

JMStV Novelle

**Stellungnahme des JusProg e.V.
zu den Vorschlägen der Rundfunkkommission
der Länder zur Reform des
Jugendmedienschutzstaatsvertrages
(JMStV-E)**

20. Juni 2022

JusProg e.V.

Paul-Sorge-Str. 73

22459 Hamburg

Ansprechpartner:

Stefan Schellenberg, Vorsitzender

schellenberg@jusprog.de

1. Inhalt

1.	Inhalt.....	2
2.	Vorbemerkung.....	3
2.1.	Bitte um persönliche Anhörungen	4
3.	Entwicklungsgefährdung durch Browser.....	4
3.1.	Niedriges Schutzniveau	5
3.2.	Technische Aktivierung von SafeModi	5
3.3.	Monopolisierung von Browsern der Betriebssystemanbieter	6
4.	Integration bestehender Jugendschutz-Lösungen	6
4.1.	Zusammenspiel mit Jugendschutzprogrammen?.....	6
5.	App-Steuerung.....	7
5.1.	Wer klassifiziert Apps?	7
5.2.	Systemeigene App-Stores.....	8
5.2.1.	Minderjährige werden von digitaler Teilhabe ausgeschlossen	8
5.2.2.	Betriebssysteme ohne eigenen App-Store	9
5.2.3.	Kommerzielle Ausrichtung der App-Stores und Willkür.....	9
5.2.4.	Datenschutz in den App-Stores	10
6.	Digitale Teilhabe	10
6.1.	Keine Profile	10
6.2.	Privatsphäre der Kinder.....	11
6.3.	Ausschluss von vielen Apps und Anwendungen	12
7.	Betriebssysteme	12
8.	Kennzeichnungspflichten	12
9.	Inkonsistenzen des JMStV-Entwurfs	13
10.	Praktikabilität	13

2. Vorbemerkung

Wir begrüßen grundsätzlich das Ziel der Rundfunkkommission der Länder und der beteiligten Staatskanzleien, durch eine Novelle des Jugendmedienschutzstaatsvertrages (JMStV) den Schutz von Kindern und Jugendlichen in Telemedien weiter zu stärken.

Gern nehmen wir die Gelegenheit wahr, als JusProg e.V. zum vorliegenden Entwurf in der von der Rundfunkkommission vorgelegten Fassung vom 15. März 2022 Stellung zu nehmen und bedanken uns dafür.

JusProg e.V. ist ein gemeinnütziger Verein, der von wichtigen Akteuren der deutschen Internet-Branche getragen wird. Satzungsgemäßer Zweck des Vereins ist Entwicklung, Bereitstellung und Förderung von Jugendschutzprogrammen, wie sie seit 2003 einer der zentralen Bausteine des JMStV sind. Dieser Aufgabe widmet sich der Verein mit viel Engagement und Erfolg. JusProg e.V. bietet die derzeit einzigen allgemeinen Jugendschutzprogramme an, die nach § 11 JMStV gesetzlich (von der FSM, zuvor der KJM) anerkannt wurden.

Der vorgelegte Entwurf des JMStV-E lässt viele sinnvolle Ziele und Ideen erkennen, was wir ausdrücklich begrüßen und unterstützen. JusProg e.V. ist gern bereit, sich wie in den vergangenen 19 Jahren auch weiterhin aktiv daran zu beteiligen, dass die Ziele des Staatsvertrages auch tatsächlich in der Praxis bei den „Kindern, Jugendlichen und Eltern ankommen“.

Allerdings ist zu befürchten, dass die konkrete Ausgestaltung der Gesetzesvorlage den erkennbaren Zielen der Staatsvertragsgeber eher abträglich ist und in der absehbaren Praxis zu einem Rückschritt beim Jugendmedienschutz statt zu einer Fortentwicklung führen wird.

Als besonders problematisch sehen wir, dass den Eltern mit der neuen Jugendschutzvorrichtung der Betriebssysteme (sog. Jugendschutz-Button) der grundlegend falsche Eindruck vermittelt wird, dass die Erziehungsberechtigten per Klick ein Smartphone, Tablet oder anderes Endgerät sozusagen zum „sicheren Kinder-Gerät“ machen können, jedoch ohne zusätzliche Installation eines Jugendschutzprogramms ausgerechnet der Zugang zu besonders gefährlichen Inhalten wie zum Beispiel Gewaltpornografie und anderen verstörenden Gewaltdarstellungen praktisch nicht verhindert wird.

