



Ausarbeitung

**„Chatkontrolle“ – Analyse des Verordnungsentwurfs 2022/0155 (COD)
der EU-Kommission**

„Chatkontrolle“ – Analyse des Verordnungsentwurfs 2022/0155 (COD) der EU-Kommission

Aktenzeichen: WD 10 – 3000 – 026/22
Abschluss der Arbeit: 07.10.2022 (letzter Abruf der Internetlinks)
Fachbereich: WD 10: Kultur, Medien und Sport

Die Wissenschaftlichen Dienste des Deutschen Bundestages unterstützen die Mitglieder des Deutschen Bundestages bei ihrer mandatsbezogenen Tätigkeit. Ihre Arbeiten geben nicht die Auffassung des Deutschen Bundestages, eines seiner Organe oder der Bundestagsverwaltung wieder. Vielmehr liegen sie in der fachlichen Verantwortung der Verfasserinnen und Verfasser sowie der Fachbereichsleitung. Arbeiten der Wissenschaftlichen Dienste geben nur den zum Zeitpunkt der Erstellung des Textes aktuellen Stand wieder und stellen eine individuelle Auftragsarbeit für einen Abgeordneten des Bundestages dar. Die Arbeiten können der Geheimschutzordnung des Bundestages unterliegende, geschützte oder andere nicht zur Veröffentlichung geeignete Informationen enthalten. Eine beabsichtigte Weitergabe oder Veröffentlichung ist vorab dem jeweiligen Fachbereich anzuzeigen und nur mit Angabe der Quelle zulässig. Der Fachbereich berät über die dabei zu berücksichtigenden Fragen.

Inhaltsverzeichnis

1.	Vorbemerkung	4
2.	Verordnungsentwurf 2022/0155 (COD) der EU-Kommission	4
2.1.	Inhaltliche Zusammenfassung des Verordnungsentwurfs 2022/0155 (COD)	4
2.2.	Kurze Problemdarstellung des Verordnungsentwurfs 2022/0155 (COD)	5
3.	Rechtlicher Rahmen	5
3.1.	Art. 7 GRCh – Achtung des Privat- und Familienlebens	6
3.1.1.	Schutzbereich	6
3.1.2.	Eingriff	8
3.2.	Art. 8 GRCh – Schutz personenbezogener Daten	9
3.2.1.	Schutzbereich	9
3.2.2.	Eingriff	9
3.3.	Art. 11 GRCh – Freiheit der Meinungsäußerung und Informationsfreiheit	10
3.3.1.	Schutzbereich	10
3.3.2.	Eingriff	10
3.4.	Art. 5 RL 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation)	11
3.4.1.	Schutz der Vertraulichkeit der Kommunikation	11
3.4.2.	Beschränkungsmöglichkeiten	11
4.	Bisherige Rechtsprechung zu den Art. 7, 8, 11 GRCh und Art. 15 RL 2002/58/EG	12
4.1.	Art. 7, 8 und 11 GRCh	12
4.2.	Art. 15 Abs. 1 RL 2002/58/EG	14
5.	Bewertende Analyse des Verordnungsentwurfs 2022/0155 (COD)	15
5.1.	Verhältnismäßigkeit des Verordnungsentwurfs 2022/0155 (COD)	15
5.1.1.	Legitimes Ziel	16
5.1.2.	Geeignetheit	16
5.1.3.	Erforderlichkeit	16
5.1.4.	Angemessenheit	17
6.	Fazit	19

1. Vorbemerkung

Auftragsgemäß wird in dieser Arbeit untersucht, ob und inwieweit der Verordnungsentwurf des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Verhütung und Bekämpfung des sexuellen Missbrauchs von Kindern (2022/0155 (COD))¹ mit geltendem Recht kollidiert, insbesondere ob die Eingriffe in die Grundrechte verhältnismäßig sind.

2. Verordnungsentwurf 2022/0155 (COD) der EU-Kommission

2.1. Inhaltliche Zusammenfassung des Verordnungsentwurfs 2022/0155 (COD)

Der Verordnungsentwurf 2022/0155 (COD) der EU-Kommission vom 11. Mai 2022 beschäftigt sich mit der Bekämpfung und Verhinderung von sexuellem Kindesmissbrauch im Internet.

Etteldorf fasst dies in ihrem Beitrag „EU-Kommission: Verordnungsvorschlag zum besseren Schutz von Kindern vor sexuellem Missbrauch“ wie folgt zusammen: „Durch den Vorschlag zur Verordnung zur Prävention und Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sollen Minderjährige effektiver online und offline vor sexuellem Missbrauch geschützt werden, indem insbesondere Anbieter von Online-Diensten stärker in die Pflicht genommen werden. Dies soll u.a. mittels Risikobewertungs- und -minderungspflichten sowie Meldepflichten erfolgen. Ein neues EU-Zentrum für die Prävention und Bekämpfung von sexuellem Kindesmissbrauch mit Sitz in Den Haag soll dabei als dezentralisierte EU-Agentur prüfend und unterstützend tätig werden. Die vorgeschlagene Verordnung verfolgt präventive und repressive Ansätze, wonach Kinder vor fortgeführtem Missbrauch geschützt, das Wiederauftauchen von Material im Zusammenhang mit sexuellem Kindesmissbrauch im Netz verhindert und die Täter effektiver verfolgt werden sollen. Hierbei sollen zunächst die Anbieter von Hosting- oder Messenger-Diensten eine Risikobewertung vornehmen, inwieweit ihre Dienste für die Verbreitung von Material über sexuellen Kindesmissbrauch oder für die Kontaktabbahnung (sog. Grooming) von Tätern gegenüber Kindern missbraucht werden könnten. Zudem sind auch Risikominderungspflichten – darunter Anpassungen durch geeignete technische und betriebliche Maßnahmen sowie Personalausstattung bei der Inhaltmoderation und im Rahmen von Empfehlungssystemen – vorgesehen. Es sollen klar vorgegebene Meldepflichten von Anbietern, die Online-Inhalte mit sexuellem Kindesmissbrauch aufgespürt haben, gegenüber dem EU-Zentrum für die Prävention und Bekämpfung von sexuellem Kindesmissbrauch eingeführt werden. Das EU-Zentrum soll die Meldungen prüfen, bevor es sie an die mitgliedstaatlichen Strafverfolgungsbehörden und Europol weiterleitet. Wird das Material über sexuellen Kindesmissbrauch nicht umgehend entfernt, können die nationalen Behörden eine Entfernungsanordnung erlassen.“²

Die bisher freiwillig geführten Untersuchungen zur Aufspürung von kindesmissbräuchlichen Inhalten sollen demnach nun verpflichtend werden.

1 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse vom 11. Mai 2022 – COM/2022/209 final. Abrufbar unter: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472>.

2 Etteldorf, Christina: Verordnungsvorschlag. In: MMR-Aktuell 2022, 449230.

2.2. Kurze Problemdarstellung des Verordnungsentwurfs 2022/0155 (COD)

Der Verordnungsentwurf 2022/0155 (COD) wirft in mehrfacher Hinsicht Bedenken auf. Er sieht eine dauerhafte und flächendeckende Analyse und Kontrolle privater Kommunikation vor.

