BUNDESRECHTSANWALTSKAMMER

Stellungnahme Nr. 11/2026
Februar 2026
Registernummer: 25412265365-88

Trilog und Ratspositionierung zum Kampf gegen sexuellen Kindesmissbrauch im Internet (sog. „Chatkontrolle“)

Mitglieder des Ausschusses Datenschutzrecht

RA Klaus Brisch, LL.M.
RA Malte Dedden
RA Michael Dreßler
RA Peter Hense,
RA Prof. Dr. Armin Herb, (Vorsitzender)
RAin Heike Kraus, MLE, LL.M
RA Jörg Martin Mathis
RAin Simone Rosenthal
RA Dr. Hendrik Schöttle
RA Sebastian Schulz
RA Dr. Volker Schumacher

RA André Haug, Vizepräsident, Bundesrechtsanwaltskammer
RA Sebastian Aurich, LL.M., Bundesrechtsanwaltskammer
Ass. jur. Frederic Boog, LL.M., Bundesrechtsanwaltskammer, Brüssel

Mitglieder des Ausschusses Europa

RA Dr. Sebastian Cording
RA Dr. Hans-Joachim Fritz
RA Marc André Gimmy
RAin Dr. Margarete Gräfin von Galen (Vorsitzende)
RA Andreas Max Haak
RA Dr. Frank J. Hospach
RA Dr. Christian Lemke
RA Maximilian Müller
RAin Dr. Kerstin Niethammer-Jürgens
RA Dr. Hans-Michael Pott

RA Jan K. Schäfer, LL.M.
RAin Stefanie Schott
Prof. Dr. Gerson Trüg
RA Andreas von Máriássy

RA Dr. Christian Lemke, Vizepräsident, Bundesrechtsanwaltskammer
RAin Astrid Gamisch, LL.M., Bundesrechtsanwaltskammer, Brüssel
Ass. jur. Nadja Wietoska, Bundesrechtsanwaltskammer, Brüssel
Ass. jur. Frederic Boog, LL.M., Bundesrechtsanwaltskammer, Brüssel
Ass. jur. Sarah Pratscher, Bundesrechtsanwaltskammer, Brüssel

Mitglieder des Ausschusses Medienrecht

RA Piet Bubenzer
RA Dr. Till Dunckel (Vorsitzender)
RA Jens Ferner
RA Prof. Dr. Jan Hegemann
RA Dr. Jonas Kahl
RA Julian Modi
RA Dr. Jasper Prigge
RA Nils Pütz
RAin Gräfin von Reichenbach Freifrau von Thüngen

RAin Sabine Fuhrmann, Vizepräsidentin Bundesrechtsanwaltskammer
RAin Friederike Wohlfeld**,** Bundesrechtsanwaltskammer

Verteiler: Europäische Kommission

Bundeskanzleramt
Bundesministerium für Justiz und für Verbraucherschutz
Bundesministerium des Innern und für Heimat
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
Landesdatenschutzbeauftragte
Rechtsausschuss 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
Bundessteuerberaterkammer
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.

Inhalt

Gegenstand

Gegenwärtig ermöglicht die zwecks Bekämpfung des sexuellen Missbrauchs von Kindern im Internet interimsmäßig erlassene sogenannte „Übergangsverordnung“ VO (EU) 2021/1232 Online-Diensteanbietern eine freiwillige Durchleuchtung von Inhalten mit dem Ziel, zum Schutz von Kindern Missbrauchsdarstellungen zu erkennen, zu entfernen und zu verfolgen. Da diese Verordnung am 3. April 2026 ausläuft, wird seit Jahren um eine Nachfolgeregelung gerungen. Diverse hierzu vorgelegte Entwürfe sahen zwischenzeitlich für die Zukunft sogar eine anlasslose Pflicht zur Erkennung, Meldung und Entfernung solcher Inhalte vor.[1] Beide Gestaltungen – freiwillige oder verpflichtende Durchleuchtung – sind bzw. wären mit massiven Eingriffen in die Vertraulichkeit der über Online-Dienste abgewickelten Kommunikation und der korrespondierenden Grundrechte verbunden. Besonders kritisch ist dies in Konstellationen, in denen solche Dienste auf Wunsch bzw. aufseiten der Mandantschaft zur Mandatskommunikation genutzt werden. Inhaltserkennungen wurden und werden daher von der Bundesrechtsanwaltskammer in jeder Form abgelehnt (vgl. Stellungnahmen 65/2020 und 22/2023).