Die zweitwichtigste Problematik der ja grundsätzlich eher rückwärtsgewandten Vorschläge im JMStV-E ist in unseren Augen, dass die Kinder und Jugendlichen umfänglich von der Medien-Teilhabe ausgeschlossen werden, auch bei Medien und Funktionen, die für sie nicht schädlich, oft sogar förderlich sind. Dies passt nicht in das ansonsten allgegenwärtige Bemühen von der EU-Ebene bis zu regionalen Organisationen und im Familien-Alltag, den Minderjährigen eine größtmögliche Teilhabe an der digitalen Welt zu ermöglichen, soweit dadurch keine Beeinträchtigung oder Gefährdung zu erwarten ist.

Darüber hinaus sehen wir den gesetzesimmanenten Eingriff in die Privatsphäre der Kinder und Jugendlichen sehr kritisch.

Begrüßenswert ist, dass die bewährten Jugendschutzprogramme weiterhin eine tragende Rolle des JMStV-E spielen sollen und insofern das auch im EU-Vergleich sehr erfolgreiche Modell der sogenannten „Privilegierung“ als Motivation für Entwicklung und Betrieb von Jugendschutzprogrammen und für die Alterskennzeichnung durch Anbieter fortgesetzt wird.

Begrüßenswert ist darüber hinaus das sichtbare Bemühen, die Gesetze auf Bundes- und Landesebene stärker zu synchronisieren, auch wenn das Ziel einer vollständigen Kongruenz weiterhin noch nicht erreicht ist.

Im Folgenden führen wir gern unsere Einschätzung weiter aus und bedanken uns bereits heute für deren Berücksichtigung bei den weiteren Beratungen.

2.1. Bitte um persönliche Anhörungen

Der vorliegende JMStV-E wirft viele Fragen der Umsetzbarkeit auf und lässt daran zweifeln, ob die erkennbaren Ziele mit den vorgeschlagenen Regelungen tatsächlich erreicht werden können, diese häufig nicht gar das Gegenteil bewirken.

Diese Fragen lassen sich sinnvoller in persönlichen Gesprächen und mündlichen Anhörungen sowie Fragerunden zur intendierten praktischen Umsetzung des JMStV-E diskutieren und bewerten. Wir würden uns deshalb über entsprechende Einladungen freuen und bieten unsere konstruktive Mitarbeit bei der Suche nach guten und praktikablen Lösungen an.

3. Entwicklungsgefährdung durch Browser

Eltern und andere Erziehungsberechtigte werden bei Aktivierung Jugendschutzvorrichtung im Betriebssystem berechtigt erwarten, dass damit ihr Kind altersgerecht vor den wichtigsten Gefahren geschützt ist, die mit der Handynutzung verbunden sind – insbesondere vor entwicklungsgefährdenden Inhalten.

Leider wird diese Erwartung der Eltern enttäuscht, ohne dass diese darauf hingewiesen werden.

Zwar werden nach Aktivierung des Jugendschutz-Buttons noch nutzbare Browser verpflichtet (§ 12.2.1 JMStV-E), Suchmaschinen in den SafeModus zu schalten, aber dieser Schutzmechanismus betrifft derzeit nach unserer Kenntnis weltweit weniger als zehn Angebote, die einen SafeModus anbieten, bei Konzentration auf „Online-Suchmaschinen“ im Wortsinn sind es noch weniger.

Weiterhin frei zugänglich sind in diesen vorgeblich schützenden Browsern auf dem „Kinder-Handy“ zum Beispiel:

- Offene Pornografie, Gewaltpornografie, Kinderpornografie
- Gewaltvideos, Splatter, Selbstmord-Darstellungen
- Verherrlichung von ProAna (Magersucht) und Selbstgefährdung
- Tierquälerei
- Politischer Extremismus
- Allgemeine Gewaltdarstellungen
- ...

Die meisten dieser Inhalte finden sich nicht in Apps, da sie von den App Stores nicht zugelassen werden, sondern nur in Browsern.

Es ist nicht zu erwarten, dass diese Webseiten SafeModi installieren werden und dass Browser diese Modi ggfls. „kennen“. Die Praxis von fast zwanzig Jahren JMStV zeigt, dass bislang nur Jugendschutzprogramme und ähnliche Sicherungsvorrichtungen Kinder und Jugendliche effektiv gegen diese meist aus dem Ausland stammenden Inhalte schützen können.

Keinesfalls sinnvoll kann es sein, dass Minderjährige Inhalte wie z.B. Splatter-Movies in Videoportalen, die von Apps mit Jugendschutzfunktion herausgefiltert werden, dann eben im weitgehend offenen Browser aufrufen.

Soweit bekannt, bieten alle großen bei Kindern und Jugendlichen beliebten Social Media-Plattformen (außer Twitter) bislang keine von außen aktivierbaren SafeModi an, so dass der Ansatz des JMStV-E diesbezüglich ins Leere laufen würde.

