Datenschutz und Mediensystem

Altersverifikation und Uploadfilter aus intradisziplinärer Perspektive

Quelle: https://unsplash.com/photos/FPtoLXKocg

von Tobias Keber

Das Recht auf den Schutz personenbezogener Daten kann mit dem Recht auf Freiheit der Meinungsäußerung und Informationsfreiheit in Konflikt geraten. Im Bereich medialer Berichterstattung, in der es naturgemäß auch um individualisierbare Personen geht, ist die Auflösung des Spannungsverhältnisses Teil des Tagesgeschäfts. Ausgleichswerkzeug ist das so genannte Medienprivileg, das die Datenverarbeitung zu journalistischen Zwecken von datenschutzrechtlichen Verpflichtungen teilweise freistellt.[1] Um die viel diskutierten Fragen zu dem Ausgleichsmechanismus soll es hier aber nicht gehen. Um schonenden Ausgleich kann sich nur bemühen, wer ein Spannungsverhältnis erkennt. Schwieriger wird es, wenn ein Konflikt nicht gesehen oder ein Problem bewusst, etwa zuständigkeitshalber ausgeklammert und damit insgesamt asymmetrisch adressiert wird. Die zwei nachfolgenden Konstellationen mögen für diesen Missstand als Beispiele dienen.

1 Aus kommunikationsrechtlicher Sicht ist diese Konzeption schon im Ansatz problematisch, denn die Möglichkeit der Berichterstattung auch unter Verwendung personenbezogener Daten ist funktional zwingend und damit konstituierendes Element der Medienfreiheit. Dazu Cornils, Matthias: Der Streit um das Medienprivileg. In: *ZUM*. Jg. 62, H. 8/9, 2018, S. 561–577.

›Blackout-Challenge‹, *TikTok* und Altersverifikation

Anfang des Jahres war eine Zehnjährige in Palermo auf Sizilien vermutlich bei einer gefährlichen Internet-Mutprobe für die Kurzvideo-App *TikTok* gestorben. Die Teilnehmer:innen der ›Blackout-Challenge‹ strangulierten sich selbst, so lange es ging. Es gewann, wer es am längsten aushielt.[1] Ein ebenso trauriges wie bekanntes Phänomen: Selbstgefährdung, gefährliche Mutproben und ihre Glorifizierung (wer mitmacht, bekommt anerkennende Likes) im Netz. Interessant an diesem Fall: nicht die Medienaufsicht, sondern die Datenschutzaufsicht in Italien (›Garante per la protezione die dati personali‹) schritt ein.[2] Die Behörde argumentierte, eine Mitgliedschaft bei *TikTok* sei (auch nach dem eigenen Hausrecht des Netzwerks) unter 13 Jahren nicht zulässig, wobei das aus datenschutzrechtlicher Sicht entgegen der Praxis des Unternehmens auch wirksam kontrolliert werden müsse. Gedanklich könnte man dies zur These verdichten: hätte es wirksamen Datenschutz gegeben, wäre die Zehnjährige nicht bei *TikTok* gewesen. Sie wäre vielleicht noch am Leben.

Tatsächlich wird man Datenschutz zunehmend auch als Jugendmedienschutz verstehen müssen. Im Mediensystem in Deutschland geschieht dies bis dato nicht, wie die nachfolgende Analyse zeigt.

Schutz vor entwicklungsbeeinträchtigenden Angeboten bei Video-Sharing-Diensten

Intuitiv würde man hierzulande die Alterskontrolle der Nutzer:innen auf einer Videoplattform zunächst einmal als jugendmedienschutzrechtliche Frage verstehen. Nach § 5a des jüngst reformierten Jugendmedienschutzstaatsvertrags (JMStV, in Kraft seit 07.11.2020) gilt, dass Video-Sharing-Dienste[3] Kinder und Jugendliche mit angemessenen Maßnahmen vor entwicklungsbeeinträchtigenden Angeboten schützen müssen. Das Angebot von *TikTok* wird man als normadressierten Video-Sharing-Dienst werten müssen, denn hier wird ›user-generated content‹ (UGC) von der Plattform nach bestimmten Ordnungskriterien (Algorithmen) aggregiert.[4] Gemäß § 5 Abs. 1 JMStV ist ein Angebot als entwicklungsbeeinträchtigend einzustufen, wenn es geeignet ist, die Entwicklung von Kindern oder Jugendlichen zu einer eigenverantwortlichen und gemeinschaftsfähigen Persönlichkeit zu beeinträchtigen. Eine ›Blackout Challenge‹ wird man als ein solches Angebot verstehen können, jedenfalls wenn es wie hier besonders jugendaffin und über den Wettbewerbscharakter für die junge Zielgruppe besonders attraktiv dargestellt wird.