Etteldorf sieht darin die Gefahr, dass eine solche „allgemeine ‚Chat-Kontrolle‘ insbesondere bei mangelnden technischen Schutzmechanismen (oder -möglichkeiten) bzw. deren Versagen zu schweren Eingriffen in die Privatsphäre auch von solchen Personen führen könne, die sich nicht an der Verbreitung von Missbrauchsmaterial oder an Kontaktabbrüchen gegenüber Kindern beteiligen. Auch lässt der Verordnungsvorschlag offen, wie diese Pflichten bei derzeit Ende-zu-Ende-verschlüsselten Kommunikationsdiensten wie z.B. WhatsApp (technisch) umgesetzt werden können.“³ Geht es um bisher Ende-zu-Ende-verschlüsselte, also für Anbieter wie Dritte uneinsehbare Dienste, so ist auch Zurawski der Auffassung, dass „die Verpflichtung zur Überprüfung noch einen weiteren, unumkehrbar schweren Eingriff nach sich ziehe: die faktische Abschaffung dieser sicheren Kommunikationswege. Überprüfen können die Diensteanbieter diese nur auf zwei Wegen. Einerseits durch die Verschlüsselung hindurch, was eine Abschaffung oder zumindest Schwächung der Verschlüsselung bedeuten würde, die dann auch Dritten die Kenntnisnahme von Kommunikationsinhalten ermöglichen würde. Oder an der Verschlüsselung vorbei, durch sog. Client-Side-Scanning, das die EU-Kommission in den Ausführungen zum Vorschlag implizit vorschlägt, das aber kodifizierte, werksseitige Hintertüren in die genutzten Geräte mit sich brächte, die Dritte wiederum ausnutzen können.“⁴

Dieses geplante Vorgehen könne demnach erheblich in das Recht auf Privatsphäre, in den Datenschutz sowie unter anderem in die Grundrechte der EU-Grundrechtecharta (Art. 7, 8, 11 GRCh) eingreifen. Zudem ist der gesamte Prozess für die Nutzer von Kommunikationsdiensten intransparent. Letztlich bleibt fraglich, ob die Regelungen dem Grundsatz der Verhältnismäßigkeit genügen.

3. Rechtlicher Rahmen

Vor der Prüfung, ob und inwiefern der Verordnungsentwurf 2022/0155 (COD) gegen die Artikel 7, 8 und 11 Charta der Grundrechte der Europäischen Union (GRCh)⁵ sowie Art. 15 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung

3 Etteldorf, Christina: Verordnungsvorschlag. In: MMR-Aktuell 2022, 449230.

4 Zurawski: EU-Kommission: Vorschlag „Chatkontrolle“ – Verhältnisse der Überwachung. In: ZD-Aktuell 2022, 01240.

5 Charta der Grundrechte der Europäischen Union. Amtsblatt C 202/389 vom 7. Juni 2016. Abrufbar unter: <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:12016P/TXT&from=LT>.

personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation – ePrivacy-Richtlinie)⁶ verstößt, seien hier die jeweiligen Schutzbereiche skizziert.

3.1. Art. 7 GRCh – Achtung des Privat- und Familienlebens

3.1.1. Schutzbereich

In seinem Urteil vom 6. November 2019 legt das Bundesverfassungsgericht (BVerfG) den Schutzbereich von Art. 7 und 8 GRCh wie folgt fest: „Art. 7 GRCh begründet das Recht auf Achtung des Privat- und Familienlebens, der Wohnung sowie der Kommunikation, Art. 8 GRCh das Recht auf Schutz personenbezogener Daten. Eine Entsprechung haben diese Garantien in Art. 8 Europäische Menschenrechtskonvention (EMRK)⁷, der seinerseits das Recht auf Achtung des Privat- und Familienlebens, der Wohnung und der Korrespondenz – und dabei insbesondere auch vor der Verarbeitung personenbezogener Daten – schützt. Die Gewährleistungen der Art. 7 und Art. 8 GRCh sind dabei eng aufeinander bezogen. Jedenfalls soweit es um die Verarbeitung personenbezogener Daten geht, bilden diese beiden Grundrechte eine einheitliche Schutzverbürgung. Art. 7 und Art. 8 GRCh schützen vor der Verarbeitung personenbezogener Daten und verlangen die ‚Achtung des Privatlebens‘. Unter personenbezogenen Daten werden dabei – wie nach dem Verständnis des deutschen Verfassungsrechts zu Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz (GG) – alle Informationen verstanden, die eine bestimmte oder bestimmbare natürliche Person betreffen. Demnach ist das Recht auf Achtung des Privatlebens nicht eng zu verstehen und beschränkt sich insbesondere nicht auf höchstpersönliche oder besonders sensible Sachverhalte. Insbesondere wird die geschäftliche und berufliche Tätigkeit hiervon nicht ausgeschlossen. Art. 7 und Art. 8 GRCh schützen damit die selbstbestimmte Persönlichkeitsentfaltung gegenüber der Datenverarbeitung Dritter.“⁸

Unter das **Privatleben** fällt das Recht auf personale Selbstbestimmung und Lebensführung, die personale Selbstdarstellung und Selbstwahrung, d.h. die autonome Entscheidung über die persönliche Lebensgestaltung und ihre öffentliche Preisgabe. Träger des Rechts auf Achtung des Privatlebens sind alle natürlichen Personen, insbesondere auch Kinder. Die Staatsangehörigkeit

6 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation). Amtsblatt L 201 vom 31. Juli 2002 S. 37-47. Abrufbar unter: <https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32002L0058>.

7 Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten. Abrufbar unter: https://www.bmj.de/SharedDocs/Downloads/DE/Themen/EuropaUndInternationaleZusammenarbeit/EuropaeischeKonventionMenschenrech-te.pdf;jsessionid=8D72A8B24CA4DBCAAC648CDF7E37414E.1_cid334?_blob=publicationFile&v=1.

8 BVerfG, Urteil vom 6. November 2019 – 1 BvR 276/17 – Recht auf Vergessen II –, Rn. 99 f.

spielt keine Rolle. Darüber hinaus sind juristische Personen und Personenvereinigungen grundsätzlich Grundrechtsträger. Dafür spricht, dass auch das geschäftliche Privatleben geschützt wird.⁹

Das **Familienleben** ist insbesondere durch den Schutz privater Lebensräume gekennzeichnet sowie durch ihre individuelle Gestaltung – vergleichbar mit dem Bereich des Privatlebens. Der weite Begriff des Familienlebens umfasst alle auf Dauer angelegten, engen persönlichen Beziehungen privaten Charakters, die auf einem Zusammenleben basieren, wie sie bei einer herkömmlichen Familie auftreten. Notwendig ist ein *tatsächliches* Familienleben, für das Anhaltspunkte wie gemeinsames Wohnen, die Art und Länge der Beziehung sowie das Interesse und die Bindung der Partner aneinander vorliegen. Träger des Rechts auf Achtung des Familienlebens sind allein natürliche Personen. Berechtig sind alle Familienmitglieder, also Eltern und Kinder, die Großeltern und die Geschwister.¹⁰

