RECHTSGUTACHTEN

ÜBER DIE

„RECHTLICHEN RAHMENBEDINGUNGEN DER AUSGESTALTUNG SEKTORSPEZIFISCHER ZULÄSSIGKEITSTATBESTÄNDE UND INSBESONDERE DER EINWILLIGUNG IN DER EPRIVACY-VO“

ERSTELLT VON

UNIV.-PROF. DR. IUR. JÜRGEN KÜHLING, LL.M.

REGENSBURG

IM AUFTRAG FOLGENDER VERBÄNDE:

BUNDESVERBAND DEUTSCHER ZEITUNGSVERLEGER E.V. (BDZV)
BUNDESVERBAND DIGITALE WIRTSCHAFT. E.V. (BVDW)
DEUTSCHER DIALOGMARKETING VERBAND E.V. (DDV)
GESAMTVERBAND DER KOMMUNIKATIONSAGENTUREN E.V. (GWA) / ORGANISATION DER MEDIAAGENTUREN E.V. (OMG)
HANDELSVERBAND DEUTSCHLAND E.V. (HDE)
MARKENVERBAND E.V. / ORGANISATION WERBUNGTREIBENDE IM MARKENVERBAND (OWM)
VERBAND DEUTSCHER AUSKUNFTS- UND VERZEICHNISMEDIEN E.V. (VDAV)
VERBAND PRIVATER MEDIEN E.V. (VAUNET)
VERBAND DEUTSCHER ZEITSCHRIFTENVERLEGER E.V. (VDZ)
ZENTRALVERBAND DER DEUTSCHEN WERBEWIRTSCHAFT E.V. (ZAW)

REGENSBURG, DEN 16. OKTOBER 2019

Gliederung

A. Sachverhalt

Auf der Basis der mir von den Auftraggebern zur Verfügung gestellten Informationen ergibt sich folgender Sachverhalt:

I. Überblick: Stand des Gesetzgebungsverfahrens zur ePrivacy-VO und Streitpunkte

Am 10. Januar 2017 hat die Kommission einen Vorschlag für eine Verordnung zum „Schutz der Privatsphäre in der elektronischen Kommunikation“ [1] vorgelegt (Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC; Regulation on Privacy and Electronic Communications, im Folgenden kurz „ePrivacy-VO-E (KOM)“). Die Verordnung (allgemein im Folgenden kurz „ePrivacy-VO-E“) soll parallel zu der bereits 2016 abgeschlossenen Novellierung des allgemeinen Datenschutzrechts durch die Datenschutz-Grundverordnung (im Folgenden DS-GVO), die an die Stelle der vorherigen allgemeinen Datenschutzrichtlinie 95/46/EG getreten ist, für den Spezialbereich der elektronischen Kommunikation die bislang geltende ePrivacy-Richtlinie 2002/58/EG modernisieren und vor allem ihren Anwendungsbereich auf sämtliche Anbieter elektronischer Kommunikation ausweiten.

Der Vorschlag befindet sich noch immer im Gesetzgebungsverfahren. Nach der Stellungnahme des Europäischen Parlaments[2] (im Folgenden kurz „ePrivacy-VO-E (EP)“) wird gegenwärtig eine gemeinsame Ratsposition abgestimmt[3] (im Folgenden kurz „ePrivacy-VO-E (Rat)“.

Besonders umstritten ist dabei, ob, in welchem Umfang und mit welcher spezifischen Ausgestaltung gegenüber der DS-GVO (dort vor allem Art. 6 und 7) abweichende Zulässigkeitstatbestände für die Datenverarbeitung geschaffen werden sollen. Das gilt gerade auch für einen möglichen eigenständigen Einwilligungstatbestand. Hier ist insbesondere mit Blick auf den Entwurf des Art. 8 ePrivacy-VO-E umstritten, inwiefern eine einwilligungsbasierte Verarbeitung in Bezug auf den Zugang zu und die Speicherung von Informationen auf Endgeräten seitens des Diensteanbieters unter Bedingungen gestellt werden kann, die eine datenfinanzierte Erbringung von Diensteange-

---

1 Vorschlag der Europäischen Kommission vom 10.1.2017, (COM(2017) final 2017/0003 (COD).
2 Legislative Entschließung des Europäischen Parlaments vom 23.10.2017, A8-0324/2017.
3 Version vom 4.10.2019, Dok. Nr. 12633/19.

boten ermöglicht. Ebenfalls umstritten ist aber auch die allgemeine Einwilligung nach Art. 9 ePrivacy-VO-E.

Mögliche Einschränkungen und Erschwernisse bei den Zulässigkeitstatbeständen allgemein bzw. bei der Einwilligung im Besonderen betreffen die gesamte Werbebranche. Ja nach Ausgestaltung kann dies einen erheblichen (negativen) Einfluss auf die Einnahmemöglichkeiten werbefinanzierter Mediengebote haben.

Im Folgenden werden die gutachterlich zu untersuchenden Bestimmungen der verschiedenen Vorschläge für eine ePrivacy-VO-E (KOM/EP/Rat) dargelegt (II.). Im Anschluss hieran werden die betroffenen Geschäftsmodelle, soweit dies für die rechtliche Begutachtung erforderlich ist, aufgezeigt (III.), um sodann die von verschiedenen Studien und Marktanalysen erwarteten Folgen der jeweiligen Bestimmungen für die Geschäftsmodelle nachzuvollziehen (IV.).

II. Die zu untersuchenden Bestimmungen nach den Vorschlägen für eine ePrivacy-VO

1. Endgeräteschutz: umfassendes Verbot mit enumerativen Zulässigkeitstatbeständen

Anknüpfend an den Entwurf der Kommission ist nach den Vorschlägen des Europäischen Parlaments und des Rats jedwede Nutzung endgerätebezogener Datenverarbeitungsmöglichkeiten verboten, es sei denn sie erfolgt durch den Endnutzer selbst (Art. 8 Abs. 1 ePrivacy-VO-E). Art. 8 Abs. 1 ePrivacy-VO-E enthält in allen Vorschlägen von Kommission, Europäischem Parlament und Rat eine abschließende Liste von Tatbeständen, die erfüllt müssen, damit die Verarbeitung ausnahmsweise zulässig ist.

2. Die Einwilligung und ihre Wirksamkeit in Fällen des Bedingungszusammenhangs („Kopplungsverbot/Entkopplungsgebot")

Die Einwilligung des Endnutzers ist nach allen Vorschlägen von Kommission, Europäischem Parlament und Rat ein hinreichender Zulässigkeitstatbestand zur Datenverarbeitung, Art. 8 Abs. 1 lit. b ePrivacy-VO-E.[4] Nach gesicherter Dogmatik des (europäischen und nationalen) Datenschutzrechts

[4] Nach der Version des Europäischen Parlaments muss die Einwilligung allerdings „ausdrücklich" erfolgen, womit besondere Anforderungen an die Art und Weise der Willensbekundung, vergleichbar Art. 7 DSGVO, gestellt werden.

und entsprechender Formulierung in der DS-GVO muss sie freiwillig erfolgen.[5] Eine Bewährungsprobe für das Wirksamkeitskriterium der Freiwilligkeit liegt in der Frage, inwieweit die Erbringung eines Internetangebots, das durch Werbung voll- oder teilfinanziert ist und bei dem zu diesem Zweck Endgerätedaten im Sinne von Art. 8 Abs. 1 ePrivacy-VO-E verarbeitet werden, davon abhängig gemacht werden darf, dass der Endnutzer in diese Datenverarbeitung einwilligt. Die Thematik wird in der laufenden Debatte unter dem wenig objektiven Begriff der „Tracking- oder Cookie-Walls" diskutiert.[6]

a) Vorschlag der Kommission

Der Vorschlag der Kommission trifft hierzu keine explizite Regelung. Im verfügenden Teil des Entwurfs wird festgestellt, dass die Begriffsbestimmung und die Voraussetzungen, die in Art. 4 Nr. 11 und Art. 7 DS-GVO niedergelegt sind, gelten, Art. 9 ePrivacy-VO-E (KOM). Dem einschlägigen Erwägungsgrund 18 des Vorschlags der Kommission sind ebenfalls keine spezifische Positionierung oder Beurteilungskriterien zur Beantwortung der Frage in Bezug auf Internetangebote zu entnehmen.[7] In einem ersten Diskussionsentwurf für eine ePrivacy-VO waren immerhin Anhaltspunkte für die Beurteilung der Fallkonstellation insofern angeklungen, als alternativ am Markt verfügbare Angebote und die Bezahlbarkeit im Fall von geldzahlungsbasierten Varianten als Kriterien für die Beurteilung der Freiwilligkeit einer Einwilligung genannt werden.[8]

Nach den Verlautbarungen der Aufsichtsbehörden zur Auslegung der DS-GVO führt die Koppelung der Erbringung einer vertraglichen Dienstleistung an die Abgabe einer datenschutzrechtlichen Einwilligung bei Internetangeboten *„regelmäßig dazu, dass die Einwilligung nicht als freiwillig*

---

5 Vgl. Art. 29-Datenschutzgruppe, Arbeitspapier (WP) 259 rev. 01 v. 10.4.2018; *Buchner/Kühling*, in: Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung/BDSG, Kommentar, 2. Aufl. 2018, Art. 7 DS-GVO, Rn. 48; *Engeler*, ZD 2018, 55 ff m.w.N.

6 Vgl. die Stellungnahme 6/2017 des *EDSB* zu dem Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation(E-Privacy-VO), S. 21; abrufbar unter https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf (letzter Abruf 15.10.2019)

7 Erwägungsgrund 18 ePrivacy-VO-E (KOM) lautet: „Grundlegende breitbandige Internetzugangs- und Sprachkommunikationsdienste gelten als unverzichtbare Dienste, damit Personen kommunizieren und an den Vorteilen der digitalen Wirtschaft teilhaben können. Eine Einwilligung in die Verarbeitung von Daten aus der Benutzung von Internet-oder Sprachkommunikationsdiensten ist unwirksam, wenn die betroffene Person keine echte und freie Wahl hat oder ihre Einwilligung nicht verweigern oder widerrufen kann, ohne Nachteile zu erleiden." Es ist unklar, inwieweit sich die Formulierung insgesamt ausschließlich auf Access-Provider und digitale Telekommunikationsdienste bezieht.

8 Siehe Erwägungsgrund 22 einer inoffiziellen Version des Entwurfs der Kommission abrufbar unter http://www.politico.eu/wp-content/uploads/2016/12/POLITICO-e-privacy-directive-review-draft-december.pdf (letzter Abruf 15.10.2019).

angesehen werden könne und damit unwirksam" sei[9]. Der Besuch einer Webseite soll hiernach *„auch dann noch möglich sein, wenn betroffene Personen sich gegen das Setzen von Cookies entscheiden und nicht in die personenbezogene Datenverarbeitung einwilligen."*[10]

b) Vorschlag des Europäischen Parlaments

Der Vorschlag des Europäischen Parlaments beantwortet die Frage eindeutig. Jedweder Bedingungszusammenhang zwischen Diensterbringung und der Erteilung einer Einwilligung ist nach Art. 8 Abs. 1a ePrivacy-VO-E (EP) ausgeschlossen: *„Unabhängig davon, ob es sich um einen vergüteten Dienst handelt, darf keinem Nutzer der Zugang zu einem Dienst oder einem Funktionselement der Informationsgesellschaft mit der Begründung verweigert werden, er habe seine Einwilligung in die Verarbeitung personenbezogener Daten bzw. in die zur Bereitstellung dieses Dienstes oder dieses Funktionselements nicht erforderliche Nutzung von Verarbeitungs- oder Speicherkapazitäten seiner Endeinrichtung nach Artikel 8 Absatz 1 Buchstabe b nicht gegeben."* Damit konstruiert das Europäische Parlament einen Kontrahierungs- bzw. Lieferzwang, der Internetangebote, sofern die Verarbeitung nicht erforderlich ist, bei Nichterteilung einer Einwilligung dennoch zur vollen Diensterbringung verpflichtet. Dabei soll die Bestimmung in Fällen, in denen das Angebot für den Nutzer direkt geldzahlungspflichtig ist, genauso greifen, wie wenn der Dienst durch datenbasierte Online-Werbung refinanziert wird. Entscheidend für die Beurteilung ist das Merkmal der *„nicht erforderlichen Nutzung"*. Es dürfte der Intention und Ratio der Regelung entsprechen, hierzu den Erlaubnistatbestand des Art. 8 Abs. 1 lit. b ePrivacy-VO-E (EP) heranzuziehen. Damit wird klar, dass der Lieferzwang weiträumig angelegt ist. Daten, die einwilligungsbasiert bei einem Bezahlangebot erhoben werden, aber zu anderen Zwecken als der vereinbarten „subscription" verarbeitet werden, (z.B. um auf andere Pay-Angebote oder Tarife aufmerksam zu machen), würden dem Kopplungsverbot unterfallen. Dasselbe würde gelten, wenn ein angeforderter Dienst durch datenbasierte Online-Werbung refinanziert wird, mithin für den Nutzer nicht geldzahlungspflichtig ist, der Endnutzer hierin aber nicht einwilligen will: Der Webseiteninhalt müsste dennoch zur Verfügung gestellt werden.

---

9 Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, Stand März 2019, S. 10, abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf (letzter Abruf 15.10.2019).

10 A.a.O. (Fn. 10) unter Berufung auf Art. 29-Datenschutzgruppe, a.a.O. (Fn. 7), S. 10 f.

Im Rahmen der Erläuterung und weiteren Ausgestaltung dieses Ansatzes referenziert das EP auf die Freiwilligkeit der Einwilligung. Erwägungsgrund 18 ePrivacy-VO-E (EP) lautet: *„Die Einwilligung sollte nicht als freiwillig gelten, wenn sie erforderlich ist, um Zugang zu einer Dienstleistung zu erhalten, oder wenn sie durch wiederholte Aufforderungen erwirkt wird. Um solche missbräuchlichen Aufforderungen zu verhindern, sollten die Nutzer in der Lage sein, Diensteanbieter anzuweisen, ihre Entscheidung, nicht einzuwilligen, zu speichern und sich nach technischen Spezifikationen zu richten, durch die eine nicht erteilte Einwilligung, ein Widerruf der Einwilligung oder ein Widerspruch angezeigt wird."* Damit schließt bereits die wiederholte Anfrage, eine Einwilligung zu erteilen, die Freiwilligkeit und damit zugleich der Wirksamkeit einer erteilten Einwilligung aus. Die Formulierung kann weiterhin so verstanden werden, dass entsprechende Praktiken zu unterbleiben haben.

Nach alledem ist der Anbieterseite die Möglichkeit verwehrt, auf die Nicht-Erteilung der Einwilligung zu reagieren. Weder die Nichterbringung seiner Dienstleistung oder Einschränkungen des Dienstumfangs noch auch nur eine spätere Kontaktaufnahme zwecks Erteilung der Einwilligung sind nach dem Vorschlag des Europäischen Parlaments zulässig. Schließlich drückt der Erwägungsgrund 18 aus, dass vorstehende Maßgaben auch für die Situation eines Widerrufs einer einmal erteilten Einwilligung und, wenngleich systematisch nicht ganz klar, auch für den Fall eines Widerspruchs des Endnutzers zur Anwendung kommen soll.[11]

c) Aktuelle Version der Ratsvorschläge

Die aktuelle Version der Ratsvorschläge verweist zunächst auf die einschlägigen Bestimmungen der DS-GVO zur Einwilligung, Art. 4a Abs. 1 ePrivacy-VO-E (Rat). In Erwägungsgrund 20 wird sodann zur Beurteilung von Konstellationen eines Bedingungszusammenhangs ausgeführt, dass es normalerweise („normally") nicht unverhältnismäßig sei, den Zugang zu Webseiteninhalten, die ohne direkte monetäre finanzielle Leistung des Endnutzers zur Verfügung gestellt werden, von der Erteilung einer Einwilligung in das Speichern eines Cookie und dem Auslesen von hierin

[11] Eine allgemeine oder auf Werbung bezogene Widerspruchsregelung (siehe Art. 21Abs. 1, 2 DSGVO) kennt die ePrivacy-VO-E in Ermangelung eines gesetzlichen Zulässigkeitstatbestands vergleichbar Art. 6 Abs. 1 lit. f DS-GVO auch nach dem Vorschlag des Europäischen Parlaments nicht. Möglicherweise meint das Europäische Parlament mit „Widerspruch" technische Einstellungen, z.B. im Browser von Endnutzern, mittels derer die Datenverarbeitung im Sine von Art. 8 ePrivacy-VO-Everhindert/geblockt werden kann. Das Gerbrauchmachen derartiger technischer Anwendungen dürfte in diesem Fall nicht dazu führen, dass der Anbieter die Diensterbringung einschränkt oder um Deaktivierung der Software bittet.

gespeicherten Informationen zu zusätzlichen Zwecken („additional purposes“) abhängig zu machen, wenn bestimmte, nicht abschließend aufgeführte, Bedingungen erfüllt seien. Davon sei unter anderem auszugehen, wenn der Endnutzer zwischen einem Angebot, das einen Bedingungszusammenhang enthalte und einem gleichwertigen („equivalent“) Angebot desselben Anbieters („by the same provider“), das bedingungsfrei, also ohne Einwilligungserfordernis, nutzbar sei, auswählen könne.

