Diskussionsentwurf zur Novellierung des Jugendmedienschutz-Staatsvertrages (April 2022)

Stellungnahme der FSM *(16. Juni 2022)*

Die Freiwillige Selbstkontrolle Multimedia-Diensteanbieter (FSM) ist seit über 17 Jahren anerkannte Einrichtung der Freiwilligen Selbstkontrolle für den Jugendmedienschutz in Telemedien (§ 19 JMStV) sowie seit Januar 2020 auch Einrichtung der Regulierten Selbstregulierung nach NetzDG. Wir beraten und beaufsichtigen unsere Mitgliedsunternehmen in allen Fragen des Jugendschutzes sowie der Nutzung digitaler Medien durch junge Menschen und Familien. Dabei spielen neben rechtlichen und technischen auch medienpädagogische Themen eine wichtige Rolle. Im Rahmen des reformierten JuSchG hat die FSM ebenfalls eine wichtige Rolle übernommen und zertifiziert gemeinsam mit der FSF Jugendschutzbeauftragte für ihre Arbeit bei der Bewertung und Freigabe von Inhalten.

Zusammenfassung

- Der Diskussionsentwurf sieht sehr weitreichende Änderungen im System des gesetzlichen Jugendmedienschutzes vor. Eine Defizitanalyse fehlt jedoch, weshalb eine Rechtfertigung für die vorgeschlagenen Maßnahmen nicht erkennbar ist. Aktuelle und relevante Fragen des Jugendschutzes werden nicht adressiert.
- Der obligatorische Einsatz von „Jugendschutzvorrichtungen“ in Betriebssystemen würde das Schutzniveau insgesamt verringern und Eltern die Möglichkeit nehmen, individuelle und zu ihrer Familie passende Schutzmaßnahmen zu ergreifen.
- Die Vorschläge würden dazu führen, dass etablierte Maßnahmen zurückgefahren und künftige Innovationen sowie überobligatorisches Engagement der Unternehmen verringert werden.
- Durch die Fokussierung auf Jugendschutzvorrichtungen als Pflicht für die Anbieter von Betriebssystemen kommt es aus Sicht der Inhalteanbieter zu neuen Abhängigkeiten und neuer Rechtsunsicherheit.
- Zahlreiche Gerätehersteller und Entwickler von Betriebssystemen sollen erstmals zu Jugendschutzmaßnahmen verpflichtet werden. Voraussichtlich sind die neuen Pflichten jedoch nicht durchsetzbar, da kaum ein betroffenes Unternehmen seinen Sitz in Deutschland hat. Handeln jedoch nicht *alle* relevanten Anbieter von Betriebssystemen für Computer, mobile Endgeräte, Fernseher, Set-top-Boxen etc. gleichermaßen schnell und einheitlich, bleibt das neu einzuführende Schutzkonzept insgesamt wirkungslos.
- Das System des technischen Jugendmedienschutzes würde insgesamt langsamer, unflexibler und intransparenter.
- Die Übergangsregelungen sind angesichts der massiven Veränderungen, die nötig wären, keinesfalls ausreichend. Sie verlangen von den Anbietern in Teilen schlicht Unmögliches.

Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V. (FSM)
Beuthstraße 6, 10117 Berlin, Telefon: 030 240484-30, office@fsm.de, www.fsm.de

Im Einzelnen

1. Allgemeines zum Diskussionsentwurf

Dem Gesetzentwurf ist keine konkrete Defizitanalyse vorangegangen. Deshalb ist weder erkennbar noch nachvollziehbar, warum die Länder ein so eingriffsintensives Konzept vorschlagen, das tiefgreifende Veränderung im bisherigen System der Verantwortlichkeit von Anbietern mit sich bringen würde. Das Vorhaben hätte zudem ganz erheblich nachteilige Auswirkungen auf das Niveau des Jugendmedienschutzes in Deutschland. Als international nicht anschlussfähiger Sonderweg Deutschlands stellt sich die Frage nach der Vereinbarkeit mit Unionsrecht.

Der Jugendmedienschutz ist eine gesamtgesellschaftliche Aufgabe, an deren Umsetzung alle denkbaren Akteure nach ihren Möglichkeiten und Fähigkeiten und in einer Weise mitwirken sollten, die zu einem funktionierenden und ertragreichen Gesamtsystem beiträgt. Es ist deshalb wichtig und richtig, nicht an starren Konzepten festzuhalten, sondern stets auch neue Möglichkeiten zu ergründen und im Idealfall die regulatorischen Voraussetzungen zu schaffen, neue Risiken unmittelbar adressieren zu können und flexibel auf neue Herausforderungen reagieren zu können.

Es ist deshalb gut, dass die Länder die Entwicklung des regulatorischen Jugendmedienschutzes nach der Novelle des Jugendschutzgesetzes durch den Bund im vergangenen Jahr nicht als abgeschlossen betrachten, sondern weitere Schritte vorschlagen. Der Prozess, der diesem Gesetzentwurf vorausging, war geprägt von einem intensiven Austausch mit zahlreichen Akteuren aus Wissenschaft, Praxis und Regulierung im Bemühen, die Umsetzbarkeit regulatorischer Ideen frühzeitig einzuschätzen. Diesen Ansatz halten wir für beispielgebend, um bereits vor der Veröffentlichung eines Entwurfs auf breite externe Expertise zurückgreifen zu können. Er hätte jedoch noch konsequenter verfolgt werden müssen.

Der Umgang mit dem vorliegenden Entwurf erwies sich insoweit als herausfordernd, als dass die gesetzgeberischen Motive, die größeren Zusammenhänge einzelner Vorschläge sowie die weitergehenden Überlegungen der Autorinnen und Autoren unklar bleiben. Eine begleitende Begründung bzw. erläuternde Ausführungen können helfen, Missverständnisse zu vermeiden und den Fokus auf die relevantesten Aspekte zu legen.

Wir halten es auch deshalb für essenziell, dass es mit Blick auf den vorliegenden Entwurf Gespräche auf fachlicher Ebene unter Einbeziehung der KJM, der Landesmedienanstalten und der Selbstkontrolleinrichtungen gibt. Während das politische Ziel des Gesetzentwurfs erkennbar ist, bleiben die technischen Umsetzungshürden aus Sicht der FSM derzeit unüberwindbar.

1.1. Fehlende Defizitanalyse

Die Länder schlagen mit dem JMStV-E eine umfangreiche Neuausrichtung des Systems des (technischen) Jugendmedienschutzes für Onlineangebote vor, die massive und nachteilige Auswirkungen auf der Seite der Anbieter von Inhalten, Plattformen und Geräten sowie für Familien haben würde. **Es entstünde eine international nicht anschlussfähige deutsche Insellösung**, die zum einen nicht mit europäischem Recht kompatibel wäre und zum anderen deutsche Anbieter auf dem internationalen Markt benachteiligen könnte, wenn sie ihre Dienste auch in anderen Ländern anbieten. Die Vorschrift ist auch nicht vergleichbar mit dem französischen „Gesetzentwurf zur Stärkung der elterlichen Aufsicht über den Internetzugang" *("Proposition de loi visant à renforcer le contrôle parental sur les moyens d'accès à internet")*: Zum einen ist der dortige Entwurf ausdrücklich technologieneutral und anerkennt zum anderen bereits vorhandene bzw. umgesetzte Maßnahmen. In Anbetracht der Tatsache, welche Schutzmaßnahmen schon heute bei von Kindern genutzten Geräten bzw. Betriebssystemen mitgeliefert und eingesetzt werden, bestünde dabei wenig bis kein Umsetzungsaufwand. Der JMStV-E schlägt demgegenüber jedoch tiefgreifende neue Verpflichtungen der Inhalte- und Betriebssystemanbieter vor.

Um eine so grundlegende Neugestaltung zu rechtfertigen, die mit zahlreichen Grundrechtseingriffen einherginge, bedürfte es einer sachlichen, empirisch belegten Begründung, für die die Länder jedoch nichts vortragen. Es ist nicht erkennbar, in welchen Nutzungsszenarien künftig ein höheres Jugendschutzniveau bestehen würde.

Wie noch zu zeigen sein wird, hätten die vorgeschlagenen Neuerungen primär Einfluss darauf, wie Nutzerinnen und Nutzer Apps über die dafür vorgesehenen Plattformen beziehen können, sowie darauf, wie sog. geschlossene Systeme (wie z.B. Video-on-Demand-Angebote oder Spielkonsolen) auszugestalten sind. Dies sind jedoch gerade diejenigen Bereiche, für die **bereits heute hohe Standards** bestehen und in denen Familien über ein breites Instrumentarium an einfach zu nutzenden Maßnahmen verfügen, um wirksamen Jugendschutz zu gewährleisten. Diese Maßnahmen werden auch eingesetzt.

Der Gesetzentwurf adressiert primär (vermeintliche) Lösungen ohne Nachweis des zugrundeliegenden Problems. Er widmet sich hingegen ganz ausdrücklich nicht denjenigen Herausforderungen, die im Onlinejugendschutz anerkanntermaßen bestehen - jugendgefährdenden Inhalten im WWW sowie Risiken für junge Menschen, die sich aus unangemessenen Kontakten und der Kommunikation mit Fremden ergeben. Letzteres wird zwar angerissen, würde im Ergebnis aber wirkungslos bleiben.

Der **Jugendmedienschutzindex** (www.jugendmedienschutzindex.de), den die FSM 2017 erstmals herausgegeben hatte, gab schon seinerzeit wichtige Einblicke in die Wahrnehmung des Jugendmedienschutzsystems durch die Eltern und ihr entsprechendes Handeln. Diese Untersuchung wird derzeit erneut durchgeführt, die Ergebnisse werden wir am 13. Oktober 2022 präsentieren. Ziel der Studie ist es, eine aktuelle, wissensbasierte Grundlage für die Weiterentwicklung des Jugendmedienschutzes zu schaffen. Mit Hilfe eines aktualisierten standardisierten Erhebungsinstruments werden dabei relevante kompetenz-, einstellungs- und handlungsbezogene Aspekte erfasst. Die repräsentative Befragung von Eltern und Kin-

dern ermöglicht es, Ergebnisse zu beiden Perspektiven gewinnen. Eltern- und Kinderantworten können direkt zueinander in Beziehung gesetzt werden, wodurch Rückschlüsse auf das genaue Zusammenspiel beider Perspektiven möglich sind. Einen besonderen Schwerpunkt wird die Untersuchung dieses Mal auf das Thema technischer Jugendmedienschutz legen: Was nutzen Eltern, was nicht - und warum? Was fehlt Familien heute bei der Medienerziehung und der Umsetzung ihrer eigenen Entscheidungen in Bezug auf den Schutz ihrer Kinder bei der Nutzung digitaler Medien?

Der Jugendmedienschutzindex wird ein entscheidendes Element sein, bestehende Defizite zu ermitteln und passgenaue Antworten von Gesetzgeber und Selbstregulierung zu finden. Die dortigen Erkenntnisse sollten unbedingt abgewartet werden, bevor das Gesetzgebungsverfahren fortgesetzt wird.

1.2. Unnötiger Systemwechsel

Konsens und Kernelement der bisherigen Jugendmedienschutzregulierung ist es, dass primär diejenigen für ausreichende Schutzmaßnahmen zu sorgen haben, die einen jugendschutzrechtlich relevanten Inhalt bereithalten. Inhalteanbieter sind naturgemäß am dichtesten an den Angeboten bzw. Inhalten und können am ehesten auf diese Einfluss nehmen. Deshalb ist es sowohl systematisch als auch regulatorisch richtig, vorrangig sie in Anspruch zu nehmen und von ihnen einen angemessenen, wirksamen Jugendschutz zu verlangen.

Der Gesetzentwurf beschreitet jedoch völlig neue Wege, indem er denjenigen eine zentrale Rolle zuweist, die von den Inhalten am weitesten entfernt sind bzw. an den Inhalten weder ein eigenes Interesse haben, noch auf diese oder deren Anbieter inhaltlich Einfluss nehmen können: „eine natürliche oder juristische Person, die Betriebssysteme bereitstellt“ (§ 3 S. 1 Nr. 6 JMStV-E). Der Entwurf setzt sich damit in Widerspruch zu dem sowohl regulatorisch wie auch in der deutschen und europäischen Rechtsprechung mehrfach hervorgehobenen Grundsatz der Subsidiarität im Rahmen der Verantwortlichkeit als Ausfluss des Prinzips der Verhältnismäßigkeit von Eingriffsmaßnahmen.

1.3. Fragliche Umsetzbarkeit

Der Gesetzentwurf ist mit seiner Fokussierung auf Betriebssysteme **sowohl eingriffsintensiv als auch sehr pauschal und weitgehend**. Bewusst oder unbewusst wird eine Vielzahl von Akteuren neu in den Kreis der Verpflichteten einbezogen, die bisher keine verpflichtende Rolle im System des gesetzlichen Jugendmedienschutzes hatten, nämlich vor allem die Anbieter von Betriebssystemen. Dabei bieten diese Anbieter bereits heute Lösungen an, mit denen sie auf eine entsprechende Nachfrage in den Familien reagiert haben, ohne dass es regulatorischer Vorgaben bedurft hätte. Sie folgen damit realen Erkenntnissen und nicht einer bloßen Vermutung im Hinblick auf das, was Eltern für die Medienerziehung und den Schutz ihrer Kinder benötigen.

