig war. Zusammen verdeutlichen diese Fälle das Spannungsverhältnis in der italienischen Rechtsprechung zwischen dem Schutz des politischen Pluralismus und der Bekräftigung des vertraglichen Rechts und der Pflicht von Plattformen, Hetze zu entfernen.

Gleichzeitig haben die Gerichte die Verantwortung der Nutzer als primäre Rechtsverletzer bestätigt, insbesondere im Fall von diffamierenden Beiträgen in sozialen Medien. Die Herausforderung besteht jedoch darin, das Recht auf freie Meinungsäußerung mit anderen kollidierenden Verfassungsinteressen in Einklang zu bringen. So wurde die Verurteilung einer Frau wegen als rufschädigend eingestufter Facebook-Posts über ein Gemeinderatsmitglied vom Obersten Gerichtshof Italiens mit der Begründung aufgehoben, dass selbst stark formulierte oder vulgäre Kommentare rechtmäßig sein können, wenn sie eine valide Ausübung des Rechts auf Kritik darstellen.[651] Hauptvoraussetzung hierfür ist, dass solche Äußerungen verhältnismäßig bleiben, kontextuell angemessen sind und keine grundlosen persönlichen Angriffe oder Demütigungen darstellen. In einem anderen Fall, in dem es um die Verbreitung diffamierender Äußerungen durch einen ehemaligen Stadtrat ging, entschied das Gericht jedoch, dass die Verwendung beleidigender Ausdrücke und persönlicher Beschimpfungen die Grenzen legitimer politischer Kritik überschreitet, sodass in solchen Zusammenhängen die Diffamierungsgesetze anzuwenden seien.[652]

Die Gerichte stehen im Umgang mit Desinformation vor der Herausforderung, dass Rechtsbehelfe von Natur aus reaktiv sind und Verfahren erfordern, die eine gewisse Zeit in Anspruch nehmen, während sich Unwahrheiten im Internet schnell und unwiderruflich verbreiten können. Darüber hinaus bedeutet das Fehlen eines speziellen Rechtsrahmens für solche Inhalte, dass sich die Richter auf bestehende Bestimmungen etwa zu Diffamierung

[648] Oberster Gerichtshof Italiens, Urteil 17360/2025.
[649] Oberster Gerichtshof Italiens, Urteil 39763/2023.
[650] Gericht von Rom, Beschluss 59264/2019; Gericht von Rom, Beschluss 64894/2019.
[651] Oberster Gerichtshof Italiens, Urteil 22341/2025.
[652] Oberster Gerichtshof Italiens, Urteil 11571/2025.

oder Hetze stützen müssen, die nicht immer ohne Weiteres auf Desinformation anwendbar sind. Dies führt zu Unsicherheit bei der Rechtsauslegung und zu einer uneinheitlichen Durchsetzung. Auch nach der Verabschiedung des DSA, der Verfahren zur Bekämpfung rechtswidriger Inhalte vorgibt, könnte das Ausmaß der Online-Desinformation, insbesondere bei Kampagnen, die Rechtsbehelfe in Frage stellen.

5.4.3.3 Herausforderungen bei der nationalen Durchsetzung

Der italienische Rechtsrahmen für Online-Inhalte ist eng an das EU-Recht angelehnt, insbesondere durch den DSA, und wird durch nationale Instrumente wie den TUSMA und das Mancino-Gesetz ergänzt. Insgesamt bilden diese Maßnahmen ein System, in dem die AGCOM die administrative Aufsicht ausübt, während die Gerichte Rechtsbehelfe bieten, sodass Probleme wie Hetze und andere Formen rechtswidriger Inhalte durch regulatorische sowie zivil- und strafrechtliche Mechanismen angegangen werden können. Dieser mehrschichtige Ansatz ist in erster Linie im EU-Recht verankert, welches auch die nationalen Durchsetzungsmöglichkeiten prägt.

Herausforderungen ergeben sich jedoch im Bereich der Desinformation. Wie andere Mitgliedstaaten setzt auch Italien auf indirekte Regulierungsinstrumente, Rechtsbehelfe und Initiativen der Plattformen. Der Geschwindigkeit und dem Ausmaß, in dem Desinformation online verbreitet wird, sind diese Mechanismen allerdings kaum gewachsen. Die Verwaltungsbehörden werden zunehmend aufgefordert, gegen die Verbreitung rechtswidriger Inhalte vorzugehen, und müssen sich dabei innerhalb der Grenzen ihres Auftrags bewegen, doch wirksame Maßnahmen auf nationaler Ebene hängen mehr und mehr von der Koordinierung zwischen den nationalen Regulierungsbehörden und den europäischen Institutionen im Rahmen des Europäischen Gremiums für digitale Dienste ab, insbesondere bei der Bekämpfung von Desinformation als systemischem Risiko.

6. Andere Bereiche schädlicher Inhalte: Durchsetzung durch Beschränkungen

6.1 Durchsetzung auf EU-Ebene

Dr Mark D. Cole, Wissenschaftlicher Direktor, Institut für Europäisches Medienrecht (EMR) und Professor für Medien- und Telekommunikationsrecht, Universität Luxemburg

Während in den vorangegangenen Kapiteln in erster Linie Durchsetzungsmechanismen für die Entfernung oder Sperrung rechtswidriger Inhalte behandelt wurden, geht es in diesem Kapitel um Inhalte, die nicht unbedingt rechtswidrig sind, aber für bestimmte Gruppen – besonders für Minderjährige – schädlich sein können und deshalb Zugangsbeschränkungen unterliegen.[653] Ein prominentes Beispiel hierfür sind pornografische Inhalte, die zwar in den meisten nationalen Rechtssystemen nicht per se verboten sind, aber mit Blick auf den Zugang Minderjähriger meist Einschränkungen unterliegen.[654] In diesem Zusammenhang haben sich Regelungen herausgebildet, die nicht die Inhalte selbst kriminalisieren, sondern vielmehr versuchen, ihre Zugänglichkeit auf Basis des Risikos und des potenziellen Schadens zu kontrollieren, die für gefährdete Gruppen von ihnen ausgehen können.

In der EU sind solche Schutzmaßnahmen am deutlichsten in der AVMD-RL formuliert. Die AVMD-RL legt einen harmonisierten Rahmen fest, der die Mitgliedstaaten verpflichtet, dafür zu sorgen, dass audiovisuelle Mediendienste keine Inhalte bieten, die die körperliche, geistige oder sittliche Entwicklung von Minderjährigen beeinträchtigen können, außer wenn diese Inhalte so bereitgestellt werden, dass Minderjährige sie üblicherweise nicht hören oder sehen können. Wie in Kapitel 2.2.2 dargelegt, gilt die AVMD-RL sowohl für den traditionellen Rundfunk als auch für Abrufdienste sowie in Teilen – darunter die Verpflichtung zum Schutz Minderjähriger – für Anbieter von VSP-Diensten, weil die Muster des Medienkonsums zunehmend konvergieren. Zu den Maßnahmen im Rahmen der AVMD-RL können technische Zugangsbeschränkungen, Instrumente zur Altersüberprüfung und die Verwendung von Klassifizierungssystemen oder Deskriptoren zur Information der Zuschauer gehören. Welche Maßnahmen die Mitgliedstaaten den VSPs auferlegen können, ist in der Richtlinie detailliert aufgeführt. Da die Europäische Audiovisuelle Informationsstelle (EAI) diese nationalen Maßnahmen zum Schutz Minderjähriger in den EU-Mitgliedstaaten kürzlich erst in der Publikation „AVMSDigest: Der

[653] Zur Definition schädlicher Inhalte in diesem Zusammenhang siehe Lacourt A., Munch E., Radel-Cormann J., *AVMSDigest, Der Schutz von Minderjährigen auf Video-Sharing-Plattformen*, Europäische Audiovisuelle Informationsstelle, Straßburg, Oktober 2024, S. 13 ff.

[654] Für weitere Einzelheiten und einen Ländervergleich siehe Ukrow J., Cole M.D., Etteldorf C., *Stand und Entwicklung des internationalen Kinder- und Jungedmedienschutzes*, EMR Script Bd. 7, dco-Verlag, Püttlingen, 2023 (mit einer englischen Zusammenfassung, S. 34ff.). Siehe auch Verdoodt V., Lievens E., Chatzinikolaou A., „The EU Approach to Safeguard Children's Rights on Video-Sharing Platforms: Jigsaw or Maze?", *Media and Communication* 11(4), 2023, S. 151–163.

Schutz von Minderjährigen auf Video-Sharing-Plattformen“[655] behandelt hat, konzentriert sich der vorliegende Bericht auf die Beschränkungen im Rahmen des DSA. Insgesamt ist festzustellen, dass die AVMD-RL inhaltsspezifische Vorschriften für audiovisuelle Mediendienste – insbesondere in Bezug auf Minderjährige und in einigen Fällen für die Allgemeinheit – enthält und der DSA diese ergänzt, indem er das gesamte Ökosystem der Verbreitung digitaler Inhalte, insbesondere durch VLOPSEs, in den Blick nimmt und sicherstellt, dass Schutzmaßnahmen genereller in die Architektur von Online-Diensten eingebettet werden.

Der DSA als europäische Verordnung führt einen horizontalen Rahmen für die Regulierung von Online-Vermittlern ein, der in Kapitel 2.2.2 beschrieben wurde. Der DSA enthält keine unmittelbaren Verbote für bestimmte Inhalte, sondern geht davon aus, dass Anbieter von Vermittlungsdiensten, ähnlich wie bei der AVMD-RL, Mechanismen anwenden, durch die der Zugang zu Inhalten eingeschränkt werden kann, insbesondere wenn diese Inhalte für schutzbedürftige Empfänger des Dienstes schädlich sind, etwa für Minderjährige. Der Schutz von Minderjährigen ist ein wichtiges politisches Ziel der EU und wird ausdrücklich im DSA erwähnt.[656] Konkret müssen Plattformen, die für Minderjährige zugänglich sind – was im Prinzip alle öffentlich zugänglichen Dienste von Online-Plattformen ohne besondere Zugangsbedingungen einschließt und daher für sehr viele Plattformen gilt –, nach Artikel 28 Absatz 1 des DSA geeignete und verhältnismäßige Maßnahmen zum Schutz von Minderjährigen ergreifen.[657] Zu diesen Maßnahmen kann gehören, die Schnittstellen der Plattform oder Teile davon gegebenenfalls standardmäßig mit einem Höchstmaß an Privatsphäre, Sicherheit und Schutz für Minderjährige zu gestalten, Standards für den Schutz von Minderjährigen anzunehmen oder sich an Verhaltenskodizes zum Schutz von Minderjährigen zu beteiligen.[658]

Schädliche Inhalte und ihre Auswirkungen auf Minderjährige stellen außerdem eines der systemischen Risiken dar, die VLOPSEs im Rahmen ihrer Bewertung systemischer Risiken berücksichtigen und nach Artikel 35 Absatz 1 des DSA mindern müssen.[659] Entsprechende systemische Risiken können sich auch aus der Gestaltung, Funktionsweise oder Nutzung von VLOPSEs – auch durch Manipulation – ergeben, mit tatsächlichen oder absehbaren negativen Auswirkungen auf den Schutz der öffentlichen Gesundheit oder von Minderjährigen und schwerwiegenden negativen Folgen für das körperliche und geistige Wohlbefinden von Personen.[660] Die Minderungsmaßnahmen müssen angemessen, verhältnismäßig und wirksam und auf die spezifischen systemischen Risiken zugeschnitten sein; dazu können eine altersgerechte Kuratierung von Inhalten, Tools zur Kontrolle durch Eltern und transparente Standardeinstellungen gehören. Bei der Auswahl der geeigneten Minderungsmaßnahmen können die Anbieter gegebenenfalls bewährte Verfahren der

[655] Lacourt, Munch, Radel-Cormann, op. cit. Siehe dazu ausführlich Weinand J., *Umsetzung der EU-Richtlinie über audiovisuelle Mediendienste*, Nomos, Baden-Baden, 2018, insbesondere S. 489 ff. und 741 ff.
[656] Erwägungsgrund 71 DSA.
[657] Zur Verhältnismäßigkeit solcher Maßnahmen siehe Liesching M., „Artikel 28 DSA“ in Liesching M. (Hrsg.), op. cit., Rn. 38 ff., und zum DSA allgemein Wilman F., Kalėda S.L, Loewenthal P.J., *The EU Digital Services Act,* Oxford University Press, Oxford, 2024, S. 218.
[658] Ebd.
[659] Zum Schutz von Minderjährigen im Rahmen des DSA siehe Buiten M., Ledger M., Busch C., *Future of the DSA: Safeguarding Minors in the Digital Age*, DSA Implementation Forum, März 2025.
[660] Erwägungsgrund 83 DSA.

Branche berücksichtigen, unter anderem solche, die durch Zusammenarbeit im Bereich der Selbstregulierung festgelegt wurden, wie etwa Verhaltenskodizes. Darüber hinaus sollten sie den Leitlinien der Europäischen Kommission Rechnung tragen.[661]

Diese Leitlinien zu Artikel 28 des DSA wurden von der Europäischen Kommission im Juli 2025 veröffentlicht, um Online-Plattformen bei ihren Bemühungen zu unterstützen, die Verpflichtung aus Artikel 28 des DSA zur Verbesserung der Privatsphäre, der Sicherheit und des Schutzes von Kindern im Internet zu erfüllen.[662] Die Leitlinien enthalten eine nicht erschöpfende Liste empfohlener Maßnahmen, die Plattformen zum Schutz von Minderjährigen ergreifen können. Diese Maßnahmen beruhen auf dem Grundsatz des „eingebauten Datenschutzes" (Privacy by Design) und befürworten einen Ansatz mit Standardeinstellungen, bei denen die Sicherheit von Kindern Priorität hat. Im Einklang mit dem übergreifenden risikobasierten Ansatz des DSA wird in den Leitlinien zunächst anerkannt, dass das Risiko, das Plattformen für Minderjährige darstellen, unterschiedlich hoch sein kann. Dies ermöglicht eine flexible Umsetzung, die es den Anbietern erlaubt, Schutzmaßnahmen auf ihre spezifischen Dienste zuzuschneiden und gleichzeitig unnötige Einschränkungen des Rechts von Kindern auf Beteiligung, Informationszugang und freie Meinungsäußerung zu vermeiden. Daher muss jede Maßnahme, die ein Anbieter einer für Minderjährige zugänglichen Plattform ergreift, um Artikel 28 Absatz 1 des DSA nachzukommen, den folgenden allgemeinen Grundsätzen entsprechen: Verhältnismäßigkeit, Achtung der Rechte von Kindern, Privatsphäre, Sicherheit und Schutz durch Technikgestaltung sowie altersgerechte Gestaltung.[663]

Einer der wichtigsten empfohlenen Ansätze ist die Einführung von Mechanismen zur Altersfeststellung, die verhindern, dass Kinder mit nicht altersgerechten Inhalten in Berührung kommen. Vor dem Einsatz eines solchen Mechanismus sollte der Anbieter jedoch prüfen, ob sich das Ziel, ein hohes Maß an Privatsphäre, Sicherheit und Schutz für Minderjährige in seinem Dienst zu gewährleisten, nicht bereits durch andere, weniger weitreichende Maßnahmen erreichen lässt.[664] In Fällen, in denen das geltende EU- oder innerstaatliche Recht ein Mindestalter für den Zugang zu bestimmten Produkten oder Dienstleistungen vorschreibt, die auf der Online-Plattform angeboten und/oder gezeigt werden (z. B. Verkauf von Alkohol, Zugang zu Pornografie oder zu Glücksspielinhalten), hält die Europäische Kommission den Einsatz einer Methode zur Altersüberprüfung für eine geeignete und verhältnismäßige Maßnahme. Dasselbe gilt für Fälle, in denen die Nutzungsbedingungen oder andere vertragliche Verpflichtungen des Dienstes vorsehen,

---

[661] Erwägungsgrund 89 DSA.

[662] Europäische Kommission, „Commission Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online Pursuant to Article 28(4) of Regulation (EU) 2022/2065", 2025; der Entwurf der Leitlinien war vom 13. Mai bis zum 10. Juni 2025 für öffentliche Stellungnahmen verfügbar und wurde am 14. Juni 2025 angenommen; siehe Europäische Kommission, Annex to the Communication to the Commission, Approval of the Content on a Draft Communication from the Commission- Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online, pursuant to Article 28(4) of Regulation (EU) 2022/2065. Siehe auch Munch, E., „Europäische Kommission veröffentlicht Leitlinien zum Schutz Minderjähriger im Rahmen des DSA", IRIS 2025-8:1/6, Europäische Audiovisuelle Informationsstelle, 2025. Für eine Einschätzung aus Sicht des Datenschutzes siehe Stalla-Bourdillon S., „A GDPR Lens on the Draft Article 28 DSA Guidelines and Their Approach to Age Assurance", *European Data Protection Law Review*, 2025, 11(2), S. 207-214.

[663] Siehe Europäische Kommission, „Commission Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online Pursuant to Article 28(4) of Regulation (EU) 2022/2065", op. cit., S. 6 ff.

[664] Ebd., S. 9.

dass ein Nutzer mindestens 18 Jahre alt sein muss, um auf den Dienst zugreifen zu können, oder in denen der Anbieter Risiken für Minderjährige festgestellt hat, die sich nicht durch andere, weniger einschneidende Maßnahmen mindern lassen. Hierbei ist anzumerken, dass die Frage der Altersüberprüfung komplex ist und schon seit Langem diskutiert wird – auch im Hinblick auf die praktischen Herausforderungen, nicht zuletzt bei der Durchsetzung.[665]

Auch wenn die entsprechenden Bestimmungen in der AVMD-RL wie auch im DSA die Notwendigkeit zum Schutz Minderjähriger und die entsprechenden Bemühungen der Plattformen klar anerkennen, bleibt für die Anbieter die Frage offen, welcher Aufwand für die Altersüberprüfung als ausreichend angesehen würde, wenn über die Umsetzung von Schutzmaßnahmen für Minderjährige entschieden wird. So verlangt die AVMD-RL etwa, dass Inhalte, die für Minderjährige schädlich sein können, „nur so bereitgestellt werden, dass sichergestellt ist, dass sie von Minderjährigen üblicherweise nicht gehört oder gesehen werden können", ohne aber spezielle Technologien zur Altersüberprüfung vorzuschreiben. Ebenso verlangt Artikel 28 Absatz 1 des DSA, dass „geeignete und verhältnismäßige Maßnahmen" ergriffen werden müssen, um für „ein hohes Maß an … Sicherheit" zu sorgen, ohne näher zu erläutern, was unter einem hohen Maß zu verstehen ist.

