20. April 2021 **RiVG Dr. Malte Engeler**

Schleswig-Holsteinisches Verwaltungsgericht
Brockdorff-Rantzau-Straße 13
24837 Schleswig
Telefon: 04621/86-0
E-Mail: malte.engeler@ovg.landsh.de

Deutscher Bundestag
19. Wahlperiode
Ausschuss für Wirtschaft und Energie

Ausschussdrucksache 19(9)1056
20. April 2021

An den

Deutschen Bundestag
Ausschuss für Wirtschaft und Energie

Nur per E-Mail an: wirtschaftsausschuss@bundestag.de

Stellungnahme

im Rahmen der Öffentlichen Anhörung
im Ausschuss für Wirtschaft und Energie
des Deutschen Bundestages am 21. April 2021

zum

Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG)
(BT-Drucksache 19/27441)

vorgelegt von

Dr. Malte Engeler[*]
Richter am Schleswig-Holsteinischen Verwaltungsgericht

[*] Die Ausführungen geben einzig die persönliche Auffassung des Sachverständigen wieder.

Diese Stellungnahme beschränkt sich in ihrem Gegenstand auf wenige Einzelfragen rund um die mit dem Entwurf des TTDSG (TTDSG-E) beabsichtigte Umsetzung des Art. 5 Abs. 3 ePrivacy-Richtlinie (RL 2002/58/EG) [1] durch § 24 TTDSG-E sowie ergänzende Kurzbemerkungen.

Einzugehen ist dabei auf

- die gegenüber Vorentwürfen gestrichene Normierung von Personal Information Management Services (PIMS, dazu unter I.) sowie
- fehlende Vorgaben für verbindliche Voreinstellungen (dazu unter II.),
- mögliche Konkretisierungen der Speicherung und des Zugriffs im erforderlichen Umfang in § 24 Abs. 2 Nr. 2 TTDSG-E (dazu unter III.),
- fehlende Regelungen zur Gestaltung von Einwilligungserklärungen und zur Bekämpfung von Dark Patterns (dazu unter IV.) sowie
- Ansatzpunkte für die Trilog-Gespräche im Kontext der geplanten ePrivacy-Verordnung (dazu unter V.).

Darüber hinaus ist meines Erachtens nach auf mögliche Unsicherheiten bei der Bestimmung der Zuständigkeit der Datenschutzaufsichtsbehörden der Länder für die Durchsetzung des § 24 TTDSG-E hinzuweisen sowie auf die Bemühungen einzugehen, die Verpflichtung zur Ermöglichung der anonymen Nutzbarkeit von Telemedien in § 19 Abs. 2 TTDSG-E zu streichen (zu beidem unter VI.).

Dieser Fokus sowie gewisse Abstriche bei der Durchdringungstiefe waren angesichts der knapp bemessenen Vorbereitungszeit für die kurzfristig einberufene Anhörung unvermeidbar.

[1] In der durch Art. 2 Nr. 5 RL 2009/136/EG geänderten Fassung.

I. Zum Regulierung von Personal Information Management Services

Der im Juli 2020 geleakte Referentenentwurf des TTDSG (TTDSG-RefE)[2] enthielt in § 3 TTDSG-RefE eine Regelung zu anerkannten Diensten zur Verwaltung persönlicher Informationen und bezog sich in seiner Entwurfsbegründung unter anderem auf Forderungen der „Verbraucherverbände" nach entsprechender Regulierung.[3]

PIMS dienen im Grunde zwei Zielen: Sie vereinfachen das Verwalten und die Erteilung datenschutzrechtlicher Einwilligungen und legen diese Verwaltung in unabhängige Hände. Letzteres soll insbesondere die Entscheidungsmacht einzelner großer Browser-Herstellenden über die technische Möglichkeit einzelner Datenverarbeitungen durch Telemedienanbietende (insbesondere der Umfang der Nachverfolgung des Verhaltens von Nutzenden) begrenzen.

Der Verzicht auf eine Regulierung von Personal Information Management Services (PIMS) ist u.a. in der juristischen Literatur[4] und aus dem Kreis der Wirtschaft[5] kritisiert worden. Der Verzicht ist meines Erachtens nach – ungeachtet ohnehin bestehender datenschutzrechtlicher Hürden (dazu unter 1.) – entgegen dieser Kritik aber im Hinblick auf effektiven Grundrechtsschutz sinnvoll (dazu unter 2.).