Es ist zweifelhaft, ob angesichts der äußerst kurzen Übergangsfristen eine angemessene und - aus Sicht von Gesetzgeber und Aufsicht - ausreichende Reaktion auf die vorgeschlagenen Regeln erfolgen *kann*. Wie später auszuführen sein wird, bilden die Regeln in § 25 JMStV-E keinesfalls einen ausreichenden Rahmen dafür.

Darüber hinaus kann in diesem Zusammenhang die **internationale Dimension** des Gesetzesvorschlags nicht hoch genug eingeschätzt werden. Soweit ersichtlich, hat - mit Ausnahme einiger weniger proprietärer Geräte und Systeme - kein Anbieter eines Betriebssystems seinen Sitz in Deutschland. Neben verschiedenen Ländern in der EU dürften hier vor allem die USA, Japan und Südkorea eine Rolle spielen, ggf. auch China. Ob die KJM nach den Vorgaben des JMStV-E über ein angemessenes Instrumentarium zur Durchsetzung verfügt und ob eine entsprechende Durchsetzung grundsätzlich überhaupt denkbar ist, ist fraglich. **Es fehlen ein dialogischer Ansatz und jegliche Möglichkeiten einer Anreizregulierung**, anders als beispielsweise im reformierten JuSchG.

Gelingt es aber nicht, Anbieter (oder, im Wortlaut des Gesetzentwurfs: Bereitsteller) von Betriebssystemen zur Implementierung einer Jugendschutzvorrichtung zu bewegen, laufen die übrigen bzw. daran anschließenden Maßnahmen komplett ins Leere. Es stellen sich zudem abermals systematische Fragen, denn das Gesetz selbst legt nahe, dass es Jugendschutzvorrichtungen nicht für alle, sondern nur für von Kindern und Jugendlichen üblicherweise genutzte Betriebssysteme (§ 12 Abs. 1 S. 1 JMStV-E) geben würde. Eine App bzw. ein Angebot wird aber für eine Vielzahl von Plattformen existieren: Ob und wie sich Anbieter hier rechtskonform verhalten könnten, ist offen.

2. Jugendschutzvorrichtung

Eine Jugendschutzvorrichtung, wie sie der Gesetzentwurf vorschlägt, würde das Niveau des Jugendschutzes verringern. Dieses Konzept benachteiligt diejenigen Anbieter, die sich bereits heute rechtskonform verhalten. Es nimmt Eltern die ihnen heute zur Verfügung stehenden individuellen und altersdifferenzierten Optionen, mit denen sie den Zugang ihrer Kinder zu digitalen Medien regulieren können. Neben systematische Unsicherheiten treten tiefgreifende Umsetzungshemmnisse in der Praxis. Das entworfene System ist nicht funktionsfähig.

2.1. Angestrebtes Ziel

Der Gesetzgeber möchte die Zugänglichkeit und Nutzbarkeit von Systemen des technischen Jugendmedienschutzes verbessern bzw. erleichtern. Dieses Ziel ist zu begrüßen. Er schlägt dazu ein pauschal wirkendes System vor, das schnell aktiviert und deaktiviert werden kann und das im Idealfall einheitlich auf das komplette Gerät wirkt.

Ausdrücklich nicht Gegenstand der Neuregelung sind jedoch Herausforderungen im Bereich des Jugendmedienschutzes, die sich aus **WWW-Inhalten** ergeben. Ebenfalls nur ganz

am Rande (§ 11 Abs. 2 S. 2 i.V.m. § 5 Abs. 2 JMStV-E) finden Risiken Beachtung, die sich aus dem Verhalten junger Menschen im digitalen Raum ergeben.

An ganz entscheidender Stelle erzeugt der Gesetzentwurf **große Unsicherheit**, nämlich bei der Frage, welche Betriebssysteme bzw. welche derer Anbieter überhaupt erfasst werden:

- Die Pflicht, eine Jugendschutzvorrichtung bereitzuhalten, gilt für jede „natürliche oder juristische Person, die Betriebssysteme bereitstellt“ (§ 3 S. 1 Nr. 6 JMStV-E), wenn jenes „von Kindern und Jugendlichen üblicherweise genutzt“ wird (§ 12 Abs. 1 S. 1 JMStV-E).

- Welche Kriterien die zu dieser Festlegung berufene KJM (§ 16 S. 2 Nr. 6 JMStV-E) hierbei anzulegen hat, bleibt offen. Die KJM allein bestimmt damit den Anwendungsbereich des Gesetzes. Ob dies mit dem Wesentlichkeitsgebot und dem Bestimmtheitsgrundsatz vereinbar ist, muss bezweifelt werden, zumal das Gesetz keine Anhaltspunkte oder Kriterien für die KJM-Entscheidung über die Üblichkeit der Nutzung vorgibt. Es stellen sich zudem erhebliche Herausforderungen im Zusammenhang mit Art. 3 GG, wenn zu begründen ist, dass Betriebssystem A in den Regelungsbereich fällt, Betriebssystem B aber nicht.

- Ob die KJM dies vorab zu entscheiden hat (und wenn ja, in welcher Rechtsform und wem gegenüber) oder ob die Verpflichtung automatisch gilt, ist unklar. Diese Frage ist auch mit Blick auf die Fristen im Zusammenhang mit dem Inkrafttreten äußerst relevant.

- In welchem Turnus die KJM diese Eigenschaft überprüft, neu feststellt bzw. nicht mehr für gegeben ansieht, ist nicht festgelegt: Ab wann ist beispielsweise eine ältere Version eines Handybetriebssystems nicht mehr von der Regelung umfasst?

- Der Zweck der Legaldefinition („natürliche oder juristische Person … bereitstellt“) wird nicht deutlich: Sollen auch andere Personen (Unternehmen, Einrichtungen, Behörden, Schulen, Bibliotheken, Verkäufer, Menschen?) neben den „klassischen“ Anbietern bzw. Herstellern von Betriebssystemen verpflichtet werden?

- Es steht zu vermuten, dass eine Vielzahl von Betriebssystemen auf unterschiedlichen Geräten zumindest potenziell betroffen sind (PCs, Handys, Tablets, Smart TVs, Satelliten-Receiver, Set-Top-Boxen, Spielekonsolen, Smartspeaker, Wearables usw.). Wie mit Open-Source-Betriebssystemen umzugehen wäre, für die es keinen zentralen Verantwortlichen gibt, ist offen. Die Nutzungsarten, -weisen und -häufigkeiten werden, ebenso wie das potenzielle Risikoniveau sehr unterschiedlich sein. Eine mit Bußgeld bedrohte automatische Verpflichtung ist unverhältnismäßig und nicht geeignet, Rechtssicherheit oder zielgerichtetes Handeln zu erzeugen.

2.2. Erwartete Auswirkungen

Die Einführung des Konzepts „Jugendschutzvorrichtung“ würde – je nach regulatorisch geforderter Ausgestaltung – erhebliche technische Maßnahmen und Eingriffe in die Strukturen

von Betriebssystemen erforderlich machen. Systembedingt erhielten die Eltern damit zwar ein einfaches, schlichtes Instrument, das jedoch durch seine pauschale Wirkweise in vielen Fällen zu einer **Verschlechterung des Schutzniveaus** führen würde.

Ob die Länder über eine entsprechende **Gesetzgebungskompetenz** verfügen, ist aus Sicht der FSM zumindest offen: Zwar handelt es sich grundsätzlich um Fragen des Jugendschutzes bei digitalen Medien, was für eine Länderzuständigkeit spricht. Gleichzeitig dürfte es sich aber bei Betriebssystemen selbst eher nicht um Telemedien handeln. Wegen der unmittelbaren Anbindung an die jeweilige Hardware fallen sie ggf. eher in den Regelungskreis, der sich mit Geräten bzw. Hardware befasst. Auch ermöglichen zahlreiche Betriebssysteme Telekommunikationsvorgänge, weshalb die Ausstrahlung in den dortigen Regulierungsbereich Einfluss auf die Kompetenzfrage haben dürfte.

Die Einführung des Konzepts „Jugendschutzvorrichtung“ setzt ein **ausgesprochen komplexes Verfahren** in Gang und verlangt von zahlreichen Beteiligten einen hohen Aufwand. Hierzu wird im Zusammenhang mit den Übergangsvorschriften vertieft vorgetragen (s.u. Ziff. 7.1).

Damit Apps „erkennen“ können, ob und mit welcher Altersstufe eine Jugendschutzvorrichtung aktiv ist, bedarf es einer offenen Schnittstelle, die die Information über das eingestellte Alter in standardisierter Weise bereithält. Auf diese Weise ist es grundsätzlich **für beliebige Dritte sofort zu erkennen, ob es sich um das Gerät eines Kindes handelt**. Dies könnte Angriffe zum Zwecke des Phishings oder des Groomings erleichtern.

Eine strukturelle Gleichbehandlung von „Walled Garden Betriebssystemen“, auf die von außen praktisch kein Einfluss genommen werden kann, und Systemen, bei dem ein Nutzer mit Administratorenrechten jede Datei des Betriebssystems verändern kann, dürfte zu Herausforderungen führen. Nach hiesigem Verständnis des Entwurfs handelt es sich bei der Kennzeichnungspflicht für Apps in § 12a S. 1 JMStV-E um eine zwingende Vorschrift. Dies würde bedeuten, dass Apps nach Ablauf der Frist aus § 25 JMStV-E nur noch auf solchen Geräten nutzbar sein dürften, die eine - bestandskräftig zertifizierte - Jugendschutzvorrichtung bereithalten. Eine andere Möglichkeit, die eigene Verpflichtung aus § 5 Abs. 1 S. 1 JMStV zu erfüllen, besteht nicht. Wegen der unter Ziff. 7.1 geschilderten Schwierigkeiten führt dies de facto zu einem **allgemeinen Verbot solcher Apps** nach Ablauf der Übergangsfrist. Die Appanbieter hätten dann keine Möglichkeit, sich rechtskonform zu verhalten; gleichzeitig haben sie keinen eigenen durchsetzbaren Anspruch gegen die Anbieter von Betriebssystemen, mit dem sie diese theoretisch zur Umsetzung von deren Verpflichtung zwingen könnten. Durch dieses faktische Verbot käme es zu einem unverhältnismäßigen Eingriff in die Grundrechte aus Art. 5 i.V.m. Art. 12 GG. Entsprechende Auswirkungen wären nur zu vermeiden, wenn die Pflicht aus § 12a JMStV-E nur dort gilt, wo auch eine Jugendschutzvorrichtung vorhanden ist. Spiegelbildlich käme es nach Fristablauf zu einem Totalverbot ganzer Appstores, wenn das dazugehörige Betriebssystem nicht über eine geeignete Jugendschutzvorrichtung verfügt.

2.2.1. Verfahren zur Eignungsprüfung

Unklar ist, ob für jede Jugendschutzvorrichtung ein formelles Verfahren zur Feststellung ihrer Eignung durchzuführen wäre. Die Verweisungskette in § 12 Abs. 4 S. 2 JMStV-E legt zwar

nahe, dass eine Einheitlichkeit mit den Verfahren zur Eignungsbewertung von Jugendschutzprogrammen (§ 11 Abs. 1 S. 2 JMStV), Altersverifikationssystemen (§ 4 Abs. 5 JMStV-E) und technischen Mitteln (§ 5 Abs. 11 JMStV-E) angestrebt wird. Eine klare Aufgabenzuweisung für die Bewertung von Jugendschutzvorrichtungen fehlt jedoch. Durch das Erfordernis eines formellen Überprüfungsverfahrens für Jugendschutzvorrichtungen analog derer für Jugendschutzprogramme käme es zu einem Flaschenhals, der für die Umsetzung des Konzepts in höchstem Maße kritisch ist.

2.2.2. Von Jugendlichen selbst eingerichtete Geräte

Nach den Praxiserfahrungen der FSM und aus dem Dialog mit ihren Mitgliedern ergibt sich kein einheitliches Bild darüber, inwieweit die Einrichtung neuer Geräte stets den Eltern obliegt oder ob die Kinder dies selbst übernehmen. Es steht zu vermuten, dass es hierbei je nach Geräteklasse deutliche Unterschiede gibt.

Einige der bereits heute verbreitet genutzten Schutzmechanismen basieren darauf, dass verschiedene Nutzerinnen und Nutzer jeweils über eigene Konten verfügen, die gemeinsam von einer Person, z.B. einem Elternteil, verwaltet werden. Zugleich wird es nicht selten vorkommen, dass insbesondere Jugendliche ihre eigenen mobilen Endgeräte weitgehend selbstständig einrichten. Dies dürfte auch für andere Geräte mit Betriebssystemen i.S.d. § 3 S. 1 Nr. 5 JMStV-E, die von jungen Menschen allein oder hauptsächlich genutzt werden, gelten. Eine gewisse Orientierung können in diesem Zusammenhang die Zahlen für den Gerätebesitz Jugendlicher aus der JIM-Studie 2021[1] geben: 94 Prozent der Jugendlichen verfügen über ein (eigenes) Smartphone, 76 Prozent über einen eigenen Laptop, 51 Prozent über ein Fernsehgerät und 47 Prozent über eine Spielkonsole (S. 7). In vielen dieser Fälle wird nicht davon auszugehen sein, dass die Systematik „Jugendschutzvorrichtung“ zum Einsatz kommt. Dies wäre dann unschädlich, wenn davon auszugehen wäre, dass es bei den derzeit angebotenen und eingesetzten Jugendschutzmaßnahmen der Inhalteanbieter nicht zu Veränderungen kommen würde, das gegenwärtig hohe Schutzniveau also beibehalten bliebe. Das Gegenteil würde jedoch geschehen.