Nachdem sich zuletzt keine Mehrheit für unmittelbar verpflichtende Durchleuchtungspflichten herstellen ließ, hat sich der Rat der EU in einer Allgemeinen Ausrichtung auf eine Fortführung der bisherigen freiwilligen Maßnahmen geeinigt.[2] Die Allgemeine Ausrichtung geht dabei jedoch deutlich über die bisherigen Regelungen hinaus: Neben den Erlaubnistatbeständen für freiwillige Durchleuchtungen sollen Anbieter von risikobehafteten Diensten künftig zur Minimierung der entsprechenden Risiken verpflichtet werden. Grundlage soll ein ausdifferenziertes Risikobewertungssystem sein. Wie bereits nach dem Vorschlag der EU-Kommission soll nach der Vorstellung des Rates Hosting-Diensten die freiwillige Durchleuchtung ermöglicht werden. Suchmaschinen sollen mit Blick auf von diesen ausgegebene Ergebnisse ggf. Löschungspflichten unterfallen. Ferner bekennt sich der Rat im Grundsatz zur Verschlüsselung.

In dem am 10.11.2025 zwischen den gesetzgebenden Organen der EU begonnenen informellen Trilog soll nun rechtzeitig vor Auslauf der Übergangsverordnung ein für alle beteiligten Institutionen zustimmungsfähiger Gesetzesvorschlag erarbeitet werden. Die vorliegende Stellungnahme nimmt die **Allgemeine Ausrichtung des Rates** in den Blick. Nicht näher eingegangen wird auf die Beschlüsse des Parlaments[3] bzw. den ursprünglichen Vorschlag der Kommission.[4]

Kurzbewertung

Die im Vergleich zu früheren Vorschlägen teilweise abgemilderten Vorschläge der Allgemeinen Ausrichtung des Rates ermöglichen weiterhin weitgehende, flächendeckende und anlasslose Einblicke in die Online-Korrespondenz und -Aktivität aller Bürgerinnen und Bürger. Sie greifen insoweit erheblich in deren Grundrechte ein. In der Zusammenschau steht eine **anlasslose Massenüberwachung** zu befürchten, die **insbesondere mit Blick auf das Mandatsgeheimnis abzulehnen** ist:

- Die Abkehr von einer unmittelbaren Pflicht zur Erkennung von Missbrauchsmaterial ist zu begrüßen. Mit der geplanten Fortführung freiwilliger Durchleuchtung verbleiben jedoch inakzep-

[1] Vgl. etwa Verordnungsentwurf der Kommission (COM 2022/209 final) – dieser sah anlasslose Aufdeckungspflichten sowie Melde- und Entfernungspflichten vor, was eine umfassende Durchleuchtung elektronischer Kommunikation durch die Diensteanbieter mit sich bringen würde.

[2] Allgemeine Ausrichtung des Rates vom 13.11.2025, hier abrufbar: https://data.consilium.europa.eu/doc/document/ST-15318-2025-INIT/en/pdf (Stand 19.11.2025)

[3] Positionierung des LIBE-Ausschusses vom 14.11.2023, angenommen vom Plenum am 22.11.2023, abrufbar unter: https://www.europarl.europa.eu/doceo/document/A-9-2023-0364_EN.html (Stand: 19.11.2025)

[4] Vgl. zu letzterem indes bereits BRAK-Stellungnahme 22/2023

table Risiken für die Vertraulichkeit der Online-Kommunikation und insbesondere der über solche Dienste abgewickelten Mandatskorrespondenz. **Auch die Fortführung der freiwilligen Durchleuchtungsmöglichkeit ist daher abzulehnen.**