1. Datenschutzrechtliche Hürden für die Regulierung von PIMS

Datenschutzrechtlich sind PIMS im Kontext von Art. 6 Abs. 1 Satz 1 Buchst. a) DSGVO und Art. 4 Nr. 11 DSGVO zu betrachten, weil sie im Vorfeld einer Datenverarbeitung eine Einwilligung einholen und im Verarbeitungsfall gewissermaßen als Boten zwischen Betroffenen und Verantwortlichen verbindliche Erklärungen transportieren sollen. Damit sehen sich rechtliche Konkretisierungen von PIMS zwangsweise einer gewissen Skepsis hinsichtlich ihrer Europarechtskonformität ausgesetzt, da sie Gefahr laufen, die Vorgaben der DSGVO zu modifizieren, ohne dass für derartige Modifikationen ein mitgliedsstaatlicher Spielraum unmittelbar erkennbar wäre. So setzen PIMS beispielsweise eine gewisse

---

[2] Referentenentwurf, Bearbeitungsstand: 14.07.2020, online verfügbar etwa unter https://www.heise.de/downloads/18/2/9/4/6/4/2/1/20200731_RefE_TTDSG_cleaned.pdf (abgerufen am 18.04.2021).

[3] Vgl. Seite 35 der Entwurfsbegründung des TTDSG-RefE.

[4] *Schwartmann/Benedikt/Reif*, MMR 2021, 99, 101.

[5] *Schwartmann/Hanloser/Weiß*, Kurzgutachten im Auftrag der European netID Foundation, online abrufbar unter https://enid.foundation/wp-content/uploads/2021/03/Schwartmann_Hanloser_Weiss-Kurzgutachten_Dienste_zur_Einwilligungsverwaltung_20210302.pdf (abgerufen am 18.04.2021).

Standardisierung von Datenverarbeitungsvorgängen bei den Verantwortlichen voraus, wenn PIMS ihr Ziel erreichen sollen, Betroffenen zu ermöglichen, sich vorab zentral und allgemein zu Verarbeitungsvorgängen zu erklären.

Dies kann im Einzelfall mit den Anforderungen der DSGVO kollidieren, die etwa in Art. 4 Nr. 11 DSGVO hohe Anforderungen an die Konkretheit von Einwilligungserklärungen stellt („unmissverständlich abgegebene Willensbekundung"). Daneben überträgt Art. 7 Abs. 1 DSGVO den für die Datenverarbeitung Verantwortlichen die Beweislast dafür, dass überhaupt eine Einwilligung erteilt worden ist. Verantwortliche wären also zwingend auf die Mitwirkung von Betreibenden der PIMS angewiesen, was gewisse Beweisnöte mit sich bringen kann. Um größtmögliche Effektivität von PIMS garantieren zu können, müsste ihre Normierung also eine gewisse Distanz zu den Anforderungen der DSGVO wagen.[6] Allein mit Blick auf die damit einhergehenden europarechtlichen Risiken erscheint die Entscheidung, auf eine Regulierung im TTDSG-E zu verzichten und stattdessen auf den Data Governments Act zu verweisen, nachvollziehbar.

2. PIMS im Kontext des Grundrechtsschutzes

Der Verzicht auf die Regulierung von PIMS ist aber vor allem mit Blick auf wirksamen Grundrechtsschutz ratsam, weil PIMS kein Werkzeug zur Durchsetzung des Rechts Betroffener auf Schutz der sie betreffenden personenbezogenen Daten (Art. 8 GRCh) sind. Sie sind vielmehr ein Werkzeug, das zugunsten von Telemedienanbietenden und Betreibenden von Werbenetzwerken einen einfachen und ungestörten Zugang zu den für ihre Geschäftsfelder so wichtigen Einwilligungserklärungen der Betroffenen sicherstellt.[7]

Die digitalpolitische Herausforderung, die im Rahmen des Datenschutzes bei Telemedien adressiert werden muss, ist größer als die Frage, wie der Prozess der Erteilung von Einwilligungen komfortabler gestaltet werden kann. Die Herausforderung ist vielmehr, eine Technologie gesellschaftsverträglich zu regulieren, die ursprünglich zwar vergleichsweise harmlosen Zielen diente (dem berechtigen Ziel der Monetarisierung digitaler Angebote), im Verlauf aber vielfältiges Missbrauchspotential offenbart hat. So basiert die telemedial mögliche Auslieferung personalisierter polarisierender Inhalte und die damit geschaffene Grundlage für toxische Kommunikationsverhältnisse in der digitalen Welt letztlich auf den gleichen technischen Grundlagen wie das Ausliefern personalisierter Werbung: Verfahren