2.2.3. Weniger Jugendschutz in den Familien

Die Art und Weise, wie Jugendschutzprogramme und andere geeignete technische Mittel mit der neuen Jugendschutzvorrichtung interagieren sollen (§ 12b Abs. 2 JMStV-E), lässt befürchten, dass Eltern künftig kaum noch individuell nutzbare Schutzmaßnahmen zur Verfügung stehen werden, was am Beispiel von Video-on-Demand-Angeboten[2] verdeutlicht werden soll:

- Hierbei ist zunächst wichtig zu wissen, dass nahezu alle in Deutschland verfügbaren und verbreitet genutzten Angebote aus dem Segment VoD über ein durch FSM oder

[1] https://www.mpfs.de/fileadmin/files/Studien/JIM/2021/JIM-Studie_2021_barrierefrei.pdf (16.6.2022).
[2] Grundsätzlich vergleichbar ist die Situation z.B. bei Spielkonsolen, in denen die Jugendschutzfunktionen oft ebenso aufgebaut sind.

KJM zertifiziertes Jugendschutzsystem (i.d.R. gem. § 11 Abs. 2, 2. Alt. JMStV) verfügen.

- Diese Angebote bieten üblicherweise individuell zu konfigurierende Profile, z.B. für die verschiedenen Familienmitglieder. Sie können so eingerichtet werden, dass der Zugang zu Inhalten ab einer bestimmten Altersstufe von der Eingabe einer PIN abhängig ist (ggf. mit verschiedenen PINs für verschiedene Profile oder unterschiedliche Altersstufen).

- Das gegenwärtige Verfahren nach §§ 11, 19a Abs. 2, 19b Abs. 2 JMStV ist durchaus anspruchsvoll. Es wird gleichwohl von den Anbietern genutzt, weil diese Art Jugendschutzprogramm von den Familien akzeptiert und genutzt wird und gleichermaßen dem Gestaltungsspielraum der Unternehmen hinreichend Rechnung trägt. Außerdem ist es derzeit *das* System der Wahl, um Inhalte mit unterschiedlicher Altersbewertung rechtskonform in Deutschland anzubieten. Es ist zugleich international relativ problemlos anschlussfähig und ist beispielgebend für die Jugendschutzfunktionen in anderen Märkten.

- Künftig würde es für den Anbieter einer VoD-App bereits genügen, nach § 12a S. 1 JMStV-E eine (einzige, pauschale) Alterskennzeichnung für eine Jugendschutzvorrichtung vorzunehmen (vgl. § 5 Abs. 4 S. 1 Nr. 2, 2. Alt. JMStV-E). Ein Jugendschutzprogramm i.S.d. § 11 JMStV und das damit verbundene aufwendige Verfahren bei der FSM wäre entbehrlich. Vor allem gäbe es keine regulatorische Anforderung im Sinne eines nach Altersstufen differenzierten Zugangs mehr.

- Den Anbietern von VoD-Apps, die bereits jetzt rechtskonform agieren und ein zertifiziertes Jugendschutzsystem anbieten, wird zudem eine zusätzliche Verpflichtung nach § 12b Abs. 2 JMStV-E zur Sicherstellung der Interaktion mit Jugendschutzvorrichtungen von Betriebssystemen auferlegt, die zu zusätzlichen, bisher nicht abschätzbaren Aufwänden der App-Anbieter führt und somit die Bereitstellung solcher Jugendschutzsysteme unattraktiver macht (s. auch nähere Ausführungen unter 3.2.).

- Entsprechende Apps würden künftig also schlicht mit einer hohen Altersstufe (z.B. 16 oder 18) gekennzeichnet werden, woraufhin die pauschale Aktivierung der Jugendschutzvorrichtung im Bedarfsfall den Zugang zur App vollständig *unterbinden* würde, ihn in keinem Fall aber *altersspezifisch ermöglichen* würde. Dies kann als - wenn auch nicht direkt intendierte - Auswirkung der Regelung im Lichte der Kinderrechte nicht hingenommen werden und behindert die Teilhabe von Kindern.

Statt der bisher angebotenen und verbreitet genutzten individuellen Schutzmaßnahmen stünden Familien also künftig vor einer einzigen, sehr limitierten Entscheidungsoption. Unternehmen sehen sich mit der schlichten wirtschaftlichen Frage konfrontiert, warum sie noch in komplexe Jugendschutzsysteme innerhalb ihrer Angebote investieren sollten.

2.2.4. Entwicklungshemmnisse für Anbieter

Wie gezeigt, bestünde künftig keine Veranlassung mehr, ein altersdifferenziertes, nutzerautonomes Jugendschutzsystem zu entwickeln. Täte ein Anbieter dies gleichwohl, müsste er

neben den Anforderungen aus § 11 JMStV *zusätzlich* die Informationen der Jugendschutzvorrichtung auslesen und entsprechend umsetzen (§ 12 Abs. 2 S. 2 JMStV-E).

Diese Vorschrift ist insbesondere unvereinbar mit der heute üblichen „Profil-Logik", die sich branchenweit durchsetzt, dass also für verschiedene Familienmitglieder individuelle Nutzungsprofile angelegt werden können. Diese Art der Konfiguration durch die Eltern würde durch die Jugendschutzvorrichtung in dem Fall pauschal überschrieben, in welchem die Altersstufe in der Jugendschutzvorrichtung niedriger ist als die in der App eingestellte. Die Option in § 12 Abs. 2 S. 1 Nr. 4 JMStV-E, nach der die Eltern eine App in einer Passlist[3] von der Behandlung durch die Jugendschutzvorrichtung ausnehmen, also in „individuell und in abgesicherter Weise [freischalten] können", führt hingegen nicht zu einer Erleichterung, sondern zu einer weiteren Verkomplizierung, sollte die App über ein Jugendschutzprogramm i.S.d. § 11 Abs. 2 JMStV verfügen:

- die App berücksichtigt grundsätzlich die Anbieter-eigenen Jugendschutzmaßnahmen (altersdifferenzierte Profile, ggf. PIN-Abfrage), da diese Funktion für alle Nutzerinnen und Nutzer unabhängig davon zur Verfügung steht, ob sie ein Gerät mit Jugendschutzvorrichtung verwenden;

- beim Aufruf altersbeschränkter Inhalte (wohl bereits „ab 12 Jahren") muss überprüft werden, ob eine Jugendschutzvorrichtung vorhanden und aktiviert ist - und wenn ja, mit welcher Altersstufe;

- die App muss – zusätzlich – prüfen, ob die Eltern sie einer individuellen Passlist hinzugefügt haben, um schließlich ggf. wieder zu den eigenen Jugendschutzfunktionen zurückzukehren. Das bedeutet auch, dass es hierfür eines eigenständigen extern auslesbaren Feldes bedarf, das diese Information dem App-Anbieter bereitstellt;

- steht die App auf einer Passlist, ist der Zugang also weiterhin nicht zwingend möglich, sondern hängt von der Konfiguration wiederum der App ab.

Weil viele Apps durch die Verwendung von Profilen gerade nicht auf der Ebene einzelner Inhalte den Zugang regulieren, ist unklar, wie eine Interaktion mit einer Jugendschutzvorrichtung hier aussehen kann. Sichtbarkeit, Lauffähigkeit und Nutzbarkeit einer App hinge zeitlich und strukturell mehrfach von dem Vorhandensein, dem Status und den Einstellungen einer Jugendschutzvorrichtung ab. Wie dies in ein nutzerfreundliches Produkt zu integrieren wäre, ist nicht erkennbar.

Beachtenswert ist, dass eine Standardisierung der Jugendschutzvorrichtung bzw. spiegelbildlich die Interoperabilität der durch die App-Anbieter zu ergreifenden Maßnahmen nach

---

[3] Mit *Passlist* wird grundsätzlich eine Funktion bezeichnet, mit der Eltern Elemente (z.B. Apps, Inhalte, Spiele, Filme, Angebote, Websites) von der Behandlung durch ein Tool (z.B. ein Jugendschutzprogramm oder ein anderer Filter) ausnehmen können, damit diese – unabhängig von z.B. eingestellten Altersstufen – stets zugänglich gemacht werden. Spiegelbildlich bezeichnet eine *Blocklist* solche Elemente, die im individuellen Kontext nicht verfügbar sein sollen, obwohl sie ausweislich ihrer Kennzeichnung altersgerecht sind. Die bisherigen Bezeichnungen „Whitelist" und „Blacklist" verwendet die FSM nicht mehr.

dem Regulierungsvorschlag nicht zu erwarten ist. Das bedeutet, dass es für das Angebot beispielsweise eines bestimmten Video-on-Demand-Dienstes eine Vielzahl Mechanismen geben müsste, um adäquat auf die Jugendschutzvorrichtungen der verschiedenen Betriebssysteme reagieren zu können.

2.2.5. (noch) Nicht als geeignet bewertete technische Mittel

Die besonderen Regelungen aus § 12b JMStV-E (Abs. 1: grundsätzliche Privilegierung/Sichtbarkeit unabhängig von der Bewertung der App; Abs. 2: Berücksichtigung der Altersstufen in Jugendschutzvorrichtung und App sowie Geltung der jeweils niedrigeren) gelten nur, wenn es sich bei dem eingesetzten Jugendschutzprogramm bzw. dem vom Anbieter verwendeten technischen Mittel um ein *geeignetes* und als solches vor allem *zertifiziertes* handelt (§ 12b Abs. 2 S. 1 i.V.m. §§ 11 Abs. 2, 5 Abs. 4 S. 1 Nr. 1, Abs. 11 JMStV-E).

Die Vorlage nach § 5 Abs. 11 JMStV-E ist jedoch optional, was bedeutet, dass es dem Anbieter unbenommen bleibt, z.B. für Inhalte ab 16 oder 18 ein technisches Mittel einzusetzen, dessen Eignung er nicht durch Vorlage bei der Selbstkontrolle hat zertifizieren lassen. Er bleibt - wie bisher - unmittelbar für die Gewährleistung eines ausreichenden Jugendschutzniveaus verantwortlich.

Unklar ist in diesem Zusammenhang,

- mit welcher Altersstufe der Anbieter eine solche App zu bewerten hat (§ 12a JMStV): Enthält die App Inhalte ab 16, die aber mit einem rechtskonformen, wenn auch nicht ausdrücklich als geeignet zertifizierten technischen Mittel geschützt sind, wäre dann eine Kennzeichnung z.B. mit „ab 12“ (oder konsequenterweise „ab 0“) zutreffend? Schließlich wären für zu junge Nutzerinnen und Nutzer ja keine entwicklungsbeeinträchtigenden Inhalte verfügbar;

- wie die Jugendschutzvorrichtung zu agieren hätte: Muss das Angebot zum einen sichtbar und zum anderen auch nutzbar sein, *weil* es mit der niedrigen Stufe gekennzeichnet ist und *obwohl* es auch Inhalte mit einer höheren Altersstufe enthält?

Die Einführung *eignungsüberprüfter* technischer Mittel (§ 5 Abs. 11 JMStV-E) ist somit auch hier nicht von Vorteil, sondern erzeugt eine Rechtsunsicherheit, die es bisher nicht gab.

2.3. Verschiedenes

Das **Zusammenspiel von Jugendschutzprogramm und Jugendschutzvorrichtung** gibt an einer entscheidenden Stelle Rätsel auf: Eine mit einer hohen Altersstufe gekennzeichnete App darf entgegen § 12 Abs. 2 S. 2 Nr. 3 JMStV-E *ausnahmsweise* dennoch (jedenfalls grundsätzlich) zugänglich gemacht werden, wenn ein geeignetes Jugendschutzprogramm oder ein geeignetes technisches Mittel eingesetzt wird (§ 12b Abs. 1 JMStV-E; für die hiesige Darstellung: „Entscheidung 1“). In der zweiten Stufe muss sodann innerhalb der App geprüft werden, ob die dort eingestellte Altersstufe oder die in der Jugendschutzvorrichtung ausgewählte niedriger ist (§ 12b Abs. 2 S. 1 JMStV-E; für die hiesige Darstellung: „Entscheidung

2“). Während „Entscheidung 1“ durch das Betriebssystem bzw. die Jugendschutzvorrichtung zu treffen ist, obliegt „Entscheidung 2“ der App. Letzteres ist nachvollziehbar und jedenfalls in der Theorie, vorbehaltlich praktischer Umsetzungsfragen, auch denkbar (z.B. Abfrage bzw. Nutzung einer entsprechenden Schnittstelle). Schon Ersteres ist jedoch unmöglich, denn die Jugendschutzvorrichtung kann gar nicht wissen, ob die fragliche App über ein geeignetes bzw. als solches zertifiziertes Jugendschutzsystem verfügt. Wie ein solcher Kommunikationskanal für „Entscheidung 1“ aussehen kann, bleibt offen und ist auch nicht ohne Weiteres denkbar. Anders als eine anzugebende Altersstufe wäre ein Datenfeld über die erfolgreiche Eignungsprüfung eines Jugendschutzprogramms in keiner Weise international anschlussfähig.