Die Leitlinien der Europäischen Kommission, sind als solche zwar nicht rechtsverbindlich, machen den Anbietern aber wesentlich konkretere Vorschläge zu neuen Standards für Instrumente zur Altersüberprüfung. Sie betrachten die geplante europäische Brieftasche für die Digitale Identität (European Digital Identity Wallet oder EUDI-Wallet)[666] als geeignetes und zuverlässiges Mittel zur digitalen Identifizierung im Rahmen des DSA. Die EUDI-Wallet, welche die Mitgliedstaaten bis zum 28. November 2026 einführen müssen, soll als harmonisierter Rahmen für die digitale Identität dienen und die zentrale Registrierung von Altersangaben ermöglichen. Auf diese Angaben könnte dann nur zugegriffen werden, um zu überprüfen, ob ein Nutzer, der etwa Zugang zu einer Website beantragt, nicht minderjährig ist, ohne dass weitere Informationen wie das genaue Alter oder personenbezogene Daten abgefragt werden. Doch schon bevor die EUDI-Wallet verfügbar ist, hat die Europäische Kommission als eigenständige Maßnahme zusammen mit den Leitlinien eine Open-Source-Lösung zur Altersüberprüfung mit einer speziellen App veröffentlicht, die ihrer Meinung nach zu einem EU-weiten „Referenzstandard für eine gerätegebundene Methode zur Altersüberprüfung" werden könnte.[667] Wie die EUDI-Wallet würde dieses System in Zukunft sicherstellen, dass neben der Altersüberprüfung keine

[665] Siehe OECD, „The Legal and Policy Landscape of Age Assurance Online for Child Safety and Well-Being", Fachbeitrag der OECD, Juni 2025. Für einen Überblick über Mechanismen für die Altersüberprüfung und die Kontrolle durch Eltern siehe Broughton Micova S., Kostovska I., *The Protection of Minors on VSPs: Age Verification and Parental Control*, Europäische Audiovisuelle Informationsstelle, Straßburg, 2023. Zu Herausforderungen bei der Durchsetzung siehe z. B. Schmitz-Berndt S., „Verwaltungsgericht Berlin lehnt im Eilverfahren Antrag auf vorläufigen Rechtsschutz von Pornoplattformen gegen Sperrverfügung der zuständigen Landesmedienanstalt ab", op. cit.

[666] Die Verpflichtung der Mitgliedstaaten, den Bürgern eine EUDI-Wallet zur Verfügung zu stellen, ergibt sich aus der Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des europäischen Rahmens für eine digitale Identität, ABl. L 2024/1183 vom 17. April 2024.

[667] Europäische Kommission, Commission Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online Pursuant to Article 28(4) of Regulation (EU) 2022/2065, op. cit., S. 10.

weiteren Details preisgegeben werden und die Plattformen, die eine Altersfeststellung verlangen, nur die Information erhalten, dass der Nutzer über 18 Jahre alt ist.

Von der Altersüberprüfung zu unterscheiden ist die Altersschätzung. Während die Altersüberprüfung Gewissheit über das Alter des Nutzers bietet, wird mit der Altersschätzung nur das ungefähre Alter des Nutzers bestimmt, also die Wahrscheinlichkeit, dass er ein bestimmtes Alter hat.[668] In den Leitlinien werden Umstände aufgeführt, unter denen Schätzungsmethoden ausreichen, etwa wenn der Anbieter auf seiner Plattform nach Maßgabe seiner Risikobewertung mittlere Risiken für Minderjährige ermittelt hat und die Beschränkung nicht für alle Minderjährigen unter 18 Jahren gelten soll, sondern nur für noch jüngere Altersgruppen. Dagegen betrachtet die Europäische Kommission die Eigenerklärung, also die Angabe des Alters durch die Person selbst, nicht als geeignete Maßnahme zur Altersfeststellung.[669]

Interessanterweise bezogen sich die ersten Maßnahmen der Europäischen Kommission zur Durchsetzung des DSA auf mögliche Verstöße gegen die Verpflichtung zum Schutz Minderjähriger. Schon mehrfach hat die Kommission Maßnahmen gegen VLOPs wegen Nichteinhaltung der Bestimmungen zum Schutz Minderjähriger vor schädlichen Inhalten ergriffen. So eröffnete sie im Mai 2025 ein förmliches Verfahren gegen Anbieter pornografischer Inhalte, nämlich die Anbieter von Pornhub, Stripchat, XNXX und XVideos, die als VLOPs eingestuft worden waren.[670] Bei den Untersuchungen der Kommission ging es um die Risiken solcher Dienste für Minderjährige, darunter auch Risiken im Zusammenhang mit dem Fehlen wirksamer Maßnahmen zur Altersüberprüfung. So stützte sich das Verfahren gegen Pornhub auf die vorläufige Feststellung, dass der Anbieter gegen Artikel 28 Absatz 1, Artikel 34 Absatz 1, Artikel 34 Absatz 2 und Artikel 35 Absatz 1 des DSA verstoßen hatte, unter anderem, weil Aylo, der Anbieter dieses Dienstes, zur Altersfeststellung auf Eigenerklärungen gesetzt hatte, um den Zugang zu dem Dienst für Minderjährige zu beschränken.[671] Infolge der Einleitung eines förmlichen Verfahrens hat die Kommission nun die Möglichkeit, weitere Durchsetzungsmaßnahmen zu ergreifen, z. B. einstweilige Maßnahmen und Nichteinhaltungsbeschlüsse. Parallel und ergänzend zu den Durchsetzungsmaßnahmen der Kommission wurden die Mitgliedstaaten im Europäischen Gremium für digitale Dienste gegen kleinere Plattformen aktiv, die pornografische Inhalte anbieten, aber nicht als VLOPs eingestuft sind und daher weiter in die Zuständigkeit der nationalen Behörden fallen. Die Mitgliedstaaten lancierten eine koordinierte Aktion, um eine einheitliche und effiziente Anwendung des DSA in der gesamten EU zu gewährleisten,[672] nachdem einzelne Mitgliedstaaten bereits zuvor Maßnahmen eingeleitet hatten.[673]

---

[668] Ebd., S. 9.
[669] Ebd., S. 15.
[670] Europäische Kommission, „Kommission leitet im Rahmen des Gesetzes über digitale Dienste Untersuchungen zum Schutz Minderjähriger vor pornografischen Inhalten ein“, Pressemitteilung, 27. Mai 2025.
[671] Europäische Kommission, Case DSA.100059 – Pornhub – Investigation into Compliance with Articles 28(1), 34(1), 34(2) and 35(1) of Regulation (EU) 2022/2065, 27. Mai 2025.
[672] Europäische Kommission, „Das Europäische Gremium für digitale Dienste leitet eine koordinierte Maßnahme zur Stärkung des Jugendschutzes in Bezug auf pornografische Plattformen ein“, Pressemitteilung, 27. Mai 2025.
[673] Siehe z. B. Schmitz-Berndt S., „Verwaltungsgericht Berlin lehnt im Eilverfahren Antrag auf vorläufigen Rechtsschutz von Pornoplattformen gegen Sperrverfügung der zuständigen Landesmedienanstalt ab“, op. cit.

6.2 Das Beispiel Polen

Dr Krzysztof Wojciechowski, Rechtsberater, Berater bei TVP, Vorsitzender des polnischen Urheberrechtsausschusses, Dozent für Postgraduiertenstudiengänge für Geistiges Eigentum, Universität Warschau

6.2.1 Nationaler Rechtsrahmen für Plattformen

Polen steht beispielhaft für ein Land, in dem die Debatten über die Freiheit des Internets besonders intensiv geführt werden, vor allem im Zusammenhang mit Initiativen zur Regulierung von Online-Aktivitäten, etwa im Bereich des Urheber- und/oder Medienrechts.[674]

Der Rechtsrahmen für Online-Plattformen in Polen ist noch nicht vollständig, da der Präsident am 9. Januar 2026 sein Veto[675] gegen die vom Parlament am 18. Dezember 2025 verabschiedete nationale Umsetzung[676] des Gesetzes über digitale Dienste (DSA)[677] einlegte. Noch vor Beginn der parlamentarischen Beratungen und dann im Parlament äußerten ein Teil des politischen Spektrums, einige Interessenträger, Nichtregierungsorganisationen und andere Gremien Befürchtungen, das vorgeschlagene Modell der präventiven Anordnungen könnte insbesondere in Bezug auf Hassreden zu „Internetzensur" führen.[678] Die weitere

---

[674] Ein früheres Beispiel ist die polnische Klage auf Nichtigerklärung von Art. 17 Abs. 4 lit . c) und d) *in fine* der Richtlinie (EU) 2019/790 des Europäischen Parlaments und des Rates vom 17. April 2019 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG, ABl. L 130/92 vom 17. Mai 2019, im Lichte von Artikel 11 der Charta der Grundrechte der Europäischen Union, was zum EuGH-Urteil vom 26. April 2022 führte (C-401/19 *Polen gegen das Europäische Parlament und den Rat der EU*, ECLI:EU:C:2022:297).

[675] Antrag des Präsidenten vom 9. Januar 2026 auf Überprüfung des Gesetzes vom 18. Dezember 2025 zur Änderung des Gesetzes über die Erbringung elektronischer Dienstleistungen und einiger anderer Gesetze
Der *Sejm* kann das Gesetz mit 3/5-Mehrheit erneut verabschieden (das Veto zurückweisen) (Art. 122 Abs. 5 der Verfassung). Dies ist jedoch unwahrscheinlich, da bei der Abstimmung im *Sejm* weniger Stimmen für das Gesetz abgegeben wurden.

[676] *Ustawa z dnia 18 grudnia 2025 r. o zmianie ustawy o świadczeniu usług drogą elektroniczną i niektórych innych ustaw* (Gesetz vom 18. Dezember 2025 zur Änderung des Gesetzes über die Erbringung elektronischer Dienstleistungen und einiger anderer Gesetze) . Die weitere Entwicklung des Entwurfs während der Regierungsarbeit und der Konsultationen ist hier dokumentiert. Die parlamentarischen Arbeiten zum Regierungsentwurf im *Sejm* [Unterhaus] und der Beschluss des Senats (poln.).

[677] Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (DSA), ABl. L 277, 27. Oktober 2022.

[678] Die Kluft lässt sich anhand der Abstimmungsergebnisse im *Sejm* vom 21. November 2025 veranschaulichen, wo das Gesetz mit 237 Stimmen, vor allem von der Regierungskoalition (KO, PSL, Polska 2050, Lewica), unterstützt wurde, während 200 Abgeordnete der Opposition (PiS, Konfederacja) dagegen stimmten und 5 Abgeordnete sich enthielten. Die unterschiedlichen Ansichten wurden bei der öffentlichen Anhörung im *Sejm* am 4. November 2025 vorgestellt. Der Entwurf wurde von Inhabern von Rechten des geistigen Eigentums unterstützt, darunter Film- und Musikproduzenten, Verwertungsgesellschaften und Presseverleger. Einige zivilgesellschaftliche Organisationen hoben die positive Entwicklung des Entwurfs hervor (zum Beispiel die Helsinki-Stiftung für Menschenrechte, Panoptykon), während andere (zum Beispiel *Ordo Iuris*, die Gesellschaft polnischer Journalisten und die KRRiT-Vorsitzende) auf die Gefahr des Missbrauchs von Sperranordnungen zur Zensur des Internets hinwiesen.

Entwicklung des Entwurfs in den Regierungs- und dann in den Parlamentssitzungen zielte zum großen Teil darauf ab, diesen Bedenken Rechnung zu tragen. Dessen ungeachtet bestritt der Präsident weiterhin eine Gefahr für die Meinungsfreiheit und weigerte sich, das vom Parlament verabschiedete Gesetz zu unterzeichnen.

Die Umsetzung des DSA sollte in Form einer umfassenden Überarbeitung des *Ustawa o świadczeniu usług drogą elektroniczną* (Gesetz über die Erbringung elektronischer Dienstleistungen – UŚUDE) erfolgen.[679] Institutionell benennt die Novelle die Regulierungsbehörde für Telekommunikation, das *Urząd Komunikacji Elektronicznej – Prezes* (Amt für elektronische Kommunikation, Präsident – UKE), zum nationalen Koordinator für digitale Dienste (DSC/KDD) und zur Aufsichtsbehörde. Ausnahmen gelten für E-Commerce-Plattformen und den Verbraucherschutz, die von der Wettbewerbsbehörde – dem Präsidenten des Amtes für Wettbewerb und Verbraucherschutz (*Urząd Ochrony Konkurencji i Konsumentów* – UOKiK) – beaufsichtigt werden, sowie für Video-Sharing-Plattformen (VSP), die in die Zuständigkeit der Medienregulierungsbehörde (Vorsitzende(r) des Nationalen Rundfunkrats - *Krajowa Rada Radiofonii i Telewizji* – KRRiT) fallen. Das Gesetz sieht zudem Regeln und Verfahren für den Präsidenten des UKE vor, nach denen er den Status eines „vertrauenswürdigen Hinweisgebers“ und „zugelassenen Forschers“ zuerkennen kann, sowie für die Zertifizierung außergerichtlicher Streitbeilegungsstellen. Die Überarbeitung legt des Weiteren Verfahren für die Überwachung der Einhaltung des DSA, für verwaltungsrechtliche Sanktionen im Falle von Verstößen und für die Bearbeitung von Beschwerden gemäß Artikel 53 des DSA fest; außerdem enthält sie Vorschriften für die zivilrechtliche Haftung bei Verstößen gegen den DSA und entsprechende Gerichtsverfahren vor.

Die wichtigsten und am heftigsten diskutierten Änderungen des Gesetzes sind die Regeln und Verfahren für Anordnungen zum Vorgehen gegen rechtswidrige Inhalte und, wenngleich weniger umstritten, für Anordnungen zur Wiederherstellung von Inhalten, die fälschlicherweise entfernt wurden.[680] Das Konzept der rechtswidrigen Inhalte hat sich während der Arbeit der Regierung an dem Entwurf erheblich weiterentwickelt. Ursprünglich bezog sich der Entwurf auf rechtswidrige Inhalte, ohne diese zu definieren. Nach Konsultationen hob er dann auf Verletzungen der Persönlichkeitsrechte, der Rechte des geistigen Eigentums, Straftaten und Verstöße gegen den Verbraucherschutz im Allgemeinen ab. Der von der Regierung dem Parlament vorgelegte und von letzterem angenommene Entwurf ist in seinem Geltungsbereich wesentlich eingeschränkter und gleichzeitig präziser, da er sich auf einen geschlossenen Katalog von 27 Straftatbeständen bezieht.

Laut der Begründung, die mit dem von der Regierung vorgelegten Entwurf eingereicht wurde, gelten drei Kriterien zur Bestimmung einer spezifischen Rechtsverletzung: 1) sie muss online erfolgen – unter Berücksichtigung des *Modus Operandi* des Täters; 2) es muss berücksichtigt werden, wie der Inhalt verbreitet wird, und 3) die Sperrung des Zugangs zu den Inhalten darf sich nicht negativ auf den demokratischen Diskurs und Wahlen auswirken. Zu den aufgelisteten Tatbeständen gehören insbesondere

[679] *Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną* (Gesetz vom 18. Juli 2022 über die Erbringung elektronischer Dienstleistungen), konsolidierter Text: *Gesetzblatt (Dziennik Ustaw*) von 2024, Punkt 1513.

[680] Kapitel 2a (Artikel 11a-11u) UŚUDE, hinzugefügt durch das Änderungsgesetz vom 18. Dezember 2025.

strafbare Drohungen, Anstiftung zum Selbstmord oder zur Selbstverletzung, Menschenhandel, Missbrauch des Abbilds einer anderen Person, unbefugte Verbreitung von Nacktbildern oder sexuellen Darstellungen, für Minderjährige unter 15 Jahren zugängliche Verbreitung von Pornografie, Kontaktaufnahme mit solchen Minderjährigen im Internet, um ein Sexualverbrechen zu begehen, Förderung von Pädophilie, Verbreitung von Pornografie, die Minderjährige, Tiere oder Gewalttätigkeiten zum Gegenstand hat, Falschalarme, die zum Einschreiten öffentlicher Organe führen, Förderung von Totalitarismus, Aufstachelung zum Hass aus rassistischen, fremdenfeindlichen oder religiösen Gründen, öffentliche Beleidigung aus solchen Gründen, Betrug, Verletzung des Urheberrechts durch unbefugte Verbreitung eines Werks oder Versandhandel von Tabak. Rechtswidrige Inhalte beschränken sich nicht nur auf Materialien, die direkt einen der aufgeführten Tatbestände darstellen, sondern umfassen auch Inhalte, die zum Begehen solcher Handlungen auffordern.[681] Das Gesetz nimmt Fälle aus, die unter Sondergesetze fallen, das heißt terroristische Inhalte, terrorismus- oder spionagebezogene IT-Daten, Verstöße gegen das Verbraucherschutzrecht; Programme, Videos oder andere Inhalte, die nicht mit den Vorschriften des *Ustawa o radiofonii i telewizji* (Rundfunkgesetz)[682] über VSP-Dienste (Artikel 47o) übereinstimmen, die auf den Schutz Minderjähriger, die Bekämpfung der Aufstachelung zu Gewalt und Hass und/oder auf Inhalte, die Terrorismus, Pornografie mit Beteiligung Minderjähriger oder rassistische, fremdenfeindliche oder religiöse Beleidigungen fördern, abzielen.

Gemäß dem verabschiedeten, jedoch mit einem Veto belegten Gesetz wären Anträge auf Anordnungen, den Zugang zu rechtswidrigen Inhalten innerhalb eines von einem Vermittlungsdienstanbieter bereitgestellten Dienstes zu unterbinden, von einem Staatsanwalt, der Polizei,[683] einer Stelle der *Krajowa Administracja Skarbowa* (Nationale Finanzverwaltung – KAS), einem Inhaber von Urheberrechten oder verwandten Schutzrechten oder einem Dienstenutzer zu stellen gewesen.[684] Solche Anträge sollten vom/von der KRRiT-Vorsitzenden für Inhalte bei VSP-Diensten und vom Präsidenten des UKE für alle anderen Inhalte geprüft und entsprechende Anordnungen erlassen werden. Die Verfahren sollten beschleunigt erfolgen, wobei Entscheidungen bei Anträgen der Staatsanwaltschaft oder der Polizei innerhalb von zwei Tagen, in anderen Fällen innerhalb von sieben Tagen und bei besonders komplexen Angelegenheiten innerhalb von 21 Tagen zu treffen gewesen wären. Die Fristen hätten mit Ablauf der zwei Tage begonnen, die dem hochladenden Nutzer zur Darlegung seines Standpunkts eingeräumt worden wären. Bei

[681] Der Regierungsentwurf und das ursprünglich vom *Sejm* verabschiedete Gesetz bezogen sich auch auf Inhalte, die solche Straftaten „rühmen". In den Änderungsanträgen strich der Senat diese Bestimmung, da er sie als nicht eindeutig und unverhältnismäßig betrachtete und sie die Freiheit der Meinungsäußerung beeinträchtigten könnte; z. B. wurden Zweifel geäußert, ob Likes oder Links zu rechtswidrigen Inhalten ein solches „Rühmen" darstellen können.

[682] *Ustawa z dnia 29 grudnia 1992 r. o radiofonii i telewizji* (Rundfunkgesetz), konsolidierter Text, Gesetzblatt *(Dziennik Ustaw*) von 2022, Punkt 1722, mit Änderungen; Englische Übersetzung.

[683] In Fällen von Menschenhandel auch der Grenzschutz.