Die Achtung der **Wohnung** umfasst den Schutz aller Räume, die der allgemeinen Zugänglichkeit durch eine räumliche Abschottung entzogen und zur Stätte des Privatlebens (i.w.S.) gemacht sind. Auch Geschäftsräume unterfallen Art. 7 GRCh. Der Europäische Gerichtshof (EuGH) orientiert sich dabei an der Rechtsprechung des Europäischen Gerichtshof für Menschenrechte (EGMR), die das entsprechende Grundrecht auf Niederlassungen und Geschäftsräume natürlicher wie juristischer Personen erstreckt. Träger des Rechts auf der Achtung der Wohnung sind alle *natürlichen* Personen, die unmittelbare Besitzer der Wohnung sind, insbesondere die Mieter, sowie *juristische* Personen und Personenvereinigungen.¹¹

Die Gewährleistung der **Kommunikation** schützt ausschließlich die Kommunikation unter Abwesenden, insbesondere wenn sie *einem Dritten* bzw. einer von einem Dritten beherrschten technischen Einrichtung zur Übermittlung an den Empfänger *überlassen* wird (*vermittelte Kommunikation*). Wegen der Übermittlung bestehen für die Kommunikation spezifische Risiken. Hierbei geht es insbesondere um die Vertraulichkeit der Kommunikation. Weiter wird, wie der Begriff der „Korrespondenz“ in der entsprechenden Regelung des Art. 8 EMRK andeutet, nur die Kommunikation geschützt, die an bestimmte Adressaten und nicht an die Öffentlichkeit gerichtet ist. Unerheblich ist, ob die Übermittlung durch staatliche Einrichtungen oder Private erfolgt. Zudem spielt die Technik der Übermittlung keine Rolle. Erfasst wird etwa eine Übermittlung durch Briefe oder Karten, durch das Telefon oder das Internet (E-Mail). Träger des Rechts auf Kommunikation sind alle *natürlichen* Personen sowie *juristische* Personen und Personenvereinigungen.¹²

9 Jarass GrCh, 4. Aufl. 2021, EU-Grundrechte-Charta, Art. 7 Rn. 3, 14 ff.

10 a.a.O., Art. 7 Rn. 18 ff.

11 a.a.O., Art. 7 Rn. 22 f.

12 a.a.O., Art. 7 Rn. 25 f.

3.1.2. Eingriff

In den Schutzbereich des Art. 7 GRCh wird durch eine Maßnahme eingegriffen, die einen der genannten Schutzbereiche berührt. Kein Eingriff liegt vor, wenn der Grundrechtsinhaber in den Eingriff eingewilligt hat.¹³

Das von Art. 7 GRCh geschützte **Privatleben** wird beeinträchtigt, sobald in die Privatsphäre, also in die persönliche Lebensführung eingedrungen wird. Dies kann beispielsweise durch die Durchsuchung einer Person oder den Zugriff auf Informationen über das Privatleben erfolgen. Das Recht auf Achtung des **Familienlebens** wird unter anderem durch die Entziehung des Sorge- oder Erziehungsrechts oder die räumliche Trennung von Familienangehörigen beeinträchtigt. Ein Eingriff im Bereich der **Wohnung** liegt vor, wenn die Privatheit der geschützten Räume beeinträchtigt wird, beispielsweise durch Betreten oder Durchsuchen der Wohnung ohne Einwilligung des Berechtigten oder durch Überwachung. Eine Beeinträchtigung der Achtung der **Kommunikation** ist bei jeglichen Handlungen gegeben, die zu einer Kenntnisnahme der Kommunikationsinhalte oder -daten führen.¹⁴ Als Beispiele seien die Briefkontrolle, die Überwachung der Telekommunikation¹⁵ sowie die Beobachtung der Internetnutzung¹⁶ genannt.

Einschränkungen des Schutzbereichs sind entsprechend Art. 52 Abs. 1 GRCh möglich. Dieser besagt:

„Jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten muss gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.“¹⁷

Nach Art. 52 Abs. 3 S. 1 GRCh sind ebenfalls die Regelungen des Art. 8 EMRK zu berücksichtigen.

„Soweit diese Charta Rechte enthält, die den durch die Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten garantierten Rechten entsprechen, haben

13 Jarass GrCh, 4. Aufl. 2021, EU-Grundrechte-Charta, Art. 7 Rn. 27.

14 Jarass GrCh, 4. Aufl. 2021, EU-Grundrechte-Charta, Art. 7 Rn. 28 ff.

15 EuGH, Urteil vom 17. Dezember 2015 – C-419/14 – WebMindLicenses –, Rn. 71 f.

16 EGMR, Urteil vom 3. April 2007 – 62617/00 – Überwachung von privater E-Mail und Internetnutzung.

17 Jarass GrCh, 4. Aufl. 2021, EU-Grundrechte-Charta, Art. 52.

sie die gleiche Bedeutung und Tragweite, wie sie ihnen in der genannten Konvention verliehen wird. Diese Bestimmung steht dem nicht entgegen, dass das Recht der Union einen weiter gehenden Schutz gewährt.“¹⁸

Zudem bedarf jede Einschränkung einer gesetzlichen Grundlage, wobei der Wesensgehalt des Grundrechts sowie die Verhältnismäßigkeit des Eingriffs gewahrt werden müssen.¹⁹

3.2. Art. 8 GRCh – Schutz personenbezogener Daten

3.2.1. Schutzbereich

Art. 8 GRCh schützt die Verarbeitung personenbezogener Daten. Personenbezogene Daten sind alle Informationen über eine natürliche Person. Der Schutzbereich des Art. 8 GRCh ist nicht eng auszulegen. Er umfasst neben Informationen, die die Privatsphäre im engen Sinne betreffen, alle personenbezogenen Daten, beispielsweise auch den Beruf oder das Vermögen (siehe auch Punkt 3.1.1).²⁰ Grundrechtsträger sind alle natürlichen Personen. Ob auch juristische Personen Grundrechtsträger sind, ist umstritten. Der EUGH erkennt juristische Personen als Grundrechtsträger an, soweit *„der Name der juristischen Person eine oder mehrere natürliche Personen enthält.“²¹*

3.2.2. Eingriff

Ein Eingriff in Art. 8 GRCh liegt vor, wenn personenbezogene Daten verarbeitet werden. Unter Verarbeitung versteht man jede Maßnahme in Bezug auf personenbezogene Daten, insbesondere die Erhebung, Speicherung, Benutzung, Veränderung, Sperrung oder Löschung. Irrelevant ist, ob die Verarbeitung zu einer Beeinträchtigung führt. Eine Beeinträchtigung liegt nicht vor, wenn der Grundrechtsträger zuvor in die Verarbeitung seiner Daten eingewilligt hat.²²

Einschränkungen sind entsprechend Art. 52 Abs. 1 GRCh möglich. Dabei ist Art. 8 Abs. 2 GRCh zu berücksichtigen. Dieser besagt:

„Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.“²³

18 a.a.O., Art. 52.