Unklar wäre zudem, wer hier die **Verantwortung** für die Weitergabe der „richtigen“ Information tragen würde.

Während § 12a JMStV-E beschränkt ist auf Apps, die in systemeigenen Vertriebsplattformen angeboten werden (Appstores), erstreckt sich § 12b JMStV-E auf *alle* Anwendungen, also auch auf solche, die nicht über Appstores vertrieben werden. Dies erzeugt für die Umsetzung weitere Hürden: Zwar wäre die „Kommunikation“ zwischen Apps und Betriebssystem im Rahmen von Appstores zumindest grundsätzlich möglich, es ließen sich also Kanäle für die wechselseitige Kommunikation finden. **Programmen, die ohne Einbeziehung eines Appstores genutzt werden können, fehlt jedoch diese Kommunikationsmöglichkeit** – und umgekehrt fehlt dem Betriebssystem die Option, bei solchen Programmen Informationen abzufordern. Damit wird eine – weitere – externe Schnittstelle, mit der das Betriebssystem offen über das (eingestellte) Alter der Nutzerin bzw. des Nutzers informieren und Informationen darüber abfragen muss, ob die App über ein als geeignet bewertetes Jugendschutzprogramm verfügt, erforderlich. Der für § 12b Abs. 2 JMStV-E notwendige Informationsaustausch kann sonst denklogisch nicht gewährleistet werden.

In § 5 Abs. 4 S. 1 Nr. 2, 2. Alt. JMStV-E wird die Alterskennzeichnung für die Jugendschutzvorrichtung als für Inhalteanbieter gleichwertige Alternative zur Kennzeichnung für ein Jugendschutzprogramm dargestellt. Das würde bedeuten, dass **grundsätzlich auch Websites entsprechend gekennzeichnet** werden könnten, denn die Regelung enthält keine Einschränkung auf Apps. Weil eine entsprechende Kennzeichnung aber vorhersehbarerweise nur von äußerst wenigen Anbietern genutzt werden würde, würden Eltern ggf. dem trügerischen Missverständnis unterliegen, sie könnten mit der Jugendschutzvorrichtung auch das Surfen im Netz reglementieren, was jedoch nicht der Fall ist. Weil das Konzept „Jugendschutzvorrichtung“ erkennbar auf Apps fokussiert und Webinhalte gar nicht umfassen *will*, sollte dies auch im Text der Norm erkennbar werden.

In der Überschrift von § 12b JMStV-E sowie in dessen Absatz 1 muss es statt „anerkanntes“ richtigerweise „geeignetes“ Jugendschutzprogramm lauten. Der Terminus „anerkanntes Jugendschutzprogramm“ wird vom Gesetz nicht mehr verwendet, seit die Zuständigkeit für die Feststellung der Eignung von der KJM auf die Selbstkontrollen übergegangen ist.

Die Regelung des § 5 Abs. 4 S. 1 Nr. 2 JMStV-E verweist zutreffend auf „*geeignete* Jugendschutzprogramme“, bei der Jugendschutzvorrichtung fehlt dieses Attribut jedoch, vermutlich

versehentlich. Richtigerweise muss wohl auch hier auf die erfolgte Eignungsüberprüfung gesetzt werden, wie der entsprechende Verweis auf das „Verfahren nach §§ 11 Abs. 4, 19a Abs. 2 und 19b Abs. 2“ in § 12 Abs. 4 S. 2 JMStV-E nahelegt.

§ 12 Abs. 2 S. 1 Nr. 3 JMStV-E begrenzt die *Zugänglichkeit* von altersangemessenen Apps. In Nr. 2 fehlt ein entsprechender Hinweis für deren *Installationsmöglichkeit*.

Die pauschale Ausnahme für - potenziell - entwicklungsbeeinträchtigende Angebote, die Nachrichten enthalten (**Nachrichtenprivileg**, § 12a S. 2 i.V.m. § 5 Abs. 8 JMStV-E), ist nicht unproblematisch. Es sollte in jedem Fall möglich sein, solche Apps einer persönlichen Blocklist (§ 12 Abs. 2 S. 1 Nr. 5 JMStV-E) hinzuzufügen, um Eltern eine entsprechende Zugangsregulierung zu ermöglichen. Beachtlich ist schließlich, dass nicht selten einzelne Inhalte von (Nachrichten-)Apps über eine **Altersbewertung einer Selbstkontrolleinrichtung** verfügen. So werden z.B. zahlreiche Dokumentationen, die in solchen Angeboten enthalten sind, durch die FSF bewertet. Enthält die App aber Inhalte, die z.B. entwicklungsbeeinträchtigend für Kinder und Jugendliche unterhalb einer bestimmten Altersstufe sind und ist dies durch eine Entscheidung der Selbstkontrolle manifestiert, so scheidet eine Kennzeichnung des Gesamtangebots als „nicht entwicklungsbeeinträchtigend/ohne Altersbeschränkung“ aus. In der Praxis bedeutet das, dass Inhalteanbieter auf eine strikte Trennung achten müssen zwischen Nachrichten-Apps (die mit „ohne Altersbeschränkung“ gekennzeichnet werden dürfen) und Angeboten, die ggf. mit einer Altersstufe bewertete Dokumentationen enthalten.

Einige Vorgaben, wie der Pflicht, bestimmte Browser zu sperren oder den Zugang zu Apps auf „die systemeigenen Vertriebsplattformen“ (§ 12 Abs. 2 S. 1 Nr. 1 und 2 JMStV-E) zu beschränken, widersprechen dem Grundgedanken europarechtlicher (Wettbewerbs-)Vorschriften (vgl. Art. 6 Nr. 4 DMA-E). Der Gesetzentwurf lässt nicht erkennen, dass und warum diese Rechtsgedanken miteinander in Einklang gebracht werden können.

Zudem scheint die Verpflichtung der Betriebssystemanbieter, bei eingeschalteter Jugendschutzvorrichtung eine **gesicherte Suchfunktion** zu aktivieren, auch technisch kaum umsetzbar zu sein. Denn Betriebssystemanbieter können einen Browser nur unter bestimmten, eng begrenzten Umständen auf technischem Wege dazu zwingen, in den Suchmaschinen eine Safe Search-Funktion zu aktivieren, da diese grundsätzlich eben eine Funktion der Suchmaschine selbst und nicht des zu diesem Dienst den Zugang ermöglichenden Browsers ist. Laut Entwurf sollen Browser, in denen die Safe Search-Funktion nicht aktiviert werden kann, nicht zugänglich gemacht werden. Da abgesehen von einer Sonderkonstellation (Anbieter eines Betriebssystems ist zugleich Anbieter eines Browsers und einer Suchmaschine) die Umsetzung dieser Pflicht nicht möglich ist, würde dies folglich zu einer **regelmäßigen Sperrung systemfremder Browser** führen.

Unklar ist in diesem Zusammenhang, wie die Feststellung, es liege eine *ausreichend* „gesicherte Suche“ vor, erfolgen soll: Die KJM legt fest, für welche Suchmaschinen die Vorschriften überhaupt anwendbar sind (§ 16 S. 2 Nr. 7 JMStV-E), und sie legt im Benehmen mit den Selbstkontrollen die Bewertungskriterien fest (§ 12 Abs. 4 S. 1 JMStV-E). Die dortige Verweiskette auf §§ 11 Abs. 4, 19a Abs. 2 und 19b Abs. 2 JMStV-E legte nahe, dass wiederum die Selbstkontrollen für die Eignungsüberprüfung (mit nachfolgender Überprüfung durch die

KJM) zuständig sein sollen. Dieses von der Prüfung von Jugendschutzvorrichtungen denklogisch strikt zu trennende Verfahren führt zu einer weiteren deutlichen Verlängerung von Vorlaufzeiten, bis die angedachte neue Systematik – theoretisch – in der Praxis funktionsfähig ist.

Hinsichtlich der Pflicht, Apps auf systemeigene Vertriebsplattformen zu beschränken, stellt sich zudem die Frage, was dies für solche **Betriebssysteme** bedeutet, **die keine systemeigene Vertriebsplattform vorhalten**.

Die Formulierung in § 12 Abs. 1 S. 3 Nr. 2 JMStV-E ist unglücklich, sie lautet:

> *„Zudem ist bei … erstmaliger Aktivierung der Jugendschutzvorrichtung … auf die Möglichkeit, die Jugendschutzvorrichtung zu aktivieren, hinzuweisen…“*

Was gewollt ist, wird nicht klar. Hingegen ist die Formulierung in Nr. 3 („bei … Aktualisierung des Betriebssystems“) ausgesprochen weitreichend, da dies, wörtlich genommen, bei vielen Betriebssystemen sehr häufig der Fall wäre. Sinn und Zweck der Regelung scheint, bei jeder grundlegenden Veränderung des Systems, bei der die Nutzerinnen und Nutzer vom Einführen neuer oder vom Wegfall bestehender Funktionen ausgehen kann, auf die Jugendschutzvorrichtung hinzuweisen - nicht jedoch bei jedem Patch. Dies sollte in der Formulierung entsprechend zum Ausdruck kommen.

3. Jugendschutzprogramme

Etablierte und bei Eltern bekannte Systeme werden durch den Gesetzentwurf zurückgedrängt. Der Einsatz individueller Schutzmechanismen würde seltener und - für Anbieter und Familien - weniger attraktiv.

3.1. Angestrebtes Ziel

Der Gesetzentwurf enthält zunächst eine unbedingt **zu befürwortende Regelung**, mit der die bisherige Ungleichbehandlung von Video on Demand und digitalem Rundfunk aufgehoben wird: § 11 JMStV-E ist künftig nicht mehr in einem eigenen Abschnitt über Telemedien verortet, sondern in einem allgemeinen zum Thema technischer Jugendmedienschutz. Zahlreiche heute bereits verfügbare Angebote enthalten sowohl Inhalte auf Abruf, als auch lineare Kanäle bzw. Sendungen. Um für die Nutzerinnen und Nutzer den Jugendschutz „aus einem Guss“ zu gewährleisten, wird nur klargestellt, dass Jugendschutzprogramme für alle Arten digital vermittelter Inhalte genutzt werden können, sofern die jeweiligen Voraussetzungen (z.B. maschinenlesbare Alterskennzeichnung) gegeben sind. Sogenannte hybride Angebote sind somit ausdrücklich umfasst.

Diesem Gedanken folgend, ist sodann aber eine **redaktionelle Folgeänderung** in § 11 Abs. 1 S. 3 JMStV erforderlich: Dort ist derzeit noch lediglich vom „differenzierten Zugang zu *Telemedien*“ die Rede.

Nicht in den Blick genommen hat der Gesetzgeber allerdings die **Stärkung und den Ausbau des bereits sehr gut etablierten Systems „Jugendschutzprogramm für geschlossene Systeme“ (§ 11 Abs. 2, 2. Alt. JMStV)**. Während im Bereich Video on Demand beinahe flächendeckend entsprechende Systeme im Einsatz sind und von den Familien auch genutzt werden sowie im Bereich Computer-/Konsolenspiele wichtige erste Schritte gegangen worden sind, fehlt es bislang an einer Zertifizierung von Appstores. Bestehende Anreize zu verstärken, die Anforderungen sektorspezifisch zu konkretisieren (bzw. zu öffnen) und für eine entsprechende Bekanntheit zu sorgen, sollte also vorrangiges Ziel sein - und nicht die Schwächung des etablierten Systems.

3.2. Erwartete Auswirkungen

Für die Anbieter von Inhalten, die nicht für Nutzerinnen und Nutzer aller Altersstufen geeignet sind, stehen die Optionen „Jugendschutzprogramm“ und „Jugendschutzvorrichtung“ ausweislich des Gesetzentwurfs als gleichwertige Alternativen zur Verfügung (§ 5 Abs. 4 S. 1 Nr. 2 JMStV-E). Bei genauerem Hinsehen ist dies jedoch tatsächlich nicht der Fall, und **die Entscheidung zugunsten eines nutzerautonomen und altersdifferenzierenden Jugendschutzprogrammes würde sich als nachteilig erweisen**:

- Für die Anbieter, die ein Jugendschutzprogramm i.S.d. § 11 Abs. 2 JMStV einsetzen, wird aus der Sollvorschrift des § 5 Abs. 2 JMStV-E (Risiken für die persönliche Integrität von Kindern und Jugendlichen) eine strikte Verpflichtung. Wer sich für eine durch die Jugendschutzvorrichtung auslesbare Alterskennzeichnung entscheidet, unterliegt dieser Verpflichtung nicht.

- Durch diese Logik müsste es künftig zu einer Filtermöglichkeit nach Interaktionsrisiken kommen (§ 11 Abs. 2 S. 2 JMStV-E). Eine solche mag grundsätzlich - eine schnelle rechtskonforme Umsetzung der entworfenen Regelungen unterstellt - in Deutschland einen gewissen Effekt haben; gleichwohl würde sie Eltern in trügerischer Sicherheit wiegen, dass sie z.B. mit einem „Chat nicht zugelassen“-Schalter jegliche Onlinekommunikation ihrer Kinder unterbinden würden: Dies wäre mit Blick auf internationale Angebote aber ausdrücklich nicht der Fall.

