Deutscher Bundestag
19. Wahlperiode
Ausschuss für Wirtschaft und Energie

Ausschussdrucksache 19(9)1039
19. April 2021

Dr. Simon Assion
Rechtsanwalt
sas@simon-assion.de

Mainz, den 18.04.2021

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

Vorbemerkung

Ich bedanke mich für die Gelegenheit, zum Entwurf des TTDSG Stellung nehmen zu dürfen. Ich bin als Rechtsanwalt und wissenschaftlicher Autor regelmäßig mit Angelegenheiten des Telekommunikations- und Telemediendatenschutzes befasst. Außerdem bin ich Mitglied des Fachausschusses Informationsrecht des DAV Mitherausgeber des Internetprojektes Telemedicus.info.[1]

In Teil 1 dieser Stellungnahme adressiere ich einige grundsätzliche Fragen, auf die die politische Debatte zum TTDSG sich bisher fokussiert hat. In Teil 2 ergänze ich konkrete Verbesserungsvorschläge zu einzelnen Vorschriften des TTDSG.

1. Grundsätzliche Aspekte

1.1 Zum rechtlichen Hintergrund und zur Notwendigkeit, ein TTDSG zu schaffen

Der wichtigste Regelungsgegenstand des TTDSG ist die Anpassung des deutschen Telekommunikations- und Telemedienrechts an den Rechtsstand seit Geltung der DSGVO. Denn seit dem 25. Mai 2018, also seit dem Geltungsbeginn der DSGVO, sind etliche Vorschriften des bereichsspezifischen Datenschutzes im Telemediengesetz (TMG) und Telekommunikationsgesetz (TKG) europarechtswidrig.[2] Diese Vorschriften werden von der DSGVO aufgrund von deren Vollharmonisierungswirkung verdrängt und sind weder durch eine der Öffnungsklauseln der DSGVO noch durch die Richtlinie 2002/58/EG über Datenschutz in der elektronischen Kommunikation (sog. ePrivacy-RL) gedeckt.

Die Folge davon ist, dass seit mittlerweile fast drei Jahren die Datenschutzbestimmungen in den zwei wichtigsten deutschen „Digitalgesetzen“, dem TMG und dem TKG, größtenteils nicht anwendbar sind. Nunmehr hat sich der deutsche Gesetzgeber dazu entschlossen, dem Problem abzuhelfen. Er hebt dazu die unwirksamen Vorschriften auf und ersetzt sie, in reduziertem Umfang, durch das TTDSG.

---

[1] Diese Stellungnahme gibt lediglich meine persönliche Auffassung wieder.
[2] Ausführlich dazu bereits die DAV Stellungnahme 34/2018, Ziffer 4.

Welche Vorschriften konkret unwirksam sind, war durch den deutschen Gesetzgeber in einem komplizierten Verfahren zu prüfen. Da diese Prüfung nicht überall gelungen ist (dazu im Einzelnen unten 1.2) stelle ich eine Erklärung voran.

1.1.1 Verhältnis zwischen DSGVO und der ePrivacy-RL

Die Problematik ergibt sich aus einem komplizierten Zusammenspiel zwischen zwei Rechtsakten der EU: Der DSGVO und der ePrivacy-RL.[3] Die beiden Rechtsakte überschneiden sich teilweise in ihrem Anwendungsbereich.

Die DSGVO regelt ausschließlich Fragen des Datenschutzes.[4] Auch die ePrivacy-RL regelt Fragen des Datenschutzes, und zwar speziell mit Bezug zur „elektronischen Kommunikation". In diesem Bereich hat sie als lex specialis Vorrang gegenüber der DSGVO (vgl. Art. 95 DSGVO).

Die ePrivacy-RL hat außerdem zwei Regelungsgegenstände, die nicht zum Datenschutz gehören und insofern *nicht* in Konkurrenz zur DSGVO treten:

1) Zum einen regelt die ePrivacy-RL ein Rechtsgut, das gleichrangig *neben* dem Datenschutz steht, nämlich die Vertraulichkeit der Kommunikation; im deutschen Recht spricht man vom Telekommunikationsgeheimnis.[5] Zu diesem Rechtsgut gehört auch der Schutz von sog. Verkehrsdaten, also von Daten über die näheren Umstände der Telekommunikation. Das Telekommunikationsgeheimnis ist historisch älter als der Datenschutz und hat einen anderen Schutzcharakter (beispielsweise schützt es anders als der Datenschutz auch juristische Personen).

2) Und zum zweiten enthält die ePrivacy-RL in Art. 5 Abs. 3 eine Vorschrift zum Schutz von „Informationen auf Endgeräten". Diese Vorschrift wird meist als „Cookie-Regelung" bezeichnet, hat tatsächlich aber einen viel größeren Anwendungsbereich. Sie bezieht sich nicht nur auf Cookies, sondern letztlich auf alle Informationen, die ein Drittanbieter auf Geräten ablegt oder abruft, die mit öffentlichen Telekommunikationsnetzen (insbesondere mit dem Internet) verbunden sind.[6] Diese „Informationen auf Endgeräten" werden unabhängig davon geschützt, ob es sich um personenbezogene Daten handelt,[7] gehören also ebenfalls nicht zum Datenschutz.

Diese beiden Rechtsgüter stehend gleichrangig *neben* der DSGVO und werden von ihr nicht verdrängt. In diesem Bereich hat aber die ePrivacy-RL ihrerseits Harmonisierungswirkung; auch dort kann der deutsche Gesetzgeber also nicht nach eigenem Ermessen die Vorgaben der ePrivacy-RL abwandeln oder zusätzliche Regelungen einführen.

---

[3] Instruktiv hierzu die Stellungnahme 5/2019 des Europäischen Datenschutzausschusses.
[4] Vgl. Art. 1 Abs. 1 DSGVO.
[5] Datenschutz: Art. 8 EU-GrCh bzw. Art. 1 Abs.1, Art. 2 Abs. 1 GG; Telekommunikationsgeheimnis: Art. 7 EU-GrCh bzw. Art. 10 GG.
[6] Vgl. beispielsweise die Empfehlungen 01/2020 des Europäischen Datenschutzausschusses zu vernetzten Fahrzeugen (die finale Version ist bislang nur auf Englisch verfügbar).
[7] Vgl. EuGH, Urt. v. 1 October 2019 - C-673/17, Rn. 69 ff. – *Planet 49*.

1.1.2 Verhältnis zwischen DSGVO und nationalem „ePrivacy-Recht“

Die zweite Problematik besteht in der Regelung von „ePrivacy-Recht“ im Mehrebenensystem und dessen Konkurrenzverhältnis zur DSGVO.

Anders als die DSGVO muss die ePrivacy-RL als Richtlinie durch ein deutsches Gesetz umgesetzt werden. Daraus folgt, dass „ePrivacy“-Recht, anders als die DSGVO, auf zwei Ebenen existiert: Auf Ebene des EU-Sekundärrechts in Form einer Richtlinie, und auf Ebene des nationalen Bundesrechts als deren Umsetzung.

Gem. Art. 95 DSGVO kann die ePrivacy-RL (und mit ihr nationales „ePrivacy“-Recht) gegenüber der DSGVO dabei vorrangig sein. Allerdings gilt das für das nationale Recht nur, soweit es sich exakt an den Wortlaut der ePrivacy-Richtlinie hält. Alles darüberhinausgehende sektorspezifische Datenschutzrecht wird ist von Art. 95 DSGVO nicht gedeckt. Es wird deshalb von der Vollharmonisierungswirkung der DSGVO verdrängt; es sei denn die DSGVO sieht in einer ihrer „Öffnungsklauseln“ die Möglichkeit für nationale Gesetzgeber vor, eigene Regelungen zu schaffen.[8]

Die Folge davon ist, dass das sektorspezifische Datenschutzrecht im TMG und TKG auf die Regelungen „zurückgebaut“ werden muss, die entweder von der ePrivacy-RL oder von einer der Öffnungsklauseln der DSGVO gedeckt sind (s.o. 1.1.1).

Dieses schwierige Konkurrenzverhältnis zwischen DSGVO und ePrivacy-RL wollte der EU-Gesetzgeber eigentlich vermeiden, indem er parallel zur DSGVO die ePrivacy-RL aufhebt und durch eine neue ePrivacy-Verordnung (ePrivacy-VO) ersetzt.[9] Die DSGVO und die neue ePrivacy-VO wären dann gleichberechtigt nebeneinandergestanden.

Der Versuch, eine ePrivacy-VO zu schaffen, ist allerdings bislang misslungen, was m.E. vor allem an grundlegenden Qualitätsproblemen des Entwurfs liegt, den die EU-Kommission seinerzeit vorgelegt hatte.[10] Derzeit befindet sich das Gesetzgebungsverfahren der ePrivacy-VO vor Beginn des Trilogs. Ob und wann es abgeschlossen werden kann, ist völlig offen. Selbst wenn der Trilog nun zügig abgeschlossen werden könnte, was unwahrscheinlich ist, so wäre frühestens in ca. eineinhalb Jahren mit dem Geltungsbeginn der ePrivacy-VO zu rechnen.[11] Denkbar ist auch, dass das Verfahren noch deutlich länger dauert oder sogar neu begonnen werden muss.

Solange es keine ePrivacy-Verordnung gibt, bleibt es aber dabei, dass das deutsche sektorspezifische Datenschutzrecht im TMG und TKG an das höherrangige EU-Recht angepasst werden muss.

---

[8] *Schramm/Shvets* MMR 2019, 228 und MMR 2019, 568.
[9] Diese Absicht ist sogar in Erwägungsgrund 173 der DSGVO dokumentiert.
[10] Vgl. dazu die DAV Stellungnahme 29/17.
[11] Ab Inkrafttreten gäbe es in der ePrivacy-VO noch eine Übergangsfrist von mindestens einem, eventuell auch zwei Jahren (vgl. Art. 29 der bisher vorliegenden Entwürfe). Eine Übergangsfrist von weniger als einem Jahr ist aber sehr unwahrscheinlich.

1.2 Zum eingeschränkten Spielraum des deutschen Gesetzgebers

In der Folge des Zusammenspiels zwischen DSGVO und ePrivacy-RL und der Vorrangwirkung beider EU-Rechtsakte gegenüber deutschem Recht sind die Möglichkeiten des deutschen Gesetzgebers, eigene politische Akzente zu setzen, gering.

- Zum einen darf der deutsche Gesetzgeber keine eigenständigen Datenschutzregelungen erlassen, die in den Bereich der Vollharmonisierung der DSGVO fallen, ohne entweder von deren Öffnungsklauseln oder von der ePrivacy-RL (i.V.m. Art. 95 DSGVO) gedeckt zu sein. Solche Regelungen wären europarechtswidrig und wegen des Vorrangs des Europarechts in der Praxis nicht anwendbar.

- Zum anderen kann und darf der deutsche Gesetzgeber auch keine Regelungen erlassen, die von der Harmonisierungswirkung der ePrivacy-RL abweichen. Die ePrivacy-RL verlangt zwar keine Vollharmonisierung, d.h. sie lässt dem deutschen Gesetzgeber Spielräume. Dort, wo die ePrivacy-RL aber *abschließend* bestimmte Rechtsfolgen vorgibt, darf der deutsche Gesetzgeber hiervon nicht abweichen.

Im Ergebnis führt dies dazu, dass der deutsche Gesetzgeber nur sehr wenig Spielraum hat, eigenes Datenschutz- oder „ePrivacy"-Recht zu setzen.

Dass dieser Spielraum begrenzt ist, ist auch politisch sinnvoll. Denn die im TTDSG geregelten Telekommunikations- und Telemediendienste werden häufig grenzüberschreitend erbracht, und zwar einheitlich für den gesamten EU-Binnenmarkt. Jede Regelung im nationalen Recht, die vom harmonisierten EU-Recht abweicht, bedeutet für derartige Dienste ein Marktzutrittshindernis und damit Zersplitterung des EU-Binnenmarkts.

Vor diesem Hintergrund habe ich bei einigen Vorschriften des TTDSG-E erhebliche Bedenken zu deren Vereinbarkeit mit höherrangigem Europarecht.

Konkret betrifft dies die folgenden Vorschriften:

Vorschrift im TTDSG-E	Bedenken zur Vereinbarkeit mit EU-Recht
§ 6 – Nachrichtenübermittlung mit Zwischenspeicherung	Diese Regelung hat keine Grundlage in der ePrivacy-RL, fällt aber in deren harmonisierten Bereich (vgl. vor allem Art. 5 Abs. 1 der RL). Unter welchen Umständen ein TK-Anbieter die von ihm übertragenen Inhalte „zwischenspeichern" darf, ist in Art. 5 Abs. 1 der ePrivacy-RL abschließend geregelt. Insbesondere darf er dies mit Einwilligung der betroffenen Nutzer und wenn dies für die Weiterleitung der Nachricht erforderlich ist. § 6 TTDSG-E würde für die Zwischenspeicherung neue Ge- und Verbote

	aufstellen, die von der ePrivacy-RL abweichen. Diese Ge- und Verbote sind europarechtswidrig und nicht anzuwenden. Auch auf die „Öffnungsklausel“ in Art. 15 Abs. 1 der ePrivacy-RL lässt sich § 6 TTDSG-E m.E. nicht stützen, da die Vorschrift keinen der dort zugelassenen Regelungszwecke verfolgt.[12] Anders als in der Begründung des Regierungsentwurfs ausgeführt, ist die Vorschrift auch nicht durch Erwägungsgrund 22 der ePrivacy-RL abgedeckt. Zum einen besagt Erwägungsgrund 22 überhaupt nicht das, was in § 6 TTDSG-E geregelt ist. Zum anderen sind Erwägungsgründe keine verbindlichen Bestimmungen von EU-Richtlinien. Sie sind lediglich Rechtsquellen, die die Auslegung der eigentlichen Bestimmungen der Richtlinie (d.h. von deren Artikeln) erleichtern sollen. Erwägungsgrund 22 ist demzufolge bei der *Auslegung* des TTDSG heranzuziehen, ist aber keine Ermächtigung für den deutschen Gesetzgeber, Recht zu schaffen, das materiell von den Vorgaben der ePrivacy-RL abweicht. Ich empfehle dem Ausschuss deshalb, § 6 aus dem TTDSG-E zu streichen.
§ 9 – Verarbeitung von Verkehrsdaten	Die Vorschrift ist deutlich restriktiver formuliert als die zugrundeliegenden Art. 6 Abs. 1 ePrivacy-RL. Aus nicht nachvollziehbaren Gründen wurde außerdem der Wortlaut gegenüber der Vorgängervorschrift (§ 96 TKG) durch einige kleine, aber durchschlagende Änderungen so geändert, dass er die Befugnis zur Verarbeitung von Verkehrsdaten deutlich einschränkt. Insbesondere wurde am Anfang das Wort „nur“ hinzugefügt und die Erlaubnis zur Verarbeitung für „die in diesem Abschnitt genannten Zwecke“ gestrichen. Außerdem wurde die Vorschrift des § 96 Abs. 1 Satz 2 TKG (der die Verwendung von Verkehrsdaten für „andere durch gesetzliche Vorschriften begründete Zwecke“ erlaubt hatte) nicht übernommen; statt dessen spricht die § 9 Abs. 1 Satz 4 TTDSG-E von einer „Pflicht zur

[12] Konkret: „nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen“.

	Verarbeitung von Verkehrsdaten auf Grund von anderen Rechtsvorschriften“. Weggefallen ist dadurch beispielsweise die Befugnis zur Verarbeitung von Verkehrsdaten für Zwecke, die in *anderen* Vorschriften dieses Teil des TKG bzw. TTDSG genannt sind.[13] Es ist unklar, ob bzw. warum der Regierungsentwurf die Vorschrift so stark verschärfen will. In der Begründung des Regierungsentwurfs ist lediglich die Rede von einer „redaktionellen Anpassung“. Wenn man die Vorschrift getreu ihrem neuen Wortlaut auslegt, so beschränkt sie jedenfalls sowohl die verwendbaren Kategorien von Verkehrsdaten als auch die erlaubten Verwendungszwecke stärker als Art. 6 Abs. 1 und 2 der ePrivacy-RL. Die Vorschrift ist insofern einerseits europarechtswidrig, andererseits aber auch politisch verfehlt. Modern aufgebaute TK-Dienste, insbesondere OTT-Dienste, verwenden die in Abs. 1 genannten Verkehrsdaten für andere als die hier erlaubten Zwecke, z.B. auch für die Spam-Abwehr, um dem Nutzer zu ermöglichen seinen Datenverbrauch zu überwachen oder zum Verkehrsmanagement. Solche Verarbeitungen würde die Neufassung unnötig in einen rechtlichen Graubereich schieben. Ich empfehle, den § 9 Abs. 1 TTDSG-E durch den (leicht anzupassenden) Wortlaut von Art. 6 Abs. 1 der ePrivacy-RL zu ersetzen. Dies würde sowohl die Europarechtswidrigkeit als auch die zu starke Restriktion vermeiden.
§ 10 – Entgeltermittlung und Entgeltabrechnung	Auch § 10 TTDSG ist im Vergleich zu seiner europarechtlichen Grundlage (Art. 6 Abs. 2 ePrivacy-RL) unnötig restriktiv und kompliziert. Wo der hiesige § 10 die Befugnisse der TK-Anbieter zur Verarbeitung von Verkehrsdaten stärker einschränken würde als

[13] Scheurle/Mayen/*Büttgen*, 3. Aufl. 2018, TKG § 96 Rn. 7.

	die ePrivacy-RL,[14] wäre er wohl europarechtswidrig. Ich schlage Ihnen vor, den § 10 durch den (im Wortlaut leicht anzupassenden) Wortlaut des Art. 6 Abs. 2 der ePrivacy-RL zu ersetzen.
§ 13 Abs. 1 - Standortdaten	Die Vorschrift bleibt teils hinter den Vorgaben von Art. 9 Abs. 1 der ePrivacy-RL[15] zurück, teils geht sie darüber hinaus. • Sie bleibt dahinter zurück, indem sie anders als Art. 9 Abs. 1 ePrivacy-RL keine konkreten Anforderungen an die Informationen stellt, die der Anbieter dem Nutzer vor dessen Einwilligung geben muss. Diese Mindestinformationen sind nicht zwingend deckungsgleich mit den Vorgaben der DSGVO für informierte Einwilligungen.[16] • Und sie geht darüber hinaus, denn sie verlangt in Abs. 1 Satz 2 eine Information des Nutzers in Form einer „Textmitteilung an das Endgerät, dessen Standortdaten ermittelt wurden“. Abs. 1 Satz 4 verlangt für den speziellen Fall der Übermittlung an Dritte sogar eine Einwilligung in Schriftform. Auch dies ist in Art. 9 ePrivacy-RL nicht vorgegeben.

[14] In einigen Teilen ist die Vorschrift zwar keine zusätzliche Einschränkung; sie wiederholt aber unnötigerweise Anforderungen, die sich aus der DSGVO ergeben (insb. aus den dort geregelten Prinzipien der Zweckbindung, Datenminimierung und Speicherbegrenzung).

[15] Art. 9 der ePrivacy-RL hat systematisch einen anderen Zuschnitt, da er sich anders als § 13 TTDSG nur auf Standortdaten bezieht, die nicht gleichzeitig auch Verkehrsdaten sind. § 13 TTDSG gilt demgegenüber für *alle* Standortdaten, unabhängig davon ob sie Verkehrsdaten sind oder „nur“ aus einem TK-Netz oder TK-Dienst stammen (vgl. die Definition in § 3 Nr. 56 des TKG-E in der Fassung des TKMoG, Regierungsentwurf).

[16] Art. 9 Abs. 1 der ePrivacy-RL verlangt eine Mitteilung, „welche Arten anderer Standortdaten als Verkehrsdaten verarbeitet werden, für welche Zwecke und wie lange das geschieht, und ob die Daten zum Zwecke der Bereitstellung des Dienstes mit Zusatznutzen an einen Dritten weitergegeben werden“. Die DSGVO verlangt lediglich, dass eine Einwilligung „informiert“ und „für bestimmte Zwecke“ erfolgen muss, was im Wortlaut der Artikel der DSGVO nicht weiter konkretisiert wird. Dem lassen sich zwar im Wege der Auslegung ähnliche Anforderungen entnehmen wie dem Wortlaut von Art. 9 der ePrivacy-RL (vgl. dazu die Empfehlungen des Europäischen Datenschutzausschusses 05/2020, Version 1.1., Rn. 55-74). Allerdings sind auch andere Auslegungen möglich. Der deutsche Gesetzgeber sollte die Vorgabe von Art. 9 Abs. 1 ePrivacy-RL deshalb wortlautgetreu umsetzen, und nicht auf Basis einer diskutablen Auslegung der DSGVO.

	Bereits die Vorgängerregelung des hiesigen § 13 TTDSG-E, der § 98 TKG, sorgt in der Praxis regelmäßig für Probleme. Vor im Bereich „Smart Services“/“Internet der Dinge“ führt die Vorschrift häufig zu Schwierigkeiten, und zwar vor allem aufgrund ihres unklaren Anwendungsbereichs[17] und der teils sehr strengen Anforderungen. Ich empfehle deshalb, den Wortlaut des § 13 Abs. 1 TTDSG-E[18] durch den leicht anzupassenden Wortlaut von Art. 9 Abs. 1 der ePrivacy-RL zu ersetzen.
§ 17 - Endnutzerverzeichnisse	Zur Umsetzung der Vorgabe aus Art. 12 Abs. 1 der ePrivacy-RL (letzter Satzteil)[19] empfehle ich Ihnen, folgenden Satz noch anzufügen: "Vor ihrem Antrag sind die Anschlussinhaber über weitere Nutzungsmöglichkeiten aufgrund der in elektronischen Fassungen der Verzeichnisse eingebetteten Suchfunktionen zu informieren."
§ 19 Abs. 4 Nr. 2 a) – Pflicht des Telemediendienstanbieters zur Verhinderung von Verletzungen des Schutzes personenbezogener Daten	Nr. 2 Buchstabe a der Vorschrift bezieht sich speziell auf die Verhinderung von Datenschutzverletzungen und hat damit denselben Regelungsgegenstand wie Art. 32 DSGVO. Da die DSGVO in diesem Bereich aber Vollharmonisierungswirkung hat (d.h. kein weiteres Recht der Mitgliedsstaaten zulässt), ist die deutsche Regelung im TTDSG europarechtswidrig.[20] Ich empfehle sie zu streichen. Nr. 2 Buchstabe b der Vorschrift bezieht sich demgegenüber nicht speziell auf den

[17] Das Problem des unklaren Anwendungsbereichs wird sich mit Inkrafttreten des TTDSG noch vergrößern, denn die Definition des Begriffs „Standortdaten“ (in Zukunft § 3 Nr. 56 TKE-E) wird sich dann auch auf Daten beziehen, die von OTT-Kommunikationsdiensten verarbeitet werden, z.B. Messenger-Diensten. Bereits nach geltendem Recht ist strittig, ob „Standortdaten“ auch Daten sind, die über GPS-Sensoren oder aus dem Auslesen von WLAN-SSIDs gewonnen wurden. Wenn diese Daten erfasst wären, dann wären die Vorgaben des § 13 Abs. 1 TTDSG dafür sehr restriktiv.

[18] Die übrigen Absätze des § 13 TTDSG-E sind demgegenüber unbedenklich: § 13 Abs. 2 TTDSG-E entspricht weitgehend Art. 9 Abs. 2 ePrivacy-RL; § 13 Abs. 3 ist eine Ausnahmeklausel für die Verwendung von Standortdaten bei Notrufen und von Art. 109 Abs. 6 des Europäischen Kommunikationskodex gedeckt.
Abs. 4 ist eine Umsetzung der Vorgabe von Art. 9 Abs. 3 der ePrivacy-RL.

[19] „Die Mitgliedstaaten stellen sicher, dass die Teilnehmer [...] über weitere Nutzungsmöglichkeiten aufgrund der in elektronischen Fassungen der Verzeichnisse eingebetteten Suchfunktionen informiert werden.“

[20] So auch zur Vorgängerregelung *Redeker* IT-Recht, 7. Auflage 2020, Teil D Rn. 1076

	Datenschutz, sondern auf „Störungen, auch soweit sie durch äußere Angriffe bedingt sind". Eine „Störung" ist eine Beeinträchtigung der Vertraulichkeit, Integrität oder Verfügbarkeit eines informationstechnischen Systems, und zwar unabhängig davon, ob personenbezogene Daten betroffen sind. Dieser Teil wird von der Vollharmonisierungswirkung der DSGVO also nicht erfasst und kann m.E. so im TTDSG-E bleiben.

1.3 Zur richtigen Umsetzung von Art. 5 Abs. 3 der ePrivacy-RL

Ich begrüße, dass § 24 TTDSG-E letztlich eine Fassung erhalten hat, die den Vorgaben des höherrangigen Art. 5 Abs. 3 der ePrivacy-RL entspricht.

Zwar ist Art. 5 Abs. 3 der ePrivacy-RL rechtspolitisch gesehen ein Fehlschlag. Er stellt einen im Internet alltäglich vorkommenden Vorgang, nämlich das Einspeichern von Informationen in Endgeräten oder deren Abruf, unter ein Verbot mit Erlaubnisvorbehalt und lässt neben der Einwilligung nur zwei sehr eng gefasste gesetzliche Ausnahmen zu. Da diese Ausnahmen häufig nicht greifen, bleibt nur die Einwilligung als Rechtsgrundlage, also der „Cookie-Banner" oder vergleichbare Einwilligungs-Schaltflächen. Art. 5 Abs. 3 der ePrivacy-RL führt auf diese Weise zur Omnipräsenz von Einwilligungs-Bannern im Internet und entwertet die Warnfunktion der datenschutzrechtlichen Einwilligung („Consent Fatigue"). Er muss deshalb dringend reformiert werden.[21]

Allerdings kann der deutsche Gesetzgeber dieses Problem nicht lösen, das kann nur der EU-Gesetzgeber. Jedes deutsche Recht wird letztlich von den Gerichten richtlinienkonform ausgelegt werden.[22] Da Art. 5 Abs. 3 der ePrivacy-RL zum autonom auszulegenden Unionsrecht gehört,[23] kann der deutsche Gesetzgeber am Auslegungsergebnis nichts ändern.

Im Ergebnis heißt das: Egal wie das deutsche Recht formuliert ist – maßgeblich ist immer der Wortlaut des zugrundeliegenden EU-Rechts, d.h. von Art. 5 Abs. 3 der ePrivacy-RL.

Das Beste, das der deutsche Gesetzgeber in dieser Situation noch tun kann, ist eine Umsetzung des Wortlauts von Art. 5 Abs. 3 der ePrivacy-RL, die sich eng an dessen

[21] Als Randbemerkung sei erwähnt, dass die Entwürfe der Kommission und des Parlaments zur ePrivacy-VO diesbezüglich in die falsche Richtung gehen. Art. 8 dieser Vorschläge würde den Anwendungsbereich des Verbots mit Erlaubnisvorbehalt sogar noch vergrößern, die gesetzlichen Erlaubnisgrundlagen würden aber weiter sehr restriktiv bleiben. An der „Consent Fatigue" würde sich also wohl nichts ändern – ganz im Gegenteil. Die Ratsfassung versucht das Problem zu lösen, indem sie zusätzliche gesetzliche Erlaubnisse hinzufügt. Dies ist aber nur eine teilweise Lösung. Zwar ermöglicht sie dann die Nutzung von Endgeräte-Informationen ohne Einwilligungs-Banner, sie führt aber auch zu mehr Datenschutz-Bürokratie und zu Rechtsunsicherheit, da über die Auslegung der gesetzlichen Ausnahmen absehbar eine Vielzahl von Meinungsstreiten entstehen wird.

[22] BGH Urteil vom 28. Mai 2020 - I ZR 7/16 - *Cookie-Einwilligung II*.

[23] EuGH Urteil v. 1. Oktober 2019 – Rs. C-673/17, Rn. 47 – *Planet 49*.

Wortlaut hält, aber besser strukturiert ist. Dies ist dem Regierungsentwurf gelungen. Er sollte im weiteren Gesetzgebungsverfahren nicht mehr geändert werden.

Soweit Abgeordnete des Bundestags ihren (m.E. durchaus berechtigten) Unmut über die allgegenwärtigen Cookie-Banner geäußert haben,[24] so empfehle ich, diesen Unmut an die jeweiligen Parteikolleg*innen im Europaparlament weiterzugeben, insbesondere an die für die ePrivacy-VO zuständigen Berichterstatter*innen und Schattenberichterstatter*innen. Diese können dann darauf hinwirken, dass die ePrivacy-VO dieses Problem behebt.

1.4 Zur möglichen Einführung eines Regelungsrahmens für Personal Information Management Systems (PIMS)

Anders als noch eine geleakter Vorabfassung des Referentenentwurfs des TTDSG,[25] enthält der finale Regierungsentwurf keine Vorschrift mehr über sog. Personal Information Management Systems (PIMS). Da über deren Einführung aber weiter diskutiert wird, folgende Stellungnahme:

Die Einführung von PIMS wäre aus Sicht der Nutzerinteressen sicherlich ein Gewinn. Zum einen können PIMS teilweise die Notwendigkeit entfallen lassen, jede Einwilligung einzeln abzugeben. Sie entlasten damit die Nutzer vom ständigen „Wegklicken“ von Cookie-Bannern und anderen Einwilligungsbannern. Zum anderen können Nutzer ihre Privatsphäre-Einstellungen bei der Konfiguration von PIMS auch in einer Situation machen, in der sie sich genau hierauf konzentrieren. Auf Cookie-Banner stoßen die Nutzer stattdessen i.d.R. in einer Situation, wo sie eigentlich etwas ganz anderes suchen (z.B. eine bestimmte Webseite im Internet aufrufen) und keine Zeit und Lust haben, über ihre Privatsphäreneinstellungen nachzudenken.

Sinnvoll wäre eine Rahmengesetzgebung, die sicherstellt, dass PIMS ihre Rolle als Intermediäre und Gatekeeper zwischen Nutzern und Einwilligungsempfängern (also z.B. Webseitenanbieter oder Hersteller von vernetzten Geräten) nicht zu Lasten der einen oder anderen Seite missbrauchen. Dies wird zwar auch durch wettbewerbsrechtliche Vorschriften sichergestellt. Die Festlegung eines institutionellen Rahmens, insbesondere dazu, dass PIMS-Anbieter keine wirtschaftlichen Eigeninteressen verfolgen dürfen, ist aber sinnvoll.

Mehrere Punkte an der Einführung eines gesetzlichen Rahmens für PIMS im TTDSG sind aber auch problematisch:

1) Zunächst ist fraglich, ob und wie PIMS-Anbieter überhaupt die Anforderungen an eine wirksame Einwilligung erfüllen können. Art. 4 Nr. 11 DSGVO und Art. 7 DSGVO stellen an eine wirksame Einwilligung eine Vielzahl von Anforderungen, darunter „für den bestimmten Fall“, „in informierter Weise“ und „in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung“. Aus Erwägungsgrund 32 DSGVO folgt außerdem, dass Pauschaleinwilligungen unwirksam sind: „Wenn die Verarbeitung mehreren

[24] Vgl. Spiegel Online v. 26.03.2021, https://www.spiegel.de/netzwelt/netzpolitik/datenschutz-wie-der-bundestag-cookie-banner-abschaffen-will-a-1f449c0d-cd5c-494a-9b99-29c621973529.
[25] https://www.heise.de/downloads/18/2/9/4/6/4/2/1/20200731_RefE_TTDSG_cleaned.pdf

Zwecken dient, sollte für alle diese Verarbeitungszwecke eine Einwilligung gegeben werden."

Diese Anforderungen zu erfüllen, dürfte für PIMS-Anbieter in der Praxis eine große Herausforderung sein.[26] Denn die Idee eines PIMS ist ja, dass der Nutzer *vorab* über seine Einwilligungen disponiert, also lange bevor er das (einwilligungsbasierte) Angebot überhaupt in Anspruch nimmt. Der Nutzer entscheidet also bei der Konfiguration des PIMS *generell-abstrakt* darüber was mit seinen Daten später *konkret-individuell* passieren soll. Wirksam ist eine datenschutzrechtliche[27] Einwilligung aber nur dann, wenn der Nutzer vor deren Abgabe konkret darüber informiert worden ist, was mit seinen Daten passieren soll, und er genau darüber auch entschieden hat.[28]

Falls die von einem PIMS-Anbieter eingeholten bzw. vermittelten Einwilligungen unwirksam sind, dann treffend die Folgen in erster Linie das Unternehmen, das auf Basis der Einwilligung die Daten verarbeitet (ich spreche in der Folge von „Einwilligungsnehmern"). Denn nicht der PIMS-Anbieter, sondern der Einwilligungsnehmer ist für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich und muss diese im Zweifelsfall auch nachweisen können (Art. 5 Abs. 2 und 7 Abs. 1 DSGVO). Ein Einwilligungsnehmer, der personenbezogene Daten (bzw. Informationen aus Endgeräten) ohne Rechtsgrundlage erhebt oder verarbeitet, setzt sich erheblichen rechtlichen Risiken aus.

Ein Einwilligungsnehmer kennt aber i.d.R. nicht die Umstände, unter denen der PIMS-Betreiber beim Einwilligenden die Einwilligung eingeholt hat und kann die Wirksamkeit der Einwilligung deshalb weder beurteilen noch nachweisen. Angesichts der Tatsache, dass die Wirksamkeit der Einwilligung bei PIMS nicht einfach sicherzustellen ist (s.o.), ist es deshalb durchaus fraglich, ob Einwilligungsnehmer sich auf solche PIMS-Einwilligungen überhaupt verlassen werden.

Dieses Problem kann nur dadurch überwunden werden, dass der Gesetzgeber selbst regelt, dass (bzw. unter welchen Bedingungen) eine PIMS-gestützte Einwilligung *immer* wirksam sein soll – und zwar unabhängig von der Frage, ob die Anforderungen der DSGVO im Einzelfall erfüllt sind oder nicht. Dies wäre jedoch eine Abweichung von Anforderungen der DSGVO bzw. ePrivacy-RL. Da diese Rechtsakte zum Recht der EU gehören, kann dies nur der EU-Gesetzgeber erreichen.

2) Funktionieren kann die Vermittlung von Einwilligungen zwischen PIMS und Einwilligungsnehmern außerdem nur, wenn diese Daten darüber austauschen, welche Personen in welche Datenverarbeitung konkret eingewilligt haben. Einen solchen Datenaustausch zu organisieren ist aber nicht trivial, insbesondere wenn er datenschutzkonform erfolgen soll (d.h. hinreichend

[26] Vgl. dazu *ConPolicy/Spindler* (Hrsg.), Innovatives Datenschutz-Einwilligungsmanagement – Abschlussbericht.
[27] Oder, je nach Fall, eine Einwilligung zum Einspeichern oder Abrufen von Informationen aus Endgeräten.
[28] Vgl. dazu BGH Urteil vom 28. Mai 2020 - I ZR 7/16, Rn. 34 ff. – *Cookie-Einwilligung II*.

sicher und entsprechend des Grundsatzes der Datenminimierung gem. Art. 5 Abs. 1 lit. c DSGVO).

Denkbar wären für diesen Datenaustausch verschiedene Wege, beispielsweise eine Direktanbindung von Einwilligungsnehmern an das System des PIMS[29] oder eine „Vermittlung" der Einwilligung über Browser und sonstige Software, mit der die Nutzer sich im Internet bewegen (so der Vorschlag von *Schwartmann/Hanloser/Weiß* in einem Kurzgutachten für den PIMS-Anbieter netID)[30]. Letzteres würde aber eine Regulierung der (weltweit agierenden) Herstellern von Internetbrowsern sowie aller Hersteller von Mobile Apps und von Betriebssoftware von vernetzten Gegenständen (z.B. intelligenten Lautsprechern oder vernetzten Fahrzeugen) verlangen.[31]

Insgesamt ist diese Problematik alles andere als leicht aufzulösen. Auf EU-Ebene werden im Kontext der ePrivacy-Verordnung ähnliche Ansätze diskutiert (dort in erster Line über automatisierte Browser-basierte Einwilligungen), aber auch dort hat die Diskussion bislang zu keinen Ergebnissen geführt.

3) Als weiteres Problem stellt sich die Frage, ob das TTDSG überhaupt der richtige Ort zur Regelung von PIMS ist. Denn im TTDSG sind lediglich zwei Bereiche geregelt, wo eine Einwilligung gefordert wird: In Bezug auf Informationen auf Endgeräten und in Bezug auf Verkehrs- und Standortdaten. Der wichtigste Anwendungsbereich von Einwilligungen ist aber die DSGVO.

   Dies würde dafür sprechen PIMS in einem separaten „PIMS-Gesetz" zu regeln. Innerhalb des TTDSG wäre eine solche Vorschrift eher ein Fremdkörper.

1.5 Zu Überlegungen, Einwilligungen für Dritte verbindlich zu machen

Diskutiert wird (u.a. im Kontext von PIMS) über Regelungen, laut denen Dritte, die die „Herausgabe" von personenbezogenen Daten technisch beeinflussen können (z.B. die Hersteller von Browsern oder Betriebssystemen) an Einwilligungen der Nutzer gebunden sein sollen. Das heißt, diese Hersteller sollen gezwungen sein, die Daten eines Nutzers, in deren Verarbeitung dieser gegenüber einem Einwilligungsnehmer eingewilligt hat, technisch auch herauszugeben.

Eine solche Regelung würde aber dem Sinn und Zweck der datenschutzrechtlichen Einwilligung nicht entsprechen und wäre auch politisch nicht sinnvoll.

Eine datenschutzrechtliche Einwilligung ist eine einseitige rechtsgeschäftsähnliche Willenserklärung. Durch diese Willenserklärung erlaubt der Einwilligende dem Verantwortlichen die Verarbeitung von Daten für Zwecke bzw. in einem Umfang, die dem Verantwortlichen anderenfalls verboten wären. Die Einwilligung verpflichtet aber weder den Verantwortlichen noch jemand anderen dazu, diese Datenverarbeitung auch vorzunehmen. Hierdurch unterscheidet sich die Einwilligung von einem Vertrag.

---

[29] So offenbar die Variante bei netID; vgl. https://enid.foundation/partner/.
[30] https://enid.foundation/wp-content/uploads/2021/03/Schwartmann_Hanloser_Weiss-Kurzgutachten_Dienste_zur_Einwilligungsverwaltung_20210302.pdf
[31] Beispielsweise kann der Abruf von Medieninhalten heute über Browser am Computer, vernetzte Gegenstände (smarte Lautsprecher/ Bildschirme) oder native Apps auf Mobiltelefonen oder Tablets erfolgen. Eine Regulierung nur von Browser-Herstellern würde deshalb zu kurz greifen.

Nun im TTDSG festzulegen, dass die Einwilligung Dritte binden können soll, beispielsweise Browserhersteller, würde aus der Einwilligung eine Art „einseitiges Rechtsgeschäft zu Lasten Dritter“ machen: Aus der Erlaubnis würden sich eine Verpflichtung ergeben, und zwar für jemanden, der nicht einmal Empfänger dieser Erlaubnis war.

Rechtlich ist das nur schwer darstellbar, aber auch praktisch stellen sich Fragen: Wie soll der Browserhersteller (bzw. Browser) denn erfahren, dass eine Einwilligung vorliegt? Wie soll er die Wirksamkeit und den Umfang der Einwilligung nachvollziehen können? Wie soll er mit widersprüchlichen Anweisungen des Nutzers umgehen (Beispiel: Der Nutzer hat in den Einstellungen seines Browsers Drittanbietercookies deaktiviert, ein Webseitenbetreiber holt aber genau dafür erfolgreich eine Einwilligung ein)? Muss der Browserhersteller den Datenaustausch bzw. den Zugriff auf Informationen im Endgerät auch dann zulassen, wenn er dies für ein IT-Sicherheitsrisiko hält (beispielsweise, weil der Zugriff von einem bekannten Verbreiter von Malware stammt)? All diese Fragen sind nicht einfach zu beantworten und sollten geklärt werden, bevor dazu eine gesetzliche Regelung erlassen wird.

Soweit Browser- oder Betriebssystemhersteller ihre Marktmacht einsetzen, um Unternehmen, die von datenschutzrechtlichen Einwilligungen abhängen, zu diskriminieren oder auszubeuten, so ist dies eine Frage des Wettbewerbsrechts sowie der Spezialregulierung von Intermediären.[32]

2. Anmerkung zu einzelnen Vorschriften

Ich mache im Folgenden konkrete Vorschläge zur Verbesserung von einzelnen Vorschriften des TTDSG-E.

2.1 Zu § 2 Abs. 2 Nr. 1 (Definition des „Anbieters von Telemedien“)

Die Definition in § 2 Abs. 2 Nr. 1 TTDSG-E ist fast wortgleich zu der Definition von „Dienstanbieter“ in § 2 Nr. 1 TMG, allerdings sind in der Definition im TTDSG auch die Mitwirkenden erfasst.

Zwei sehr ähnliche Begriffe unterschiedlich zu definieren, dient nicht der Normenklarheit und führt in der Praxis dazu, dass nur spezialisierte Juristen das TTDSG-E rechtssicher anwenden können.

Besser wäre, aus § 2 Abs. 2 Nr. 1 TTDSG auf die Definition in § 2 Nr. 1 TMG zu verweisen oder die abweichende Definition im TTDSG ganz zu streichen.

[32] Potenziell anwendbare Regelungen finden sich - ohne dies weiter geprüft zu haben - im Medienstaatsvertrag (MStV), der Platform-to-Business-Verordnung (EU) 2019/1150) oder den noch im Entwurf befindlichen EU-Rechtsakten Digital Services Act (DSA) und Digital Markets Act (DMA)

2.2 Zu § 2 Abs. 2 Nr. 2 (Definition von „Bestandsdaten“)

Der Begriff „Bestandsdaten“ ist in § 3 Nr. 6 TKG-E[33] anders definiert als im TTDSG. Die Definition im TKG betrifft Bestandsdaten von TK-Diensteanbietern, die Definition in § 2 Abs. 2 Nr. 2 TTDSG Bestandsdaten von Telemedienanbietern.

Aufgrund von § 2 Abs. 1 TTDSG-E finden *beide* Definitionen auf das TTDSG Anwendung. Konkret: Die Definition aus § 2 Abs. 2 Nr. 2 TTDSG-E findet ausweislich ihres Wortlauts Anwendung auf Teil 3 des TTDSG, die Definition aus dem TKG aufgrund von § 2 Abs. 1 TTDSG-E auf den übrigen Teil. Das Wort „Bestandsdaten“ kommt zwar dort nicht vor. In späteren Novellen des TTDSG kann sich das allerdings wieder ändern.

Dass dasselbe Wort für unterschiedliche Abschnitte des TTDSG unterschiedlich definiert ist, dient nicht der Normenklarheit. Das Gesetz wäre deutlich leichter zu verwenden, wenn es für die Kundendaten von Telemediendiensteanbietern nicht den Begriff „Bestandsdaten“ verwenden würde, sondern stattdessen einen Begriff, der nicht bereits belegt ist, beispielsweise „Kundendaten von Telemediendiensteanbietern“ oder „Nutzerdaten“.

Falls der Ausschuss dieser Empfehlung folgen will, müsste er im gesamten TTDSG den Begriff „Bestandsdaten“ gegen den neu gewählten Begriff austauschen.

2.3 Zu § 2 Abs. 2 Nr. 6 (Definition von „Endeinrichtung“)

Der Begriff „Endeinrichtung“ ist in § 2 Abs. 2 Nr. 6 TTDSG-E wortgleich definiert wie der Begriff "Telekommunikationsendeinrichtung" in § 3 Nr. 62 TKG-E. Insofern stellt sich die Frage, ob es nicht sinnvoller wäre im TTDSG ebenfalls den Begriff „Telekommunikationsendeinrichtung“ zu verwenden, so dass keine zusätzliche Definition notwendig wäre.

Sollte der Ausschuss eine abweichende Bezeichnung für notwendig halten, so schlage ich den deutlich besser verständlichen Begriff „Endgerät“ vor. Dieser Begriff wird auch in der zugrundeliegenden deutschen Sprachfassung der ePrivacy-RL verwendet. Gemeint ist damit dasselbe wie die „Telekommunikationsendeinrichtung“ i.S.d. TKG.[34]

Falls der Ausschuss dieser Empfehlung folgen will, wäre im gesamten TTDSG der Begriff „Endeinrichtung“ durch „Endgerät“ zu ersetzen.

2.4 Zur amtlichen Überschrift von § 3 („Fernmeldegeheimnis“)

Es würde nicht nur die Verständlichkeit des TTDSG, sondern auch dessen Wirksamkeit verbessern, wenn statt „Fernmeldegeheimnis“ der modernere Begriff „Telekommunikationsgeheimnis“ verwendet würde. Der Begriff „Fernmeldegeheimnis“ wird zwar auch in Art. 10 GG verwendet, er wirkt aber antiquiert.

---

[33] Ich zitiere aus der Fassung des Regierungsentwurfs des TKMoG-E, BT-Drs. 19/26108.

[34] Sichtbar wird dies erst bei einem Blick auf die englische Sprachfassung der zugrundeliegenden EU-Richtlinien: Sowohl die ePrivacy-RL als auch die Richtlinie zum neuen Europäischen Kodex über die Elektronische Kommunikation (EKEK) verwenden den Begriff „Terminal Equipment“. Dieser ist definiert in Art. 1 Abs. 1 lit. a der Richtlinie 2008/63/EC.

Das Telekommunikationsgeheimnis ist aber keineswegs veraltet oder antiquiert. In Zeiten, in Menschen fortwährend elektronisch kommunizieren, ist es eines der wichtigsten Privatsphärenrechte überhaupt. Der Begriff „Fernmeldegeheimnis“ suggeriert, es ginge um eine Art Überbleibsel aus grauer Vorzeit. Genau das Gegenteil ist aber der Fall: Das Telekommunikationsgeheimnis war noch nie so wichtig und aktuell wie heute. Die Formulierung des § 3 TTDSG-E sollte dem Rechnung tragen.

Würde der Ausschuss dieser Empfehlung umsetzen, so wäre im gesamten TTDSG der Begriff „Fernmeldegeheimnis“ durch „Telekommunikationsgeheimnis“ zu ersetzen.

2.5 Zu § 4 TTDSG-E (Fernmeldegeheimnis und Erbrecht)

Diese Regelung soll offenbar die BGH-Entscheidungen i.S. „Digitaler Nachlass“[35] in Form einer gesetzlichen Regelung zementieren. Der Regierungsentwurf begründet dies mit weiterhin bestehender Rechtsunsicherheit.

Ich würde den Ausschuss an dieser Stelle darum bitten, kritisch zu prüfen, ob er die im Regierungsentwurf vorgeschlagene Regelung überhaupt für politisch sinnvoll hält. Dass der BGH auf Basis bestehenden Rechts zu der Auffassung gelangt ist, dass Erben unabhängig vom Fernmeldegeheimnis auf gespeicherte Telekommunikationsinhalte des Erblassers zugreifen können, heißt nicht, dass diese Entscheidung *de lege ferenda* auch politisch richtig ist.

Würde § 4 TTDSG-E so in Kraft treten, so könnten Erben auf vom Telekommunikationsgeheimnis geschützte Kommunikationsinhalte der jeweiligen Erblasser zugreifen. Häufig wären diese Erben entweder die Kinder, Eltern oder Ehepartner der verstorbenen Person.

Solchen engen Verwandten in § 4 TTDSG-E ein Zugriffsrecht einzuräumen, erscheint mir nicht sachgerecht. Denn das Geheimhaltungsinteresse derjenigen, die Telekommunikationsdienste nutzen, ist oft *gerade* auf Geheimhaltung gegenüber den eigenen Verwandten gerichtet. Wer befürchten muss, dass gespeicherte Telekommunikationsinhalte[36] nach dem Tod gegenüber engen Verwandten offengelegt werden, wird bereits zu Lebzeiten, während der Telekommunikation, deutliche Befangenheit spüren. Genau diese Einschüchterungswirkung zu vermeiden, ist aber der Sinn des Telekommunikationsgeheimnisses.[37]

Jede*r der Mitglieder des Ausschusses möge sich fragen, wie sie/er es fände, wenn die jeweiligen Erben nach deren Tod automatisch Zugriff auf alle Messenger-Nachrichten

---

[35] BGH, Urteil v. 12.07.2018, III ZR 183/17; BGH, Beschluss vom 27.08.2020 - III ZB 30/20.

[36] Unbenommen bleibt hier die Streitfrage, ob solche gespeicherten Nachrichten überhaupt noch vom Fernmeldegeheimnis betroffen sind. Instruktiv dazu *Neumann*, Kochneumann.de v. 3.3.2018, „Wer muss in eine Durchbrechung des Fernmeldegeheimnisses einwilligen?“, https://kochneumann.de/2018/03/03/wer-muss-in-eine-durchbrechung-des-fernmeldegeheimnisses-einwilligen/

[37] Statt vieler BVerfG, Urteil v. 14. Juli 1999 - 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95, Rn. 234: „Die Befürchtung einer Überwachung [...] kann schon im Vorfeld zu einer Befangenheit in der Kommunikation, zu Kommunikationsstörungen und zu Verhaltensanpassungen, hier insbesondere zur Vermeidung bestimmter Gesprächsinhalte oder Termini, führen.“

erhalten würden, die sie oder er auf verschiedenen Diensten verschickt hat.[38] In den allermeisten Fällen wäre das wohl nicht gewünscht.

Besser wäre es m.E., in § 4 zu regeln, dass das Fernmeldegeheimnis ein höchstpersönliches Rechtsgut ist, in das Erben *nicht* im Wege der Gesamtrechtsnachfolge eintreten können. Etwas anderes sollte nur gelten, wenn die jeweiligen Verstorbenen dies bei der Regelung ihres „digitalen Nachlasses" anders entschieden haben, beispielsweise durch Einstellungen in ihren Social Media-Profilen oder über eine Verfügung von Todes wegen.

In jedem Fall sollte in den § 4 aufgenommen werden, dass Einstellungen, die die Nutzer zur Regelung ihres „digitalen Nachlasses" selbst getroffen haben, gegenüber der Gesamtrechtsnachfolge der Erben und sonstigen Zugriffsrechten im Zusammenhang mit dem Erbfall (z.B. durch Testamentsvollstrecker) vorrangig sein sollten. Niemand sollte befürchten müssen, dass nach seinem Tod Dritte gegen den eigenen Willen auf höchst private Kommunikationsinhalte zugreifen.

2.6 Zu § 6 (Nachrichtenübermittlung mit Zwischenspeicherung)

Die Vorschrift ist m.E. mit höherrangigem EU-Recht nicht vereinbar und sollte gestrichen werden. Ich verweise auf Abschnitt 1.2.

2.7 Zu § 8 (Missbrauch von Telekommunikationsanlagen)

Auch in § 8 TTDSG-E könnte anstatt des Begriffs „Telekommunikationsanlage" der Begriff „Endgerät" verwendet werden. Das würde inhaltlich nichts ändern, aber der Verständlichkeit der Vorschrift dienen.

2.8 Zu § 9 Abs. 1 (Verarbeitung von Verkehrsdaten)

Die Vorschrift ist m.E. mit höherrangigem EU-Recht nicht vereinbar und sollte angepasst werden. Ich verweise auf Abschnitt 1.2.

2.9 Zu § 10 (Entgeltermittlung und -abrechnung)

Die Vorschrift ist m.E. mit höherrangigem EU-Recht nicht vereinbar und sollte angepasst werden. Ich verweise auf Abschnitt 1.2.

2.10 Zu § 12 Abs. 1 Satz 2 (Zugriff auf „Telekommunikations- und Datenverarbeitungssysteme der Nutzer")

Die Vorschrift entspricht im Wortlaut weitgehend dem bisherigen § 100 TKG. § 12 TTDSG-E wird zukünftig aber auch auf OTT-Diensteanbieter Anwendung finden.

Im Unterschied zu „klassischen" Telekommunikationsdiensten gibt es aber bei OTT-Diensten nicht immer Endgeräte. An deren Stelle tritt oft ein web-basierter Account. Das heißt die zugegangenen Kommunikationsinhalte werden nicht auf dem Endgerät des Nutzers gespeichert, sondern in einer „Mailbox" des Nutzers, auf die dieser über das Internet zugreift.