19 Kingreen, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, 6. Aufl. 2022, Art. 7 Rn. 14.

20 EuGH, Urteil vom 9. November 2010 – C-92, 93/09 – Volker und Markus Schecke GbR –, Rn. 59.

21 EuGH, Urteil vom 9. November 2010 – C-92, 93/09 – Volker und Markus Schecke GbR –, Rn. 53.

22 Jarass GrCh, 4. Aufl. 2021, EU-Grundrechte-Charta, Art. 8 Rn. 9 ff.

23 a.a.O. Art. 8.

Jede Einschränkung bedarf einer gesetzlichen Grundlage und muss den Wesensgehalt des Grundrechts sowie den Grundsatz der Verhältnismäßigkeit wahren.²⁴

3.3. Art. 11 GRCh – Freiheit der Meinungsäußerung und Informationsfreiheit

3.3.1. Schutzbereich

Art. 11 GRCh schützt die Meinungs- und Informationsfreiheit sowie die Freiheit und Pluralität der Medien. Unter Meinungen sind insbesondere Werturteile zu verstehen.²⁵ Geschützt ist das Bilden, Haben oder Nicht-Haben, Äußern und Verbreiten einer Meinung sowie das Recht, seine Meinung nicht zu äußern.²⁶ Die Informationsfreiheit schützt den gesamten Informationsprozess, also den Empfang von Informationen und Ideen, die Weitergabe sowie Nutzung von Anlagen. Von der Medienfreiheit umfasst sind die klassischen Medien (Presse-, Rundfunk- und Filmfreiheit) sowie die „neuen Medien“.²⁷ Über den Begriff der Pluralität wird die Meinungsvielfalt gesichert. Grundrechtsträger sind natürliche Personen, Bedienstete und Beamte der Union sowie juristische Personen.²⁸

3.3.2. Eingriff

In die Meinungs- und Informationsfreiheit wird durch sämtliche Behinderungen der Kommunikation eingegriffen. Nicht nur unmittelbare Handlungen, sondern auch mittelbare Wirkungen oder faktische Handlungen können Eingriffe darstellen, wenn sie in qualifizierter Art den geschützten Bereich unmöglich machen oder zumindest erschweren.²⁹

Für die Eingriffsrechtfertigung findet bei der Meinungs- und Informationsfreiheit nach Art. 52 Abs. 3 GRCh die spezielle Regelung des Art. 10 Abs. 2 EMRK Anwendung. Die Schranke des Art. 52 Abs. 1 GRCh findet keine Anwendung, solange die EMRK einen weiterreichenden Schutz gewährt.³⁰ Für Einschränkungen der Rechte des Art. 11 GRCh wird eine gesetzliche Grundlage benötigt. Zudem ist auch hier der Grundsatz der Verhältnismäßigkeit zu wahren.

24 Jarass GrCh, 4. Aufl. 2021, EU-Grundrechte-Charta, Art. 8 Rn. 13-15.

25 Jarass GrCh, 4. Aufl. 2021, EU-Grundrechte-Charta, Art. 11 Rn. 10.

26 Thiele, in: Pechstein/Nowak/Häde (Hrsg.), Frankfurter Kommentar, EUV/GRC/AEUV, 1. Aufl. 2017, Art. 11 Rn. 9-12.

27 Jarass GrCh, 4. Aufl. 2021, EU-Grundrechte-Charta, Art. 11 Rn. 15 f.

28 Jarass GrCh, 4. Aufl. 2021, EU-Grundrechte-Charta, Art. 11 Rn. 16.

29 Jarass GrCh, 4. Aufl. 2021, EU-Grundrechte-Charta, Art. 11 Rn. 20.

30 Calliess, in: Calliess/Ruffert/Kingreen (Hrsg.), EUV/AEUV, 6. Aufl. 2022, Teil II, Art. 11 Rn. 29.

3.4. Art. 5 RL 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation)³¹

3.4.1. Schutz der Vertraulichkeit der Kommunikation

Artikel 5 Abs. 1 Richtlinie 2002/58/EG (Vertraulichkeit der Kommunikation) legt Folgendes fest:

*„Die Mitgliedstaaten stellen die **Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten** durch innerstaatliche Vorschriften sicher. Insbesondere untersagen sie das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer, wenn keine Einwilligung der betroffenen Nutzer vorliegt, es sei denn, dass diese Personen gemäß Artikel 15 Absatz 1 gesetzlich dazu ermächtigt sind. Diese Bestimmung steht unbeschadet des Grundsatzes der Vertraulichkeit – der für die Weiterleitung einer Nachricht erforderlichen technischen Speicherung nicht entgegen.“³²*

3.4.2. Beschränkungsmöglichkeiten

Artikel 15 Abs. 1 RL 2002/58/EG (Anwendung einzelner Bestimmungen der Richtlinie 95/46/EG) sieht dabei folgende Möglichkeiten der Beschränkung der Rechte aus Art. 5 Abs. 1 Richtlinie 2002/58/EG vor:

*„Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für **die nationale Sicherheit**, (d. h. die Sicherheit des Staates), **die Landesverteidigung, die öffentliche Sicherheit** sowie die **Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen** in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass **Daten** aus den in diesem Absatz aufgeführten Gründen **während einer begrenzten Zeit aufbewahrt werden**. Alle in diesem Absatz genannten Maßnahmen müssen den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen.“³³*

31 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), Abrufbar unter: [EUR-Lex - 32002L0058 - DE \(europa.eu\)](https://eur-lex.europa.eu/lexuri-uri.do?uri=CELEX:32002L0058-DE).

32 a.a.O., Art. 5 Abs. 1.

33 a.a.O., Art. 15.

4. Bisherige Rechtsprechung zu den Art. 7, 8, 11 GRCh und Art. 15 RL 2002/58/EG

Zu den Art. 7, 8, 11 GRCh sowie Art. 15 Abs. 1 ePrivacy-Richtlinie existiert in Bezug auf die Verhütung und Bekämpfung des sexuellen Missbrauchs von Kindern bislang keine Rechtsprechung. Infolgedessen wird in dieser Arbeit die bisherige Rechtsprechung in vergleichbaren Sachverhalten, insbesondere der Vorratsdatenspeicherung, unter Berücksichtigung der Verhältnismäßigkeit dargestellt.

4.1. Art. 7, 8 und 11 GRCh

Der EuGH vertritt die Auffassung, dass die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (VDS-RL)³⁴ unverhältnismäßig im engeren Sinn ist, da sie eine anlasslose und dauerhafte Vorratsdatenspeicherung vorsieht.³⁵

Ein Eingriff in die Grundrechte ist unter anderem gegeben, wenn die Kommunikationsdienste den nationalen Behörden die Verkehrsdaten zugänglich machen³⁶ sowie, wenn Kommunikationsdienste „Daten über das Privatleben einer Person und ihre Kommunikationsvorgänge während eines bestimmten Zeitraums auf Vorrat“³⁷ speichern. Die VDS-RL sieht solche Eingriffe vor. Zudem betrifft sie dabei alle Menschen, die sich in der EU befinden und Kommunikationsmittel verwenden, „ohne dass sich jedoch die Personen, deren Daten auf Vorrat gespeichert werden, auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte“.³⁸ Darüber hinaus wird die Vorratsdatenspeicherung vorgenommen, ohne die Nutzer darüber zu informieren, und dadurch „bei den Betroffenen das Gefühl zu erzeugt, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist“.³⁹ **Ziel** der Maßnahmen der VDS-RL ist die Steigerung der Sicherheit. Dabei ist die Vorratsdatenspeicherung zumindest abstrakt dazu **geeignet**, die Steigerung der Sicherheit zu erreichen.⁴⁰ In Bezug auf die **Erforderlichkeit** und **Angemessenheit** stellt

34 Die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG. Amtsblatt L 105/54 vom 13. April 2006. Abrufbar unter: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:DE:PDF>.