Soll in dem Bereich der Inhalte in Browsern ein signifikanter Fortschritt für mehr Jugendmedienschutz erzielt werden, dann ist dieser nur sinnvoll unter Einbeziehung von Jugendschutzprogrammen und ähnlichen Filtersystemen möglich. Dazu bedarf es der entsprechenden technischen Voraussetzungen, z.B. der umgehungssicheren Möglichkeit zur Implementierung von nameserverbasierter Filterung wie z.B. durch JusProgDNS oder OpenDNS.

3.1. Niedriges Schutzniveau

Der JMStV fordert eine hohe Umgehungssicherheit von Jugendschutzprogrammen (§ 11) und sieht für den Zugang zu Inhalten für Erwachsene in einer sog. Geschlossenen Benutzergruppe (§ 4.2) hohe Hürden vor, wie sie ähnlich bei einer Bankkonto-Eröffnung gefordert werden.

Im Vergleich dazu erscheint es zumindest unverständlich, dass ausgerechnet der „staatlich verordnete Jugendschutz-Button“ nur ein minimales Schutzniveau vorsieht, nach dem Kinder und Jugendliche in Apps herausgefilterte Inhalte einfach via Browser aufrufen können – also die Umgehungssicherheit lediglich durch den notwendigen Wechsel der App erreicht wird.

3.2. Technische Aktivierung von SafeModi

Der JMStV-E basiert darauf, dass sogenannte „Online-Suchmaschinen“ SafeModi anbieten und diese über das Betriebssystem oder den Browser aktivierbar sind, was technisch zumindest im Fall der Betriebssysteme wegen der Daten-Verschlüsselung zumindest einige Umsetzungszweifel aufwirft. Zwar bieten derzeit die beiden großen Suchmaschinen Google und Bing von außen aktivierbare SafeSearch-Funktionen an, aber schon deren White Label-Derivate wie z.B. die bei Minderjährigen besonders beliebte Suchmaschine Ecosia, die eingenommene Werbegelder in ökologische Aktionen investiert, bietet nach unserer Kenntnis keinen extern aktivierbaren SafeModus an – mit dieser Suchmaschine können die Minderjährigen dann uneingeschränkt z.B. Links zu Gewaltpornografie-Angeboten recherchieren, wenn Google und Bing im SafeModus sind.

Bei der Definition von Standards für SafeModi wäre ein Verweis auf die ohnehin für Altersklassifizierungen von Anbietern sinnvolle age.xml (age-de.xml) zielführend.

3.3. Monopolisierung von Browsern der Betriebssystemanbieter

Seit vielen Jahren bemüht sich die EU darum, die Monopolisierung von Browsern zu brechen, die von den Anbietern von Betriebssystemen vorinstalliert werden. Dem würden die Regelungen im JMStV-E diametral widersprechen, dabei die Rechte der Kinder und ihrer Eltern bei der freien Browserwahl unverhältnismäßig einschränken.

Ergänzende Anmerkung: Große Unsicherheit ergibt sich aus der Begrifflichkeit „systemeigener Browser“. Wenn z.B. Samsung ein Tablet auf Basis des Android-Betriebssystems anbietet, auf dem der Firefox-Browser vorinstalliert ist, ist das dann ein „systemeigener“ oder ein „systemfremder“ Browser? Was ist mit Betriebssystemen wie z.B. vielen Linux-Distributionen, die zur Installation keine Browser mitliefern?

4. Integration bestehender Jugendschutz-Lösungen

Das dem nun vorgelegten JMStV-Entwurf vor rund einem Jahr vorangegangene Konzeptpapier „Verbesserter Jugendmedienschutz mittels eines übergreifenden und individuell einstellbaren Kinderschutzmodus auf Endgeräten“ hatte noch als Ziel formuliert, bestehende Jugendschutzmaßnahmen bestehen zu lassen und zu integrieren.

Im JMStV-E findet sich dies jedoch nicht wieder. Die sogenannte Jugendschutzvorrichtung über das Betriebssystem integriert weder die bestehenden guten Jugendschutz-Lösungen der meisten Anbieter von Betriebssystemen (Family Safety, Family Link etc.), noch integriert sie bestehende Jugendschutzfilter wie z.B. JusProg-Jugendschutzprogramme, OpenDNS oder Saalfeld oder Altersklassifizierungssysteme wie z.B. IARC (dazu mehr unten) oder technische Standards wie age.xml / age-de.xml.

Schlimmer noch: Wenn Eltern auf die trügerische Sicherheit des Jugendschutz-Buttons hereinfallen, besteht zu befürchten, dass wirksamere bestehende Lösungen weniger häufig eingesetzt werden. Das Angebot an Lösungen ist bereits jetzt für viele Eltern schwer zu überschauen, ein weiterer Ansatz wird voraussichtlich nicht zu mehr Klarheit, sondern zu mehr Verwirrung und damit in der Praxis zu weniger Nutzung führen.