- **Keinesfalls** darf die geplante Pflicht zur Erkennung und Minimierung von Risiken zu einer **mittelbaren Einführung von Durchleuchtungspflichten** werden. Sofern die freiwillige Durchleuchtungsmöglichkeit beibehalten wird, sollte die vom Rat zur Abwendung dieser Gefahr vorgesehene Klarstellung, dass eine solche Auslegung nicht bezweckt werde, unbedingt beibehalten werden.
- Das begrüßenswerte **Bekenntnis zur Verschlüsselung darf nicht durch Client-seitige Maßnahmen unterlaufen werden**. Insbesondere dürfen solche weder, zwecks Risikoklassifizierung, noch zur Risikominderung zugelassen oder gar u. U. implizit verpflichtend postuliert werden.
- Begrüßenswert ist der in Erwägungsgrund 12a angestrebte **Schutz von Berufsgeheimnissen**. Dieser wird jedoch **nicht hinreichend gewährleistet**.
- Anreize und eine teilweise Pflicht zur Durchführung von **Altersverifikationen begrenzen die Möglichkeiten der anonymen Kommunikation im Internet** und engen insbesondere die Möglichkeit ein, von Dritten unerkannt anwaltlichen Rat in Anspruch zu nehmen. Dies ist nicht akzeptabel. Es bedarf mindestens einer Ausnahme für alltäglich genutzte Kommunikationsmittel.

Die BRAK mahnt einen **Verzicht auf die angestrebte Verordnung** an und schlägt hilfsweise konkrete **Maßnahmen zur Begrenzung ihrer negativen Auswirkungen** vor.

Stellungnahme im Einzelnen

Die BRAK hat in ihren Stellungnahmen zum Verordnungsentwurf der Kommission (COM 2022/209 final) und zur Übergangsverordnung (EU) 2021/1232 bereits massive Bedenken zur anlasslosen Durchleuchtung von Kommunikationsinhalten und die hohe Invasivität der mit ihr einhergehenden Eingriffe gerade in die Rechte von Opfern solcher Straftaten, von Jugendlichen generell, sowie von Mandantinnen und Mandanten geäußert. Diese Bedenken werden durch die in der Ausrichtung des Rates festgehaltenen Regelungsvorschläge nicht ausgeräumt, wenn auch mit Blick auf inzwischen aufgegebene Regelungsvorschläge teilweise obsolet.

1.1 Tatsächlicher und rechtlicher Rahmen

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. All dies wäre nicht mehr möglich, sofern die nach dem Verordnungsvorschlag zugelassene Erkennung von Inhalten durch Kommunikations- und Hosting-Anbieter realisiert wird.

Zudem muss Anwältinnen und Anwälten in der modernen arbeitsteiligen Welt die Möglichkeit bleiben, unter besonderen Sicherheitsvorkehrungen vertrauensvoll Hosting-Dienste in Anspruch zu nehmen. Wo Dienste-Anbieter Inhalte freiwillig durchleuchten, wäre dies nicht möglich.

Je stärker der möglicherweise mit abstrakten Vorgaben zur Risikominimierung geschaffene Anreiz zur Implementierung entsprechender Inhaltserkennungsmaßnahmen ist, desto geringer wird der Raum, in dem Kanzleien vertraulich mit ihrer Mandantschaft kommunizieren bzw. Hosting-Dienste nutzen können.

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.

1.2 Geeignetheit und Verhältnismäßigkeit

Nach wie vor bestehen erhebliche Zweifel schon an der Geeignetheit der in der Verordnung vorgesehenen Maßnahmen zur effektiven Bekämpfung von Kindesmissbrauch, insbesondere wenn, wie in der Position des Rates enthalten, auch Textnachrichten erfasst sein sollen. Insbesondere die Aufdeckung neuer Materialien durch andere Methoden als das sog. Hashing, welche der Rat in seine Allgemeine Ausrichtung mit aufgenommen hat, vor allem auch unter Einsatz künstlicher Intelligenz, leidet an einer nicht hinnehmbaren Fehlerintensität. Hinzukommt, dass die Maßnahmen durch Private durchgeführt werden sollen, welchen eine Sicherstellung des erforderlichen Grundrechtsschutzes nicht zumutbar ist und diesen auch nicht anvertraut werden sollte. Solche Eingriffe sind mithin nicht verhältnismäßig, hierzu ausführlich die o.g. Stellungnahmen.

