Februar 2017

Überprüfung der e-Datenschutz-Richtlinie

Richtlinie 2002/58 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

Mit der Reihe „Bewertungen der Umsetzung", zu der auch dieses Briefing zählt, wird untersucht, wie geltende EU-Rechtsvorschriften in der Praxis funktionieren. In jedem Briefing wird schwerpunktmäßig eine bestimmte europäische Rechtsvorschrift behandelt, die nach den Vorgaben des jährlichen Arbeitsprogramms der Kommission voraussichtlich geändert oder überarbeitet werden soll. In den Bewertungen der Umsetzung sollen die öffentlich zugänglichen Dokumente zur bisherigen Umsetzung, Anwendung und Wirksamkeit von EU-Rechtsvorschriften kurz zusammengefasst werden; dabei wird auf verfügbare Informationen von den Gemeinschaftsorganen und externen Organisationen zurückgegriffen. Ferner sollen sie den parlamentarischen Ausschüssen dabei helfen, die neuen Vorschläge der Kommission nach ihrer Einreichung zu prüfen.

Federführender Ausschuss des EP zum Zeitpunkt der Annahme der EU-Rechtsvorschrift: Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE).[1]
Datum der Verabschiedung des ursprünglichen Rechtsakts im Plenum: 30. Mai 2002.
Datum des Inkrafttretens des ursprünglichen Rechtsakts: 31. Juli 2002 (Artikel 20).
Datum der Umsetzung: bis zum 31. Oktober 2003 (Artikel 17). Die im Jahr 2009 angenommenen Änderungen[2] mussten bis zum 25. Mai 2011 (Artikel 17 der Richtlinie 2009/136) in nationales Recht umgesetzt werden.
Vorgesehenes Datum für die Überprüfung des Rechtsakts: Gemäß Artikel 18 der Richtlinie muss die Kommission dem Europäischen Parlament und dem Rat spätestens drei Jahre nach dem Datum der Umsetzung einen Bericht über die Durchführung[3] und etwaige Vorschläge zur Änderung der Richtlinie vorlegen, um deren Wirksamkeit zu verbessern.
Zeitplan für die Änderung der Rechtsvorschriften: Die Änderung der Verordnung 2002/58 ist in Anhang 1 des Arbeitsprogramms der Kommission 2017 (APK 2017) vorgesehen. Der Vorschlag wurde am 10. Januar 2017 veröffentlicht.

[1] Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres zum Zeitpunkt der Annahme.

[2] Der ursprüngliche Text wurde 2009 durch die Richtlinie 2009/136 (Richtlinie zu den Rechten der Bürger) abgeändert. Die Verordnung 611/2013 der Kommission über die Maßnahmen für die Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten ist eine der weiteren Maßnahmen im Zusammenhang mit der e-Datenschutz-Richtlinie. Eine detaillierte Analyse der Änderungen und deren Auswirkungen finden Sie bei Poullet, Y (2010), Commentary on Directive 2002/58/EC, article3, 4 and 5 - *Concise European IT law*, S. 183-199. Papakonstantinou, V, De Hert, P (2011), The Amended EU Law on ePrivacy and Electronic Communications after its 2011 Implementation; New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights, J. *Marshall Journal of Computer & Information Law* 29 (1).

[3] Die einschlägigen Berichte finden Sie hier.

EPRS | Wissenschaftlicher Dienst des Europäischen Parlaments
Verfasserin: Lorna Schrefler
Referat Politikzyklus
PE 587.347

1. Hintergrund

Seit dem Erlass der Richtlinie 2002/58 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (e-Datenschutz-Richtlinie) haben tief greifende technologische, wirtschaftliche und soziale Veränderungen die Art und Weise, wie elektronische Kommunikation und die dafür verwendeten Geräte wie Mobiltelefone oder Laptops genutzt werden, spürbar beeinflusst. Dieser Wandel hat unter anderem einen direkten Einfluss darauf, inwieweit auf unsere persönlichen Daten zugegriffen werden kann, wie diese verarbeitet und letztlich auch geschützt werden.[4] Dies wiederum hat sich auch darauf ausgewirkt, in wie weit eines der Hauptanliegen der e-Datenschutz-Richtlinie umgesetzt werden kann, nämlich dass die Achtung des Privat- und Familienlebens und der Schutz personenbezogener Daten (Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union) in der elektronischen Kommunikation gleichermaßen gesichert werden.[5] Die Richtlinie ist Teil des Rechtsrahmen für elektronische Kommunikation. Somit findet hier die Definition von „elektronischer Kommunikation" gemäß Artikel 2 der Richtlinie 2002/21 (die Rahmenrichtlinie) Anwendung.[6] Dies hat, worauf später noch einmal genauer eingegangen wird, direkte Auswirkungen auf den derzeitigen Anwendungsbereich der e-Datenschutz-Bestimmungen und darauf, inwieweit diese in einem schnelllebigen technologischen Umfeld Rechtsklarheit schaffen können. Trotz der im Jahr 2009 verabschiedeten Änderungen der Richtlinie 2002/58 lässt die in jüngster Zeit gestiegene Zahl an Over-the-Top-Anbietern (OTTs), die Verbrauchern zahlreiche Online-Dienste, wie das Versenden von Sofortnachrichten (Instant Messaging) anbieten, weiterhin Raum für Unsicherheiten, da OTTs derzeit nicht unter den Anwendungsbereich der bestehenden e-Datenschutz-Bestimmungen fallen.[7]