---

[6] Ebenso und mit weiteren Nachweisen *Buchner/Kühling*, DS-GVO BDSG 3. Auflage 2020, Art. 7 Rn. 66; *Specht*, Specht/Mantz DatenschutzR-Hdb § 9 Rn. 39.

[7] Kritisch zu dieser Bedeutung von PIMS als Kommerzialisierungswerkzeug personenbezogener Daten auch *Peitz/Schweitzer*, NJW 2018, 275, 278.

der Erfassung, Aggregation und Auswertung von Informationen über das Verhalten von Menschen im digitalen Raum.

Aus diesem Grund sollte die Lösung auch nicht darin gesucht werden, diese technischen Verfahren mithilfe einer Einwilligung datenschutzrechtlich zu legitimieren. Die Lösung kann stattdessen nur in einer Regulierung jener Verfahren liegen, die die Auslieferung personalisierter Inhalte überhaupt erst ermöglichen. PIMS sind in diesem Kontext also nicht Teil einer Lösung, weil auch sie nur darauf hinauslaufen, es Betroffenen leichter zu machen, die datenschutzrechtliche Grundlage für derartige Verfahren – die Einwilligung – zu liefern, statt die Frage zu beantworten, in welchem Umfang überhaupt derartige Verfahren zulässig sein sollen. Die datenschutzrechtliche Einwilligung entfaltet in diesem Zusammenhang kaum Schutz, dementsprechend sind Werkzeuge wie PIMS, die lediglich die Erteilung der Einwilligung erleichtern, gleichermaßen ungeeignet, um das Problem technischer Tracking- und Personalisierungsverfahren wirksam zu adressieren.[8]

Soweit für PIMS darüber hinaus als Argument ins Feld geführt wird, sie würden die Macht der Gatekeeper bändigen,[9] handelt es sich dabei ebenfalls um eine verkürzte Darstellung. Wenn Browserherstellende mit nennenswerter Verbreitung selbstständig die Möglichkeit des Zugriffs aus Third-Party-Cookies begrenzen,[10] setzen sie damit jenen (Überwachungs) Technologien Grenzen, deren Gefahren gerade auch die ePrivacy-Richtlinie adressieren will. PIMS sind in diesem Zusammenhang indes ebenfalls kein Werkzeug zum Schutz von Rechten der Nutzenden, sondern dienen letztlich dem Ziel, den Browser- und App-Herstellenden die Kontrolle darüber wieder zu entziehen, welche technischen Verfahren der Gestaltung und Auslieferung personalisierter Inhalte möglich sind und den Betreibenden von Werbenetzwerken verlorenen Spielraum zurückzugeben.

Sich in diesem Zusammenhang auf einen einwilligungsbasierten Ansatz zurückzuziehen (und diesem Ziel dienen PIMS), sorgt lediglich dafür, dass Tracking-Verfahren praktisch möglich bleiben, die andernfalls durch diese Gatekeeper unterbunden würden. Das ohne Zweifel vorhandene Problem marktbeherrschender Browser wie Chrome, Safari, Edge oder

---

[8] In diesem Kontext zu kurz greift daher die primär auf (informationelle) Selbstbestimmung abstellende Empfehlung der Datenethikkommission, vgl. Gutachten der Datenethikkommission, S. 133.

[9] Stellungnahme des Zentralverbandes der deutschen Werbewirtschaft vom 20.01.2021, S. 7, online abrufbar unter https://www.bmwi.de/Redaktion/DE/Downloads/Stellungnahmen/Stellungnahmen-TTDSG/zaw.pdf (abgerufen am 20.04.2021).

[10] Vgl. etwa das mit Safari 13.1 eingeführte, aggressive Blocken von Third-Party-Cookies. Dazu https://www.heise.de/mac-and-i/meldung/Apple-Browser-Safari-blockiert-saemtliche-Third-Party-Cookies-4690467.html (abgerufen am 19.04.2021).