Mit der Betriebssystems-Schutzvorrichtung wurde eine „Insel-Lösung“ erdacht, die weder an in Deutschland bewährte Jugendschutzsysteme anknüpft noch international anschlussfähig ist. Dabei würde sich mit euCONSENT, DSA, Parental Control und anderen europäisch gedachten Ansätzen wirksamer Jugendmedienschutz im Ergebnis effektiver und erfolgversprechender umsetzen lassen.

4.1. Zusammenspiel mit Jugendschutzprogrammen?

Die Regelungen des JMStV-E berücksichtigen keine Verknüpfung der neuen Schutzvorrichtung mit Jugendschutzprogrammen (in dem Sinne, dass sich die anerkannten Jugendschutzprogramme der Altersinformationen bedienen und sozusagen „mit einem Klick“ die Jugendschutzprogramme mit dem zum jeweils nutzenden Kind passenden Einstellungen ein- und ausgeschaltet werden.)

Denn die Anforderungen für die Anerkennung von Jugendschutzprogrammen nach § 11 JMStV / JMStV-E erfordern eine hohe Nutzerfreundlichkeit sowie Einstellmöglichkeiten nach Altersstufen.

Diese Faktoren werden von der neuen Jugendschutzvorrichtung nicht adressiert, so dass Jugendschutzprogramme sich nicht „an die Lösung andocken“ können, ohne ihre Anerkennung zu riskieren.

- Zur Nutzerfreundlichkeit gehören Profile für Kinder verschiedener Altersstufen bei gemeinsam genutzten Endgeräten mit den Möglichkeiten für nutzerautonome Einstellungen. Diese sieht die Jugendschutzvorrichtung nicht vor.
- Wesentliche Anerkennungsvoraussetzung für Jugendschutzprogramme ist nach § 11.1 JMStV, dass diese „einen nach Altersstufen differenzierten Zugang zu Telemedien“ ermöglichen. Die Jugendschutzvorrichtung sieht nach unserem Verständnis keine derartigen Altersstufen vor, da diese mit Profilen verknüpft sein müssten.

Wir regen an, gemeinsam Regelungsvorschläge zu erarbeiten, die eine Integration von Jugendschutzprogrammen und Jugendschutzvorrichtungen ermöglichen, die die Anerkennungsvoraussetzungen im Blick behalten.

5. App-Steuerung

Ungeachtet dessen, dass die Definition von „Apps“ einerseits und „Software-Anwendungen“ andererseits im JMStV-E einen großen Interpretationsspielraum offenlässt, was genau eigentlich gemeint ist, werfen die Regelungen bei den Überlegungen zur konkreten Umsetzbarkeit und zu den vermutlich eher ungewünschten „Neben-Effekten“ viele Fragen auf.

5.1. Wer klassifiziert Apps?

Die §§ 12.3 und §12a JMStV-E fordern, dass „Anbieter ihre Apps mit einer Alterseinstufung ... versehen, die vom Betriebssystem ausgelesen werden kann“. Apps ohne diese Alterseinstufung sollen bei aktiviertem Jugendschutz-Button künftig für Minderjährige nicht mehr zugänglich sein.

Diese Regelung verkennt, wie heute die bewährte Praxis bei der Altersklassifizierung von Apps im z.B. Android- und Windows-Betriebssystem ist, wie Apple vorgeht und wie Alterseinstufungen von Apps und Softwareanwendungen auf anderen Betriebssystemen erfolgen – und was die sehr unerwünschten Folgen der vorgeschlagenen Regelungen wären.

Die Alterseinstufung erfolgt heute nicht durch die Anbieter, wie es der JMStV-E offenbar annimmt. Diese füllen lediglich beim App-Upload neutralisierte Fragebögen zu den Inhalten und Funktionen von Apps und Software aus, die dann von den Selbstkontrollenrichtungen, die den App-Stores angeschlossen sind, mit Hilfe von Algorithmen (IARC) in Altersstufen übersetzt werden oder im Fall von z.B. Apple vom App-Store-Anbieter vergeben werden.

Dies bedeutet: Wenn der JMStV-E mit der vorgeschlagenen Regelung in Kraft tritt, werden die Minderjährigen von einem Großteil der Apps ausgeschlossen – alle außer der Handvoll deutscher Apps, die ein eigenes „geschlossenes“ Jugendschutzprogramm im Sinne des JMStV haben.

Es ist auch nicht zu erwarten, dass sich diese Situation der mangelnden Teilhabe der Kinder und Jugendlichen an der digitalen Welt mit der Zeit wesentlich verbessern wird – eher unwahrscheinlich, dass beispielsweise der australische Anbieter einer auch in Deutschland beliebten Compass-App oder der Anbieter der kostenlosen Bildbearbeitung GIMP diese künftig für die speziellen deutsche Jugendschutzanforderungen entwickeln und nur noch über die systemeigenen App-Stores anbieten werden. Der weit überwiegende Teil der bei Minderjährigen beliebten Apps kommt aus dem Ausland.