- Die Pflicht zur technischen Auslesbarkeit bestimmter Interaktionsrisiken (§ 11 Abs. 2 S. 2 JMStV-E i.V.m. § 5 Abs. 2 JMStV-E) führt zu einer erneut weitergehenden Belastung für Anbieter von Jugendschutzprogrammen und damit zu einer Benachteiligung gegenüber denjenigen, die sich zugunsten der Jugendschutzvorrichtung gegen ein solches Programm entscheiden.

- Ein Jugendschutzprogramm muss nicht nur die komplexen Eignungskriterien des § 11 JMStV erfüllen, sondern es muss zusätzlich noch die fehlerfreie Interaktion mit

der Jugendschutzvorrichtung sicherstellen (§ 12b Abs. 2 JMStV-E). Weil beide Systeme - wenn überhaupt - nur sehr aufwendig miteinander in Einklang zu bringen sind, kommt es also zu einer Schlechterstellung derjenigen Anbieter, die sich bereits heute an die hohen JMStV-Standards halten.

- Die bislang im Bereich technischer Jugendschutz bereits sehr engagierten Akteure werden für ihr Engagement mit zusätzlichen Entwicklungs- und Umsetzungspflichten „bestraft". Statt Anreize zu schaffen, individualisierbare und moderne Jugendschutzfeatures (weiter-)zu entwickeln, werden die Anbieter im Gegenteil dazu ermutigt, weniger gute Systeme anzubieten, die den Familien einen deutlich kleineren Gestaltungsspielraum geben.

- Wenn ein einfaches, preiswertes Jugendschutzsystem gleichwertig ist mit einem anspruchsvollen, nutzerautonomen, dann werden Unternehmen sich für die günstige Option entscheiden und damit hinter das heute bereits erreichte Niveau zurückfallen. Hierbei werden betriebswirtschaftliche Aspekte sehr schnell den Ausschlag geben, wenn die Entwicklung und der Einsatz eines guten, aber teuren Systems durch die Anwendung eines kostengünstigeren, aber deutlich schlechteren Systems ersetzt werden können. Der Gesetzgeber würde mit der von ihm angestrebten Lösung dem Jugendschutz in Deutschland den sprichwörtlichen Bärendienst erweisen.

4. Apps

Die neuen Pflichten für Anbieter von Apps bringen Unsicherheit in das System des gesetzlichen Jugendmedienschutzes. Sie haben unerwünschte und - für Anbieter und Familien - unvorhersehbare Auswirkungen und können die Qualität von Altersfreigaben negativ beeinflussen.

Durch die Legaldefinition von Apps in § 3 S. 1 Nr. 7 JMStV-E, die nicht dem allgemeinen Begriffsverständnis entspricht, kommt es zu Unsicherheiten, die weder auf der Ebene des Gesetzes, noch durch die beteiligten Akteure oder durch die Eltern aufzulösen sein werden. Wenn der JMStV-E ausdrücklich nur solche Programme adressiert, „die der unmittelbaren Ansteuerung von Angeboten nach Nr. 1 [eine Sendung oder der Inhalt von Telemedien] dien[en]", nimmt er Dienstprogramme und Anwendungen wie z.B. Taschenrechner, eine Textverarbeitung oder den E-Mail-Client bewusst aus. Dies ist aus Jugendschutzsicht folgerichtig. Im allgemeinen Begriffsverständnis wird jedoch als App eine „zusätzliche Applikation, die vor allem auf Smartphones und Tablet-PCs heruntergeladen werden kann"[4], bezeichnet,

[4] https://www.duden.de/rechtschreibung/App (13.06.2022).

also ohne diese inhaltliche Beschränkung. Die jugendschutzrechtlichen (Kennzeichnungs-) Pflichten sollen nun nur erstere betreffen, für letztere würde das Gesetz nicht gelten.

Weil ordnungswidrig handelt, wer seine App (i.S.d. JMStV-E) nicht nach § 12a S. 1 JMStV-E mit einer Altersstufe versieht (§ 24 Abs. 1 Nr. 12 JMStV-E), kommt es für deutsche Anbieter, also solche, die durch die KJM erreichbar und sanktionierbar sind, zu einer **Kennzeichnungspflicht** von Inhalten unabhängig von deren Jugendschutzrelevanz. Dies widerspricht der bisherigen Regelungslogik des § 5 JMStV, der nur solche Inhalteanbieter zu Maßnahmen verpflichtet, die auch tatsächlich jugendschutzrelevante Inhalte verbreiten.

§ 12 Abs. 2 Nr. 3 JMStV-E sieht vor, dass bei aktivierter Jugendschutzvorrichtung lediglich jene Programme zugänglich gemacht werden dürfen, deren Alterskennzeichnung dem betriebssystemseitig eingestellten Alter entspricht. Dies bedeutet, dass **Apps ohne Alterskennzeichnung nicht angezeigt** werden. Weil aber durch das Betriebssystem i.d.R. nicht unterschieden werden kann, ob es sich um App i.S.d. JMStV-E handelt oder um ein Dienstprogramm, müssten *alle* Applikationen mit einer Altersstufe versehen werden. Es stellt sich hier auch die Frage, ob dies ansonsten mit der Erwartungshaltung von Eltern vereinbar ist. Denn Eltern, die eine Jugendschutzvorrichtung aktivieren, erwarten die Unterbindung unproblematischer Programme (z.B. Taschenrechner, Textverarbeitung, E-Mail-Client) eben gerade nicht. Dies ist vor allem im **schulischen Kontext** relevant.

Die Regelung führt somit zu einer **faktischen Kennzeichnungspflicht für alle Appanbieter**, also auch für diejenigen, die bisher keine Alterskennzeichnung haben, da sie überhaupt keine jugendschutzrechtliche Relevanz aufweisen und völlig unproblematisch sind, oder die – eigentlich – nicht von den Regeln des JMStV-E erfasst werden, weil sie nicht dem Zugang zu Telemedien dienen.

Unterschiedslos gilt das auch für Anbieter mit Sitz im Ausland, die einer Sanktionsgewalt der KJM nicht unterliegen. Weil dies unmittelbar beschränkende Wirkungen für Anbieter in einem EU-Mitgliedsstaat hätte, stellt sich hier erneut die Frage nach der **Vereinbarkeit mit Europarecht**. Denn die jetzt vorgeschlagene Regelungssystematik führt dazu, dass auch solche Anbieter praktisch den Pflichten des §12b Abs. 2 JMStV-E unterliegen, deren Apps andernfalls in Deutschland von einem Betriebssystem auf Geräten mit aktivierter Jugendschutzvorrichtung nicht angezeigt werden dürften. Ob diese App nach den Vorschriften des Sitzlands des Anbieters rechtskonform ist und auch objektiv eine gute Schutzwirkung erzielt, ist dabei irrelevant. Eine Durchbrechung des Herkunftslandsprinzips auf diese Weise dürfte aber nicht gerechtfertigt und damit unzulässig sein.

Anders als § 12a JMStV-E ist die Regelung des § 12 Abs. 2 Nr. 3 JMStV-E nicht auf solche Apps beschränkt, die über systemeigenen Vertriebsplattformen verteilt werden. Das bedeutet, dass solche Apps tendenziell grundsätzlich gesperrt werden müssen, weil es für sie gar keine Kennzeichnungsmöglichkeit gibt. Dies betrifft gerade bei den eher offenen Betriebssystemen wohl die Mehrzahl der verfügbaren Programme. Aus diesem Grund sollte diese Vorgabe auf Apps beschränkt werden, die über die systemeigene Vertriebsplattform zugänglich sind.

Die Pflicht, *irgendwie* eine Altersstufe für eine App zu ermitteln und diese - maschinenlesbar - anzugeben, führt zu einer weiteren Unsicherheit im Hinblick auf die **Qualität der Alterskennzeichnung**: Zwar könnte das Fehlen einer Alterseinstufung sanktioniert werden (entweder direkt durch die KJM oder indirekt durch das Ausschließen der App aus dem Kreis verfügbarer Angebote). Für die Richtigkeit der Alterseinstufung besteht jedoch keine Gewähr, zumal der Anbieter der Jugendschutzvorrichtung bzw. des Betriebssystems die ordnungsgemäße Alterseinstufung in der Regel nicht überprüfen kann. Gleichzeitig müssten sich die Eltern aber darauf verlassen können, dass entsprechend ihrer Vorgaben nur die *richtigen*, altersangemessenen Apps verfügbar sind.

Unklar ist nämlich auch, wie sich der offenbar beabsichtigte Wechsel im System der Verantwortlichkeiten (vgl. oben Ziff. 1.2) auf den Vorgang der Alterskennzeichnung bzw. die Verantwortlichkeit für das Zutreffen der Bewertung auswirken würde: Darf der Appanbieter abschließend über die Altersstufe seiner App entscheiden oder kann der Anbieter des Appstores bzw. des Betriebssystems diese Entscheidung überstimmen bzw. abändern? Sollte sich die Altersbewertung falsch als zu niedrig erweisen, das Angebot also rechtswidrig sein, fragt sich, welche Partei entsprechend Betroffener bzw. Verantwortlicher gegenüber der KJM wäre. Dadurch, dass der **Betriebssystemanbieter neu in die Rolle eines Jugendschutz-Gatekeepers hineinwächst** und er letztlich über die Verfügbarkeit von Inhalten entscheiden kann, ist er auch potentieller Adressat von Aufsichtsmaßnahmen. Er ist jedoch, wie oben ausgeführt, ausgesprochen „weit weg“ von den Inhalten und wird vor allem bei komplexeren Angeboten kaum je in der Lage sein, eine zutreffende Bewertung zu gewährleisten. Gleichwohl getroffene Entscheidungen der Betriebssystemanbieter sind im Hinblick auf die Medien- und Rundfunkfreiheit der Appanbieter höchst kritisch zu betrachten.

Bislang nicht erkennbar ist, wie eine App zu kennzeichnen wäre, die entwicklungsbeeinträchtigende Inhalte **nur zu bestimmten Zeiten** zugänglich macht (§ 5 Abs. 4 S. 1 Nr. 3 JMStV-E): Erhalten sie eine hohe Altersstufe, sind sie auch tagsüber, wenn also keine ungeeigneten Inhalte verfügbar sind, gesperrt. Erhalten sie eine niedrige Altersstufe (weil problematische Inhalte auf andere Weise reguliert werden), kommt es zu einer Lücke in der Jugendschutzvorrichtung, die von der Tageszeit abhängig ist. Dies müsste für Eltern transparent und ggf. steuerbar sein.

5. Risikodimensionen, Kennzeichnungen

Das Verhältnis der neuen Risikodimension „persönliche Integrität“ im JMStV zu einer ähnlichen, aber spezifischeren Regelung im JuSchG ist unklar. Im Zusammenhang mit den neuen Kennzeichnungspflichten stellen sich systematische Fragen, die der Gesetzentwurf nicht beantworten kann.

5.1. Persönliche Integrität

In § 1 JMStV-E werden die Schutzziele des Gesetzes um die „persönliche Integrität“ ergänzt. Damit soll eine Angleichung an die Regelung des JuSchG (dort §§ 10a Nr. 3, 10b Abs. 3) und eine Öffnung des JMStV für sog. Interaktionsrisiken erfolgen. An dieser Stelle sei zunächst darauf hinzuweisen, dass diese Risikodimension im JMStV keine Definition oder Eingrenzung erfährt. So bleibt unklar, welche Risiken damit genau gemeint sind.

Weiter wird der Begriff der „persönlichen Integrität“ in § 5 Abs. 2 JMStV-E aufgegriffen, wo eine Pflicht zur Kenntlichmachung der Interaktionsrisiken durch optische und technisch auslesbare Kennzeichen geschaffen wird. Doch auch hier bleibt fraglich, wie und durch wen eine Definition und Eingrenzung erfolgen soll. § 19a Abs. 3 JMStV-E sieht zwar eine Aufgabenzuschreibung hinsichtlich der Kriterien für Hinweise auf die Gründe der Alterseinstufung (§ 5 Abs. 1 S. 3 JMStV-E) vor, nicht jedoch für die Ausgestaltung der optischen und technisch auslesbaren Kennzeichen. Dass sich hierbei in kurzer Zeit eine Vielzahl unterschiedlicher Optionen herausbilden würde, ist sehr wahrscheinlich; eine Standardisierung ist im Hinblick auf die insoweit vergleichbaren Regelungen im JuSchG erforderlich.

Ein Vergleich mit dem JuSchG zeigt, dass hier eine sehr pauschale Regelung getroffen wurde, die gegebenenfalls sehr weitreichend sein kann, da beispielsweise weder ein *numerus clausus* der Risiken, noch der anzuwendende Gefährdungsmaßstab genannt wird. Auch eine Bagatellgrenze für die Kennzeichnung (z.B. wenig genutzte Angebot), wie sie das JuSchG kennt, fehlt. Des Weiteren bleibt unklar, wie das Verhältnis zwischen der Alterskennzeichnung und dem Deskriptor für die Beeinträchtigung der persönlichen Integrität sein soll.