1.3 Grundrechtsverletzungen auch auf freiwilliger Basis rechtswidrig

Dass die Diensteanbieter die Erkennung nun nur noch auf freiwilliger Basis durchführen sollen, wie es bereits in der seit Juli 2021 geltenden Übergangsverordnung vorgesehen ist, mag eine scheinbare Entlastung darstellen. Jedoch ändert die Freiwilligkeit nichts an der Unverhältnismäßigkeit und Ungeeignetheit dieser Maßnahmen, noch dazu wenn sie flächendeckend ermöglicht werden. Ermöglicht der Gesetzgeber solche Maßnahmen anstatt sie zu unterbinden, wird er seinen Schutzaufträgen aus Art. 6 Abs. 1 Satz 1, Abs. 3 lit. c EMRK Art. 8 Abs. 1 EMRK, Art. 7 GRCh, Art. 47 Abs. 1 Satz 2 GRCh – bzw. mit Blick auf die im Rat mitwirkende Bundesregierung Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 2, Art. 20 Abs. 2, Art. 103 Abs. 1 GG – nicht ansatzweise gerecht. Dies verstößt gegen europäisches Primär und Verfassungsrecht.

Die BRAK spricht sich mithin auch gegen die freiwillige Durchleuchtung der Kommunikation aus.

1.4 Keine Durchleuchtungspflicht durch die Hintertür

In Gestalt der in der Allgemeinen Ausrichtung neu vorgesehenen Pflichten zur Risikoanalyse und -minimierung werden Anreize für Diensteanbieter geschaffen, CSAM-Scanning als faktisch verpflichtend durchzuführen und Technologien zu verwenden, die die Vertraulichkeit der Kommunikation verletzen. Dies ist auch die Bewertung der Bundesdatenschutzbeauftragten[5]. Im Vergleich zu früheren Entwurfsfassungen begrüßenswert - und **im Falle der Beibehaltung der freiwilligen Durchleuchtung und der**

[5] https://social.bund.de/@bfdi/115497859112865101

Pflicht zur Risikominimierung unbedingt erforderlich - ist daher die vom Rat als Erwägungsgrund 17a vorgeschlagene Klarstellung *„Nothing in this Regulation should be understood as imposing any detection obligations on providers."*

1.5 Anreize zu Erkennungsmaßnahmen vermeiden

Auch die Klarstellung des Erwägungsgrundes 17a der Ratspositionierung wird nicht ausschließen können, dass Dienste-Anbieter im Wege eigener betriebswirtschaftlicher Risikoanalysen zu der Einschätzung gelangen, dass sich die mit der Pflicht zur Risikoerkennung und -minimierung einhergehenden Kosten und Risiken betriebswirtschaftlich am günstigsten durch Aufdeckungsmaßnahmen begrenzen lassen. Damit stünde eine Ausweitung freiwilliger Durchleuchtungen weiter zu befürchten.

Über den vorgeschlagenen Erwägungsgrund 17a hinaus muss daher auf die Kombination aus freiwilliger Durchleuchtungsbefugnis und Risikominimierungspflicht verzichtet werden.

1.6 Schutz von Berufsgeheimnissen in nicht-öffentlichen Kommunikationsdiensten

Die BRAK begrüßt grundsätzlich Erwägungsgrund 12a, in welchem u.a. dem **Berufsgeheimnis** unterfallende, sowie nicht der Öffentlichkeit zugängliche Kommunikationsdienste vom Anwendungsbereich der Verordnung ausgenommen werden. Davon wird auch das besondere elektronische Anwaltspostfach erfasst, welches Anwältinnen und Anwälten in Deutschland als sicherer Übermittlungsweg im Rahmen des elektronischen Rechtsverkehrs zur Verfügung steht. Dies sollte klargestellt werden mittels folgender Ergänzung:

> *"In the light of the more limited risk of their use (…). Accordingly, this Regulation should not apply to interpersonal communications services that are not available to the general public and the use of which is instead restricted to persons involved in the activities of a particular company, organisation, body or authority* ***or of a profession being subject to professional secrecy."***

Ferner sollte dieser Erwägungsgrund im Regelungsteil gespiegelt werden.