[684] Der Regierungsentwurf schlug vor, auch vertrauenswürdige Hinweisgeber zu berechtigen, solche Anträge zu stellen. Dies wurde von den Gegnern des Entwurfs kritisiert, da angeblich die Gefahr bestehe, dass einige Organisationen mit dem Status eines vertrauenswürdigen Hinweisgebers politisch oder ideologisch motivierte Anträge auf Anordnungen einreichen. Im Anschluss an die Änderungsanträge des Senats beschloss das Parlament schließlich, vertrauenswürdige Hinweisgeber von der Liste der antragsberechtigten Stellen und Einrichtungen zu streichen. Stattdessen wurden Inhaber von Urheberrechten und verwandten Schutzrechten in die Liste aufgenommen.

Anträgen von Dienstenutzern auf Aufhebung von Hosting-Beschränkungen gemäß Artikel 17 Absatz 1 DSA hätten Entscheidungen innerhalb von 14 Tagen nach ähnlichen Verfahrensregeln erlassen werden müssen. Die Parteien hätten binnen 14 Tagen über die anordnende Behörde Einspruch bei Gericht einlegen können; das Gericht hätte ein nichtstreitiges Zivilverfahren angewendet, und seine Entscheidung hätten angefochten werden können, auch auf dem Kassationsweg. Entscheidungen über Anordnungen wären nicht für sofort vollstreckbar erklärt worden, sondern erst nach Ablauf der Einspruchsfrist, wenn kein solcher eingelegt wurde.[685] Das Verzeichnis der Internetdomains, die zur Verbreitung rechtswidriger Inhalte genutzt werden, wäre vom Präsidenten des UKE zu führen gewesen, um Domains zu erfassen, die keine wirksamen Maßnahmen zur Durchsetzung von Anordnungen vorhalten, und die Anbieter von Internetzugangsdiensten wären verpflichtet gewesen, den Zugang zu Websites, die gelistete Domainnamen verwenden, zu sperren und die Nutzer auf die Website des UKE umzuleiten.

Der vorgeschlagene Mechanismus für präventive Anordnungen war während der gesamten Ausarbeitung der Umsetzungsvorlage zum DSA umstritten. Kritiker haben insbesondere auf die vermeintliche Ungenauigkeit der Kriterien in einigen Fällen und die Gefahr subjektiver Urteile in Verbindung mit der Tatsache hingewiesen, dass die Befugnis zum Erlass solcher Anordnungen bei der staatlichen Regulierungsbehörde (dem vom *Sejm* auf Vorschlag des Ministerpräsidenten ernannten Präsidenten des UKE) liegen würde. Diese Bedenken sollten auf die potenzielle Gefahr von Zensur hinweisen. Nach der Eingrenzung und Klärung der Definition von rechtswidrigen Inhalten, mit der die frühere weit gefasste Bezugnahme auf jegliche Verletzung von Persönlichkeitsrechten oder Rechten des geistigen Eigentums ersetzt wurde, konzentrierte sich die Kritik auf bestimmte aufgelistete Straftatbestände, die häufig unter dem Begriff „Hassrede“ zusammengefasst werden, weil sie mutmaßlich die genannten Risiken bergen. Die Befürworter des Entwurfs wiederum betonen die konkrete Auflistung der Arten rechtswidriger Inhalte, die mit einschlägigen schweren Straftaten verknüpft sind, und die Sicherstellung der gerichtlichen Überprüfung präventiver Anordnungen.[686] Während der parlamentarischen Sitzungen wurden im *Sejm* und im Senat weitere Schritte zur Entkräftung der Bedenken unternommen, darunter einige Garantien für eine politisch neutrale Haltung, Unparteilichkeit und Fairness der Personen, die die Anträge auf Anordnungen prüfen, die Streichung vertrauenswürdiger Hinweisgeber von der Liste der antragsberechtigten Stellen, fehlende sofortige Durchsetzbarkeit von Anordnungen und Streichung des „Rühmens“ von aufgelisteten Straftaten als mögliche Rechtfertigung für eine Entfernung.[687] Der Präsident hielt diese Schritte für unzureichend und weigerte sich, das Gesetz zu unterzeichnen. In der Begründung des Antrags des Präsidenten auf Überprüfung des Gesetzes wird auf die politische Uneinigkeit über das Gesetz im Parlament und den daraus resultierenden fehlenden Konsens hingewiesen; die

[685] Mangelnde Durchsetzbarkeit von Anordnungen vor Ablauf der Frist für eine gerichtliche Überprüfung war der Beweggrund für einen weiteren Änderungsantrag des Senats als Reaktion auf Bedenken wegen der angeblichen Gefahr einer Online-Zensur durch staatliche Stellen. Der Regierungsentwurf und das ursprünglich vom *Sejm* verabschiedete Gesetz sahen die Möglichkeit vor, die sofortige Durchsetzbarkeit von Anordnungen zu verfügen, wenn dies durch das Ausmaß des Schadens oder das öffentliche Interesse gerechtfertigt ist.

[686] *Ministerstwo Cyfryzacji*, „*Nowe zasady w internecie - sprawdź, co zmieni DSA*" (Neue Regeln im Internet – Finden Sie heraus, was der DSA ändern wird), 3. November 2025, Regierungsportal des Ministeriums.

[687] Vgl. z. B. Art. 11c, Art. 11a Abs. 1, Art. 11n UŚUDE in der Fassung des Änderungsgesetzes vom 18. Dezember 2025. Zur Begründung der Änderungen durch den Senat – vgl. die Begründung zu seinem Beschluss vom 10. Dezember 2025.

definierte Liste von Straftatbeständen wird zwar gelobt, bestimmte Straftaten wie die Verletzung von Rechten des geistigen Eigentums bedürfen demnach jedoch einer weiteren gerichtlichen Bewertung. Die Übertragung der Befugnis zur Sperrung von Inhalten ohne vorherigen Gerichtsbeschluss auf „staatliche Exekutivorgane" wie den Präsidenten des UKE wird im Hinblick auf die Meinungsfreiheit angesichts der Gefahr politischer Einflussnahme kritisiert. Auch die Verhältnismäßigkeit der administrativen Sperrung von Inhalten wird in Frage gestellt, da diese als solche nicht vom DSA gefordert wird und es andere verfügbare Maßnahmen wie das Melde- und Abhilfeverfahren und/oder Gerichtsverfahren mit dem Antrag auf einstweiligen Rechtsschutz (zum Beispiel eine Anordnung zur vorübergehenden Entfernung von Inhalten) gibt. Sowohl die mangelnde Durchsetzbarkeit von Anordnungen vor einer gerichtlichen Überprüfung als auch das Fehlen von Dringlichkeitsverfahren, die es dem Gericht ermöglichen, Einsprüche zu überprüfen, werden als potenzielle Gründe für die Unwirksamkeit des Verfahrens kritisiert.[688] Das Veto des Präsidenten wurde von der Regierung und der Regierungskoalition sowie von einigen Nichtregierungsorganisationen als politisch motiviert kritisiert, während es von den Oppositionsparteien unterstützt wurde. Es bleibt abzuwarten, wie sich die Dinge entwickeln werden, und ob die Initiative in dem wahrscheinlichen Fall, dass das Veto im *Sejm* nicht zurückgewiesen wird, in geänderter Form oder mit reduziertem Umfang erneut vorgelegt wird.

Über die Umsetzung des DSA hinaus enthält der aktuell für Online-Plattformen relevante nationale Rechtsrahmen hauptsächlich Bestimmungen des UŚUDE, das die EC-RL[689] umsetzt und weitgehend deren Struktur und Inhalt widerspiegelt. Im UŚUDE sind die einschlägigen Begriffe definiert, insbesondere die Erbringung elektronischer Dienstleistungen. Demnach unterliegen solche Dienste dem Recht des EU- oder EFTA-/EWR-Mitgliedstaates, in dem der Diensteanbieter seinen Geschäfts- oder Wohnsitz hat (Herkunftslandprinzip), mit bestimmten Ausnahmen (zum Beispiel Schutz des geistigen Eigentums) und möglichen Einschränkungen, vorbehaltlich des nach Artikel 3 Absatz 4 und 5 der EC-RL festgelegten Verfahrens.[690] Darüber hinaus legt das UŚUDE die Pflichten der Diensteanbieter in Bezug auf Informationen, die eine Identifizierung ermöglichen, auf Geschäftsbedingungen sowie kommerzielle Kommunikation und personenbezogene Daten fest. Das UŚUDE enthält zudem noch Bestimmungen über Haftungsausnahmen für Anbieter von reinen Durchleitungs-, Caching- und Hosting-Diensten sowie den Grundsatz, dass keine allgemeine Überwachungspflicht besteht; diese Bestimmungen werden aufgehoben, da diese Fragen nun direkt in Kapitel II (Artikel 4-8) des DSA geregelt sind.

Eine wichtige Ausnahme vom Herkunftslandprinzip für Online-Dienste betrifft Online-Glücksspiele. Solche Dienste unterliegen polnischem Recht, wenn das Glücksspiel auf dem Hoheitsgebiet Polens veranstaltet wird, der Dienstenutzer auf diesem Hoheitsgebiet am

---

[688] Als ein weiterer Grund für das Veto wird die Möglichkeit betrachtet, dass Zuwendungen aus dem Staatshaushalt an vertrauenswürdige Hinweisgeber zu einem „Interessenkonflikt" führen, der ihre Unabhängigkeit beeinträchtigt.

[689] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, ABl. L 178, 17. Juli 2000.

[690] Artikel 3a und 3b, UŚUDE. Interessanterweise sollten in dem vom Präsidenten mit einem Veto belegten Gesetz vom 18. Dezember 2025 zur Änderung des UŚUDE (zur Umsetzung des DSA) Anordnungen zur Bekämpfung rechtswidriger Inhalte und zur Wiederherstellung von Inhalten in die Liste der Ausnahmen vom Herkunftslandprinzip aufgenommen werden (Art. 3a Abs. 2 UŚUDE).

Spiel teilnimmt und/oder der Dienst auf Nutzer in Polen ausgerichtet ist, insbesondere wenn er in polnischer Sprache angeboten und/oder in Polen beworben wird.[691] Die detaillierten Pflichten von Veranstaltern von Online-Glücksspielen sind im *Ustawa o grach hazardowych* (Glücksspielgesetz)[692] festgelegt, das die Teilnehmer vor negativen Folgen des Glücksspiels schützen soll. Diese Maßnahmen umfassen unter anderem ein Verbot der Teilnahme von Personen unter 18 Jahren, Verfahren zur Altersverifizierung sowie Schutzmaßnahmen für Minderjährige im Zusammenhang mit Werbung für Online-Glücksspiele. Das Finanzministerium führt ein Verzeichnis von Domains, die nicht gesetzeskonforme und in Polen zugängliche Online-Glücksspiele anbieten. Telekommunikationsbetreiber, die Zugang zu Internetdiensten anbieten, müssen den Zugang zu Websites verhindern, die in dem Verzeichnis aufgeführte Domainnamen verwenden. Ferner ist die Erbringung von Zahlungsdiensten für solche Websites untersagt. Dieses Instrument diente als Inspiration für die jüngsten Gesetzentwürfe zum Schutz Minderjähriger vor schädlichen Inhalten/Pornografie, die unten erörtert werden.

Der bestehende Rechtsrahmen für Online-Plattformen umfasst auch Bestimmungen im Rundfunkgesetz über VSP[693] zur Umsetzung der Artikel 28a und 28b der Richtlinie über audiovisuelle Mediendienste (AVMD-RL).[694] Geregelt werden unter anderem die Kriterien für die polnische Gerichtsbarkeit über VSP, Transparenzpflichten, darunter in Bezug auf die Eigentümerstruktur von Anbietern, die von der Medienregulierungsbehörde KRRiT geführt Liste der VSP sowie die Pflicht der Anbieter, ihre VSP bei der KRRiT zu melden. In Bezug auf Inhalte auf VSP sind die Anbieter verpflichtet, Maßnahmen zu ergreifen, die die Verbreitung von jugendgefährdenden Inhalten und von Inhalten, die zu Gewalt und/oder Hass aufstacheln, terroristische Straftaten begünstigen, zu rassistischen oder fremdenfeindlichen Beleidigungen animieren sowie Pornografie mit Beteiligung Minderjähriger beinhalten, verhindern. Darüber hinaus müssen diese Anbieter den Nutzern Möglichkeiten anbieten, Verstöße gegen die Vorschriften über schädliche oder rechtswidrige Inhalte zu melden, und den Nutzern innerhalb von 48 Stunden antworten. Streitigkeiten über den Umgang mit solchen gemeldeten Verstößen können durch Schlichtung beigelegt werden. Wird der Verstoß durch den hochladenden Nutzer nicht innerhalb einer bestimmten Frist behoben, muss der VSP-Anbieter den Zugang zu den nicht konformen Inhalten sperren.

In den allgemeinen Geschäftsbedingungen für Online-Dienste, die von VSP-Anbietern angeboten werden, sollten die Bedingungen für die Klassifizierung und

---

[691] Art. 3a[1] UŚUDE.

[692] *Ustawa z dnia 19 listopada 2009 r. o grach hazardowych* (Glücksspielgesetz vom 19. November 2009), konsolidierter Text: Gesetzblatt *(Dziennik Ustaw*) von 2025, Punkt 595; vgl. Artikel 15d - 15i.

[693] Kapitel 6b, Artikel 47l - 47w Rundfunkgesetz, op. cit.

[694] Richtlinie 2010/13/EU des Europäischen Parlaments und des Rates vom 10. März 2010 zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste (AVMD-Richtlinie), ABl. L 95/1, zuletzt geändert durch Richtlinie (EU) 2018/1808 des Europäischen Parlaments und des Rates vom 14. November 2018 zur Änderung der Richtlinie 2010/13/EU zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste (Richtlinie über audiovisuelle Mediendienste) im Hinblick auf sich verändernde Marktgegebenheiten, ABl. L 303 vom 28. November 2018, sowie durch Verordnung (EU) 2024/1083 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Schaffung eines gemeinsamen Rahmens für Mediendienste im Binnenmarkt und zur Änderung der Richtlinie 2010/13/EU (Europäisches Medienfreiheitsgesetz), ABl. L 2024/1083, 17. April 2024.

Kennzeichnung von Inhalten, die Regeln für kommerzielle Kommunikation, die Verfahren für die Meldung jugendgefährdender Inhalte und die Kriterien für die Bewertung der Einhaltung der Vorschriften über schädliche Inhalte festgelegt sein; zudem sollten sie Informationen dazu enthalten, wie Beschwerden gegen die Sperrung des Zugangs zu Nutzerinhalten eingelegt werden können und wie personenbezogene Daten verarbeitet werden.

Der Anbieter kann einen Nutzer, der trotz vorheriger Aufforderung zur Unterlassung eines bestimmten Verhaltens wiederholt Verstöße begeht, vom Hochladen von Inhalten ausschließen. Im Allgemeinen gilt der Ausschluss für drei Monate, wenn die Verstöße jedoch Förderung von Terrorismus, Pornographie mit Beteiligung Minderjähriger oder Aufstachelung zu rassistischen Beleidigungen betreffen, kann ein dauerhafter Ausschluss verhängt werden. Derartige Entscheidungen des VSP-Anbieters sind zu begründen und können Gegenstand einer Beschwerde bei der KRRiT sein. Die KRRiT-Vorsitzende ist befugt, Beschlüsse zu fassen, mit denen der Zugang zu Inhalten auf der VSP, die gegen die Vorschriften über schädliche oder rechtswidrige Inhalte verstößt, eingeschränkt wird, aber auch den Zugang zu den von einem Nutzer hochgeladenen Inhalten wiederherzustellen oder einem Nutzer wieder die Möglichkeit zu geben, Inhalte auf die Plattform hochzuladen. Ähnlich wie Mediendiensteanbieter haben VSP-Anbieter die Pflicht zur Beweissicherung, das heißt sie müssen Kopien von Inhalten für 28 Tage ab dem Zeitpunkt der Entfernung von der Plattform aufbewahren und diese der KRRiT-Vorsitzenden auf Verlangen vorlegen.

Die Bestimmungen des Rundfunkgesetzes zu audiovisuellen Abrufmediendiensten[695] können auch für Inhalte relevant sein, die auf VSP – auch außerhalb der polnischen Rechtshoheit – angeboten werden, da kommerziell betriebene Kanäle auf Plattformen mit Katalogen von Videoinhalten als Mediendienste gelten. Die von der KRRiT verwaltete Liste von Anbietern audiovisueller Abrufmediendienste umfasst daher über 900 Dienste, von denen ein Großteil auf YouTube, X, Facebook, Instagram oder TikTok verfügbar ist.[696] Die KRRiT-Liste der VSP-Anbieter, für die das Rundfunkgesetz gilt, enthält dagegen lediglich 14 Dienste.[697] Die Regulierung von Anbietern audiovisueller Abrufmediendienste in Polen basiert weitgehend auf der AVMD-RL.[698] Die Anbieter solcher Dienste unterliegen jedoch neben einer grundlegenden Identifizierungspflicht auch einer Verpflichtung zur Transparenz der Eigentumsverhältnisse, die sich auch auf ihre sonstigen Mediendienste erstreckt. Anbieter audiovisueller Abrufmediendienste müssen die Eintragung in die von der KRRiT geführte Liste der VoD-Anbieter beantragen und der KRRiT jährliche Berichte über die Einhaltung der Bestimmungen zum Jugendschutz, zur Förderung europäischer Werke und zur Barrierefreiheit für Menschen mit Behinderungen vorlegen. Wenn innerhalb von 12 Monaten mindestens zweimal jugendgefährdende Inhalte ohne technische Schutzvorkehrungen oder andere Schutzmaßnahmen bereitgestellt wurden,

[695] Kapitel 6a, Art. 47a- 47k Rundfunkgesetz, op. cit.

[696] Von der KRRiT-Vorsitzenden geführte Liste der Anbieter von audiovisuellen Mediendiensten auf Abruf (VoD) - 4. August 2025 *(Lista dostawców audiowizualnych usług medialnych na żądanie (VOD) wpisanych do wykazu Przewodniczącej KRRiT stan na 4 sierpnia 2025 r.*)

[697] Von der KRRiT-Vorsitzenden geführte Liste der VSP-Anbieter – 4. August 2025 *(Lista dostawców Platform Udostępniania Wideo (VSP) wpisanych do wykazu Przewodniczącej KRRiT stan na 4 sierpnia 2025 r.*)

[698] Dies gilt insbesondere für Bestimmungen über die Förderung europäischer Werke und die kommerzielle Kommunikation. Die Barrierefreiheit für Menschen mit Behinderungen wird durch die Verpflichtung gewährleistet, mindestens 30 % des Katalogs mit entsprechenden Funktionen anzubieten.

kann die KRRiT-Vorsitzende (nach einer erfolglosen Aufforderung zur Einstellung dieser Praktiken) den Anbieter des betreffenden Dienstes durch einen förmlichen Beschluss von der Liste streichen.