Hierzu passt es nicht, dass § 11 Abs. 2 S. 2 JMStV-E eine Pflicht für Jugendschutzprogramme vorsieht, diese Risiken zu steuern. Inkonsistent erscheint es zudem, dass eine Jugendschutzvorrichtung diese Option nicht bieten soll.

5.2. Erweiterte Kennzeichnungspflichten

Im Zusammenhang mit der Kennzeichnungs- und Hinweispflicht wirft jedoch nicht nur § 5 Abs. 2 JMStV-E Fragen auf, sondern auch **§ 5 Abs. 1 JMStV-E**. So heißt es dort in Satz 3, dass auf die wesentlichen Gründe für die Alterseinstufung an geeigneter Stelle hingewiesen werden solle. Diese Formulierung in Form einer Soll-Vorschrift steht jedoch im Widerspruch zu der tatsächlich nicht bestehenden Kennzeichnungspflicht. Denn § 5 Abs. 1 JMStV zwingt zur Alterseinschätzung/-bewertung, aber nicht zu einer Kennzeichnung. Wenn es also keine Pflicht zur Mitteilung der Altersstufe gibt, so kann es erst recht keine Pflicht zur Begründung geben. Zudem sei an dieser Stelle darauf hingewiesen, dass die Parallelvorschrift in § 14a Abs. 1 S. 3 i.V.m. § 14 Abs. 2a JuSchG anders als hier auf Anbieter beschränkt ist, die mindestens eine Million Nutzer haben (§ 14a Abs. 2 JuSchG).

Die Kennzeichnungspflicht in **§ 10 JMStV-E** entspricht zunächst im Wesentlichen der Regelung aus dem bisherigen § 12 S. 1 JMStV, soweit auf Filme oder Spiele auf Bildträgern verwiesen wird. Neu ist, dass „Sendungen im Fernsehen“ und deren „Alterseinstufung nach § 5 Abs. 1“ einbezogen werden. Dies erscheint mit dem Ziel der Vereinheitlichung von Kennzeichnungen nach JuSchG und JMStV zunächst sinnvoll. Hierbei ist jedoch beachtlich, dass

- anders als nach §§ 14, 14a JuSchG - Sendezeitfreigaben oder andere Alterseinstufungen für den Rundfunk nicht angegeben werden *müssen*, es gibt also - mit Ausnahme von § 5c Abs. 2 JMStV – richtigerweise keine Kennzeichnungspflicht im Fernsehen. Der Anwendungsbereich der ergänzenden Regelung dürfte also sehr schmal sein, zumal in der Formulierung auch unklar bleibt, wessen „Alterseinstufung“ gemeint ist: die einer Selbstkontrolle, die von Jugendschutzbeauftragten der Sender oder die implizite Einstufung von Sendungen im Tagesprogramm, die oftmals keiner besonderen Überprüfung unterzogen werden? Nachdem es bereits weitreichende Kennzeichnungspflichten in Telemedien gibt (§§ 5c Abs. 2, 12 JMStV sowie § 14a JuSchG), sollte daher die Formulierung *„oder Sendungen im Fernsehen“* wegen mangelnder Klarheit gestrichen werden.

Sinn und Zweck der neuen Kennzeichnungspflicht in **§ 5 Abs. 5 JMStV-E** sind unklar. Zunächst wird richtigerweise lediglich die erfolgte Kennzeichnung für ein Jugendschutzprogramm nach § 11 Abs. 1 JMStV (nicht: für geschlossene Systeme nach Abs. 2, 2. Alt.) gemeint sein können. Die Kennzeichnung für eine Jugendschutzvorrichtung ist hingegen entbehrlich: Handelt es sich um eine App, die über eine systemeigene Vertriebsplattform des Betriebssystems abrufbar ist, muss sie in jedem Fall (mit einer Altersstufe) gekennzeichnet werden (§ 12a S. 1 JMStV-E); dann aber ergibt sich aus der Kennzeichnung nach § 5 Abs. 5 JMStV-E kein Mehrwert. Nach hiesigem Verständnis bleibt als Regelungsgehalt die Hinweispflicht auf eine erfolgte (technische) Alterskennzeichnung mit **age-de.xml**; dann sollte die Verweisung aber entweder spezifisch auf § 5 Abs. 4 S. 1 Nr. 2, 1. Alt. JMStV-E oder (besser) im Sinne der leichteren Verstehbarkeit auf die “Kennzeichnung für ein Jugendschutzprogramm im Sinne des § 11 Abs. 1 JMStV” erfolgen.

6. Aufgabenverteilung zwischen KJM und Selbstkontrollen

Ein bewährtes und von allen Akteuren geschätztes System soll einer vollständigen Neuorganisation unterzogen werden. Warum dies erfolgen soll, ist unklar. Im Ergebnis käme es zu Entwicklungs- und Innovationshemmnissen, höheren Kosten und langwierigeren Verfahren. Das Konzept ist inkompatibel mit einem wesentlichen Element der „BIK+ Strategie“ der Europäischen Kommission.

6.1. Situation nach geltendem Recht

Die Vorgaben zum technischen Jugendmedienschutz werden bislang so verstanden, dass sie einen direkten Einfluss auf die Bewertung bzw. die Zulässigkeit von Inhalten haben. Das bedeutet, dass ein Angebot nur dann rechtskonform sein kann, wenn es - soweit erforderlich - ordnungsgemäß abgesichert ist. Die Ausgestaltung der technischen Schutzmaßnahmen liegt damit grundsätzlich im Pflichtenkreis der jeweiligen Anbieter. Jugendschutzprogramme nach § 11 Abs. 1 JMStV bilden insoweit eine Ausnahme.

KJM und FSM sind gleichermaßen zur Überprüfung der Jugendschutzkonformität von Onlineangeboten berufen: die FSM als Selbstkontrolle dabei primär beschränkt auf die ihr angeschlossenen Unternehmen, die KJM spiegelbildlich grundsätzlich unter Ausklammerung dieser Anbieter.

Diese geteilte Aufgabenwahrnehmung von KJM und FSM hat dazu geführt, dass über die Jahre eine Vielzahl an unterschiedlichen technischen Mitteln und Altersverifikationssystemen (AVS) entwickelt worden und den beiden Stellen zur Überprüfung vorgelegt worden ist. Dabei hat es sich als gewinnbringend erwiesen, dass die KJM ihre Rechtsauffassung zu den jeweiligen Anforderungen veröffentlicht und allen Akteuren damit einen allgemeinen Rahmen vorgibt, zum Teil ergänzt um detaillierte Ausführungen zu technischen Einzelheiten (Bewertungsraster).

Diese Bewertungsraster werden auch durch die FSM in ihren Entscheidungen einbezogen, wobei sie ausdrücklich nicht zwingendes Recht darstellen. Die FSM kann im Rahmen ihres Beurteilungsspielraumes (§ 20 Abs. 5 JMStV) eine im Detail abweichende Entscheidung treffen. Dies wird immer dann relevant, wenn Mitgliedsunternehmen der FSM Systeme zur Begutachtung und Bewertung vorlegen, die einen neuen technologischen Ansatz verfolgen und innovative Lösungen beinhalten.

Naturgemäß können die Bewertungsraster der KJM solche Ansätze nicht in jeder denkbaren Konstellation vorhersehen, auch wenn sie grundsätzlich technologieoffen sind. Bisher bezieht die KJM neue Entwicklungen jedoch bei der Weiterentwicklung ihrer Bewertungsraster mit ein, um anderen Anbietern für künftige Entwicklungen die Orientierung zu erleichtern, was ausgesprochen hilfreich ist.

Es sind weder von der KJM noch von den Selbstkontrollen Äußerungen bekannt, die eine Veränderung dieses Systems einfordern würden. Auch am Markt sind insoweit keine Defizite erkennbar. Wissenschaftliche Erkenntnisse über Unzulänglichkeiten fehlen ebenfalls.

6.2. Angestrebtes Ziel

Mit der vorgeschlagenen Neuregelung würden zwei grundsätzliche Punkte verändert:

- Bewertungskriterien und Eignungsanforderungen müssen von der KJM verbindlich vorab festgelegt werden, wobei das Benehmen mit den Selbstkontrolleinrichtungen hergestellt werden soll (§§ 4 Abs. 4, 5 Abs. 10 JMStV-E).
- Es wird ein formelles Eignungsfeststellungsverfahren eingeführt, das dem für Jugendschutzprogramme nachempfunden ist. Hier sollen die Selbstkontrolleinrichtungen eine Entscheidung treffen (§§ 4 Abs. 5, 5 Abs. 11 JMStV-E), die sodann zwingend der KJM zur Prüfung auf Beurteilungsfehler vorzulegen ist (§ 19b Abs. 2 JMStV-E).

Die KJM verlöre somit ihre Befugnis, Positivbewertungen auszusprechen, was sie derzeit kostenfrei tut; die kostenpflichtige Begutachtung durch die Einrichtungen der Freiwilligen Selbstkontrolle wäre künftig die einzige Möglichkeit, die Eignung technischer Systeme rechtssicher vorab feststellen zu lassen.

6.3. Erwartete Auswirkungen

Auf den ersten Blick erscheinen die Neuregelungen als Stärkung der Selbstkontrolleinrichtungen. Dies ist jedoch trügerisch: Können die Selbstkontrollen bisher allein auf Grundlage des Gesetzes und der sich daraus ergebenden Anforderungen an das Schutzniveau Beurteilungen technischer Systeme vornehmen, die durch die KJM nur bei behaupteten Verstößen von Anbietern gegen den Jugendschutz auf mögliche Überschreitungen der rechtlichen Grenzen des Beurteilungsspielraums überprüft werden können, so kann eine Bewertung durch die Selbstkontrollen künftig allein auf Grundlage von vorab verbindlich durch die KJM festgelegten Kriterien erfolgen und muss in jedem Fall der KJM vorgelegt werden, die durch ihre Entscheidung oder deren Unterlassen (§ 19b Abs. 2 JMStV-E) die Bewertung zu einem unbefristeten bestandskräftigen Verwaltungsakt erstarken lässt.

Beide Neuerungen würden **nachteilige Auswirkungen** haben:

Die abstrakte Festlegung von verbindlichen Kriterien für die Eignungsprüfung müsste entweder sehr pauschal und allgemein sein, um entwicklungsoffen und technologieneutral sein zu können. Dann böte sie aber weder Mehrwert noch Orientierung für die Entwickler und Anbieter solcher Systeme. Wenn diese Kriterien hingegen sehr spezifisch und detailliert wären, so würden künftige Entwicklungspfade ohne Not eingeengt. Positivbewertungen wären nur auf „ausgetretenen Pfaden“ möglich, technische Innovationen würden unterbleiben. Aus aktuellem Anlass sei auf die Pressemitteilung der KJM vom 24. Mai 2022 verwiesen, in der sie über die Positivbewertung von AVS berichtet, welche durch Nutzung „künstlicher Intelligenz“ auf den Einsatz von Ausweispapieren zur rechtssicheren Volljährigkeitskontrolle verzichten können[5]. Diese Art von Altersverifikation war bislang im KJM-Raster nicht vorgesehen. Gleichwohl war nun festzustellen, dass das erreichte Schutzniveau ausreichend ist und die Anforderungen aus § 4 Abs. 2 S. 2 JMStV erfüllt werden. Entsprechende Kriterien für noch unbekannte Systeme vorab zu erdenken und rechtssicher festzuschreiben, ist denklogisch ausgeschlossen. Die Praxis zeigt, dass dies auch gar nicht erforderlich ist: Zwei der von der KJM bewerteten Systeme werden von Mitgliedern der FSM angeboten. Die Argumentation für die Erfüllung des gesetzlich geforderten Schutzstandards sowie die Gütekriterien und deren Überprüfung wurden durch die Gutachterkommission der FSM entwickelt und gemeinsam mit einem der beiden Unternehmen erstmals und vor der Vorlage bei der KJM zur Anwendung gebracht. Die KJM konnte ihrerseits diese Argumentation in ihre Bewertung einbeziehen und eine eigene Entscheidung mit ähnlichem Tenor treffen.

Durch die Systematik des Diskussionsentwurfs würde zwar - aus Sicht der Anbieter - Rechtssicherheit geschaffen: Sie könnten vor der Implementierung eines Schutzsystems prüfen, ob es eine bestandskräftige Eignungsfeststellung durch Selbstkontrolle und KJM gibt bzw. selbst eine solche Bewertung einholen. Diese Rechtssicherheit hat jedoch einen hohen zeitlichen Preis, denn wirklich verlässlich ist die Entscheidung erst nach Überprüfung durch die

[5] https://www.kjm-online.de/service/pressemitteilungen/meldung/kjm-bewertet-altersverifikationssysteme-mit-biometrischer-alterskontrolle-positiv (16.6.2022).

KJM. Heute können Anbieter, die ihre Systeme durch die FSM haben prüfen und zertifizieren lassen, diese unmittelbar nach Erteilung der Positivbewertung einsetzen; weitere Schritte oder ein weiteres Zuwarten ist nicht erforderlich. Durch die fehlende Befristung der Entscheidungen entsteht zudem ggf. ein Zuviel an Rechtssicherheit: Es fehlt derzeit eine Regelung, die nach Ablauf einer gewissen Zeit eine erneute Überprüfung einfordert (so aber für Jugendschutzprogramme in § 11 Abs. 4 S. 1 JMStV sowie in der Prüfpraxis der FSM für technische Mittel und Altersverifikationssysteme), womit ein einmal als geeignet bewertetes System grundsätzlich für alle Zeit eingesetzt werden kann: Die Entscheidung der KJM stellt einen bestandskräftigen Verwaltungsakt dar.