Altersverifikationssysteme (AV-Systeme) als Schutzmaßnahme

§ 5a Absatz 2 JMStV benennt dann als Schutzmaßnahme (nicht abschließend) die Einrichtung und den Betrieb von Systemen zur Altersverifikation. Altersverifikationssysteme in diesem Sinne sind über die geschlossenen Benutzergruppen im Sinne des § 4 Abs. 2 S. 2 (Zugang nur »ab 18«) JMStV hinausgehende, altersstufendifferenzierende[5] Maßnahmen der Zugangsbeschränkung auf Grundlage eines durch das System zu prüfenden Alters der Nutzenden.[6] Auch wenn die Altersverifikationssysteme des § 5a Absatz 2 JMStV damit nicht deckungsgleich mit den bereits vor der JMStV-Reform etablierten Systemen nach § 4 Abs. 2 S. 2 JMStV sind, ließe sich technisch daran anknüpfen, denn ein System, das den Nachweis der Volljährigkeit erbringen soll, könnte grundsätzlich ebenso gut die Altersstufe »ab 12« belegen.

Damit könnten die Erfahrungen und die Bewertung der AV-Systeme auch für Video-Sharing-Dienste wie *TikTok* fruchtbar gemacht werden. Am Ausgangsfall anknüpfend könnte das bedeuten, mit implementierter Altersverifikation auf der Plattform würde der Gefahr eines solchen Unfalls im deutschen Mediensystem künftig wirksam begegnet. Um diese These verifizieren zu können, ist ein näherer Blick auf das System der Altersverifikation im Jugendmedienschutz erforderlich.

Bewertung von AV-Systemen durch die Kommission für Jugendmedienschutz (KJM)

Die Bewertung von AV-Systemen obliegt der Kommission für Jugendmedienschutz (KJM) als Organ der Landesmedienanstalten in Deutschland. Ein von der KJM positiv bewertetes AV-System kann ein Anbieter wählen, um seinen gesetzlichen Pflichten aus dem Jugendmedienstaatsvertrag (mutmaßlich) zu entsprechen.[7] In der aktuellen Positivliste der KJM finden sich technisch unterschiedliche Lösungen verschiedenster Anbieter.[8] Die Kriterien zur Bewertung von Konzepten zur Altersverifikation hat die KJM als »AVS-Raster« veröffentlicht.[9] In der Liste der KJM positiv bewertet wird beispielsweise das Angebot *Yoti* App der Yoti Ltd., einem Unternehmen mit Sitz in London (UK). Die KJM kam im Dezember 2020 zu dem Ergebnis, dass das System bei entsprechender Umsetzung als vollständiges AVS-Konzept im Sinne der KJM-Kriterien zur Sicherstellung einer geschlossenen Benutzergruppe (§ 4 Abs. 2 Satz 2 JMStV) gemäß Jugendmedienschutz-Staatsvertrag (JMStV) geeignet ist. Kurz: Der Anbieter medialer Inhalte kann durch Einbindung der *Yoti* Altersverifikation in seine Angebotsinfrastruktur sicherstellen, dass Jugendliche keinen Zugriff auf für sie ungeeignete Inhalte haben.

Ließe sich die *Yoti* App dann auch altersdifferenziert für den Video-Sharing-Dienst *TikTok* einsetzen, der selbst ja keine Inhalte anbietet, sondern lediglich als Plattform für ›user-generated content‹ fungiert und würde dies den schutzwürdigen Interessen der Rezipient:innen gerecht?