Es ist also dringend geboten, die zumindest missverständliche Formulierung in § 12.3 und § 12a JMStV-E zur Alterskennzeichnung durch Anbieter durch eine klare Regelung zu ersetzen, die Systeme wie IARC gesetzlich absichert und zugleich dafür sorgt, dass die vielen Millionen bestehenden Apps mit niedriger Alterseinstufung den Minderjährigen nahtlos weiter zur Verfügung stehen.

Allerdings darf es dabei nicht passieren, dass Anbieter von App-Stores aus dem Ausland, vor allem aus den USA und China, künftig willkürlich Altersstufen vergeben und Apps nach Gutdünken blockieren können, ohne dass einem europäischen App- und Software-Anbieter ein geordnetes, unabhängiges Widerspruchsverfahren zur Verfügung steht, wie es zum Beispiel beim Zusammenspiel von IARC und USK gute Praxis ist.

5.2. Systemeigene App-Stores

In § 12.2.3 legt der JMStV-E fest, dass „die Installation von Apps nur über die systemeigene Vertriebsplattform möglich ist“. Das dahinterstehende Anliegen der Umgehungssicherheit ist nachvollziehbar, gleichwohl führt diese Regelung in der vorgeschlagenen Form zu einer Vielzahl im Ergebnis inakzeptabler Effekte.

5.2.1. Minderjährige werden von digitaler Teilhabe ausgeschlossen

Bei Smartphones und Tablets dominieren die App-Stores der Anbieter als Bezugsquellen für Apps, aber bei allen anderen Betriebssystemen inklusive Windows, Mac und Linux ist es heute eher die Ausnahme als die Regel, dass neue Apps und Software über die systemeigenen Stores vertrieben und installiert werden – die Nutzung wäre für Minderjährige mit dem neuen JMStV-E nicht mehr möglich.

Ein Großteil der auf Windows- und Mac-Rechnern genutzten Apps/Software kommt von Anbietern aus dem Ausland. Häufig handelt es sich um technische Helfer von der Systemuhr über Virenschutz-Software bis zur digitalen Bildbearbeitung und dem Videoschnitt. Es ist nicht zu erwarten, dass die internationalen Anbieter insbesondere von kostenloser Freeware sich die Mühe machen werden, ihre Apps und Softwareanwendungen mit deutscher „Insel“-Jugendschutz-Funktionalität zu versehen und diese nicht mehr zum freien Download, sondern nur noch über die sehr viel weniger besuchten App-Stores der Betriebssysteme anzubieten. Damit werden die Kinder und Jugendlichen verstärkt in kommerzielle Produkte getrieben, die sich aus wirtschaftlichem Interesse eher auf lokale Anforderungen einstellen werden. Damit würde der Jugendschutz für Eltern kostspielig und würde für Kinder zu eingeschränkten Möglichkeiten führen.

An dieser Stelle sei ergänzend als Beispiel erwähnt, dass auch JusProgNet für Windows sowie die Software für JusProgDNS für Windows und für Mac (aus gutem Grund) frei zu Download und nicht über die systemeigenen App-Stores von Windows und Apple angeboten werden.

Im Ergebnis werden deutsche Kinder und Jugendliche durch den JMStV-E noch mehr von der digitalen Entwicklung abgehängt, als sie es im internationalen Vergleich ohnehin schon sind. Dies würde alle Digitalisierungsoffensiven und auch den begrüßenswerten „Digitalpakt Schule“ konterkarieren.

5.2.2. Betriebssysteme ohne eigenen App-Store

Längst nicht alle von Minderjährigen genutzte Betriebssysteme verfügen über systemeigene App-Stores. Am augenfälligsten ist dies beim Linux-Betriebssystem. Nach den Regelungen des JMStV-E könnten Minderjährige bei diesen Systemen keine Apps und Software mehr installieren und wären insofern von der digitalen Welt weitgehend abgeschnitten.

5.2.3. Kommerzielle Ausrichtung der App-Stores und Willkür

Wenn der JMStV-E die Anbieter von Apps und Software faktisch verpflichtet, ihre Angebote künftig über die systemeigenen App-Stores zu vertreiben, wenn sie Kinder und Jugendliche nicht ausschließen wollen, dann sollte dies auch in einem geregelten Verfahren möglich und demokratisch abgesichert sein.