Firefox ist nicht, dass diese einzelne Verfahren technisch verhindern. Das Problem ist, dass sie dies eigenmächtig ohne gesellschaftliche Debatte darüber tun, welche technischen Verfahren bei der Monetarisierung digitaler Angebote (noch) als gesellschaftsverträglich anzusehen sind. Gerade diese Frage muss aber Kerngegenstand jeder Regulierung von Telemedien sein. Die Einwilligung entzieht sich dem und wälzt die Beantwortung dieser Frage auf eine als Selbstbestimmung getarnte Überforderung der Nutzenden ab.[11]

Die mangelnde Eignung der datenschutzrechtlichen Einwilligung als Regulierungsansatz – und damit zwangsläufig auch die Verzichtbarkeit eine Regulierung von PIMS – zeigt sich sodann auch in der Diskussion rund um das Kopplungsverbot. Telemedienanbietende sind seit Geltungsbeginn der DSGVO verbreitet dazu übergegangen, die Einwilligung in Tracking-Verfahren zur Bedingung für den „kostenlosen" Zugang zu Inhalten zu machen. Trackingfreier Zugang hingegen wird an finanzielle Kompensation gekoppelt.[12] Gegen derartige Praktiken bietet die DSGVO keine Handhabe.[13] Im Ergebnis führt dies u.a. dazu, dass einkommensschwache Bevölkerungsgruppen tendenziell eher zur Abgabe von Einwilligungen bewogen werden, was wiederum zur Folge hat, dass die für die Auslieferung personalisierter Inhalte eingesetzten (Analyse-) Verfahren auch vorrangig anhand dieser Bevölkerungsanteile „trainiert" werden. Dies bringt das Risiko mit sich, dass technische Verfahren nicht erwünschte gesellschaftliche Ungleichheit abbilden und zusätzlich verfestigen. Ein PIMS-gestützter, rein einwilligungsbasierter Ansatz hat auf diese Herausforderung keine Antwort.

Die Umsetzung des Art. 5 Abs. 3 ePrivacy-Richtlinie lässt freilich derzeit keinen Raum für eine anderweitige Regulierung des Zugriffs auf Informationen auf den Endgeräten der Nutzenden. Vor diesem Hintergrund wäre eine Kritik an dem geplanten § 24 TTDSG-E also verfehlt. Dass die Bundesregierung darüber hinaus davon absah, einer einwilligungsbasierten Regulierung durch die Normierung von PIMS weiteren Vorschub zu leisten, ist indes ausdrücklich zu begrüßen.

---

[11] Kritisch ebenso *Veil*, NVwZ 2018, 686, 688 („Utopie der Selbstbestimmung") sowie *Katko/Babaei-Beigi*, MMR 2014, 360, 363 („formalisiertes Ritual").

[12] Zur Diskussion um die Zulässigkeit derartiger „Cookie-Walls" siehe etwa *Rauer/Ettig*, ZD 2021, 18, 22, mit weiteren Nachweisen.

[13] Ausführlich *Engeler*, ZD 2018, 55; enger *Golland* MMR 2018, 130; siehe auch *Schätzle*, PinG 2017, 203.

II. Zur Regulierung verbindlicher Voreinstellungen

Der Entwurf des TTDSG verzichtet ebenfalls darauf, technische Verfahren wie „Do-Not-Track" und eine Befolgungspflicht des darin ausgedrückten Willens von Nutzenden aufzugreifen. Auch dies ist letztlich zu begrüßen.

Das verbindliche Setzen von Voreinstellungen in Browsern löst die unter I. diskutierten Herausforderungen nur dann, wenn die zentral erklärte Ablehnung von Tracking-Verfahren dauerhaft im Sinne eines „Do-Not-Ask" verpflichtend durch Browser und Apps zu berücksichtigen wäre. Dies liefe im Wesentlichen auf eine Abstimmung aller Telemedien-Nutzenden über die Akzeptanz von Tracking als Monetarisierungsmodell via Mausklick im Browser hinaus. Ein derartiges „Verbot von Tracking-Verfahren" durch die Hintertür entbehrt angesichts seiner Konsequenz nicht eines gewissen Charmes, könnte sich aber als einseitige Lösung zu Lasten gering-invasiver Tracking-Verfahren und berechtigter Monetarisierungswünsche von Telemedienanbietenden erweisen.