Die Aussagen des Erwägungsgrundes, der die Auslegung der Regelungen der DS-GVO für die exemplarisch herausgestellte Speicher- und Verarbeitungstechnologie „Cookie“ spezifizieren und mit Vorrang determinieren soll (Art. 1 Abs. 3 ePrivacy-VO-E (Rat)) sind auslegungsbedürftig. Tatbestandlich einschlägig ist der Erwägungsgrund nur dann, wenn ein Internetangebot ohne Zahlungsverpflichtungen des Endnutzers („without direct monetary payment“) in Rede steht, worunter begrifflich-systematisch voll- aber auch teilweise werbefinanzierte Geschäftsmodelle fallen. Die zur Bedingung erhobene Einwilligung muss nach Erwägungsgrund 20 zu zusätzlichen Zwecken erfolgen. Nach dem Wortlaut und bei systematischer Betrachtung des gesamten Erwägungsgrunds werden hierunter diejenigen Verarbeitungszwecke fallen, die nicht bereits durch die Zulässigkeitstatbestände in Art. 8 Abs. 1 ePrivacy-VO-E (Rat) unmittelbar legitimiert sind. Geschäftsmodelle, bei denen eine endgerätebezogene Datenverarbeitung zwecks der Schaltung von Online-Werbung erfolgt, unterfallen demnach dem Erwägungsgrund.

Die Beurteilung der Freiwilligkeit der Einwilligung und damit ihre Wirksamkeit wird mit dem Begriff der Verhältnismäßigkeit in Verbindung gebracht. Dieser Maßstab ist der DS-GVO in Art. 7 Abs. 4 nicht unbekannt. Für Sachverhalte, bei denen die Erteilung einer Einwilligung im Zusammenhang mit der Erfüllung eines Vertrags oder der Erbringung einer Dienstleistung zur Bedingung erhoben wurde, kommt es hiernach auf die „Erforderlichkeit“ der Datenverarbeitung zur Vertragserfüllung an. Erwägungsgrund 20 ePrivacy-VO-E (Rat) weicht hiervon dennoch ab. Der in dem Erwägungsgrund ausformulierte Test stellt bei genauerer Betrachtung nicht auf eine Verhältnismäßigkeitsprüfung ab. Die Frage nach der Erforderlichkeit der Datenverarbeitung zur Bereitstellung eines Internetangebots ist hiernach nicht maßgeblich. Der Vorschlag kann deshalb auch nicht als Fortsetzung oder Spezialisierung des Regelungskonzepts der DS-GVO eingeordnet werden. Nach dem Erwägungsgrund hängt die Zulässigkeit eines Bedingungszusammenhangs zwischen der Einwilligung zu dem Zweck „Online-Werbung“ und der Diensterbringung allein davon ab, ob derselbe Anbieter ein vergleichbares Angebot ohne Bedingungszusammenhang zur

Verfügung stellt. Was unter dem für das Ergebnis des Vergleichs letztlich entscheidenden Begriff der Gleichwertigkeit zu subsumieren ist, wird indes nicht ausgeführt. In jedem Fall aber statuiert der Ratsvorschlag für werbefinanzierte Internetangebote immer das Erfordernis eines alternativen Zugangs ohne datenbezogenes Einwilligungserfordernis zum Zwecke der Online-Werbung.

Für bestimmte Angebote, der Erwägungsgrund benennt beispielsweise Dienste von Behörden („provided by public authorities"), soll ein Bedingungszusammenhang schlechthin unverhältnismäßig und damit unzulässig sein. Dies ist der Fall, wenn und soweit die Inanspruchnahme des Angebots für den Endnutzer alternativlos oder quasi-alternativlos ist. Damit wird ein Gedanke ins Spiel gebracht, der, weil marktbezogen, auch aus der Sicht der Endnutzer tragfähige Differenzierungen zur Freiwilligkeit der Einwilligung erlauben könnte. Zugleich vermengt Erwägungsgrund 20 in der Version des Rats jedoch unterschiedliche Bezugsperspektiven unter dem Begriff der Verhältnismäßigkeit und trägt damit weder zur Rechtsklarheit noch zu einer sinnvollen Rechtsanwendung bei.

3. Die weiteren Erlaubnistatbestände

Bei minimalen Abweichungen zwischen den Vorschlägen der Kommission, des Europäischen Parlaments und des Rates enthält Art. 8 Abs. 1 ePrivacy-VO-E keine weiteren Erlaubnistatbestände, die zu werbewirtschaftlichen Zwecken in Gestalt einer auf Endgeräte bezogenen datenverarbeitenden Schaltung von Online-Werbung genutzt werden können.

Die Erlaubnis nach Art. 8 Abs. 1 lit. a ePrivacy-VO-E erfasst lediglich Verarbeitungen zum technischen Zweck der Übermittlung eines elektronischen Kommunikationsvorgangs über ein elektronisches Kommunikationsnetzwerk.

Art. 8 Abs. 1 lit. d ePrivacy-VO-E beinhaltet ungeachtet der Unterschiede bei der näheren Ausgestaltung zwischen den einzelnen Vorschlägen des Europäischen Parlaments, der Kommission und des Rats die Erlaubnis, Reichweitenmessungen über die Nutzung eines Internetangebots durchzuführen.[12] Die hiernach erlaubte digitale Auflagenmessung ist funktional vergleichbar

[12] Aus datenschutzrechtlicher Sicht fällt auf, dass die Erlaubnis nach allen Versionen noch nicht auf grundlegende Kategorien der DS-GVO eingestellt ist. Art. 8 Abs. 1 lit d ePrivacy-VO-E lässt die Durchführung für die in der Praxis nahezu immer gegebene arbeitsteilige Organisation von Datenverarbeitungsprozessen nur nach Maßgabe der Regelungen zur Auftragsverarbeitung zu, was nach der mittlerweile ergangenen Rechtsprechung des EuGH zur Einordnung datenschutzrechtlicher Verantwortlichkeiten (siehe EuGH, Urt. v. 29.7.2019, Rs. C-40/17, ECLI:EU:C:2019:629 – *Fashion ID* m.w.N. zu den vorausgegangenen Entscheidungen des Gerichts) mit der

Auflagenmessungen bei Printmedien oder TV-Quoten. Wie diese sind auch digitale Reichweitendaten in der Regel eine Voraussetzung, um ein Internetangebot überhaupt als Werbeträger am Markt platzieren zu können. Digitale Reichweitenmessungen sind jedoch konzeptionell nicht für Online-Werbeschaltungen nutzbar und hierauf auch nicht ausgerichtet. Der Erlaubnistatbestand erlaubt überdies nach sämtlichen Versionen auch keinerlei Verarbeitung von Daten zu dem Zweck, Online-Werbung auf einem Endgerät (nutzerbezogen) zu schalten.

Art. 8 Abs. 1 lit d ePrivacy-VO-E legitimiert die endgerätebezogene Verarbeitung soweit sie erforderlich ist, um ein von einem Endnutzer angefordertes Internetangebot erbringen zu können. Die Auslegung des Begriffs der Notwendigkeit ist nach der Version des Europäischen Parlaments qualifiziert: Die Verarbeitung muss hiernach „zwingend technisch notwendig sein", um das angeforderte Internetangebot erbringen zu können. Der Begriff der „Notwendigkeit zur Diensterbringung" – hierauf stellt die Version der Kommission ab – ist aus der ePrivacy-RL bekannt, Art. 5 Abs. 3 der e-Privacy-RL. Er erfasst nach Ansicht der Datenschutzaufsichtsbehörden keinerlei auf die Finanzierung von Internetangeboten ausgerichtete werbewirtschaftlichen Verarbeitungszwecke und -vorgänge.[13] Die Erwägungsgründe zu den Vorschlägen einer ePrivacy-VO (nach der Version der Kommission wie auch des Europäischen Parlaments) sind überdies so zu verstehen, dass es hierbei bleiben soll.[14] Lediglich in der Version des Rates wird in Erwägungsgrund 21 a.E. eine andere Position eingenommen: Die endgerätebezogene Verarbeitung kann hiernach als erforderlich angesehen werden, wenn das von einem Endnutzer angeforderte Internetangebot durch Werbung vollständig oder teilweise finanziert wird, der Endnutzer über die zu diesem Zweck erfolgende Datenverarbeitung transparent informiert wurde und er diese Verarbeitung akzeptiert.[15]

---

starken Betonung einer gemeinsamen Verantwortung i.S.v. Art. 26 ff. DS-GVO kaum tragfähig sein dürfte, um den Zulässigkeitstatbestand zu nutzen.

13 Vgl. nur Art. 29-Datenschutzgruppe, WP 171 vom 22.6.2010, S. 10; Opinion 04/2012 194, v. 7.6.2012, abrufbar unter https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf (letzter Abruf 15.10.2019).

14 Vgl. jeweils Erwägungsgrund 21.

15 Die Formulierung lautet insoweit: *„In some cases the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment may also be necessary for providing an information society service, requested by the end-user, that is wholly or mainly financed by advertising provided that, in addition, the end-user has been provided with clear, precise and user-friendly information about the purposes of cookies or similar techniques and has accepted such use."* Der Terminus „accepted such use" ist nicht eindeutig. Der Erwägungsgrund trifft indes nur dann eine verwertbare Aussage, wenn hiermit nicht die Einwilligung des Endnutzers gemeint ist, sondern die tatsächliche Nutzung des Dienstes durch den Endnutzer unter Einschluss der anbieterseitig vorgesehenen Datenverarbeitung zu Werbezwecken.

Alle weiteren, vom EP und dem Rat (im Vergleich zur Version der KOM) eingefügten gesetzlichen Erlaubnistatbestände in Art. 8 Abs. 1 ePrivacy-VO-E stehen ersichtlich in keinem operativen Sachzusammenhang zur werbewirtschaftlichen Refinanzierung von Internetangeboten.

III. Übersicht über die betroffenen Geschäftsmodelle

Internetangebote finanzieren sich im Wesentlichen entweder durch digitale Vertriebserlöse oder durch Online-Werbung. In der Praxis sind auch Mischmodelle anzutreffen.

Weil digitale Vertriebserlöse („pay-Angebote") für die allermeisten Internetangebote, insbesondere der Anbieter redaktionell-journalistischer Dienste, gering ausfallen, haben digitale Anzeigenerlöse zur Refinanzierung der Inhalte eine herausragende Bedeutung.[16]

Die Auslieferung von Online-Werbung basierend auf der Segmentierung/Kategorienbildung anhand von Zielgruppenmerkmalen ist hierfür unverzichtbar. Die Schaltung von Online-Werbung aufgrund von rein kontextualen Kriterien (sog. Umfeldbuchung) ohne endgerätebezogene Datenverarbeitungen spielt in quantitativer und qualitativer Hinsicht, d.h. dem Umfang nach und gemessen an den hierfür erzielbaren Anzeigenpreisen, eine absolut untergeordnete Rolle.[17] Aufgrund der Menge an Inhalten im Internet und der Möglichkeiten, diese online abzurufen, sowie einem entsprechend thematisch extrem stark segmentierten digitalen Mediennutzungsverhalten der Verbraucher, besteht für werbefinanzierte Angebote die Notwendigkeit, Online-Werbung zielgruppenspezifisch platzieren zu können. Hierdurch wird eine hinreichende Werbeeffektivität und damit Wettbewerbsfähigkeit auf dem Werbemarkt erzielt.[18]

---

16 Vgl. *PWC,* German Entertainment & Media Outlook 2018-2022 (Zeitungsmarkt), abrufbar unter: https://www.pwc.de/de/technologie-medien-und-telekommunikation/german-entertainment-and-media-outlook-2018-2022/zeitungsmarkt.html (letzter Abruf 15.10.2019); zur Bedeutung von Online-Werbung als Erlösquelle s.a. *BKartA*, Online-Werbung, in: Wettbewerb und Verbraucherschutz in der digitalen Wirtschaft, Februar 2018, S. 7 ff.

17 Werbung, die ohne datenverarbeitende Technologien, insbesondere Cookies, ausgespielt wird, führt laut einer aktuellen empirischen Studie von *Google* bei digitalen Verlagsangeboten zu Umsatzeinbrüchen von mehr als 50 Prozent, abrufbar unter https://ppc.land/ads-without-cookies-represent-52-less-revenue-for-the-publishers-google-finds/ (letzter Abruf 15.10.2019).

18 *Reisch/Büchel/Joos/Zander-Hayat*, Digitale Welt und Handel: Verbraucher im personalisierten Online-Handel. Veröffentlichungen des Sachverständigenrats für Verbraucherfragen. Berlin, 2016; siehe auch *WIK,* Economic Impact of the ePrivacy Regulation on Online Advertising and Ad-based Digital Business Mo-del, 2017, https://www.wik.org/fileadmin/Studien/2017/2017_ePrivacy-BMW.pdf (letzter Abruf 15.10.2019); *BKartA*, a.a.O. (Fn. 17), S. 4 ff.

Der weitaus größte Anteil digitaler Werbeerlöse und nahezu das vollständige Wachstum des Gesamtmarktes infolge der weiter voranschreitenden Verlagerung von Werbebudgets in digitale Kanäle wird im deutschen und europäischen Markt von sehr wenigen (US-amerikanischen) Plattformen mit enormer Reichweite und Nutzerzahlen und umfassender technologischer Exzellenz erzielt.[19] Werbebezogene Datenverarbeitungsbefugnisse werden hier über Log-In-Prozesse, oftmals unter Erhebung von Klardaten, eingeholt. Die jeweiligen Datenverarbeitungsprozesse werden dabei im Rahmen proprietärer Systeme vollumfänglich alleinverantwortlich durchgeführt.

Demgegenüber steht eine Mehrheit an Onlineangeboten mit einem selbst in der Gesamtaddition im Vergleich zu den marktdominanten Plattformen weitaus geringeren Marktanteil bei den digitalen Werbeerlösungen. Die werbewirtschaftliche Datenverarbeitung wird hier im Wege der Zusammenarbeit mit Dritten („Werbepartnern") arbeitsteilig organisiert. Schon wegen der im Vergleich zu den Akteuren der Plattformökonomie geringeren Reichweiten und Nutzerzahlen müssen diese Angebote mit einer größeren Anzahl von Werbepartnern zusammenarbeiten, um am Wettbewerb um die digitalen Werbebudgets teilnehmen zu können. Die zu verarbeitenden Daten können dabei mangels direkter Kundenbeziehungen der Werbepartner in ihrer Eigenschaft als reine Technologieanbieter zu Verbrauchern nicht durch zentrale Log-In-Prozesse eingeholt werden. Soweit die von den ePrivacy-VO-E erfassten Datenverarbeitungen nicht auf der Basis eines gesetzlichen Zulässigkeitstatbestands erfolgen, müssen Einwilligungen zur Datenverarbeitung in diesen Fällen im Wege jeweils spezifischer Einwilligungsanfragen im Zuge der Nutzung eines Internetangebots eingeholt werden.

IV. Auswirkungen der Gesetzgebungsvorschläge auf die verschiedenen Geschäftsmodelle

Nach einer vom BMWI in Auftrag gegeben Studie zu den Vorschlägen des Entwurfs der Kommission ist in Deutschland kurzfristig mit einer Reduktion des gesamten digitalen Werbebudgets von etwa einem Drittel zu rechnen, wobei die Einschnitte zwischen den jeweiligen Werbegeschäftsmodellen der Plattformunternehmen auf der einen und digitalen Medienangeboten auf der anderen Seite höchst ungleich, nämlich zu Lasten letzterer ausfallen werden.[20] Übereinstimmend mit

---

19 *Horizont*, vom 13.12.2018, abrufbar unter: https://www.horizont.net/medien/nachrichten/omg-prognose-deutscher-werbemarkt-waechst-dank-google-und-facebook-171691 (letzter Abruf 15.10.2019).