Datenschutz als fehlendes Bewertungskriterium der KJM

Aus datenschutzrechtlicher Perspektive wird man die Bewertung der *Yoti* App durch die KJM kritisch sehen müssen. Dies jedenfalls, nachdem man sich die Funktionsweise der App vergegenwärtigt und das ›Privacy‹-Statement des Anbieters auf der Webseite gelesen hat: Technisch handelt es sich um ein Verfahren, dass die Identität der Nutzer:in über eine Mehrfaktor-Authentifizierung bei Anmeldung und nachfolgend eine Lebenderkennung des Gesichts (Bewegtselfie) mit dem Smartphone und den Abgleich des Ausweisdokuments ermöglicht. Im ›Privacy‹-Statement auf der Webseite ist zu lesen: »In future we may send your personal information to countries outside the UK. [...]However, we will make sure that your personal information is properly protected.«[10] Das ist nicht gerade besonders transparent, weder mit Blick auf die Kategorien der zu transferierenden Daten (auch die biometrischen Daten im Zusammenhang mit dem angefertigten Bewegtselfie?) noch hinsichtlich des Ziels eines Drittstaatentransfers.

Datenschutzrechtliche Bedenken haben im bisherigen Modell der Positivbewertung eines AV-Systems durch die KJM allerdings kein Gewicht. Natürlich nicht, könnte man sagen, denn die KJM ist keine datenschutzrechtliche Aufsichtsbehörde, die Prüfung datenschutzrechtlicher Fragen ist nicht ›ihr Business‹. Dem entsprechend heißt es im AVS-Raster auch nur lapidar: »Die für die Altersprüfung jeweils benötigten Personendaten der zu identifizierenden Person sollten in erforderlichem Maße unter Beachtung datenschutzrechtlicher Vorgaben erfasst und gespeichert werden (z. B. Geburtsdatum, Name, Adresse). Eine Erfassung nur des Alters der identifizierten Person ist nur dann ausreichend, wenn dieses im gleichen Schritt mit eindeutigen Authentifikationsmerkmalen verknüpft ist.«[11] Das datenschutzrechtliche Gebot der Datenminimierung (Art. 5 Abs. 1 lit. c) DSGVO) wird hier also zu einem ›nice to have‹ degradiert.

Altersverifikation ist Jugendschutz ist Datenschutz.

Ist das aus Sicht der problematische Inhalte potentiell rezipierenden Nutzer:innen nicht defizitär? Müsste die KJM im Rahmen der Positivbewertung auf der Webseite nicht wenigstens der guten Ordnung halber (deutlicher Disclaimer) darauf hinweisen, dass ein von ihr positiv bewertetes System datenschutzrechtlich ungeprüft ist?

In Zukunft müssten datenschutzrechtliche Erwägungen jedenfalls bei AV-Systemen i. S. d. § 5a JMStV eine Rolle spielen, denn nach Absatz 1 der Vorschrift müssen die von den Video-Sharing-Dienst-Anbietern ergriffenen Maßnahmen »angemessen« sein. Der Einsatz von datenschutzrechtlich defizitären AV-Systemen kann in der für die Angemessenheit erforderlichen Gesamtschau aller Umstände[12] doch jedenfalls keine zu vernachlässigende Größe sein.

Uploadfilter und der Datenschutz

Bleiben wir bei Video-Sharing-Diensten und wenden uns einem zweiten Beispiel asymmetrischer, bzw. defizitär geführter Diskussion vor dem Hintergrund des eingangs erwähnten Spannungsverhältnisses zu: automatisierte Mechanismen zur Verhinderung urheberrechtlich nicht erlaubter Nutzungen auf diesen Plattformen. Die Debatte rund um die so genannten Uploadfilter ist in der öffentlichen Wahrnehmung leiser geworden. Unionsrechtlich ist das Thema (von dem noch anhängigen Verfahren des Europäischen Gerichtshofs abgesehen[13]) derzeit ausdiskutiert, die *Directive on Copyright in the Digital Single Market*[14] (DSM-RL) ist seit dem 6. Juni 2019 in Kraft und bis zum 7. Juni 2021 in nationales Recht umzusetzen.