6.2.2 Spezielle Vorschriften im Rundfunkgesetz zum Schutz Minderjähriger vor Online-Gefahren

Das Rundfunkgesetz enthält ein spezielles Regelwerk zum Schutz Minderjähriger vor schädlichen Inhalten, das für lineare Programmdienste (Hörfunk und Fernsehen) einschließlich online übertragener Dienste[699] und, wie bereits erwähnt, auch für audiovisuelle Abrufmediendienste[700] und VSP[701] gilt.

Bei linearen Programmdiensten und audiovisuellen Abrufmediendiensten unterscheidet das Gesetz zwischen Inhalten, die „der körperlichen, geistigen oder sittlichen Entwicklung Minderjähriger abträglich sind", insbesondere Inhalte, die Pornografie oder grundlose Gewalttätigkeit enthalten, und Inhalten, die „eine nachteilige Auswirkung auf die gesunde körperliche, geistige oder sittliche Entwicklung von Minderjährigen haben können", bei denen eine solche negative Auswirkung lediglich wahrscheinlich ist.[702] Die erste Kategorie von Inhalten ist in linearen Programmdiensten vollständig und in VoD-Diensten, wenn die Inhalte ohne wirksame technische Schutzvorkehrungen oder sonstige geeignete Maßnahmen zur Verhinderung des Zugriffs Minderjähriger bereitgestellt werden, bedingt verboten.[703] Inhalte, die in die zweite Kategorie fallen, dürfen bei linearen Programmdiensten nur zwischen 23.00 Uhr und 6.00 Uhr ausgestrahlt werden und müssen hinsichtlich ihres jugendgefährdenden Potenzials und der Art des schädlichen Inhalts (Gewalt, Sex, Vulgärsprache, Drogen) ordnungsgemäß klassifiziert und gekennzeichnet

[699] Art. 18 Abs. 4-6 Rundfunkgesetz, op. cit., Punkt 938.
[700] Ebd., Art. 47a Rundfunkgesetz, S., op. cit., Punkt 913.
[701] Ebd., Art. 47o Abs. 1 Ziff. 1 und Abs. 2, Art. 47p Rundfunkgesetz, Punkt 1019.
[702] Diese Unterscheidung stützt sich auf frühere Wortlaute der Richtlinie des Rates 89/552/EWG vom 3. Oktober 1989 zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Ausübung der Fernsehtätigkeit (Fernsehrichtlinie) und der AVMD-RL vor ihrer Änderung durch Richtlinie 2018/1808.
[703] Diese Schutzvorkehrungen und -maßnahmen sind in der Selbstregulierung, dem Verhaltenskodex vom 26. Juni 2014, geändert 2022, festgelegt, mit detaillierten Regeln für den Schutz Minderjähriger bei audiovisuellen Abrufmediendiensten. Zu diesen Schutzvorkehrungen und -maßnahmen gehören: a) ein System, das den Inhalt nur nach Angabe der Kreditkartendaten des Nutzers, einer Zahlung mit einer Kreditkarte, einer elektronischen Überweisung oder einer gleichwertigen Lösung (zum Beispiel PayPal), einer Zahlung durch Hinzufügen zur Rechnung, einem Login in ein Online-Banking-System, das eine Altersverifizierung oder eine Bestätigung der Volljährigkeit durch einen eID-Anbieter ermöglicht, und/oder der Anwendung eines technischen Systems für eine wirksame elterliche Kontrolle zugänglich macht; b) ein anderes System, das den Nutzerzugang zum Inhalt von einer effektiven Überprüfung der Volljährigkeit abhängig macht (gemeldet an IAB Polska). Bei Anwendung eines dieser Modelle kann ein Anbieter innerhalb eines VoD-Dienstes einen geschützten Modus (Kindersicherung) einrichten, der ungeeignete Inhalte aus der Ansicht entfernt und nur mit einem PIN-Code oder einer gleichwertigen, von einem erwachsenen Nutzer vorzunehmenden Maßnahme deaktiviert werden kann.

werden;[704] auch bei audiovisuellen Abrufmediendiensten unterliegen solche Inhalte derselben Klassifizierung und gleichen Kennzeichnungsanforderungen.[705] Darüber hinaus besteht die Pflicht, ausgestrahlte oder auf Abruf zur Verfügung gestellte Sendungen je nach dem Grad der Schädlichkeit für Minderjährige in verschiedenen Altersgruppen zu kennzeichnen. Die Kategorien an Altersgruppen sind in den Verordnungen der KRRiT definiert und beschrieben; für lineare Programmdienste bestehen fünf Kategorien (ohne Altersgrenze, ab 7, 12, 16 und 18 Jahren), während es für VoD-Dienste vier Altersgruppen gibt (ohne Altersgrenze, ab 12, 16 und 18 Jahren). Bei Hörfunk- und Fernsehdiensten dürfen Sendungen, die als für Minderjährige ab 16 Jahren geeignet gekennzeichnet sind, nur nach 20.00 Uhr ausgestrahlt werden.

Für VSP-Dienste regelt das Rundfunkgesetz Inhalte, die „der gesunden körperlichen, geistigen oder sittlichen Entwicklung Minderjähriger abträglich sind, insbesondere solche, die pornografische Inhalte enthalten oder grundlose Gewalttätigkeit zeigen". Die Übermittlung solcher Inhalte ohne wirksame technische Schutzvorkehrungen ist verboten. VSP-Anbieter sind verpflichtet, wirksame technische Schutzvorkehrungen einschließlich elterlicher Kontrollsysteme oder anderer geeigneter Maßnahmen zu treffen, um Minderjährige vor dem Zugriff auf schädliche Inhalte zu schützen, und sie sind verpflichtet, Nutzern die Möglichkeit zu geben, ihre hochgeladenen Inhalte zu klassifizieren und technische Schutzvorkehrungen zu treffen. Die Bedingungen für die Klassifizierung und Kennzeichnung jugendgefährdender Inhalte sind in den KRRiT-Verordnungen festgelegt, wonach vier Alterskategorien unterschieden werden: keine Altersgrenze, 12+, 16+ und 18+. Diese werden dort beschrieben und es werden Vorlagen für visuelle Kennzeichnungen für Inhalte, die jeweils für die drei Kategorien über 12 Jahre geeignet sind, festgelegt.[706] Wie bereits erwähnt, müssen VSP-Anbieter diese Anforderungen an die Klassifizierung und Kennzeichnung sowie die Verfahren zur Meldung jugendgefährdender Inhalte in ihren allgemeinen Geschäftsbedingungen berücksichtigen.

6.2.3 Schutz Minderjähriger im Zusammenhang mit dem Zugang zu pornografischen Inhalten – neue Initiativen

Das polnische Strafgesetzbuch[707] enthält Bestimmungen zu Pornografie, die insbesondere die öffentliche Darstellung solcher Inhalte für Personen, die nicht damit konfrontiert werden möchten, und die für Minderjährige unter 15 Jahren zugängliche Verbreitung von Pornografie unter Strafe stellen, sowie verschiedene Bestimmungen zu Pornografie, die

[704] Einschlägige grafische Symbole müssen für Fernsehzuschauer mindestens fünf Sekunden vor der Ausstrahlung und fünf Sekunden nach jeder Werbeunterbrechung sichtbar sein; bei Hörfunksendungen muss der vorgeschriebene mündliche Warnhinweis vorangestellt werden.
[705] Dauer und Platzierung einschlägiger grafischer Symbole sind jedoch flexibler geregelt – mit der Maßgabe, dass der Nutzer eines VoD-Dienstes die Kennzeichnung zum Zeitpunkt der Auswahl des Programms und während seiner Dauer leicht erkennen kann.
[706] KRRiT-Verordnung vom 13. April 2022, Gesetzblatt *(Dziennik Ustaw)* von 2022, Punkt 1019.
[707] *Ustawa z dnia 6 czerwca 1997 r. Kodeks karny* (Act of 6 June 1997), konsolidierter Text: Gesetzblatt *(Dziennik Ustaw*) 2025, Punkt 383.

Minderjährige, Tiere oder Gewalttätigkeiten zum Gegenstand hat.[708] Der Begriff Pornografie ist jedoch nicht gesetzlich definiert, sondern wird vielmehr durch die Rechtslehre und die Rechtsprechung ausgelegt.

Jüngste Bedenken hinsichtlich des Schutzes Minderjähriger vor Online-Gefahren, insbesondere vor Pornografie, haben zu Gesetzesvorschlägen geführt, die darauf abzielen, den Zugang Minderjähriger zu solchen Inhalten zu beschränken. Verfügbare Statistiken verdeutlichen das Ausmaß des Problems: Über 70 % der Kinder und Jugendlichen geben an, dass Pornografie leicht zugänglich ist; das Durchschnittsalter für den ersten Kontakt liegt bei 11 Jahren, während 18,5 % der Befragten angeben, vor ihrem 10. Lebensjahr mit sexuellen Inhalten in Berührung gekommen zu sein. Darüber hinaus haben 80 % der Kinder keine Software zur elterlichen Kontrolle auf ihren Mobilgeräten; etwa 54 % der Teenager sagen, dass ihre Eltern keine Regeln für die Internetnutzung festlegen, während etwa 29 % die elterliche Kontrolle von Inhalten und Bildschirmzeit für unwirksam halten.[709]

Bereits im Mai 2023 legte die Regierung einen Gesetzentwurf zum Schutz Minderjähriger vor ungeeigneten Online-Inhalten vor,[710] der es den Abonnenten von Internetzugangsdiensten ermöglicht, von den Anbietern solcher Dienste zu verlangen, dass sie den Zugang zu Pornografie einschränken. Der Vorschlag wurde vor den Parlamentswahlen 2023 zurückgezogen. Anfang 2025 veröffentlichte das Ministerium für Digitalisierung den Entwurf eines „Gesetzes über den Schutz Minderjähriger vor dem Zugang zu schädlichen Online-Inhalten" (im Folgenden der „Ministerialentwurf") und leitete öffentliche Konsultationen ein.[711] Eine ähnliche Initiative, die sich allerdings auf Pornografie beschränkte, wurde zuvor als „Bürgerentwurf" dem *Sejm* vorgelegt.[712] Der Ministerialentwurf hatte ursprünglich einen breiten Anwendungsbereich, da er Pornografie und andere schädliche Inhalte umfasste, ohne diese Begriffe zu definieren. Nach Kritik im Rahmen der Konsultationen wurde ein überarbeiteter Ministerialentwurf auf Pornografie eingegrenzt und entsprechend umbenannt;[713] jegliche Verweise auf andere schädliche Inhalte wurden entfernt. Die für die Ausarbeitung der Entwürfe Verantwortlichen lehnten jedoch die Forderung nach einer Definition von Pornografie mit der Begründung ab, dass der Begriff in der strafrechtlichen Lehre und Rechtsprechung hinreichend klar sei und dass eine gesetzliche Definition einen dynamischen Ansatz behindern könnte. Interessanterweise

[708] Art. 202 Abs. 1, Art. 200 Abs. 3-6, Art. 202 Abs. 3-5 Strafgesetzbuch.

[709] Begründung des Gesetzentwurfs durch das Ministerium für Digitalisierung – 29. August 2025, 3, Datei: *Projekt ustawy i uzasadnienie małoletni 29.08.2025 r.*.docx, S. 13-14.

[710] Regierungsentwurf vom 19. Mai 2023 (poln.), amtliche Veröffentlichung des *Sejm* (IX. Wahlperiode) Nr. 3238.

[711] *Projekt ustawy o ochronie małoletnich przed dostępem do treści szkodliwych w internecie* (Gesetzentwurf zum Schutz Minderjähriger vor dem Zugang zu schädlichen Inhalten im Internet) zeigt die Entwicklung des Gesetzentwurfs des Ministeriums für Digitalisierung mit der Begründung und einer Folgenabschätzung sowie Konsultationsbeiträgen.

[712] Bürgerentwurf des Gesetzes zum Schutz Minderjähriger vor pornografischen Inhalten im Internet und zur Änderung des Gesetzes – Telekommunikationsgesetz (poln.). Der Entwurf wurde am 20. Dezember 2024 von einem Ausschuss vorgelegt, der sich aus einigen konservativen Organisationen und Abtreibungsgegnern zusammensetzte. Die Verfassung (Artikel 118.2) räumt einer Gruppe von mindestens 100 000 Bürgern das Recht auf Gesetzesinitiative ein.

[713] Gesetzentwurf für den Schutz Minderjähriger vor dem Zugang zu pornografischen Inhalten im Internet, 29. August 2025, verfügbar seit 1. September 2025.

enthielt der dem Parlament vorgelegte Bürgerentwurf eine Definition von Pornografie,[714] die auf den Elementen des Begriffs „sexuell eindeutiger Inhalt" basiert, wie sie im Begründungsbericht zum Übereinkommen des Europarats über Computerkriminalität beschrieben werden.[715]

Im Ministerialentwurf wird ein Mechanismus zum Schutz Minderjähriger vorgeschlagen, der aus drei wesentlichen Elementen besteht: 1) die Verpflichtung der Anbieter von Online-Diensten,[716] die Zugang zu pornografischen Inhalten bieten, wirksame Maßnahmen zur Altersverifizierung zu ergreifen, um Minderjährige am Zugang zu solchen Inhalten zu hindern; 2) die Erstellung eines Verzeichnisses von Domainnamen nicht konformer Dienste; 3) die Verpflichtung für Anbieter von Internetzugangsdiensten, den Zugang zu Websites zu verhindern, die in dem Verzeichnis aufgeführte Domainnamen verwenden.

Die Verpflichtung zur Umsetzung effektiver Maßnahmen zur Altersverifizierung würde für alle Anbieter von elektronisch erbrachten Diensten gelten, ein Begriff, der im polnischen Recht als Äquivalent zu „Anbietern von Diensten der Informationsgesellschaft" im EU-Recht verwendet wird. Im Rahmen der Konsultationen wurde in einigen Beiträgen vorgeschlagen, den Anwendungsbereich des Entwurfs einzuschränken, zum Beispiel auf groß angelegte pornografische Dienste oder auf Websites mit einem erheblichen Anteil an pornografischen Inhalten, oder bestimmte Anbieter wie reine Durchleiter oder Kleinstunternehmen auszunehmen. Diese Vorschläge wurden von den Verfassern des Entwurfs mit der Begründung abgelehnt, dass eine Differenzierung der Verpflichtungen nach Art des Anbieters zu einem uneinheitlichen Schutz Minderjähriger führen würde.

Die vorgeschlagenen Vorschriften sollen einen breiten territorialen Anwendungsbereich haben, der für „Anbieter, die Online-Dienste für Nutzer im Hoheitsgebiet Polens erbringen, unabhängig vom Ort der Niederlassung oder der beruflichen Tätigkeit des Anbieters" gilt. Trotz des in den Konsultationen vorgebrachten Arguments des Herkunftslandprinzips gemäß Artikel 3 der EC-RL enthält der Entwurf in Bezug auf die in der EU/im EWR ansässigen Anbieter keinen Hinweis auf Anforderungen für Maßnahmen, die von diesem Prinzip abweichen.[717] In der Begründung des Entwurfs wird erklärt, dass es im Interesse der Wirksamkeit unerlässlich ist, Klagen gegen Websites zuzulassen, die von außerhalb Polens stammen und auf die polnische Minderjährige zugreifen, und es wird auf die „ähnliche Konstruktion" des DSA in Bezug auf

[714] Art. 2 Abs. 3 des Bürgerentwurfs: „Pornografische Inhalte – Inhalte, die in irgendeiner visuellen Form, sei es real, simuliert, geschaffen und/oder bearbeitet, a) Geschlechtsverkehr, einschließlich genital-genital, oral-genital, anal-genital oder oral-anal, zwischen Personen des anderen oder des gleichen Geschlechts; b) Masturbation; c) Sodomie oder d) sadistische oder masochistische Praktiken in einem sexuellen Kontext darstellen."

[715] Begründungsbericht zum Übereinkommen des Europarats über Computerkriminalität (engl.), Abs. 100. Das Ministerium für Digitalisierung nimmt die Definition des Europarats zur Kenntnis, hält sie jedoch für unzureichend, da das Erfordernis der „Absicht, sexuelle Erregung hervorzurufen," fehlt, das nach der vorherrschenden Auffassung ein wesentlicher Aspekt des Begriffs der Pornografie im polnischen Strafrecht ist.

[716] Der Entwurf bezieht sich auf den Begriff des Diensteanbieters im Sinne von Art. 2 Abs. 6 UŚUDE, der dem Begriff des Anbieters eines Dienstes der Informationsgesellschaft gemäß der EC-RL entspricht.

[717] Art.3 Abs. 4 und 5 EC-RL; Art. 3b UŚUDE.

Vermittlungsdienste verwiesen, die Nutzern in der EU angeboten werden, unabhängig davon, wo der Diensteanbieter niedergelassen ist.

Mit dem Mechanismus zur Altersverifizierung soll eindeutig festgestellt werden, dass der Nutzer des Dienstes die Volljährigkeit erreicht hat; Selbstdeklaration, Altersschätzungsmethoden und biometrische Methoden sind ausdrücklich ausgeschlossen. Der Entwurf enthält zwar keine genauen Angaben zu den zu verwendenden Methoden, legt aber die Anforderungen an den Mechanismus fest, wie zum Beispiel Gewährleistung des höchsten Schutzstandards für personenbezogene Daten und die Privatsphäre des Nutzers, Bereitstellung von mindestens zwei Methoden, die allgemein zugänglich und für die Nutzer leicht zu verwenden sind (darunter mindestens eine, die für Menschen mit Behinderungen und/oder nicht polnischsprachige Personen geeignet ist), ständige Verfügbarkeit der gewählten Methode, Zuverlässigkeit der Daten, auf denen die Methode beruht, Verhinderung einer leichten Umgehung der Methode durch die Nutzer und, soweit möglich, Interoperabilität mindestens einer angebotenen Methode mit anderen Online-Diensten. Darüber hinaus muss die Altersverifizierung die Kriterien erfüllen, die einem hohen Sicherheitsniveau für elektronische Identifizierungsmittel entsprechen,[718] und wenn die Verarbeitung personenbezogener Daten erforderlich ist, muss sie mit der DSGVO im Einklang stehen,[719] insbesondere mit dem Grundsatz der Datensparsamkeit; die erhobenen Daten dürfen nur für die Altersverifizierung und nicht für die Erstellung von Nutzerprofilen verwendet werden. Einige dieser Datenschutzgarantien wurden als Reaktion auf die bei den Konsultationen zum ersten Ministerialentwurf geäußerten Bedenken eingeführt. In der Begründung des Entwurfs wird auf die Arbeiten an der europäischen digitalen Brieftasche (EUDI-Wallet) verwiesen und betont, dass diese die Möglichkeit einer Altersverifizierung ohne Erhebung zusätzlicher Informationen bieten wird.[720]

Das Verzeichnis der Domainnamen, die Zugang zu pornografischen Inhalten ohne vorherige Altersverifizierung bieten, wird vom Wissenschaftlichen und Akademischen Computernetzwerk – Nationales Forschungsinstitut *(Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy* – NASK) verwaltet.[721] Die Auswahl des NASK beruht auf seiner Erfahrung und seinem technologischen Hintergrund, insbesondere auf seiner bisherigen Rolle bei der Pflege einer Warnliste für gefährliche Websites.[722] Vor der Versendung des Bescheids muss der Präsident des UKE den Domaininhaber (Diensteanbieter) informieren und ihm eine Frist von zwei Tagen zur Stellungnahme einräumen. Der Bescheid muss außerdem dem Diensteanbieter übermittelt werden, der

[718] Wie in Art. 8 Abs. 2 lit. c) der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG [2104] ABl. L 257/73 niedergelegt.