Vor diesem Hintergrund sah eine der Prioritäten der Strategie für einen digitalen Binnenmarkt vom Mai 2015 auch eine Überarbeitung/ Verbesserung der geltenden e-Datenschutz-Bestimmungen vor. Eine solche Überarbeitung sollte dazu dienen, den EU-Datenschutz-Rechtsrahmen zu ergänzen und weiter zu konkretisieren. Die Überarbeitung der Richtlinie 2002/58 sollte ebenfalls dafür sorgen, dass künftige e-Datenschutz-Bestimmungen in Einklang mit der ab Mai 2018 geltenden Datenschutz-Grundverordnung stehen.[8] Ein dahingehender Vorschlag wurde am 10. Januar 2017 von der Europäischen Kommission vorgelegt. Ziel des Vorschlags ist es, die ursprüngliche Richtlinie aufzuheben und diese mit einer Verordnung zu ersetzen. Durch zielgerichtete Änderungen des aktuellen Textes sollen drei grundlegende Ziele erreicht werden:[9] 1) Tatsächliche Vertraulichkeit der gesamten elektronischen Kommunikation mithilfe einer technologisch neutraleren und zukunftssicheren Gesetzgebung; 2) Tatsächlicher Schutz vor unerbetener

---

[4] Zur Definition von personenbezogenen Daten, dem Thema „Vertrauen" in einer digitalen Umgebung und den größten Herausforderungen des Datenschutzes, siehe: Monteleone, S., Golden Eye: Who rules tomorrow's Europe?, Auf einen Blick, Wissenschaftlicher Dienst des Europäischen Parlaments, April 2016. Für einen umfassenden Überblick darüber, welche Auswirkungen technologische Entwicklungen auf den Datenschutz in vielen Bereichen unseres Lebens haben, siehe: Akrivopoulou, C., Psygkas, A. (Hg.), Personal data privacy and protection in a surveillance era: technologies and practices, IGI global, 2011; und Payton, T., Claypoole, T., Privacy in the age of big data recognizing threats, defending your rights, and protecting your family, Rowman & Littlefield, 2014.

[5] Artikel 1 der e-Datenschutz-Richtlinie nimmt im Zusammenhang mit der Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation Bezug auf das Recht auf Privatsphäre. An dieser Stelle muss betont werden, dass sowohl natürliche als auch juristische Personen, die elektronische Kommunikationsdienste nutzen, unter den Schutz der Richtlinie fallen. Ein weiteres in Artikel 1 erwähntes, zentrales Ziel der Richtlinie ist es, den freien Verkehr der im Bereich der elektronischen Kommunikation verarbeiteten Daten und von elektronischen Kommunikationsgeräten und -diensten im EU-Binnenmarkt zu gewährleisten.

[6] Weitere Details zum Rechtsrahmen und der aktuellen Debatte, inwieweit das Konzept der elektronischen Kommunikation überarbeitet werden kann, finden Sie bei: Schrefler, L, Reforming the regulatory framework for electronic communications networks and services, Bewertung der Umsetzung, Wissenschaftlicher Dienst des Europäischen Parlaments, August 2016. Eine ausführliche Analyse finden Sie in der Stellungnahme 03/2016 zur Bewertung und Überarbeitung der Richtlinie (2002/58/EG) der Artikel 29 Datenschutzgruppe vom Juli 2016; sowie in der Vorläufigen Stellungnahme des EDSB zur Überarbeitung der Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) des Europäischen Datenschutzbeauftragten vom Juli 20016, Stellungnahme 5/2016. Bei der Artikel 29 Datenschutzgruppe handelt es sich um eine Kooperationsplattform, die sich aus Vertretern der nationalen Datenschutzbehörden, der Kommission und dem EDSB zusammensetzt.

[7] Siehe hierzu die Mitteilung der Kommission Online-Plattformen im digitalen Binnenmarkt - Chancen und Herausforderungen für Europa vom 25. Mai 2016, COM (2016) 288, S. 6-7.

[8] Weitere Details finden Sie hier: Review of the ePrivacy Directive - Legislative Train Schedule, Train N. 2, Europäisches Parlament.