Schon heute zeigt sich bei den App-Stores mit „Quasi-Monopol“ (Apple für iOS, Google für Android), dass deren Anbieter die Vertriebsmacht nutzen, um eigene kommerzielle und strategische Interessen durchzusetzen und mitunter eher offensichtlich willkürlich die Bereitstellung von Apps ablehnen, ohne dass der Anbieter unabhängig dies einfordern könnte.

Dies ist kein theoretisches Problem, sondern vermutlich jede auf App-Entwicklung spezialisierte Agentur kann umfangreich von abgelehnten Apps und Problemen mit den App-Stores berichten sowie von undurchsichtigen Verfahren der Store-Anbieter mit wenigen Widerspruchsmöglichkeiten.

Einige Beispiele von vielen: Die in Deutschland weit verbreitete Tolino-App als ebook-Reader musste in diesem Sommer die Kaufmöglichkeit für Bücher in der App einstellen, da sie sonst entweder Google an den Buch-Verkäufen finanziell hätte beteiligen müssen oder aber aus dem Play-Store geflogen wäre. Die JusProg-App für Android wurde vor einiger Zeit ohne Vorwarnung aus dem App-Store entfernt und der Account deaktiviert, da eine KI-Funktion sie fälschlich als sexualisierten Content interpretierte. Nicht einmal der Store-Support konnte dies rückgängig machen. Apple hat kürzlich die App eines großen deutschen Klinikums abgelehnt und auch Widersprüche abgelehnt, da dem US-Store-Anbieter zu viele Inhalte erst nach Nutzer-Login zugänglich waren.

Aus gutem Grund gibt es also alternative App-Stores neben den systemeigenen App-Stores, damit die Nutzerinnen und Nutzer wenigstens auf diesem Wege die Möglichkeit haben, auch Apps zu installieren, die nicht den kommerziellen Interessen der großen Betriebssystem-Anbieter entsprechen.

Wenn also der JMStV-E für Kinder und Jugendliche die Installationsmöglichkeit (kartellrechtlich eher bedenklich) auf die systemeigenen App-Stores beschränkt, dann sollte zwingend zugleich im Sinne der Presse- und Medienfreiheit und der digitalen Teilhabe der Kinder und Jugendlichen ein geordnetes Verfahren für den Vertrieb über die Stores und für unabhängige Widerspruchsverfahren bei Ablehnungen mit berücksichtigt werden.

5.2.4. Datenschutz in den App-Stores

Die meisten systemeigenen App-Stores erfordern eine Registrierung der Nutzerinnen und Nutzer, wenn diese Apps und Software installieren möchten. Die Speicherung der Daten erfolgt nicht immer auf Servern in der EU und eine CLOUD Act -Problematik ist häufig unvermeidbar.

Es ist unverständlich, wenn selbst im Angesicht von digitalem Schul-Notbetrieb während der Corona-Pandemie US-amerikanische Videokonferenz-Anbieter aus Datenschutzgründen für die Nutzung im Homeschooling untersagt werden, zugleich aber der JMStV-E dauerhaft implementieren möchte, dass Kinder und Jugendliche für die Installation von Apps zwingend ihre persönlichen Daten den Anbietern aus vorwiegend USA und China (z.B. Huawei, günstige Smartphones, TV-Boxen) bereitstellen müssen.

6. Digitale Teilhabe

In verschiedenen Wirkweisen reduziert der JMStV-E die Möglichkeiten der Kinder und Jugendlichen für digitale Teilhabe und wirkt in ihre Privatsphäre. Dies ist überraschend angesichts dessen, dass ansonsten von der EU bis in regionale Organisationen aktuell überall versucht wird, die digitale Teilhabe der Minderjährigen zu verbessern.

Bekanntermaßen steht Jugendmedienschutz häufig im Gegensatz zu anderen wichtigen Schutzgütern wie z.B. dem Datenschutz und eben der digitalen Teilhabe. Hier ist eine Balance zu finden.

In unseren Augen ist dies jedoch beim vorliegenden JMStV-E nur bedingt gelungen. Es werden für eher geringe Vorteile beim Jugendmedienschutz, die sich auf wenige Nutzungssituationen beschränken, sehr erhebliche Nachteile bei Privatsphäre, digitaler Selbstbestimmung und Teilhabe der Kinder und Jugendlichen in Kauf genommen.

Es sollten noch einmal dringend die Vor- und Nachteile der neuen Regelungen für die Minderjährigen gegeneinander abgewogen und eine bessere Balance gefunden werden. Dazu gehört auch eine Analyse des objektiven Regelungsbedarfs und welche Instrumente diesbezüglich zielführend sind.

6.1. Keine Profile

Die Schutzvorrichtung der Betriebssysteme sieht keine Profile für Kinder unterschiedlicher Altersstufen vor, sondern geht lediglich von einem On-/Off der Jugendschutz-Funktion aus.