[719] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

[720] Weitere Informationen über die europäische digitale Brieftasche finden sich auf der speziellen Website der Europäischen Kommission.

[721] Forschungs- und Entwicklungsorganisation, Betreiber von Datennetzen und Betreiber eines Internet-Domainnamen-Registers für die länderspezifische .pl Top-Level-Domain und ein Teil des nationalen Cybersicherheitssystems.

[722] Auf der Grundlage des Gesetzes vom 28. Juli 2023 über die Bekämpfung von Missbräuchen in der elektronischen Kommunikation *(Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej*), konsolidierter Text: Gesetzblatt *(Dziennik Ustaw*), 2024, Punkt 1803.

jederzeit Einspruch gegen die Eintragung in das Verzeichnis erheben kann.[723] Einsprüche sind binnen 14 Tagen vom Präsidenten des UKE zu prüfen, wobei im Falle einer Zurückweisung das Recht besteht, Beschwerde bei Gericht einzulegen. Wird dem Einspruch stattgegeben, muss der Präsident das NASK anweisen, die Domain binnen drei Tagen aus dem Verzeichnis zu streichen. Die Anbieter von Internetzugangsdiensten sind verpflichtet, den Zugang zu Websites, die im Verzeichnis aufgeführte Domainnamen verwenden, innerhalb von 48 Stunden nach deren Eintragung in das Verzeichnis kostenlos zu unterbinden. Die Sperrung erfolgt durch die Entfernung der betreffenden Namen aus Domain-Namen-Systemen (DNS) und die Umleitung der Nutzer auf eine UKE-Website, auf der eine entsprechende Meldung angezeigt wird. Wenn eine Domain aus dem Verzeichnis gestrichen wird, muss der Zugang binnen 48 Stunden wiederhergestellt werden. Das Verzeichnis, das in einem IT-System gepflegt wird, um eine automatische Datenübermittlung an die Anbieter zu ermöglichen, wird nicht öffentlich zugänglich sein.

Der Ministerialentwurf räumt dem Präsidenten des UKE außerdem die Befugnis ein, die Einhaltung der oben genannten Pflichten seitens der Anbieter von Online-Diensten und Internetzugängen zu überwachen, Geldstrafen zu verhängen, Empfehlungen für die Zeit nach der Kontrolle auszusprechen und Entscheidungen zu treffen, die die Beseitigung von Unregelmäßigkeiten anordnen und Abhilfemaßnahmen festlegen. Im Gegensatz zum Bürgerentwurf und zum Glücksspielgesetz, die Beschränkungen für gelistete Domains vorsehen, die nicht mit den Jugendschutzbestimmungen übereinstimmen, schlägt der Ministerialentwurf nicht vor, die Erbringung von zahlungspflichtigen Diensten auf Websites zu verbieten, die im Verzeichnis der Domainnamen, welche Zugang zu pornografischen Inhalten ohne vorherige Altersverifizierung bieten, eingetragen sind.

Ende 2025 befand sich der ministerielle Gesetzentwurf zum Schutz Minderjähriger vor pornografischen Inhalten im Internet noch in einem frühen Entwicklungsstadium. Es ist ungewiss, ob, wann und in welcher Form der Entwurf beschlossen werden wird. Es besteht jedoch kein Zweifel daran, dass die Verabschiedung des Gesetzes zur Umsetzung des DSA die weitere Prüfung zusätzlicher Initiativen zum Schutz Minderjähriger erleichtern kann. Das Verhältnis solcher Initiativen zu EU-Rechtsvorschriften, insbesondere dem DSA, der EC-RL und der AVMD-RL, sowie zu Bestimmungen des polnischen Rechts, mit denen sie umgesetzt werden und die die nationale Politik in den jeweiligen Bereichen festlegen, ist nach wie vor eine komplexe Angelegenheit, die einer weiteren sorgfältigen Prüfung bedarf.

[723] Das Fehlen einer Frist für die Einreichung des Einspruchs unterscheidet sich von der Lösung für gelistete Glücksspiele, für die eine zweimonatige Frist gilt.

6.3 Beispiel Vereinigtes Königreich

Dr Marriet Jones, Dozentin für Recht, Middlesex University, London

6.3.1 Nationaler Rechtsrahmen für Plattformen im Gesetz über Online-Sicherheit

Das britische Gesetz über Online-Sicherheit (Online Safety Act, OSA) wurde im September 2023 nach fast zehnjähriger Vorarbeit verabschiedet.[724] Mittlerweile sind die meisten Bestimmungen anwendbar, und bis 2026 dürfte es vollständig umgesetzt sein. Der OSA ist ein gewichtiges Instrument, sowohl vom Umfang und der Zahl der Bestimmungen her als auch vom Geltungsbereich und den erklärten Zielen. Er versucht, fast alle denkbaren Schäden zu erfassen, die online oder über ein Online-Medium verursacht werden können, und beschränkt sich im Hinblick auf Kinder nicht auf rechtswidrige Inhalte, sondern regelt auch „legale, aber schädliche" Online-Inhalte.

Die zentrale Wirkungsweise des OSA besteht darin, dass der Staat private Unternehmen dazu verpflichtet, von Dritten erstellte Inhalte aktiv zu überwachen, zu bewerten und zu entfernen, und Maßnahmen zum Schutz von Kindern vorschreibt, wie etwa eine verstärkte Altersüberprüfung. So müssen Dienste, die pornografische Inhalte veröffentlichen, seit dem 25. Juli 2025 eine „hochwirksame Altersfeststellung" verwenden, um Kindern den Zugriff darauf zu verwehren.[725]

Der OSA gilt für eine breite Palette von Nutzer-zu-Nutzer-Diensten, Suchmaschinen und Inhaltsanbietern, auf die britische Nutzer zugreifen können, unabhängig vom Sitz des Dienstes. Er gilt sowohl für „Nutzer-zu-Nutzer-Dienste", darunter auch Plattformen wie YouTube oder Facebook, auf denen Nutzer Inhalte hochladen und teilen können, als auch „Suchdienste", zu denen Suchmaschinen wie Google gehören. Ein Nutzer-zu-Nutzer-Dienst ist ein regulierter Dienst, wenn er im Vereinigten Königreich eine beträchtliche Anzahl von Nutzern hat. Mit wenigen vorgeschriebenen Ausnahmen (etwa E-Mail- und Messaging-Diensten) sind alle nutzergenerierten Inhalte in einem regulierten Nutzer-zu-Nutzer-Dienst auch selbst reguliert.

Für verschiedene Kategorien von Diensten enthält der OSA zusätzliche Pflichten. Am strengsten sind die Pflichten und die Aufsicht bei Diensten der Kategorie 1. Bei seiner Einführung enthielt der OSA separate Bestimmungen, die Erwachsene vor „legalen, aber schädlichen" Inhalten schützen sollten. Diese Bestimmungen wurden zwar gestrichen, aber an ihre Stelle traten die Pflichten, die für Anbieter der Kategorie 1 gelten. In Kategorie 1 fallen Anbieter, die entweder im Durchschnitt mehr als 34 Millionen monatliche Nutzer im

[724] Britische Regierung, Online Safety Act 2023.

[725] In Abschnitt 81 des OSA heißt es:

(2) Eine Pflicht, durch Altersüberprüfung oder Altersschätzung (oder beides) sicherzustellen, dass Kinder üblicherweise nicht auf Inhalte stoßen können, bei denen es sich um regulierte pornografische Inhalte des Anbieters in Bezug auf den Dienst handelt. (3) Die Altersüberprüfung oder Altersschätzung muss so beschaffen sein und so eingesetzt werden, dass sie in hohem Maße geeignet ist, korrekt festzustellen, ob ein bestimmter Nutzer ein Kind ist oder nicht.

Vereinigten Königreich haben und ein System zur Empfehlung von Inhalten verwenden oder aber mehr als 7 Millionen monatliche Nutzer im Vereinigten Königreich haben, ein System zur Empfehlung von Inhalten verwenden und eine Funktion bereitstellen, mit der Nutzer regulierte nutzergenerierte Inhalte in dem Dienst weiterleiten oder mit anderen Nutzern dieses Dienstes teilen können.[726] Für Dienste, bei denen die Wahrscheinlichkeit hoch ist, dass Kinder auf sie zugreifen, gelten zusätzliche, strengere Verpflichtungen.

Der OSA unterscheidet folgende Hauptkategorien schädlicher Inhalte: An erster Stelle stehen rechtswidrige Inhalte wie Terrorismus, sexuelle Ausbeutung und Missbrauch von Kindern, Hetze und Betrug. Des Weiteren gibt es für Kinder schädliche Inhalte, unterteilt in Inhalte mit Primärpriorität (z. B. Pornografie oder Inhalte, die für Suizid, Selbstbeschädigung oder Essstörungen werben), Inhalte mit Priorität (z. B. Mobbing, Aufstachelung zum Hass oder zur Teilnahme an gefährlichen Stunts) und nicht benannte Inhalte, die dennoch ein erhebliches Risiko für beträchtlichen Schaden darstellen.

Bei der Regelung handelt es sich nicht um das übliche „Notice-and-Takedown"-System, das aus anderen Rechtsvorschriften und Rechtsordnungen bekannt ist, sondern um eine proaktive Verpflichtung zur Identifizierung und Entfernung bestimmter Inhalte. Der OSA erlegt allen regulierten Nutzer-zu-Nutzer-Diensten Pflichten auf. So müssen diese die von bestimmten Arten rechtswidriger Inhalte ausgehenden Risiken bewerten, mindern und steuern, den Nutzern die Möglichkeit zur Meldung rechtswidriger Inhalte geben, ein Beschwerdeverfahren einrichten und bei der Umsetzung von Sicherheitsmaßnahmen und -strategien das Recht auf freie Meinungsäußerung und Privatsphäre berücksichtigen.

Wie bereits erwähnt, haben Anbieter der Kategorie 1 strengere Pflichten, denn sie müssen (1) die Nutzer entscheiden lassen, ob sie ihre Identität verifizieren und was für Inhalte sie sehen, wozu auch gehört, ob sie Inhalte von Nutzern sehen, die ihre Identität nicht verifiziert haben, (2) die Meinungsfreiheit schützen, (3) die Nutzer vor betrügerischer Werbung schützen, (4) die Einhaltung der Nutzungsbedingungen des Dienstes gewährleisten (wozu auch gehört, dass der Diensteanbieter nutzergenerierte Inhalte entfernt, wenn –aber nur dann, wenn – sie den Nutzungsbedingungen nicht entsprechen), (5) einen jährlichen „Transparenzbericht" an das Ofcom[727] mit den von diesem geforderten Angaben veröffentlichen (siehe Abschnitt 6.1.3.4) und (6) verschiedene zusätzliche Pflichten erfüllen, darunter die Erstellung einer Zusammenfassung der jüngsten Risikobewertung des Dienstes in Bezug auf rechtswidrige Inhalte und Kinder und die Einrichtung eines Beschwerdeverfahrens.

Kurz gesagt schreibt der OSA eine Sorgfaltspflicht analog zur Sorgfaltspflicht im Deliktsrecht oder in den Gesundheits- und Sicherheitsgesetzen vor. Die Plattformen müssen nun Maßnahmen ergreifen, um das Posten rechtswidriger Inhalte zu verhindern, und bereits gepostete Inhalte entfernen oder sperren. Dazu gehören Inhalte, die nach britischem Recht schon lange als rechtswidrig gelten, darunter terroristische Inhalte, Material von sexuellem Kindesmissbrauch, Hassverbrechen und Betrug. In Bezug auf Kinder erstreckt sich diese Pflicht auch auf ansonsten legale Inhalte, die für Kinder schädlich sein können (siehe Abschnitt 6.3.2). Neben dieser Pflicht zur Moderation von Inhalten haben Diensteanbieter und Plattformen auch die Pflicht, Risikobewertungen vorzunehmen und für eine

[726] Vorschrift 3 des OSA (Schwellenwert-Bedingungen der Kategorien 1, 2A und 2B) Vorschriften 2025.
[727] Das Ofcom (Office of Communications) ist die britische Regulierungsbehörde für Kommunikationsdienste.

angemessene Risikominderung zu sorgen. Dazu kommen Pflichten im Zusammenhang mit der Berichterstattung und der Plattformgestaltung.

Zur Durchsetzung der neu geschaffenen Pflichten überträgt der OSA dem Ofcom als unabhängiger Aufsichtsbehörde für die britische Kommunikationsbranche umfangreiche neue Befugnisse. Er benennt das Ofcom als unabhängige Regulierungsbehörde für Online-Sicherheit. Zu seinen Aufgaben gehört die Überwachung und Durchsetzung des neuen Regulierungsrahmens.[728]

Daher gehört zu den Aufgaben des Ofcom auch die Ausarbeitung von Verfahrensregeln, mit denen die Bestimmungen des OSA konkretisiert werden. Diese Verfahrensregeln umfassen unter anderem Leitlinien für Plattformgestaltung, Empfehlungsalgorithmen, Inhaltsmoderation, Aufsicht und Governance, Mechanismen für Beschwerden, Meldungen und die Kontrolle durch Eltern, die Bewertung der Einhaltung von Vorschriften und die Untersuchung von Verstößen, die Durchsetzung von Pflichten und die Verhängung von Sanktionen.[729] Diese Sanktionen können sehr hoch ausfallen: Möglich sind Geldbußen von bis zu GBP 18 Millionen oder 10 % des weltweiten Umsatzes sowie die Sperrung von Diensten.[730]

6.3.2 Konkrete Vorschriften für den Schutz von Kindern

Kinder gelten als besonders gefährdete Online-Nutzer, die anfälliger für Ausbeutung, Manipulation und psychische Schäden sind. Der OSA zielt daher darauf ab, den Online-Schutz für Kinder zu verbessern,[731] indem er einer Philosophie der eingebauten Sicherheit („Safety by Design")[732] folgt, wonach Plattformen Personen unter 18 Jahren proaktiv schützen müssen.[733] Laut OSA müssen Plattformen, bei denen die Wahrscheinlichkeit hoch ist, dass Kinder auf sie zugreifen, eine Bewertung der Risiken für deren Sicherheit durchführen und vorbeugende Maßnahmen zur Verhinderung von Schäden ergreifen.[734] Dabei legt Abschnitt 37 des OSA die Latte sehr niedrig, denn eine hohe Wahrscheinlichkeit, dass Kinder auf eine Plattform zugreifen, liegt danach bereits vor, „wenn es für Kinder möglich ist, auf den Dienst oder einen Teil davon zuzugreifen".

Die Pflicht, Schäden zu verhindern, umfasst nicht nur den Schutz vor illegalen Inhalten wie Material von sexuellem Missbrauch, sondern auch vor potenziell schädlichen legalen Inhalten, darunter Inhalte, die Suizid, Selbstverletzung oder Essstörungen fördern

[728] Britische Regierung, Online Safety Act 2023, Teil 7.
[729] Britische Regierung, Department for Science, Innovation and Technology (Ministerium für Wissenschaft, Innovation und Technologie), Online Safety Act: Protection of Children Codes of Practice – explanatory memorandum – GOV.UK, 24. April 2025.
[730] Anhang 13 des OSA; OSA (Weltweite Umsatzerlöse) Verordnung 2025/1032.
[731] Ebd., Abschnitt 1(3)(b)(i).
[732] Ebd., Abschnitt 1(3)(a).
[733] Diese Pflichten ergeben sich aus den Abschnitten 11 „Pflichten zur Bewertung der Risiken für Kinder", 12 „Sicherheitspflichten zum Schutz von Kindern" und 13 „Sicherheitspflichten zum Schutz von Kindern: Auslegung" des OSA, op. cit.
[734] Ebd., Abschnitte 35, 36 und 37.

oder dazu verleiten, sowie Pornografie.[735] Zu den erforderlichen Schritten gehören, strenge Maßnahmen zur Altersfeststellung mit geeigneten Verifizierungstechnologien zu ergreifen, Algorithmen so einzustellen, dass Minderjährigen keine schädlichen Inhalte empfohlen werden, bei der Einstellung von Berechtigungsfunktionen für Gruppenchats oder beim automatischen Hinzufügen Kinder zu berücksichtigen und unerwünschte Kontakte zu verhindern, etwa Direktnachrichten an Kinder von Fremden.[736]

Für die Altersüberprüfung sieht der OSA vor, dass eine Selbstauskunft nicht ausreicht und Methoden wie Gesichtserkennung oder Ausweiskontrollen eingesetzt werden müssen.[737] Es dürfte sich als schwierig erweisen, diese Pflicht mit konkurrierenden Gesetzen zum Schutz von Privatsphäre und personenbezogenen Daten in Einklang zu bringen, die ihrerseits ebenfalls Kinder stärker schützen als Erwachsene. Zu den Governance-Anforderungen gehört die Ernennung leitender Mitarbeiter zu Compliance-Verantwortlichen. Zudem müssen Plattform ihre Meldekanäle, ihre Inhaltsvorschriften und die zur Erkennung von Schäden eingesetzten Technologien veröffentlichen. Transparente Beschwerde- und Meldesysteme müssen Minderjährigen und deren Erziehungsberechtigten zugänglich gemacht werden. Der OSA nimmt die Plattformen außerdem in die Pflicht, indem er von ihnen verlangt, regelmäßig Bewertungen der Risiken für Kinder durchzuführen und Zusammenfassungen dieser Bewertungen zu veröffentlichen.[738]

6.3.3 Online-Glücksspiele, Kinder und das Gesetz über Online-Sicherheit

Der OSA hat neue Straftatbestände wie das „Cyberflashing“[739] eingeführt und fasst bestehende Bestimmungen zu Straftaten, soweit diese online begangen oder erleichtert werden, unter einem Dach zusammen. Darüber hinaus ist einer der wichtigsten Aspekte des OSA die Einführung rechtlicher Pflichten in Bezug auf Inhalte, die zwar legal sind, aber für Kinder schädlich sein können, wie oben dargelegt. Die Vermischung bestehender gesetzlicher Bestimmungen und Straftatbestände und die Art und Weise, wie das Gesetz diese in Bezug auf Kinder erweitert und extrapoliert, wird durch die Auswirkungen auf den britischen Rechtsrahmen für Glücksspiele veranschaulicht.