Lohnenswert bleibt es aber, über die mit dem neuen Regelwerk verbundenen und im öffentlichen Diskurs nur am Rande diskutierten datenschutzrechtlichen Fragen nachzudenken. Das betrifft beispielsweise die Gefahr der Begründung eines Filtertechnikdatenmonopols, wie es der Bundesdatenschutzbeauftragte Ulrich Kelber 2019 formuliert hat.[15] Die Befürchtung ist, dass insbesondere kleinere Plattformen Uploadfilter nicht als teure Eigenentwicklungen mit datensouveräner Verarbeitung implementieren werden, sondern die Infrastruktur der marktführenden Unternehmen (Alphabet Inc. mit *YouTube*) einbinden werden. Dabei geht es also weniger um die individualrechtliche Perspektive, sondern um die datenwettbewerbsrechtliche Seite. Wie sich dies in Zukunft entwickeln wird, lässt sich derzeit schwer abschätzen. Greifbarer sind vielleicht die individualrechtlichen Implikationen, denn die Umsetzung der DSM-RL und namentlich der Uploadfilter im Rahmen des Urheberrechts-Diensteanbieter-Gesetzes (UrhDaG)[16] sind nun weitestgehend abgeschlossen. Der Entwurf eines Gesetzes zur Anpassung des Urheberrechts an die Erfordernisse des digitalen Binnenmarktes[17] war zuletzt Gegenstand einer öffentlichen Anhörung im Ausschuss für Recht und Verbraucherschutz am 12. April 2021.

DSM-RL, UrhDaG und der Datenschutz

Der Gesetzgeber steht vor einer großen Herausforderung: den hochkomplexen Vorgaben des Art. 17 DSM-RL Rechnung zu tragen (was für sich betrachtet

schon als die Quadratur des Kreises bezeichnet wurde[18]) und (das wird gerne übersehen) das Ganze auch noch datenschutzkonform nach Artikel 28 DSM-RL auszugestalten.

Plattformen haften nach dem neuen Regime nur dann nicht für die öffentliche Widergabe der hochgeladenen Inhalte, wenn sie sich einerseits »bestmöglich« um den Erwerb von urheberrechtlichen Lizenzen bemühen (§ 4 Abs. 1 UrhDaG) und zum anderen Mechanismen zur Verhinderung unerlaubter Nutzungen implementieren (§§ 7–11 UrhDaG).[19] Vor diesem Hintergrund spannt sich ein komplexes Prozessdiagramm auf, das ausschnittsweise wie folgt visualisiert werden kann (siehe Abb. 1).[20]

Inhalte liegen bei den durch das UrhDaG adressierten Plattformen als Dateien vor. Diese müssen eindeutig zuordnungsfähig und maschinenlesbar sein. Rechteinhaber müssen dabei helfen, dafür erforderliche und für die Plattform lesbare Stempel zu definieren. Auf dieser Grundlage kann der Mechanismus dann bestimmte Inhalte standardmäßig blockieren und/oder Nutzer:innen die Möglichkeit einräumen, den Upload bestimmter Inhalte als ausnahmsweise zulässig (etwa weil es sich um ein Zitat handelt) zu kennzeichnen. Aus datenrechtlicher Perspektive geht es zunächst nur um werkinhaltsbezogene Daten (Stempel mit Werksidentifikationsdaten), was datenschutzrechtlich so lange unproblematisch ist, als kein Personenbezug gegeben ist.[21]

Datensammlung und Missbrauchsmanagement

Für das hier adressierte Problem entscheidend sind aber u. a. die rund um das Missbrauchsmanagement (§ 18) entstehenden Daten. Das Konzept des UrhDaG sieht Maßnahmen vor, die den missbräuchlichen Gebrauch bestimmter Maßnahmen innerhalb des UrhDaG sanktionieren. So kann ein Rechteinhaber einen »Not-Aus-Knopf« (diese Maßnahme kann bei der Erklärung der Nutzer:innen, sie dürfen ausnahmsweise hochladen, zur Anwendung kommen) ebenso missbräuchlich einsetzen wie die Nutzer:innen die Möglichkeit der Kennzeichnung einer Nutzung als ausnahmsweise erlaubt überstrapazieren können. Für beide Szenarien gilt: häufen sie sich, verlieren die betroffenen Rechteinhaber oder Nutzer:innen bestimmte Rechte (siehe Abb. 2).