Dies entspricht weder der Lebenswirklichkeit noch den Wünschen der Eltern, wie wir sie aus unserer Erfahrung kennen.

Während Smartphones, zumindest ab einem bestimmten Alter, häufig einem einzigen Kind zugeordnet sind, gilt dies für alle anderen Geräte und Betriebssysteme hingegen nicht. Tablets,

Notebooks, Desktop-Rechner, Spielekonsolen und TV-Boxen werden in der Regel von mehreren Personen in einem Haushalt verwendet.

Bei mehreren Kindern unterschiedlicher Altersstufen in einem Haushalt, ein üblicher Fall, können diese Szenarien passieren:

- Die Eltern stellen das Alter im Jugendschutz-Button vorsichtshalber auf das jüngste Kind ein: Die älteren Kinder werden unangemessen in ihren digitalen Möglichkeiten und ihrer Teilhabe im Internet beschränkt.
- Die Eltern stellen das Alter im Jugendschutz-Button auf das älteste Kind ein: Die jüngeren Kinder werden mit Inhalten konfrontiert, die nicht für ihr Alter geeignet sind.
- Die Eltern stellen vor jeder Nutzung das Alter in der neuen Schutzvorrichtung um: Der Vorteil einer „schnellen Lösung“ ist dahin. Die Eltern sind vermutlich hingegen schnell von den Mühen genervt und deaktivieren die gesamte Funktionalität.

Die Problematik verschärft sich noch deutlich angesichts dessen, dass ja nicht nur Altersstufen pro Kind einzustellen sind, sondern ggfls. auch gezielt ansonsten „ausgegraute“ Apps aktiviert werden müssen, wenn die Kinder diese z.B. für die Schule benötigen oder die Eltern diese für ältere Kinder gezielt erlauben möchten.

Da die Jugendschutzvorrichtung der Betriebssysteme keine Profile vorsieht, müssten diese Einstellungen von den Eltern bei jedem Nutzer/innen-Wechsel erneut erfolgen. In der Praxis ist kaum zu erwarten, dass sich Eltern diese Mühe machen werden. Im Ergebnis wären die Kinder von den Apps ausgeschlossen, die sie eigentlich nutzen dürften und auch hier die digitale Teilhabe ohne nennenswerten Vorteil beschränkt.

6.2. Privatsphäre der Kinder

Sowohl Kinder und Jugendliche als auch ihre Eltern sehen insbesondere die persönlichen Smartphones der Minderjährigen als deren Privatsphäre an – dies zeigen sowohl unsere Erfahrungen als auch diverse Studien sowie die Lebenserfahrung.

Die Regelungen des JMStV-E implizieren jedoch eine permanente Verletzung dieser wichtigen Privatsphäre, da Eltern häufig die Endgeräte ihrer Kinder in die Hand nehmen müssen. Kaum vermeidbar, dass sie dabei auch z.B. in dem Moment eintreffende WhatsApp-Nachrichten lesen, auch wenn die Jugendlichen z.B. ihren Eltern aktuell noch nicht verraten wollten, wer ihnen gerade Herzchen-Smileys schickt.

Jugendmedienschutz ist wichtig, aber darf im Ergebnis nicht zu „gläsernen Kindern“ führen.

6.3. Ausschluss von vielen Apps und Anwendungen

Wie vorstehend bereits ausgeführt, werden mit den Regelungen des JMStV-E die Kinder und Jugendlichen auf vielfältige Weise von der Nutzung von Apps und Software ausgeschlossen, auch wenn diese nicht entwicklungsbeeinträchtigend ist.

Dies beeinträchtigt nach unserer Einschätzung die Möglichkeiten zur digitalen Teilhabe der Minderjährigen in nicht angemessener Weise.

7. Betriebssysteme

Zur Grundidee und den Zweifeln an der juristischen wie praktischen Möglichkeiten nach Bundes- und Europarecht, Betriebssysteme über den Jugendmedienschutzstaatsvertrag zu regulieren, werden andere Organisationen und auch die Betreiber der Betriebssysteme nach unserer Kenntnis umfangreich Stellung nehmen. Wir möchten diese Anmerkungen deshalb hier nicht wiederholen, da sie JusProg und die praktischen Auswirkungen der neuen Regelungen nur am Rande betreffen.

Wir verweisen jedoch auf diese Stellungnahmen und erklären, dass auch wir die Zweifel teilen, dass die neuen Regelungen bei den Betriebssystemen in der Praxis durchsetzbar sind und über den JMStV Betriebssysteme reguliert werden können.