Das Glücksspielgesetz[740] von 2005 ist das zentrale Gesetz zur Regelung des Glücksspiels im Vereinigten Königreich. Eines seiner drei lizenzrechtlichen Ziele ist der Schutz von Kindern und anderen gefährdeten Personen vor Schädigung oder Ausbeutung durch Glücksspiele. Das Glücksspielgesetz stellt es unter Strafe, Personen unter 18 Jahren zu Glücksspielen einzuladen, aufzufordern oder zuzulassen, und sieht eine Altersüberprüfungs- und Lizenzierungsregelung vor, die sicherstellt, dass nur Personen

[735] Ebd., Abschnitt 61.
[736] Ebd., Abschnitte 11, 12 und 13, sowie die entsprechenden Pflichten für Suchmaschinen in den Abschnitten 28, 29 und 30.
[737] Ofcom, Age Assurance and Children’s Access Statement, 16. Januar 2025.
[738] Abschnitt 36 OSA.
[739] Crown Prosecution Service (Strafverfolgungsbehörde für England und Wales), „Prison sentence in first cyberflashing case“, 19. März 2024.
[740] Britische Regierung, Gambling Act 2005.

über 18 Jahren online spielen können, wobei lizenzierte Betreiber verpflichtet sind, Identität und Alter zu überprüfen. Glücksspielwerbung unterliegt Regeln, die von einem unabhängigen Gremium aufgestellt werden: dem Ausschuss für Werbepraktiken (Committee of Advertising Practice (CAP)) der Werbeaufsichtsbehörde (Advertising Standard Authority (ASA)). Die vom CAP aufgestellten Regeln sowie die Bestimmungen des Gambling Act und des Gambling (Licensing and Advertising) Act 2014[741] verbieten Werbung, die sich an Minderjährige richtet oder diese stark anspricht, und sehen vor, dass in den meisten Glücksspielwerbungen keine Personen vorkommen dürfen, die jünger aussehen als 25 Jahre.

Bei diesem Thema ist gut zu erkennen, wie der OSA die bestehenden britischen Rechtsvorschriften ergänzt. Er verbessert den bestehenden Schutz von Minderjährigen, indem er die Zuständigkeiten und Aufgaben auf Plattformen ausweitet, die Glücksspielinhalte anbieten oder bewerben. So erstrecken sich die Bestimmungen des Glücksspielgesetzes, die Glücksspiele für Minderjährige verbieten und lizenzierte Glücksspielanbieter zur Überprüfung des Alters verpflichten, nun auch auf soziale Medien, Suchmaschinen und Streaming-Plattformen. Die ASA, die die Werberegeln[742] des Glücksspielgesetzes durchzusetzen hat, verbot im Jahr 2023 mehrere Glücksspielwerbungen, weil darin enthaltene Animations- und Zeichentrickszenen geeignet waren, Kinder anzusprechen.[743] Sie wurden als Verstoß gegen Abschnitt 16 des Kodex für Werbung und direktes und werbliches Marketing außerhalb des Rundfunks (CAP Code)[744] gewertet, der die Ausbeutung junger und gefährdeter Menschen in Werbung und Marketing verbietet. Zudem verbot die ASA Werbung für Glücksspielplattformen mit Spitzenfußballern, da diese für Minderjährige besonders attraktiv ist.[745] Während also die bisherigen Rechtsvorschriften reaktiv wirkten, indem etwa Werbung wie oben beschrieben bewertet wurde, müssen diese Unternehmen nach dem Inkrafttreten des OSA nun proaktive Maßnahmen ergreifen, damit Kinder nicht mit Glücksspielwerbung und entsprechenden Inhalten in Berührung kommen.

Während die potenzielle Haftung für die Werbung für Glücksspiel-Websites bisher in erster Linie bei den Websites selbst lag oder bei den Werbern, etwa Influencern auf Plattformen wie YouTube, könnten gemäß dem OSA auch die Plattformen, die die Websites, Influencer und Werber hosten, selbst haften.

Ein weiterer anschaulicher Punkt sind Aktivitäten in Online-Spielen, die die Mechanismen von Glücksspielen nachahmen, indem sie Kinder dazu ermutigen, Geld für zufallsbasierte Belohnungen auszugeben, wie etwa Lootboxen in Online-Spielen. Deren Inhalt ist zufällig, und der Spieler erfährt erst, was er bekommt, wenn er die Box öffnet. Spieler können Lootboxen in der Regel mit Geld (auch mit virtuellen Währungen) kaufen oder über das Spiel darauf zugreifen. Es wurde die Befürchtung geäußert, dass diese

---

[741] Britische Regierung, Gambling (Licensing and Advertising) Act 2014.

[742] Code of Non-broadcast Advertising and Direct and Promotional Marketing (CAP Code); Code of Broadcast Advertising (BCAP Code).

[743] Siehe beispielsweise ASA, „ASA Ruling on Buzz Group Ltd.“, Complaint Ref. A23-1217474 Buzz Group Ltd, Pressemitteilung, 3. Januar 2024.

[744] Code of Non-broadcast Advertising and Direct and Promotional Marketing (CAP Code).

[745] Zu bestimmten Fällen siehe ASA, „Gambling, betting and gaming: Appeal to children – ASA | CAP“, 9. Mai 2023, sowie ASA, „ASA Ruling on LC International Ltd t/a Ladbrokes“,Complaint Ref. A22-1171467 Ladbrokes Betting Gaming Ltd, Pressemitteilung, 21. Dezember 2022.

Mechanismen in Spielen für Kinder schädlich sein könnten, etwa weil sie einer Spielsucht Vorschub leisten könnten.[746] Das Glücksspielgesetz von 2005 regelt Lootboxen nicht als Glücksspiel, und die britische Regierung lehnte nach umfangreichen Konsultationen ein Lootbox-Verbot ab. Stattdessen forderte sie im Jahr 2023 eine Selbstregulierung der Branche, um die Risiken zu minimieren.[747] Immerhin erkannte sie aber die unter anderem von der britischen Glücksspielkommission geäußerten Bedenken hinsichtlich der potenziellen Risiken für Kinder und gefährdete Spieler an. Durch die Einführung einer proaktiven Pflicht zur Verhinderung legaler, aber für Kinder potenziell schädlicher Inhalte hat der OSA die Selbstregulierung der Branche nun in eine gesetzliche Regulierung umgewandelt.

Berücksichtigt man alle oben erörterten Aspekte, so ist der OSA in Bezug auf seinen Geltungsbereich, seine Ziele und seine Funktionsweise ambitioniert, sodass sich an einer Vielzahl von Fronten Herausforderungen ergeben. Um nur ein Beispiel zu nennen: Der Zwang zu einer „hochwirksamen" Altersfeststellung, die auch eine biometrische Überprüfung oder Dokumentenprüfung einschließen könnte, würde möglicherweise gegen die Bestimmungen zum Schutz von Privatsphäre und personenbezogenen Daten verstoßen und wirft Fragen hinsichtlich der Inklusivität für Kinder ohne formellen Ausweis auf, ganz zu schweigen von der Frage, ob die Implementierung robuster, aber nicht-invasiver Verifizierungssysteme insbesondere für kleinere Diensteanbieter technisch überhaupt machbar ist.

Sowohl auf das Ofcom als zuständige Regulierungsbehörde als auch auf die vom OSA regulierten Anbieter kommen aufwändige und anspruchsvolle Pflichten zu, die in vielfacher Hinsicht noch nicht vollständig geklärt sind. Klar werden diese Pflichten erst nach einer gerichtlichen Prüfung, und dann müssen sie wohl in weiteren Regelungen oder Leitfäden konkretisiert werden. Für den ersten rechtlichen Test der neuen Regelung hat kürzlich Wikipedia gesorgt, indem sie Einspruch dagegen erhob, wie das Ofcom Dienste der Kategorie 1 in Regulation 3 des OSA definiert.[748] Sie beanstandete die Tatsache, dass sie als gemeinnützige Organisation in dieselbe Kategorie eingestuft wurde wie multinationale Großunternehmen wie Google oder Facebook. Der High Court of England and Wales ließ in seinem Urteil vom August 2025 die gerichtliche Überprüfung von zwei Aspekten des Entscheidungsprozesses des Ofcom zu, wies aber die beiden auf den Menschenrechten basierenden Einwände von Wikipedia entschieden zurück.[749] Gegen das Urteil kann noch Berufung eingelegt werden, und es ist davon auszugehen, dass die Gesetzgebung und die damit verbundenen Regelungen noch öfter gerichtlich überprüft werden, weil sich herausstellen könnte, dass sie erhebliche Auswirkungen auf Rechtsbereiche wie Redefreiheit und Privatsphäre sowie auf die digitale und sonstige Wirtschaft des Vereinigten Königreichs haben.

---

[746] Zendle D. et. al. (2020) „Paying for loot boxes is linked to problem gambling, regardless of specific features like cash-out and pay-to-win", *Computers in Human Behavior,* 102, S. 181–191, zitiert mit Genehmigung der britischen Regierung, Department for Culture, Media and Sport (Ministerium für Kultur, Medien und Sport): Government response to the call for evidence on loot boxes in video games – GOV.UK, 18. Juli 2022.

[747] Britische Regierung, Department for Culture, Media and Sport (Ministerium für Kultur, Medien und Sport) Loot boxes in video games: update on improvements to industry-led protections – GOV.UK, 18. Juli 2023.

[748] *Wikimedia Foundation (a charitable foundation registered in the United States of America), BLN v. Secretary of State for Science, Innovation and Technology* [2025] EWHC 2086 (Admin).

[749] Ebd., Rn. 133–137.

7. Vergleichende Analyse

Dr Mark D. Cole, Wissenschaftlicher Direktor, Institut für Europäisches Medienrecht (EMR), und Professor für Medien- und Telekommunikationsrecht, Universität Luxemburg, und Dr Sandra Schmitz-Berndt, Wissenschaftliche Mitarbeiterin, Institut für Europäisches Medienrecht (EMR)

Ungeachtet eines gemeinsamen internationalen Grundrechtsrahmens und – in den meisten der in dieser Veröffentlichung behandelten Länder – eines gemeinsamen EU-Rechtsrahmens zeigen die nationalen Berichte Unterschiede in der Rechtsdurchsetzung gegenüber Internetvermittlern in Europa.

Ein umfassendes Verständnis der Schwierigkeiten bei der Durchsetzung der geltenden Gesetze gegen illegale Inhalte und Desinformation in Europa erfordert einen Vergleich der nationalen gesetzlichen Anforderungen sowie der diesbezüglichen Sanktionsmechanismen und länderspezifischen Lösungen. Obwohl die EU-Gesetzgebung – hauptsächlich durch die jüngsten Ergänzungen des „digitalen Regelwerks" – eine erhebliche Harmonisierung vorangetrieben hat, die nur für die Mitgliedsstaaten unmittelbar bindend ist, bemühen sich Drittstaaten wie Türkiye ebenfalls, ihre Gesetze an EU-Standards anzugleichen.

Da der Schwerpunkt auf der Durchsetzung liegt, wird die folgende Analyse nicht auf nationale Unterschiede hinsichtlich der Definition illegaler Inhalte eingehen, insbesondere nicht im nationalen Strafrecht. Eine echte „Europäisierung" des Strafrechts hat außerhalb der EU-Rechtshoheit noch keine Gestalt angenommen, und innerhalb der EU beschränkt sich die Harmonisierung bisher auf besonders schwere Straftaten mit grenzüberschreitender Dimension im Rahmen des Vertrags von Lissabon und die Umsetzung der polizeilichen und justiziellen Zusammenarbeit im Rahmen des AEUV. Darüber hinaus betrifft die Harmonisierung in einigen Fällen bestimmte Verhaltensweisen, die die Grundwerte der EU gefährden, etwa diejenigen, auf die die Richtlinie zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt abzielt.[750] Im Gegensatz dazu ist es besonders interessant, Unterschiede in den nationalen Ansätzen beim Umgang mit Inhalten zu beobachten, die möglicherweise nicht per se illegal sind, aber schädliche Auswirkungen haben, z. B. das derzeit viel diskutierte Problem, wie auf Desinformationskampagnen reagiert werden soll. Aus diesem Grund bildet dieser Bereich den Ausgangspunkt der folgenden Analyse, bevor die nationalen Ansätze zur Durchsetzung von Vorschriften, die auf illegale Inhalte abzielen, und im letzten Abschnitt andere Arten von Vorschriften gegen schädliche Inhalte näher betrachtet werden.

[750] Richtlinie (EU) 2024/1385 des Europäischen Parlaments und des Rates vom 14. Mai 2024 zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt [2024] ABl. L, 2024/1385.

7.1 Durchsetzung von Vorschriften zur Bekämpfung von Desinformation

Desinformation in der EU stellte ein ernsthaftes Problem im Zusammenhang mit weitreichenden Themen dar, darunter die Verbreitung von Informationen über Gesundheitsfragen, Verschwörungstheorien und (politische) Einflussnahme aus dem Ausland. Sie wird nunmehr als systemisches Risiko im Online-Umfeld durch eine Kombination freiwilliger und gesetzlicher Rahmenbedingungen bekämpft, wobei der Schwerpunkt insbesondere auf sogenannten FIMI-Kampagnen und der Wahlbeeinflussung liegt. Daher hat die EU schrittweise von weichen Maßnahmen wie dem *Code of Practice on Disinformation* (freiwilliger Verhaltenskodex zur Bekämpfung von Desinformation) von 2018 auf verbindliche Verpflichtungen im Rahmen des DSA umgestellt und damit ihre Reaktion auf Desinformation durch eine Mischung aus Selbstregulierung, gesteigerter Koordinierung und verbesserter Risikoerkennung gestärkt. Dieser Ansatz wird weiter durch die TTPW-VO und den EMFA unterstützt, die sich mit Themen wie aus dem Ausland finanzierter politischer Werbung und unseriösen Mediendiensteanbietern befassen. In Anerkennung der entscheidenden Rolle sehr großer Online-Plattformen und Suchmaschinen (VLOPSE) für den Zugang zu Informationen gehen Selbstregulierungsverpflichtungen daher mit erhöhten Sorgfaltspflichten für Anbieter von VLOPSE einher. Um Desinformation mit Durchsetzungsmaßnahmen entgegenzuwirken, stützt sich der DSA auf ein hybrides Durchsetzungssystem, bei dem die Europäische Kommission und die EU-Mitgliedsstaaten als Koregulierungsbehörden fungieren und die Rolle der Vermittler selbst ergänzen. Die zuständigen nationalen Behörden sind für die Überwachung und Durchsetzung des DSA in Bereichen zuständig, die nicht ausdrücklich an andere benannte Behörden delegiert wurden, was bedeutet, dass die nationalen Behörden Vorschriften in Bezug auf Anbieter von Vermittlungsdiensten, die in ihrem Hoheitsgebiet niedergelassen sind, durchsetzen. Die Europäische Kommission ist in erster Linie für die Überwachung und Durchsetzung in Bezug auf VLOPSE zuständig. Dieser zweistufige Durchsetzungsansatz wird am Beispiel von TikTok veranschaulicht, das im rumänischen Länderbericht analysiert wird.

Rumänien, wo Plattformen wie Facebook, WhatsApp, YouTube und TikTok als Informationsquellen weit verbreitet sind – eine Entwicklung, die mit jener in anderen Mitgliedsstaaten vergleichbar ist – ist in Kombination mit einer geringen digitalen Kompetenz ein Umfeld, das besonders anfällig für Desinformation ist. So hat sich gezeigt, dass die Bevölkerung des Landes sehr empfänglich für Desinformationskampagnen war, die sich auf die öffentliche Meinung und demokratische Prozesse auswirkten. Dieses Risiko wurde vor der Präsidentschaftswahl 2024 deutlich, zu einem Zeitpunkt, als der DSA bereits vollständig anwendbar war. Das Beispiel Rumäniens lässt die Grenzen des DSA erkennen, der sich mehr auf die Einführung von Mechanismen als auf ein endgültiges Regelwerk konzentriert, um das systemische Risiko von Desinformation und Wahlbeeinflussung zu bekämpfen und zu mindern. Diese Lücke wurde nun teilweise durch den *Strengthened Code of Practice on Disinformation* (Verstärkter Verhaltenskodex zur Bekämpfung von Desinformation) geschlossen, der ursprünglich freiwillig war, aber nun als *Code of Conduct on Disinformation* (verbindlicherer Verhaltenskodex zur Bekämpfung von Desinformation) in den Rahmen des DSA integriert wurde. Durch seine Integration in den DSA-Rahmen im

Februar 2025 wird der Kodex als Leitfaden für VLOPSE dienen, um die Einhaltung ihrer Verpflichtungen in Bezug auf Systemrisiken zu erreichen.

Unabhängig vom nationalen Wahlprozess in Rumänien hatte die Europäische Kommission bereits ein DSA-Durchsetzungsverfahren eingeleitet. Im Zusammenhang mit den rumänischen Wahlen erließ die Kommission daraufhin gegenüber TikTok eine Aufbewahrungsanordnung zum Einfrieren und Speichern von Daten im Hinblick auf tatsächliche und vorhersehbare systemische Risiken, die sein Dienst für Wahlprozesse und den gesellschaftlichen Diskurs in der EU bergen könnte. Die vorläufigen Untersuchungsergebnisse der Europäischen Kommission bestätigten, dass TikTok gegen mehrere Sorgfaltspflichten gemäß dem DSA verstoßen hat, darunter hinsichtlich der Art und Weise der Zielgruppenansprache und der Nutzung von Sponsoring für politische Werbung.[751] Derartige Fragen könnten nunmehr auch im Rahmen der TTPW-VO behandelt werden, was bedeutet, dass eine nationale Reaktion auf die Gefährdung der Integrität des Wahlprozesses, wie sie Rumänien in Form der nationalen Dringlichkeitsverordnung Nr. 1/2025 unternommen hat, unnötig wäre. Sich auf einen allgemeinen Rechtsrahmen stützen zu können, würde auch für mehr Transparenz sorgen als eine Notfallmaßnahme der Exekutive.

Parallel zu diesen Verfahren auf EU- und nationaler Ebene wurden politische Maßnahmen zur Vorbereitung der Wahlen verabschiedet, die wiederholt wurden, nachdem sie aufgrund von Einflussnahme von außen annulliert worden waren. Diese politischen Maßnahmen wurden von den verstärkten Kooperationsmechanismen, die durch die verschiedenen Teile des neuen EU-Rechtsrahmens für den digitalen Bereich eingeführt wurden, günstig beeinflusst. So zielte beispielsweise ein Runder Tisch mit VLOPSE, dem rumänischen Koordinator für digitale Dienste (ANCOM), zuständigen Behörden und Organisationen der Zivilgesellschaft darauf ab, Informationen zu erheben und die Vorbereitung auf die anstehenden Wahlen in Rumänien sicherzustellen.[752] Angesichts der Dauer des formellen Verfahrens der Europäischen Kommission war es verständlich, dass der nationale Gesetzgeber die wahrgenommenen Mängel durch innerstaatliche Maßnahmen beheben wollte. In Anbetracht der Entscheidung des EuGH[753] zum österreichischen Kommunikationsplattformen-Gesetz, das wegen Missachtung des Herkunftslandprinzips gemäß der EC-RL außer Kraft gesetzt wurde, bleibt jedoch unklar, ob ein Gesetz wie das in Rumänien vorgeschlagene (aber noch nicht endgültig verabschiedete) als mit einschlägigem EU-Sekundärrecht vereinbar angesehen werden würde. Der rumänische Vorschlag verlangt unter anderem, dass Plattformen die Verbreitung potenziell schädlicher Inhalte auf höchstens 150 Nutzende beschränken und illegale

[751] Europäische Kommission, „Vorläufige Feststellung der Kommission: TikTok-Werbearchiv verstößt gegen das Gesetz über digitale Dienste“, Pressemitteilung, 15. Mai 2025. Siehe jedoch auch die Ankündigung der Europäischen Kommission, die Zusagen von TikTok hinsichtlich der festgestellten Werbeprobleme zu akzeptieren und diesen Teil der Untersuchung abzuschließen, „Kommission akzeptiert Verpflichtungszusagen von TikTok zur Transparenz der Werbung im Rahmen des Gesetzes über digitale Dienste“, Pressemitteilung, 5. Dezember 2025.

