BUNDESRECHTSANWALTSKAMMER

Stellungnahme Nr. 22/2023
Mai 2023
Registernummer: 25412265365-88

Verordnung zur Bekämpfung des Kindesmissbrauchs online („Chatkontrolle“)

Mitglieder des Ausschusses Datenschutzrecht

RA Klaus Brisch, LL.M.
RA Michael Dreßler
RAin Simone Eckert
RA Prof. Dr. Armin Herb, (Vorsitzender)
RAin Simone Kolb
RA Jörg Martin Mathis
RA Dr. Hendrik Schöttle
RA Prof. Dr. Ralph Wagner, LL.M.
RA André Haug, Vizepräsident BRAK
RA Sebastian Aurich, LL.M., BRAK (Berichterstatter)

Mitglieder des Ausschusses Europa

RA Dr. Hans-Joachim Fritz
RA Marc André Gimmy
RAin Dr. Margarete Gräfin von Galen
RA Andreas Max Haak
RA Dr. Frank J. Hospach
RA Guido Imfeld
RA Dr. Christian Lemke
RA Maximilian Müller
RAin Dr. Kerstin Niethammer-Jürgens
RAuN a.D. Kay-Thomas Pohl (Vorsitzender und Berichterstatter)
RA Dr. Hans-Michael Pott
RA Jan K. Schäfer, LL.M.
RAin Stefanie Schott
Prof. Dr. Gerson Trüg
RA Andreas von Máriássy

RAuN Dr. Thomas Remmers, Vizepräsident, Bundesrechtsanwaltskammer
RAin Astrid Gamisch, LL.M., Bundesrechtsanwaltskammer, Brüssel
Ass. jur. Viliana Ilieva, Bundesrechtsanwaltskammer, Brüssel
Ass. jur. Frederic Boog, LL.M., Bundesrechtsanwaltskammer Brüssel
Ass. jur. Nadja Flegler, Bundesrechtsanwaltskammer Brüssel

Verteiler:
Bundesministerium des Innern und für Heimat
Bundesministerium der Justiz
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
Landesdatenschutzbeauftragte
Rechtsausschuss des Deutschen Bundestages
Innenausschuss des Deutschen Bundestages
Arbeitskreise Recht der Bundestagsfraktionen
Landesjustizminister/Justizsenatoren der Länder
Rechtsanwaltskammern
Bundesnotarkammer
Bundessteuerberaterkammer
Bundesverband der Freien Berufe
Deutscher Anwaltverein
Deutscher Juristinnenbund
Deutscher Notarverein
Deutscher Richterbund
Neue Richtervereinigung e.V.
Patentanwaltskammer
Deutscher Steuerberaterverband e.V.
Wirtschaftsprüferkammer
Gesellschaft für Datenschutz und Datensicherheit e. V.
Berufsverband der Datenschutzbeauftragten Deutschlands e. V.
Deutsche Vereinigung für Datenschutz e. V.
Bitkom e. V.
davit – Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein e. V.
eco – Verband der Internetwirtschaft e. V.
VAUNET – Verband Privater Medien e. V.
Stiftung Datenschutz
Datenschutzberater
Computer und Recht
Redaktionen der NJW, ZAP, AnwBl, DRiZ, FamRZ, FAZ, Süddeutsche Zeitung, Die Welt, taz, Handelsblatt, dpa, Spiegel, Focus, Deubner Verlag Online Recht, Beck aktuell, Jurion Expertenbriefing, Juris Nachrichten, LexisNexis Rechtsnews, Otto Schmidt Verlag

Die Bundesrechtsanwaltskammer ist die Dachorganisation der anwaltlichen Selbstverwaltung. Sie vertritt die Interessen der 28 Rechtsanwaltskammern und damit der gesamten Anwaltschaft der Bundesrepublik Deutschland mit rund 166.000 Rechtsanwältinnen und Rechtsanwälten gegenüber Behörden, Gerichten und Organisationen – auf nationaler, europäischer und internationaler Ebene.

Die Bundesrechtsanwaltskammer bedankt sich für die Möglichkeit einer Stellungnahme und gibt Nachstehendes zu bedenken.

Inhalt

Zusammenfassung

Der vorgelegte Entwurf sieht mit der Verpflichtung zur Erkennung von Missbrauchsinhalten sowie daran anschließenden Datenverarbeitungen in einem Rechtsstaat inakzeptabel weitreichende Grundrechtsbeeinträchtigungen vor, die auch angesichts des Zieles des Missbrauchsschutzes nicht gerechtfertigt werden können. Der von der EU-Kommission immer wieder betonte Ausgleich der Grundrechtspositionen ist nicht gelungen. Er kann ohne eine Beschränkung der Zielrichtung des Entwurfs, weitreichende Inhaltserkennungen zu ermöglichen, auch nicht erreicht werden. Über die in dieser Grundentscheidung angelegte grundsätzliche Beeinträchtigung der Vertraulichkeitsgrundrechte können auch die – nur begrenzt – vorgesehenen Sicherungsmechanismen und Verpflichtungsbeschränkungen nicht hinweghelfen. Auch die durch den Berichtsentwurf vorgenommenen Änderungen sind nicht ausreichend.

Verschlimmert wird diese Ausgangssituation durch zu weite Tatbestandsvoraussetzungen der Erkennungsverpflichtung, einen übermäßigen Umfang derselben und weit reichende Datensammlungs- und Austauschbefugnisse.

Besonders bedauerlich und rechtsstaatlichen Maßstäben nicht genügend ist, dass das auf der Hand liegende, von den Rechtsanwaltsorganisationen mehrfach vorgetragene und wenigstens in den Erwägungsgründen der derzeit übergangsweise geltenden Verordnung (EU) 2021/1232 noch anerkannte Bedürfnis nach einem Schutz des Mandatsgeheimnisses in diesem Gesetzesvorhaben noch nicht einmal erwähnt – geschweige denn gewährleistet wird. Dies kann nicht anders gedeutet werden, als dass die Autoren sich bewusst über dieses Erfordernis und die dadurch geschützten Grundrechte hinweggesetzt haben ohne der gesetzgeberischen Pflicht, eine gewissenhafte Grundrechtsabwägung vorzunehmen, auch nur im Ansatz zu genügen. Dies stellt die Beteuerungen der Kommission, einen angemessenen Grundrechtsausgleich angestrebt und erzielt zu haben, ad absurdum.

Die Bundesrechtsanwaltskammer fordert die EU-Institutionen vor diesem Hintergrund dazu auf, von der vorgesehenen Einführung der Erkennungspflicht abzusehen.

Soweit dies nicht geschieht, sind dringend weitere – indes naturgemäß nicht ausreichende – Sicherungsmechanismen vorzusehen und der Verpflichtungsbereich durch klarere und engere Definitionen einzugrenzen.

Entsprechende Vorschläge finden sich in dieser Stellungnahme unter 1.1.7 und 1.1.8. Insbesondere müssen Erkennungsmaßnahmen, durch welche die anwaltliche Verschwiegenheit beeinträchtigt würde, ausgeschlossen werden (s. dazu 1.1.6). Insoweit sollte auch klargestellt werden, dass jedenfalls Dienste des elektronischen Rechtsverkehrs von jeglicher Erkennungspflicht ausgenommen sind (1.1.7.3).

Auch sollten zur Vermeidung wiederholter Grundrechtsbeeinträchtigungen der ursprünglichen Erkennung nachgelagerte Datenverarbeitungen und -austausche reduziert werden. Entsprechende Vorschläge finden sich in dieser Stellungnahme unter 1.1.8.

Kritisch zu bewerten ist auch die vorgesehene Altersverifizierung, die regelmäßig nicht ohne identifizierende Maßnahmen erfolgen wird können. Um die rechtsstaatlich gebotene Möglichkeit der unerkannten Inanspruchnahme anwaltlicher Beratung zu gewährleisten, sollten Altersverifizierungen nur auf Plattformen vorgeschrieben werden, auf denen mit einer Inanspruchnahme anwaltlicher Beratung nicht gerechnet werden kann. Ein entsprechender Regelungsvorschlag findet sich unter 2. Altersprüfung.

Die vorgesehenen Aufsichtsbefugnisse müssen zum Schutz des Mandatsgeheimnisses in Bezug auf Berufsgeheimnisträger beschränkt werden. Ein entsprechender Regelungsvorschlag findet sich unter 3.1.

Aufgrund der Möglichkeit des Rückgriffs auf fremde Ausweisdokumente erscheint die Altersverifizierung ohnehin wenig erfolgsversprechend.

Es muss sichergestellt werden, dass eingebundene Private – und namentlich die Beschäftigten der verpflichteten Diensteanbieter – den einschlägigen mitgliedstaatlichen Verschwiegenheitsverpflichtungen sowie im Mindesten den der Art. 339 AEUV geregelten Verpflichtungen unterliegen (1.1.4). Die in dem Entwurf bereits vorgesehenen Verschwiegenheitssicherungen der Aufsichtsbehörden und der neu zu schaffenden Zentralstelle sollten geschärft werden (3.1 und 4.). Einer weitergehenden Flankierung zur Gewährleistung der Verschwiegenheit bedarf es auch bei der – im Grundsatz zu begrüßenden – menschlichen Aufsicht der Missbrauchserkennung (1.1.9).

Erforderlich ist ferner eine Klarstellung, dass Inhaltserkennungen allenfalls auf der Grundlage einer richterlichen Anordnung und keinesfalls auf freiwilliger Grundlage erfolgen dürfen (siehe dazu 1.2).

Das Erfordernis der Durchführung einer Datenschutz-Folgenabschätzung sollte dem Grundsatz der Unberührtheit des EU-Datenschutzregimes folgend von der Erkennung von Grooming-Kommunikation auch auf die Erkennung von Missbrauchsdarstellungen ausgeweitet werden (5.).

Diensteanbieter sollten verpflichtet werden, Nutzer auf etwaig bestehende alternative Möglichkeiten der vertraulichen Inanspruchnahme anwaltlicher Beratung hinzuweisen (1.1.6).

Stellungnahme

1. Erkennung

Die in dem Entwurf vorgesehene Erkennung von Missbrauchsinhalten stößt auf grundlegende Bedenken. Sie ist daher abzulehnen.

1.1 Verpflichtende Erkennung

Artt. 7 – 10 des Entwurfs sehen für Anbieter interpersoneller Kommunikationsdienste sowie von Hosting-Diensten eine Verpflichtung zur Erkennung von Missbrauchsdarstellungen sowie von Kontakt-Aufnahmen (sog. Grooming-Kommunikation) vor, wenn dies auf behördlichen Antrag hin gerichtlich oder durch eine andere unabhängige Behörde angeordnet wurde (sog. detection order).

1.1.1 Auswirkungen auf die anwaltliche Verschwiegenheit

Um einen effektiven Zugang zum Recht zu gewährleisten, ist es erforderlich, dass Mandantinnen und Mandanten anwaltliche Beratung vertrauensvoll über die von ihnen im Alltag eingesetzten Kommunikationswege in Anspruch nehmen können. Spiegelbildlich sind Anwältinnen und Anwälte zur Ausübung ihres Berufs darauf angewiesen, ihre Dienste auf diesem Wege anbieten zu können. Zudem muss Anwältinnen und Anwälten in der modernen arbeitsteiligen Welt die Möglichkeit bleiben, unter besonderen Sicherheitsvorkehrungen vertrauensvoll Hosting-Dienste in Anspruch zu nehmen. All dies wäre nicht mehr möglich, wenn die in dem Verordnungsvorschlag vorgesehene Pflicht zur Erkennung von Inhalten durch Kommunikations- und Hosting-Anbieter realisiert würde (dazu im Einzelnen sogleich ab 1.1.2).

Die Kommission scheint trotz mehrfacher Hinweise die Bedeutung des Mandatsgeheimnisses und die zu seinem Schutz zwingend erforderliche Möglichkeit der Inanspruchnahme vertraulicher Online-Kommunikation zu verkennen oder – schlimmer – schlicht zu ignorieren. Für letzteres spricht, dass sogar die in den Erwägungsgründen der Übergangsverordnung ((EU) 2021/1232) noch enthaltene Klausel zum Schutz des Mandatsgeheimnisses sich in dem nun vorgelegten Vorschlag nicht wiederfindet. Die BRAK sieht sich daher gezwungen, ihre mehrfach erfolgten Erläuterungen zur Bedeutung des Mandatsgeheimnisses zu wiederholen: Die anwaltliche Verschwiegenheit ist eine Voraussetzung für die Inanspruchnahme rechtsanwaltlicher Beratung und damit ein Grundpfeiler eines jeden Rechtsstaats. Sie unterfällt dem Schutz der europäischen wie nationalen Rechtsstaatsgarantien aus Art. 47 Abs. 1 Satz 2 GRCh, Art. 6 Abs. 1 Satz 1, Abs. 3 lit. c EMRK sowie Art. 20 Abs. 2 GG, Art. 103 Abs. 1 GG. Zugleich ist sie im Kontext anwaltlicher Beratung Voraussetzung für die Verwirklichung europäischer wie nationaler Grundrechte aus Art. 6 Abs. 1 Satz 1, Abs. 3 lit. c EMRK, Art. 47 Abs. 1, 2 Satz 2 GRCh, Art. 20 Abs. 3, Art. 103 Abs. 1 GG, Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, Art. 8 Abs. 1 EMRK, Art. 7 GRCh, Art. 12 Abs. 1 GG. Sie dient in erster Linie dem Schutz des Mandanten und seines Zugangs zum Recht. Das Mandatsgeheimnis schützt Opfer, Täter und sonstige Rechtsuchende gleichermaßen. Wird sein Schutz nicht gewährleistet und können Mandanten daher keinen Rechtsrat in Anspruch nehmen, wird dadurch zugleich die Anwaltschaft in ihrer Berufsausübungsfreiheit beeinträchtigt.

1.1.2 Inakzeptable Kommunikationszugriffe durch die Pflicht zur Erkennung in jedem Fall zu erwarten

Jede Art der Erkennung von Missbrauchsdarstellungen bzw. von Grooming-Kommunikation wird einen Zugriff auf die Kommunikations- bzw. Speicherinhalte erfordern. Dies gilt auch, wenn die Erkennung mittels – vergleichsweise – vertraulichkeitsschonender Technologien wie etwa durch einen Abgleich von Hashwerten erfolgt. Denn sobald die hierzu zwingend erforderliche Möglichkeit des Kommunikationszugriffs – etwa zum Zwecke der Erstellung bzw. des Abgleichs von Hashwerten – eröffnet ist, können die Kommunikationsteilnehmer nicht länger auf die Vertraulichkeit der Kommunikation vertrauen und der mit dem Mandatsgeheimnis verfolgte Zweck, Rechtsuchende nicht durch die Befürchtung von Vertraulichkeitsverlusten von der Inanspruchnahme anwaltlicher Beratung abzuhalten, könnte nicht länger erfüllt werden. Der in der Verordnung vorgesehene Einsatz schonender technischer Mittel ist aus dem genannten Grund nicht geeignet, diese Bedenken auszuräumen. Gleiches gilt für die organisatorischen und prozessualen Schutzvorkehrungen sowie die wiederholten Betonungen des – ohnehin zwingend zu beachtenden – Verhältnismäßigkeitsgrundsatzes. Bereits aus diesem Grund ist jede Erkennung von Kommunikationsinhalten abzulehnen.

1.1.3 Anlasslosigkeit und unzureichende Risiko- bzw. Verdachtskonkretisierung

Überdies können die primär- und verfassungsrechtlichen Anforderungen der Anlassbezogenheit bzw. der hinreichenden Risikokonkretisierung angesichts der in der Verordnung vorgesehenen, keinen konkreten Verdacht erfordernden und nicht auf einzelne Sachverhalte oder Korrespondenzen bezogene, Pflicht zu Erkennung nicht erfüllt werden. Vielmehr lässt Art. 7 Abs. 4 lit. a im Gegenteil bereits ein „signifikantes Risiko“ ausreichen. Auch die in den Folgeabsätzen 5 bis 7 vorgenommenen Konkretisierungen des Risikobegriffs begrenzen den Anwendungsbereich nicht auf konkrete Anlässe oder Verdachtsfälle. Besonders zu beanstanden ist in diesem Zusammenhang, dass die Konkretisierungen mit der Formulierung „gilt als“ („shall be deemed“) als bloße Regelbeispiele verstanden werden könnten, sodass zu befürchten steht, dass Behörden und Gerichte ein signifikantes Risiko auch in Fällen annehmen werden, in denen die dort genannten Voraussetzungen nicht erfüllt sind. Auch der Einbezug bloß vergleichbarer Dienste gemäß Art. 7 Abs. 5 lit b, Abs. 6 lit. b und Abs. 7 lit. c läuft den Erfordernissen eines Anlassbezugs und einer Risikokonkretisierung zuwider.

1.1.4 Problematischer Einbezug Privater Akteure

Die vorgesehenen Verpflichtungen zur Erkennung, Sammlung und Weiterleitung von Inhaltsinformationen treffen zuvorderst die Diensteanbieter und damit überwiegend private Stellen, die weder einem Dienstgeheimnis noch einer demokratischen Kontrolle unterliegen. Überdies haben sich einige von ihnen durch Datenlecks und Skandale als geradezu untauglich zur Verarbeitung höchstsensibler Inhalte erwiesen. Die Beharrlichkeit, mit der sich große Plattformanbieter seit Jahren trotz aufsichtsbehördlicher Maßnahmen, hoher Bußgeldandrohungen und privater Initiativen über elementarste datenschutzrechtliche Anforderungen hinwegsetzen, zeigt, dass gesetzlich vorgegebene Sicherungsmechanismen in diesem Bereich keine hinreichende Gewähr für die Vertraulichkeit der Datenverarbeitungen bieten. Auch dieses Problem wird sich nur zufriedenstellend lösen lassen, indem auf die Pflicht zur Inhaltserkennung verzichtet wird. Sollte der europäische Gesetzgeber sich indes über alle rechtsstaatlichen und praktischen Bedenken hinwegsetzen und an der Erkennungspflicht festhalten, so wären zumindest erheblich weitergehende Flankierungen zum Schutz der Vertraulichkeit erforderlich, die über die bisher bereits datenschutzrechtlich vorgegebenen hinausgehen. Dies gilt insbesondere mit Blick auf Berufsgeheimnisse.

Ferner sollte in Art. 40 Abs. 2 des Entwurfs, nach welchem die EU-Zentralstelle in nicht näher spezifizierter Weise mit privaten Organisationen zusammenarbeiten soll, konkretisiert werden, welche Arten der Zusammenarbeit gemeint sind und welche Kooperationen ausgeschlossen sind. Auch in diesem Zusammenhang muss der Vertraulichkeitsschutz – insbesondere mit Blick auf Berufsgeheimnisse – gewährleistet werden.

Entsprechende Änderungsvorschläge werden sogleich unter 1.1.6 Insbesondere: fehlender Schutz von Berufsgeheimnissen im Zusammenhang mit den dort unterbreiteten Vorschlägen dargestellt.

1.1.5 Grundrechtsabwägung und unzureichende Sicherungsmechanismen

Art. 7 Abs. 4 lit. b stellt den Erlass einer Erkennungsanordnung unter den Vorbehalt einer umfassenden Grundrechts- und Interessensabwägung. Wenngleich dieses – selbstverständliche – Erfordernis grundsätzlich zu begrüßen ist, ist es in diesem Zusammenhang nicht geeignet, einen hinreichenden Grundrechtsschutz zu gewährleisten.

Zunächst ist zu beanstanden, dass die Grundrechtsabwägung bei derart einschneidenden Grundrechtseingriffen bereits weitest möglich auf Ebene des Gesetzgebers erfolgen muss und nicht den Gerichten überlassen bleiben darf. Abgesehen von den übrigen unzureichenden Einschränkungen des Art. 7 Abs. 4 – 8 sind jedoch keinerlei gesetzgeberische Wertungen vorgegeben. Als Wertentscheidung des Gesetzgebers erkennbar ist einzig, dass es bei signifikanten Risiken in einer kaum überschaubaren Vielzahl von Fällen möglich sein soll, (Kommunikations-)Inhalte zu erkennen. Damit wird in weiten Teilen die Möglichkeit der vertraulichen elektronischen Kommunikation und Datenverarbeitung abgeschafft und ohne hinreichende Rechtfertigung oder ausgleichende Sicherungsmechanismen in Vertraulichkeitsgrundrechte eingegriffen.

Soweit der Entwurf etwa in Art. 7 Abs. 8 und 9 sowie den Artt. 8 – 10 Sicherungsmechanismen vorsieht, sind diese angesichts der Grundentscheidung, dass Inhalte auf breiter Front und weitestgehend ohne Möglichkeiten der Differenzierung zwischen betroffenen Nutzern erkannt und zu diesem Zweck eingesehen werden sollen, ebenso untauglich, Grundrechtsverletzungen zu verhindern, wie die Erfordernisse einer Grundrechtsabwägung durch Behörden und Gerichte sowie eines signifikanten Risikos. Die strafrechtlich relevante Nutzung eines Dienstes durch Einzelne vermag massenhafte Eingriffe in die Vertraulichkeitsgrundrechte anderer Nutzer nicht zu rechtfertigen – auch nicht unter Opferschutzgesichts-

punkten. Dies gilt umso mehr als mittlerweile ein Großteil der vertraulichkeitsbedürftigen Grundrechtsausübungen im Onlinebereich erfolgt – sei es bei der Inanspruchnahme elektronischer Kommunikation oder der Nutzung von Cloud-Diensten. Würde in diesem Bereich die Möglichkeit vertraulicher Kommunikation eingeschränkt, verbliebe für die entsprechende Grundrechtsausübung kaum noch Raum. Die Grundrechte wären damit faktisch in weiten Teilen nicht länger gewährleistet. Ausweis dieser inakzeptablen Grundentscheidung der Entwurfsautoren zulasten der Vertraulichkeitsgrundrechte ist auch Erwägungsgrund 23 Satz 2, in welchem zwar die Verhältnismäßigkeit angemahnt wird, und zu deren Erreichung allerlei Sicherungsmechanismen aufgezählt werden, diese jedoch unter den Vorbehalt gestellt werden, dass die Effektivität der Inhaltserkennung dadurch nicht beeinträchtigt werde. Der von der Kommission angestrebte und beanspruchte Grundrechtsausgleich kann auf diese Weise nicht erreicht werden.

Der im EP-Berichtsentwurf enthaltene Änderungsantrag 99 zu Art. 5 a über freiwillige Aufdeckungsanordnungen ist deswegen ebenfalls nicht unterstützenswert. Auch der Zusatz des Berichterstatters zu Art. 7 (Änderungsantrag 111, Art. 7 (2) UAbs. 1 a), welche eine „fair balance between the fundamental rights“ vorsieht, verkennt die Bedeutung dieser Grundrechte.

An dieser Stelle wird auch auf die Ergebnisse der ergänzenden Folgenabschätzung des Wissenschaftlichen Dienstes des Europäischen Parlaments aus dem April 2023 und die gemeinsame Stellungnahme zum Kommissionsvorschlag des Europäischen Datenschutzausschusses und des Europäischen Datenschutzbeauftragten verwiesen.

Änderungsvorschlag:

- **Die in den Artt. 7 – 10 vorgesehene Verpflichtung zur Erkennung von Inhalten ist zu streichen**

1.1.6 Insbesondere: Fehlender Schutz von Berufsgeheimnissen

Insbesondere in Fällen, in denen ein Berufsgeheimnis betroffen ist, kann nach dem vorgelegten Entwurf ein hinreichender Grundrechtsschutz bzw. ein hinreichender Grundrechtsausgleich nicht geschaffen werden. Denn eine grundrechtskonforme Erkennung und Aussonderung anwaltlicher, ärztlicher oder sonstiger streng vertraulicher Kommunikation erscheint weder vorgesehen noch technisch möglich.

In rechtlicher Hinsicht ist mit Blick auf Berufsgeheimnisse und die diesen zugrundeliegenden Grundrechte zudem zu beachten, dass sie im Vergleich zu basalen Persönlichkeitsrechten regelmäßig deutlich höher zu gewichten und an entsprechende Eingriffe höhere Anforderungen zu stellen sind. Dies gilt wie bereits oben unter 1.1.1 dargestellt in besonderem Maß für das anwaltliche Mandatsgeheimnis. So sind Einblicke in der anwaltlichen Verschwiegenheit unterliegende Informationen nur ausnahmsweise zum Schutz gewichtigster Rechtsgüter und unter Beachtung strenger Anforderungen – beispielsweise zur Verhinderung einer mit hinreichender Gewissheit unmittelbar bevorstehenden schweren Straftat – zulässig. Eingriffe in das Mandatsgeheimnis müssen also im Regelfall und namentlich unter den im Entwurf vorgesehenen geringen Anforderungen und dem dort angelegten Umfang unterbleiben. Im Kontrast zu dieser rechtlichen Anforderung scheint dem vorgelegten Entwurf jedoch die Logik zugrunde zu liegen, dass Eingriffe in der Regel zulässig seien. Denn anderenfalls verbliebe für die vorgesehene Erkennungsanordnung kaum ein Anwendungsbereich. Es steht zu befürchten, dass Gerichte und Aufsichtsbehörden diese Logik fälschlicherweise übernehmen und das Mandatsgeheimnis im Rahmen der gemäß Art. 7 Abs. 4 Unterabsatz 1 lit. b vorgesehenen Grundrechtsabwägung missachten oder falsch gewichten. Es gilt dringend zu verhindern, dass das Mandatsgeheimnis auf diese Weise im Online-Bereich faktisch außer Kraft gesetzt wird.

Sofern nicht auf die Erkennungsverpflichtung verzichtet wird, muss eine solche daher zumindest die Gewährleistung des Berufs- bzw. Mandatsgeheimnisschutzes zur Voraussetzung haben und um technische und organisatorische Maßnahmen zur Erreichung dieses Zwecks ergänzt werden. Ferner sollten Anbieter in diesem Fall verpflichtet werden, Nutzer auf etwaig bestehende Möglichkeiten hinweisen, Rechtsrat vertraulich in Anspruch zu nehmen. Die oben unter 1.1.4 Problematischer Einbezug Privater Akteure dargestellten Aspekte müssen dabei beachtet werden.

Überdies sollte das Verhältnis zwischen den Verpflichtungen nach der Verordnung und solchen, die aus nationalen berufsrechtlichen Verpflichtungen erwachsen, analog zur datenschutzrechtlichen Kollisionsregel des Art. 1 Abs. 3 lit. d zugunsten der berufsrechtlichen (Verschwiegenheits-)Verpflichtungen geregelt werden.

Änderungsvorschläge:

Damit ergeben sich die nachstehenden Änderungsvorschläge.

- **Art. 1 Abs. 3** sollte wie folgt ergänzt werden:

  „Diese Verordnung berührt nicht die in den folgenden Rechtsakten festgelegten Vorschriften:

  (a) Richtlinie 2011/93/EU zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie, die den Rahmenbeschluss 2004/68/JI des Rates ersetzt;

  (b) Richtlinie 2000/31/EG und Verordnung (EU) .../... [über einen Binnenmarkt für digitale Dienste (Digital Services Act) und zur Änderung der Richtlinie 2000/31/EG];

  (c) Richtlinie 2010/13/EU;

  (d) die Verordnung (EU) 2016/679, die Richtlinie 2016/680, die Verordnung (EU) 2018/1725 und, vorbehaltlich des Absatzes 4 des vorliegenden Artikels, die Richtlinie 2002/58/EG;

  ***(e) Nationale sowie unions- und konventionsrechtliche Regelungen betreffend die Ausübung freier Berufe und namentlich solcher betreffend den Schutz von Berufsgeheimnissen**.“*

  (Hinzufügungen hervorgehoben)

- Am **Ende des sechsten Abschnitts des zweiten Kapitels** sollte nach dem derzeitigen Art. 24 ein zusätzlicher Artikel mit folgendem Inhalt eingefügt werden:

  „Artikel xx

  Verschwiegenheit und Vertraulichkeit

1. *Diensteanbieter sind auch im Rahmen ihrer Tätigkeit nach dieser Verordnung zur Achtung der Vertraulichkeit verpflichtet. Inhalte und sonstige Informationen, die einem Berufsgeheimnis wie etwa der anwaltlichen Verschwiegenheitspflicht unterliegen, dürfen nicht erhoben, gespeichert oder weitergegeben werden. Berufsgeheimnissen unterliegende Informationen dürfen auch anderen Stellen gegenüber nicht offenbart werden, gegenüber denen nach dieser Verordnung eine Pflicht zur Zusammenarbeit oder zum Datenaustausch besteht.*

2. *Mitarbeiter von Diensteanbietern sowie von deren Auftragnehmern unterliegen mit Blick auf nach dieser Verordnung erhobene oder übermittelte Informationen den Verschwiegenheitsanforderungen des Art. 339 AEUV; dies gilt auch für Organe, freie Mitarbeiter oder sonstige Beschäftigte.*

3. *Diensteanbieter haben geeignete Vorkehrungen zu treffen, um Offenbarungen von Informationen, die einem Berufsgeheimnis und namentlich dem anwaltlichen Mandatsgeheimnis unterliegen, zu verhindern. Dies gilt auch für Offenbarungen gegenüber eigenen Mitarbeitern. Sofern dem Diensteanbieter oder einem Beschäftigten gleichwohl derart geschützte Informationen zur Kenntnis gelangen, sind diese unverzüglich zu löschen. Der Diensteanbieter und die Beschäftigten sind in diesem Fall in gleicher Weise zur Verschwiegenheit verpflichtet, wie die betroffenen Berufsgeheimnisträger. Bestehen Zweifel über das Bestehen oder die Reichweite einer mitgliedstaatlichen Verschwiegenheitspflicht nehmen sie den Rat der in dem Mitgliedstaat zur Beurteilung des Bestehens einer Verschwiegenheitspflicht zuständigen berufsständischen Vertretung – etwa der Anwalts- oder Ärztekammer – in Anspruch.*

4. *Personenbezogene Daten sind vor jeder Weiterverarbeitung zu anonymisieren, sofern der Zweck der Verarbeitung dies zulässt.*

- **Art. 26 Abs. 5** sollte wie folgt um einen dritten Satz ergänzt werden:

  „Artikel xx [hier Verweis auf vorgenannten Artikel] Abs. 1 und 3 gelten entsprechend."

- In **Art. 74** sollte ein neuer Absatz 5 eingefügt werden:

  „Artikel xx [hier ebenfalls Verweis auf den nach Artikel 24 neu vorgeschlagenen Artikel zur Verschwiegenheit] Abs. 1 und 3 gelten entsprechend. Inhalte, die einem Berufsgeheimnis unterliegen, dürfen insbesondere Mitgliedern der Leitungsebene gegenüber nicht offenbart werden, die zugleich anderen Institutionen und namentlich Europol angehören."

- **Art. 40 Abs. 2** sollte wie folgt geändert werden:

  „Die EU-Zentralstelle trägt zur Verwirklichung des Ziels dieser Verordnung bei, indem sie die Umsetzung ihrer Bestimmungen über die Aufdeckung, Meldung, Beseitigung oder Sperrung des Zugangs zu sexuellem Kindesmissbrauch im Internet und die Sperrung des Zugangs dazu unterstützt und erleichtert, Informationen und Fachwissen sammelt und austauscht und die Zusammenarbeit zwischen den einschlägigen öffentlichen und privaten Stellen im Zusammenhang mit der Verhütung und Bekämpfung des sexuellen Kindesmissbrauchs, insbesondere im Internet, erleichtert. ***Diese Zusammenarbeit darf nicht die Weitergabe von persönlichen oder inhaltlichen Informationen beinhalten, es sei denn, dies ist ausdrücklich vorgesehen oder rechtlich erforderlich. Informationen, die einem Berufsgeheimnis wie insbesondere der anwaltlichen Verschwiegenheit unterliegen, dürfen nicht offenbart werden."***

  (Änderungen hervorgehoben)

- **Art. 40** sollte um den folgenden dritten Absatz erweitert werden:

  „Für private Stellen im Sinne des Absatzes 2 gilt Art. xx [hier Verweis auf die am Ende des sechsten Abschnitts des zweiten Kapitels nach dem derzeitigen Artikel 24 einzufügende Verschwiegenheitsvorschrift – s.o.] *entsprechend."*

- Die in den **Artt. 7 – 10** vorgesehene Verpflichtung zur Erkennung von Inhalten muss auch aus Gründen des Berufsgeheimnisschutzes ersatzlos gestrichen werden.

- **Hilfsweise:** Sollte der EU-Gesetzgeber sich über alle rechtsstaatlichen und praktischen Bedenken hinwegsetzen und die Erkennungsverpflichtung beibehalten werden, bedürfte es im Mindesten der folgenden Änderungen:

  - In **Art. 7 Abs. 4 Unterabsatz 1 lit. b** bedürfte es zumindest eines Hinweises auf Berufsgeheimnisse sowie einer abstrakten gesetzgeberischen Abwägungsentscheidung zugunsten derselben. Art. 7 Abs. 4 Unterabsatz 1 lit. b sollte dann wie folgt ergänzt werden:

    „(b) die Gründe für den Erlass der Aufdeckungsanordnung überwiegen die nachteiligen Folgen für die Rechte und berechtigten Interessen aller Betroffenen, wobei insbesondere ein angemessener Ausgleich zwischen den Grundrechten dieser Betroffenen zu gewährleisten ist. ***Einblicke in und Erkennungen von Informationen, die einem Berufsgeheimnis unterliegen, dürfen nicht erfolgen und müssen sicher ausgeschlossen sein.“***

    (Hinzufügungen hervorgehoben)

  - **Art. 7 Abs. 8** sollte wie folgt ergänzt werden:

    „Wenn die Koordinierungsbehörde des Niederlassungsortes um den Erlass von Aufdeckungsanordnungen ersucht bzw. die zuständige Justiz- oder unabhängige Verwaltungsbehörde die Aufdeckungsanordnung erlässt, richten sie diese so aus und präzisieren sie so, dass die in Abs. 4 Unterabsatz 1 Buchstabe b genannten negativen Folgen auf das beschränkt bleiben, was unbedingt erforderlich ist, um dem unter Buchstabe a genannten erheblichen Risiko wirksam zu begegnen. ***Der in lit. b vorgesehene Schutz von Berufsgeheimnissen ist in jedem Fall zu gewährleisten. Ist dies nicht möglich, darf keine Erkennungsanordnung ergehen.”***

    (Hinzufügungen hervorgehoben)

  - **Art. 10 Abs. 3** müsste um die folgende, neu einzufügende litera d) ergänzt werden:

    „Offenbarungen von Informationen, die einem Berufsgeheimnis unterliegen, wirksam verhindern.“

  - **Art. 10 Abs. 4 lit. a-b** müsste wie folgt ergänzt werden:

    „4. Der Anbieter muss:

    (a) alle erforderlichen Maßnahmen treffen, um sicherzustellen, dass die Technologien und Indikatoren sowie die Verarbeitung personenbezogener Daten und anderer Daten im Zusammenhang damit ausschließlich zum Zweck der Aufdeckung der Verbreitung von bekanntem oder neuem Material des sexuellen Missbrauchs von Kindern bzw. der Anwerbung von Kindern verwendet werden, soweit dies zur Ausführung der an ihn gerichteten Aufdeckungsaufträge unbedingt erforderlich ist;

(b) wirksame Maßnahmen zum Schutz von Mandatsgeheimnissen etablieren

~~(b)~~ (c) *wirksame interne Verfahren zur Verhinderung und erforderlichenfalls zur Aufdeckung des Missbrauchs der Technologien, Indikatoren und personenbezogenen Daten sowie anderer unter Buchstabe a genannter Daten, einschließlich des unbefugten Zugriffs auf und der unbefugten Weitergabe solcher personenbezogenen Daten und anderer Daten;“*

(Änderungen hervorgehoben)

- **Art. 10 Abs. 5 Satz 1** müsste um die folgende neu einzufügende litera d) ergänzt werden:

  „etwaig bestehende alternative Kommunikationswege, um vertraulich Rechtsrat in Anspruch zu nehmen.“

1.1.7 Verschärfung durch zu weite Definitionen und fehlende Ausnahmen

Verschärft werden diese grundlegenden Probleme durch zu weite Anwendungsbereichs- und Tatbestandsdefinitionen.

So ist der Anwendungsbereich in Art. 1 äußerst weit definiert. Ausnahmen etwa für den elektronischen Rechtsverkehr fehlen. Ferner erscheinen angesichts der weiten Definitionen der zu erkennenden, zu meldenden und vorzuhaltenden Inhalte und Parameter vergleichsweise eingriffsarme Erhebungen und Prüfungen, die nähere Befassungen mit den Inhalten nicht erfordern würden, nicht ausreichend, um die vorgesehenen Erkennungsverpflichtungen zu erfüllen. Anordnungen in den Artt. 7 – 10, die eine möglichst schonende Vorgehensweise – eher scheinbar – vorsehen, laufen damit ins Leere.

Im Einzelnen:

1.1.7.1 Bekannte Missbrauchsdarstellungen

In besonderem Maße abzulehnen ist zunächst die in Art. 2 lit. m enthaltene Definition bekannter Missbrauchsdarstellungen als bloß „potentielle“ Missbrauchsdarstellungen, die anhand der Indikatoren des Art. 44 Abs. 1 lit. a erkannt wurde. Eine derart weite Tatbestandsfassung läuft den primär- und verfassungsrechtlichen Erfordernissen der Anlassbezogenheit und der hinreichenden Risikokonkretisierung deutlich zuwider.

Änderungsvorschlag:

- **Art. 2 lit. m** ist wie folgt zu ändern:

  *„„bekanntes Material über den sexuellen Missbrauch von Kindern": **~~potenzielles~~** Material über den sexuellen Missbrauch von Kindern, das anhand der Indikatoren in der Datenbank der Indikatoren nach Art. 44 Abs. 1 Buchstabe a ermittelt wurde;“*

1.1.7.2 Unbekannte Missbrauchsdarstellungen

Gleiches gilt – in noch erheblicherem Umfang – für den Einbezug auch unbekannter Missbrauchsdarstellungen in den Artt. 7 – 9 und deren wiederum viel zu weitgehende Definition in Art. 2 lit. n als ebenfalls „potentielle“ Missbrauchsdarstellung. Hinzukommt in diesem Zusammenhang, dass die Ermittlung

unbekannter Darstellungen eine eingehendere Auseinandersetzung mit den zu prüfenden Kommunikationsinhalten anhand einer größeren Anzahl von – überdies im Vergleich etwa zu Hashwerten bekannter Darstellungen weniger treffsichereren – Kriterien erfordern würde. Dadurch würde die Menge der betroffenen Kommunikationsinhalte noch einmal erheblich vergrößert und die Gefahr falsch-positiver Treffer zugleich deutlich erhöht.

Änderungsvorschläge:

- **Art. 2 lit. n** ist zu streichen.

- In den **Artt. 7 – 9** sind die Bezugnahmen auf neue Missbrauchsdarstellungen und die spezifischen Regelungen derselben zu streichen.

- **Art. 44 Abs. 1 lit. b ist zu streichen**

- Alle weiteren Bezugnahmen auf und spezifische Regelungen im Umgang mit neuen Missbrauchsdarstellungen sind zu streichen.

1.1.7.3 Grooming-Kommunikation

Die Erkennung von Kontaktaufnahmen im Sinne von Art. 2 lit. o (sog. Grooming-Kommunikation) wird aufgrund der individuellen Prägung einer jeden Kontaktaufnahme in besonderem Maße eine Auseinandersetzung mit Kommunikationsinhalten auch betreffend darin gewählter Formulierungen und Kontexte erfordern. Eine einigermaßen schonende, abstrakte Prüfung und Einordnung – etwa anhand von Hashwerten – erscheint daher kaum möglich. Insbesondere die in Art. 36 Abs. 1 lit. a vorgesehene Übermittlung von Konversationstransskripten wird eine inhaltliche Auseinandersetzung mit der Korrespondenz erfordern; Art. 44 Abs. 2 lit. c gibt dementsprechend bereits vor, dass „Sprachidentifikatoren“ („language identifiers“) vorzuhalten seien. Angesichts derartiger Vertraulichkeitsbeeinträchtigungen ist jegliche Pflicht zur Erkennung von Grooming-Kommunikationen abzulehnen.

Änderungsvorschlag:

- **Art. 7 Abs. 1** sollte wie folgt geändert werden:

  „Die Koordinierungsbehörde ist befugt, das zuständige Gericht des Mitgliedstaats, in dem sie benannt wurde, ***~~oder eine andere unabhängige Verwaltungsbehörde dieses Mitgliedstaats~~*** *zu ersuchen, eine Aufdeckungsanordnung zu erlassen, mit der ein Anbieter von Hosting-Diensten oder ein Anbieter von interpersonellen Kommunikationsdiensten, der der Rechtshoheit dieses Mitgliedstaats unterliegt, verpflichtet wird, die in Artikel 10 genannten Maßnahmen zu ergreifen, um den sexuellen Online-Missbrauch von Kindern in einem bestimmten Dienst aufzudecken.* ***Nicht öffentliche einsehbare Inhalte dürfen nicht auf Kontaktaufnahmen im Sinne von Art. 2 lit. o hin überprüft werden.“***

  (Hinzufügungen hervorgehoben)

- In den **Artt. 7 – 8** sollten sämtliche Bezugnahmen auf Kontaktaufnahmen bzw. spezifische Regelungen derselben gestrichen werden.

1.1.7.4 Ausschluss des elektronischen Rechtsverkehrs

Nach dem Verständnis der Bundesrechtsanwaltskammer sind Systeme des elektronischen Rechtsverkehrs, das heißt solche, die einzig zum Zwecke der Kommunikation zwischen Rechtsanwälten, Gerichten, Behörden und Mandanten bzw. Verfahrensparteien eingerichtet sind, weder von der Definition eines Hosting-Dienstes gemäß Art. 2 lit. a noch von der eines öffentlichen interpersonellen Kommunikationsdienstes gemäß Art. 2 lit. b umfasst. Zur Vermeidung von Missverständnissen und unnötigen Belastungen sollte gleichwohl klargestellt werden, dass die Verordnung auf Anbieter solcher Dienste nicht anwendbar ist. Denn es ist bereits absehbar, dass die in dem Entwurf vorgesehenen Verpflichtungen in Bezug auf Anbieter solcher Dienste unter keinem rechtlichen Gesichtspunkt zu rechtfertigen wären. Solche Dienste werden nicht zur Verbreitung von Missbrauchsdarstellungen oder zur Anwerbung von Kindern genutzt. Zudem verbieten der Grundsatz des Zugangs zum Recht sowie die im Bereich des elektronischen Rechtsverkehrs geltenden besonderen Vertraulichkeitsverpflichtungen wie namentlich das Mandatsgeheimnis sowie nicht zuletzt die anwaltliche und justizielle Unabhängigkeit eine Verpflichtung zur Erkennung von Inhalten ebenso wie die diesbezüglich vorgesehene Beaufsichtigung durch die Koordinierungsbehörden.

Änderungsvorschlag:

- **Art. 1 Abs. 2** der sollte daher wie folgt ergänzt werden:

  „Diese Verordnung gilt für Anbieter einschlägiger Dienste der Informationsgesellschaft, die diese Dienste in der Union anbieten, unabhängig vom Ort ihrer Hauptniederlassung. ***Sie gilt nicht für Anbieter von Systemen des elektronischen Rechtsverkehrs, das heißt solcher Systeme, die spezifisch zum Zwecke der Kommunikation zwischen Rechtsanwälten, Gerichten, Behörden und Mandanten bzw. Verfahrensparteien eingerichtet wurden.“***

  (Hinzufügungen hervorgehoben)

1.1.8 Nachgelagerte Risiken durch Erhebung, Sammlung und Austausch von Informationen

Im Interesse der Missbrauchsbekämpfung werden im Verordnungsentwurf bezüglich der zu erkennenden Inhalte zahlreiche sich anschließende Erhebungen, Sammlungen und Austausche von Informationen vorgesehen (so in Art. 37, Art. 38, Art. 39 Abs. 1, Art. 40 Abs. 2, Art. 43 Abs. 1 lit. a, Abs. 2 lit. b und c, Abs. 3 lit. a und b, Abs. 5 lit. c, d und f, Abs. 6 lit. a, Art. 46 Abs. 2, Abs. 3, Abs. 4, Abs. 5, Abs. 7, Art. 48 Abs. 3, Art. 50 Abs. 2 lit. a, Art. 53 Abs. 2, Art. 54 Abs. 1, Art. 83). Neben der vorgelagerten Erkennung durch die Anbieter sind diese Vorgänge ihrerseits mit weiteren Vertraulichkeitsbeeinträchtigungen verbunden, bezüglich derer ebenfalls auf eine Wahrung von Grund- und Verfassungsrechten sowie des Verhältnismäßigkeitsgrundsatzes zu achten ist. Insbesondere muss auch und gerade bei diesen Vorgängen der Schutz von Berufsgeheimnissen gewährleistet werden. Dabei ist zu berücksichtigen, dass die Rechte der Betroffenen umso stärker beeinträchtigt werden, je länger die Inhalte aufbewahrt, je umfangreicher sie mit anderen Akteuren geteilt und je leichter sie mit anderen Daten verknüpft werden können. Insbesondere für Opfer und Täter sexuellen Missbrauchs, die sich anwaltlich über die der Verordnung unterfallende Dienste beraten lassen, können rechtsstaatlich und persönlichkeitsrechtlich unter keinen Umständen zu rechtfertigende Beeinträchtigungen entstehen, wenn Daten an andere Akteure und insbesondere Strafverfolgungsbehörden, Europol oder Gerichte weitergegeben werden. Dies gilt aber auch für Mandanten, die keiner dieser Gruppen angehören, deren Mandatskommunikation aber als falsch-positiver Treffer erfasst und ggf. weitergeleitet wird. Vor diesem Hintergrund sind die entsprechenden Informationserhebungs-, Sammlungs-, und Austauschpflichten auf ein absolut erforderliches Minimum zu beschränken und vor jeder Weitergabe eine gewissenhafte Prüfung des Materials

vorzusehen. Insoweit besteht jedoch der Zielkonflikt, dass eine gewissenhafte Prüfung regelmäßig auch nähere Beschäftigung mit dem Material sowie einen menschlichen Einblick erfordern dürfte, wodurch seinerseits Beeinträchtigungen von Grund- und Verfassungsrechten sowie des Mandatsgeheimnisses begründet wären. Um der so programmierten Wiederholung von Beeinträchtigungen von Grund- und Verfassungsrechten entgegenzuwirken, müssen daher bereits auf der vorgelagerten Ebene der Erkennung durch die Diensteanbieter größtmögliche Begrenzungen der zu erfassenden Inhalte vorgenommen bzw. auf diese verzichtet werden. Wo dies nicht möglich ist, sollten Folgebeeinträchtigungen durch die nachstehenden Maßnahmen begrenzt werden.

1.1.8.1 Achtung von Verschwiegenheitspflichten bei nachfolgenden Verarbeitungsvorgängen

Es bedarf zunächst der bereits in den Änderungsvorschlägen zu 1.1.6 zu einem hinter Art. 24 neu einzufügenden Artikel enthaltenen Klarstellung, dass die Erhebung oder Sammlung von Inhalten und Informationen, die einem Berufsgeheimnis und insbesondere dem anwaltlichen Mandatsgeheimnis unterliegen, ausgeschlossen ist, und dass diese anderen Akteuren gegenüber auch dann nicht offenbart werden dürfen, wenn ein Datenaustausch nach dieser Verordnung vorgesehen ist.

1.1.8.2 Keine Weiterverarbeitungsbefugnis beim Diensteanbieter

Ferner muss die nach dem derzeitigen Wortlaut von Art. 22 Abs. 1 Unterabsatz 2 Satz 2 mögliche Nutzung mandatsbezogener Informationen zur Produktverwendung klarstellend auch dort ausgeschlossen werden.

Änderungsvorschlag:

- **Art. 22 Abs. 1 Unterabsatz 2 Satz 2** sollte wie folgt ergänzt werden

  *„Er darf jedoch keine personenbezogenen Daten **oder solche, die einem Berufsgeheimnis unterliegen, zu diesem Zweck** speichern."*

  (Änderungen hervorgehoben)

1.1.8.3 Kein Sammeln und Reporting von Mandatsinformationen

Es muss klargestellt werden, dass die derzeit in Art. 83 bzw. 84 für Diensteanbieter vorgesehenen Datenspeicherungs- bzw. Reporting-Verpflichtungen keine Mandatsinformationen umfasst.

Änderungsvorschläge:

- ***Art. 83 Abs. 4 Satz 2*** *sollte wie folgt ergänzt werden:*

  *„Die gespeicherten Daten dürfen keine personenbezogenen Daten **oder solche, die einem Berufsgeheimnis unterliegen,** enthalten.*

  (Änderungen hervorgehoben)

- ***Art. 84 Abs. 5 Satz 2*** *sollte wie folgt ergänzt werden:*

  *„Sie dürfen auch keine personenbezogenen Daten **oder solche, die einem Berufsgeheimnis unterliegen,** enthalten."*

(Änderungen hervorgehoben)

1.1.8.4 Beschränkung der Kooperationsbefugnisse

Es bedarf einer Klarstellung, dass die teils vage formulierten Kooperationsbefugnisse bzw. -gebote nach der Verordnung (vgl. Art. 38 Abs. 1, 39 Abs. 1, 40 Abs. 2, 43 Abs. 1 a) keine über die explizit darin vorgesehenen Befugnisse hinausgehende Befugnis zur Erhebung, Sammlung oder Weitergabe von erkannten Inhalten beinhalten.

Änderungsvorschläge:

- **Am Ende des vierten Abschnitts des dritten Kapitels nach dem derzeitigen Art. 39** sollte daher der folgende zusätzliche Artikel eingefügt werden:

  „Artikel xx

  Beschränkungen

  „Den Kooperationsbefugnissen bzw. -geboten nach dieser Verordnung und insbesondere den Artikeln 38 Abs. und 39 Abs. 1 ist keine, über die explizit in der Verordnung vorgesehenen Befugnisse hinausgehende Befugnis zur Erhebung, Sammlung oder Weitergabe von erkannten Inhalten zu entnehmen."

- **Am Ende des vierten Abschnitts des vierten Kapitels nach dem derzeitigen Art. 54** sollte ferner der folgende Artikel aufgenommen werden:

  „Artikel xx

  Beschränkungen

  „Artikel xx [hier Verweisung auf den vorgenannten Artikel am Ende des vierten Abschnitts des dritten Kapitels nach dem derzeitigen Artikel 39] *gilt auch für Kooperationen nach diesem Abschnitt."*

1.1.8.5 Vermeidung von Personenbezügen

Schließlich bedarf es zur Vermeidung nachgelagerter Risiken der ebenfalls bereits in den Änderungsvorschlägen unter 1.1.6 zu einem hinter Art. 24 neu einzufügenden Artikel vorgeschlagenen Klarstellung, dass jegliche Erhebung, Sammlung oder Weitergabe von Inhalten oder Informationen, soweit möglich und mit dem Zweck vereinbar, ohne Bezug zu natürlichen Personen erfolgen muss und dass hierzu im Rahmen des Möglichen auch Anonymisierungen erfolgen müssen.

1.1.9 Menschliche Aufsicht (human oversight)

Der Entwurf sieht in Art. 10 Abs. 4 lit. c) die Implementierung einer menschlichen Aufsicht (human oversight) für automatisierte Erkennungsprozesse vor. Angesichts der potenziell einschneidenden Auswirkungen, die falsch-positive Treffer auf die Rechte und Interessen der Betroffenen haben können und angesichts der Fehleranfälligkeit und Voreingenommenheit vieler automatisierter Erkennungsprozesse ist dieses Erfordernis – als lediglich zweitbeste Lösung zum eigentlich gebotenen Verzicht auf Erkennungsmaßnahmen – im Grundsatz zu begrüßen. Zu beachten ist allerdings, dass hierdurch zugleich Offenbarungen von Inhalten gegenüber Mitarbeitern der jeweiligen Diensteanbieter bzw. Institutionen

befördert werden. Zudem steht dieses Erfordernis einer, zumindest auf der ersten Erhebungsebene, vergleichsweise eingriffsarmen Erkennung – etwa anhand von Hashwerten – entgegen. Ein hinreichender Vertraulichkeitsschutz kann angesichts dieses Dilemmas nur durch ein Absehen von der Erkennung insgesamt erzielt werden. Wo indes in Ermangelung eines Erhebungsverbots auf erster Ebene zur Vermeidung schlimmerer Folgen eine menschliche Aufsicht sinnvollerweise zum Einsatz kommt, muss die Vertraulichkeit der Inhalte durch weitreichende Verschwiegenheitsverpflichtungen geschützt werden. Dies gilt insbesondere mit Blick auf die Einbindung privater Akteure (s. dazu oben unter 1.1.4).

Änderungsvorschlag:

- **Art. 10 Abs. 4 lit. c)** sollte daher wie folgt ergänzt werden:

  *„eine regelmäßige menschliche Aufsicht gewährleisten, um sicherzustellen, dass die Technologien hinreichend zuverlässig funktionieren und erforderlichenfalls, insbesondere wenn potenzielle Fehler und eine mögliche Anwerbung von Kindern festgestellt werden, menschlich eingegriffen wird**; es gelten die Verschwiegenheitsverpflichtungen des Art. xx* [Verweis auf den am Ende des sechsten Abschnitts des zweiten Kapitels nach dem derzeitigen Art. 24 einzufügenden Artikel zur Vertraulichkeit – *siehe Änderungsvorschläge unter 1.1.6 Insbesondere: fehlender Schutz von Berufsgeheimnissen*]“;

  (Änderungen hervorgehoben)

1.2 Ausschluss von Erkennungsmaßnahmen auf freiwilliger Basis und Richtervorbehalt

Art. 4 des Entwurfs verpflichtet Anbieter interpersoneller Kommunikationsdienste sowie von Hosting-Diensten zur Risikominimierung. In diesem Zusammenhang bedarf es einer Klarstellung, dass Maßnahmen zur Inhaltserkennung nicht ergriffen werden dürfen. Sofern der EU-Gesetzgeber trotz aller rechtsstaatlichen und sachlichen Bedenken an der Erkennungsverpflichtung gemäß Artt. 7 – 10 festhalten sollte, bedürfte es zumindest einer Klarstellung, dass Erkennungsmaßnahmen keinesfalls auf freiwilliger Basis erfolgen dürfen. Angesichts der mit dieser Maßnahme verbundenen einschneidenden Grundrechtsbeeinträchtigung bedarf es darüber hinaus eines unbedingten Richtervorbehaltes; die alternative Anordnung durch eine sonstige Verwaltungsbehörde, wie derzeit vorgesehen, ist nicht ausreichend.

Änderungsvorschläge:

- In **Art. 4 Abs. 1** sollte daher ein dritter Satz mit folgendem Inhalt eingefügt werden.

  „Maßnahmen zur Inhaltserkennung dürfen nicht ergriffen werden.“

- Sofern an der Erkennungsverpflichtung gemäß Artt. 7 – 10 festgehalten werden sollte, sollte es an gleicher Stelle alternativ heißen:

  „Maßnahmen zur Inhaltserkennung dürfen nur auf richterliche Anordnung und ausschließlich unter den Voraussetzungen der Artt. 7 – 10 ergriffen werden.“

- *In **Art. 7 Abs. 1** sollten die Worte „oder eine andere unabhängige Verwaltungsbehörde dieses Mitgliedstaats” gestrichen werden.*

2. Altersprüfung

Die in Erwägungsgrund 28, Art. 3 Abs. 2 lit. b) Spiegelstrich 3, Art. 4 Abs. 3, und Art. 6 Abs. 1 lit. c) des Entwurfs vorgesehenen Verpflichtungen zur Durchführung einer Altersverifikation bergen Risiken für den Zugang zum Recht. So steht zum einen – insbesondere mit Blick auf Art. 4 Abs. 3 – zu befürchten, dass Rechtsuchende aufgrund der mit den meisten Altersverifikationsmethoden einhergehenden Identifizierungsmöglichkeiten fürchten, bei der Inanspruchnahme von Rechtsrat erkannt zu werden, und daher von dieser Abstand nehmen. Zum anderen könnten Minderjährige durch Altersverifikationserfordernisse von der Nutzung von Kommunikationsdiensten – und damit von der Inanspruchnahme von Rechtsrat über dieselben – ausgeschlossen werden. Beides gilt es durch konkretisierende Beschränkungen der Anspruchsvoraussetzungen zu verhindern. Hierfür streiten neben der Möglichkeit der Inanspruchnahme von Rechtsrat auch allgemeinere Teilhabegesichtspunkte. Zweckmäßiger Weise sollte die Verpflichtung zur Altersverifikation daher auf solche Dienste beschränkt werden, die ihrer Natur gemäß erhöhte Risiken bergen – wie etwa Dating-Plattformen. Demgegenüber sollten allgemeine Kommunikationsdienste und unspezifisch ausgerichtete Social-Media-Plattformen explizit vom Erfordernis der Altersverifikation ausgenommen werden.

Änderungsvorschläge:

- **Art. 4 Abs. 3** sollte wie folgt geändert werden:

  „Anbieter interpersoneller Kommunikationsdienste, die gemäß der nach Artikel 3 durchgeführten oder aktualisierten Risikobewertung ein Risiko der Nutzung ihrer Dienste zum Zwecke der Anwerbung von Kindern festgestellt haben, ***das in der Art ihres Dienstes angelegt ist,*** *ergreifen die erforderlichen Maßnahmen zur Altersüberprüfung und -bewertung, um die Nutzer im Kindesalter zuverlässig zu identifizieren, wie dies bei Dating-Diensten in ihren Diensten der Fall sein könnte, und so in die Lage zu versetzen, die erforderlichen Abhilfemaßnahmen zu treffen.* ***Dies gilt nicht für Kommunikationsdienste mit allgemeinem Zuschnitt und insbesondere nicht für solche, von denen vernünftigerweise angenommen werden kann, dass Nutzer sich darüber von einem Rechtsanwalt beraten lassen oder anderweitig besonders gewichtige Grundrechte darüber ausüben."***

  (Änderungen hervorgehoben)

- ***Art. 6 Abs. 1 lit. c)*** *sollte wie folgt geändert werden:*

  „die erforderlichen Maßnahmen zur Altersüberprüfung und -bewertung ergreifen, um die Nutzer ihrer Dienste im Kindesalter zuverlässig zu identifizieren, damit sie die unter Buchstabe b genannten Maßnahmen ergreifen können. ***Aufgrund von Risiken, die nicht in der Natur des jeweiligen Dienstes liegen, und für den Zugang zu Kommunikationsdiensten mit allgemeinem Zuschnitt und insbesondere zu solchen, von denen vernünftigerweise angenommen werden kann, dass Nutzer sich darüber von einem Rechtsanwalt beraten lassen oder anderweitig besonders gewichtige Grundrechte darüber ausüben, dürfen Maßnahmen zur Altersüberprüfung nicht angewendet werden."***

3. Behördliche Aufsicht

Der Entwurf sieht eine unabhängige Aufsicht mit Parallelen zum EU-Datenschutz-Regime vor.

3.1 Aufsichtsbefugnisse

Die in Art. 27 Abs. 1 lit. a und b vorgesehenen Aufsichtsbefugnisse bergen das Risiko, dass Aufsichtsmaßnahmen gegenüber Rechtsanwältinnen und Rechtsanwälten ergehen und so Mandatsgeheimnisse offenbart werden.

