



# Vorschlag für eine Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (sog Chatkontrolle-VO)

20.12.2023 Gesetzgebung » EU

Der ÖRAK fordert in diesem Zusammenhang erneut, verbindliche Mindeststandards für Gesetzgebungsverfahren einzuführen, die aus einer rechtsstaatlichen Notwendigkeit heraus einzuhalten sind.

Nach Ansicht des ÖRAK hat im Sinne eines effektiven Rechtsschutzes jeder Bürger jederzeit das Recht zu erfahren, worauf sich die Zulässigkeit einer KI-Entscheidung stützt und worauf diese inhaltlich beruht. Eine solche Auskunft sollte jederzeit gerichtlich ohne Angaben von Gründen überprüft werden können, dies sowohl vor dem Einsatz von KI als auch im Nachhinein.

Der ÖRAK fordert die ersatzlose Abschaffung der Rechtsgeschäftsgebühren. Sie belasten Bürgerinnen und Bürger sowie Unternehmen über die Maßen und haben negative Auswirkungen auf die Rechtssicherheit.

Der ÖRAK hält folgende Maßnahmen zur nachhaltigen Sicherung des Zugangs zum Recht für erforderlich:

- Reform der Gerichtsgebührenstruktur in Österreich
- Beseitigung des Selbstverständnisses der Justiz als Großunternehmen
- Abflachung der Kurve des progressiven Tarifs bei den Gerichtsgebühren
- Deckelung der Gerichtsgebühren bei hohen Streitwerten (Attraktivierung des Gerichtsstandortes Österreich)
- Reduktion der Gerichtsgebühren für jeden Vergleich
- Reduktion der Pauschalgebühr im Revisionsverfahren für den Fall einer Zurückweisung der Revision durch den OGH
- Reduktion der Pauschalgebühr bei Klagsrückziehungen auch nach Zustellung an die Gegnerin bzw den Gegner und ebenso für den Fall des ewigen Ruhens des Verfahrens

- Gebührenfreiheit hinsichtlich einer Generalbereinigungsklausel im Vergleich
- Außerdem fordert der ÖRAK als Mindestgrenze die Beibehaltung eines Bezirksgerichts pro Bezirk

Im Sinne der Rechtsstaatlichkeit sowie eines fairen Verfahrens dürfen keinesfalls Verfahrensverzögerungen über mehrere Jahre stattfinden.

Der ÖRAK betont nachdrücklich die Wichtigkeit des effektiveren Kampfes gegen den sexuellen Missbrauch von Kindern in allen Mitgliedstaaten der Europäischen Union und darüber hinaus.

Nach Auffassung des ÖRAK verstößt der vorgelegte Vorschlag zur sog Chatkontrolle, allerdings massiv gegen Grundrechte und kann in der vorliegenden Fassung durch die Co-Gesetzgeber nicht angenommen werden. Es bestehen auch Zweifel an der Vereinbarkeit der geplanten Maßnahmen mit der Rechtsstaatlichkeit in den Mitgliedstaaten, zB im Hinblick auf Befugnisse der ermittelnden Behörden und die erhöhte Gefahr der Eröffnung von Ermittlungsverfahren gegen unschuldige Personen.

Grundsätzlich sieht der Vorschlag die **Möglichkeit einer Durchleuchtung von Inhalten unterschiedslos aller Nutzer von Hosting- und interpersonellen Kommunikationsdiensten** vor. Damit kann niemand mehr auf die Vertraulichkeit der Kommunikation zählen. Nach Auffassung des ÖRAK verstößt dies massive gegen eine Vielzahl von in der Europäischen Menschenrechtskonvention und in der Grundrechtecharta verankerten Grundrechten.

Das vorgeschlagene komplexe System, das zu einer Anordnung führt, ändert nichts an dem damit einhergehenden **ungerechtfertigten und unverhältnismäßigen Grundrechtseingriff gegenüber Personen, die gerade nicht unter Verdacht 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 E-Mail-Postfächern 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**, nutzen sonstige ausländische Betreiber, selbst gehostete Dienste usw.

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 eine Grundvoraussetzung für die Inanspruchnahme rechtsanwaltlicher Beratung und damit auch für den Zugang zum**

**Recht.** Es besteht keine Technologie, die derzeit oder in Zukunft vom Verschwiegenheitsgebot geschützte Daten von anderen unterscheiden könnte. Nach Auffassung des ÖRAK verstoßen die vorgeschlagenen Aufdeckungsanordnungen damit gegen eine Reihe von Grundrechten. Insbesondere, aber nicht abschließend, ist auf folgende Grundrechte hinzuweisen:

- Anspruch auf ein faires Verfahren inklusive einer Verteidigung, Art 6 EMRK,
- Recht auf einen wirksamen Rechtsbehelf inklusive der Beratung, Verteidigung und Vertretung, Art 47 GRC,
- Recht auf Achtung des Privatlebens sowie die Vertraulichkeit elektronischer Kommunikation, Art 8 EMRK, Art 7 GRC,
- Recht auf Eigentum, Art. 17 GRC, Art. 1 Zusatzprotokoll zur EMRK sowie die
- Freiheit der Medien, Art. 11 GRC (im Hinblick auf Quellenschutz).

Diese Grundrechte müssen zwingend auch im digitalen Raum, geschützt werden.

Rein vorsorglich: Eine Berufung auf das Verschwiegenheitsgebot ist nie möglich, wenn ein Rechtsanwalt oder eine Rechtsanwältin selbst in kriminelle Aktivitäten involviert ist.

Bereits die bloße rechtliche Möglichkeit einer Aufdeckungsanordnung wäre schwerwiegend: Indem diese erlaubt, jedwede Kommunikation auch unbeteiligter Personen zu durchleuchten, wird das **Grundvertrauen in fundamentale Werte einer demokratischen und rechtsstaatlichen Gesellschaft verletzt**.

Der Verordnungsvorschlag führt im Ergebnis auch 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.

Der Verordnungsvorschlag sieht zwar richtigerweise verschiedene Rechtsbehelfe vor, das **Recht auf Verteidigung betroffener Personen** ist dennoch nicht gewahrt. Der Vorschlag 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 selbst lernenden Technologien (Künstlicher Intelligenz) ausgeht, die zum Erkennen von Bildmaterial eingesetzt werden. 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 überhaupt 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.**

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