20 *WIK*, Economic Impact of the ePrivacy Regulation on Online Advertising and Ad-based Digital Business Model, 2017, https://www.wik.org/fileadmin/Studien/2017/2017_ePrivacy-BMW.pdf (letzter Abruf 15.10.2019).

diesem Befund belegen vom VDZ durchgeführte Erhebungen, dass die Umsatzverluste in besonderer Weise Online-Medienangebote betreffen werden. Die Mehrheit der befragten Manager der Verlagshäuser und Vermarktungsspezialisten rechnet mit einem Umsatzverlust von über 30 Prozent im digitalen Werbegeschäft für journalistische Medien.[21]

Die Plausibilität dieser Befunde wird deutlicher, wenn man die zuvor dargelegten Vorschläge anhand der beiden wesentlichen werbewirtschaftlichen Geschäftsmodelle durchspielt. Nach den Vorschlägen von Kommission und Europäischem Parlament werden die im Bereich der Online-Werbung etablierten endgerätebezogenen Datenverarbeitungsmöglichkeiten vollständig auf die einwilligungsbasierte Verarbeitung reduziert. Unternehmen, die auf Basis von Log-In-Strukturen Internetnutzern gegenübertreten, sind hiervon nicht betroffen. Ihr Geschäftsmodell wäre hierdurch zwar an die bereits bestehenden formalen Anforderungen für datenschutzrechtliche Einwilligungen nach der DS-GVO anzupassen, deren Erfüllung ungeklärt ist. Ihre einwilligungszentrierte Regulierungsarchitektur an sich stünde jedoch in Übereinstimmung mit dem Geschäftsmodell der Nutzerregistrierung. Für den Vorschlag des Europäischen Parlaments ist dies in besonderer Weise nachvollziehbar. Angesichts des bereits erwähnten Erfordernisses einer „ausdrücklichen Einwilligung" kann die Einwilligung nach der Version des Europäischen Parlaments praktisch ausschließlich durch einen formalisierten Log-In-Prozess erteilt werden. Denjenigen Anbietern hingegen, die im freien Internet keine formalen Registrierungsprozesse gegenüber Endnutzern anbieten (können), würden nicht nur die Zulässigkeitstatbestände der DS-GVO entzogen werden. Auch in Bezug auf die Erlangung von Einwilligungen wären sie gegenüber den Log-In-Angeboten strukturell benachteiligt. Die Möglichkeit zur Abfrage formal datenschutzrechtlich ausdifferenzierter Einwilligungen, die hinsichtlich ihrer Wirkungen aber eine Art Generaleinwilligung darstellen, besteht für die Angebote des freien Internets wie oben aufgezeigt nur sehr beschränkt. Einzig nach dem Vorschlag des Rats könnten diese Konsequenzen vermieden werden.

Die Ungleichgewichtslage wird weiter verschärft, betrachtet man die Regelung zum Themenkomplex des Bedingungszusammenhangs zwischen Einwilligung und Zugang zu einem Internetangebot. Nach dem Vorschlag des Europäischen Parlaments ist ein Bedingungszusammenhang *per se* unzulässig. Der Zugang zum Angebot muss gewährt werden, unabhängig davon, wie sich ein

[21] Den erwarteten wirtschaftlichen Schaden für die gesamten digitalen Werbeumsätze aller Websites (unter Einschluss auch der nicht-journalistischen Websites, aber ohne Google und Facebook) beziffert die VDZ-Erhebung auf deutlich über 300 Millionen Euro pro Jahr; abrufbar unter https://www.vdz.de/nachricht/artikel/e-privacy-ueber-30-prozent-umsatzverlust-im-digitalen-werbegeschaeft-fuer-journalistische-medien/?L=0&cHash=1788ad5e661a0f2bb5e486906341ec8d (letzter Abruf 15.10.2019).

Endnutzer verhält.[22] Für Webseiten, die kein Log-In-Geschäftsmodell betreiben, bedeutet dies, dass sie – nach dem Vorschlag des Europäischen Parlaments bereits nach erster (!) Bitte um die Erteilung einer Einwilligung – bereit sein müssen, sämtliche produzierten Inhalte ohne Datenverarbeitung zwecks Werbung zur Verfügung zu stellen, wenn der Endnutzer keine Einwilligung erteilt. Auf dieser Basis, ein tragfähiges Refinanzierungskonzept zu finden, ist sehr problematisch. Digitale Vertriebserlöse, insbesondere bei journalistisch-redaktionen Angeboten, sind, wie soeben dargelegt, nicht so tragfähig, dass sie Erlöse auf dem Werbemarkt ersetzen könnten.[23]

Hinzu kommt, dass Verbraucher zwar durchaus eine Zahlungsbereitschaft für ihren digitalen Medienkonsum haben. Die ermittelten Werte lagen bislang jedoch erheblich unter der Konsumentenrendite, die durch digitale Werbung erwirtschaftet wird. Dabei wird darunter derjenige Betrag verstanden, den Verbraucher investieren müssten, wenn die Nutzung digitaler Dienste und Medien monetär zu vergüten wäre.[24] Der Wechsel auf andere nicht datenbasierte Formen der Online-Werbung erscheint ebenfalls nicht realistisch, betrachtet man, wie oben dargelegt, die erzielbaren Anzeigenpreise für „datenlos" geschaltete Online-Werbung.[25] Solange keine anderen gesetzlichen Verarbeitungsmöglichkeiten als die Nutzereinwilligung zur Verfügung stehen, muss es medienökonomisch daher als höchst problematisch angesehen werden, wenn der Anbieterseite weitgehend sämtliche Reaktionsmöglichkeiten (nach dem Europäischen Parlament sogar Kommunikationsmöglichkeiten) für den Fall der Nichterteilung einer Einwilligung genommen werden. Auch wenn ein Vergleich zu den Log-In-basierten Geschäftsmodellen, die ja ebenfalls einem strikten Kopplungsverbot (nach der Version des Europäischen Parlaments) unterlägen, nicht genau quantifiziert werden kann, sprechen eine Reihe von Gründen dafür, dass die Zahl der Einwilligungsverweigerungen in Bezug auf werbefinanzierte Diensten signifikant geringer ausfallen würde. Ausschlaggebend hierfür ist die oftmals dominante Marktstellung dieser Geschäftsmodelle in ihrem jeweiligen Marktsegment (Social Media, Online Video, E-Commerce), die damit einhergehenden

---

22 Nach der Version der KOM ist dies, folgt man der Interpretation der Aufsichtsbehörden (siehe Fn. 10 und 11), regelmäßig der Fall.

23 *PWC*, a.a.O. (Fn. 17).

24 *vzbv*, Verbraucher würden für mehr Datenschutz und Werbefreiheit zahlen (Studie 2015): 10 Prozent der Verbraucher würden hiernach 1 EUR , 54 Prozent bis zu 5 EUR und 33 Prozent mehr als 5 EUR pro Monat zahlen; abrufbar unter: https://www.vzbv.de/pressemitteilung/verbraucher-wuerden-fuer-mehr-datenschutz-zahlen (letzter Abruf 15.10.2019). Die Konsumentenrendite betrug indes bereits im Jahr 2010 40 EUR pro Monat, vgl. *McKinsey*, Consumer driving the digital uptake, Studie im Auftrag des IAB, 2010, abrufbar hier: http://www.frische-fische.de/pdf/1100.pdf (letzter Abruf 15.10.2019).

25 Zu beiden Aspekten vgl. auch *WIK*, a.a.O (Fn. 21), III.

Netzwerkeffekte und die weitgehend proprietäten Angebotsarchitekturen, die Wechsel von Nutzern zu anderen Produkten erschweren.

Auch mit dem Vorschlag des Rats wären weitreichende Erschwerungen für eine tragfähige Finanzierung von Internetangeboten der Medien verbunden. Aus dem vom Rat kreierten Vergleichstest resultieren, wie zuvor festgestellt, konkrete Vorgaben zur Geschäftsmodellgestaltung. Ein einwilligungsbasiertes werbefinanziertes Angebot, dessen Zugang von der Erteilung einer Einwilligung in die werbewirtschaftliche Datenverarbeitung abhängig gemacht werden soll, ist hiernach nicht zulässig. Auf der sicheren Seite ist ein Anbieter aber, wenn er zugleich ein identisches Angebot, ohne ein werbewirtschaftlich ausgerichtetes Einwilligungserfordernis realisiert. Diese Vorgehensweise ist aber abgesehen von den seltenen Einzelfällen eines Angebots, das sich von freiwilligen Spenden der Endnutzer oder Dritter refinanziert, nicht tragfähig. Inwiefern ein alternatives Pay-Angebot desselben Anbieters als gleichwertiges Alternativangebot in die Betrachtung eingestellt werden kann (und zu welchen Konditionen), wird von Erwägungsgrund 20 nicht thematisiert. Die hierin liegende Ungewissheit für die Anbieter bei einer sehr grundlegenden wirtschaftlichen Entscheidung ist durchaus problematisch. In Anbetracht der Tatsache, dass auch ein solches Angebot zu realisieren wäre, damit der „Vergleichstest“ nach der Version des Rats „bestanden“ wird, stellt sich im Übrigen auch hier der Effekt der Geschäftsmodellvorgabe ein.

B. Die gutachterlich zu klärenden Rechtsfragen

Vor dem Hintergrund dieses Sachverhalts stellen sich folgende rechtsgutachterlich zu klärende Fragen:

1. Inwiefern ist es rechtssystematisch und dogmatisch möglich, im Sekundärrecht von der DS-GVO abweichende Zulässigkeitstatbestände in der ePrivacy-VO zu normieren, die gegebenenfalls strengere oder weniger strenge oder schlicht anderweitig ausgestaltete („aliud") Vorgaben enthalten?
2. Inwiefern ist es rechtspolitisch sinnvoll, in der ePrivacy-VO sektorspezifische Zulässigkeitstatbestände zu schaffen?
3. Welche Vorgaben ergeben sich insoweit aus den primärrechtlichen Anforderungen und insbesondere aus der Grundrechte-Charta der EU an ein entsprechendes sektorspezifisches Sonderregime im Allgemeinen und für die Einwilligung im Besonderen? Inwiefern kann insbesondere die einwilligungsbasierte Verarbeitung in Bezug auf den Zugang zu und die Speicherung von Informationen auf Endgeräten seitens des Diensteanbieters unter Bedingungen gestellt werden, um eine datenfinanzierte Erbringung von Diensteangeboten zu ermöglichen?

C. Rechtsgutachterliche Bewertung

Die aufgeworfenen drei Fragenkomplexe sind in drei Schritten zu beantworten: Zunächst ist zu prüfen, welche rechtssystematischen und rechtsdogmatischen Vorgaben für die Entscheidung über das „Ob" und das „Wie" einer sektorspezifischen Regulierung des Datenschutzrechts in der ePrivacy-VO greifen (dazu I.). Angesichts des Befundes eines weiten Spielraums des EU-Sekundärrechts-Gesetzgebers ist sodann zu prüfen, inwiefern dieser durch weiche rechtspolitische (dazu II.) und bindende primärrechtliche Vorgaben (dazu III.) eingeengt wird.

I. Rechtssystematische und rechtsdogmatische Vorgaben für sektorspezifische Zulässigkeitstatbestände in der ePrivacy-VO

Ausgehend von allgemeinen rechtssystematischen und rechtsdogmatischen Vorgaben (dazu 1.) ist zur Beantwortung der ersten Frage ergänzend eine spezifische Untersuchung der etwaigen Sperrwirkung der DS-GVO anhand der in dem Regelwerk vorhandenen normativen Anknüpfungspunkte und allgemeiner demokratietheoretischer Überlegungen erforderlich (dazu 2.).

1. Allgemein: Lex-specialis- und Lex-posterior-Grundsatz im EU-Sekundärrecht

Der Grundsatz „Lex specialis derogat legi generali"[26] besagt als juristische Auslegungsregel[27], dass ein thematisch[28] spezielleres, besonderes Gesetz das allgemeinere verdrängt. Sofern also ein breiterer Regelungsbereich für einen Teilbereich spezifischer normiert wird, sind diese spezifischeren Normen anzuwenden. Hintergrund dieser Vermutungsregel ist die Überlegung, dass nur so die Spezialregelung einen Anwendungsbereich erlangt und andernfalls gegenstandslos bliebe. Das setzt voraus, dass die speziellere Norm die Merkmale der allgemeinen aufweist, aber eine weitere zusätzliche Tatbestandsvoraussetzung zur Einengung des Anwendungsbereichs enthält.[29] Im

---

26 „Das besondere Gesetz verdrängt das allgemeine."

27 Siehe dazu und zu den verschiedenen konzeptionellen Klassifikationen der Grundsätze *Vranes*, Lex Superior, Lex Specialis, Lex Posterior – Zur Rechtsnatur der „Konfliktlösungsregeln", ZaöRV 2005, 391 ff.

28 *Groh*, in: Creifelds (Hrsg.), Rechtswörterbuch, 23. Edition 2019.

29 *Beaucamp/Treder*, Methoden und Technik der Rechtsanwendung, 2. Aufl. 2011, Rn. 241; *Bydlinski*, Methodenlehre und Rechtsbegriff, 2. Aufl. 2011, S. 465; *Larenz/Canaris*, Methodenlehre der Rechtswissenschaft, 3. Aufl. 1995, S. 87; *Schmidt*, JuS 2003, 649 (650).

Rahmen der Auslegung beider Regelwerke ist sodann zu ermitteln, ob subsidiär auf das allgemeinere Gesetz zurückgegriffen werden kann. Dies hängt davon ab, inwiefern das spezifischere Normenwerk abschließende Regelungen schafft. Im Rahmen der Auslegung werden damit im Ergebnis Normanwendungskonflikte vermieden, die sich andernfalls aus divergierenden Steuerungsvorgaben der unterschiedlichen Regelungswerke für identische Normadressaten ergeben würden.

Der Grundsatz „Lex posterior derogat legi priori"[30] sagt davon abweichend als weitere Auslegungsregel, dass in zeitlicher Hinsicht die später geschaffene Regelung die frühere verdrängt. Damit wird verhindert, dass Normanwendungskonflikte von Bestimmungen mit identischem Regelungsbereich und identischen Regelungsadressaten aber unterschiedlichen Regelungsvorgaben entstehen, die zu verschiedenen Zeitpunkten geschaffen wurden.

Diese bei der Interpretation und Anwendung des Rechts geltenden Auslegungsregeln sind gleichermaßen konzeptionelle Leitvorgabe bei dessen Schaffung.

Sie greifen darüber hinaus bei der Auslegung und Anwendung des Unionsrechts[31] genauso wie im nationalen Recht. Auf unionaler Ebene gilt dies sodann für alle Regelungsebenen[32] einschließlich der sekundärrechtlichen Vorgaben in Verordnungen.[33]

Im vorliegenden Zusammenhang bedeutet das: Wenn für den besonderen Bereich der elektronischen Kommunikationsdienste in der ePrivacy-VO speziellere datenschutzrechtliche Regelungen gegenüber der allgemeinen datenschutzrechtlichen Regelung in der DS-GVO in der Form geschaffen werden, dass diese für den spezifischen Anwendungsbereich der elektronischen Kommunikationsdienste als zusätzlicher, den Anwendungsbereich einengender Tatbestandsvoraussetzung greifen, so werden später diese Bestimmungen vorrangig gegenüber der DS-GVO anzuwenden sein. Es käme insoweit der Lex-specialis-Grundsatz zur Anwendung, da es sich um speziellere Regeln handelt. Ein Rückgriff auf den Lex-posterior-Grundsatz würde hingegen nicht erfolgen und wäre auch nicht notwendig, da der Normanwendungskonflikt schon durch die Anwendung des Lex-specialis-Grundsatzes ausgeräumt wird. Es werden somit gar nicht zwei unterschiedliche

---

30 „Das jüngere Gesetz verdrängt das ältere Gesetz."

31 Dazu allgemein etwa *von Danwitz*, in: Dauses/Ludwigs (Hrsg.), Handbuch des EU-Wirtschaftsrechts, 47. EL März 2019, B. II. Rechtsetzung und Rechtsangleichung, Rn. 70; *Kreuzer/Wagner/Reder*, in: Dauses/Ludwigs (Hrsg.), Handbuch des EU-Wirtschaftsrechts, 47. EL März 2019, Q.I. Grundlagen, Rn. 23; *Nettesheim*, in: Grabitz/Hilf/Nettesheim (Hrsg.), Das Recht der EU, 67. EL Juni 2019, Art. 288 AEUV, Rechtakte, Katalog, Rn. 228.

32 Für das EU-Primärrecht explizit EuGH, Beschluss vom 7.12.2017, Rs. C-323/16 P, ECLI:EU:C:2017:952 – *Euroallumina SpA*, Rn. 56.

33 Dazu die Nachweise in Fn. 31.

Regelungsregime für *denselben* Anwendungsgegenstand zu unterschiedlichen Zeitpunkten erlassen, sondern für *unterschiedliche* Anwendungsgegenstände, nämlich einmal allgemein und einmal bezogen auf elektronische Kommunikationsdienste.