Ergänzend weisen wir darauf hin, dass die Definition von Betriebssystemen einen hohen Unsicherheitsfaktor bedingt. Wer ist eigentlich künftig für die Realisierung einer Jugendschutzvorrichtung verantwortlich, also „Anbieter“ eines Betriebssystems? Beispiel: Wenn ein Smartphone von einem Technikmarkt z.B. in einer gebrandeten Version angeboten wird, es von einem Smartphone-Hersteller mit einem stark customizten Betriebssystem versehen wurde, dieses aber auf z.B. Android basiert – wer ist dann der „Anbieter“ des Betriebssystems nach JMStV-E?

8. Kennzeichnungspflichten

Grundsätzlich ist das Bemühen um mehr Transparenz durch Kennzeichen und Hinweise durchaus begrüßenswert. Der JMStV-E führt jedoch eine Fülle neuer Kennzeichnungspflichten ein, die zudem nicht immer deckungsgleich sind mit den Anforderungen an Hinweise, die sich aus dem novellierten JuSchG ergeben.

Eine Überflutung der Eltern und Kinder mit Kennzeichen und Hinweisen wird nach unserer Ansicht eher das Gegenteil des Gewünschten bewirken – die Rezipienten schalten ähnlich „auf Durchzug“, wie es heute schon beim quasi automatisierten Wegklicken von Cookie-Bannern zu beobachten ist.

Wir regen deshalb an, die Kennzeichnungspflichten im Zusammenspiel mit dem JuSchG noch einmal kritisch auf den Prüfstand zu stellen und einen „digitalen Schilderwald“ zu vermeiden.

Dabei sollten auch diese Hinweise Berücksichtigung finden:

- Wenn Apps und Inhalte für Minderjährige blockiert werden, machen an diese gerichtete Kennzeichen und Hinweise an der Stelle keinen Sinn, da sie die Kinder und Jugendlichen ohnehin nicht aufrufen können.
- Webseiten beinhalten häufig Inhalte verschiedener Altersstufen und Art, sie können nicht mit „einem zentralen Kennzeichen“ sinnvoll beschrieben werden. Es ist weder realistisch, dass Eltern jede Einzelseite auf Kennzeichen prüfen, bevor ihre Kinder diese aufrufen, noch dass die Anbieter jede Einzelseite mit einem optischen Kennzeichen versehen. Das age.xml / age.-de.xml Label sieht hingegen eine URL-genaue Filterung bereits vor, so dass Minderjährige vor ungeeigneten Einzelseiten geschützt werden können.

9. Inkonsistenzen des JMStV-Entwurfs

Dem JMStV-E scheint uns an vielen Stellen noch die innere Konsistenz zu fehlen. Es ist zum Beispiel offensichtlich, dass die Autorinnen und Autoren bei einigen Regelungen einen sehr offenen Betriebssystem-Begriff vor Augen hatten, an anderen Stellen jedoch eigentlich gezielt Smartphones im Sinn hatten – was dann zu Regelungen geführt hat, die für andere Betriebssysteme nicht passen.

Ebenso bergen die Definitionen von Begrifflichkeiten (§ 3 u.a.) hohe Unsicherheit und werden diese Begriffe nach unserem Eindruck nicht durchgängig konsistent genutzt. Der unklare Unterschied zwischen „Apps“ und „Software-Anwendungen“ ist dafür ein Beispiel. Auch bleibt beispielsweise unklar, was genau der Begriff „Online-Suchmaschinen“ umfassen soll.

10. Praktikabilität

Der sogenannte Jugendschutz-Button soll vor allem Nutzerfreundlichkeit und Praktikabilität bringen und Eltern und andere Erziehungsberechtigte durch seine Einfachheit zur Nutzung motivieren.

Es bestehen in unseren Augen jedoch Zweifel, ob dieses begrüßenswerte Ziel in der Praxis auch erreicht wird.

Denn tatsächlich ist es mit dem Klicken des einen Buttons „ähnlich dem Dunkelmodus“ nicht getan, wenn Eltern sinnvoll Jugendmedienschutz auf dem Smartphone, Tablet, Notebook oder anderem Gerät einrichten möchten. Denn Eltern müssen außerdem:

- Einzelne Apps zusätzlich freigeben oder blockieren
- Bei mehreren Kindern ständig Altersstufen umstellen und Apps neu freigeben oder blockieren.
- Sich selbst per Passwort oder anderer Funktionalität autorisieren, wenn sie z.B. ein gemeinsam genutztes Tablet ohne Einschränkungen nutzen möchten.
- ... anschließend daran denken, die Jugendschutzvorrichtung wieder zu aktivieren

- Für den Schutz im Browser vor z.B. Gewaltpornografie zusätzlich ein Jugendschutzprogramm installieren und darin Profile pflegen.

Angesichts dessen scheint es zweifelhaft, ob die mit den neuen Regelungen verbundenen Einschränkungen für Kinder wie Eltern und Mühen der verschiedenen Beteiligten im sinnvollen Verhältnis zum gewünschten Effekt stehen.