[752] Europäische Kommission, „Kommission, Online-Plattformen und Zivilgesellschaft verstärken Überwachung während Wahlen in Rumänien“, Pressemitteilung, 5. Dezember 2024.

[753] Gerichtshof der Europäischen Union, C-376/22 Google Ireland Ltd. und andere gegen Kommunikationsbehörde Austria (KommAustria) [2023] ECLI:EU:C:2023:835.

Inhalte innerhalb von 15 Minuten nach Veröffentlichung auf der Grundlage einer automatisierten Klassifizierung entfernen müssen.

Das Beispiel Frankreichs zeigt in diesem Zusammenhang, wie nationale Regulierungs- und Politikmaßnahmen das Ziel der gemeinsamen Bekämpfung von Desinformation unterstützen können. Im Gegensatz zum rumänischen Gesetzentwurf greift der französische Ansatz nicht in die harmonisierte EU-Plattformregulierung ein, sondern legt den nationalen Fokus auf die Bekämpfung von Desinformation mittels eines Rechtsrahmens zur algorithmischen Identifizierung diesbezüglichen Materials und unterstützt damit indirekt die DSA-Vorschriften mit einer Durchsetzungskomponente. Ein wichtiges Mittel zur Erreichung des Ziels ist die begleitende Arbeit des speziellen Gremiums VIGINUM, das FIMI überwacht, erkennt und analysiert und insbesondere die angewandten Techniken und die beteiligten Bedrohungsakteure identifiziert und charakterisiert, um Vorsorgemaßnahmen und das öffentliche Bewusstsein zu stärken. In Ermangelung eines formellen Mandats zur Durchsetzung von Vorschriften gegen falsche Informationen bleibt die Rolle von VIGINUM unterstützend. Der französische Fokus auf Bewusstseinsbildung spiegelt sich auch in weiteren Maßnahmen wie der Verbesserung der Informationskompetenz auf Schulebene wider. Frankreich hat besonderes Augenmerk darauf gelegt, Antworten auf FIMI-Risiken zu finden, die sich nicht nur in den Aufgaben von VIGINUM zeigen, sondern auch im Léotard-Gesetz, das unter anderem die französische Aufsichtsbehörde für audiovisuelle und digitale Kommunikation, ARCOM, damit beauftragt, gegen audiovisuelle Kommunikationsdienste vorzugehen, die von einem ausländischen Staat kontrolliert oder beeinflusst werden und absichtlich falsche Informationen verbreiten, insbesondere in den drei Monaten vor einer Wahl.

Da der übergeordnete Rahmen in Frankreich und Rumänien sowie allen anderen EU-Mitgliedsstaaten aufgrund bestehender EU-Verordnungen größtenteils harmonisiert ist, ist der Vergleich mit einem Land interessant, das nicht Mitglied der EU oder des EWR, aber Vertragspartei der EMRK ist. In diesem Zusammenhang ist die Ukraine ein besonders anschauliches Beispiel, da sie seit mehr als einem Jahrzehnt massiven FIMI-Kampagnen eines feindlichen Akteurs ausgesetzt ist. Die ukrainische Gesetzgebung regelt keine Online-Plattformen, sondern lediglich Video-Sharing-Plattformen (VSP), die ihrer Rechtshoheit unterliegen, durch das ukrainische Mediengesetz. Für Plattformen im Allgemeinen sind bisher nur weiche Rechtsansätze wie Memoranden oder Kooperationsvereinbarungen vorgesehen. Diese Regulierungslücke wird angesichts der groß angelegten Informationsangriffe Russlands und der wachsenden Abhängigkeit der Bevölkerung von Sozialen Medien als Nachrichtenquelle, die gleichzeitig für die Verbreitung von Desinformation genutzt werden, als besorgniserregend empfunden. Mit der Einführung des Kriegsrechts im Jahr 2022, das auch Beschränkungen der Meinungsäußerungsfreiheit erleichtert, wurden jedoch vorübergehende Sperrungen von audiovisuellen Mediendiensten auf Abruf und von Diensten von Anbietern audiovisueller Dienste des Aggressorstaates auf dem Hoheitsgebiet der Ukraine möglich. Darüber hinaus sind VSP verpflichtet, vorübergehende Verbote für die Verbreitung von Desinformation im Zusammenhang mit der bewaffneten Aggression gegen die Ukraine vorzunehmen.

Da dem Staat keine wirksamen Mechanismen zur Einflussnahme auf ausländische Online-Plattformen zur Verfügung stehen, um seine nationalen Interessen zu schützen, wurden Websites und Online-Plattformen auf der Grundlage des ukrainischen

Sanktionsgesetzes und als Folge der groß angelegten russischen Invasion in der Ukraine auch aufgrund spezifischer Anordnungen des Nationalen Zentrums für operationelles und technisches Management von Telekommunikationsnetzen gesperrt. In Ermangelung eines einschlägigen Rahmens für die Bedingungen dieser Sperrmaßnahmen bleiben diese umstritten. Die Sperrung solcher Dienste ist auch unter Kriegsrecht möglich. Diese Maßnahmen sind jedoch untrennbar mit dem Schutz nationaler Interessen verbunden und müssen daher angesichts des Fehlens eines allgemeineren Regulierungsrahmens für Online-Plattformen als Ultima Ratio gelten. Ähnlich wie Frankreich setzt die Ukraine auch auf präventive Kontrolle, indem sie versucht, die Medienkompetenz zu stärken und Sensibilisierungskampagnen durchzuführen, unter anderem im Hinblick auf die Erkennung von Desinformation und insbesondere von FIMI.

7.2 Durchsetzung von Vorschriften zur Bekämpfung terroristischer Inhalte

Als Reaktion auf terroristische Online-Inhalte setzt die EU auf eine Kombination aus verbindlicher Regulierung und freiwilliger Zusammenarbeit der Vermittler, wobei sowohl plattformspezifische Pflichten eingeführt als auch solche Inhalte bekämpft werden.

Die AVMD-RL verpflichtet die EU-Mitgliedsstaaten, mit angemessenen Mitteln dafür zu sorgen, dass die von den ihrer Rechtshoheit unterworfenen AVMD- und VSP-Anbietern bereitgestellten Dienste keine Inhalte enthalten, die eine öffentliche Aufforderung zur Begehung terroristischer Straftaten darstellen.[754] Im Juni 2022 wurde mit der Verordnung über terroristische Online-Inhalte (TCO-VO) ein breiter anwendbarer Satz harmonisierter Vorschriften eingeführt, die für alle Hostingdiensteanbieter gelten, die Dienste in der EU anbieten. Neben einer einheitlichen Definition terroristischer Inhalte wurden Entfernungsanordnungen eingeführt, die Anbieter verpflichten, terroristische Inhalte binnen einer Stunde zu entfernen, sowie freiwillige Aufforderungen zur Entfernung; die Verordnung enthält insbesondere auch Verfahrensregeln in beiden Bereichen. Ein Schwerpunkt liegt auf der grenzüberschreitenden Zusammenarbeit und Koordinierung zwischen den Mitgliedsstaaten und beispielsweise auch Europol. Darüber hinaus sind terroristische Inhalte nach dem DSA ein systemisches Risiko, was bedeutet, dass VLOPSE eine präventive Risikobewertung in Bezug auf solche Inhalte durchführen müssen. Diese präskriptive Verordnung wird durch freiwillige Zusammenarbeit und koordinierte Reaktionsmechanismen ergänzt.

Wie der TCO-VO-Rahmen in der Praxis funktioniert, zeigen die Erkenntnisse aus Deutschland als dem Mitgliedsstaat, in dem die Behörden nach dem Terroranschlag der Hamas auf Israel besonders aktiv Schritte zur Entfernung von Inhalten im Rahmen der Verordnung ergriffen haben. Tatsächlich hat sich Deutschland bei der Durchsetzung der TCO-VO als der proaktivste EU-Mitgliedsstaat erwiesen und in diesem Zusammenhang auch die meisten Fälle im Rahmen des DSA zur weiteren Untersuchung an die Europäische Kommission verwiesen. Der deutsche Durchsetzungsansatz in Bezug auf die TCO-VO konnte

[754] Artikel 6 der AVMD-RL.

auf der bereits bestehenden institutionellen Infrastruktur und den Erfahrungen mit einer zentralen Meldestelle auf der Grundlage früherer nationaler Rechtsvorschriften zur Entfernung illegaler Inhalte aufbauen, die inzwischen größtenteils durch die harmonisierten Bestimmungen ersetzt wurden. Die Anwendung der TCO-VO in Deutschland hat gezeigt, dass mehr als 95 % der Entfernungsanordnungen erfüllt wurden. Anstatt sich auf formelle Entfernungsanordnungen zu konzentrieren, verlässt sich Deutschland stark auf Meldungen, die mit einem Antrag auf freiwillige Entfernung einhergehen, bevor Entfernungsanordnungen erlassen werden. Das BKA fungiert als zentrale Behörde gemäß der TCO-VO und ist auch gemäß Artikel 18 DSA für die Entgegennahme von Meldungen strafbarer Inhalte zuständig. Die strikte Durchsetzung der TCO-VO spiegelt auch die historische Sensibilität für Terrorismus und Antisemitismus und letztendlich die fortgeschrittene rechtliche und institutionelle Bereitschaft dieses Mitgliedsstaats aufgrund seiner früheren Gesetzgebung und institutionellen Strukturen wider, die auf dieser Grundlage eingeführt wurden.

Eine ebenso entschiedene Haltung gegen terroristische Inhalte im Netz nimmt der Nicht-EU-Mitgliedsstaat Türkiye ein. Doch abgesehen davon, dass das türkische Internetgesetz die Entfernung illegaler Inhalte durch den Hostingdiensteanbieter vorschreibt, wenn Inhalte nicht freiwillig entfernt werden, bestand die langjährige Praxis der türkischen Verwaltungsbehörden darin, den Zugang zu ganzen Websites zu sperren, was zu ernsthaften Bedenken hinsichtlich der Meinungsäußerungs- und Medienfreiheit geführt hat, wie auch die Urteile des EGMR in einschlägigen Fällen aus Türkiye zeigen. Die Wirksamkeit dieses Ansatzes ist ebenfalls fraglich, da Inhalte außerhalb des durch die Einschränkung abgedeckten Gebiets weiterhin verfügbar sind. Dementsprechend zielt der neue türkische Regulierungsansatz darauf ab, rechtswidrige Inhalte an ihrer Quelle zu entfernen, anstatt lediglich den Zugang zu beschränken. Für terroristische Inhalte gilt ein kurzer Zeitrahmen von vier Stunden für die Entfernung. Social-Media-Plattformen müssen lokale Vertreter ernennen, auf Nutzeranfragen reagieren, Transparenzberichte veröffentlichen, Daten lokalisieren und Minderjährige auf ähnliche Weise schützen wie das Regulierungssystem des DSA. Um die Einhaltung durchzusetzen, hat Türkiye Sanktionen eingeführt, darunter Geldbußen, Werbeverbote, Bandbreitenbeschränkung und gemeinsame Haftung für illegale Inhalte. In der Praxis scheint es, dass Zugangssperren, insbesondere in Zeiten von Protestbewegungen, aus verschiedenen Gründen immer noch stark genutzt werden.[755]

7.3 Durchsetzung von Vorschriften gegen diffamierende, hetzerische und zu Gewalt aufstachelnde Äußerungen

Der Ansatz der EU zur Regulierung diffamierender, hetzerischer und zu Gewalt aufstachelnder Äußerungen im Netz hat sich als Reaktion auf die Zunahme solcher Äußerungen, insbesondere in digitalen Räumen, weiterentwickelt. Während der Rahmenbeschluss des Rates zur Bekämpfung von Rassismus und Fremdenfeindlichkeit von 2008 eine grundlegende Definition illegaler Hassrede enthält, weiten die

[755] Siehe z. B. Schräer, F., „Access to Various Internet Platforms in Turkey Restricted“, heise.de, 20. März 2025.

Mitgliedsstaaten oftmals den Schutz vor Hass auf andere Gründe als die in der Definition des Rahmenbeschlusses enthaltenen aus, z. B. auf Geschlecht oder Behinderung.

Wie zuvor erwähnt, hat der DSA mehrschichtige Verantwortlichkeiten für Online-Plattformen mit einer Reihe von Verpflichtungen speziell für VLOPSE eingeführt. Der Verhaltenskodex für die Bekämpfung illegaler Hassreden im Internet, der 2025 überarbeitet und als Verhaltenskodex+ veröffentlicht wurde, wurde in den Koregulierungsrahmen des DSA integriert. Er unterstützt die schnellere Entfernung illegaler Hassrede und gleicht die Plattformmoderation an. Die EU hat damit begonnen, diese Vorschriften gegen VLOPSE durchzusetzen, die unter die Zuständigkeit der Kommission fallen. Insbesondere hat die Kommission Maßnahmen gegen X (vormals Twitter) ergriffen und auf unzureichende Risikominderungs- und Moderationspraktiken verwiesen. Die Europäische Kommission berief sich auf Untersuchungsbefugnisse im Rahmen des DSA und überwacht weiterhin die Einhaltung.[756]

Es bestehen weiterhin offene Fragen, insbesondere bei Inhalten wie Diffamierung, bei denen die Rechtmäßigkeit in hohem Maße vom Kontext und nationalen Normen abhängt. Wie die Länderbeispiele zeigen, gibt es einige Unterschiede in Bezug auf die nationalen straf- und zivilrechtlichen Vorschriften, die für diffamierende, hetzerische oder zu Gewalt aufstachelnde Äußerungen gelten, obwohl diese Vorschriften denselben europäischen und internationalen Menschenrechtsnormen unterliegen. Im Vergleich zu Irland beispielsweise hat Italien eine klarere strafrechtliche Haftung für diffamierende oder hetzerische Inhalte eingeführt, die über öffentliche Kommunikationsmittel verbreitet werden. Das Beispiel Irland wiederum beweist, dass Gesetze, die sich in der Offline-Welt bewährt haben, möglicherweise nicht mit der gleichen Wirksamkeit auf Äußerungen im Netz angewendet werden können.

In Bezug auf Haftungsfragen hält der DSA am Grundsatz der EC-RL fest, dass Vermittlern keine allgemeinen Überwachungspflichten obliegen, lässt jedoch Verfügungen zu, die Plattformen verpflichten können, das erneute Hochladen illegaler Inhalte zu verhindern, die denen ähneln, die bereits zuvor als illegal eingestuft wurden („Staydown"-Verpflichtung), sofern die Prüfung einer solchen Verfügung keine unabhängige rechtliche Prüfung durch die betroffenen Anbieter erfordert.

Eine verstärkte EU-Harmonisierung in Form einer unmittelbar anwendbaren Verordnung (DSA) anstelle einer Richtlinie (EC-RL), die nur hinsichtlich des Ziels verbindlich ist, aber eine nationale Umsetzung erfordert, bedeutet, dass es in den EU-Ländern, die als Beispiele in dieser Veröffentlichung enthalten sind, einen übergeordneten, einheitlichen Plattformregulierungsrahmen gibt. Wie die Beispiele zeigen, beruht die tatsächliche Durchsetzung jedoch auf nationalen Mechanismen. Im Vergleich zu Irland verfügt Italien in der Praxis über ein fortgeschritteneres Durchsetzungssystem mit starken Verwaltungsbefugnissen, die der nationalen Aufsichtsbehörde für das Kommunikationswesen, AGCOM, übertragen wurden, die auch die Koordinatorin für digitale Dienste gemäß dem DSA ist. Das italienische System – das EU-weit geltende Vorschriften (DSA, AVMD-RL), nationale Instrumente (TUSMA, Mancino-Gesetz), die

[756] Siehe auch die erste DSA-basierte Sanktionsentscheidung zu einem Teil der Ermittlungen gegen X, der nicht die hier diskutierten Elemente betrifft. Europäische Kommission, „Gesetz über digitale Dienste: Kommission verhängt Geldbuße in Höhe von 120 Mio. EUR gegen X", Pressemitteilung, 5. Dezember 2025.

Verwaltungsrolle der AGCOM und gerichtliche Rechtsbehelfe kombiniert – bildet eine mehrschichtige Durchsetzungsstruktur. Im Gegensatz dazu basierte ein Großteil der Plattformhaftung in Irland früher auf der zivilrechtlichen Haftung und der Meldepflicht, wobei es in der Vergangenheit (vor Einführung des DSA) nur wenige Vorschriften gab, die speziell auf die Verpflichtungen von Plattformen in Bezug auf Hassrede und Diffamierung abzielten. Es scheint, dass die verzögerte Umsetzung von Teilen der überarbeiteten AVMD-RL und die erst im März 2023 erfolgte Einrichtung der neuen irischen Aufsichtsbehörde CnAM dazu geführt haben, dass infolge dieser Verzögerung bisher nur begrenzte Durchsetzungsmaßnahmen ergriffen wurden, obwohl die CnAM auch für die Durchsetzung des DSA auf nationaler Ebene zuständig ist und die Regulierungsbehörde für Online-Sicherheit ist. Angesichts der ausschließlichen Befugnisse der Europäischen Kommission zur Überwachung systemischer Risiken von VLOPSE und der jüngsten diesbezüglichen Maßnahmen der Kommission sind jedoch verstärkte Aktivitäten von CnAM zu beobachten und künftig zu erwarten, unter anderem bei der Unterstützung der Arbeit der Europäischen Kommission durch die Erhebung und den Austausch von Informationen über die zahlreichen in Irland ansässigen VLOPSE.

Während verstärkte Durchsetzungsmaßnahmen sicherstellen, dass Vorschriften und Verpflichtungen wirksam angewendet und umgesetzt werden, hat das Beispiel Österreichs einen weiteren Aspekt der Bekämpfung von Hass im Netz deutlich gemacht: Es hat gezeigt, dass angesichts der vollständigen Harmonisierung der Haftungsvorschriften für Vermittlungsdienste auf EU-Ebene der Spielraum für die Regulierung illegaler Online-Inhalte weitgehend auf das materielle Recht beschränkt ist. Die neue österreichische Gesetzgebung zu Hass im Netz wurde als Reaktion auf aufkommende Formen von Online-Hass eingeführt, um die spezifischen Merkmale der Kommunikation im Cyberspace besser widerzuspiegeln. Änderungen des bestehenden innerstaatlichen Rahmens zur Bekämpfung diffamierender, hetzerischer und zu Gewalt aufstachelnder Äußerungen betreffen auch das Verfahrensrecht und erleichtern und unterstützen dadurch die private Rechtsdurchsetzung.

