Deutscher Bundestag
19. Wahlperiode
Ausschuss für Wirtschaft und Energie

Ausschussdrucksache 19(9)1054
20. April 2021

Dr. Alexander Golland
Rechtsanwalt

Anschrift
Dr. Alexander Golland
c/o PricewaterhouseCoopers Legal
Moskauer Straße 19
D-40227 Düsseldorf

Kontakt
E-Mail: info@alexandergolland.de
Web: www.alexandergolland.de

Dr. Alexander Golland | PwC Legal | Moskauer Str. 19 | D-40227 Düsseldorf

An den
Deutschen Bundestag
Herrn MdB Klaus Ernst
Vorsitzender des Ausschusses für Wirtschaft und Energie
Platz der Republik 1
10117 Berlin

3. Mai 2021

Stellungnahme

Öffentliche Anhörung
des Ausschusses für Wirtschaft und Energie
am 21. April 2021 um 9.30 Uhr

Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien

BT-Drucksache 19/27441

Sachverständiger: Dr. Alexander Golland[1]

I. Zusammenfassung der Stellungnahme

Der Regierungsentwurf des TTDSG („TTDSG-RegE“) ist grundsätzlich positiv zu beurteilen. Es werden zahlreiche Rechtsunsicherheiten adressiert und insbesondere einige zentrale Gesetzeslücken geschlossen bzw. Umsetzungsdefizite behoben. Im Bereich der Telemedien, den die vorliegende Stellungnahme im Schwerpunkt behandelt, besteht jedoch auch in einigen Bereichen Optimierungsbedarf. Die Stellungnahme konzentriert sich auf Hinweise und mögliche Lösungen auf nationaler Ebene. Insofern sind folgende sechs Aspekte hervorzuheben:

[1] Diese Stellungnahme gibt lediglich die persönliche Auffassung des Verfassers wieder.

- **Anwendungsbereich:** Das Marktortprinzip ist uneindeutig formuliert und wirft Fragen zur Zuständigkeit der Aufsicht sowie dem grenzüberschreitenden Vollzug auf. Die Aufnahme des Begriffs der „Mitwirkung“ im Anwendungsbereich und in der Definition des „Anbieters von Telemedien“ führt zu einer uferlosen Erstreckung auf Akteure ohne faktische Einwirkungsmöglichkeit (einschließlich abhängig Beschäftigter). Daher sollte insbesondere das Kriterium der „Mitwirkung“ entfallen.

- **Verhältnis zur DSGVO**: Eine (z.T. geforderte) Klarstellung ist nicht geboten; eine Normierung würde keinen Mehrwert schaffen und wäre ggf. europarechtswidrig.

- **Problem der „Einwilligeritis“**: Die stärkere Anlehnung an die ePrivacy-Richtlinie ist zu begrüßen, hilft in der Praxis jedoch kaum. Im Bereich von ePrivacy hat der deutsche Gesetzgeber – anders als im Datenschutzrecht – einen nicht ausgeschöpften Umsetzungsspielraum. Der Gesetzgeber sollte die in Bezug auf funktionale Cookies allgemein anerkannten Ausnahmen vom Einwilligungserfordernis im Gesetzestext normieren, damit Rechtssicherheit geschaffen wird, unnötige Einwilligungen vermieden werden und für Nutzer der Ausnahmecharakter der Einwilligung wiederhergestellt wird. Zudem wäre eine interessengerechte Regelung zur Reichweitenmessung denkbar.
  (Ein Regelungsvorschlag ist dieser Stellungnahme als Anhang beigefügt.)

- **Gestaltung von Einwilligungen**: Die Rahmenbedingungen für die Gestaltung von Einwilligungen sind durch die Rechtsprechung hinreichend konturiert. Rechtwidrige Cookie-Banner resultieren vor allem aus einem Vollzugsdefizit. Der Gesetzgeber hat keine über ePrivacy hinausgehende Kompetenz zur Normierung von Einwilligungsmodalitäten; eine entsprechende Regelung birgt die Gefahr der Europarechtswidrigkeit. Vielmehr sollten Aufsichtsbehörden ihre Kontrolltätigkeit intensivieren; verbleibende Rechtsunsicherheiten sollten der Klärung durch die Judikative vorbehalten sein.

- **„Do Not Track“**: Solange Browserhersteller keinen Anforderungen über die Implementierung oder Interpretation von DNT unterliegen, würde eine Berücksichtigungspflicht von DNT für Diensteanbieter zu einer erheblichen Marktmachtverschiebung zugunsten transatlantischer Akteure führen. Die Normierung von an Softwarehersteller gerichteten Vorgaben wäre in diesem Gesetzgebungsverfahren jedoch verfehlt.

- **Zuständigkeit der Datenschutzaufsicht**: Die Zuständigkeit für die Aufsicht über Telemedien der Privatwirtschaft ist nicht ausdrücklich geregelt. Sämtliche drohenden Kompetenzkollisionen lassen sich zwar nicht allein auf nationaler Ebene regeln; ein klarstellender Verweis in die BDSG-Vorschriften erscheint jedoch sinnvoll.

II. Einzelne Themenkomplexe im Detail

Im Folgenden seien einige rechtliche Herausforderungen – unter besonderer Berücksichtigung der Anbieter von Telemedien – im Detail beleuchtet.

1. Anwendungsbereich: Einschränkung notwendig

Nach § 1 Abs. 3 TTDSG-RegE unterliegen dem Gesetz alle Unternehmen und Personen,[2] die im Geltungsbereich des Gesetzes eine Niederlassung haben oder Dienstleistungen erbringen oder daran mitwirken. Der Begriff des Orts des Erbringens einer Dienstleistung ist nicht eindeutig definiert und wird in den unterschiedlichen Rechtsmaterien unterschiedlich interpretiert.[3] Soweit der Ort des Erbringens der Dienstleistung – wie in Art. 3 Abs. 2 der Verordnung (EU) 679/2016 (Datenschutz-Grundverordnung – im Folgenden: „DSGVO") – im Sinne eines Marktortprinzips verstanden wird, würde dies zu einer Ausweitung auf außerdeutsche Dienstleister führen, bei der unklar ist, wie der Vollzug gegenüber diesen Dienstleistern erfolgen soll. Hierfür mangelt es zuvorderst an Mechanismen vergleichbar der Benennung eines Vertreters nach Art. 27 DSGVO. Auch die Zuständigkeitsregelungen sehen, jedenfalls im Bereich der Telemedien, keinen grenzüberschreitenden Vollzug vor. Insoweit mangelt es an Kooperations- und Kohärenzverfahren im Falle von Diensteanbietern, die ihre Angebote aus oder in mehreren Mitgliedstaaten erbringen.[4] Eine vollständige Regelung des Marktortprinzips erscheint damit nur auf europäischer Ebene realisierbar.