Unklar ist, ob die Eignungsbewertung durch eine Selbstkontrolle konstituierend wirken soll: Eine Vorlage scheint optional zu sein, die Erfüllung der Schutzpflichten aus §§ 4 Abs. 2 S. 2 und 5 Abs. 1 JMStV ist davon offenbar nicht abhängig. Etwas anderes gilt offenbar nur, wenn das technische Mittel in einer App eingesetzt werden soll: Die Wirkung von § 12b Abs. 1 JMStV-E tritt nur ein, wenn ein *geeignetes* technisches Mittel eingesetzt wird.

Auch mit Blick auf die jüngst vorgestellte **BIK+ Strategie der Europäischen Kommission**[6] stellt sich die Frage, ob die vorgesehene Aufgabenzuschreibung und insbesondere die Befugnis der KJM zur verbindlichen Festlegung der Standards erforderlich ist. Ein wichtiges Element dieser Strategie wird nämlich sein, Maßnahmen für Altersnachweis und Altersverifikation zu implementieren, die europäischen Regelungen entsprechen. Klares Ziel der Kommission ist es dabei offenbar, nationale Sonderregelungen perspektivisch abzulösen. In die gleiche Richtung weisen entsprechende europäische Vorgaben zum elektronischen Identitätsnachweis.

6.4. Verschiedenes

Die neue Formulierung in §§ 19a Abs. 2, 19b Abs. 2 JMStV-E ist unsauber: Dort wird offenbar der Begriff “technisches Mittel” auch auf Altersverifikationssysteme (in § 4 Abs. 4 JMStV-E richtigerweise hingegen „Maßnahmen zur Sicherstellung einer geschlossenen Benutzergruppe“) erstreckt. Hiervon ist abzuraten. Technische Mittel und Altersverifikationssysteme haben verschiedene Einsatzzwecke und unterscheiden sich auch hinsichtlich der Eignungsanforderungen.

[6] https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids (16.6.2022).

7. Zeitplan, Übergangsregelungen

Keine der beiden Übergangsregelungen ist in der Praxis umsetzbar. Je nach Auslegung der Vorschriften käme es zu unverhältnismäßigen und nicht gerechtfertigten Grundrechtseingriffen. Teilweise wird ein unmögliches Verhalten verlangt.

7.1. Einjährige Frist (§ 25 S. 1 JMStV-E)

Die neuen Vorschriften für Anbieter von Betriebssystemen und Apps sollen ein Jahr nach Inkrafttreten des erneuerten JMStV gelten. **Die Einhaltung der Frist ist denklogisch nahezu ausgeschlossen**, wie der folgende Zeitstrahl verdeutlichen soll:

- Zunächst wird durch die KJM der Kreis der (potenziell) Verpflichteten zu definieren sein (§ 12 Abs. 1 S. 1 i.V.m. § 16 S. 2 Nr. 6 JMStV-E). Zwar ist nach dem Entwurfstext nicht ganz klar, ob die "Bestimmung" durch die KJM konstituierend ist; wegen der evidenten Rechtsunsicherheit im Zusammenhang mit dem durch den Entwurf gewollten Paradigmenwechsel kann jedoch von den Betriebssystemanbietern kein proaktives Handeln erwartet werden, zumal diese weit überwiegend ihren Sitz außerhalb Deutschlands haben. Dass Anbieter zum Kreis der Verpflichteten gehören, werden sie tendenziell nur durch die KJM erfahren können.

- Sodann muss die KJM die Kriterien für die Eignung einer Jugendschutzvorrichtung festlegen (§ 12 Abs. 4 S. 1 JMStV-E). Dass dies ein äußerst komplexes Vorhaben sein wird, ist den maßgeblichen Akteuren aus der Arbeit an den Kriterien für Jugendschutzprogramme bekannt.

- Die KJM muss sich mit den anerkannten Einrichtungen der Freiwilligen Selbstkontrolle bezüglich der entworfenen Kriterien ins Benehmen setzen (§ 12 Abs. 4 S. 1 JMStV-E). Zwar ist dies weniger aufwändig als ein Einvernehmen herzustellen. Gleichwohl muss hier sowohl den vier derzeit anerkannten Selbstkontrollen ausreichend Zeit zur Analyse und Stellungnahme gegeben werden, als auch müssen diese Stellungnahmen durch die KJM im Detail ausgewertet und bei der Verabschiedung der finalen Standards in Erwägung gezogen werden. Nach Auffassung der FSM muss die KJM begründen, wenn sie den durch die Selbstkontrollen vorgetragenen, ggf. abweichenden Anmerkungen nicht folgt.

- Erst danach können die Eignungsanforderungen publiziert werden. Je nach Festlegung der KJM kann es sich hierbei durchaus um komplexe technische Vorgaben handeln. Selbst wenn die KJM nur einen allgemeinen Rahmen und Umsetzungsziele vorgibt, machte eine Umsetzung in jedem Fall aufwändige Entwicklungsarbeiten aufseiten der Betriebssystemanbieter erforderlich, was zwingend eine konkrete und klare Regelung voraussetzt.

- Dass die erforderlichen Schritte bis hierhin in weniger als sechs bis neun Monaten ab Inkrafttreten des Gesetzes erfolgen können, scheint aus der Praxiserfahrung quasi unmöglich.

- Die publizierten Eignungsanforderungen müssten nun durch die jeweiligen Industrieakteure in technische Spezifikationen übersetzt werden. Hierbei ist besonders zu berücksichtigen, dass es sich weder um einen allgemein gültigen Umsetzungsstandard handeln kann, da eine Vielzahl unterschiedlichster Geräte- bzw. Systemklassen betroffen ist, noch dass innerhalb eines Unternehmens die Umsetzung “aus einem Guss” möglich sein wird, da in der Regel eine Vielzahl an Betriebssystemversionen für verschiedene Geräte bedacht werden muss. Zudem wird es nur in seltenen Fällen möglich sein, Betriebssystemversionen ausschließlich für Deutschland zu erstellen, weshalb die in der Regel global agierenden Unternehmen in internationale Abstimmungsprozesse eintreten müssen, damit Wechselwirkungen mit anderen Prozessen sowie mit Anforderungen aus anderen Märkten ausgeschlossen werden können.

- Ob die auf diese Weise konzipierten und in lauffähige Software umgesetzten Jugendschutzvorrichtungen zur Prüfung ihrer Eignung der Selbstkontrolle vorgelegt werden müssen (§ 12 Abs. 4 S. 2 JMStV-E), ist unklar (vgl. oben 2.2.1.). Sollte dies der Fall sein, ist mit langwierigen und aufwendigen Verfahren zu rechnen. Die FSM verfügt mittlerweile über einige Erfahrung bei der Prüfung von Jugendschutzprogrammen, an deren Bewertungsverfahren sich die Prüfung von Jugendschutzvorrichtungen ggf. anzulehnen hätte. Ein idealtypisches Verfahren kann in sechs Wochen abgeschlossen werden. Dies setzt aber voraus, dass zum einen auf Anbieterseite Routine in der Anwendung der gesetzlichen und untergesetzlichen Vorgaben besteht und zum anderen auf eine gesicherte Spruchpraxis der FSM-Prüfausschüsse zurückgegriffen werden kann. Beides ist im Zusammenhang mit einer Jugendschutzvorrichtung nicht gegeben. Die FSM wird vor der erstmaligen Entscheidung insoweit Auslegungsmaximen für die KJM-Kriterien entwickeln müssen, um den ihr eingeräumten Beurteilungsspielraum rechtsfehlerfrei ausfüllen zu können. Erst danach kann das erste Verfahren abgeschlossen werden und zur Prüfung binnen einer Dreimonatsfrist an die KJM übermittelt werden.

- Zu bedenken ist, dass potenziell eine Vielzahl von Geräteklassen mit einer großen Anzahl unterschiedlicher Betriebssysteme bzw. Versionen von Betriebssystemen von der Neuregelung umfasst sein wird. Selbst wenn die Prüftätigkeit von mehreren Selbstkontrolleinrichtungen umgesetzt würde, so wären immer noch zahlreiche Industrieakteure gleichzeitig auf den reibungslosen Ablauf von Eignungsüberprüfungsverfahren angewiesen. Die Selbstkontrollen müssten jedoch allein schon aus Kapazitätsgründen eine Priorisierung vornehmen, für die sachliche Gründe zu finden wären. Eine reine zeitliche Priorisierung nach Antragseingang würde dazu führen, dass (vor-)schnell agierende Akteure gegenüber denen bevorzugt würden, die auf die Entwicklung stabiler und fehlerfreier Systeme setzen.

- Nach positiver Eignungsfeststellung durch die Selbstkontrolle (und dem Ablauf der KJM-Prüffrist bzw. nach einem entsprechenden Votum der KJM) steht nun erstmals

fest, wie eine Jugendschutzvorrichtung für die Praxis aussehen kann und welche Spezifikationen mit ihr verbunden sind.

- Bis hierhin werden mindestens weitere sechs bis neun Monate vergangen sein, sodass selbst im Idealfall (entsprechendes Engagement aller Akteure vorausgesetzt) wohl kaum vor Ablauf von anderthalb Jahren nach Inkrafttreten des Gesetzes vom Vorliegen einer ersten Jugendschutzvorrichtung auszugehen werden kann. Dies gilt auch nur dann, wenn es zwischen Selbstkontrolle und KJM nicht zu unterschiedlichen Rechtsauffassungen kommt: Weil sich bei der Eignungsprüfung von Jugendschutzvorrichtungen voraussichtlich ähnliche Rechtsfragen stellen, wie sie zwischen KJM und FSM bezüglich der Bewertung von JusProg für Windows im Jahr 2019 im Streit waren (Eignung für *welches* System führt zu welchen *konkreten* Auswirkungen für Inhalteanbieter?), kann dies nicht sicher angenommen werden. Selbstverständlich werden KJM und Selbstkontrollen in professioneller Kooperation mögliche Meinungsverschiedenheiten versuchen zu antizipieren, was einen Rechtsstreit vermeiden mag, jedoch kaum zu einer Verfahrensbeschleunigung führen würde.

- Nach Abschluss dieses Verfahrens müssen nunmehr wiederum die Betriebssystemanbieter die entwickelte Schnittstelle publizieren und so dokumentieren, dass die Anbieter von Apps sie auffinden und richtig nutzen können. Da es sich bei den in Rede stehenden Apps in aller Regel um Angebote handeln wird, die ihrerseits auf einer Vielzahl von Plattformen bzw. Betriebssystemen verfügbar sind, entsteht auch dort ein Vielfaches an Entwicklungsaufwand. Es erscheint ausgeschlossen, dass die Schnittstellen für verschiedene Geräte bzw. Betriebssysteme auf die gleiche Weise funktionieren bzw. von den Apps auf die gleiche Weise angesprochen werden können. Hinzu kommt, dass die neuen Vorgaben beispielsweise im Bereich Video on Demand zu tiefgreifenden Änderungen in der bisherigen Jugendschutzlogik führen müssen, weil die dort eingerichteten altersdifferenzierenden Nutzerprofile durch die Jugendschutzvorrichtung „überstimmt“ werden sollen (§ 12 Abs. 2 S. 2 1. HS JMStV-E).

- Das Zusammenspiel von Betriebssystem/Schnittstelle und Apps muss getestet werden. Wegen der durch den Regelungsentwurf angestrebten tiefen Eingriffe in das Betriebssystem und die grundsätzliche Änderung der Steuerungslogik von Angeboten ist ein oberflächliches, (vor-)schnelles Vorgehen hier ausgeschlossen.

- Die an die neuen Vorgaben angepassten Apps müssen an die Nutzerinnen und Nutzer ausgespielt werden und von denen installiert und eingerichtet werden. In diesem Zusammenhang ist stets darauf zu achten, dass der technische Jugendmedienschutz mit seinem Fokus auf die Elternverantwortung erklärungsbedürftig ist. In der Prüfpraxis der FSM nimmt die Nutzerfreundlichkeit und die transparente Erklärung der angebotenen Maßnahmen eine zentrale Rolle ein. Wenn also das seit mehreren Jahren etablierte, bekannte und akzeptierte System des Jugendmedienschutzes von Grund auf verändert wird, muss dies gegenüber den Eltern sorgfältig kommuniziert werden. Ein plötzliches “Umschalten” von der einen Logik auf eine neue verbietet sich dabei.