Das speziellere Regelwerk kann sodann strengere, weniger strenge oder schlicht abweichende Bestimmungen schaffen. Es kann darüber hinaus abschließende Regelungen des Datenschutzregimes treffen oder nur spezifische Aspekte aufgreifen und im Übrigen auf die DS-GVO verweisen und diese ganz oder in Teilen für subsidiär anwendbar erklären. In methodischer Hinsicht ist der Gesetzgeber im Übrigen auch vollkommen frei, inwieweit er speziellere Regelungen für Teilbereiche des Rechtsgebiets in das allgemeine Gesetz aufnehmen möchte, wie es ja schon mit besonderen Kategorien von Daten (in Art. 9 DS-GVO und andernorts) der Fall ist. Damit besteht im vorliegenden Kontext in methodischer Hinsicht ein breiter Spielraum für den Gesetzgeber: Er kann gänzlich auf spezielle Datenschutzregeln für elektronische Kommunikationsdienste verzichten, diese in die DS-GVO aufnehmen oder – entsprechend der bisherigen Tradition – in einem gesonderten Regelwerk in Form der ePricacy-VO verorten. Schlägt er den letztgenannten Weg ein, hat er wieder eine Vielzahl von Handlungsalternativen: So kann er ein vollkommen abgeschlossenes Spezialregime schaffen oder nur für Teilsegmente (etwa die Zulässigkeitstatbestände) und im Übrigen – wiederum ganz oder in Teilen – auf die DS-GVO verweisen. Wenn er dabei ganz oder teilweise strengere, weniger strenge oder schlicht abweichende Regelungen schafft, greifen insoweit keine methodischen Einschränkungen, sondern als einzige Leitplanken rechtspolitische Überlegungen (dazu II.) und zwingende primärrechtliche Rahmenbedingungen (dazu III.).

2. Insbesondere: keine sonstige Sperrwirkung („effet cliquet") der DS-GVO

a) Normative Anknüpfungspunkte in der DS-GVO

Ergänzend ist darauf hinzuweisen, dass sich auch aus der DS-GVO selbst keine abweichenden Vorgaben ergeben. Zunächst lassen sich im Text der DS-GVO keine Anhaltspunkte für eine Sperrwirkung gegenüber dem „Ob" und dem „Wie" spezialgesetzlicher datenschutzrechtlicher Regelungen allgemein oder für elektronische Kommunikationsdienste im Besonderen entnehmen. Vielmehr verweist die DS-GVO selbst auf weitere – mögliche – sektorspezifische Vorgaben auf unionaler und – im Rahmen der Ausfüllung der Öffnungsklauseln der DS-GVO – auch nationaler Ebene, etwa in Erwägungsgrund 10.

Spezifischer mit Blick auf die elektronische Kommunikation bestimmt Erwägungsgrund 173 die Subsidiarität der DS-GVO gegenüber der bisherigen RL 2002/58/EG. Wörtlich heißt es insoweit:

> „Diese Verordnung sollte auf alle Fragen des Schutzes der Grundrechte und Grundfreiheiten bei der Verarbeitung personenbezogener Daten Anwendung finden, die nicht den in der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates (2) bestimmte Pflichten, die dasselbe Ziel verfolgen, unterliegen, einschließlich der Pflichten des Verantwortlichen und der Rechte natürlicher Personen. Um das Verhältnis zwischen der vorliegenden Verordnung und der Richtlinie 2002/58/EG klarzustellen, sollte die Richtlinie entsprechend geändert werden. Sobald diese Verordnung angenommen ist, sollte die Richtlinie 2002/58/EG einer Überprüfung unterzogen werden, um insbesondere die Kohärenz mit dieser Verordnung zu gewährleisten."

Normativ wird dieser Erwägungsgrund insbesondere in Art. 95 DS-GVO aufgenommen. In dieser Bestimmung werden zusätzliche Pflichten aus der DS-GVO gegenüber der RL 2002/58/EG ausgeschlossen. Art. 95 DS-GVO regelt so das Verhältnis der DS-GVO zum Sonderregime der RL 2002/58/EG gerade so wie das bisherige Verhältnis der überkommenen RL 95/46/EG zu jener spezifischen Regelung: Die RL 2002/58/EG enthält Sondervorschriften für Dienste der elektronischen Kommunikation und verdrängt damit allgemeinere Regeln – insbesondere zur Zulässigkeit der Datenverarbeitung – aus der DSRL und nunmehr der DS-GVO.[34] Zwar ist einzuräumen, dass hier in den Details vieles umstritten ist, da Art. 95 DS-GVO für den Maßstab der Identifikation des Spezialitätsverhältnisses der Verordnung gegenüber der RL 2002/58/EG entscheidend darauf abstellt, ob die Richtlinie jeweils Vorschriften enthält, die „dasselbe Ziel verfolgen" wie die Bestimmungen der DS-GVO. Damit ist der Regelungsgegenstand der jeweiligen Norm entscheidend, da die Ziele der RL 2002/58/EG und der DS-GVO nicht völlig deckungsgleich sind.[35] Trotz dieser „Arbeit im Detail" ist damit jedenfalls als status quo das Spezialitätsverhältnis dem Grunde nach bestätigt. Gemäß Art. 29 Abs. 2 ePrivacy-VO-KOM-E sollte diese Verordnung zeitgleich mit der DS-GVO zum 25. Mai 2018 Geltung erlangen. Dieses Ziel hat sich letztlich als zu ambitioniert erwiesen. Damit ist der Regelungsgehalt der ePrivacy-VO weiterhin offen, ebenso wie dessen Verhältnisbestimmung zur DS-GVO in den Details. Genau dies – so die Implikation der DS-GVO – soll aber im weiteren Gesetzgebungsprozess der ePrivacy-VO geklärt werden. Art. 1 Abs. 3 ePrivacy-VO-KOM-E will dieses Spezialitätsverhältnis zwischen DS-GVO und ePrivacy-VO künftig

---

34 So etwa *Kühling/Raab*, in: Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung/BDSG, Kommentar, 2. Aufl. 2018, Art. 95 DS-GVO, Rn. 1 und passim m.w.Nachw.

35 *Heun/Assion* in: Eßer/Kramer/Lewinski (Hrsg.), Auernhammer. DS-GVO/BDSG, Kommentar, 6. Aufl. 2018, Art. 95 DS-GVO, Rn. 16.

klären, kann jedoch ebenso wie das „Ob“ und „Wie“ der ePrivacy-VO auch anderweitig geregelt werden.

Das entspricht auch dem Regelungsgehalt des Art. 98 DS-GVO, der eine Überprüfung anderer Rechtsakte der Union zum Datenschutz mit dem Ziel eines einheitlichen und kohärenten Datenschutzes vorsieht. Art. 98 DS-GVO ist erst im Trilog in das Gesetzgebungsverfahren eingespeist worden. Zu diesem Zeitpunkt war klar, dass eine parallele Novellierung der Richtlinie 2002/58/EG im Bereich der elektronischen Kommunikation, nicht gelingen wird.[36] So lag beim Inkrafttreten der DS-GVO noch nicht einmal ein entsprechender Entwurf einer Novellierung im Telekommunikationsbereich vor.[37]

Die Bestimmung dokumentiert zwar den gesetzgeberischen Willen, dass die DS-GVO künftig als Maßstab für den Schutz personenbezogener Daten anzusehen ist,[38] hat aber gleichwohl lediglich Appellcharakter[39] und entfaltet jedenfalls keine normative Bindungswirkung hinsichtlich des „Ob“ und „Wie“ einer gegebenenfalls gewünschten partiellen sektorspezifischen Konkretisierung.

b) Allgemeine demokratietheoretische Überlegungen

Die Annahme einer diesbezüglichen Sperrwirkung wäre auch methodisch vor dem Hintergrund der bisherigen Ausführungen gar nicht möglich. Ein allgemeines Gesetz kann sich demnach nicht gegen spezialgesetzliche Modifikationen „abschirmen“. Auch demokratietheoretisch wäre eine derartige Vorstellung abwegig. Denn der (in der vorangegangenen Legislaturperiode gefundene) politische Kompromiss zur DS-GVO kann nicht den jetzigen, gleichermaßen demokratisch legitimierten EU-Gesetzgeber einschränken, der nunmehr über das „Ob“ und das „Wie“ datenschutzrechtlicher Spezialregelungen für elektronische Kommunikationsdienste debattiert. Aus denselben Gründen kann auch keine Beschränkung der inhaltlichen Ausrichtung etwaiger künftiger Spezialregelungen auf unionaler Ebene im Sinne eines „effet cliquet“ dahin gehend erfolgen, dass lediglich eine Verschärfung der datenschutzrechtlichen Anforderungen der DS-GVO in einer Spezialgesetzgebung möglich sein könne. Vielmehr handelt es sich bei der DS-GVO um einen rechtspolitischen Kompromiss im Rahmen einer Vielzahl denkbarer daten*schutz*freundlicherer oder

---

36 Dazu kritisch *Albrecht*, Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung, CR 2016, 88 (90).

37 Siehe dazu *Kühling/Raab*, in: Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung/BDSG, Kommentar, 2. Aufl. 2018, Art. 99 DS-GVO, Rn. 1 und passim m.w.Nachw.

38 *Zerdick*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, Kommentar, 2016, Art. 98, Rn. 1.

39 *Kühling/Raab*, in: Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung/BDSG, Kommentar, 2. Aufl. 2018, Art. 99 DS-GVO, Rn. 2.

umgekehrt daten*verarbeitungs*freundlicherer Regelungen oder schlichtweg abweichender Ausgestaltungskonzepte. Dieser kann jederzeit durch den Gesetzgeber derselben oder einer späteren Legislaturperiode innerhalb der DS-GVO oder außerhalb des Normenwerkes durch speziellere Regelungen modifiziert werden. Wiederum greifen als einzige Leitplanken insoweit (weiche) rechtspolitische Überlegungen und bindende primärrechtliche Vorgaben. Dabei ist schon hier auf die grundrechtliche Perspektive hinzuweisen, die deutlich macht, dass es sich bei der Datenverarbeitung um einen multipolaren Grundrechtskonflikt mit einer Vielzahl widerstreitender Interessen der betroffenen Personen und Datenverarbeiter handelt und schon von daher keine Optimierung in eine Richtung (etwa im Sinne eines immer strengeren Datenschutzes) geboten ist (dazu ausführlicher III.).

3. Zwischenergebnis

Der Grundsatz „Lex specialis derogat legi generali" greift auch bei der Auslegung und Anwendung des EU-Sekundärrechts. Er ist daher gleichermaßen konzeptionelle Leitvorgabe bei dessen Schaffung. Wenn danach für den besonderen Bereich der elektronischen Kommunikationsdienste in der ePrivacy-VO speziellere Regelungen in der Form geschaffen werden, dass diese für den spezifischen Anwendungsbereich in Teilen oder im Ganzen strengere, weniger strenge oder schlicht abweichende Bestimmungen formulieren, gehen diese den vergleichbaren Bestimmungen in der DS-GVO vor.

Es gibt insoweit keine Besonderheiten in Bezug auf die DS-GVO. Vielmehr bestätigen die Regelungen in Art. 95 und 98 DS-GVO diesen Ansatz einer freien Spezialregelung in der noch geltenden ePrivacy-Richtlinie und der künftigen ePrivacy-VO. Jene Freiheit entspricht im Übrigen auch demokratietheoretischen Überlegungen. Die DS-GVÄO kann daher sowohl durch eine spätere abweichende spezifischere Regelung innerhalb als auch außerhalb des Normtextes der DS-GVO modifiziert werden. Insbesondere gibt es keine Restriktion dogmatischer oder rechtssystematischer Art, dass für Spezialbereiche lediglich strengere (d.h. datenschutzfreundlichere) Bestimmungen geschaffen werden dürften. Insofern greift auch keine Sperrwirkung („effet cliquet") der DS-GVO.

In der Konsequenz kann eine ePrivacy-VO strengere, weniger strenge oder schlicht abweichende Regelungen gegenüber der DS-GVO in Bezug auf elektronische Kommunikationsdienste für einzelne oder sämtliche Aspekte der DS-GVO normieren und im Übrigen auf diese ganz, teilweise oder gar nicht verweisen, sofern dies im Einklang mit dem Primärrecht und insbesondere den

grundrechtlichen Vorgaben der GrCh steht (dazu III.). Auch rechtspolitisch sollte die Vorgehensweise sinnvoll sein (dazu II.).

II. Rechtspolitische Steuerungsvorgaben einer denkbaren bereichsspezifischen Regelung in der ePrivacy-VO

In rechtspolitischer Hinsicht sprechen die Grundsätze der Normenklarheit und der Normenbestimmtheit eher für eine bereichsspezifische Regelung (dazu 1.), die Anpassungsflexibilität und Einfachheit des Regelwerkes eher für eine möglichst allgemeine einheitliche Kodifizierung (dazu 2.). So oder so besteht die Notwendigkeit einer angemessenen Ausbalancierung der relevanten Interessen (dazu 3.).

1. Normenklarheit, Bestimmtheit und weitere Vorzüge einer bereichsspezifischen Regelung

In rechtspolitischer Hinsicht streitet für eine spezialgesetzliche Regelung zunächst der Umstand, dass es sich bei der elektronischen Kommunikation zum Teil um Daten handelt, die als besonders geschützt anzusehen sind, insbesondere, sofern es um die Inhalte der Kommunikation geht. Soll diesen Besonderheiten Rechnung getragen werden, kann dies grundsätzlich durchaus sinnvoll in spezifischen Regelungen erfolgen. Diese ermöglichen bereichsspezifisch eine normenklarere und bestimmtere Regelung als dies in einer allgemeinen Regelung möglich ist. Auch kann eine bereichsspezifische Regelung differenzierter und damit durch den Unionsgesetzgeber auf einer tiefergreifenden Detailebene umfassender legitimiert einen Interessenausgleich herbeiführen, anstatt dies – wie im Fall allgemeinerer Regelungen – den Anwendungsbehörden und ultimativ der Judikative zu überlassen.

2. Einfachheit, Anpassungsflexibilität und weitere Vorzüge einer einheitlichen Kodifizierung

Die EU hat jedoch gerade im Vergleich mit anderen Regelungsregimen wie etwa dem fragmentarischen Ansatz im US-amerikanischen Datenschutzrecht mit der DS-GVO den Vorteil einer

umfassenden normativen Regelung[40], die grundsätzlich sämtliche Datenverarbeitungsprozesse erfasst.[41] Allerdings gilt dies bei näherer Betrachtung nur dem Grunde nach. Denn durch die zahlreichen optionalen Öffnungsklauseln der DS-GVO verfügen die Mitgliedstaaten über die Möglichkeit, bereichsspezfische Regelungen zu schaffen.[42] Davon hat Deutschland in Teilbereichen – wie etwa dem Gesundheitsdatenschutzrecht[43] – umfassend Gebrauch gemacht. Für den vorliegenden Fall der Verarbeitung von Daten der elektronischen Kommunikation greifen allerdings nur begrenzt Öffnungsklauseln.[44] Daher hätte ein Rückgriff auf die DS-GVO den Vorteil, dass dieses einheitliche Datenschutzregime zur Anwendung gelangt. Die – jedenfalls mit Blick auf die Zulässigkeitstatbestände – dem Grunde nach einfach strukturierten Normen, die zudem im Wesentlichen der bewährten Regelung in Art. 7 der RL 95/46/EG folgen, weisen auch die nötige Anpassungsflexibilität auf, um den besonderen Bedürfnissen des Schutzes von Daten der elektronischen Kommunikation gerecht zu werden. So können die Erforderlichkeitsanforderungen der Zulässigkeitstatbestände des Art. 6 DS-GVO einschließlich etwaiger berechtigter Interessen der Betroffenen sowie die Einwilligung nach Art. 7 und 8 DS-GVO situationsadäquat ausgelegt werden und damit gerade auch dem besonderen Schutz des Inhalts der Kommunikation gerecht werden. Standortdaten fallen dagegen nicht nur bei Diensten der elektronischen Kommunikation an, sondern auch unter dem Rahmen der DS-GVO und bedürfen hier wie dort eines angemessenen Schutzes, aber auch entsprechender Verarbeitungsmöglichkeiten im Sinne einer gewünschten Dienstequalität. Die Vertragsdaten des Kunden im Bereich der elektronischen Kommunikation können dagegen genauso wie die Daten sonstiger Vertragskunden unter der DS-GVO geschützt werden.

3. Notwendigkeit einer angemessenen Ausbalancierung der relevanten Interessen

Dies zeigt bereits auf, dass Daten, die im Rahmen elektronischer Kommunikationsdienste anfallen, unterschiedlich sensibel sind (besonders geschützte Inhaltsdaten, Verkehrsdaten, sonstige Daten

---

40 In der US-amerikanischen Literatur wird insofern teilweise von einer „Omnibus"-Regulierung gesprochen (siehe nachfolgende Fn.), während dieser Begriff in Deutschland zuletzt auch dazu verwendet wurde, um die umfassende Anpassung der deutschen Datenschutzgesetze im Rahmen der Ausfüllung der Öffnungsklauseln der DS-GVO zu bezeichnen.