Die Daten rund um das Missbrauchsmanagement müssen jedenfalls personenbeziehbar sein und die Frage ist, was mit diesen Daten über das plattforminterne Missbrauchsmanagement hinaus passieren darf. Relevant jedenfalls sind die daraus ableitbaren Informationen, denn Schadensersatzansprüche gegen uploadende Nutzer:innen bleiben unter bestimmten Voraussetzung möglich (vgl. § 12 Abs. 3 UrhDaG e.contr.) und da kann es (bspw. für die Bestimmung der Vorsatzebene) durchaus relevant sein, wie oft ›false-flagging‹ betrieben wurde.

Missbrauchsmanagementdaten und Auskunftspflicht

Hinsichtlich der Herausgabe dieser Daten findet sich im UrhDaG keine spezielle Regelegung (namentlich

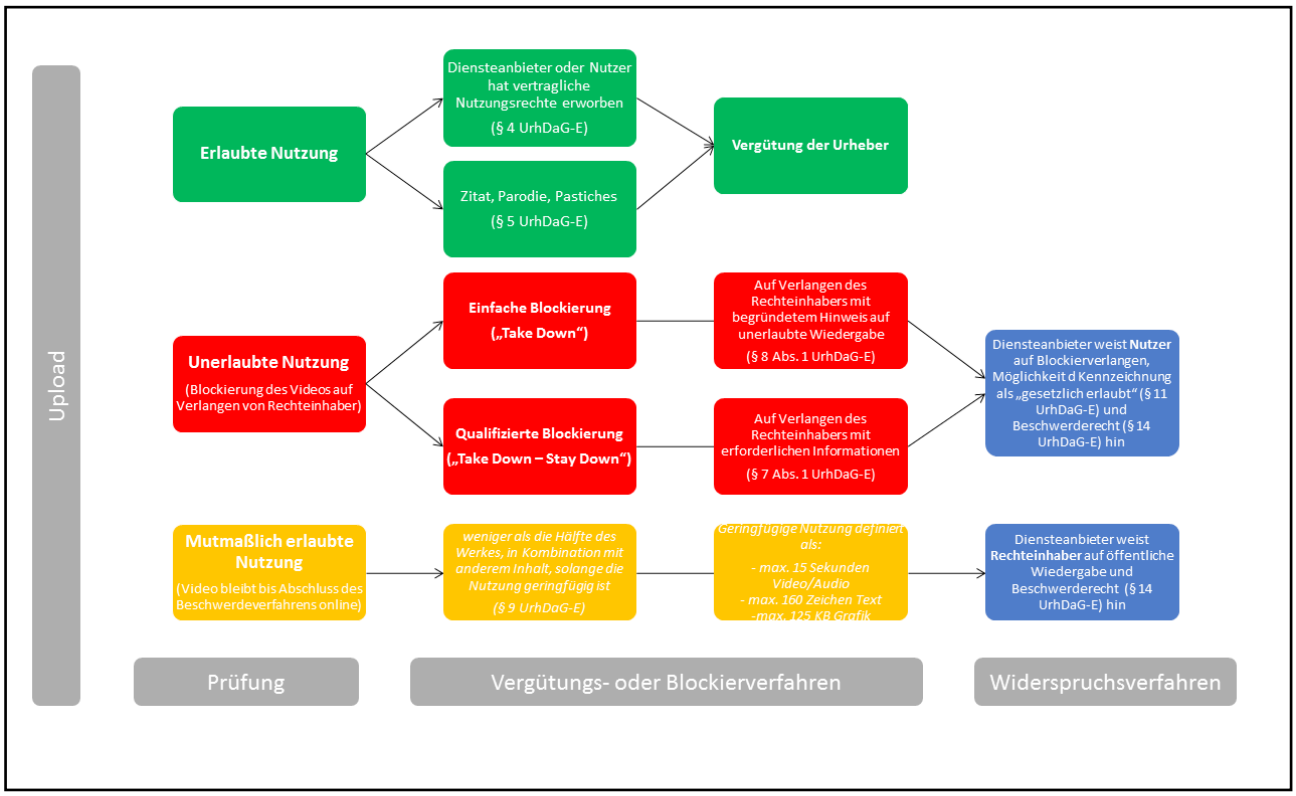

Abb. 1: Prozessdiagramm Upload nach UrhDaG-E; eigene Darstellung.