Würde man die Verbindlichkeit derartiger Voreinstellungen hingegen unter den Vorbehalt eines Zeitablaufs oder einer Zustimmung im Einzelfall stellen, liefe dies darauf hinaus, dass die derzeitigen Cookie/Consent-Banner abgelöst würden durch „Do-Not-Track-Override"-Banner, die um Erlaubnis bitten, die gesetzte Voreinstellung überschreiben zu dürfen. Für Dialogboxen-müde Nutzende wäre damit nichts gewonnen.

Hinsichtlich der auch bzgl. verbindlicher Voreinstellungen bestehenden Zweifel an der Vereinbarkeit mit den Anforderungen der DSGVO an wirksame Einwilligungserklärungen sei im Übrigen auf die Literatur verwiesen.[14]

III. Zur „Erforderlichkeit" i.S.d. § 24 Abs. 2 Nr. 2 TTDSG-E

Mit § 24 TTDSG-E wird Art. 5 Abs. 3 ePrivacy-Richtlinie praktisch deckungsgleich in deutsches Recht überführt. Der Entwurf beseitigt damit die nicht erst seit der Planet49-Entscheidung des EuGH offensichtliche Lücke im deutschen Telemedienrecht.

Mit seiner eng an der Richtlinie orientierten Umsetzung trägt § 24 TTDSG-E aber auch die Debatte um die Abgrenzung zwischen Einwilligungserfordernis und einwilligungsfreiem Zugriff auf Informationen auf den Endgeräten in das deutsche Recht hinein. In § 24 Abs. 2 Nr. 2 TTDSG-E wird die Privilegierung des Art. 5 Abs. 3 Satz 2 Alt. 2 ePrivacy-Richtlinie umgesetzt und die Speicherung von Informationen in der Endeinrichtung der Endnutzenden oder der Zugriff auf bereits in der Endeinrichtung gespeicherte

[14] Siehe Fußnote 6.

Informationen für zulässig erklärt, wenn dies unbedingt erforderlich ist, damit Anbietende von Telemediendiensten einen von Nutzenden ausdrücklich gewünschten Telemediendienst zur Verfügung stellen können.

Diese Umsetzung ist grundsätzlich nicht zu kritisieren, die Richtlinie eröffnet insofern wenig Spielraum. Nichtsdestotrotz wäre es in diesem Zusammenhang wünschenswert gewesen, Regelbeispiele von „unbedingt erforderlichen" Zugriffen in die deutsche Umsetzung mit aufzunehmen. Dies zeigt sich insbesondere am Beispiel minimalinvasiver, First-Party-Cookies basierter Reichweitenanalysedienste, wie sie etwa Anbietende wie Matomo (ehemals Piwik) anbieten. Diese Verfahren waren je nach technischer Ausgestaltung zuvor auch nach Auffassung der Datenschutzaufsichtsbehörden ohne Einwilligung auf Basis einer Interessenabwägung zulässig.[15] Der Regulierungsansatz des Art. 5 Abs. 3 ePrivacy-Richtlinie kennt hingegen kaum Grauzonen und könnte auch derartige „unkritische" Verfahren zukünftig unter Einwilligungsvorbehalt stellen. Dies hätte nachteilige Folgen für entsprechende datenschutzsparsame Verfahren, für die Verantwortliche nunmehr den gleichen datenschutzrechtlichen Aufwand betreiben müssten, wie für potentiell mächtigere – aber problematische – Tools wie Google Universal Analytics. Der Verzicht auf gewisse Analysefähigkeiten wurde bisher aufgrund der abgesenkten datenschutzrechtlichen Anforderungen aber durch echte Vorteile aufgewogen. § 24 Abs. 2 Nr. 2 TTDSG-E schafft diesen wesentlichen Anreiz für datensparsame Reichweitenanalysetools nun – gezwungenermaßen – ab.[16]

Auch die Normierung derartiger Regelbeispiele würde zwar unweigerlich Bedenken hinsichtlich ihrer Europarechtswidrigkeit ausgesetzt sein. Ihrer Notwendigkeit tut das freilich wenig Abbruch, allein um Bestrebungen entgegen zu treten, den Begriff der Erforderlichkeit sehr weitgehend im Sinne einer wirtschaftlichen Nützlichkeit[17] auszulegen.