[38] Eine Offenlegung kann selbstverständlich ohnehin nur erfolgen, soweit der Anbieter darauf überhaupt Zugriff hat. Das ist nicht der Fall bei Diensten mit Ende-zu-Ende-Verschlüsselung.

Diese Accounts bzw. Mailboxen sollten aber gleichwertig geschützt werden wie die in § 12 Abs. 1 Satz 2 genannten „Telekommunikations- und Datenverarbeitungssysteme der Nutzer".

Ich würde deshalb vorschlagen, wie folgt umzuformulieren:

„Dies gilt auch für Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Telekommunikationsdiensten oder zu einem unerlaubten Zugriff ~~auf Telekommunikations- und Datenverarbeitungssysteme~~ auf Systeme, Daten oder Telekommunikationsinhalte der Nutzer führen können."

2.11 Zu § 12 Abs. 1 Satz 4 (Informationspflicht des Endnutzers bei Datenverarbeitung zur Datensicherheit)

Der letzte Satz von § 12 Abs. 1 TTDSG-E wirkt so, als sei der Endnutzer, der von einer Datenverarbeitung zu Sicherheitszwecken betroffen ist, immer zu benachrichtigen. Eine solche Regelung ist aber nicht sinnvoll; es käme sonst zu sehr vielen Benachrichtigungen, da grundsätzlich fast aller Datenverkehr im Internet in irgendeiner Weise automatisiert überwacht wird, um IT-Sicherheitsrisiken zu erkennen und einzudämmen. Gemeint ist offenbar, wie auch im vorigen Satz, der Fall einer *manuellen* Auswertung von Verkehrsdaten.

Demzufolge wäre der Satz umzuformulieren zu:

„In diesem Fall sind auch betroffene Endnutzer ~~sind~~ von dem nach § 3 Absatz 2 Satz 1 Verpflichteten zu benachrichtigen, sofern sie ermittelt werden können."

Durch die Hinzufügung wird klargestellt, dass die Benachrichtigungspflicht, wie der vorige Satz, nur im Fall der nicht-automatisierten Erhebung und Verwendung von Verkehrsdaten besteht.

2.12 Zu § 13 Abs. 1 (Standortdaten)

Die Vorschrift ist m.E. mit höherrangigem EU-Recht nicht vereinbar und sollte angepasst werden. Ich verweise auf Abschnitt 1.2.

Unabhängig davon sollten im letzten Satz die Worte „seines Mobilfunkanschlusses" durch „seines Telekommunikationsdienstes" ersetzt werden. Denn der Wortlaut der Vorschrift wird sich nach dem TTDSG nicht nur auf klassische Mobilfunkangebote beziehen, sondern auch auf OTT-Dienste. Dort gibt es aber keine Mobilfunkanschlüsse.

2.13 Zu § 14 Abs. 1 (Mitteilen ankommender Verbindungen)

Im Wortlaut der Vorschrift sollte klargestellt werden, dass sie sich nur auf Sprachkommunikationsdienste bezieht, also nur auf nummerngebundene Dienste (vgl. § 3 Nr. 55 TKG-E). So ist sie offenbar gemeint, aber der Wortlaut sagt es nicht eindeutig.

2.14 Zu § 15 Abs. 3 (Verbot der Rufnummernunterdrückung bei Werbeanrufen)

Diese Regelung ist politisch zwar sinnvoll, an dieser Stelle des Gesetzes aber ein Fremdkörper. Während die übrigen Absätze des § 15 TTDSG-E Pflichten von TK-

Diensteanbietern regeln, regelt dieser Absatz die Pflichten der Anrufer. Und inhaltlich geht es hier um eine spezielle Vorschrift zur Direktwerbung.

Systematisch passend eingeordnet wäre die Vorschrift in den §§ 113 ff. TKG (z.B. als neuer Absatz des § 119 TKG-E) oder als neuer Absatz in § 7 UWG.

2.15 Zu § 22 Abs. 3 Nr. 8 TTDSG-E

Hier wird eine weitere Berechtigung für den BND geschaffen, Ermittlungen auch im Inland und gegen Personen im Inland durchzuführen.[39]

Diese gesetzliche Änderung ist Teil der sehr bedenklichen Entwicklung, den Auslandsgeheimdienst BND zu einer Art „Super-Sicherheitsbehörde“ auszubauen, die eine Vielzahl von neuen Aufgaben und Kompetenzen erhält, die teils in Richtung eines Inlandgeheimdienstes und teils in Richtung einer geheim agierenden Polizeibehörde gehen. Im vorliegenden Fall erhält der BND die Möglichkeit, von Internet-Diensteanbietern vertrauliche Informationen über Personen im In- und Ausland herauszuverlangen, ohne dass diese davon etwas erfahren. Die Tatbestandsmerkmale des § 22 Abs. 3 Nr. 8 TTDSG-E schränken den BND dabei nicht relevant ein, denn die Voraussetzung des Buchstaben a) entsprechen dem Aufgabenprofil des BND (vgl. § 1 Abs. 2 BNDG). Der BND darf also die Daten erheben, die er braucht, und unterliegt keinen weiteren Beschränkungen.

Eine derart weite Berechtigung zum Datenabruf dürfte verfassungswidrig sein. Notwendig sind effektive gesetzliche Schutzmaßnahmen zum Schutz des Grundrechts auf informationelle Selbstbestimmung.

Diese Vorschrift ist außerdem auch aus einem zweiten Grund verfassungsrechtlich bedenklich. Sie könnte dazu führen, dass der BND seine Befugnis zur verdachtsfreien „Schleppnetzfahndung“ in Telekommunikationsverkehren nicht mehr ausüben darf. Diese Befugnis darf der BND nur ausüben, weil er im Inland keine operativen Befugnisse hat.[40] Genau solche Befugnisse gewinnt der BND (nicht nur) hier aber hinzu.

2.16 Zu § 22 Abs. 4 Satz 1

An Stelle der Worte „Auskunft nach Abs. 1 Satz 3“ sollte hier im Interesse der Normenklarheit stehen, was (wohl) gemeint ist: Eine „Auskunft auf Basis einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse (Abs. 1 Satz 3)“.

2.17 Zu § 23 (Herausgabepflicht von Passwörtern und sonstigen Zugangsdaten)

An der Sinnhaftigkeit dieser Vorschrift habe ich Zweifel. Ein Telemedienanbieter, die Passwörter oder sonstige Authentifizierungscodes des Nutzers im Klartext speichert, würde eindeutig seine gesetzlichen Pflichten nach § 19 TTDSG-E und Art. 32 DSGVO verletzen. Solche „Zugangsdaten“ wird es in aller Regel also gar nicht geben.

---

[39] Nach dem Wortlaut der Vorschrift muss lediglich das *Ziel* der Ermittlungen auf "Informationen über das Ausland" gerichtet sein. Ermitteln darf der BND aber gegenüber *Personen* im Inland.
[40] Vgl. BVerfG v. 19.05.2020 - 1 BvR 2835/17, fünfter Leitsatz.

Was es, je nach Anbieter, geben mag sind Zugriffsmöglichkeiten auf die von Nutzern eingespeicherten Daten von Anbieterseite (z.B. über einen Admin-Zugang). Von solchen Admin-Zugängen spricht die hiesige Vorschrift aber nicht, so dass wohl weder ein Admin-Zugang noch die darüber abrufbaren Daten herausgegeben werden müssen.

Ich hoffe, dass diese Anmerkungen hilfreich sind und verbleibe

mit freundlichen Grüßen

Dr. Simon Assion
Rechtsanwalt