35 Ziebarth, Wolfgang: Die Vorratsdatenspeicherung im Wandel. In: ZUM 2017, 398 ff. [401].

36 EuGH, Urteil vom 21. Dezember 2016 – C-203/15, C-698/15 – Tele2 Sverige –, Rn. 92.

37 EuGH, Urteil vom 08. April 2014 – C-293/12, C-594/12 – Ungültigkeit der EU-Richtlinie –, Rn. 34.

38 EuGH, Urteil vom 08. April 2014 – C-293/12, C-594/12 – Ungültigkeit der EU-Richtlinie –, Rn. 48.

39 EuGH, Urteil vom 21. Dezember 2016 – C-203/15, C-698/15 –, Tele2 Sverige –, Rn. 100.

40 EuGH, Urteil vom 08. April 2014 – C-293/12, C-594/12 – Ungültigkeit der EU-Richtlinie –, Rn. 41, 49.

die Vorratsdatenspeicherung jedoch einen Eingriff großen Ausmaßes dar und vermittelt ein beunruhigendes Gefühl einer omnipräsenten Überwachung des Einzelnen.⁴¹ Aus diesem Grund ist der Grundsatz der Verhältnismäßigkeit nur gewahrt, wenn sich der Eingriff auf das absolut Notwendige beschränkt. Es obliegt den zuständigen nationalen Behörden, *„in jedem Einzelfall zu gewährleisten, dass sich sowohl die Kategorie oder Kategorien erfasster Daten als auch die Dauer, für die der Zugang zu ihnen begehrt wird, nach Maßgabe der konkreten Umstände auf das für die fraglichen Ermittlungen absolut Notwendige beschränken“*.⁴² Die VDS-RL enthält jedoch keine Bestimmungen, *„die zu gewährleisten vermögen, dass sich der Eingriff tatsächlich auf das absolut Notwendige beschränkt“*.⁴³ Eine allgemeine und unterschiedslose Vorratsdatenspeicherung überschreitet somit die Grenzen des absolut Notwendigen.⁴⁴

In seinen Entscheidungen bestätigte der EuGH das Verbot der anlasslosen Speicherung von Massendaten.⁴⁵ Zudem braucht es einen effektiven Schutz vor Missbrauchsrisiken.⁴⁶ Es bedarf eindeutiger und präziser Bestimmungen, die die Tragweite und den Gebrauch der Handlung regeln *„und Mindestanforderungen aufstellen, sodass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen“*.⁴⁷ Die nationale Regelung *„muss insbesondere angeben, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme der Vorratsdatenspeicherung vorbeugend getroffen werden darf, um so zu gewährleisten, dass eine derartige Maßnahme auf das absolut Notwendige beschränkt wird“*.⁴⁸ Unter einem Missbrauch oder falschen Gebrauch sind die zufällige oder unbefugte Zerstörung, der zufällige Verlust sowie der unbefugte Zugang, die unbefugte Veränderung oder das unbefugte Bekanntgeben zu verstehen.⁴⁹ Der unberechtigte Zugang liegt vor, wenn eine Behörde in Art. 8 EMRK eingreift, obwohl der Eingriff gesetzlich nicht vorgesehen und in einer demokratischen Gesellschaft nicht notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.⁵⁰

41 EuGH, Urteil vom 08. April 2014 – C-293/12, C-594/12 – Ungültigkeit der EU-Richtlinie –, Rn. 37.

42 EuGH, Urteil vom 02. März 2021 – C-746/18 – Vorabentscheidung –, Rn. 38.

43 EuGH, Urteil vom 08. April 2014 – C-293/12, C-594/12 – Ungültigkeit der EU-Richtlinie –, Rn. 65.

44 Priebe, Reinhard: Strenge Anforderungen des EuGH an nationale Regelungen. In: EuZW 2017, 136 ff. [138].

45 Etteldorf, Christina: EuGH: Präzisierung der Rechtsprechung. In: MMR-Aktuell 2022, 448557.

46 Zeitmann, Sebastian: EuGH: Anlasslose Vorratsdatenspeicherung. In: MMR-Aktuell 2021, 437661.

47 EuGH, Urteil vom 08. April 2014 – C-293/12, C-594/12 – Ungültigkeit der EU-Richtlinie –, Rn. 54.

48 EuGH, Urteil vom 21. Dezember 2016 – C-203/15, C-698/15 – Tele2 Sverige –, Rn. 109.

49 EuGH, Urteil vom 04. Dezember 2008 – 30562/04 u. 30566/04 – Marper/Vereinigtes Königreich –, Rn. 103.

50 EuGH, Urteil vom 08. April 2014 – C-293/12, C-594/12 – Ungültigkeit der EU-Richtlinie –, Rn. 54.

Das BVerfG führt in seinem Urteil vom 2. März 2010 zur Vorratsdatenspeicherung aus:

„Eine globale und pauschale Überwachung in Form einer flächendeckenden Erfassung der Telekommunikationsverbindungen, wie sie die Vorratsdatenspeicherung darstelle, sei selbst zur Abwehr größter Gefahren verfassungswidrig. Die Wahrscheinlichkeit, dass die gespeicherten Daten später zu Gefahrenabwehr- oder Strafverfolgungszwecken benötigt würden, sei verschwindend gering und könne so schwerwiegende Eingriffe nicht rechtfertigen. Die Vorratsdatenspeicherung ermögliche Persönlichkeitsbilder mit einer noch nie dagewesenen Genauigkeit. Die Kommunikationsdaten seien inhaltlich äußerst aussagekräftig. Der Zugriff auf die näheren Umstände der Telekommunikation wiege nicht weniger schwer als der auf den Kommunikationsinhalt. Er ermögliche umfassende Persönlichkeits- und Verhaltensprofile. Verkehrsdaten lieferten eine Vielzahl von Informationen über soziale Beziehungen. Die Vorratsdatenspeicherung erhöhe außerdem das Risiko, zu Unrecht Ermittlungsmaßnahmen ausgesetzt oder unschuldig verurteilt zu werden, und die Gefahr des Datenmissbrauchs. Verkehrsdaten könnten gezielt gegen missliebige Personen eingesetzt werden und eigneten sich zur Kontrolle von Personen und Gruppierungen ebenso wie zur Wirtschaftsspionage. Nur das Absehen von der Datenspeicherung schütze wirksam vor Missbrauch. Die Vorratsdatenspeicherung beeinträchtige die für die Demokratie unerlässliche Unbefangenheit der Kommunikation. Der Schutz der Menschenwürde verlange ein gewisses Maß an unbeobachteter Kommunikation insbesondere auch im Rahmen besonderer Vertrauensverhältnisse. Der Schaden, der durch die Überwachung des Bürgers entstehe, werde durch den damit verbundenen Effizienzgewinn nicht aufgewogen. [...] Die Vorratsdatenspeicherung sei unverhältnismäßig, weil der zu erwartende Nutzen in einem deutlichen Missverhältnis zu ihren Nachteilen für die Betroffenen und die Gesellschaft insgesamt stehe. Der Rechtsgüterschutz werde nur in wenigen Fällen verbessert. Mit einer Senkung des Kriminalitätsniveaus sei nicht zu rechnen.“⁵¹

Abschließend bleibt festzuhalten, dass die Vorratsdatenspeicherung zwar nicht per se ausgeschlossen wurde, der EuGH jedoch hohe Anforderungen an eine Neuregelung stellt, die bis heute auf EU-Ebene nicht umgesetzt wurde. Die Verhältnismäßigkeit ist danach nur gewahrt, wenn eine Vorratsdatenspeicherung entweder zur Bekämpfung schwerer Kriminalität oder zur Verhütung ernstster Bedrohungen der öffentlichen Sicherheit vorgenommen wird, da andernfalls die tiefgreifenden Eingriffe in die Grundrechte nicht gerechtfertigt sind.⁵²

4.2. Art. 15 Abs. 1 RL 2002/58/EG

Art. 15 Abs. 1 RL 2002/58/EG gestattet es den Mitgliedstaaten, Ausnahmen von der in Art. 5 Abs. 1 der Richtlinie aufgestellten grundsätzlichen Pflicht zur Sicherstellung der Vertraulichkeit personenbezogener Daten zu schaffen. Voraussetzung dafür ist, dass eine solche Beschränkung für die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs elektronischer Kommunikationssysteme in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Für die vorgenannten Zwecke können die Mitgliedstaaten unter

51 BVerfG, Urteil vom 2. März 2010 – 1 BvR 256/08 –, BVerfGE 125, 260-385, juris Rn. 102 ff.

52 EuGH, Urteil vom 06 Oktober 2020 – C-511/18, C-512-/18, C-520/18 – La Quadrature –, Rn. 140.

anderem durch Rechtsvorschriften vorsehen, dass Daten aus einem dieser Gründe für begrenzte Zeit aufbewahrt werden. Die Befugnis, von den Rechten und Pflichten, wie sie die Art. 5, 6 und 9 RL 2002/58/EG vorsehen, abzuweichen, kann es aber nicht rechtfertigen, dass die Ausnahme von dieser grundsätzlichen Pflicht zur Sicherstellung der Vertraulichkeit elektronischer Kommunikationen und der damit verbundenen Daten und insbesondere von dem in Art. 5 der Richtlinie ausdrücklich vorgesehenen Verbot, solche Daten zu speichern, zur Regel wird.⁵³

Der EuGH hat in mehreren Entscheidungen⁵⁴ festgestellt, dass Art. 15 Abs. 1 RL 2002/58/EG mit einer Vorschrift kollidieren würde, die eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten vorsieht.⁵⁵ Lediglich im Fall einer ernstesten, realen und aktuellen, wenigstens jedoch vorhersehbaren Gefahr der nationalen Sicherheit sollen Ausnahmen gemacht werden können.⁵⁶ Art. 15 Abs. 1 RL 2002/58/EG steht somit, unter Berücksichtigung von Art. 7, 8 und 11 GRCh, einer Regelung entgegen, die „präventiv zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung der Verkehrs- und der Standortdaten“⁵⁷ vorsieht. Eine Beschränkung der in der Richtlinie festgelegten Pflichten kann nur unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit sowie der Grundrechte der EU-Grundrechtscharta beschränkt werden.⁵⁸ Insofern wird auf die Rechtsprechung zu den Art. 7, 8 und 11 GRCh verwiesen (siehe 4.1).

5. Bewertende Analyse des Verordnungsentwurfs 2022/0155 (COD)

Unter Berücksichtigung der bisherigen Rechtsprechung zu der Vorratsdatenspeicherung wird der Verordnungsentwurf 2022/0155 (COD) untersucht und analysiert.

5.1. Verhältnismäßigkeit der vorgesehenen Eingriffe des Verordnungsentwurfs 2022/0155 (COD)

Unter Berücksichtigung der Urteile des EuGH zur Vorratsdatenspeicherung werden hinsichtlich des Verordnungsentwurfs des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Verhütung und Bekämpfung des sexuellen Missbrauchs von Kindern verfassungsrechtliche Bedenken vorgebracht. Der Gesetzesentwurf verfolgt das legitime Ziel des Kinderschutzes. Dies soll unbestritten durch Eingriffe in die Kommunikationsprivatheit geschehen. Die Regelungen wirken „*sich auf Vertraulichkeit und Geheimnis der Kommunikation*“ aus.⁵⁹ Eingriffe

53 EuGH, Urteil vom 06. Oktober 2020 – C-511/18, C-512/18, C-520/18 – Anlasslose Vorratsdatenspeicherung nur bei erheblicher Gefahrenlage –, Rn. 110.

54 EuGH, Urteil vom 21. Dezember 2016 – C-203/15 u. C-698/15 – Tele2 Sverige –, Rn. 96.

55 Etteldorf, Christina: EuGH: Präzisierung der Rechtsprechung. In: MMR-Aktuell 2022, 448557.

56 Etteldorf, Christina: EuGH: Präzisierung der Rechtsprechung. In: MMR-Aktuell 2022, 448557.

57 EuGH, Urteil vom 05. April 2022 – C-140/20 – G. D./Commissioner of An Garda Síochána –, 536.

58 Zeitmann, Sebastian: EuGH: Anlasslose Vorratsdatenspeicherung. In: MMR-Aktuell 2021, 437661.

59 Zurawski, Paul: EU-Kommission: Vorschlag „Chatkontrolle“. In: ZD-Aktuell 2022, 01240.

in die Kommunikationsprivatheit liegen unter anderem durch die „*automatisierte Scannung aller Inhalte*“⁶⁰ vor oder durch Fehler infolge von automatisierten Chatkontrollen, woraufhin die private Nachricht an die europäische Koordinierungsbehörde gelangt.⁶¹

5.1.1. Legitimes Ziel

Ziel des Verordnungsentwurfs ist die präventive Bekämpfung des sexuellen Missbrauchs von Kindern im Internet. Um dieses Ziel zu erreichen, möchte die Kommission u.a. Messengerdienste wie etwa WhatsApp, Signal oder Threema verstärkt in die Pflicht nehmen und fordert, dass diese sämtliche Privatnachrichten ihrer Nutzer scannen und entsprechende Auffälligkeiten melden müssen. Die bisher freiwilligen Scanning- Aktivitäten der großen Internetkonzerne (u.a. Facebook/Meta, Microsoft, Google/Alphabet) von unverschlüsselten Messenger- und E-Mail-Nachrichten sowie gehosteten Dateien und gepostetem Content auf Kindesmissbrauchsdarstellungen soll damit verpflichtend gemacht und ausgeweitet werden, um dann auch bisher untätige Anbieter und nicht gescannte Dienste zu erfassen. Der Verordnungsentwurf 2022/0155 (COD) verfolgt zudem das Ziel, „das sogenannte ‚Grooming‘, also die auf sexuellen Missbrauch gerichtete Kontaktaufnahme eines Erwachsenen zu einem Kind, sowie das Verbreiten kinderpornographischer Dateien“ zu bekämpfen.⁶²

5.1.2. Geeignetheit

Bereits bei der Frage der Geeignetheit der Maßnahmen des Verordnungsentwurfs, also ob das intendierte Ziel mit dem Verordnungsentwurf erreicht wird, könnten Bedenken aufkommen. So kommt etwa Woerlein in ZD-Aktuell 2022 zu folgender Einschätzung: *„Bei der Betrachtung potenzieller Folgen einer Chatkontrolle muss zunächst der Frage nachgegangen werden, ob das beabsichtigte Vorhaben der Kommission mit einem tatsächlichen Mehrwert für das verfolgte Ziel verbunden ist. Dies ist vorliegend fraglich. Bezweifelt werden darf bereits, ob die einschlägigen Messengerdienste bislang überhaupt eine tragende Rolle bei der Verbreitung kinderpornographischer Dateien gespielt haben. Selbst wenn man dies bejaht, liegt die Vermutung nahe, dass die Dienste spätestens dann nicht mehr zur Verbreitung der Dateien genutzt werden, wenn bekannt ist, dass die Anbieter die Chatkontrolle zuverlässig durchführen.“*⁶³

5.1.3. Erforderlichkeit

Auch bei der Frage der Erforderlichkeit können bereits Bedenken aufkommen, inwiefern eine anlasslose, dauerhafte und flächendeckende Überwachung als das mildeste Mittel angesehen werden kann. Dieser Punkt wird jedoch nicht weiter vertieft, da die hauptsächlich vorgebrachten Bedenken sich auf die Angemessenheit beziehen.

60 Zurawski, Paul: EU-Kommission: Vorschlag „Chatkontrolle“. In: ZD-Aktuell 2022, 01240.

61 Flamme, Florian: EU-Kommission: Gesetzesentwurf zur Chatkontrolle. In: MMR-Aktuell 2022, 448870.

62 Woerlein, Andreas: Gesetzesvorschlag im Kampf gegen Kindesmissbrauch. In: ZD-Aktuell 2022, 01251.

63 Woerlein, Andreas: Gesetzesvorschlag im Kampf gegen Kindesmissbrauch. In: ZD-Aktuell 2022, 01251.

5.1.4. Angemessenheit

Im Rahmen der Angemessenheit der Maßnahmen des Verordnungsentwurfs – der Verhältnismäßigkeit im engeren Sinn – werden diverse Bedenken angeführt:

So bringt die derzeitige Ausgestaltung zum „Grooming“ nicht nur Vorteile für die Minderjährigen mit sich, sondern auch Nachteile. Das Vorhaben könne sich auf das Kommunikationsverhalten der Minderjährigen auswirken, was zu einer Beeinträchtigung der Kommunikation bzw. zu einem verhaltenen Umgang mit Kommunikation führe und sich dadurch ebenfalls auf die Entwicklung der Minderjährigen auswirke. Eine Ansicht hebt dazu hervor, dass *„der massenhafte Eingriff in die Kommunikationsprivatheit die gesunde Entwicklung und das Kommunikationsverhalten von Kindern, in deren Privatsphäre und Schutzräume eingedrungen wird, indem z.B. einvernehmliches ‚Sexting‘ zwischen Minderjährigen zum Auslöser von Strafverfolgung wird, gefährdet.“*⁶⁴ Auch der Kinderschutzbund hält das Vorhaben in diesem Zusammenhang für *„unverhältnismäßig und nicht zielführend“*⁶⁵. Dem Bundesbeauftragten für Datenschutz und Informationsfreiheit zufolge bietet der Verordnungsentwurf *„kaum Schutz für Kinder, wäre aber Europas Einstieg in eine anlasslose und flächendeckende Überwachung der privaten Kommunikation“*⁶⁶. Dabei macht die permanente Überwachung auch vor Kindern keinen Halt, was zu den vorgenannten Folgen führen kann.

Der Verordnungsentwurf 2022/0155 (COD) soll nunmehr auch bisher Ende-zu-Ende-verschlüsselte, also für Anbieter wie Dritte bisher uneinsehbare Dienste erfassen. Die Verpflichtung zur Überprüfung solcher Dienste führt zu einem weiteren, schweren Eingriff und damit faktisch zur Abschaffung einer vertraulichen Kommunikation. Zurawski führt dazu in ZD-Aktuell 2022 aus: *„Überprüfen können die Diensteanbieter diese nur auf zwei Wegen. Einerseits durch die Verschlüsselung hindurch, was eine Abschaffung oder zumindest Schwächung der Verschlüsselung bedeuten würde, die dann auch Dritten die Kenntnisnahme von Kommunikationsinhalten ermöglichen würde. Oder an der Verschlüsselung vorbei, durch sog. Client-Side-Scanning, das die EU-Kommission in den Ausführungen zum Vorschlag implizit vorschlägt, das aber kodifizierte, werksseitige Hintertüren in die genutzten Geräte mit sich brächte, die Dritte wiederum ausnutzen können. Die hoffnungsvollen Formulierungen des Vorschlags und der Ausführungen, alle technischen Maßnahmen nach dem Stand der Technik und Sicherheit gestalten zu müssen, verkennen*

64 Zurawski, Paul: EU-Kommission: Vorschlag „Chatkontrolle“. In: ZD-Aktuell 2022, 01240 [01240].

65 Kinderschutzbund EU-Info: Kinderschutzbund gegen anlasslose Scans verschlüsselter Nachrichten. Bericht vom 08.05.2022. Abrufbar unter: <https://www.eu-info.de/dpa-europaticker/316232.html>.

66 Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: BfDI fordert Einhaltung der Grundrechte bei Chatkontrolle. Abrufbar unter: <https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2022/09/Chatkontrolle.html>.

hier die schlichte Realität, dass jeder Eingang in ein System stets auch von Dritten geöffnet werden kann.“⁶⁷ Die **konkrete Umsetzung** durch die Unternehmen bleibt in dem Entwurf jedoch **offen**, sodass unklar ist, wie die genaue Gestaltung, bzw. der Ablauf auszusehen haben.⁶⁸ Insbesondere ist unklar, wie die Umsetzung der Pflicht bei der Ende-zu-Ende-Verschlüsselung aussehen soll.⁶⁹ Zudem rechnet Zurawski mit mittelbaren Auswirkungen auf zahlreiche andere Grundrechte. „Sogenannte ‚Chilling Effects‘, die Zurückhaltung von (legalen) Äußerungen oder Handlungen aus Angst vor deren Kenntnisnahme durch den Staat oder Dritte, wirken intensiv auf Meinungs- und Pressefreiheit (hier besonders die Quellenarbeit), ebenso wie Koalitions-, Bekenntnis- und allgemeine Handlungsfreiheit ein.“⁷⁰

Die EU-Kommission verspricht in ihrem Entwurf eine weitest mögliche Achtung der Grundrechte und der Privatsphäre und verpflichtet die Diensteanbieter zur Nutzung minimalinvasiver technischer Maßnahmen. Sie geht jedoch selbst von Fehlern aus, wie aus einem veröffentlichten Bericht bekannt wurde.⁷¹ Woerlein führt zur Fehleranfälligkeit aus, dass „der eingesetzten Technologie eine generelle Fehleranfälligkeit nicht abgesprochen werden kann. Auch wenn die Fehlerquoten im niedrigen Prozentbereich liegen, müssen sie stets in Relation zu der Gesamtzahl an gesendeten Nachrichten gesetzt werden. Allein über den Anbieter WhatsApp werden weltweit pro Tag ca. 100 Mrd. Nachrichten verschickt (Wert für Oktober 2020 nach Rabe, statista.com⁷²). Selbst eine Fehlerquote von 0,1 % würde somit eine extrem hohe Zahl an zu überprüfenden Fällen verursachen.“⁷³ Zudem ist fraglich, wie die Technologien legale Kommunikation, z.B. harmlose Urlaubsfotos und einvernehmliches Sexting, von Straftaten unterscheiden sollen.⁷⁴

In Ergänzung dazu stellt Zurawski das zukünftige Vorgehen wie folgt dar: „Werden Inhalte durchsucht, so müssen zunächst alle Inhalte einbezogen werden, denn auch ein automatisierter Prozess kann nicht vor inhaltlicher Kenntnisnahme feststellen, ob eine Information relevant oder etwa der absoluten Intimsphäre zuzuordnen ist. So bedarf es wenigstens der vorübergehenden Speicherung eines Inhalts im Arbeitsspeicher, damit ein Inhalt automatisiert klassifiziert werden kann. Hat die eingesetzte Technik, z.B. ein Algorithmus, eine Vorauswahl von Inhalten vorgenommen, bleibt nach wie vor eine menschliche Überprüfung notwendig, um die korrekt erkannt-

67 Zurawski, Paul: EU-Kommission: Vorschlag „Chatkontrolle“. In: ZD-Aktuell 2022, 01240.

68 Montag, Miriam: EU-Kommission plant neues Gesetz gegen Kindesmissbrauch. In: becklink 2023186.

69 Etteldorf, Christina: Verordnungsvorschlag. In: MMR-Aktuell 2022, 449230.

70 a.a.O.

71 Netzpolitik: EU-Kommission nimmt hohe Fehlerquoten bei Chatkontrolle in Kauf. Abrufbar unter: <https://netzpolitik.org/2022/geleakter-bericht-eu-kommission-nimmt-hohe-fehlerquoten-bei-chatkontrolle-in-kauf/>.

72 Statistika: Anzahl der versendeten WhatsApp-Nachrichten pro Tag weltweit. Abrufbar unter: <https://de.statista.com/statistik/daten/studie/868733/umfrage/anzahl-der-taeglich-verschickten-whatsapp-nachrichten-weltweit/>.

73 Woerlein, Andreas: Gesetzesvorschlag im Kampf gegen Kindesmissbrauch. In: ZD-Aktuell 2022, 01251.

74 Montag, Miriam: EU-Kommission plant neues Gesetz gegen Kindesmissbrauch. In: becklink 2023186.

ten Inhalte von den irrelevanten zu trennen. Microsoft etwa berichtet für seine ‚grooming detection‘ eine Fehlerrate von 12 %, was bei mehreren Millionen überprüften und gemeldeten Konversationen zur menschlichen Kenntnisnahme privater Unterhaltungen hunderttausender Unionsbürger führen würde. Ähnliches berichtet die Schweizer Bundespolizei, die eine Trefferquote von 14 % für die maschinelle Bilderkennung bekannter Kindesmissbrauchsdarstellungen nennt, die von der Verordnung geforderte Suche nach unbekanntem Darstellungen ist erwartbar noch erheblich ungenauer. Auch hier werden, bei Millionen zu erwartender Meldungen, die privaten Bilder von Millionen Unionsbürgern massenhaft sinnlos von menschlichen Kontrolleuren zur Kenntnis genommen – Fotos, die zwar keine Kindesmissbrauchsdarstellungen, aber durchaus intime Szenen zeigen können. Insgesamt ist damit ein Verstoß gegen die Überwachungsprinzipien zu erkennen, die der EuGH in seinen Entscheidungen zur Vorratsdatenspeicherung ausgearbeitet hat.⁷⁵

Aus den genannten Gründen und vor dem Hintergrund der bisherigen Rechtsprechung des EUGH zur Vorratsdatenspeicherung spricht allein schon das Vorliegen einer anlasslosen Massenüberwachung für die Unverhältnismäßigkeit des Eingriffs. Bei den Betroffenen wird dabei ein Gefühl ständiger Überwachung, welche tatsächlich permanent stattfindet, hervorgerufen, welches das kommunikative Verhalten einschränkt und beeinflusst.⁷⁶

6. Fazit

Der Schutz vor sexuellem Missbrauch an Minderjährigen im Internet wird immer wichtiger, da das Internet bzw. Messengerdienste bei Jugendlichen eine immer größer werdende Rolle im Leben einnehmen und somit auch die Gefahr eines solchen Missbrauchs steigt. Aus vorgenannten Gründen ist jedoch fraglich, ob der aktuelle Verordnungsentwurf für das bezweckte Vorhaben überhaupt einen Mehrwert darstellt. Vor dem Hintergrund der bisherigen Rechtsprechung des EUGH zur Vorratsdatenspeicherung ist davon auszugehen, dass an die Verordnung 2022/0155 (COD) hohe Anforderungen zu stellen sind und der Verordnungsentwurf in seiner aktuellen Fassung so nicht in Kraft treten dürfte. Es erscheint unwahrscheinlich, dass eine grundsätzliche Überwachung von Individualkommunikation der Überprüfung der (europäischen) Grundrechte standhalten würde. Zudem wäre eine Ausweitung der Überwachung auch auf andere Bereiche möglich und zu befürchten. Ausgehend von den genannten Aspekten und Problemen, sieht der aktuelle Verordnungsentwurf unverhältnismäßige Eingriffe in die geprüften Grundrechte der GRCh vor.

Zudem sind bislang viele Fragen und Anforderungen an die Chatkontrolle, insbesondere das konkrete Verfahren im Hinblick auf Ende-zu-Ende verschlüsselte Dienste, noch offen geblieben und bedürfen der Klärung. Somit bedarf es im Verlauf des Gesetzgebungsverfahrens weiterer Anstrengungen, um das wichtige Ziel des Kinderschutzes realisieren zu können, ohne die Grundsätze der Verschlüsselung von individuellen Messenger-Nachrichten aufzugeben.

75 Zurawski, Paul: EU-Kommission: Vorschlag „Chatkontrolle“. In: ZD-Aktuell 2022, 01240.

76 Dörr, Grote, Marauhn: EMRK/GG Konkordanzkommentar. Tübingen 2022, Kap. 20 Rn. 97.