1.7 Schutz von Berufsgeheimnissen in bislang nicht ausgenommenen (öffentlichen) Diensten

Viele Mandantinnen und Mandanten sind aus unterschiedlichen Gründen teils nicht in der Lage oder willens, Ende-zu-Ende-verschlüsselt mit ihrer Rechtsanwaltskanzlei zu kommunizieren. Insbesondere mit Blick auf Eilfälle muss vermieden werden, dass solche Personen durch Befürchtungen einer Offenbarung ihrer Korrespondenz von der Inanspruchnahme anwaltlicher Beratung oder Vertretung abgehalten werden. Das gilt auch für Opfer, Täter und Beschuldigte sexualisierter Gewalt und insbesondere bei erstmaliger Kontaktaufnahme zur Kanzlei.

Die Vertraulichkeit anwaltlicher Korrespondenz muss daher auch jenseits der Anwendungsfälle des Erwägungsgrundes 12a geschützt werden. Mandatskorrespondenz muss sowohl von freiwilligen Erkennungsmaßnahmen als auch bei etwaigen Aufdeckungsanordnungen ausgenommen bleiben.

Da jedoch keine technischen Möglichkeiten zur Aussonderung von Mandatskorrespondenz ersichtlich sind, die nicht ihrerseits das Mandatsgeheimnis verletzten würden,[6] müssen Erkennungsmaßnahmen im Bereich der Kommunikations- und Hosting-Dienste in Gänze unterbleiben.

Sofern die Möglichkeit oder gar eine Pflicht zur Erkennung von Missbrauchsdarstellungen dennoch auch in diesen Bereichen beibehalten wird, bedürfte es mindestens einer Regelung zum Schutz von Berufsgeheimnissen.

Wie bereits in ihrer Stellungnahme[7] zum Vorschlag der Kommission, fordert die BRAK daher die Aufnahme eines konkreten Artikels über das Bekenntnis im Erwägungsgrund hinaus.

Regelungsvorschlag:

„Art. Xx - Schutz von Berufsgeheimnissen

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. *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.*
3. *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.*

1.8 Ausweitung des Amtsgeheimnisses auf Private erforderlich

Die für staatliche Stellen geltenden Verschwiegenheitsanforderungen dürfen durch vorgelagerte Ermittlungstätigkeiten der Diensteanbieter nicht ausgehebelt werden. Dort tätige Personen sind daher in gleicher Weise auf das Amtsgeheimnis zu verpflichten.

Regelungsvorschlag:

„Für Mitarbeitende von Diensteanbietern sowie von deren Auftragnehmern gelten mit Blick auf nach dieser Verordnung erhobene oder übermittelte Informationen die im jeweiligen Mitgliedsstaat für staatliche Ermittlungsstellen geltenden Verschwiegenheitsvorschriften entsprechend.

---

[6] Regelmäßig wird der Mandatsbezug nur durch dessen, wenn auch begrenzte, Offenbarung feststellbar sein, wodurch das Mandatsgeheimnis bereits beeinträchtigt wäre.

[7] BRAK-Stellungnahme 22/2023

Im Mindesten gilt Art. 339 AEUV. Satz 1 und 2 gelten auch für Organe, freie Mitarbeiter oder sonstige Beschäftigte.“

1.9 Personenbezogene Daten

Zur Vermeidung nachgelagerter Risiken sollte klargestellt werden, 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. Dadurch würden zugleich die allgemeinen Vertraulichkeitsrisiken des Verordnungsvorschlags etwas mitigiert.

Regelungsvorschlag:

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

1.10 Altersverifizierung

Altersverifikationen schränken die Möglichkeit ein, sich zum Schutz der eigenen Person unerkannt im Internet zu bewegen. Mit Blick auf das anwaltliche Mandatsgeheimnis verengen sie den Raum, in dem anwaltliche Beratung von Dritten unerkannt in Anspruch genommen werden kann.

Der Verordnungsvorschlag listet das Vorhandensein von Altersverifikationsmöglichkeiten in Art. 3 Abs. 2 lit. b als im Rahmen der obligatorischen Risikoanalyse zu berücksichtigendes Kriterium auf und schafft damit einen Anreiz zur Implementierung von Altersverifikationen. Ferner sieht er in Art. 4 Abs. 3 für interpersonelle Kommunikationsdienste, bei denen ein Risiko zur sexuellen Kontaktanbahnung gegenüber Kindern erkannt wurde (sog. Grooming) verpflichtende Altersverifikationen vor.