- Der Gesetzentwurf erstreckt dasselbe Verfahren auch auf die Suchmaschinen bzw. die sichere Suchfunktion (Festlegung der Verpflichteten durch die KJM: § 16 Abs. 1

S. 2 Nr. 7; Festlegung der Eignungsanforderungen durch die KJM im Benehmen mit den Selbstkontrollen: § 12 Abs. 4 S. 1; Eignungsfeststellungsverfahren durch Selbstkontrollen mit nachgelagerter Überprüfung durch die KJM: § 12 Abs. 4 S. 2 i.V.m. §§ 11 Abs. 4, 19a Abs. 2 und 19b Abs. 2). Hierbei handelt es sich aber denklogisch um etwas völlig anderes als die Jugendschutzvorrichtung. Akteure und Verantwortliche unterscheiden sich ebenso wie die in der Praxis erforderlichen Schritte auf dem Weg zu einer Eignungsfeststellung. Weil es sich grundsätzlich um die gleichen Schritte handelt wie bei der Jugendschutzvorrichtung, ist auch mit einem ähnlichen zeitlichen Aufwand zu rechnen, der die Zeitdauer bis zu einer möglichen vollständigen Verfügbarkeit der angedachten Systematik weiter drastisch verlängern würde.

Ohne weitere Voraussetzungen handeln Anbieter eines Betriebssystems i.S.d. § 12 Abs. 1 S. 1 JMStV-E und Anbieter von Apps nach Ablauf der Jahresfrist rechtswidrig und könnten mit einem Bußgeld von bis zu 500.000 EUR belegt werden. Dabei sind Anbieter von Betriebssystemen von der Dauer der Prozesse bei KJM und Selbstkontrolle abhängig, die Anbieter von Apps zusätzlich von der Dauer der Umsetzung durch die Betriebssystemanbieter.

Eine auf derart vielen Variablen fußende Regelung ist **keine rechtsstaatliche Grundlage für polizeirechtliches Handeln**. Vielmehr braucht es ein Anknüpfen an bestimmte entscheidende Zeitpunkte innerhalb des Gesamtgefüges, beispielsweise eine bestandskräftige Entscheidung nach § 12 Abs. 4 S. 2 JMStV-E, mit der die Selbstkontrolle die Eignung einer Jugendschutzvorrichtung anerkannt hat.

Zu Bedenken gegeben wird, dass es keine Übergangsfristen für die Pflichten aus § 12b JMStV-E (v.a. Absatz 2) gibt. Dies führt in der Theorie dazu, dass zu einem unklaren Zeitpunkt, in dem eine als geeignet bewertete Jugendschutzvorrichtung für ein bestimmtes Betriebssystem existiert, ab Tag 1 entsprechende Pflichten entstehen. Auch wenn diese offenbar nicht mit einem Bußgeld abgesichert werden sollen (§ 24 Abs. 1 Nr. 11 JMStV-E), bleiben es doch Handlungspflichten, die durch Maßnahmen der KJM durchgesetzt werden können.

7.2. Zweijahresfrist (§ 25 S. 2 JMStV-E)

Auf Geräten, deren Betriebssysteme nicht aktualisiert werden können, sollen die neuen Vorgaben ausweislich § 25 S. 2 JMStV-E dennoch gelten, wenn eine zweijährige Übergangsfrist abgelaufen ist. Mit anderen Worten: **Etwas technisch Unmögliches soll gleichwohl unter Androhung eines Bußgeldes erzwungen werden.** Dies läuft dem Gebot der Rechtsstaatlichkeit evident zuwider.

Im Einzelnen muss der rückwirkende Charakter der Norm beanstandet werden. Einer Sanktionierung unterworfen werden dadurch Personen, die keine - grundrechtsschonende - Möglichkeit haben, sich rechtskonform zu verhalten. Einzig das Einstellen eines Angebots käme in der Theorie in Betracht. Dies bedeutet aber mit Blick auf Betriebssysteme, dass zahlreiche Geräte nicht mehr verwendet werden dürften. Hersteller von TV-Geräten oder Set-top-Boxen

müssten diese Geräte unbrauchbar machen, damit Nutzerinnen und Nutzer über diese Geräte keinen - dann rechtswidrigen - Zugang zu Angeboten mehr haben. Nur in seltenen Fällen dürfte dies praktisch überhaupt möglich sein.

Dies verletzt, ohne dass es eine angemessene Verhaltensalternative gäbe und ohne dass das grundgesetzlich vorgeschriebene Zitiergebot eingehalten wäre, die Grundrechte der Anbieter sowie auch der Nutzerinnen und Nutzer aus Art. 14 GG.

Sodann stellt sich aus der Perspektive der Apps die Frage, wie deren Anbieter das Ausführen auf “nicht aktualisierbaren” Betriebssystemen verhindern sollen. Hierzu wären sie gezwungen, um nicht ihrerseits gegen § 12a JMStV-E zu verstoßen. Dazu müsste die App bei jedem Start die Versionsnummer des Betriebssystems bzw. dessen Updatestand ermitteln. Es dürfte schlechterdings unmöglich sein, auch nur einen rudimentären Überblick über alle in Deutschland genutzten Betriebssystemversionen zu gewinnen, wobei viele davon sich nur in Details voneinander unterscheiden. Hinzu kommt, dass eine App grundsätzlich nur erkennen kann, ob eine Jugendschutzvorrichtung i.S.d. § 12 JMStV-E *aktiviert* ist, nicht aber, ob sie überhaupt *vorhanden* ist: Entscheiden sich Nutzerinnen und Nutzer gegen die Verwendung einer Jugendschutzvorrichtung, erfolgt auch kein Informationsaustausch zwischen Betriebssystem und App, und eine Reaktion nach §§ 12a, 12b JMStV-E ist nicht erforderlich. Auch aus Sicht der Appanbieter ist also ein rechtskonformes Verhalten in vielen Situationen nicht mit vertretbarem Aufwand möglich. Die Schwelle zum Beginn der Fahrlässigkeit (§ 24 Abs. 1 S. 1 JMStV) ist dabei diffus.

Erschwerend kommt hinzu, dass die **Pflichten von Appanbietern in jedem Fall nach einem Jahr beginnen** sollen, unabhängig von der Updatefähigkeit des jeweils genutzten Betriebssystems (§ 25 S. 1 JMStV-E).

Eine Erstreckung des Regelungsvorschlags auf Geräte und Systeme, die vor Inkrafttreten bereits am Markt verfügbar waren und in Deutschland genutzt werden, muss demnach ausscheiden.

7.3. Bestandskraft bisheriger Entscheidungen zu Jugendschutzprogrammen

Der Gesetzentwurf enthält keine Aussagen zum Umgang mit bisherigen bestandskräftigen Entscheidungen nach §§ 19a Abs. 2, 19b Abs. 2 JMStV. Diese Entscheidungen sind stets befristet (§ 11 Abs. 4 S. 1 JMStV). Innerhalb dieses Zeitraumes müssen deshalb die Eignungsfeststellungen zu Gunsten der Apps mit eigenem Jugendschutzprogramm i.S.d. § 11 Abs. 2 JMStV fortgelten. Die zusätzlichen Anforderungen aus §§ 11 Abs. 2 S. 2, 12b JMStV-E kommen erst nach Ablauf des jeweiligen Gültigkeitszeitraumes zum Tragen.

8. Verschiedenes

Die Aufhebung von § 9 Abs. 2 JMStV (Satzungsermächtigung für Jugendschutz im digitalen Rundfunk) wird begrüßt. Entsprechende Sonderregelungen sind nicht mehr erforderlich.

9. Alternativen, Vorschläge

Vor der substanziellen Verschiebung der Verantwortlichkeiten im deutschen Jugendmedienschutz sollten zwingend **aktuelle empirische Daten** erhoben und ausgewertet werden. Der Jugendmedienschutzindex der FSM wird im Herbst 2022 hierzu wichtige Erkenntnisse bringen.

Ein wichtiger Grundgedanke im Jugendmedienschutz ist es, durch die einfache Verfügbarkeit einer großen Zahl kindgeeigneter bzw. altersgerechter Inhalte das Risiko zu verringern, dass Kinder und Jugendliche mit für sie ungeeigneten Inhalten in Kontakt kommen. In diesem Zusammenhang ist es essentiell, **Suchmaschinen für Kinder (wie z.B. fragFINN)** noch stärker in das Bewusstsein der Familien zu rücken. Wenn das Ziel verfolgt wird, durch eine Jugendschutzvorrichtung sehr drastische Einschnitte in die Verfügbarkeit von Apps vorzunehmen, gleichzeitig aber das Surfen im Internet ausdrücklich nicht zu beeinflussen, könnte durch eine deutlich sichtbare Einbeziehung des Angebots von fragFINN mit überschaubarem Aufwand viel gewonnen werden.

Zwischen BzKJ, KJM und den Selbstkontrolleinrichtungen dürfte es Konsens sein, dass derzeit bereits zahlreiche gute Möglichkeiten für Eltern bestehen, ihren Kindern eine geschützte Nutzung digitaler Medien zu gewähren. Diese müssen weiterhin „Vorfahrt“ haben. Der „Quasi-Industriestandard“ im Bereich Video on Demand sowie die sich durchsetzende Verbesserung des Schutzstandards im Bereich Games wurden bereits angesprochen. Konsens ist aber auch, dass das Bewusstsein über die zur Verfügung stehenden Maßnahmen noch nicht ausreichend ist. Zwar haben Hersteller von Geräten und Software sowie Anbieter von Diensten in der jüngeren Vergangenheit hier große Fortschritte erzielt (Google Family Link und Microsoft Family Safety seien beispielhaft genannt), die **leichte Auffindbarkeit und Nutzbarkeit** ist dabei aber noch nicht in jedem Fall gegeben. Hier anzusetzen, ist im Vergleich zur „Systemrevolution“ des Diskussionsentwurfs in jedem Fall vorzugswürdig.

In der Medienerziehung ist anerkannt, dass elterliche Maßnahmen dann am besten akzeptiert werden und wirken können, wenn sie **im Dialog mit den Kindern** getroffen werden, wenn Eltern ihre Entscheidungen transparent treffen und sie begründen. Dies verringert Frustration und Umgehungsversuche. Entsprechende Lösungen sind in der jüngeren Vergangenheit sehr erfolgreich und in großem Stil eingeführt worden, sowohl Android, als auch für Windows. Im Praxiseinsatz erweist es sich als unbedingt vorzugswürdig, Jugendschutzeinstellungen individuell und nach Absprache festzulegen. Auf diese Weise können beispielsweise auch sehr unkompliziert Inhalte oder Anwendungen nachträglich durch die Eltern freigegeben werden, die einer Freigabeliste bislang fehlten oder die nur für eine bestimmte Übergangszeit (für die Erledigung von Schulaufgaben; während der Ferienzeit; am Wochenende) zur Verfügung stehen sollen. Dass die Verwaltung dieser Einstellungen auch auf die Distanz bzw. von einem anderen Gerät (nämlich dem der Eltern) möglich sein sollte, rundet das Anforderungsportfolio ab und ist zudem ein wesentlicher Erfolgsfaktor. Nur auf diese Weise lässt sich eine angemessene Regelung finden, die die Kinderrechte respektiert und im Sinne des Konzepts der ***„Evolving Capacities“*** auch zeitgemäß ist. Die pauschale Lösung „Jugendschutzvorrichtung“ mag für Eltern bequemer sein - dies ist jedoch nicht der Maßstab.

Deutlich wirksamer und deshalb vorzugswürdig sind individuelle Maßnahmen, welche durch das Gesetz im Idealfall ausdrücklich befürwortet oder jedenfalls nicht gehemmt werden sollten.

Als förderlich dürfte es sich auch erweisen, wenn die durch KJM und ggf. Selbstkontrollen positiv bewerteten Systeme transparenter dargestellt bzw. aufgelistet werden und potentielle Einsatzzwecke leichter erkennbar sind. Entsprechende Listen müssen aktuell gehalten werden und zwischenzeitliche Veränderungen widerspiegeln. Gerade weil es in verschiedenen Rechtsgebieten durchaus vergleichbare Anforderungen gibt, die sich teils nur in Nuancen unterscheiden (z.B. Jugendmedienschutz, Glücksspiel, Geldwäscheprävention, Versandhandel, Identitätsnachweise für Vertragsschlüsse), sollte eine Vereinheitlichung der Standards und ggf. auch klarere Zuständigkeitszuweisung erfolgen. Das Thema elektronischer Identitätsnachweis gewinnt derzeit sowohl auf Bundesebene als auch in der EU mit großer Dynamik an Bedeutung. Um einer fortschreitenden Verkomplizierung der unterschiedlichen Normen entgegenzuwirken, könnte über ein **System „vererbter Standards“** nachgedacht werden, in dem beispielsweise klargestellt wird, dass ein im Bereich Geldwäsche anerkanntes System auch für den Zugang zu Erwachseneninhalten online geeignet ist.

Im gesetzlichen Jugendmedienschutz Deutschlands bestehen im internationalen Vergleich sehr hohe Schutzstandards. Diese Standards einzuhalten und ein hohes Schutzniveau zu erzielen, bleibt der gemeinsame Anspruch von FSM und ihren Mitgliedsunternehmen. Keinesfalls ist es eine Option, die Wege zur Zielerreichung zu limitieren und individuelle, passgenaue Möglichkeiten abzuschaffen. Im Gegenteil: **Die Optionen, um dieses hohe Schutzniveau zu erreichen, müssen noch zahlreicher werden.** Die bereits angesprochene, von KJM und FSM zertifizierte Möglichkeit, das Alter einer Person mit hinreichender Sicherheit und Genauigkeit durch Mechanismen maschinellen Lernens auf äußerst datensparsame Weise zu ermitteln, steht beispielhaft für eine gelungene Anreizregulierung.

* * *