7.4 Durchsetzung von Vorschriften, die auf andere Bereiche schädlicher Inhalte abzielen

Nach Erörterung der Entfernung illegaler Inhalte liegt der letzte Schwerpunkt dieses IRIS-Berichts auf anderen schädlichen, aber rechtmäßigen Inhalten. Dazu gehört insbesondere für Kinder ungeeignetes Material, das die Entwicklung Minderjähriger beeinträchtigen kann, etwa Pornografie. In der EU müssen die Mitgliedsstaaten gemäß AVMD-RL, die sowohl für den traditionellen Rundfunk als auch für Abrufdienste sowie in Teilen – einschließlich der Verpflichtung zum Schutz Minderjähriger – für VSP-Anbieter gilt, sicherstellen, dass derartige Inhalte durch Instrumente wie Altersverifikations- und Klassifizierungssysteme, die von den Anbietern angewendet werden, für Minderjährige unzugänglich sind. Der DSA ergänzt dies, indem er Online-Plattformen horizontale Verpflichtungen auferlegt, denen zufolge sie geeignete und verhältnismäßige Maßnahmen zum Schutz Minderjähriger ergreifen müssen, einschließlich Datenschutz- und Sicherheitsstandards durch Technikgestaltung. Im Juli 2025 hat die Europäische Kommission Leitlinien gemäß Artikel 28 DSA herausgegeben, in denen Maßnahmen wie

Instrumente zur Sicherstellung des Alters empfohlen werden und der Schwerpunkt auf Verhältnismäßigkeit, Kinderrechten und minimaler Offenlegung von Daten liegt – die möglicherweise durch die Verwendung der kommenden EU-Brieftasche für die Digitale Identität realisiert werden können. Die Durchsetzung hat in diesem Zusammenhang bereits begonnen, da die Kommission 2025 Verfahren wegen unzureichender Altersverifikation gegen große Pornografieplattformen eingeleitet hat, während die nationalen Behörden parallele Maßnahmen mithilfe des Europäischen Gremiums für digitale Dienste (EGDD) koordinierten, um eine Angleichung der Durchsetzungsmaßnahmen gegen solche Inhalte sicherzustellen.

Das Beispiel Polens zeigt, dass einige Mitgliedsstaaten mit der innerstaatlichen Umsetzung des DSA Schwierigkeiten haben[757] und daher keine nationalen Durchsetzungsverfahren vorsehen. Im September 2025 verabschiedete die polnische Regierung schließlich das nationale Durchführungsgesetz, das den bestehenden Rechtsrahmen erheblich verändern wird. Als EU-Mitgliedsstaat folgt Polen dem zuvor beschriebenen dezentralen Durchsetzungsmodell des DSA und der AVMD-RL, bei dem der Europäischen Kommission in Bezug auf VLOPSE besondere Zuständigkeiten übertragen werden. Während der Gesetzentwurf zur Umsetzung des DSA die Verfahren für die Entfernung illegaler Inhalte detailliert beschreibt, befasst er sich über die unmittelbar anwendbaren Vorschriften des DSA hinaus nicht speziell mit legalen, aber schädlichen Inhalten. Einschlägige Vorschriften zu schädlichen Inhalten finden sich indes in Sondergesetzen, die sich beispielsweise auf Online-Glücksspiele oder VSP beziehen. In der Praxis verhindert die Beschränkung des Zugangs zu beispielsweise Pornografie auf VSP die Zugriffsmöglichkeit für Minderjährige nicht, wenn solche Inhalte an anderer Stelle leicht online abgerufen werden können. Der polnische Gesetzgeber versucht, durch die Einführung eines neuen Gesetzes zum Schutz Minderjähriger vor dem Zugang zu schädlichen Inhalten im Netz diese Regulierungslücke zu schließen. Der Gesetzentwurf konzentriert sich in erster Linie auf die Verhinderung des Zugangs Minderjähriger zu Pornografie, indem Online-Dienste verpflichtet werden, wirksame Maßnahmen zur Altersverifikation umzusetzen, die mit denen vergleichbar sind, die für VSP im Rahmen der nationalen Umsetzung der AVMD-RL verpflichtend sind.

Ähnlich wie bei der bestehenden Online-Glücksspiel-Verordnung werden die Vorschriften zu Zugangsbeschränkungen von einem detaillierten Durchsetzungssystem begleitet. In beiden Fällen wendet Polen ein registergestütztes Durchsetzungsmodell an, das behördliche Festlegungen (Auflistung nicht konformer Websites) mit technischen Verpflichtungen für Vermittler kombiniert. Dementsprechend ist die Durchsetzung nicht unmittelbar auf die nicht konformen Dienste ausgerichtet, die in der Regel außerhalb der territorialen Zuständigkeit Polens lokalisiert sind. Der Rahmen für Glücksspiele sieht mit der Sperrung von Zahlungen an nicht konforme Dienste eine zusätzliche finanzielle Durchsetzungsdimension vor, während sich der Gesetzentwurf zum Schutz Minderjähriger vor dem Zugang zu schädlichen Online-Inhalten ausschließlich auf die Kontrolle des

[757] Im Mai 2025 beschloss die Europäische Kommission, Klage gegen mehrere Mitgliedsstaaten, darunter Polen, beim GHdEU einzureichen, da sie keinen nationalen Koordinator gemäß dem DSA benannt und/oder diesem nicht die entsprechenden Befugnisse erteilt hatten, siehe Europäische Kommission, „Commission Decides to Refer Czechia, Spain, Cyprus, Poland and Portugal to the Court of Justice of the European Union due to lack of effective implementation of the Digital Services Act“, Pressemitteilung, 7. Mai 2025.

Zugangs zu Inhalten konzentriert. Diese Unterscheidung spiegelt die unterschiedlichen wirtschaftlichen Strukturen und regulatorischen Ziele der beiden Systeme wider. Online-Glücksspiel-Dienste erzielen ihre Einnahmen aus direkten Nutzerzahlungen, daher ist das Verbot von Zahlungsdiensten ein wirksames Durchsetzungsinstrument, das die Einkommensströme des Betreibers unterbricht und die Konsumierenden vor finanziellen Verlusten schützt. Darüber hinaus verhindert das Durchsetzungsmodell einen Geldverkehr zwischen minderjährigen Nutzern und Betreibern. Die meisten Pornografie-Websites betreiben hingegen ein auf Werbung oder der Zahl der Aufrufe beruhendes Monetarisierungsmodell, das Nutzern freien Zugang bietet und Einnahmen von Drittinserenten oder Affiliate-Netzwerken erzielt. Der Gesetzentwurf spiegelt die begrenzte praktische Wirkung von Zahlungssperren in dieser Konstellation wider und konzentriert sich daher auf die Zugangsverhinderung als gezieltere und verhältnismäßigere Maßnahme, die mit dem Schutzziel vereinbar ist.

Im Gegensatz zur Regulierung schädlicher Inhalte in der EU, welche in verschiedenen spezifischen Rechtsakten geregelt ist, strebt das Vereinigte Königreich eine allumfassende Gesetzgebung an. Nach dem Brexit hat das Vereinigte Königreich das Online-Sicherheits-Gesetz (Online Safety Act - OSA) als innerstaatliches britisches Gesetz verabschiedet, das ein substanzielles nationales Regelwerk festlegt, welches sowohl für illegale als auch schädliche Online-Inhalte gilt. Der OSA geht sowohl im Geltungsbereich als auch in der Tiefe der Regulierung deutlich über den DSA hinaus und schafft neue rechtliche Pflichten für Plattformen. Die Durchsetzung im Rahmen des OSA erfolgt zentralisiert durch eine einzige nationale Behörde, und zwar durch das Ofcom, die britische Medienaufsichtsbehörde, die über umfassende Ermittlungs-, Aufsichts- und Sanktionsbefugnisse verfügt, einschließlich Geldbußen von bis zu 10 % des weltweiten Umsatzes oder Sperrungen von Diensten.

Gemäß dem OSA obliegen Plattformen proaktive Sorgfaltspflichten, denen zufolge sie illegale und für Minderjährige schädliche Inhalte identifizieren, entfernen und verhindern müssen. Tatsächlich wird die Haftung in viel stärkerem Maße auf die Plattformen verlagert als unter dem DSA. Zusammenfassend führt der DSA unter anderem die Bewertung systemischer Risiken, Transparenzberichtspflichten sowie Melde- und Abhilfeverfahren ein, indes beispielsweise Artikel 28 DSA von Plattformen, die für Minderjährige zugänglich sind, lediglich verlangt, dass sie geeignete und verhältnismäßige Maßnahmen zu deren Schutz ergreifen, dabei jedoch risikobasiert und flexibel verfahren. Die Kinderschutzbestimmungen des OSA schreiben dagegen strenge Maßnahmen zur Sicherstellung des Alters, Sicherheit durch Technikgestaltung in den Systemen und regelmäßige Risikobewertungen vor, die sich auf Bereiche wie Online-Glücksspiele und Computerspiel-Lootboxen erstrecken. Die Durchsetzung hat bereits zu regulatorischen Maßnahmen und rechtlichen Anfechtungen geführt – wie etwa der gerichtlichen Beschwerde von Wikipedia gegen das Ofcom –, wodurch die Spannungen zwischen Online-Sicherheit, Datenschutz und Freiheit der Meinungsäußerung deutlich werden, während das Regelwerk auf die vollständige Umsetzung im Jahr 2026 zusteuert.

8. Schlussfolgerungen und Ausblick

Dr Mark D. Cole, Wissenschaftlicher Direktor, Institut für Europäisches Medienrecht (EMR), und Professor für Medien- und Telekommunikationsrecht, Universität Luxemburg

Das digitale Umfeld hat sowohl die Reichweite von Äußerungen als auch den Umfang der Verantwortung im Zusammenhang mit geäußerten und verbreiteten Informationen neu definiert. Wie dieser IRIS-Bericht zeigt, vergrößert dieselbe Online-Infrastruktur, die beispiellose Partizipation und Pluralität im öffentlichen Diskurs ermöglicht, auch die Risiken, die von illegalen Inhalten und Desinformation für die Rechte der Einzelperson, den sozialen Zusammenhalt und die demokratische Resilienz ausgehen. Gleichzeitig wird das Online-Umfeld von einer kleinen Anzahl mächtiger Plattformen dominiert. Die rechtlichen Rahmenbedingungen auf internationaler, insbesondere aber auf europäischer und nationaler Ebene haben sich schrittweise weiterentwickelt, um diesen Risiken zu begegnen, doch die Durchsetzung bleibt teilweise fragmentiert und uneinheitlich, was die Unterschiede in den nationalen Traditionen, Regulierungskapazitäten und politischen Prioritäten widerspiegelt. Der DSA sowie der OSA im Vereinigten Königreich und andere neu entwickelte Instrumente deuten auf eine Verlagerung zu einer systematischeren, risikobasierten und proaktiven Regulierung von Online-Vermittlern hin, offenbaren aber auch die anhaltenden Spannungen bei Durchsetzungsmaßnahmen zwischen dem Schutz der Meinungsäußerungsfreiheit und der Gewährleistung der Sicherheit und Rechenschaftspflicht im Netz auf.

Eine wirksame Durchsetzung kann nicht durch rein nationale oder einseitige Maßnahmen erreicht werden. Der grenzenlose Charakter der Online-Kommunikation erfordert grenzüberschreitende Zusammenarbeit und Mechanismen, die die Kohärenz fördern und gleichzeitig die nationalen Rechtsordnungen und Grundrechtsgarantien achten. Er erfordert zudem mehr Transparenz und verfahrenstechnische Maßnahmen von Plattformen, denen zunehmend eine Kontrollfunktion im digitalen Bereich zukommt. Dementsprechend ist der rote Faden der Digitalgesetze, der sich in letzter Zeit gezeigt hat, ein Fokus auf Transparenz und einem risikobasierten Ansatz, um auf Risiken zu reagieren und sie zu mindern.[758] Die Durchsetzung entwickelt sich somit von Ad-hoc-Entfernungspraktiken zu einem kohärenten Regelungsmodell.

In allen in diesem Bericht untersuchten Themenbereichen lassen sich drei übergreifende Dynamiken identifizieren:

Erstens diversifizieren sich die Durchsetzungsmodelle als Reaktion auf die unterschiedlichen Rollen und Kapazitäten der Vermittler. Die ursprünglichen Grundsätze des Haftungsprivilegs und des Vermeidens einer allgemeinen Überwachung, die aus der Frühphase des Internets übernommen wurden, bleiben im Prinzip bestehen, koexistieren jedoch zunehmend mit granularen Pflichten für Plattformen, die eine systemische Rolle bei der Gestaltung der öffentlichen Kommunikation spielen. Dies wirft die Frage auf, ob der

[758] Siehe hierzu bereits Cappello, M. (Hrsg.), *Algorithmische Transparenz und Rechenschaftspflicht bei digitalen Diensten*, IRIS *Special*, Europäische Audiovisuelle Informationsstelle, Straßburg, 2023.

Ansatz des „sicheren Hafens“ für Vermittler weiter aufrechterhalten werden kann. Der risikobasierte Regulierungsansatz der EU, insbesondere im Rahmen des DSA, aber auch anderer rechtlicher Instrumente wie der TCO-VO, veranschaulicht eine Verlagerung von reaktiver, Meldungs- und Entfernungslogik hin zu vorausschauender Aufsicht. Nationale Beispiele zeigen, wie Mitgliedsstaaten gemeinsame Regeln durch (bisweilen) unterschiedliche institutionelle und verfahrensrechtliche Vorschriften umsetzen. Nicht-EU-Länder wie Türkiye und die Ukraine zeigen ebenfalls, dass innerstaatliche Durchsetzungsmodelle stark vom politischen Kontext, geopolitischen Realitäten und verfassungsrechtlichen Zwängen geprägt sind.

Zweitens werden die Grenzen bestehender Rahmenbedingungen im Zusammenhang mit Desinformation und anderen Formen schädlicher, aber rechtmäßiger Inhalte am deutlichsten sichtbar. Während Illegalität grundsätzlich definiert werden kann, bewegen sich schädliche Inhalte an der Schnittstelle von öffentlichem Interesse, demokratischer Sicherheit und Grundrechten. Für diese Kategorie ist der regulatorische Eingriff von Natur aus umstrittener und nur die Anwendung bestehender Ansätze wird in Zukunft zeigen, ob diesem Bereich ebenfalls ein strengeres regulatorisches Augenmerk zukommen wird oder nicht.

Drittens zeigen die nationalen Fallstudien die wachsende Bedeutung institutioneller Kapazitäten, grenzüberschreitender Zusammenarbeit und technischen Fachwissens auf. Rechtsvorschriften allein gewährleisten keine wirksame Durchsetzung. Vielmehr hängen die Ergebnisse davon ab, wie gut die Regulierungsbehörden aufgestellt sind, wie gut die Zusammenarbeit zwischen den Behörden funktioniert, ob technische Instrumente zugänglich sind und wie sehr sich die Plattformen selbst einbringen sowie inwieweit mit ihnen kooperiert werden kann. Die Beispiele Rumäniens und der Ukraine unterstreichen die strukturelle Verwundbarkeit von Staaten mit geringerer digitaler Kompetenz, stärkerer Exposition gegenüber FIMI oder begrenzten Einflussmöglichkeiten auf globale Plattformunternehmen. Umgekehrt zeigen die Erfahrungen Deutschlands und Frankreichs, wie etablierte Regulierungsinfrastrukturen für schnelle und koordinierte Reaktionen sorgen können – auch wenn sich diese Systeme ebenfalls kontinuierlich an neue Risiken und Technologien anpassen müssen.

Die als Beispiele ausgewählten Bereiche Desinformation sowie illegale und schädliche Inhalte machen deutlich, dass es keinen allgemeingültigen Ansatz gibt, sondern dass die Regulierung Maßnahmen erfordern kann, die in einem angemessenen Verhältnis zu den von den Inhalten ausgehenden Risiken stehen, ähnlich dem granularen Ansatz im DSA mit strengeren Vorschriften für VLOPSE und seinem allgemeinen risikobasierten Charakter, der auch in anderen Technologieregulierungen wie der KI-VO zu finden ist. In ähnlicher Weise erfordern einige unerwünschte Inhalte möglicherweise eine strengere Regulierung als andere illegale Inhalte, mit festgelegten Fristen und harmonisierten Verfahren, wie dies in der EU bei terroristischen Inhalten der Fall ist. Die erörterten Länderbeispiele für Desinformation haben gezeigt, dass die Bekämpfung von Desinformation mehr bedarf als straf- oder entfernungsbasierte Ansätze. Hierzu braucht es eine ganzheitlichere gesellschaftliche Reaktion, die die Stärkung der Medienkompetenz und zuverlässiger Medien umfasst und sicherstellt, dass algorithmische Designentscheidungen nicht ungewollt schädliche Narrative verstärken. Die Durchsetzung sollte daher nicht nur schädliches Verhalten unterbinden, sondern auch die strukturellen

Bedingungen stärken, die vertrauenswürdige, pluralistische und demokratische Informationsökosysteme aufrechterhalten.

Mit Blick auf die Zukunft muss der Schutz der Grundrechte im Netz – insbesondere der Meinungsäußerungsfreiheit, des Zugangs zu Informationen und des Rechts auf Teilnahme an der öffentlichen Debatte – der richtungsweisende Kompass für politisch Verantwortliche, Regulierungsbehörden und schließlich Plattformen bleiben. Gleichzeitig können die Pflichten der Staaten zur Gewährleistung einer Situation, in der der Meinungsbildungsprozess unabhängig, frei und sicher stattfinden kann, sowie das Bekenntnis der EU zu ihren Grundwerten weitere Regulierungsmaßnahmen erforderlich machen. Dennoch ist eine sorgfältige Prüfung solcher Vorschriften wichtig, um sicherzustellen, dass die Durchsetzung im Netz nicht zu einer voreiligen Einschränkung der Meinungsäußerung führt, sondern nur dort wirksam zum Einsatz kommt, wo dies zur Bekämpfung illegaler und unter bestimmten Bedingungen schädlicher Äußerungen notwendig ist. Dies wird durch den zunehmenden Einfluss der KI-gesteuerten Erstellung von „Inhalten“ auf den Kommunikationssektor noch verstärkt, einschließlich der Auswirkungen auf den Markt, die sich aus der Ablenkung der Aufmerksamkeit und der Umleitung von Finanzmitteln von den Quellen ergeben, die die Informationsinhalte ursprünglich erstellt haben. Ebenso wird der Einfluss der durch algorithmische Logik gesteuerten Verbreitung von Inhalten im Bereich der öffentlichen Meinungsbildung eine sorgfältige Beobachtung in Bezug darauf erfordern, ob die in diesem Bericht vorgestellten Durchsetzungsmaßnahmen in der Zukunft wirksam und ob weitere Anpassungen möglicherweise unvermeidbar sind.

Eine Publikation
der Europäischen Audiovisuellen Informationsstelle

Europäische
Audiovisuelle
Informationsstelle

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE