DIE ÖSTERREICHISCHEN RECHTSANWÄLTE

Wien, 09.05.2023

ÖRAK-Stellungnahme Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (COM(2022) 209), einschließlich Berichtsentwurf Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres (2022/0155(COD)

Der Österreichische Rechtsanwaltskammertag (ÖRAK) ist die gesetzlich eingerichtete Vertretung der Rechtsanwälte in Österreich und als solche zur Wahrung der Rechte und Angelegenheiten sowie zur Vertretung der österreichischen Rechtsanwälte auf nationaler, europäischer und internationaler Ebene berufen. Als solcher obliegen ihm besonders die Erstattung von Gesetzesvorschlägen und Stellungnahmen zu Gesetzesentwürfen sowie die Anzeige von Mängeln der Rechtspflege und Verwaltung bei der zuständigen Stelle und die Erstattung von Vorschlägen zur Verbesserung von Rechtspflege und Verwaltung.

Der Österreichische Rechtsanwaltskammertag kommentiert im Folgenden **sowohl den Verordnungsvorschlag** zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (COM(2022) 209) als auch **einzelne neue Vorschläge aus dem Berichtsentwurf** zum Vorschlag, der dem Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) vorgelegt wurde (2022/0155(COD)). In Anbetracht der Komplexität des vorliegenden Dossiers sind die Anmerkungen des ÖRAK nicht als abschließend zu betrachten.

Der ÖRAK unterstreicht nachdrücklich die Wichtigkeit des effektiven Kampfes gegen den sexuellen Missbrauch von Kindern in allen Mitgliedstaaten der Europäischen Union und darüber hinaus. Nach Auffassung des ÖRAK verstößt der vorgelegte Verordnungsvorschlag allerdings teilweise massiv gegen **Grundrechte** und kann in der vorliegenden Fassung durch die Co-Gesetzgeber nicht angenommen werden, auch bestehen Zweifel an dessen **Rechtsstaatlichkeit**, insbesondere im Hinblick auf Befugnisse der ermittelnden Behörden sowie die Gefahr der Eröffnung von Ermittlungsverfahren gegen unschuldige Personen.

Österreichischer Rechtsanwaltskammertag
Wollzeile 1-3 | 1010 Wien | Tel. +43 (1) 535 12 75 | Fax +43 (1) 535 12 75-13 | rechtsanwaelte@oerak.at | www.rechtsanwaelte.at

Folgend Anmerkungen in der Reihenfolge der Elemente des Verordnungsvorschlags:

Die im Vorschlag vorgesehenen **Aufdeckungsanordnungen, insbesondere Artikel 7 und 8 VO-Vorschlag**, sind abzulehnen.

Grundsätzlich sieht der Vorschlag die Möglichkeit einer Durchleuchtung von Inhalten unterschiedslos aller Nutzer von Hosting- und interpersonellen Kommunikationsdiensten vor, sodass niemand mehr auf die Vertraulichkeit der Kommunikation zählen kann. Nach Auffassung des ÖRAK verstößt dies gegen **Grundrechte,** namentlich EMRK und GRC.

Das vorgeschlagene komplexe System, das zu einer Anordnung führt, ändert nichts an dem damit einhergehenden ungerechtfertigten und unverhältnismäßigen Grundrechtseingriff ggü Personen, die gerade nicht unter einem Tatverdacht oä stehen. Dasselbe gilt für den Einwand, dass es sich um eine Ausnahmemaßnahme handeln solle.

Die Häufigkeit bzw Seltenheit des Scannens ist ebenfalls kein Argument zur Abschwächung des Eingriffs. Im digitalisierten Zeitalter befinden sich selbst Jahre zurückliegende persönliche Daten zB in Emailpostfächern oder Chats. Auch das einmalige Scannen führt demnach zum Zugriff auf fast alle persönlichen Daten einer Person seit Beginn der Nutzung eines Dienstes.

Herauszustellen ist auch, dass der Vorschlag gerade nicht auf Netzwerke im Darknet abstellt, deren Nutzern man ggf mehrheitlich die Nutzung zu bestimmten kriminellen Aktivitäten nachweisen kann, sondern um alltägliche Internetdienste. Dieser Umstand beschränkt auch die Wirksamkeit derartiger Aufdeckungsanordnungen erheblich, denn bereits jetzt weichen Täter auf das Darknet aus.

Aus Sicht des ÖRAK ist daneben auch insbesondere auf die mit dem Vorschlag einhergehende **ständige Möglichkeit der Verletzung des rechtsanwaltlichen Verschwiegenheitsgebots** und damit eines **rechtsstaatlichen Grundprinzips zutiefst besorgniserregend**.

Die Geltung des rechtsanwaltlichen Verschwiegenheitsgebots ist für viele Mandantinnen und Mandanten eine **Grundvoraussetzung für die Inanspruchnahme rechtsanwaltlicher Beratung und damit auch für den Zugang zum Recht**.[1] Es besteht keine Technologie, die derzeit oder in Zukunft vom Verschwiegenheitsgebot geschützte Daten von anderen unterscheiden könnte.

[1] Vorsorglich ist klarzustellen, dass eine Berufung auf das Verschwiegenheitsgebot nie möglich ist, wenn ein Rechtsanwalt oder eine Rechtsanwältin selber in kriminelle Aktivitäten involviert sind.

Es mag zwar sein, dass Grundrechtseingriffe unter bestimmten Voraussetzungen zulässig sind. Artikel 8 EMRK legt dazu etwa fest, dass eine Behörde in dieses Recht eingreifen darf, wenn der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft 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. Ein Eingriff hat daher nicht nur einem bestimmten, definierten Zweck zu diesen, der unter eine der angeführten Ziele zu subsumieren ist, er hat auch das Verhältnismäßigkeitsgebot zu wahren . Diese Kriterien gelten im Wesentlichen für jeden Eingriff in die nachstehenden Grundrechte, soweit diese nicht ohnedies schrankenlos garantiert werden.

Nach Auffassung des ÖRAK verstoßen die vorgeschlagenen Aufdeckungsanordnungen damit gegen eine Reihe von **Grundrechten,** namentlich der EMRK und der GRC. Insbesondere, aber nicht abschließend, ist auf folgende Grundrechte hinzuweisen: den Anspruch auf ein faires Verfahren inklusive einer Verteidigung (Art 6 Abs 1 Satz 1, Abs 3 lit c EMRK), das Recht auf einen wirksamen Rechtsbehelf inklusive der Beratung, Verteidigung und Vertretung (Art 47 Abs 1 und Abs 2 Satz 2 GRC), das Recht auf Achtung des Privatlebens sowie die Vertraulichkeit elektronischer Kommunikation (Art 8 Abs 1 EMRK und Art 7 GRC), Recht auf Eigentum (Art. 17 GRC, Art. 1 Zusatzprotokoll zur EMRK) sowie die Freiheit der Medien (Art. 11 Abs. 2 GRC unter dem Gesichtspunkt des Quellenschutzes). Diese Grundrechte müssen zwingend auch im digitalen Raum, geschützt werden.

Der Eingriff durch die bloße Möglichkeit einer Aufdeckungsanordnung ist schwerwiegend: Sie erlaubt, jedwede Kommunikation auch unbeteiligter Personen zu durchleuchten. Sie verletzt damit das Grundvertrauen in fundamentale Werte einer demokratischen und rechtsstaatlichen Gesellschaft. Hinzu kommt die eingeschränkte Wirksamkeit eines solchen Eingriffs, da gerade die typischerweise von Tätern genützten digitalen Kommunikationskanäle nicht erfasst sind; Täter können ohne weiteres und ohne besondere Kenntnisse andere Kanäle (Darknet, sonstige ausländische Betreiber, selbst gehostete Dienste usw) nützen. Außerdem sind die technologischen Möglichkeiten nur beschränkt wirksam. Es besteht nicht nur das Risiko, dass Filter nicht anschlagen, vielmehr besteht die Gefahr falsch-positiver Treffer. Derartige Eingriffe, auch wenn sie einem legitimen Ziel dienen sollen, können daher **nicht verhältnismäßig** sein.

Im Hinblick hierauf ist auch der im LIBE-**Berichtsentwurf** enthaltene Vorschlag von **freiwilligen Aufdeckungsanordnungen, Artikel 5a BE, Änderungsantrag 99**, abzulehnen.

Der Berichtsentwurf sieht generell keine ausreichenden Änderungen im Hinblick auf Aufdeckungsanordnungen vor. Der Vorschlag in **Änderungsantrag 111, Artikel 7**

(2) Unterabsatz 1a neu BE, zu einer „fair balance between the fundamental rights“ verkennt, dass Grundrechte nicht einfach arbiträr gegeneinander „abgewogen“ werden, insbesondere nicht bei einer hohen Eingriffsintensität. Bestimmte Eingriffe sind aus grundrechtlicher Sicht auch schlicht nicht zu rechtfertigen.

Der Vorschlag scheint weiters das **Risiko des Datenmissbrauchs** völlig zu unterschätzen.

Erwägungsgrund (26) des Verordnungsvorschlags **führt im Ergebnis zu einer Abschaffung von echter Ende-zu-Ende-Verschlüsselung**. In diesem wird „den betreffenden Anbietern mit dieser Verordnung die Wahl der zur Erfüllung der Aufdeckungsanordnungen zu betreibenden Technologien überlassen“, dies gelte auch für Ende-zu-Ende-Verschlüsselung. Solange allerdings der Erfolg der Aufdeckungsanordnungen geschuldet ist, werden Anbieter zB allgemeine Entschlüsselungs-Keys standardmäßig bei sich vorhalten müssen. Diese de facto Abschaffung von echter E2E-Verschlüsselung würde jegliche vertrauliche Kommunikation im digitalen Raum in Frage stellen. So greifen bereits jetzt Geheimdienste unterschiedslos auf Internetströme zu und könnten die von den Anbietern vorbehaltenen Entschlüsselungstechnologien erlangen und ebenfalls nutzen, dasselbe gilt für Ermittlungsbehörden, die Zugriffsmöglichkeiten überziehen oder missbrauchen könnten, zB auch um rechtsanwaltliche oder journalistische Kommunikation zu überwachen.

Nicht akzeptabel ist auch, dass der Schutz, die Überprüfung der höchstpersönlichen Daten sowie Entscheidungen zu Meldungen **privaten Konzernen** anvertraut wird, die nicht unabhängig sind und eigene Gründe für ihre Reaktionen auf entsprechende Anordnungen haben können.

An dieser Stelle ist auch klarzustellen, dass ein **Scannen von Metadaten im Rahmen eines Aufdeckungsanordnung kein aus grundrechtlicher Sicht akzeptabler Eingriff** wäre. Auch über Metadaten erfährt man im Ergebnis alles über einen Nutzer, die Eingriffsintensität ist sehr hoch. Nutzer können im Nachhinein recht einfach identifiziert werden (siehe hierzu auch **Änderungsantrag 17, Erwägungsgrund 26 a neu BE** oder **Änderungsantrag 106, Artikel 6a neu BE**).

Schlussendlich scheint die EU-Kommission das **Risiko der Überschwemmung von Behörden mit Falschmeldungen** nicht zu sehen oder falsch einzuschätzen.

Artikel **9 VO-Vorschlag** sieht zwar richtigerweise verschiedene **Rechtsbehelfe** vor, das **Recht auf Verteidigung betroffener Personen ist dennoch nicht gewahrt**. Der Verordnungsvorschlag geht offensichtlich davon aus, dass Meldungen der

Diensteanbieter korrekt sind. Sollte sich das belastende Material dann nicht mehr finden lassen, würde man wohl auf eine Löschung des Nutzers schließen. Hier ist völlig unklar, wie sich ein normaler Bürger gegen ein Tech-Unternehmen, dessen Reputation auf dem Spiel steht, wirksam wehren kann, zumal ein Negativum zu beweisen wäre, dass sich bestimmtes Material gerade nicht in seinem Besitz befand.

Hier ist zunächst auf *proprietary rights*, dh Rechte an den Algorithmen, der Anbieter zu verweisen, die jegliche Nachvollziehbarkeit sehr erschweren. Übersehen wird auch die Gefahr, die von eingesetzten selbst lernenden Technologien (künstlicher Intelligenz) ausgeht, die zum Erkennen von Bildmaterial eingesetzt wird. Diese Technologien sind letztlich nicht mehr kontrollierbar und/oder nachvollziehbar. Gerade im Bereich der justiziellen Entscheidungsfindung dürfen solche Technologien keinen Platz haben; dies gilt auch für vorgeschaltete Erkenntnishilfen.

Auch die Kosten für die Verteidigung im Ermittlungsverfahren und dann ggf im strafgerichtlichen Verfahren sind nicht zu unterschätzen, gerade auch, da kostspielige unabhängige Expertisen notwendig sind. Ob ein Gegenbeweis gelingt, dürfte auch bei einer fehlerhaften Meldung fraglich sein.

Beachtenswert ist in den Konstellationen nach dieser Verordnung, dass es sich um anlasslose Überprüfungen handelt. Anders als bei anderen Ermittlungsmaßnahmen bestehen keine weiteren Ansatzpunkte, auf die sich Ermittlungen stützen, zB Hinweisgeber, Kontakte zu anderen Beschuldigten etc..

Schlussendlich: selbst wenn der Beweis des Negativen erfolgt, so ist zu beachten, dass Ermittlungsverfahren eine gewisse Dauer haben. Innerhalb dieser dürfte das familiäre und gesellschaftliche Leben eines zu Unrecht Verdächtigen zerstört sein.

Artikel 10, Technologien und Schutzvorkehrungen, sowie **Artikel 44 (l) c)** erwecken den Eindruck als würden zuverlässige Technologien zum Auffinden von sogenanntem **Grooming** bereits bestehen. Dies ist nicht der Fall. Problematisch sind hier zum einen die Tatsache, dass sogenanntes Grooming ja gerade oft durch „normale“ Gespräche erfolgt, zum anderen die verschiedenen Sprachen der Europäischen Union. Zu Ersterem ist nicht absehbar, ob jemals eine verlässliche Technologie entwickelt werden kann.