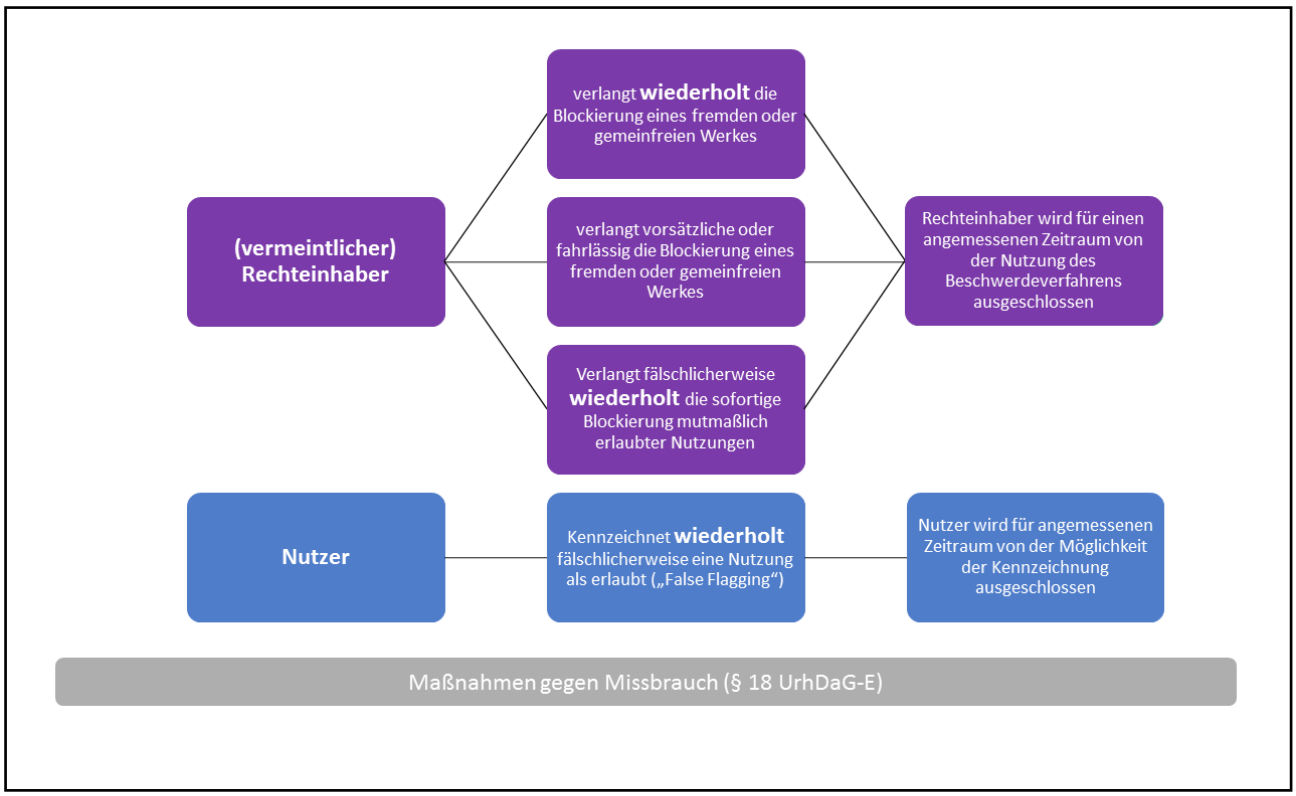

Abb. 2: Maßnahmen gegen Mißbrauch nach UrhDaG-E; eigene Darstellung.

§ 19 greift nicht), also bleibt der Rückgriff auf die Auskunftsrechte aus § 101 Absatz 1 Urheberrechtsgesetz (UrhG) gegen den Verletzenden und § 101 Absatz 2 Ziffer 3 UrhG gegen die filternde Plattform. Der Umfang der Auskunft bestimmt sich nach § 101 Absatz 3 UrhG. Den wird man im Lichte der Rechtsprechung des Europäischen Gerichtshofs[22] wohl so lesen müssen, dass Missbrauchsmanagementdaten nicht auskunftsgegenständlich sind. Daraus müsste dann auch folgen, dass ein von § 101 UrhG unabhängiger und über § 242 Bürgerliches Gesetzbuch begründeter Auskunftsanspruch ausgeschlossen ist. Klar gemacht hat der Entwurfsgesetzgeber das bis dato indes nicht.