---

[15] Art. 29-Datenschutzgruppe, Stellungnahme 04/2012, angenommen am 07.06.2012, S. 11, 12, online abrufbar unter: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/wp194_de.pdf (abgerufen am 20.04.2021); Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, März 2019, S. 17, online abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf (abgerufen zu viel zu später Stunde am 19.04.2021).

[16] Dazu bereits *Engeler*, PinG 2018, 141, 146, mit Verweis auf *Schleipfer*, ZD 2017, 460, 465.

[17] So etwa Hanloser, ZD 2021, 121.

IV. Zur Normierung von Gestaltungspflichten von Einwilligungserklärungen

Zuletzt verzichtet der Entwurf auch auf Regelungen, die das Problem von Dark Patterns adressieren. Durch missbräuchliches Design von Einwilligungserklärungen werden Nutzende zur Abgabe einer Erklärung motiviert, die Zweifel an der Wirksamkeit der Einwilligung aufkommen lassen, sei es durch täuschende, unnötig komplizierte oder nicht barrierefreie Gestaltung.[18]

Auch dieser Verzicht erscheint letztlich aber konsequent. Verpflichtende Vorgaben für die Gestaltung von Einwilligungserklärungen ergeben nur im Kontext einer einwilligungsbasierten Regulierung Sinn und adressieren die dargestellten Herausforderungen damit nicht im Kern. Sie laufen zudem ihrerseits Gefahr, den Maßstab wirksamer Einwilligungen der DSGVO zu modifizieren, was die bereits mehrfach angesprochenen europarechtlichen Bedenken nach sich zieht.

Es erscheint daher sachgerecht, bezüglich Dark Patterns weiter auf die konkretisierende Rechtsprechung und Aufsichtspraxis zur Frage der Gestaltung wirksamer Einwilligungserklärung im Bereich von Telemedien zu setzen. Die Entscheidung des EuGH in Sachen Planet49 ist ein Beispiel dafür.

V. Ansatzpunkte für die Trilog-Gespräche im Kontext der geplanten ePrivacy-Verordnung

Die angesprochenen Nachteile der Umsetzung des Art. 5 Abs. 3 ePrivacy-Richtlinie offenbaren diverse Ansatzpunkte für die derzeit laufenden Trilog Gespräche um die kommende ePrivacy-Verordnung.[19] Allem voran soll im Rahmen dieser Stellungnahme für eine weitgehende Abkehr von einer einwilligungsfokussierten Regulierung geworben werden.

Für alltäglich unzählige Datenverarbeitungsvorgänge wie den Zugriff auf Telemedien ist die Einwilligung kein tauglicher Regelungsansatz. Erforderlich ist stattdessen eine gesetzgeberische Positionierung zu der Frage, in welchem Umfang Datenverarbeitung zu

---

[18] Zur Definition und rechtlichen Einordnung *Weinzierl*, NVwZ 2020, 1087, mit weiteren Nachweisen.

[19] Zum Kommissionsentwurf aus Perspektive der aufsichtsbehördlichen Praxis *Engeler/Felber*, ZD 2017, 251; zum Parlamentsentwurf *Engeler*, ZD 2017, 549; zur Ratsfassung *Engeler*, PinG 2018, Heft 4, 141.

Zwecken der bedarfsgerechten Gestaltung und Monetarisierung von Telemedien einwilligungsfrei zulässig sind unter gleichzeitiger Untersagung weitergehender Verfahren.

Eine „harte Regulierung" in diesem Sinne würde nicht nur das Problem der Einwilligungsmüdigkeit adressieren (sie würde Consent-Banner oder DNT-Override-Banner entbehrlich machen), sondern auch verhindern, dass die Erteilung von entsprechenden Einwilligungen aufgrund ungleicher Verteilung von Wohlstand zu einem Phänomen einkommensschwacher Bevölkerungsteile wird. Andererseits könnte so aber auch ein akzeptabler Umfang des einwilligungsfreien Einsatzes von Technologien zur Auslieferung von personalisierten Inhalten definiert werden, um ein Mindestmaß an wirtschaftlicher Bewegungsfreiheit von Telemedienanbietenden zu gewährleisten.