So soll die Aufsichtsbehörde gemäß Art. 27 Abs. 1 lit. a) neben den eigentlich verpflichteten Diensteanbietern Auskünfte auch von allen anderen Personen verlangen können, „die im Rahmen ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit handeln und nach vernünftigem Ermessen Kenntnis von Informationen über einen mutmaßlichen Verstoß gegen diese Verordnung haben können“. Demnach könnten auch Rechtsanwältinnen oder Rechtsanwälte, die Diensteanbieter beraten zur Auskunft über Mandatsinhalte herangezogen werden, was mit dem Mandatsgeheimnis nicht zu vereinbaren wäre.

Darüber hinaus sind in Art. 27 Abs. 1 lit. b) Vorort-Untersuchungen mit einer Befugnis zur Kopie und Beschlagnahme von Informationen – ungeachtet von der Natur des Datenträgers – vorgesehen. Dies birgt die Gefahr, dass etwa gehostete Akteninhalte oder anwaltliche Korrespondenzen beschlagnahmt und den Aufsichtsbehörden offenbart werden. Auch dies ist weder mit dem Mandatsgeheimnis noch der anwaltlichen Unabhängigkeit vereinbar.

Entsprechende Beeinträchtigungen des Mandatsgeheimnisses und der anwaltlichen Unabhängigkeit müssen dringend durch entsprechende Beschränkungen der Aufsichtsbefugnis verhindert werden. Bei deren Ausgestaltung bietet sich angesichts der gesetzgeberischen Kompetenzverteilung in systematischer Hinsicht eine Orientierung an den datenschutzrechtlichen Normen des Art. 90 Abs. 1 DS-GVO bzw. des § 29 BDSG an. Dabei gilt es inhaltlich jedoch zu beachten, dass diese Normen sich in der Praxis als unzureichend erwiesen haben. So musste festgestellt werden, dass Aufsichtsbehörden ihre durch diese Vorschriften nicht ausgeschlossene Befugnis, gemäß Art. 58 Abs. 1 lit. a DS-GVO Auskunft zu verlangen, zu Befragungen zu Mandatshinhalten nutzten. Die Befugnisbeschränkung muss daher insoweit umfassender erfolgen und der Tatsache Rechnung tragen, dass ein Bruch der anwaltlichen Verschwiegenheit regelmäßig nicht zu rechtfertigen ist.

Änderungsvorschlag:

- **Art. 27** sollte daher wie folgt um einen dritten Absatz ergänzt werden:

  „Aufsichtsmaßnahmen gegenüber Berufsgeheimnisträgern sind unzulässig. Die Mitgliedstaaten können die Befugnisse der Aufsichtsbehörden im Übrigen abweichend regeln und weiter einschränken, soweit dies notwendig ist, um den Schutz von Berufsgeheimnissen und gleichwertigen Verschwiegenheitspflichten zu gewährleisten. Jeder Mitgliedstaat teilt der Kommission bis zum xx.xx.20xx die Vorschriften mit, die er aufgrund von Satz 1 erlässt, und setzt sie unverzüglich von allen weiteren Änderungen dieser Vorschriften in Kenntnis.“.

3.2 Verschwiegenheit

Die in Art. 26 des Entwurfs vorgesehene Verschwiegenheit der Aufsicht muss beibehalten werden und wie oben unter 1.1.6 Insbesondere: fehlender Schutz von Berufsgeheimnissen vorgeschlagen ergänzt werden.

4. Verschwiegenheit der Zentralstelle

Die in Art. 74 des Entwurfs vorgesehene Verschwiegenheit der Aufsicht muss beibehalten werden und wie oben unter 1.1.6 Insbesondere: fehlender Schutz von Berufsgeheimnissen vorgeschlagen insbesondere um eine Verschwiegenheitspflicht gegenüber doppelfunktionalen Führungspersonen im Sinne der Art. 56 und 61 ergänzt werden, um zu vermeiden, dass vertrauliche Informationen durch Personenidentität faktisch einer anderen Stelle und insbesondere Europol gegenüber offenbart werden.

5. Verhältnis zum übrigen Datenschutzrechtsregime und Datenschutz-Folgenabschätzung

Art. 1 Abs. 3 lit. d erklärt die Geltung des bestehenden Datenschutzrechtsregimes zustimmungswürdiger Weise für unberührt. Indes sieht Art. 7 Abs. 3 Unterabsatz 2 Satz 2 lit. b eine Datenschutz-Folgenabschätzung nur für Fälle der Erkennung einer Kontaktaufnahme vor, obwohl eine Risikoabschätzung im Rahmen des – ohnehin anwendbaren – Art. 35 auch hinsichtlich der Erkennung von Missbrauchsinhalten zu dem Ergebnis regelmäßig führen wird, dass eine Datenschutz-Folgenabschätzung durchgeführt werden muss. Die Klarstellung des Art. 7 Abs. 3 Unterabsatz 2 Satz 2 lit. b sollte daher auch auf Fälle der Erkennung von Missbrauchsinhalten ausgeweitet werden. Anderenfalls könnte bei Rechtsanwendern der falsche und unbedingt zu vermeidende Eindruck entstehen, dass eine Datenschutz-Folgenabschätzung in diesen Fällen entbehrlich sei.

Änderungsvorschlag:

- **Art. 7 Abs. 3 Unterabsatz 2 Satz 2 lit. b** sollte daher wie folgt geändert werden:

  „(b) wenn der Entwurf des Durchführungsplans eine beabsichtigte Aufdeckungsanordnung ~~***in Bezug auf die Anwerbung von Kindern***~~ *betrifft, bei der es sich nicht um die Verlängerung einer zuvor ergangenen Aufdeckungsanordnung ohne wesentliche Änderungen handelt, eine Datenschutz-Folgenabschätzung und ein vorheriges Konsultationsverfahren gemäß Artikel 35 bzw. Artikel 36 der Verordnung (EU) 2016/679 in Bezug auf die im Durchführungsplan dargelegten Maßnahmen durchführen;“*

6. Evaluation

Art. 85 sieht eine Evaluation der Verordnung alle 5 Jahre vor. Gemäß Erwägungsgrund 77 sollen dabei insbesondere die Auswirkungen auf Vertraulichkeitsgrundrechte beleuchtet werden. Der vorliegende Entwurf verdeutlicht, wie erforderlich es ist, Entscheidungsträgern die Bedeutung des Mandatsgeheimnisses in diesem Regelungszusammenhang vor Augen zu führen. Aus diesem Grund sollte das Mandatsgeheimnis in einer etwaigen Verordnung explizit als Evaluationskriterium aufgeführt werden.

Änderungsvorschlag:

- Erwägungsgrund 77 sollte daher wie folgt ergänzt werden:

  „Die Bewertung soll anhand der Kriterien der Effizienz, Notwendigkeit, Wirksamkeit, Verhältnismäßigkeit, Relevanz, Kohärenz und des Mehrwerts für die Union vorgenommen werden. Sie sollte das Funktionieren der verschiedenen in dieser Verordnung vorgesehenen operativen und technischen Maßnahmen bewerten, einschließlich der Wirksamkeit der Maßnahmen zur Verbesserung der Aufdeckung, Meldung und Beseitigung von sexuellem Missbrauch von Kindern im Internet, der Wirksamkeit der Schutzmechanismen sowie der Auswirkungen auf potenziell betroffene Grundrechte, die unternehmerische Freiheit, das Recht auf Privatleben,

*~~**und***~~ *den Schutz personenbezogener Daten **und Berufsgeheimnisse**. Die Kommission sollte auch die Auswirkungen auf potenziell betroffene Interessen Dritter bewerten.“*

7. Alternative Ansätze

Die Bundesrechtsanwaltskammer spricht sich für den Rückgriff auf andere Methoden zur Bekämpfung des online-Kindesmissbrauchs aus. In erster Linie muss eine verstärkte Aufklärungsarbeit unter Einbeziehung von Akteuren wie Sozialarbeitern, Betroffenenhilfe, Schulen sowie Ärztinnen und Ärzten stattfinden.

Begrüßenswert ist der Vorschlag im EP-Berichtsentwurf für ein Victims‘ Consultative Forum (ÄA 273 für einen neuen Art. 66 a), das in diesem Zusammenhang eine Rolle spielen könnte.

Angeregt werden ferner Meldekanäle bzw. Beschwerdesysteme gerade auch für jugendliche Nutzer, so dass diese Inhalte vertraulich melden und dagegen vorgehen können.

Grundsätzlich ist eine Beschränkung auf gezielte Einzelfallmaßnahmen infolge entsprechender Ermittlungen und auf richterliche Anordnung der vorzugswürdige Ansatz.

* * *