Zudem normiert § 1 Abs. 3 TTDSG-RegE eine Anknüpfung an das „Mitwirken" an der Erbringung von Dienstleistungen. Eine „Mitwirkung" dürfte aber auch bei Unternehmen vorliegen, die keine Möglichkeit zur Steuerung, inhaltlichen Gestaltung oder Zielrichtung des Telemediums haben (insbesondere Auftragsverarbeiter als rein technische Dienstleister, z.B. Host Provider). Das Problem verschärft sich durch die Definition des Telemediums in § 2 Abs. 2 Nr. 1 TTDSG-RegE, wonach auch eine „natürliche […] Person, die an der Erbringung mitwirkt […]" erfasst werden soll. Bei wörtlicher Lesart wären hiervon auch Beschäftigte des Diensteanbieters unmittelbare Adressaten des Gesetzes. Der Sinn einer derart weiten Definition des „Anbieters von Telemedien" erschließt sich nicht.[5] Insbesondere wäre denkbar, in § 2 Abs. 2 Nr. 1

---

2 Aus Platzgründen wird im Text verallgemeinernd das generische Maskulinum verwendet. Die verwendeten Formulierungen umfassen gleichermaßen Personen jeglichen Geschlechts und jeglicher Geschlechteridentität.

3 Z.T. hängt dies sogar von der Rechtspersönlichkeit der Beteiligten ab, vgl. nur § 3a UstG.

4 Vgl. unten B.VI.

5 Im Übrigen kann dies zu Folgeproblemen bei Bestimmung der zuständigen Aufsichtsbehörde führen, siehe unten B.VI.

TTDSG auf § 2 Satz 1 Nr. 1 TMG zu verweisen. Eine solche Erstreckung des Anwendungsbereichs bzw. eine solch weitreichende Definition sollten durch Anpassung von § 1 Abs. 3 und § 2 Abs. 2 Nr. 1 TTDSG vermieden werden.

2. Verhältnis zur DSGVO: Keine Klarstellung notwendig

Das Nebeneinander von DSGVO und nationalen datenschutzrechtlichen Vorschriften, welche eine Umsetzung der Richtlinie 2002/58/EG (im Folgenden: „ePrivacy-RL“) darstellen, ist komplex und nicht abschließend geklärt. Begrüßenswert ist, dass der Regierungsentwurf durch Aufhebung des Abschnitts 5 des TMG einige dieser Rechtsunsicherheiten beseitigt. Einzelne Unsicherheiten, insbesondere der Art. 5 Abs. 3 ePrivacy-RL umsetzende § 24 TTDSG-RegE, bleiben jedoch. Aufsichtsbehörden und Teile der Literatur gehen davon aus, dass in den Bereichen der Umsetzung von Art. 5 Abs. ePrivacy-RL eine Anwendung der allgemeinen Zulässigkeitstatbestände der DSGVO unterbleibt.[6] Zum Teil wird jedoch auch in den überschneidenden Bereichen eine kumulative Anwendbarkeit beider Regelungskataloge vertreten.[7] Der Bundesgerichtshof ließ die Frage offen.[8]

Eine zum Teil geforderte Klarstellung dieses Verhältnisses im TTDSG birgt für den Rechtsanwender jedoch nur vordergründig Sicherheit: Soweit der deutsche Gesetzgeber eine solche Klarstellung vornähme, ungeachtet ihrer Ausgestaltung, wäre diese Vorschrift entweder rein deklaratorischer Natur oder aber europarechtswidrig und damit nach dem Grundsatz Lex superior derogat legi inferiori nicht anzuwenden. Die Praxisrelevanz dieser Frage ist gleichwohl gering,[9] da bei Einhaltung der Vorgaben des § 24 TTDSG-RegE, soweit im Zuge dessen personenbezogene Daten verarbeitet werden, stets auch ein Zulässigkeitstatbestand des Art. 6 Abs. 1 DSGVO vorläge. Vor diesem Hintergrund sollte von einer Klarstellung abgesehen werden.

3. Problem der „Einwilligeritis“: Gesetzliche Klarstellung geboten

Zunächst ist begrüßenswert, dass mit § 24 TTDSG-RegE eine Norm geschaffen wurde, die sich stark an den Vorgaben von Art. 5 Abs. 3 ePrivacy-RL orientiert und als europarechtskonforme Umsetzung der Norm betrachtet werden kann. Positiv ist zudem

---

6 *Europäischer Datenschutzausschuss*, Stellungnahme 5/2019 zum Zusammenspiel zwischen der e-Datenschutz-Richtlinie und der DSGVO, Rn. 40; *Golland*, in: Taeger/Gabel, DSGVO/BDSG, 3. Aufl. 2019, Art. 95 Rn. 9 ff.; wohl auch *Heun/Assion,* in: Auernhammer, DSGVO/BDSG, 7. Aufl. 2020, Art. 95 Rn. 34 f.; explizit zum Zusammenspiel von § 15 Abs. 3 TMG und Art. 6 ff. DSGVO *Gierschmann,* MMR 2020, 614 (615); *Golland,* in: Taeger/Gabel, DSGVO/BDSG, 4. Aufl. 2021, Art. 95 Rn. 23 (im Erscheinen).

7 *Benedikt*, DSB 2021, 76 (79); *Ettig/Herbrich,* K&R 2020, 719 (720); *Rauer/Ettig,* ZD 2021, 18 (20).

8 BGH, Urt. v. 28.05.2020 – I ZR 7/16 („Cookie Einwilligung II“), hier insbesondere Rz. 58-62.

9 So auch *Ettig/Herbrich,* K&R 2020, 719 (720); *Rauer/Ettig,* ZD 2021, 18 (20).

hervorzuheben, dass der Wortlaut von § 24 TTDSG-RegE den – bislang in Deutschland nicht regulierten – Bereich des Einsatzes nicht-personenbezogener Cookies und ähnlicher Technologien erfasst. Die Frage wird häufig auf den Hauptanwendungsfall der Cookies verengt, stellt sich aber ebenso für sämtliche anderen Technologien, bei denen eine Speicherung von Informationen in der Endeinrichtung des Endnutzers erfolgt oder ein Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, stattfindet.

Der Stellungnahme des Bundesrats ist dabei zuzustimmen, dass die Nutzung des Internets beschwerlicher geworden ist. Dieses Problem manifestiert sich sowohl auf Seiten der Nutzer als auch auf Seiten der Rechtsanwender. In der Umsetzung des derzeitigen § 15 Abs. 3 TMG, der in der Interpretation des Bundesgerichtshofs dem Art. 5 Abs. 3 ePrivacy-RL entsprechen soll,[10] stellen sich für zahlreiche Unternehmen Fragen, welche Cookies ohne Einholung einer Einwilligung des Nutzers verwendet werden können. Vielfach führt dies dazu, dass eine Einwilligung „sicherheitshalber" eingeholt wird, obwohl keine Einwilligung erforderlich ist. Diese Rechtsunsicherheiten können – teilweise – durch eine Konkretisierung von § 24 TTDSG-RegE ausgeglichen werden.