41 Grundlegend zum Vergleich des US-amerikanischen mit dem europäischen Ansatz insoweit *Schwartz/Peifer*, Transatlantic Data Privacy Law, Geo. L. J. 2017, S. 115 ff.

42 Zu den Öffnungsklauseln grundlegend *Kühling/Martini u.a.*, Die Datenschutz-Grundverordnung und das nationale Recht. Erste Überlegungen zum innerstaatlichen Regelungsbedarf, 2016.

43 Dazu zuletzt kritisch *Kühling*, Datenschutz im Gesundheitswesen, MedR 2019, 611 (622).

44 Da es vor allem um die Datenverarbeitung durch Unternehmen geht, dazu bereits *Kühling*, Neues Bundesdatenschutzgesetz – Anpassungsbedarf bei Unternehmen, NJW 2017, 1985 ff.

wie einfache Vertragsdaten oder nicht inhalts- oder ortsbezogene Nutzungsdaten). Dies kann innerhalb einer angemessenen Anwendung und Auslegung der DS-GVO oder im Rahmen der Schaffung einer Spezialregelung gewährleistet werden. In beiden Fällen ist auch eine angemessene Ausbalancierung der relevanten Interessen an einem Datenschutz und an einer Datenverarbeitung erforderlich. Dabei ist ein sinnvoller Rahmen für die Datenverarbeitung keineswegs nur im Interesse des Datenverarbeiters, der damit beispielsweise die Finanzierung des Dienstes ganz oder in Teilen betreibt. Vielmehr wird der Nutzer des Dienstes, immer dann, wenn er keine pekuniäre Zahlungsbereitschaft in Bezug auf die Dienste hat, diesen aber dennoch weiterhin nutzen möchte, ein ureigenes Interesse daran haben, dass dieser finanziert wird, was, wenn keine Finanzierung durch Spenden mit der Möglichkeit des Trittbrettfahrens (wie etwa bei Wikipedia) erfolgt, regelmäßig auch eine personalisierte Werbung und damit eine Verarbeitung der Daten des betroffenen Nutzers verlangt. Unabhängig davon, ist ein Teil der Datenverarbeitung auch im Interesse des Dienstenutzers, weil sie eine Optimierung des Diensteangebots ermöglicht. Beispielsweise wird eine Erfassung standortbezogener Daten gerade oftmals im Interesse der betroffenen Person sein. So dürfte für eine standortbezogene Suche (etwa nach Restaurants) regelmäßig eine Verarbeitung des Standortdatums gewünscht sein, so dass dem Betroffenen als Nutzer unmittelbar weitere Informationen zur Entfernung und Erreichbarkeit des gesuchten Objektes übermittelt werden können.

Auf einer horizontalen Ebene sind zudem die Auswirkungen der Regulierung für die verschiedenen konkurrierenden Geschäftsmodelle zu beachten. Wie noch näher darzulegen sein wird (dazu III.4.), haben unterschiedliche Ausgestaltungen der Datenverarbeitungsregeln höchst heterogene Konsequenzen für die verschiedenen Geschäftsmodelle. Auch unter dem Blickwinkel der unternehmerischen Freiheit, sollte die Datenschutzregelung nicht spezifische Geschäftsmodelle privilegieren, sofern dies nicht aus datenschutzrechtlichen Gründen geboten ist und auch vor dem Hintergrund gegenläufiger Grundrechtsinteressen der betroffenen Diensteanbieter eine nicht zu rechtfertigende Ungleichbehandlung darstellt. Daher gilt grundsätzlich, dass die Regulierung wettbewerbsneutral ausfallen sollte, d.h. den verschiedenen gleichermaßen geschützten Geschäftsmodellen bei der Werbefinanzierung vergleichbare Verwirklichungschancen einräumen sollte.

4. Zwischenergebnis

Rechtspolitisch ist eine große Bandbreite an Ausgestaltungen der Zulässigkeitstatbestände und anderer Vorgaben zur Verarbeitung von Daten der elektronischen Kommunikation denkbar. Sie reichen von einem gänzlichen Verzicht auf sektorspezifische Vorgaben bis hin zu einer Ausgestaltung eigenständiger Zulässigkeitstatbestände. Letzteres kann etwa in Form der Regelung von spezifischen Sonderfällen im Bereich der Erbringung elektronischer Kommunikationsdienste ggfls. einschließlich eines (spezifizierten) berechtigten Interesses sowie einer (ggfls. modifizierten) Einwilligung erfolgen.

Während ganz allgemein die Grundsätze der Normenklarheit und Bestimmtheit eher für eine bereichsspezifische Regelung streiten, sprechen die Gründe der Einfachheit und Anwendungsoffenheit für eine umfassende, einheitliche Kodifizierung. Die DS-GVO enthält ohnehin bezogen auf besondere Kategorien von Daten bereits abgeschichtete, spezifische Vorgaben.

Jegliche Ausgestaltung muss jedenfalls die verschiedenen, teilweise widerstreitenden Interessen an einer Datenverarbeitung auf der einen Seite und einem Verzicht darauf zum Schutz der Privatsphäre auf der anderen Seite zum Ausgleich bringen. Dabei muss es insbesondere auch darum gehen, dass die von den Konsumenten gewünschten Dienste unter Berücksichtigung eines angemessenen Datenschutzes der betroffenen Personen funktionsfähig erbracht und dabei auch auskömmlich finanziert werden können, damit sie den Nutzern weiterhin zur Verfügung gestellt werden können. Ferner sollte die Regulierung wettbewerbsneutral ausfallen, d.h. den verschiedenen gleichermaßen geschützten Geschäftsmodellen bei der Werbefinanzierung vergleichbare Verwirklichungschancen einräumen.

III. Rechtsstaatliche und grundrechtliche Steuerungsvorgaben für die etwaige Ausgestaltung bereichsspezifischer Regelungen in der ePrivacy-VO

Bindende primärrechtliche Steuerungsvorgaben folgen zunächst aus dem – wenig strengen – unionsrechtlichen Gesetzesvorbehalt sowie den rechtsstaatlichen Anforderungen an die Normbestimmtheit und Sektorspezifität (dazu 1.). In grundrechtlicher Perspektive ergeben sich Einschränkungen hinsichtlich eines Mindestmaßes an Datenschutz aus Art. 7 und 8 GrCh (dazu 2.). Die Datenschutzinteressen sind gegen Interessen an einem „free flow of data“ abzuwägen, die aus der

unternehmerischen Freiheit gemäß Art. 16 GrCh und weiteren Grundrechtspositionen folgen, wobei gerade die Medienfreiheit aus Art. 11 Abs. 2 GrCh von überragender Bedeutung ist (dazu 3). Trotz eines unbestrittenen legislativen Spielraums folgen daraus Grenzen in allgemeiner Hinsicht für die Schaffung von Zulässigkeitstatbeständen in der DS-GVO (dazu 4.) und speziell mit Blick auf die Einwilligung (dazu 5.).

1. Rechtsstaatliche Anforderungen an die Normbestimmtheit/Sektorspezifität; Gesetzesvorbehalt

In den mitgliedstaatlichen Rechtsordnungen finden sich teils ausdifferenzierte Anforderungen an den Gesetzesvorbehalt und die Normbestimmtheit bzw. Notwendigkeit sektorspezifischer Regelungen, die jedoch im Unionsrecht weniger streng sind (dazu a)) und schon angesichts des Spannungsverhältnisses von Normenbestimmtheit und Normenklarheit (dazu b)) jedenfalls im Fall der Regelung der Verarbeitung von Daten der elektronischen Kommunikation durch Private von einem weiten Spielraum des Unionsgesetzgebers zeugen (dazu c)).

a) Keine strengen Anforderungen im vorliegenden Fall im EU-Recht

Das in manchen mitgliedstaatlichen Rechtsordnungen wie der deutschen eher strenge Verständnis des Parlamentsvorbehalts kombiniert mit dem Erfordernis bereichsspezifischer Regelungen greift in seiner ganzen Schärfe regelmäßig gerade *nicht* für das gesamte Datenschutzrecht, sondern nur im Bereich der öffentlichen Sicherheit und vergleichbaren Konstellationen einer hohen Eingriffsintensität wie der zwangsweisen Datenerhebung im Rahmen der Volkszählung und Maßnahmen mit hoher Streubreite.[45]

Dies entspricht auch dem Ansatz auf unionsrechtlicher Ebene bzw. wird dort jedenfalls keineswegs verschärft. Normativer Anknüpfungspunkt ist insoweit Art. 52 Abs. 1 S. 1 GrCh im Allgemeinen und Art. 8 Abs. 2 S. 1 GrCh im Besonderen. Die danach erforderliche gesetzliche Grundlage muss klare und präzise Regeln über die Tragweite und Anwendung einer Maßnahme vorsehen und

[45] Etwas anders liegt wiederum der Fall gerichtlicher Maßnahmen in privaten Rechtsverhältnissen, etwa in Bezug auf die Regelung von Abstammungsgutachten in Familiensachen, wo wiederum eine gesetzliche Regelung erforderlich ist, BVerfG, FamRZ 2013, 1195 (1196).

Mindestanforderungen für die der Person zur Verfügung stehenden Garantien aufstellen, um sich gegen einen unberechtigten Zugriff auf ihre Daten zu wehren.

Insoweit lassen sich in der bisherigen Rechtsprechung des EuGH besondere Anforderungen an die gesetzliche Ausdifferenzierung ebenfalls nur in Fällen besonders schwerer Datenschutzeingriffe durch die öffentliche Gewalt festmachen. Wegweisend ist insoweit das EuGH-Urteil zur Vorratsdatenspeicherungs-Richtlinie.[46] Hier führt die Rechtsprechung des Luxemburger Gerichtshofs jedenfalls dazu, dass die Steuerungsvorgaben zur Reichweite der Datenverarbeitung und zu gegenläufigen Schutzmechanismen in der Richtlinie selbst wesentlich ausdifferenzierter sein müssen als dies vom EU-Gesetzgeber angelegt gewesen war. Damit wird – tendenziell vergleichbar der soeben skizzierten, vom Bundesverfassungsgericht aus den Grundrechten abgeleiteten Wesentlichkeitslehre zum Gesetzesvorbehalt – ein Wesentlichkeitsmaßstab für die Richtlinie aufgestellt: Die Sicherung der Grundrechtsstandards kann also nicht dem nationalen Umsetzungsgesetzgeber überlassen werden, sondern muss in den wesentlichen Elementen im Richtlinientext selbst durch den Unionsgesetzgeber angelegt und damit legitimiert sein.

Dieses Anforderungsprofil gilt für das gesamte Sekundärrecht der EU und damit auch für Verordnungen. Das ist in der datenschutzrechtlichen Rechtsprechung bereits früh im Urteil des EuGH zur Agrar-Verordnung angeklungen.[47] In dem Fall ging es um die in einer Verordnung der EU vorgesehene Veröffentlichungspflicht von Agrarsubventionen. Hinsichtlich der Erforderlichkeit jener Veröffentlichungspflicht merkte der EuGH an, dass Ausnahmen und Einschränkungen in Bezug auf personenbezogene Daten auf das „absolut Notwendige" zu beschränken sind.[48] So sei ein milderes Mittel zur Zweckerreichung durchaus gegeben. Denn das legitime Ziel werde auch dann erreicht, wenn sich bei natürlichen Personen die Veröffentlichung auf bestimmte Empfänger von Agrarbeihilfen beschränke. Hierbei könne beispielsweise nach Kriterien des Bezugszeitraums, der Bezugshäufigkeit und der Art und des Umfangs des Bezugs differenziert werden. Da die Verordnungen dies nicht vorgäben, fehle es an der Erforderlichkeit der Veröffentlichungspflicht.[49] Damit wird im Ergebnis auch hier eine verhältnismäßigkeitsorientierte legislative Ausdifferenzierung für

---

46 EuGH, Urteil vom 8.4.2014, verb. Rs. C-293/12 u. C-594/12, ECLI:EU:C:2014:238 – *Digital Rights Ireland und Seitlinger u.a.*; siehe dazu und zu den folgenden Ausführungen bereits *Kühling*, Der Fall der Vorratsdatenspeicherungsrichtlinie und der Aufstieg des EuGH zum Grundrechtsgericht, NVwZ 2014, 681 ff.

47 Siehe zum Folgenden bereits *Kühling/Klar*, Transparenz vs. Datenschutz – erste Gehversuche des EuGH bei der Anwendung der Grundrechtecharta, JURA 2011, 771 ff.

48 EuGH, Urteil vom 9.11.2010, Rs. C-92/09 und C-93/09, ECLI:EU:C:2010:662 – *Schecke und Eifert*, Rn. 77.

49 EuGH, Urteil vom 9.11.2010, Rs. C-92/09 und C-93/09, ECLI:EU:C:2010:662 – *Schecke und Eifert*, Rn. 79 ff.

eine angemessene Ausbalancierung der Interessen durch den Gesetzgeber verlangt, die allerdings in ihrer Strenge davon abhängt, wie scharf der staatliche Eingriff ist.

b) Spannungsverhältnis von Normenbestimmtheit und Normenklarheit

Ergänzend verlangt die Normenklarheit die Erkennbarkeit, Verständlichkeit und Nachvollziehbarkeit des Regelungsgehalts, d. h. anwendungsfreundliches Recht. Diese Anforderungen der Normenklarheit stehen in einem austarierungsbedürftigen Spannungsverhältnis zur notwendigen Normenbestimmtheit. Allerdings zeigt gerade das Datenschutzrecht, dass die Klarheit von Normen unter einer hohen Regelungsdichte und -tiefe tendenziell leidet.[50] Normenklarheit bedeutet im Datenschutzrecht, jedenfalls dass die Normadressaten den Regelungsgehalt und vor allem den Verwendungszweck der Daten klar erkennen können müssen,[51] und auch eine effektive judikative Rechtskontrolle möglich ist.[52]

c) Weite Regelungsfreiheit für EU-Gesetzgeber bei Regelung der Verarbeitung von elektronischen Kommunikationsdaten durch Private

Zwischen privaten Akteuren ohne spezifische hoheitliche Anordnung von Datenverarbeitungen aus öffentlichen (primär sicherheitspolitischen) Interessen verfügt der Unionsgesetzgeber dagegen über einen weiten rechtlichen Spielraum hinsichtlich der Regelungstiefe und damit auch der Frage, ob er sektorspezifische Regelungen erlassen möchte oder auf die Anwendung der vorhandenen allgemeinen Regeln setzt, die in der gerichtlichen bzw. exekutiven Anwendungspraxis gegebenenfalls einer stärkeren Konkretisierung bedürfen. Das gilt sowohl allgemein als auch konkret in Bezug auf die Regulierung von elektronischen Kommunikationsdiensten. So hat der EuGH mit Urteil vom 13. Juni 2019 – wenn auch mit wenig überzeugender Begründung – entschieden, dass interpersonelle Kommunikationsdienste wie Web-Mail-Dienste (im konkreten Fall Gmail) nach bislang geltendem Recht nicht als elektronische Kommunikationsdienste einzustufen sind.[53] Damit hat der EuGH diese dem allgemeinen Datenschutzrecht unterworfen, ohne insoweit primärrechtliche Bedenken zu formulieren. Gerade diese Dienste sollen aber künftig ausdrücklich unter den erweiterten

50 Dazu allgemein *Petersen*, Grenzen des Verrechtlichungsgebotes im Datenschutz, 2000, S. 113.
51 Vgl. dazu grundlegend im deutschen Recht BVerfGE 65, 1 (62).
52 Siehe dazu wiederum im deutschen Recht BVerfGE 110, 33 (54).
53 EuGH, Urteil vom 13.6.2019, Rs. C-193/18, ECLI:EU:C:2019:498 – *Gmail*.

Anwendungsbereich der ePrivacy-VO fallen,[54] also fortan sektorspezifisch und nicht mehr allgemein datenschutzrechtlich geregelt werden. Dagegen hat der EuGH in einem anderen Verfahren „SkypeOut" als elektronischen Kommunikationsdienst im Sinne des bisherigen Telekommunikations-Richtlinienrechts eingestuft.[55] Auch wenn der EuGH in einem Vorlageverfahren nur die aufgeworfenen Fragen beantwortet, hätte es nahe gelegen, etwaige grundrechtliche Zweifel an einem engen Verständnis des Begriffs der elektronischen Kommunikation mit Blick auf die datenschutzrechtliche Ausgestaltung zu thematisieren. Insofern zeigt sich damit zumindest implizit, dass die Einschlägigkeit des sektorspezifischen Rechtsrahmens für verschiedene moderne elektronische Kommunikationsformen faktisch weitgehend flexibel durch den Unionsgesetzgeber im Rahmen der Definition des jeweiligen Anwendungsbereichs fixiert werden kann, ohne dass insoweit durchgreifende primärrechtliche Steuerungsvorgaben relevant wären.