VI. Abschließende Kurzbemerkungen

1. Zu möglichen Kompetenzfragen im Vollzug

Die ePrivacy-Richtlinie geht in Art. 5 Abs. 3 in ihrem Anwendungsbereich über die Regulierung der Verarbeitung von personenbezogenen Daten hinaus und erfasst jedweden Zugriff auf Informationen bzw. Abspeichern von Informationen – unabhängig davon, ob sich daraus ein Eingriff in Persönlichkeitsrechte oder des Rechts auf Schutz personenbezogener Daten ergibt. Damit schützt Art. 5 Abs. 3 ePrivacy-Richtlinie ein separates Schutzgut, das sich nicht ohne Weiteres erschließt.[20]

Dies ist insofern relevant, als dass viele Landesdatenschutzgesetze die Zuständigkeiten der Landesdatenschutzaufsichtsbehörden dahingehend beschreiben, dass diese als Aufsichtsbehörden im Sinne des Art. 51 Abs. 1 DSGVO die Einhaltung der DSGVO und darüber hinaus die Regelungen der jeweiligen Landesdatenschutzgesetze überwachen. Die Landesdatenschutzgesetze hingegen beschränken ihren Anwendungsbereich ihrerseits vielfach auf die Verarbeitung personenbezogener Daten. Auch § 113 Satz 1 MStV spricht von „Datenschutzgesetzen". Damit stellt sich die Frage, welche Aufsichtsbehörde für den „Datenschutz-überschießenden Teil" des § 24 TTDSG-E zuständig sein wird. Um hierzu unnötige Kompetenzfragen zu vermeiden, sollte der Versuch einer gesetzlichen Klarstellung erwogen werden.

2. Zur Pflicht der Ermöglichung einer anonymen Nutzung

Abschließend ist zu begrüßen, dass der Entwurf in § 19 Abs. 2 TTDSG-E unverändert daran festhält, Telemedienanbietende (im Rahmen des Zumutbaren) dazu zu verpflichten, eine

[20] Ausführlich *Engeler/Marosi*, Computer & Recht 2019, 707, 709.

anonyme Nutzbarkeit zu ermöglichen. In der Literatur ist dazu vereinzelt argumentiert worden, dass eine Anonymität im Sinne des Datenschutzrechts mit Blick auf die Vielzahl an identifizierenden (Meta-) Daten im Internetverkehr ohnehin praktisch unmöglich sei,[21] so dass diese Verpflichtung zu streichen sei.

Dies darf einerseits bereits technisch in Frage gestellt werden. In aller Regel ist der hohe Maßstab der Anonymität im Sinne der DSGVO zwar nur schwer erreichbar. Unter Aufwand großer Mühen, etwa unter Einbeziehung von Anonymitätstools wie dem Tor-Netzwerk, unter Nutzung von Prepaid-Kennungen oder Kommunikationsplattformen, die keine Metadaten speichern, ist Anonymität im datenschutzrechtlichen Sinne aber auch nicht gänzlich ausgeschlossen. Es sollte daher darauf verzichtet werden, hier ein Zeichen gegen derartige Technologien und Anwendungen zu setzen.

Andererseits würde es auch nicht einer gewissen Ironie entbehren, zunächst mit rechtlichen Verpflichtungen, etwa zur Erhebung von Ausweisdaten im Rahmen der Anschlussvergabe (§ 111 TKG) [22] oder zur Mitwirkung an der Speicherung von Verkehrsdaten entgegen datenschutzoptimierter Geschäftsmodelle,[23] eben jene technische Unmöglichkeit einer anonymen Nutzung im Sinne des § 19 Abs. 2 TTDSG-E überhaupt erst zu schaffen, um unter Verweis darauf die Pflicht zur Ermöglichung einer anonymen Nutzung dann mangels Anwendungsbereichs zu streichen. Auf den Wert anonymer Teilnahme an internetbasierter Kommunikation – nicht nur für journalistische Tätigkeiten – sei an dieser Stelle eindringlich hingewiesen.[24]

---

[21] Schwartmann/Benedikt/Reif, MMR 2021, 99, 101.

[22] Dazu BVerfG, Beschluss vom 24. Januar 2012 – 1 BvR 1299/05.

[23] Dazu BVerfG, Beschluss vom 20. Dezember 2018 – 2 BvR 2377/16.

[24] Siehe etwa Resolution des Human Rights Council der Vereinigten Nationen vom 26. September 2016, online abrufbar unter https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/211/94/PDF/G1621194.pdf (abgerufen am 20.04.2021.).