Während technisch erforderliche Cookies (z.B. Load-Balancing-Cookies, sodass das Telemedium überhaupt störungsfrei ausgeliefert werden kann) nach § 24 Abs. 2 Nr. 1 TTDSG-RegE eindeutig keiner Einwilligung bedürfen,[11] ebenso reine Marketing-Cookies wohl unstreitig eine solche Einwilligung voraussetzen,[12] stellt sich weiterhin – insbesondere hinsichtlich sogenannter „funktionaler Cookies" – die Frage, was die Anforderungen an einen „vom Nutzer ausdrücklich gewünschten Telemediendienst" i.S.d. § 24 Abs. 2 Nr. 2 TTDSG-RegE sind. Insoweit ist von den Aufsichtsbehörden anerkannt, dass unter diese Ausnahme Cookies fallen, die erforderlich sind, um dem Nutzer eine bestimmte Funktion zur Verfügung zu stellen und die der Nutzer des Diensts ausdrücklich angefordert hat.[13]

---

10 BGH, Urt. v. 28.05.2020 – I ZR 7/16 („Cookie Einwilligung II").

11 *Artikel-29-Gruppe,* WP 194, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, S. 6.

12 U.a. *Moos,* MMR 2019, 732, 737; *Moos/Strassemeyer,* DSB 2020, 207, 209; *Rauer/Ettig*, ZD 2021, 18, 20.

13 Zu Art. 5 Abs. 3 Satz 2 ePrivacy-RL: *Artikel-29-Gruppe,* WP 194, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, S. 4.

Von den Aufsichtsbehörden anerkannte Fallgruppen[14] sind u.a.:

- Authentifizierungscookies: seitenübergreifende Identifikation des Nutzers, sodass sich dieser nicht auf jeder einzelnen Seite desselben Telemediums erneut einloggen muss;
- User-Input-Cookies: temporäres Speichern von Eingaben in mehrseitigen Formularen oder zum Speichern eines Warenkorbes beim Online-Einkauf;
- Nutzerorientierte Sicherheitscookies: Cookies, um wiederholt fehlgeschlagene Anmeldeversuche zu erkennen und so den Nutzer vor Identitätsdiebstahl zu schützen,
- Cookies zur Anpassung der Benutzeroberfläche: Speicherung der vom Nutzer vorgenommenen Einstellungen des Telemediums, z.B. Anzeigeformat, Design oder Sprache;
- Multimedia-Player-Cookies: Cookies zur Wiedergabe von nutzerseitig angeforderten Audio- oder Videoinhalten.[15]

In der Praxis werden allerdings auch in diesen Fällen häufig Einwilligungen eingeholt, obwohl diese nicht erforderlich sind. Damit geht jedoch die mit der Einwilligung einhergehende Warnfunktion verloren, die dem Nutzer anzeigt, dass gerade eine Disposition über die informationelle Integrität seines Endgeräts erfolgt. Die Einwilligung wird zunehmend eine Belastung für Nutzer, etwaige Fenster werden gedankenlos „weggeklickt".

Um Rechtssicherheit zu schaffen und die Funktion der Einwilligung wiederherzustellen, sollten in § 24 Abs. 2 Nr. 2 TTDSG die Ausnahmen vom Einwilligungserfordernis klar benannt werden. Die Zahl unnötig eingeholter Einwilligungen und die mit ihrer Erteilung verbundenen Unannehmlichkeiten für die Nutzer dürften hierdurch drastisch reduziert werden.

Daneben bestehen auf Seiten der Unternehmen jedoch weitere Bedürfnisse, wovon zwei Fallgruppen hervorzuheben sind:

- Dienstorientierte Sicherheitscookies: Cookies, die allein der Sicherheit des Diensts bzw. Diensteanbieters dienen (z.B. zur Betrugsprävention);

---

14 *Artikel-29-Gruppe,* WP 194, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, S. 7 ff.

15 So auch LG Köln, Beschl. v. 29.10.2020 – 31 O 194/20.

- Cookies zur Reichweitenmessung: Cookies, die Statistiken über die Reichweite des Telemediums ermöglichen und z.B. für die Abrechnung gegenüber Werbetreibenden erforderlich und somit für kostenlose Dienste essenziell sind.

Dienstorientierte Sicherheitscookies können – soweit sie nicht der technischen Aufrechterhaltung des Diensts dienen – bei Zugrundelegung der strengen Kriterien der *Art.-29-Gruppe*[16] nicht als „technisch notwendig" i.S.d. Art. 5 Abs. 3 Satz 2 Alt. 1 ePrivacy-RL bzw. § 24 Abs. 2 Nr. 1 TTDSG-RegE interpretiert werden. Der Sinn eines Einwilligungserfordernisses erschließt sich jedoch nicht, da maliziös agierende Personen die Erteilung einer solchen Einwilligung ohnehin verweigern würden.

Cookies zur Reichweitenmessung sind häufig nötig, um Provisionen gegenüber Werbenetzwerken oder direkt gegenüber Werbetreibenden abzurechnen. Dieses Vorgehen ist zwar wirtschaftlich erforderlich, um den Dienst kostenlos zur Verfügung zu stellen, eine solche Abrechnung ist aber typischerweise nicht durch den Nutzer „ausdrücklich gewünscht" i.S.d. Art. 5 Abs. 3 Satz 2 ePrivacy-RL bzw. § 24 Abs. 2 Nr. 2 TTDSG-RegE.[17] Die Folge davon ist, dass Diensteanbieter gezwungen sind, eine Einwilligung einzuholen oder das angebotene Telemedium anderweitig zu finanzieren.

Letztere Fallgruppe, die zahlreiche Dienste der Digitalwirtschaft betrifft, ist eng verknüpft mit der Frage des in Art. 7 Abs. 4 DSGVO kodifizierten Kopplungsverbots, der durch den Pauschalverweis in § 24 Abs. 1 Satz 2 TTDSG-RegE Anwendung findet. In Fällen, in denen die Nutzung des Dienstes von der Erteilung der Einwilligung abhängig gemacht wird, gilt eine Einwilligung als unfreiwillig und wäre unwirksam; der Cookie-Einsatz wäre rechtswidrig. Daher wird auch die Errichtung sogenannter „Cookie-Walls" ohne Alternativen zur Inanspruchnahme des Diensts für unzulässig gehalten.[18] Würde der Diensteanbieter die Einwilligung dagegen einholen, ohne die Nutzung des Dienstes von der Erteilung der Einwilligung abhängig zu machen, hätte der Nutzer keinen Grund, seine Einwilligung zu erteilen.[19] Ein profitabler Betrieb ist dann nur möglich, wenn der Diensteanbieter einen entgeltlichen Alternativzugang einrichtet, bei dem der Nutzer die freie Wahl zwischen dienstseitig benötigten Cookies und Bezahlung hat („Pay or Okay"). Zugleich wird der Nutzer vor sozialpolitisch

---

16 Siehe *Artikel-29-Gruppe,* WP 194, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, S. 3.

17 Für eine weite Interpretation des § 24 Abs. 2 Nr. 2 TTDSG-RegE hingegen *Hanloser,* ZD 2021, 121.

18 *Europäischer Datenschutzausschuss*, Erklärung des Europäischen Datenschutzausschusses zur Überarbeitung der ePrivacy-Verordnung und zu den Auswirkungen auf den Schutz der Privatsphäre von Personen im Hinblick auf die Geheimhaltung und die Vertraulichkeit ihrer Kommunikation, S. 3.