2. Unionsgrundrechtliche Anforderungen eines angemessenen Datenschutzes gemäß Art. 7 und 8 GrCh

Art. 7 GrCh normiert das Recht auf Achtung des Privatlebens und der Kommunikation und entspricht in Formulierung und Gewährleistungsgehalt weitgehend Art. 8 EMRK. Der Europäische Konvent, der den Text der Charta formuliert hat, stellt fest, dass die Rechte nach Art. 7 GrCh den Rechten entsprechen, die durch Art. 8 EMRK garantiert werden. Sie haben daher gemäß Art. 52 Abs. 3 GrCh grundsätzlich die gleiche Bedeutung und Tragweite wie die Konventionsrechte. Lediglich der Begriff der Korrespondenz wurde durch den Begriff der Kommunikation ersetzt, ohne dass sich hieraus materielle Unterschiede ergäben.[56]

Mit dem Inkrafttreten der Grundrechtecharta im Jahr 2009 hat auch der EuGH die Gelegenheit ergriffen, die Entsprechung des Art. 7 GrCh mit Art. 8 EMRK sowohl in der Gewährleistungs- als auch in der Rechtfertigungsdimension festzustellen.[57] Geschützt ist damit insbesondere das Brief-, Post- und Telekommunikationsgeheimnis, wobei auch moderne Formen der Kommunikation (E-

---

54 Siehe Art. 4 und Art. 12 – 14 ePrivacyVO-KOM-E.

55 EuGH, Urteil vom 5.6.2019, Rs. C-142/18, ECLI:EU:C:2019:460 – *Skype*.

56 Erläuterungen des Präsidiums des Europäischen Konvents, ABl. EU 2004, C 310, 430; *Jarass*, EU-Grundrechte, 2005, § 12, Rn. 2 f.; *Bernsdorff*, in: Meyer (Hrsg.), Kommentar zur Charta der Grundrechte der Europäischen Union, 4. Aufl. 2014, Art. 7 Rn. 24; *Grabenwarter*/*Pabel*, EMRK, 6. Aufl. 2016, § 22, Rn. 10; *Kingreen*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, 5. Aufl. 2016, Art. 7 GrCh, Rn. 10.

57 EuGH, Urteil vom 9.11.2010, Rs. C-92/09 u. C-93/09, ECLI:EU:C:2010:662 – *Schecke und Eifert*, Rn. 52, 59, 72 u. 87.

Mail, SMS) in den Schutzbereich fallen.[58] Der effektive Schutz der Vertraulichkeit der (vermittelten) Kommunikation verlangt nicht nur die Gewähr der Vertraulichkeit des Inhalts der Kommunikation, sondern beinhaltet auch den Schutz vor Kenntnisnahme der Umstände der Kommunikation durch Dritte. Solche Kommunikationsumstände stellen die bei der Kommunikation erzeugten Kommunikationsdaten (z.B. Verkehrsdaten) dar. Diese können Aufschluss geben über Ort, Zeit, Dauer und weitere Informationen der Kommunikation einer Person.[59] Als personenbezogene Daten fallen sie jedoch auch in den grundsätzlich spezielleren Schutzbereich des Art. 8 GrCh.

Für die Rechtfertigung des Eingriffs ist vor allem Art. 52 GrCh zu beachten. Art. 8 Abs. 2 S. 1 GrCh enthält eine Qualifikation der Einschränkungsgründe.[60] So werden neben dem Erfordernis einer gesetzlichen Grundlage weitere, in der datenschutzrechtlichen Dogmatik und in der Datenschutzgesetzgebung entwickelte Vorgaben primärrechtlich verankert: nämlich zum einen der Zweckbindungsgrundsatz und zum anderen die dreipolige Zulässigkeitsregelung aus Einwilligung, gesetzlicher Spezial- und Allgemeinregelung.

Somit weist Art. 8 GrCh sowohl von der Ausrichtung des Schutzbereichs als auch von der Ausdifferenzierung der Schranken für einen Eingriff in diesen Schutzbereich Besonderheiten auf. Es spricht daher durchaus einiges dafür, die Bestimmung grundsätzlich als *lex specialis* gegenüber Art. 7 GrCh anzuwenden.[61] Zunächst stellte der EuGH insoweit auch fest, dass Art. 8 Abs. 1 GrCh in einem engen, konkretisierenden Verhältnis zu Art. 7 GrCh stehe,[62] ohne damit jedoch insoweit eine grundlegende und dogmatisch überzeugende Abgrenzung vorzunehmen. Später wurde indes deutlich, dass das Gericht beide Grundrechte nebeneinander anwendet und weitgehend parallel begreift.[63]

Insofern lässt sich der Architektur der Grundrechtecharta und auch der Rechtsprechung des EuGH gerade *nicht* entnehmen, dass elektronische Kommunikationsdaten grundrechtlich über Art. 7

---

58 *Kingreen*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, 5. Aufl. 2016, Art. 7 GrCh, Rn. 10; vgl. auch *Schorkopf*, in: Ehlers (Hrsg.), Europäische Grundrechte und Grundfreiheiten, 4. Aufl. 2015, § 16 II 1, Rn. 25; *Jarass*, Kommentar zur Charta der Grundrechte der Europäischen Union, 3. Aufl. 2016, Art. 7, Rn. 31.

59 *Jarass*, Kommentar zur Charta der Grundrechte der Europäischen Union, 3. Aufl. 2016, Art. 7, Rn. 31.

60 Vgl. auch *Schorkopf*, in: Ehlers (Hrsg.), Europäische Grundrechte und Grundfreiheiten, 4. Aufl. 2015, § 16 III 3, Rn. 47.

61 *Jarass*, Kommentar zur Charta der Grundrechte der Europäischen Union, 3. Aufl. 2016, Art. 8, Rn. 4; *Kingreen*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, 5. Aufl. 2016, Art. 8 GrCh, Rn. 1 f.; *Wolff*, in: Pechstein/Nowak/Häde (Hrsg.), Frankfurter Kommentar EUV, GRC, AEUV, Bd. 1, 2017, Art. 8 GrCh, Rn. 3.

62 EuGH, Urteil vom 9.11.2010, C-92/09 u. C-93/09, ECLI:EU:C:2010:662, Rn. 47 – *Schecke und Eifert*.

63 EuGH, Urteil vom 8.4.2014, C-293/12 und C-594/12, ECLI:EU:C:2014:238 – *Digital Rights Ireland und Seitlinger u.a.*; vgl. jüngst auch EuGH, Gutachten 1/15 vom 26.7.2017, ECLI:EU:C:2017:592, Rn. 133 – *PNR-Abkommen mit Kanada.*

GrCh *per se* strenger geschützt sind als sonstige Kommunikationsdaten über Art. 8 GrCh. Vielmehr kommt es auf die konkret betroffenen Daten (Wie sensibel sind diese?) und auf die Tiefe des Eingriffs an (Geht es etwa um eine Vorratsdatenspeicherung?). So lassen sich etwa aus dem bereits angeführten strengen Urteil zur Vorratsdatenspeicherungs-Richtlinie[64] und aus dem tendenziell noch strengeren *Tele-2-Sverige*-Urteil des EuGH[65] primär Schlussfolgerungen für den aus Sicht des EuGH besonders massiven Eingriffs der Vorratsdatenspeicherung von elektronischen Kommunikationsdaten ziehen, nicht jedoch für die Frage einer Verarbeitung dieser Daten zur Ermöglichung von Diensten, die vom Betroffenen gewünscht sind. Schon grundrechtlich handelt es sich im einen Fall um einen „klassischen" und als besonders schwer angesehenen Eingriff im „Staat-Bürger"-Verhältnis, während es im anderen Fall um eine Grundrechtsabwägung in einer komplexen multipolaren Grundrechtskonstellation mit privaten Akteuren auf beiden Seiten geht (dazu sogleich ausführlicher unter 3.). Im Übrigen hat der EuGH auch in den Fällen zur Vorratsdatenspeicherung Art. 7 und Art. 8 GrCh parallel geprüft, ohne zwischen den beiden Grundrechten und zwischen einer Verarbeitung elektronischer und sonstiger Daten insoweit zu differenzieren. Auch jüngere Urteile deuten keineswegs auf eine abweichende Entwicklung hin. So hat der EuGH etwa im jüngsten *Planet-49*-Urteil vom 1. Oktober 2019 lediglich eine Analyse des Sekundärrechts durchgeführt und ist auf grundrechtliche Überlegungen gar nicht eingegangen.[66]

Ganz grundsätzlich verfolgt der EuGH allerdings eine tendenziell strenge Beschränkung der Datenverarbeitung auf das „absolut Notwendige".[67] Gerade mit Blick auf die Einwilligung ist vor diesem Hintergrund durchaus davon auszugehen, dass der EuGH die strengen Vorgaben der Informiertheit und Freiwilligkeit aus Art. 4 Nr. 11 und Art. 7 (sowie 8) DS-GVO auch aus dem grundrechtlichen Anforderungsprofil des Art. 8 (und 7) GrCh ableiten wird. Umgekehrt ist es umso wichtiger, die gegenläufigen Interessen herauszuarbeiten, die eine Eröffnung von Datenverarbeitungsmöglichkeiten gegebenenfalls notwendig machen.

---

64 EuGH, Urteil vom 8.4.2014, verb. Rs. C-293/12 u. C-594/12, ECLI:EU:C:2014:238 – *Digital Rights Ireland und Seitlinger u.a*.

65 EuGH, Urteil vom 21.12.2016, verb. Rs. C-203/15 und C-698/15, ECLI:EU:C:2016:970 – *Tele2 Sverige AB*.

66 EuGH, Urteil vom 1.10.2019, Rs. 673/17, ECLI:EU:C:2019:801 – *Planet49 GmbH*. So bezieht sich folgender Satz (Rn. 46 des Urteils) explizit auf die Auslegung des geltenden Sekundärrechts bzw. einer spezifischen Norm und gibt keinerlei grundrechtliche Schranke vor: „Nach dieser Klarstellung ist darauf hinzuweisen, dass Art. 5 Abs. 3 der Richtlinie 2002/58 die Mitgliedstaaten dazu verpflichtet, sicherzustellen, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46 u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat."

67 Zuletzt EuGH, Gutachten 1/15 v 26.7.2017, ECLI:EU:C:2017:592 – *PNR-Abkommen mit Kanada,* Rn. 140.

3. „Free flow of data" und unternehmerische Freiheit aus Art. 16 GrCh; Medienfreiheit aus Art. 11 Abs. 2 GrCh und weitere Grundrechtspositionen als gegenläufige Interessen

Diese bisherige Rechtsprechung des EuGH gibt insgesamt Anlass zur Sorge, dass der Luxemburger Gerichtshof diese gegenläufigen (Grund-)Rechtspositionen zu gering bewertet.[68] Insgesamt ist eine strikte Kontrolle zu beobachten, bei der nicht hinreichend deutlich wird, was – bei aller Berechtigung des Datenschutzes – dessen ganz besondere Verdrängungskraft gegenüber anderweitigen Grundrechtspositionen begründet. Das ist im Safe-Harbor-Urteil besonders deutlich geworden, in dem der EuGH das Safe-Harbor-Abkommen verworfen hat, ohne dass klar wurde, wie die davon betroffenen 4400 Unternehmen kurzfristig ihren transatlantischen Datenaustausch rechtssicher organisieren können. Einen Übergangszeitraum hat der EuGH nicht näher erwogen und pragmatische Reaktionen sind anschließend den nationalen Datenschutzbehörden überantwortet worden. Der EuGH betonte stattdessen, dass Ausnahmen vom Schutz personenbezogener Daten auf das absolut Notwendige zu beschränken seien.[69] Die Möglichkeiten, Unternehmens- oder Nutzerinteressen hinreichend zu gewichten, sind durch diesen Maßstab durchaus begrenzt.

Jene gegenläufigen Schutzpositionen aus dem Blick zu verlieren, gefährdet nicht nur berechtigte Interessen der Unternehmen, sondern auch derjenigen Nutzer, die etwa einen größeren Wert auf einfach zugängliche, kostenlose, datenintensive Dienste legen als auf einen möglichst hohen Datenschutz. Jene Ausübung einer informationellen Selbstbestimmung oder Datensouveränität darf nicht einfach übergangen werden. Dabei ist die multipolare Grundrechtssituation tendenziell anders zu beleuchten als bei der isolierten Bewertung einer gesetzlichen Speicherpflicht oder behördlicher Zugriffsrechte auf die zu speichernden Datenbestände. Vor diesem Hintergrund ist es problematisch, dass der EuGH im Safe-Harbor-Urteil die insoweit einschlägigen Grundrechtsnormen, namentlich die unternehmerische Freiheit aus Art. 16 GrCh, gegebenenfalls die allgemeine Handlungsfreiheit als allgemeiner Rechtsgrundsatz, nicht näher angeführt hat.[70] Auch im Google-Spain-Urteil hat der EuGH die gegenläufigen Grundrechtspositionen der unternehmerischen Freiheit von

---

68 Siehe zu einer Aufzählung der bislang angeführten gegenläufigen Schutzinteressen *Schneider*, in: Wolff/Brink, BeckOK Datenschutzrecht, Kommentar, Stand: 1.5.2018, Syst. B Rn. 29.1.; siehe zum Folgenden bereits *Kühling/Raab*, in: Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung/BDSG, Kommentar, 2. Aufl. 2018, Einführung, Rn. 30 ff.

69 EuGH, Urteil vom 6.10.2015, Rs. C-362/14, ECLI:EU:C:2015:650 – *Schrems*, Rn. 91 f.

70 Zu dieser Kritik bereits *Kühling/Heberlein*, EuGH „reloaded": „unsafe Harbor" USA vs. „Datenfestung" EU, NVwZ 2016, 7 (12).

Google, der Pressefreiheit des von der Streichung des Links betroffenen Presseunternehmens und den öffentlichen Informationsinteressen im Rahmen der Auslegung der DSRL 95/46/EG nicht näher thematisiert.[71] Das konnte jedoch noch als Zurückhaltung gegenüber einer weiteren Ausdifferenzierung des Löschanspruchs auch im Verbund mit den mitgliedstaatlichen Gerichten verstanden werden.[72] Genauso ist es nun gekommen: So hat der EuGH im ganz aktuellen zweiten Google-Urteil vom 24. September 2019 für die Frage der Reichweite des Auslistungsanspruchs gegenüber dem Suchmaschinenbetreiber die gegenläufigen Interessen der Informationsfreiheit klarer in den Blick genommen und dabei unterschiedliche Abwägungsergebnisse innerhalb der EU für möglich gehalten.[73]

Insgesamt sind vor dem Hintergrund der konfligierenden Grundrechtspositionen in der Grundrechtecharta in multipolaren Grundrechtskonstellationen diese – teils – gegenläufigen Grundrechte gleichermaßen zu berücksichtigen. Das betrifft regelmäßig die unternehmerische Freiheit nach Art. 16 GrCh, teils aber auch spezifischere Grundrechtspositionen. Geht es etwa um die (Teil-)Finanzierung von Medienprodukten über Datenverarbeitungsprozesse greift zusätzlich die Medienfreiheit aus Art. 11 Abs. 2 GrCh. Diese schützt auch davor, dass legislative Maßnahmen die Finanzierungsbedingungen der Medien gefährden.[74] Insoweit geht es vor allem darum, dass die geschaffenen Regelungen auch faktisch eine Finanzierbarkeit der Mediendienste ermöglichen. Da Online-Mediendienste existenziell auf die Werbeeinnahmen angewiesen sind, die je nach Ausgestaltung der Verarbeitungsregeln in der ePrivacy-VO stark beeinträchtigt werden können wie etwa die im Sachverhalt angeführten Studien und Erhebungen belegen, darf dieser Finanzierungskanal nicht gefährdet werden. Andernfalls läge ein massiver Eingriff in die Medienfreiheit nach Art. 11 Abs. 2 GrCh vor, der sich nicht mit etwaigen datenschutzrechtlichen Interessen rechtfertigen ließe und auch nicht im Einklang stünde mit einem angemessenen Verständnis der informationellen Selbstbestimmung. In diesem Zusammenhang ist darauf hinzuweisen, dass Art. 11 Abs. 2 GrCh vom Konvent zur Schaffung einer Grundrechtcharta gerade deshalb eigens aufgenommen wurde, um der besonderen Schutzbedürftigkeit der Medien einschließlich ihrer Finanzierungslogik gerecht zu werden. Viele Konventsmitglieder forderten gerade deshalb eine eigenständige Erwähnung der

---

71 EuGH, Urteil vom 13.5.2014, Rs. C-131/12, ECLI:EU:C:2014:317 – *Google Spain*.

72 So bereits *Kühling*, Rückkehr des Rechts: EuGH verpflichtet „Google & Co." zu Datenschutz, EuZW 2014, 527 (529 f.).

73 EuGH, Urteil vom 24.9.2019, Rs. C-507/17, ECLI:EU:C:2019:772 – *Google LLC*, Rn. 67 ff.

74 Vgl. *Kühling*, § 24: Medienfreiheit (Rundfunk-, Presse- und Filmfreiheit), in: Heselhaus/Nowak (Hrsg.), Handbuch des Grundrechtsschutzes in der Europäischen Union, 2006, Rn. 60.