Zwar ist zu begrüßen, dass der Rat in seiner Allgemeinen Ausrichtung die damit für die Betroffenen einhergehenden Risiken durch – im Wesentlichen klarstellende – Formulierungen und Schutzvorschriften in Erwägungsgrund 16a bzw. Art. 6 Abs. 1 lit. c zu minimieren sucht. Es verbleibt jedoch die Gefahr, dass Altersverifizierungen künftig übermäßig häufig und insbesondere auf weithin genutzten Kommunikationsdiensten mit unterschiedlich risikogeneigten Anwendungsfeldern eingeführt werden.

Um nicht die Möglichkeit zu beeinträchtigen, sich unerkannt im Internet zu bewegen und insbesondere anwaltliche Beratung in Anspruch nehmen zu können, sollten für interpersonellen Kommunikationsdienste mit unterschiedlich risikogeneigten Anwendungsfeldern, die überwiegend zu allgemeinen Kommunikationszwecken verwendet werden, Ausnahmen von der Pflicht zur Altersverifikation vorgesehen werden.

Regelungsvorschlag:

Ergänzung in Art. 4 Abs. 3 am Ende:

„Interpersonelle Kommunikationsdienste mit unterschiedlich risikogeneigten Anwendungsfeldern, die überwiegend zu allgemeinen Kommunikationszwecken eingesetzt werden, sind nach dieser Verordnung nicht zur Altersverifikation verpflichtet.“

1.11 Verschlüsselung

Die BRAK begrüßt grundsätzlich das ausdrückliche Bekenntnis zur Verschlüsselung in Erwägungsgrund 26. Offen bleibt dabei jedoch, ob die gewählte Formulierung auch ein sog. Client Side Scanning ausschließt. Dabei handelt es sich um Scans am Gerät des Nutzers, bevor diese verschlüsselt und versendet werden können, welche mittels lokal verorteter Software durchgeführt werden, so dass die Verschlüsselung umgangen werden kann.

Auch eine derartige Inhaltsprüfung ist, wie der juristische Dienst des Rates der EU bereits zutreffend herausgestellt hat, nicht mit Art. 7 und Art. 8 der Grundrechtecharta zu vereinbaren. Zwar dürfte Client-Side-Scanning als Unterfall der Umgehung nachdem Wortlaut des Erwägungsrundes 26 der Allgemeinen Ausrichtung des Rates „*nothing shall be interpreted as … circumventing …end-to-end encryption…*“ ausgeschlossen sein. Jedoch legt die im gleichen Satz enthaltene Würdigung von Technologien, die die Einhaltung der Anforderungen der Verordnung unter Wahrung der Ende-zu-Ende-Verschlüsselung ermöglichten („*Having regard to the availability of technologies that can be used to meet the requirements of this Regulation whilst still allowing for end-to-end encryption*“) das Gegenteil nahe. Es bedarf daher eines expliziten Ausschlusses des Client-Side-Scannings.

Regelungsvorschlag:

Ergänzung in Erwägungsgrund 26 am Ende:

„Als Umgehung in diesem Sinne ist auch Client-Side-Scanning zu betrachten“.

1.12 Evaluierung

Besorgniserregend ist ferner, dass in der Vorschrift, auf deren Grundlage die Kommission, wie bei Rechtsakten üblich, dazu aufgefordert wird, die Verordnung regelmäßig zu evaluieren, gleichsam eine Abkehr von der Aufrechterhaltung der Verschlüsselung, sowie von der Freiwilligkeit, enthalten sind (vgl. Artikel 85 Nr. 1a). So sollen danach die Erforderlichkeit verpflichtender Inhaltsdurchleuchtungen sowie technische Möglichkeiten der Inhaltserkennung auf Ende-zu-Ende-verschlüsselten Diensten betrachtet werden. Dies wirkt gleichsam wie eine Ankündigung künftiger Maßnahmen. Sollte eine künftige Evaluierung der Verordnung ergeben, dass die in ihr enthaltenen Maßnahmen nicht wirksam zum Kampf gegen online-Kindesmissbrauch beitragen, so ist zu erwarten, dass dies nicht am Freiwilligkeitskriterium oder der Verschlüsselung, sondern, wie vielfach beschrieben, an der geringen Geeignetheit der Maßnahmen selbst liegen wird.

* * *