19 Ausführlich *Golland*, MMR 2018, 130 (133 f.); siehe auch *Brinkmann*, in: BeckOGK/BGB, Stand: 15.3.2021, § 307 Datenschutzklausel Rz. 73; *Golland*, in: Ochs/Friedewald/Hess/Lamla, Die Zukunft der Datenökonomie, 2019, S. 54 f.; in diese Richtung ebenso *Krohm/Müller-Peltzer*, ZD 2017, 551 (554).

unerwünschter Preisgestaltung geschützt, da ein Forcieren der Einwilligung durch überhöhte Preise ebenfalls die Freiwilligkeit ausschließt.[20] Insoweit ermöglicht die derzeitige Rechtslage unter Einhaltung der maßgeblichen datenschutzrechtlichen Vorschriften die Freiwilligkeit der Entscheidung und die Datensouveränität auf Nutzerseite bei gleichzeitiger Berücksichtigung des wirtschaftlichen Betriebs des Telemediums. Dies geht jedoch mit einer erhöhten Notwendigkeit zur Einholung einer Einwilligung einher.

Sofern – wie vom Bundesrat angedeutet[21] – auch in diesen Fällen ein Kompromiss zwischen Wirtschaftlichkeit des Angebots, kostenfreier Inanspruchnahme und Verzicht auf Einwilligung herbeigeführt werden soll, stellt sich die Frage, ob dies de lege ferenda auf nationaler Ebene erfolgen kann oder auf europäischer Ebene erfolgen muss. Die französische Aufsichtsbehörde *CNIL* sowie i.E. auch die italienische Aufsichtsbehörde *GPDP* sind der Auffassung, dass auch Cookies zur Reichweitenmessung ohne Einholung der Einwilligung bereits unter Geltung von Art. 5 Abs. 3 ePrivacy-RL unter bestimmten Voraussetzungen möglich sind.[22] Zentrale Voraussetzungen sind nach Auffassung der französischen Aufsicht, dass die Cookies ausschließlich für den Zweck der Reichweitenmessung und Segmentierung des Publikums in Kohorten eingesetzt werden, keine telemedienübergreifende Erfassung stattfindet, die Cookies ausschließlich durch den Diensteanbieter oder seine weisungsgebundenen Auftragsverarbeiter gesetzt/ausgelesen werden, der Nutzer eine Widerspruchsmöglichkeit hat, und dass die erhobenen Daten, soweit und solange sie personenbezogen sind, nicht mit anderen Daten zusammengeführt oder an Dritte weitergegeben werden.[23]

Eine solche Privilegierung sogenannter „First-Party Data“ würde dazu beitragen, die Zahl der Einwilligungen, die für minimalinvasive Cookies eingeholt werden, zu reduzieren und der Einwilligung wieder ihre ursprüngliche Signal- und Warnfunktion zukommen zu lassen. Auch die Vorschläge der Kommission zur ePrivacy-Verordnung,[24] des Parlaments zur ePrivacy-Verordnung[25] und zuletzt des Rats,[26] in der ePrivacy-

---

20 *Brinkmann*, in: BeckOGK/BGB, Stand: 15.3.2021, § 307 Datenschutzklausel Rn. 74; *Golland*, MMR 2018, 130 (134 f.); *Golland,* CR 2020, 186 (190). Auch die österreichische Aufsichtsbehörde *DSB* ließ ein entsprechendes Angebot von „DerStandard.at“ nur deshalb zu, weil das erhobene Entgelt „nicht unverhältnismäßig teuer“ war.

21 BT-Drucks. 19/28396, S. 3.

22 *CNIL*, Délibération n° 2019-093, 4.7.2019, Art. 5; *GPDP,* Cookie e privacy: dalla parte degli utenti, abrufbar unter https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/4020961 (zuletzt abgerufen: 18.04.2021).

23 *CNIL*, Délibération n° 2019-093, 4.7.2019, Art. 5.

24 Art. 8 Abs. 1 lit. d ePrivacy-VO-E-KOM, siehe COM(2017) 10 final vom 10.1.2017.

25 Art. 8 Abs. 2 lit. ba ePrivacy-VO-E-EP, siehe den Bericht A8-0324/2017, angenommen am 26.10.2017.

26 Art. 8 Abs. 1 lit. d ePrivacy-VO-E-Rat, siehe Ratsdokument Nr. 6087/21 vom 10.2.2021.

Verordnung die Reichweitenmessung zu erlauben, gehen sämtlich in diese Richtung, berücksichtigen allerdings die Nutzerinteressen am Schutz der informationellen Integrität ihrer Endgeräte in unterschiedlichem Maße.

Rechtstechnisch ließe sich diese Fallgruppe auf zweierlei Weise in das TTDSG integrieren. Weder die Normierung einer mutmaßlichen Einwilligung i.S.d. Art. 5 Abs. 3 Satz 1 ePrivacy-RL noch die Regelung des „unbedingt erforderlichen" i.S.d. Art. 5 Abs. 3 Satz 2 ePrivacy-RL sind per se ausgeschlossen:

Art. 5 Abs. 3 Satz 1 ePrivacy-RL verweist hinsichtlich der Einwilligung durch die Nutzer über Art. 2 Satz 2 lit. f ePrivacy-RL auf die Richtlinie 95/46/EG – d.h. auf die Einwilligungsnormen der DSGVO.[27] Die DSGVO lässt jedenfalls konkludente Einwilligungen zu.[28] Nach der ePrivacy-RL selbst soll genügen, dass der Nutzer irgendeine Tätigkeit durchführt, die zur Speicherung bzw. zum Auslesen von Informationen in Endeinrichtungen des Nutzers führt, und dieser in Kenntnis dieser Umstände das Recht auf Ablehnung nicht ausübt („Einräumung des Rechts auf Ablehnung", engl.: „right to refuse").[29] Eine weitere Präzisierung existiert allerdings in dem die Mitgliedstaaten bindenden Normtext nicht. Nach der Rechtsprechung des Europäischen Gerichtshofs setzt allerdings auch die „ePrivacy-Einwilligung" ein aktives Element voraus; reine Untätigkeit des Nutzers soll – sowohl unter der ePrivacy-RL als auch unter der DSGVO – nicht genügen.[30] Es erschiene es also vertretbar, zwischen einer „ePrivacy-Einwilligung" und einer „DSGVO-Einwilligung" zu differenzieren, d.h. im Rahmen der Umsetzungsspielräume, die den Mitgliedstaaten bei unionsrechtlichen Richtlinien grundsätzlich zustehen, eine Einwilligung in Abweichung von der Richtlinie 95/46/EG bzw. der DSGVO zuzulassen, solange das Kernkonzept der Einwilligung nicht berührt wird (also u.a. das Erfordernis einer Nutzeraktivität vorliegt). Ein solcher Vorschlag mag an den derzeit geltenden § 15 Abs. 3 TMG erinnern, den der Bundesgerichtshof europarechtskonform auslegte.[31] Insofern ist zu betonen, dass der Bundesgerichtshof im Verfahren „Planet 49" dem Europäische Gerichtshof die Frage, ob § 15 Abs. 3 TMG europarechtskonform ist, nicht zur Vorabentscheidung vorlegte, sondern sich das vorlegende Gericht

---

27 Verweise auf die Richtlinie 95/46/EG gelten gemäß Art. 94 Abs. 2 DSGVO als Verweise auf die DSGVO.

28 Erwägungsgrund 32 Satz 2 der DSGVO.

29 Erwägungsgrund 66 Satz 3 und 4 der Richtlinie 2009/136/EG (sog. „Cookie-Richtlinie", welche die ePrivacy-RL änderte).

30 EuGH, Urt. v. 1.10.2019 – C-673/17 („Planet 49"), Rz. 52 ff.

31 BGH, Urt. v. 28.5.2020 – I ZR 7/16 („Cookie-Einwilligung II"), hier insbesondere Rz.

unabhängig von den Umsetzungsspielräumen des nationalen Gesetzgebers allein nach der Auslegung des europäischen Sekundärrechts erkundigte.[32]

Näher an den Entwürfen der ePrivacy-VO wäre die mitgliedstaatliche Ausgestaltung des Begriffs des „unbedingt Erforderlichen“ (vgl. Art. 5 Abs. 3 Satz 2 ePrivacy-RL). Die ePrivacy-RL enthält zwar die Vorgabe, dass die Speicherung von Informationen im Endgerät des Nutzers bzw. der Zugriff auf die im Endgerät des Nutzers gespeicherten Informationen „unbedingt erforderlich“ sein muss, aber keine Maßgabe, was die Bemessungskriterien des „unbedingt erforderlichen“ sind. In der bereits aus dem Jahre 2012 stammenden Stellungnahme der europäischen Aufsichtsbehörden wurde dieser Terminus noch eng ausgelegt.[33] Dennoch war bereits zu dieser Zeit der minimalinvasive Charakter von First-Party-Analysen unter den europäischen Aufsichtsbehörden anerkannt, sofern ausreichende Datenschutzgarantien[34] vorhanden sind.[35] Dass die Aufsichtsbehörden inzwischen das Begriffspaar weiter interpretieren, zeigen u.a. die bereits erwähnten Vorgaben für einwilligungsfreie Reichweitenmessung in Frankreich. Auch unter den deutschen Aufsichtsbehörden scheint es Konsens zu sein, unter eng definierten Kriterien Reichweitenmessung ohne Einwilligung, aber mit Widerspruchsmöglichkeit des Nutzers zuzulassen.[36] Ein Vorschlag, der im TTDSG die absehbaren Entwicklungen in der europäischen ePrivacy-Gesetzgebung vorwegnimmt und dabei die Kriterien der europäischen Aufsichtsbehörden berücksichtigt, dürfte von größerer Akzeptanz getragen sein und könnte als „Brücke“ bis zur Geltung der künftigen ePrivacy-VO fungieren.

Zusammenfassend lässt sich konstatieren, dass eine Konkretisierung des § 24 Abs. 2 Nr. 2 TTDSG-RegE für Nutzer und Wirtschaft gleichermaßen hilfreich wäre und daher Regelbeispiele in den Normtext aufgenommen werden sollte. Ferner könnte eine Regelung ergänzt werden, die unter gesetzlich klar definierten Maßgaben zum Schutz der Nutzer eine begrenzte Reichweitenmessung durch Anbieter von Telemedien

---

32 BGH, Beschl. v. 5.10.2017 – I ZR 7/16.

33 *Artikel-29-Gruppe,* WP 194, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, S. 3 f., 11.

34 Hier sollen eine benutzerfreundliche Möglichkeit zur Abwahl dieser Cookies sowie hinreichende Aggregierung/Anonymisierung zählen.

35 *Artikel-29-Gruppe,* WP 194, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, S. 12.

36 *Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder*, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, S. 17: „[…] für den Nutzer vorhersehbar, dass der Verantwortliche die Reichweite seines Online-Angebots misst, etwa um das Online-Angebot bedarfsgerecht zu gestalten. Für diesen Zweck sind keine andauernde Wiedererkennung und stetig umfangreichere Profilbildung sowie keine Weitergabe von Daten an Dritte nötig. Statistische Angaben geben hinreichend Aufschluss über das allgemeine Nutzungsverhalten, sodass die Vorhaltung von individuellen Nutzungsprofilen für den Zweck Reichweitenmessung nicht erforderlich ist. Die Beeinträchtigung des Nutzers ist dann als gering zu bewerten mit der Folge, dass die Interessenabwägung zugunsten des Verantwortlichen ausfällt.“

erlaubt, mit dem Ziel, Privatsphäreschutz und Interessen der deutschen Digitalwirtschaft in Einklang zu bringen.

Ein Vorschlag für § 24 TTDSG ist dieser Stellungnahme als Anhang beigefügt. Der Vorschlag enthält auch eine Ausnahme für die Reichweitenmessung, welche sich stark an den jüngeren aufsichtsbehördlichen Leitlinien sowie an den Entwürfen der ePrivacy-VO orientiert.

4. Gestaltung von Einwilligungen: Behebung von Vollzugsdefiziten und Konkretisierung durch Rechtsprechung

Derzeit ist eine enorme Varianz von auf Websites genutzten Einwilligungsbannern festzustellen. Dies ist – teilweise – ein Resultat der im vorherigen Abschnitt dargestellten Unsicherheiten. Teilweise handelt es sich aber auch um Mechanismen, die die Nutzer davon abhalten sollen, ihre Einwilligung zu verweigern. Rechtsdogmatisch kann dies als Beeinträchtigung der Informiertheit, Bestimmtheit und/oder Freiwilligkeit der Einwilligung (Art. 4 Nr. 11 DSGVO) zu qualifizieren sein, welche die Wirksamkeit der Einwilligung ausschließt.