Medienfreiheit. Die Argumente dafür waren vor allem die Sorge um die Absicherung der Meinungs- und Informationsvielfalt und Pluralität angesichts einer verstärkten Medienkonzentration (die „mittlerweile Orwell'sche Ausmaße angenommen" habe), die herausragende Stellung der Pressefreiheit als „eines der vornehmsten Rechte in einem demokratischen und rechtsstaatlichen Gemeinwesen", die „Aushängeschild für eine moderne und freiheitliche Verfassung und von existentieller Bedeutung" sei.[75] Die Sicherung der Finanzierungsbedingungen von Medienangeboten auch über – personalisierte – Werbung und die dazu erforderliche Datenverarbeitung sind daher in einem angemessenen Maß ebenso zu gewährleisten wie etwaige eigentumsrechtliche Einschränkungen gemäß Art. 17 GrCh hinzunehmen sind, sofern es um die Ermöglichung der Datenverarbeitung in den Endgeräten des Nutzers geht. Damit ist grundrechtlich keineswegs vorgezeichnet, dass insoweit nur eine Einwilligung als Zulässigkeitstatbestand in Betracht kommt bzw. wie dieser konkret ausgestaltet sein soll. Entscheidend ist allein, dass eine angemessene Balance gefunden wird zwischen den betroffenen Interessen, was einzelne Ausgestaltungen, die eine Grundrechtsposition ohne hinreichend gewichtige Gründe allzu sehr zurückdrängt (etwa die Medienfreiheit in Form der Finanzierungserforderlichkeiten von Mediendiensten), als nicht grundrechtskonform qualifiziert (dazu sogleich 4. – 6.).

4. Allgemeine Konsequenzen für die Interessenabwägung im Rahmen der Schaffung einer ePrivacy-VO

Mit Blick auf die Abwägung der vorliegend relevanten Interessen ist darauf hinzuweisen, dass es in den Google-Fällen um offensichtliche Löschinteressen der betroffenen Personen ging, die selbst keinen Dienst in Anspruch nehmen möchten, sondern gleichsam „Gegenstand eines Dienstes" sind. Vorliegend besteht hingegen die oben bereits skizzierte abweichende Interessenlage, dass die betroffenen Personen ein Interesse an den Datenverarbeitungsprozessen haben können, sofern dies zur Verbesserung der Dienste beiträgt und/oder zu deren Finanzierung in angemessener bzw. „fairer"[76] Art und Weise. So verlangt Art. 8 Abs. 2 GrCh in grundrechtlicher Perspektive: „data must

---

[75] Siehe dazu die umfassenden Nachweise bei *Bernsdorff/Borowski*, Die Charta der Grundrechte der Europäischen Union. Handreichungen und Sitzungsprotokolle, 2002, S. 188 f., 288 f.; ausführlich dazu auch *v. Coelln*, in: Stern/Sachs (Hrsg.), Europäische Grundrechtecharta, Kommentar, 2016, Art. 11 Rn. 1 ff.

[76] Zur Verankerung des Fairness-Konzepts im europäischen Datenschutzrecht *Kalimo/Majcher,* The concept of fairness: Linking EU competition and data protection law in the digital marketplace*,* E. L. Rev. 2017, S. 210 ff.

be processed fairly".[77] Dieser in Art. 5 lit. a DS-GVO auch sekundärrechtlich kodifizierte Grundsatz beinhaltet sowohl eine prozedurale bzw. formale Komponente, insbesondere im Sinne einer Transparenz der Datenverarbeitung, als auch eine materielle Fairness-Komponente, die im Rahmen der Verhältnismäßigkeit einer Datenverarbeitung bzw. bei der Feststellung der Freiwilligkeit einer Einwilligung von Bedeutung ist.[78]

Dabei beruht etwa die Einwilligung auf dem Prinzip der Waffengleichheit der beteiligten Akteure, also des Datenverarbeiters und der betroffenen Person. Unter dieser Prämisse kann unterstellt werden, dass die Beteiligten ihre Rechtsbeziehungen eigenverantwortlich regeln können.[79] Sind die Bedingungen für eine selbstbestimmte Entscheidung der betroffenen Person als datenpreisgebende Seite erfüllt, kann die so gefällte Entscheidung als fair bezeichnet werden. Diese Kriterien verlangen somit einen zu sichernden Mindeststandard, der für eine privatautonome Entscheidungsfindung notwendig ist. Eine zu starke Aufladung der materiellen Kriterien und eine damit einhergehende Einschränkung der kommerziellen Nutzbarkeit von Daten konfligiert wiederum mit dem Leitbild des auf selbstbestimmter Entscheidung beruhenden Datenschutzes und kann demzufolge nicht automatisch als datenschutzfördernd betrachtet werden. Letztlich entsteht ein Konflikt zwischen dem Fremdschutz der Privatheit, etwa über das datenschutzrechtliche Erforderlichkeitskriterium oder eine Einschränkung der Kopplungsmöglichkeiten einer Einwilligungserklärung, und dem Selbstschutz des Einzelnen im Rahmen seiner privatautonomen Möglichkeiten.

Die Defizite des Informationsmodells insbesondere im Rahmen der Einwilligung als Legitimationstatbestand (Schwierigkeiten bei der Herstellung von Transparenz, Verständlichkeit etc.) verweisen auf einen fließenden Übergang zu abwägungsoffenen, stark wertungsabhängigen materiellen Fairnessgrundsätzen. Diese sind etwa in Tatbeständen wie der Erforderlichkeit oder in der Freiwilligkeit zu verorten, die eine genauere, kontextabhängige Analyse des wirtschaftlichen und wettbewerblichen Kontextes der Datenerhebung erforderlich machen. Insoweit ist es keineswegs trivial, materielle Steuerungsnormen zu entwickeln, die sich vom Informationsmodell entfernen und die Maßstäbe beispielsweise in Anbetracht deutlicher Machtasymmetrien enger fassen. Im Rahmen der Überlegungen zur rechtlichen Ausgestaltung sollten vor diesem Hintergrund auch die Auswirkungen der Abfassung der Zulässigkeitstatbestände auf die Marktstruktur berücksichtigt werden:

---

77 Weniger „sprechend" ist hier der deutsche Wortlaut: „nach Treu und Glauben".

78 Insoweit wiederum *Kalimo/Majcher,* The concept of fairness: Linking EU competition and data protection law in the digital marketplace*,* E. L. Rev. 2017, S. 220 f.

79 Vgl. *Kalimo/Majcher,* The concept of fairness: Linking EU competition and data protection law in the digital marketplace*,* E. L. Rev. 2017, S. 218.

So sollten die Anforderungen so formuliert sein, dass sie insbesondere nicht eine Marktkonzentration beflügeln, da diese im Anschluss wiederum den Rückgriff auf die Einwilligung im Falle dann gestärkter Marktstellungen erschwert.[80]

Im Übrigen muss das Regelwerk in seiner Gesamtheit diesem Ausgleich gerecht werden: Je enger also Zulässigkeitstatbestände gefasst werden, desto größer ist die Bedeutung der Einwilligung, ebenso wie umgekehrt gilt, je strenger die Anforderungen an die Einwilligung, desto wichtiger sind die übrigen Zulässigkeitstatbestände. Dabei ist dafür zu sorgen, dass die Anforderungen an die Zulässigkeitstatbestände einschließlich einer Einwilligung rechtlich wie auch faktisch und technisch erfüllbar sind. Das gilt insbesondere für die Möglichkeiten der Erteilung einer Einwilligung und hier für die Frage, ob der Zugang zu einem werbefinanzierten Angebot von der Erteilung einer Einwilligung abhängig gemacht werden kann. Werden die vorgesehenen Regelungen dabei so anspruchsvoll formuliert, dass sie nur schwer erfüllbar sind, müssen die übrigen Zulässigkeitstatbestände so formuliert werden, dass sie die Datenverarbeitung im erforderlichen Umfang ermöglichen und so für einen sinnvollen Interessenausgleich sorgen. Davon unabhängig unterliegen aber auch die Einzelnormen den aufgezeigten Interessenabwägungen. So kann beispielsweise nicht eine enge Fassung der Zulässigkeitstatbestände zur Begründung eines Einwilligungstatbestandes herangezogen werden, der das auch grundrechtlich indizierte Maß an Transparenz oder Freiwilligkeit nicht gewährleistet.

Gleichwohl verbleibt dem Gesetzgeber vor diesem Hintergrund ein weiter Spielraum, wie er die konfligierenden Interessen gegeneinander abwägt und dabei einen angemessenen Datenschutz generiert, der die notwendige, freiheitsschützende Datenverarbeitung eröffnet, die im Interesse des Datenverarbeiters ist, aber im Falle der Wahrung der Fairness der Datenverarbeitung auch im Interesse der betroffenen Person sein sollte. Diese wollen die entsprechenden Dienste nämlich gegebenenfalls ohne pekuniäres Entgelt nutzen. Auch wenn es dazu bislang noch keine Rechtsprechung

---

[80] Siehe dazu kritisch mit Blick auf die strengen Anforderungen an die Zulässigkeit von Datenverarbeitungsprozessen in den Entwürfen der ePrivacy-VO die *Monopolkommission* im jüngsten Hauptgutachten, 2018, S. 401 ff., https://www.monopolkommission.de/images/HG22/HGXXII_Kap4_Medien.pdf; sehr kritisch auch *WIK*, Economic Impact of the ePrivacy Regulation on Online Advertising and Ad-based Digital Business Model, 2017, https://www.wik.org/fileadmin/Studien/2017/2017_ePrivacy-BMW.pdf; vor diesem Hintergrund ferner kritisch gegenüber einem strengen Verständnis der gemeinsamen Verantwortlichkeit, das die Anreize für eine Marktkonsolidierung mit einer stärkeren Binnenverarbeitung erhöht, *Hanloser*, https://betriebs-berater.ruw.de/bb-standpunkte/standpunkte/Bremst-der-Datenschutz-die-smarte-Zukunft-aus--eine-moegliche-Konsequenz-auch-aus-der-EuGH-Entscheidung-Fashion-ID-38932, in Reaktion auf das aktuelle Urteil des EuGH vom 29.7.2019, Rs. C-40/17, ECLI:EU:C:2019:629 – *Fashion ID*. Auch die Verlagerung der Zulässigkeit auf die Einwilligung sieht *Hanloser* als Konzentrationstreiber, da diese regelmäßig nur von großen Unternehmen mit unmittelbarem Kundenkontakt eingeholt werden kann; letzter Abruf aller Internet-Quellen 2.10.2019.

des EuGH gibt, sprechen überzeugende Gründe dafür, dass er sie wird entwickeln müssen, sobald entsprechende Verfahren in multipolaren Grundrechtskonflikten vom EuGH entschieden werden. Diese werden zunächst vor allem die Auslegung sekundärrechtlicher Normen zum Gegenstand haben, dabei gegebenenfalls aber – wie in den Google-Urteilen – auch grundrechtliche Überlegungen anstellen.[81]

5. Konkrete Konsequenzen für eine mögliche Ausgestaltung der Einwilligung in der ePrivacy-VO

a) Konsequenzen für die bisherigen Regelungsvorschläge

Die bislang vorgelegten Regelungsvorschläge genügen diesem Anforderungsprogramm nicht.

Das gilt bereits für den Vorschlag der Kommission. Insoweit ist auf die im Sachverhalt angeführten Studien zu verweisen (siehe oben A.IV.). Diese lassen es plausibel erscheinen, dass die Gesamtregelung, die zudem an erheblichen rechtlichen Unklarheiten leidet, zu erheblichen Ungleichgewichten zwischen den Geschäftsmodellen führen wird, und bei Mediendiensteanbietern außerhalb der großen Online-Plattformen das Erzielen hinreichender Werbeeinnahmen zur Finanzierung der Diensteangebote deutlich erschweren wird. Damit wäre mit Blick auf die Einschränkung der Finanzierungsnotwendigkeit ein erheblicher Eingriff in die Medienfreiheit aus Art. 11 Abs. 2 GrCh verbunden. Auch die Monopolkommission hat in ihrer Begutachtung der Vorschläge[82] darauf hingewiesen, dass die Entwürfe „einerseits die Position der ohnehin marktstarken Akteure im Online-Werbebereich, also der großen Online-Plattformen, im Vergleich zu anderen Marktteilnehmern weiter stärken, obwohl sie zugleich auch deren Geschäft negativ beeinflussen". Und weiter: „Andererseits werden die Möglichkeiten anderer Anbieter im Werbemarkt und die Refinanzierungs-

---

81 Im ganz aktuellen Urteil des EuGH im Fall des Vorabentscheidungsverfahrens Planet49 GmbH des BGH (EuGH, Urteil vom 1.10.2019, Rs. 673/17, ECLI:EU:C:2019:801 – *Planet49 GmbH*) hat der Luxemburger Gerichtshof diese Gelegenheit allerdings nicht ergriffen. Hier hatte Generalanwalt Szpunar in seinen Schlussanträgen vom 21.3.2019 neben strengen formalen Anforderungen hinsichtlich der eher materiell-rechtlichen Anforderungen mit Blick auf das Koppelungsverbot des Art. 7 Abs. 4 DS-GVO die Erforderlichkeit der Verarbeitung personenbezogener Daten für den Fall bejaht, „dass der hinter der Teilnahme am Gewinnspiel stehende Zweck der ‚Verkauf' personenbezogener Daten ist (d. h. die Einwilligung, von sogenannten ‚Sponsoren' mit Werbeangeboten kontaktiert zu werden). Mit anderen Worten besteht die Hauptpflicht, die der Nutzer erfüllen muss, um an dem Gewinnspiel teilnehmen zu können, darin, personenbezogene Daten zur Verfügung zu stellen.", Ziff. 99 der Schlussanträge unter Verweis auf *Buchner/Kühling*, in: Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung/BDSG, Kommentar, 2. Aufl. 2018, Art. 7 DS-GVO, Rn. 48.

82 *Monopolkommission*, XXII. Hauptgutachten v. 3.7.2018, Kapitel IV, Rz. 1198.

möglichkeiten kleinerer Inhalteanbieter geschwächt." Skeptisch werden auch dort die Vorteile in Bezug auf den Datenschutz bewertet. So heißt es im Folgenden: „Im Übrigen wäre hiermit auch dem Datenschutz sowie der Privatsphäre der Nutzer kaum geholfen."

Der Vorschlag des Europäischen Parlaments würde diese Situation noch verschärfen, da u.a. auch die Kommunikationsmöglichkeiten der Diensteanbieter – jenseits der großen Internet-Plattofrmen – mit ihren (potenziellen) Endkunden erheblich erschwert würden.

Auch der gegenwärtige Vorschlag des Rates schafft nicht die notwendige Rechtssicherheit insbesondere für kleinere Anbieter, die auf ein einwilligungsbasiertes werbefinanziertes Angebot setzen.

Insgesamt liegen damit erhebliche Eingriffe in die unternehmerische Freiheit aus Art. 16 GrCh und über die gefährdeten Finanzierungsmöglichkeiten gerade von nicht Log-In-basierten Geschäftsmodellen auch in die Medienfreiheit aus Art. 11 Abs. 2 GrCh vor, die nicht durch hinreichende Gründe des Datenschutzes gerechtfertigt werden können. Das gilt gerade vor dem Hintergrund, dass das Datenschutzgrundrecht nicht darauf abzielt, eine selbstbestimmte einwilligungsbasierte Nutzung von Diensten einschließlich einer darauf fundierten Finanzierung zu untersagen. Vielmehr ist es gerade Ausdruck der Selbstbestimmung, eine Einwilligung, sofern eine Freiwilligkeit angesichts der mangelnden Marktbeherrschung des Diensteanbieters möglich ist, zu eröffnen, wie schon der Wortlaut von Art. 8 Abs. 2 S. 1 GrCh deutlich macht.

b) Anforderungsprofil einer angemessenen Ausgestaltung

Die angeführten allgemeinen Anforderungen stehen dementsprechend in keiner Weise einer Ausgestaltung der Einwilligung (oder eines Zulässigkeitstatbestands) entgegen, die gerade zum Schutz der informationellen Selbstbestimmung auch Modelle einer datenfinanzierten Diensteerbringung ermöglicht („Leistung gegen Daten" statt oder neben einer „Leistung gegen Zahlung" bzw. gemischten Modellen).

Zur Wahrung der Freiwilligkeit ist dann allerdings darauf zu achten, dass marktmächtige Unternehmen nicht auf der Basis eines „take it or leave it" eine letztlich nicht „freiwillige" Entscheidung erzwingen können, da es kein vergleichbares alternatives Diensteangebot und damit keine Ausweichmöglichkeit gibt.[83] Hier könnten in der Konsequenz marktmächtige Unternehmen

[83] Siehe zu diesen Anforderungen bereits *Buchner/Kühling*, in: Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung/BDSG, Kommentar, 2. Aufl. 2018, Art. 7 DS-GVO, Rn. 52 ff.

verschiedene Entgeltmodelle anbieten müssen. In ersten Diskussionsentwürfen zum Kommissionsvorschlag für die ePrivacy-VO war dieser Ansatz im Rahmen der Erwägungsgründe für die Einwilligung zumindest insofern angeklungen, als alternative verfügbare Angebote und die Bezahlbarkeit im Fall von geldzahlungsbasierten Varianten als Kriterien für die Freiwilligkeit einer Einwilligung genannt werden.[84] Demnach entspricht es einer angemessenen Abwägung der Grundrechtspositionen, wenn eine Nutzung von nicht marktdominanten Diensten, die über personalisierte Werbung finanziert werden, von einer Einwilligung der dazu erforderlichen Datenverarbeitung abhängig gemacht wird, sofern diese hinreichend klar und transparent ist. Andernfalls wird ein Diensteangebot „Leistung gegen Daten" von vornherein ausgeschlossen.

Die Datenschutzgrundrechte verlangen es dabei keineswegs, dass ein datenfinanzierter Dienst in derselben Ausgestaltung und insbesondere kostenlos angeboten werden muss, wenn der Nutzer eine Finanzierung mit seinen Daten ablehnt. Dies entspricht schon nicht einem angemessenen Verständnis eines auf Selbstbestimmung ausgerichteten Datenschutzgrundrechts. Erst recht wäre dies nicht mit dem Ziel einer angemessenen Ausbalancierung in Bezug auf die unternehmerischen Interessen an der Finanzierung und damit auch dem Verbraucherinteresse an der weiteren Bereitstellung von Diensten in Einklang zu bringen. Im Fall der Finanzierung von Medienprodukten greift insoweit wiederum die Schutzwirkung der Medienfreiheit aus Art. 11 Abs. 2 GrCh ein (dazu oben 3.). Die Möglichkeit, einen Bedingungszusammenhang zwischen Datenverarbeitung und Dienstebringung herzustellen, ist daher außerhalb der soeben skizzierten Besonderheiten für marktbeherrschende oder marktstarke Unternehmen gesetzgeberisch zu achten.

Dieses Ergebnis und insbesondere ein grundsätzlich der DS-GVO entsprechendes, dort aber noch nicht hinreichend klar bestimmtes Kopplungsverbot bzw. Entkopplungsgebot gilt für jegliche Ausgestaltung eines etwaigen Zugangs von Diensteanbietern zu Daten auf den Endgeräten gemäß eines geplanten Art. 8 ePrivacy-VO sowie für alle Regelungen der Einwilligung in der ePrivacy-VO.

---

[84] Siehe Erwägungsgrund 22 einer inoffiziellen Version des Entwurfs der Kommission abrufbar unter http://www.politico.eu/wp-content/uploads/2016/12/POLITICO-e-privacy-directive-review-draft-december.pdf; letzter Abruf 2.10.2019.

6. Zwischenergebnis

Primärrechtlich vorgesteuert werden die oben (unter II.) aufgezeigten rechtspolitischen Überlegungen durch die rechtsstaatlichen Anforderungen an die Normbestimmtheit und Normenklarheit sowie durch die grundrechtlichen Vorgaben.

Die bisherige Rechtsprechung des EuGH lässt dem Unionsgesetzgeber – insbesondere mit Blick auf die Datenverarbeitung durch Unternehmen – grundsätzlich einen weiten Spielraum im Datenschutzrecht in Bezug auf die Frage, ob dieser bereichsspezifische Regelungen in Bezug auf die Datenverarbeitung durch Unternehmen treffen möchte oder nicht. Das gilt sowohl allgemein als auch konkret in Bezug auf die Regulierung von elektronischen Kommunikationsdiensten.

Dabei lässt sich der Architektur der Grundrechtecharta und auch der Rechtsprechung des EuGH gerade *nicht* entnehmen, dass elektronische Kommunikationsdaten grundrechtlich über Art. 7 GrCh *per se* strenger geschützt sind als sonstige Kommunikationsdaten über Art. 8 GrCh. Der Gerichtshof wendet beide Grundrechte nebeneinander an und begreift sie weitgehend parallel. Vielmehr kommt es auf die konkret betroffenen Daten (Wie sensibel sind diese?) und auf die Tiefe des Eingriffs an (Geht es etwa um eine Vorratsdatenspeicherung?).

Die – nur teilweise – widerstreitenden grundrechtlichen Anforderungen eines angemessenen Datenschutzes gemäß Art. 7 und 8 GrCh einerseits und insbesondere der unternehmerischen Freiheit aus Art. 16 GrCh andererseits, die einen „Free flow of data“ zu begründen vermögen, verlangen ebenfalls eine angemessene Interessensbalance und damit ausgewogene Zulässigkeitstatbestände. Allerdings verfügt der Gesetzgeber wiederum über einen erheblichen Spielraum. Strengere Schranken lassen sich dabei der Rechtsprechung des EuGH bislang vor allem hinsichtlich einer hinreichenden Berücksichtigung eines angemessenen Datenschutzes entnehmen. Dabei kann und gegebenenfalls muss der Gesetzgeber in unterschiedlichem Umfang eine datenfinanzierte Diensteerbringung eröffnen, und zwar jeweils soweit diese „faire“ Datenverarbeitungsmodelle und eine hinreichende Selbstbestimmung der betroffenen Person ermöglichen.

D. Ergebnisse

1. Der Grundsatz „Lex specialis derogat legi generali“ greift auch bei der Auslegung und Anwendung des EU-Sekundärrechts. Wenn danach für den besonderen Bereich der elektronischen Kommunikationsdienste in der ePrivacy-VO speziellere Regelungen in der Form geschaffen werden, dass diese für den spezifischen Anwendungsbereich strengere, weniger strenge oder schlicht abweichende Bestimmungen schaffen, gehen diese den vergleichbaren Bestimmungen in der DS-GVO vor.
2. Es gibt insoweit keine Besonderheiten in Bezug auf die DS-GVO. Vielmehr bestätigen die Regelungen in Art. 95 und 98 DS-GVO diesen Ansatz einer freien Spezialregelung in der noch geltenden ePrivacy-Richtlinie und der künftigen ePrivacy-VO.
3. Jene Regelungsfreiheit entspricht im Übrigen auch demokratietheoretischen Überlegungen.
4. Insbesondere gibt es keine Restriktion dogmatischer oder rechtssystematischer Art, dass für Spezialbereiche lediglich strengere (d.h. datenschutzfreundlichere) Bestimmungen geschaffen werden dürfen. Insofern greift auch keine Sperrwirkung („effet cliquet“) der DS-GVO. In der Konsequenz kann eine ePrivacy-VO strengere, weniger strenge und schlicht abweichende Regelungen gegenüber der DS-GVO in Bezug auf elektronische Kommunikationsdienste normieren, sofern dies im Einklang mit den rechtsstaatlichen und grundrechtlichen Vorgaben der Grundrechtecharta der EU (GrCH) steht.
5. Rechtspolitisch sind eine große Bandbreite an Ausgestaltungen denkbar. Sie reichen von einem gänzlichen Verzicht auf sektorspezifische Vorgaben bis hin zu einer Ausgestaltung eigenständiger Zulässigkeitstatbestände. Letzteres kann etwa in Form der Regelung von spezifischen Sonderfällen im Bereich der Erbringung elektronischer Kommunikationsdienste ggfls. einschließlich eines (spezifizierten) berechtigten Interesses sowie einer (ggfls. modifizierten) Einwilligung erfolgen.
6. Jegliche Ausgestaltung muss die verschiedenen, teilweise widerstreitenden Interessen an einer Datenverarbeitung auf der einen Seite und einem Verzicht darauf zum Schutz der Privatsphäre auf der anderen Seite zum Ausgleich bringen. Dabei muss es insbesondere auch darum gehen, dass die von den Konsumenten gewünschten Dienste unter Berücksichtigung eines angemessenen Datenschutzes der betroffenen Personen auskömmlich finanziert werden können, damit sie diesen auch weiterhin als Konsumenten zur Verfügung gestellt werden können. Ferner sollte die Regulierung wettbewerbsneutral ausfallen, d.h. den verschiedenen gleichermaßen geschützten Geschäftsmodellen bei der Werbefinanzierung vergleichbare Verwirklichungschancen einräumen.
7. Die bisherige Rechtsprechung des EuGH lässt dem Unionsgesetzgeber – insbesondere mit Blick auf die Datenverarbeitung durch Unternehmen – grundsätzlich einen weiten Spielraum im Datenschutzrecht hinsichtlich der Frage, ob dieser bereichsspezifische Regelungen treffen möchte oder nicht. Das gilt sowohl allgemein als auch konkret in Bezug auf die Regulierung von elektronischen Kommunikationsdiensten.

8. Dabei lässt sich der Architektur der Grundrechtecharta und auch der Rechtsprechung des EuGH gerade *nicht* entnehmen, dass elektronische Kommunikationsdaten grundrechtlich über Art. 7 GrCh *per se* strenger geschützt sind als sonstige Kommunikationsdaten über Art. 8 GrCh. Der Gerichtshof wendet beide Grundrechte nebeneinander an und begreift sie weitgehend parallel. Vielmehr kommt es auf die konkret betroffenen Daten (Wie sensibel sind diese?) und auf die Tiefe des Eingriffs an (Geht es etwa um eine Vorratsdatenspeicherung?).

9. Die – nur teilweise – widerstreitenden grundrechtlichen Anforderungen eines angemessenen Datenschutzes gemäß Art. 7 und 8 GrCh einerseits und insbesondere der unternehmerischen Freiheit aus Art. 16 GrCh andererseits, die einen „Free flow of data" zu begründen vermögen, verlangen eine angemessene Interessenbalance und ausgewogene Zulässigkeitstatbestände.

10. Geht es um die (Teil-)Finanzierung von Medienprodukten über Datenverarbeitungsprozesse greift zusätzlich die Medienfreiheit aus Art. 11 Abs. 2 GrCh. Diese schützt davor, dass legislative Maßnahmen die Finanzierungsbedingungen der Medien gefährden. Insoweit geht es vor allem darum, dass die geschaffenen Regelungen gleichermaßen auch faktisch eine Finanzierbarkeit der Mediendienste ermöglichen. Da Online-Mediendienste existenziell auf die Werbeeinnahmen angewiesen sind, die je nach Ausgestaltung der Verarbeitungsregeln in der ePrivacy-VO stark beeinträchtigt werden können, darf dieser Finanzierungskanal nicht gefährdet werden. Andernfalls läge ein massiver Eingriff in die Medienfreiheit nach Art. 11 Abs. 2 GrCh vor, der sich nicht mit etwaigen datenschutzrechtlichen Interessen rechtfertigen ließe und auch nicht im Einklang stünde mit einem angemessenen Verständnis der informationellen Selbstbestimmung.

11. Die Sicherung der Finanzierungsbedingungen von Medienangeboten auch über – personalisierte – Werbung und die dazu erforderliche Datenverarbeitung sind daher in einem angemessenen Maß ebenso zu gewährleisten wie etwaige eigentumsrechtliche Einschränkungen gemäß Art. 17 GrCh hinzunehmen sind, sofern es um die Ermöglichung der Datenverarbeitung in den Endgeräten des Nutzers geht. Damit ist grundrechtlich keineswegs vorgezeichnet, dass insoweit nur eine Einwilligung als Zulässigkeitstatbestand in Betracht kommt bzw. wie dieser konkret ausgestaltet sein soll. Entscheidend ist allein, dass eine angemessene Balance gefunden wird zwischen den betroffenen Interessen. Das schließt einzelne Ausgestaltungen, die eine Grundrechtsposition ohne hinreichend gewichtige Gründe allzu sehr zurückdrängen (etwa die Medienfreiheit in Form der Finanzierungserforderlichkeiten von Mediendiensten), als nicht grundrechtskonform aus.

12. Im Übrigen muss das Regelwerk in seiner Gesamtheit dem aufgezeigten Interessenausgleich gerecht werden: Je enger also Zulässigkeitstatbestände gefasst werden, desto größer ist die Bedeutung der Einwilligung, ebenso wie umgekehrt gilt, je strenger die Anforderungen an die Einwilligung, desto wichtiger sind die übrigen Zulässigkeitstatbestände. Dabei ist dafür zu sorgen, dass die Anforderungen an die Zulässigkeitstatbestände einschließlich einer Einwilligung rechtlich wie auch faktisch und technisch erfüllbar sind. Das gilt insbesondere für die Möglichkeiten der Erteilung einer Einwilligung und hier für die Frage, ob der Zugang zu einem werbefinanzierten Angebot von der Erteilung einer

Einwilligung abhängig gemacht werden kann. Werden die vorgesehenen Regelungen dabei so anspruchsvoll formuliert, dass sie nur schwer erfüllbar sind, müssen die übrigen Zulässigkeitstatbestände so formuliert werden, dass sie die Datenverarbeitung im erforderlichen Umfang ermöglichen und so für einen sinnvollen Interessenausgleich sorgen.

13. Dies steht in keiner Weise einer Ausgestaltung der Einwilligung (oder eines Zulässigkeitstatbestands) entgegen, die gerade zum Schutz der informationellen Selbstbestimmung auch Modelle einer datenfinanzierten Diensterbringung ermöglicht („Leistung gegen Daten“ statt oder neben einer „Leistung gegen Zahlung“ bzw. gemischten Modellen).

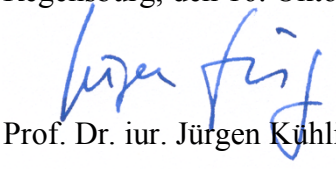
14. Die bislang vorgelegten Regelungsvorschläge genügen diesem Anforderungsprogramm nicht. Sie verdrängen einwilligungsbasierte werbefinanzierte Diensteangebote im Medienbereich jenseits der großen Internetplattformen. Insgesamt bedingen sie erhebliche Eingriffe in die unternehmerische Freiheit aus Art. 16 GrCh und über die gefährdeten Finanzierungsmöglichkeiten insbesondere von nicht Log-In-basierten Geschäftsmodellen auch in die Medienfreiheit aus Art. 11 Abs. 2 GrCh, die nicht durch hinreichende Gründe des Datenschutzes gerechtfertigt sind.

15. Zur Wahrung der Freiwilligkeit ist allerdings darauf zu achten, dass marktmächtige Unternehmen nicht auf der Basis eines „take it or leave it“ eine letztlich nicht „freiwillige“ Entscheidung vom Nutzer fordern können, da es kein vergleichbares alternatives Dienstangebot und damit keine Ausweichmöglichkeit gibt. Hier könnten in der Konsequenz marktmächtige Unternehmen verschiedene Entgeltmodelle anbieten müssen.

16. Die Datenschutzgrundrechte verlangen es hingegen keineswegs, dass ein datenfinanzierter Dienst in derselben Ausgestaltung und insbesondere kostenlos angeboten werden muss, wenn der Nutzer eine Finanzierung mit seinen Daten ablehnt. Dies entspricht schon nicht einem angemessenen Verständnis eines auf Selbstbestimmung ausgerichteten Datenschutzgrundrechts. Erst recht wäre dies nicht mit dem Ziel einer angemessenen Ausbalancierung mit Blick auf die unternehmerischen Interessen an der Finanzierung und damit auch dem Verbraucherinteresse an der weiteren Bereitstellung von Diensten in Einklang zu bringen. Die Möglichkeit, einen Bedingungszusammenhang zwischen Datenverarbeitung und Diensterbringung herzustellen, ist daher außerhalb der unter der vorangegangenen Ergebnisziffer dargelegten besonderen Konstellation marktbeherrschender bzw. marktstarker Unternehmen gesetzgeberisch zu achten.

17. Dieses Ergebnis und insbesondere ein grundsätzlich der DS-GVO entsprechendes, dort aber noch nicht hinreichend klar bestimmtes Kopplungsverbot bzw. Entkopplungsgebot gilt für jegliche Ausgestaltung eines etwaigen Zugangs von Diensteanbietern zu Daten auf den Endgeräten gemäß eines geplanten Art. 8 ePrivacy-VO sowie für alle Regelungen der Einwilligung in der ePrivacy-VO.

Regensburg, den 16. Oktober 2019



Prof. Dr. iur. Jürgen Kühling, LL.M.