Fazit

Im Schatten offenkundiger Konfliktlinien zwischen dem Datenschutzrecht und den Medien- und Informationsfreiheiten, wie sie beispielsweise beim sogenannten Medienprivileg zu Tage tritt, stehen die Rechtspositionen auch andernorts in vitaler Wechselwirkung, ohne dass dies in der angemessenen Symmetrie diskutiert würde.

Das Beispiel zu entwicklungsbeeinträchtigenden Inhalten bei *TikTok* wirft die Frage auf, warum der Datenschutz bei der Bewertung von zugangsbeschränkenden Mechanismen im Jugendmedienschutz derart marginalisiert wird. Mit dem Verweis auf die der Kompetenzverteilung geschuldeten Sachzwänge und die Situation de lege lata darf es nicht sein Bewenden haben. Datenschutz und Jugendmedienschutz müssen gemeinsam gedacht werden, denn auch Datenschutz ist Jugendmedienschutz.

Defizitär diskutiert wird der Datenschutz auch im Rahmen der Urheberrechtsreform im Zusammenhang mit den für Plattformen zukünftig (faktisch) verpflichtend zu implementierenden Uploadfiltern. Auch an dieser Stelle wünscht man sich mehr intradisziplinären Diskurs und konstruktiven, fachgebietsübergreifenden Austausch.

Prof. Dr. Tobias Keber

Professor für Medienrecht und Medienpolitik in der digitalen Gesellschaft, Hochschule der Medien (HdM) Stuttgart

Endnoten

1 Süddeutsche Zeitung: Tiktok in Italien sagt Alterskontrolle zu. In: *Süddeutsche Zeitung* vom 04.02.2021. Online: https://www.sueddeutsche.de/panorama/italien-unglueck-und-unfall-tiktok-datenschutz-altersgrenze-1.5196538 (25.05.2021).

2 Zum Hintergrund des Verfahrens vgl. die Meldung auf der Webseite des European Data Protection Boards: Italian DPA imposes limitation on processing on TikTok after the death of a Girl from Palermo. In: *edpb* vom 26.01.2021. Online: https://edpb.europa.eu/news/national-news/2021/italian-dpa-imposes-limitation-processing-tiktok-after-death-girl-palermo_en (25.05.2021).

3 Als solchen wird man *TikTok* einstufen müssen, vgl. § 2 Ziff. 22 Medienstaatsvertrag (MStV).

4 Vgl. § 2 Ziff. 22 MStV, wonach ein Video-Sharing-Dienst als ein Telemedium definiert wird, »bei dem der Hauptzweck des Dienstes oder eines trennbaren Teils des Dienstes oder eine wesentliche Funktion des Dienstes darin besteht, Sendungen mit bewegten Bildern oder nutzergenerierte Videos, für die der Diensteanbieter keine redaktionelle Verantwortung trägt, der Allgemeinheit bereitzustellen, wobei der Diensteanbieter die Organisation der Sendungen oder der nutzergenerierten Videos, auch mit automatischen Mitteln oder Algorithmen, bestimmt«.

5 § 5 Abs. 1 S. 2 JMStV sieht die Altersstufen ab 6 Jahren, ab 12 Jahren, ab 16 Jahren und ab 18 Jahren vor.

6 Lamprecht-Weißenborn, Nicola. In: Bornemann, Roland/Erdemir, Murad (Hg.): *Jugendmedienschutz-Staatsvertrag.* Baden-Baden: Nomos 2021, § 5a JMStV, Rn. 20.

7 Zu Hintergrund und (beschränkter) Reichweite der Positivbewertung vgl. die Informationen der KJM: *Altersverifikationssysteme.* Online: https://www.kjm-online.de/aufsicht/technischer-jugendmedienschutz/unzulaessige-angebote/altersverifikationssysteme/ (25.05.2021).

8 Vgl. die Positivliste ebd.

9 Das Papier ist online abrufbar. Kommission für Jugendmedienschutz: *Kriterien zur Bewertung von Konzepten für Altersverifikationssysteme als Elemente zur Sicherstellung geschlossener Benutzergruppen in Telemedien nach § 4 Abs. 2 S. 2 JMStV (»AVS-RASTER«)*. Online: https://www.kjm-online.de/fileadmin/user_upload/KJM/Aufsicht/Technischer_Jugendmedienschutz/KJM-AVS-Raster.pdf (25.05.2021).