(An dieser Stelle ist anzumerken, dass auch die Wirksamkeit einer Alterskontrolle sehr zweifelhaft sein dürfte da viele Täter aus dem familiären Umfeld Zugriff auf Ausweisdokumente von Minderjährigen haben dürften.)

Hinweise an den Nutzer zur Nutzung entsprechender Technologien, Artikel 10 (5) würden in einer digitalisierten Welt, in der Nutzer auf die entsprechenden Dienste angewiesen sind, maximal zu einer (in einer demokratischen Gesellschaft nicht gewünschten) Selbstzensur führen. Vermeiden kann man die entsprechenden

Dienste trotz Hinweis im Ergebnis wohl nicht in Anbetracht des weiten Anwendungsbereichs der geplanten Verordnung.

Sollten **Artikel 14, 15 VO-Vorschlag** beibehalten werden, wäre nach Auffassung des ÖRAK bei einer **Entfernungsanordnung** zumindest eine geeignete Sicherheitskopie anzufertigen für eine spätere Überprüfung.

In **Artikel 27 VO, Untersuchungsbefugnisse der Koordinierungsbehörden**, sollte eine Regelung zum Schutz des Verschwiegenheitsgebots eingefügt werden bzw zumindest ein klarstellender Erwägungsgrund zur Anwendbarkeit der entsprechenden nationalen Vorschriften.

Artikel 29 (2) (b) sieht eine Art temporärer Datenenteignung der Nutzer vor. Dieser Schritt ist bedenklich, da damit Zugriff auf Verträge, Nachweise, Tickets vorenthalten werden. Der Vorschlag sieht kein zeitliches Limit vor, die entsprechende Behörde kann die Anordnung auch für eine sehr lange Zeit treffen. Hier wäre zumindest eine richterliche Anordnung, ggf eine Begrenzung der Dauer vorzusehen.

Artikel 49 (1) (b), Durchsuchungen, ist im Vorschlag sehr weit gefasst, sodass *fishing expeditions* möglich sein dürften, die aus rechtsstaatlichen Erwägungen gerade nicht legal sind. Auch sollte eine richterliche Anordnung in jedem Fall einer Durchsuchung notwendig sein. Die Aufforderung, freiwillig bestimmte Inhalte zu entfernen, **Artikel 49 (2)** könnte zu aus rechtsstaatlicher und demokratischer Sicht zu nicht gewollter *overcompliance* der Anbieter aus Sorge um ihren guten Ruf führen, selbst wenn das in Rede stehende Material keine Entfernung rechtfertigt.

Die Anregung in **Änderungsantrag 273, Artikel 66a neu BE,** ein **Victims' Consultative Forum** einzurichten wird nachdrücklich unterstützt, wobei der ÖRAK die Frage der Details nicht kommentieren möchte. Hier sollten die entsprechenden Organisationen gehört werden.

Artikel 71 ff, Bestimmungen zum Personal, mangelt es noch an Sicherheitsbestimmungen für die Mitarbeiterinnen und Mitarbeiter des geplanten EU-Zentrums. Da die EU über keine eigenen Sicherheitsbehörden verfügt, ist hier in besonderer Weise darauf zu achten, dass eine Sicherheitsüberprüfung mit Hilfe der Behörden der Mitgliedstaaten erfolgt.

Artikel 74, 75, Berufsgeheimnis und Verschlusssachen, wäre um eine Vorschrift zu ergänzen, die den Umgang mit vom Verschwiegenheitsgebot gedeckten Daten regelt, die versehentlich erlangt worden sind.

<u>Aus Sicht des ÖRAK bieten sich weiters folgende grundsätzliche Erwägungen zur Verbesserung des Vorschlags an:</u>

- Beschränkung auf **gezielte Maßnahmen**, dh basierend auf richterlichen Anordnungen und aufgrund von Ermittlungsergebnissen oder glaubwürdigen Hinweisen; sowohl Grundrechte als auch Verfahrensrechte sind zu wahren,

- Einrichtung von **effektiven Meldesystemen**, zB für jugendliche Nutzer, die Verdächtiges entdecken, die Strafverfolgungsbehörden nicht überlasten, sodass den eingehenden Hinweisen umgehend nachgegangen werden kann.

Der ÖRAK fordert die Co-Gesetzgeber nachdrücklich dazu auf, sich für den Schutz der Grund- und Freiheitsrechte, sowie insbesondere des Mandatsgeheimnisses einzusetzen und rechtsstaatliche Grundwerte im Zusammenhang mit diesem Gesetzesvorhaben zu schützen.