Die Grenzen zwischen einem datenschutzrechtlich eher unbedenklichen Nudge, der für einen verständigen Internetnutzer keine Beeinträchtigung seiner Informiertheit oder Entscheidungsfreiheit bedeutet,[37] und kritisch zu betrachtenden Dark Pattern, die darauf ausgelegt sind, die Möglichkeit der Nicht-Einwilligung vollständig zu verschleiern oder den Aufwand der Nicht-Einwilligung so hoch zu treiben, dass Nutzer aus Überforderung die Einwilligung erklären, sind bereits konturiert: So urteilte beispielsweise der Bundesgerichtshof, dass eine Einwilligungserklärung unwirksam sei, wenn die beanstandete Gestaltung der Einwilligungserklärung darauf angelegt sei, den Verbraucher mit einem aufwendigen Verfahren zur Auswahl von in einer Liste aufgeführten Partnerunternehmen zu konfrontieren, um ihn zu veranlassen, von dieser Auswahl abzusehen.[38]

Trotz dieser höchstrichterlichen Rechtsprechung werden weiterhin vergleichbare, unwirksame Einwilligungserklärungen, insbesondere im Bereich der Apps und Websites, eingeholt. Häufig sind auch Schaltflächen zum „Wegklicken“ bzw. zum „Nicht-Einwilligen“ ohne Funktion; Cookies werden unabhängig vom Nutzerverhalten

---

37 So dürfte es beispielsweise unbedeutend sein, ob der Einwilligung-Button mit der Aufschrift „Einwilligung“, „Ich willige ein“ oder „Jau, ich will!“ beschriftet ist. Rechtsanwender werden hier nach Zielpublikum differenzieren und z.B. für Telemedien, die sich an Minderjährige richten, besondere Maßstäbe anlegen müssen.

38 BGH, Urt. v. 28.5.2020 – I ZR 7/16 („Cookie-Einwilligung II“), Rz. 57.

gesetzt oder Einwilligungsbanner lassen sich – auch nachdem der Nutzer zum Ausdruck gebracht hat, nicht einwilligen zu wollen – nicht schließen. Dieses aufsichtsbehördliche Vollzugsdefizit wird jedoch nicht dadurch behoben, dass nun zusätzliche Anforderungen an die Gestaltung der Einwilligung gesetzlich normiert werden.

Hinzu kommt, dass der deutsche Gesetzgeber diese Anforderungen ausschließlich für den Geltungsbereich der ePrivacy-RL treffen könnte. Vielmehr sind die Vorschriften der Art. 4 Nr. 11, Art. 6 Abs. 1 Satz 1 lit. a, Art. 7, Art. 8, Art. 9 Abs. 2 lit. a DSGVO insoweit abschließend. Für eine Normierung einer Vorschrift zur Konkretisierung der allgemeinen datenschutzrechtlichen Anforderungen an die Einwilligungsmodalitäten mangelt es an der Kompetenz des nationalen Gesetzgebers bzw. an einschlägigen Öffnungsklauseln im unionalen Sekundärrecht. Die Gefahr, dabei durch gesonderte Anforderungen an die Modalitäten der Einwilligung i.S.d. § 24 Abs. 1 TTDSG-RegE eine europarechtswidrige Norm zu schaffen, deren chilling effects zu einer Beeinträchtigung deutscher Unternehmen im europäischen Wettbewerb führen, ist hoch. Bei Umsetzung des Vorschlags des Bundesrats[39] sähen sich Unternehmen wohl in hohem Maße genötigt, unterschiedliche Einwilligungsbanner – einmal nach TTDSG, einmal nach DSGVO – einzusetzen. Für Nutzer könnte dies bedeuten, dass sich der Aufwand der Erteilung bzw. Nichterteilung der Einwilligung verdoppelt, d.h. genau der gegenteilige Effekt des Gewünschten erzielt wird.

Bei der derzeitigen Rechtslage erscheinen Vorgaben zur Gestaltung der Einwilligung nicht zielführend. Ein bereits jetzt bestehendes Vollzugsdefizit wird nicht dadurch ausgeglichen, dass zusätzliche Normen geschaffen werden, sondern allenfalls vergrößert. Die Konkretisierung der Anforderungen an eine Einwilligung sollte insoweit der Judikative überlassen werden. Zu diesem Zweck sollten die Aufsichtsbehörden gegenüber Diensteanbietern stärker auf datenschutzkonforme Einwilligungserklärungen hinwirken.

5. „Do not track“: Berücksichtigungspflicht wäre kontraproduktiv

Nahezu alle Internetbrowser bieten dem Nutzer an, durch entsprechende Konfiguration besuchten Seiten als http-Header eine „Do-Not-Track“-Anforderung (DNT) zukommen zu lassen. Die derzeitige Marktstruktur der Internetbrowser stellt sich als ein Oligopol dar, welches seit 2014 sowohl im mobilen als auch im stationären Bereich von Googles Browser „Chrome“ dominiert wird.[40] Die Verortung und Bezeichnung der

39 Vgl. insoweit BT-Drucks. 19/28396, S. 6.

40 Derzeit entfallen über 85% der Seitenaufrufe von Desktop-Systemen und Notebooks auf Google Chrome, Apple Safari und Microsoft Edge, siehe https://de.statista.com/statistik/daten/studie/157944/umfrage/marktanteile-der-browser-bei-der-internetnutzung-weltweit-seit-2009/, sowie über 95% der

jeweils maßgeblichen Einstellung sind höchst unterschiedlich;[41] ihre Bedeutung wird mitunter nicht näher in den Browsereinstellungen erläutert. So wird eine Erklärung, was unter der Option „Bei Browserzugriffen eine ‚Do Not Track'-Anforderung mitsenden" zu verstehen ist, beim marktführenden Browser erst dann angezeigt, wenn der Nutzer diese aktivieren will.

Eine differenzierte Möglichkeit zur Konfiguration, wie ihn Art. 4 Nr. 11 DSGVO für die Einwilligung („für den bestimmten Fall") vorschreibt, lassen die gängigen Browserkonfigurationen für das „Do Not Track" nicht zu. Zielbild eines funktionierenden „Do Not Track" im Sinne der Wahrung der Datensouveränität der Nutzer wäre die Ermöglichung einer Einwilligung für vom Nutzer bestimmte Szenarien.[42] Die Entscheidungsvielfalt des Nutzers wird in den meisten Fällen jedoch pauschal auf eine Schwarz-Weiß-Entscheidung heruntergebrochen.

Neben den dem Nutzer zur Verfügung gestellten Konfigurationsmöglichkeiten wird auch die Interpretation einer Do-not-track-Konfiguration in hohem Maße dem Browserhersteller überlassen. Denkbar ist, dass Browserhersteller eine Angabe des „Do Not Track" nicht als allgemeines „Do Not Track", sondern als Erklärung, lediglich allen Angeboten Dritter entsprechende DNT-Header zu übertragen, interpretieren.[43] Ebenso ist denkbar, dem Nutzer die „Do-Not-Track"-Funktion gar nicht zur Verfügung zu stellen, sodass der Browserhersteller frei darüber entscheiden könnte, welche Websites eine DNT-Anforderung erhalten.[44] Der gewünschte positive Effekt von DNT wird dadurch konterkariert, dass die scheinbar privatsphäreschonende Option dem Nutzer eine trügerische Sicherheit suggeriert, während die tatsächliche Entscheidung über das Tracking bei den Browserherstellern liegt.

Die Regelung einer Berücksichtigungspflicht von „Do Not Track" mag prima facie höchst wünschenswert erscheinen. Für Browserhersteller existiert allerdings keine Pflicht zum „Do not track" per Default oder überhaupt eine Pflicht, dem Nutzer die Option zur Übersendung eines entsprechenden http-Headers zur Verfügung zu stellen. Insofern dürfte der praktische Effekt gering sein. Hinzu kommt, dass daneben

---

Seitenaufrufe von Mobiltelefonen auf Google Chrome, Apple Safari und Samsung Internet, siehe https://de.statista.com/statistik/daten/studie/184297/umfrage/marktanteile-mobiler-browser-bei-der-internetnutzung-in-deutschland-seit-2009/ (jeweils zuletzt abgerufen: 18.04.2021).

41 Siehe https://allaboutdnt.com/#adjust-settings (zuletzt abgerufen: 18.04.2021).

42 Vgl. auch die Äußerung des Bundesrats, BT-Drucks. 19/28396, S. 4.

43 Vgl. etwa die Google Chrome-Hilfe: „Die meisten Websites und Webdienste, einschließlich die von Google, ändern ihr Verhalten nicht, wenn sie eine ‚Do Not Track'-Anforderung erhalten.", abrufbar unter https://support.google.com/chrome/answer/2790761 (zuletzt abgerufen: 18.04.2021).

44 So hat Apple die Do-not-Track-Funktion in dem Browser „Safari" entfernt, siehe: https://developer.apple.com/documentation/safari-release-notes/safari-12_1-release-notes (zuletzt abgerufen: 18.04.2021).

keinerlei verbindliche Vorgaben für Softwarehersteller existieren, wie die Ausgestaltung von „Do Not Track“ in der Nutzeroberfläche zu erfolgen hat. An Softwarehersteller gerichtete Vorgaben zu datenschutzrechtlichen Voreinstellungen – wie vom Bundesrat angeregt – wären jedoch in einem Gesetz, welches TK- und Telemedienanbieter adressiert, systematisch verfehlt.

Solange diese Parameter nicht gesetzlich konturiert sind, ist zu befürchten, dass eine Berücksichtigungspflicht von „Do Not Track“ im besten Fall dazu führt, dass Hersteller die Option deaktivieren und keinerlei Verbesserung für den Nutzer eintritt – im schlechtesten Fall, dass Hersteller die DNT-Option instrumentalisieren und marktbeherrschende Strukturen auf nachgelagerte Märkte übertragen werden, d.h. der Wettbewerb zugunsten einzelner transatlantischer Profiteure verzerrt wird.

6. Zuständigkeit der Datenschutzaufsicht: Unklarheiten

Die Aufsicht über die Einhaltung des Teil 3 des TTDSG-RegE wird bis auf eine für Telemedien der Privatwirtschaft unbedeutende Ausnahme[45] nicht ausdrücklich geregelt. Die Länder führen das TTDSG als Bundesgesetz gemäß Art. 83 GG als eigene Angelegenheit aus.[46] Auf Landesebene überweist § 113 Satz 1 MStV die Aufgabe der Aufsicht den „nach allgemeinen Datenschutzgesetzen zuständigen Aufsichtsbehörden“, d.h. den Landesdatenschutzbehörden. „Allgemeine Datenschutzbestimmungen“ i.S.d. § 113 Satz 1 MStV sind nach in der Literatur vertretener Auffassung die Anforderungen aus DSGVO, BDSG, Telemediengesetz und etwaigen weiteren datenschutzrechtlichen Normen,[47] auch das künftige TTDSG könnte von dieser Norm erfasst sein.[48] Dabei weisen dann die einzelnen, jeweils anzupassenden „Telemedienzuständigkeitsgesetze“ der Länder die Telemedienaufsicht der jeweiligen Landesbehörde zu.[49]

Das allgemeine Datenschutzrecht folgt im Grundsatz dem in Art. 56 DSGVO kodifizierten „One-Stop-Shop“, welcher durch die Regelungen des Kapitels 7 – die Zusammenarbeits- und Kohärenzmechanismen – flankiert wird. Hiernach ist grundsätzlich die Aufsichtsbehörde am Ort der Hauptniederlassung eines Verantwortlichen zuständig oder, wenn nur eine Niederlassung innerhalb der EU existiert, die Behörde am Ort

---

45 § 27 Abs. 2 TTDSG-RegE.

46 I.E. auch *Lang*, K&R 2020, 714 (718).

47 *Fiedler,* in: Gersdorf/Paal, BeckOK Informations- und Medienrecht, 31. Ed., MStV, § 113 Rn. 3.

48 *Hanloser,* ZD 2021, 121 (122).

49 Vgl. für Nordrhein-Westfalen: § 1 Abs. 2 Satz 1 des Gesetzes zur Regelung der Zuständigkeit für die Überwachung von Telemedien nach dem Telemediengesetz und nach § 59 Abs. 2 Rundfunkstaatsvertrag.

dieser einzigen Niederlassung.[50] §§ 40, 19 BDSG übertragen diese Systematik in die föderale Struktur der Bundesrepublik Deutschland. Einen nationalen „One-Stop-Shop“ ordnet das TTDSG zwar nicht konkret an, eine Anwendung dieser Vorschriften kann aber aus dem pauschalen Verweis zur Bestimmung der Zuständigkeit in § 113 Satz 1 MStV nach den dort referenzierten „allgemeinen Datenschutzgesetzen“ zu folgern sein. Diese Interpretation ist jedoch nicht zwingend: Zum einen können die Vorschriften des TTDSG insgesamt nicht als „Datenschutzvorschriften“, wie sie von § 113 Satz 1 MStV und § 40 Abs. 1 BDSG vorausgesetzt werden, eingestuft werden. Überwiegend handelt es sich nämlich um Vorschriften zum Schutz des Fernmeldegeheimnisses und – im Falle des § 24 TTDSG-RegE – zum Schutz der informationellen Integrität des Endgeräts. Darüber hinaus ist eine Verweisung auf noch nicht in Kraft getretene Vorschriften wie das TTDSG nur in Ausnahmefällen möglich;[51] inhaltsbezogenen Verweise wie in § 113 Satz 1 MStV sollten zudem nur verwendet werden, sofern die Bezugsnormen mit zumutbarem Aufwand herausgefunden werden können.[52]

Diese Unklarheiten resultieren bereits jetzt – unter Geltung der §§ 11 ff. TMG – in Schwierigkeiten, die wohl nicht allein darauf zurückzuführen sind, dass einige Länder ihre Zuständigkeitsregelungen noch nicht an den MStV angepasst haben.[53] Bei einzelnen Aufsichtsbehörden, die ihrer Kontrolltätigkeit im Bereich von Cookies bzw. dem Schutz von Endgeräten nachkommen, ist jedenfalls zu beobachten, dass diese ihre Zuständigkeit nicht begründen (können). Das erwähnte Vollzugsdefizit[54] wird damit verstärkt.

Eine zusätzliche Schwierigkeit bergen dabei die unterschiedlichen Anknüpfungspunkte der beiden Regelungsregimes: Während bei der DSGVO sowohl die Anwendbarkeit als auch die Bestimmung der zuständigen Behörde (primär) an die Belegenheit der Niederlassung des Verantwortlichen anknüpfen,[55] knüpft zwar die Anwendbarkeit des TTDSG-RegE (primär) an die Person des Diensteanbieters (§ 2 Abs. 1 TTDSG-RegE), aber nicht an seine datenschutzrechtliche Rolle an.[56] Insbesondere in Konzernkonstellationen droht eine künstliche Aufspaltung der Zuständigkeit für denselben Sachverhalt, nämlich der Verarbeitung über Websites. Hieraus könnten

---

50 Art. 56 Abs. 1 DSGVO.

51 BMJV, Handbuch der Rechtsförmlichkeit, 3. Aufl. 2008, Rn. 251.

52 BMJV, Handbuch der Rechtsförmlichkeit, 3. Aufl. 2008, Rn. 238.

53 Vgl. für Nordrhein-Westfalen: Art. 3 des Entwurf eines zur Änderung des WDR-Gesetzes, des Landesmediengesetzes Nordrhein-Westfalen und zur Änderung weiterer Gesetze (19. Rundfunkänderungsgesetz), LT-Drucks. 17/12307.

54 Siehe oben B.IV.

55 Vgl. Art. 3 Abs. 1 und Art. 55 f. DSGVO.

56 Für § 24 TTDSG-RegE auch *Benedikt,* DSB 2020, 76 (78).

höhere Erfüllungsaufwände für Wirtschaft und Verwaltung resultieren. Die vollständige Lösung letzteren Problems kann nur durch (flankierende) Regelungen auf europäischer Ebene erfolgen und ist bereits in den Entwürfen der ePrivacy-Verordnung angelegt.[57]

Es erscheint möglich, die absehbaren Probleme jedenfalls für innerdeutsche Sachverhalte zu reduzieren. Sinnvoll wäre eine Ergänzung/Konkretisierung der Verweisnorm im MStV, die jedoch im laufenden Gesetzgebungsverfahren nicht möglich wäre. Daher ist eine klarstellende Verweisung auf eine entsprechende Anwendung der §§ 40, 9 BDSG, wobei der Begriff des „Verantwortlichen" als „Anbieter von Telemedien" und der Begriff „betroffene Person" als „Nutzer" bzw. „Endnutzer" verstanden werden sollte, in den §§ 26, 27 des TTDSG zu empfehlen.

Ich bedanke mich für die kurzfristige Gelegenheit zur Stellungnahme und hoffe, dass meine Anmerkungen hilfreich für das weitere Gesetzgebungsverfahren sind.

Mit freundlichen Grüßen

Dr. Alexander Golland
Rechtsanwalt

57 Siehe Art. 18 ePrivacy-VO-E-KOM, siehe COM(2017) 10 final vom 10.1.2017.

III. Anhang: Vorschlag für § 24 TTDSG

Eine Regelung, die sämtliche unter B.III. geschilderten Vorschläge aufnimmt, könnte wie folgt gestaltet sein (Änderungen im Vergleich zum RegE sind kursiv hervorgehoben):

§ 24 Schutz der Privatsphäre bei Endeinrichtungen

(1) Die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, sind nur zulässig, wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat. Die Information des Endnutzers und die Einwilligung haben gemäß der Verordnung (EU) 2016/679 zu erfolgen.

(2) Die Einwilligung nach Absatz 1 ist nicht erforderlich,

1. wenn der alleinige Zweck der Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der alleinige Zweck des Zugriffs auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen die Durchführung der Übertragung einer Nachricht über ein öffentliches Telekommunikationsnetz ist oder

2. wenn die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen unbedingt erforderlich ist, damit der Anbieter eines Telemediendienstes einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann*; dies ist insbesondere der Fall, wenn die Speicherung oder der Zugriff ausschließlich dazu dient*

   a. *nach erfolgreicher Authentifizierung aufgrund aktiver Eingaben des Nutzers eine wiederholte Authentifizierung innerhalb desselben Diensts zu vermeiden oder*

   b. *aktive Eingaben des Nutzers während der Nutzung desselben Diensts zu speichern oder*

   c. *den Endnutzer, sein Nutzerkonto, den von ihm angefragten Dienst oder die gegenüber dem Diensteanbieter zur Authentifizierung genutzten Authentifizierungsinstrumente zu schützen oder*

   d. *durch den Nutzer aktiv vorgenommene Konfigurationen des Diensts zu speichern oder*

   e. *aktiv vom Nutzer angefragte audiovisuelle Medien innerhalb des Diensts anzuzeigen.*

(3) Als unbedingt erforderlich im Sinne des Absatzes 2 Nr. 2 gelten auch die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen, wenn

1. *der alleinige Zweck darin besteht, die Reichweite des Diensts und die Erfassung des Publikums in Kohorten zu messen,*
2. *die Speicherung oder der Zugriff ausschließlich durch den Diensteanbieter oder seinen durch ein Rechtsinstrument nach Artikel 28 Absatz 3 der Verordnung (EU) 2016/679 gebundenen Auftragsverarbeiter erfolgt,*
3. *eine Zusammenführung mit anderen Informationen des Endnutzers ausgeschlossen ist,*
4. *eine Weitergabe erhobener personenbezogener Informationen an Dritte nicht erfolgt,*
5. *die erhobenen Informationen nach spätestens 12 Monaten gelöscht werden und*
6. *der Endnutzer auf eine bestehende, einfach durchzuführende Widerspruchsmöglichkeit hingewiesen wurde und der Speicherung oder dem Zugriff nicht widersprochen hat.*