10 Die *Yoti* ›Privacy‹-Informationen sind online abrufbar. Yoti: *Privacy Centre*. Online: https://www.yoti.com/privacypolicy/ (25.05.2021).

11 AVS-RASTER der KJM, S. 5.

12 Vgl. dazu Art. 28 b Abs. 3 S. 1 und S. 2 der Richtlinie über audiovisuelle Mediendienste (AVMD-RL), die mit § 5 a JMStV umgesetzt wurden.

13 Am 24.05.2019 reichte Polen eine Nichtigkeitsklage gegen Artikel 17 Absatz 4 der Urheberrechtsrichtlinie ein (Rechtssache C-401/19).

14 Richtlinie (EU) 2019/790 des Europäischen Parlaments und des Rates vom 17.04.2019 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG.

15 Interview von Simon Hurtz mit Ulrich Kelber: »Upload-Filter halten wir für falsch und gefährlich«. In: *Süddeutsche Zeitung* vom 15.03.2019. Online: https://www.sueddeutsche.de/digital/ulrich-kelber-datenschutz-upload-filter-1.4366777 (25.05.2021).

16 Entwurf eines Gesetzes über die urheberrechtliche Verantwortlichkeit von Diensteanbietern für das Teilen von Online-Inhalten (UrhDaG). Die finale Fassung des Urheberrechts-Diensteanbieter-Gesetz (UrhDaG) vom 31. Mai 2021 (BGBl. I S. 1204, 1215) ist am 1.8.2021 in Kraft getreten.

17 Bundestagsdrucksache (BT-Drs.) 19/27426 v. 09.03.2021.

18 So der Sachverständige Frey in der Anhörung am 12.04.2021. Die Sachverständigenstellungnahmen zum Gesetzesentwurf im Rahmen der öffentlichen Anhörung im Ausschuss für Recht und Verbraucherschutz sind abrufbar unter Deutscher Bundestag: *Geteiltes Experten-Echo zur Urheberrechtsnovelle*. In: https://www.bundestag.de/dokumente/textarchiv/2021/kw15-pa-recht-830028 (25.05.2021).

19 Instruktiv zum Mechanismus des UrhDaG: Conrad, Albrecht /Nolte, Georg: Schrankenbestimmungen im Anwendungsbereich des UrhDaG. In: ZUM. Jg. 65, H. 2, 2021, S. 111–151; Kaesling, Katharina/Knapp, Jakob: Umsetzung der urheberrechtlichen Verantwortlichkeit von Upload-Plattformen. In: MMR. 2021, S. 11–15.

20 Eigene Darstellung. Für eine Visualisierung einer früheren (!) Entwurfsfassung vgl. ferner auch das beim Bundesjustizministerium abrufbare Papier: *Grafik Öffentliche Wiedergabe und Vergütungen* vom 16.10.2020. Online: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_Urheberrecht_Grafik-Wiedergabe-Verguetung.pdf (25.05.2021).

21 Zu den datenschutzrechtlichen Implikationen im UrhDaG insgesamt Becker, Maximilian: Automatisierte Rechtsdurchsetzung im Umsetzungsentwurf zu Art. 17 DSM-RL. In: ZUM. Jg. 64, H. 10, 2020, S. 681–691 (689); Vgl. ferner Stellungnahme der Digitalen Gesellschaft e.V. im Rahmen der Konsultation des BMJV zum Diskussionsentwurf für ein Zweites Gesetz zur Anpassung des Urheberrechts an die Erfordernisse des digitalen Binnenmarkts. Jennisen, Tom: Uploadfilter und Datenschutz: Gesetzgeber ignoriert das Problem. In: *Digitale Gesellschaft* von 13.11.2020. Online: https://digitalegesellschaft.de/2020/11/uploadfilter-und-datenschutz-gesetzgeber-ignoriert-das-problem/ (25.05.2021).

22 Vgl. EuGH C 264/19, 09.07.2020 Constantin Film Verleih GmbH gegen YouTube LLC und Google Inc.