[9] Weitere Details finden Sie unter Abschnitt 6.2 der Folgenabschätzung SWD (2017)3 zum Vorschlag.

kommerzieller Kommunikation, unter anderem durch ein Verbot anonymisierter Anrufe zu Werbezwecken; und 3) Größere Harmonisierung und Vereinfachung des bestehenden Rechtsrahmens durch einheitliche Regeln für die gesamte EU und die Abschaffung redundanter und überholter Bestimmungen.[10]

2. Berichte, Evaluierungen und Studien auf EU-Ebene

E-Datenschutz-Richtlinie: Bewertung der Umsetzung, der Wirksamkeit und der Vereinbarkeit mit der vorgeschlagenen Datenschutzverordnung - Bericht für die Europäische Kommission

Schwerpunkt der im Jahr 2015 für die Europäische Kommission abgeschlossenen externen Studie[11] sind 5 zentrale Themen der e-Datenschutz-Richtlinie: Der örtliche und sachliche Anwendungsbereich der Richtlinie (Artikel 1 bis 3); die Vertraulichkeit der Kommunikation (Artikel 5(1)); Cookies und andere Techniken gemäß Artikel 5(3); Verkehrs- und Standortdaten (Artikel 6 und 9) sowie unerbetene Nachrichten zu Werbezwecken (Artikel 13). Mit dem Bericht wurden drei Zielsetzungen verfolgt: Der Stand der Umsetzung und Durchführung der genannten fünf Elemente sollte bewertet werden;[12] es sollte beurteilt werden, ob die Ziele der Richtlinie 2002/58 erreicht worden sind und es sollte analysiert werden, inwieweit die e-Datenschutz-Richtlinie mit künftigen Datenschutzgesetzen in Wechselwirkung steht.[13]

Mit Blick auf den **örtlichen und sachlichen Anwendungsbereich** der e-Datenschutz-Richtlinie kommt der Bericht zu dem Schluss, dass für Dienstleistungen, die (zumindest aus der Sicht der Verbraucher) ähnlich geartet sind, weiterhin drei verschiedene Regelwerke gelten: der Rechtsrahmen für elektronische Kommunikation (zu welchem die e-Datenschutz-Richtlinie gehört), die Rechtsvorschriften bezüglich der Dienste der Informationsgesellschaft sowie die Bestimmungen zu audiovisuellen Mediendiensten. Daher wurde die Richtlinie 2002/58 unter verschiedenen Rechtsrahmen auf nationaler Ebene umgesetzt. In einigen Ländern ist sie Teil der Gesetzgebung zu elektronischer Kommunikation, in anderen fällt sie jedoch unter das allgemeine Datenschutzgesetz oder Verbraucherschutzvorschriften. Das kann letztlich bedeuten, dass der Anwendungsbereich einzelner Bestimmungen der Richtlinie, insbesondere Artikel 3 zu den von der Gesetzgebung betroffenen Diensten, sich je nach Mitgliedstaat unterscheidet. Im Bericht wurde auch darauf hingewiesen, dass der Anwendungsbereich der Richtlinie selbst nicht eindeutig ist, da sie einige Dienste der Informationsgesellschaft nicht enthält, die unbestritten in den Anwendungsbereich fallen sollten. Diese Unklarheit hat dazu geführt, dass Dienstleistungen, die in funktioneller Hinsicht große Ähnlichkeiten aufweisen, dennoch unterschiedlich

Wie funktionieren Cookies?

Die e-Datenschutz-Richtlinie wird oft auch als „Cookie-Richtlinie" bezeichnet, da sie Bestimmungen zur Speicherung von Informationen und zum Zugriff auf Informationen, die sich auf dem Endgerät eines Nutzers befinden, festlegt (Artikel 5(3)). Der Artikel deckt verschiedene Techniken und insbesondere „Cookies" ab, d. h. kleine Datenmengen, zu deren Speicherung der Browser aufgefordert werden kann, wenn ein Nutzer eine Website besucht. Mithilfe von Cookies kann eine Internetseite das Endgerät des Nutzer wiederzuerkennen, wenn die Seite wiederholt aufgerufen wird. Außerdem werden die Vorlieben des Nutzers mit der Zeit verdeutlicht und diese Informationen genutzt, um Werbung gezielter einsetzen oder das Online-Erlebnis auf den Kunden anpassen zu können. Es gibt verschiedene Arten von Cookies. Gemessen an ihrer Lebensdauer kann es sich bei Cookies entweder um **Sitzungscookies**, also solche, die nach dem Schließen des Browsers gelöscht werden, oder um **Dauercookies** handeln, die für eine bestimmte Zeit auf dem Endgerät des Nutzers gespeichert bleiben. Des Weiteren ist bei Cookies zwischen den verschiedenen Hosting-Diensten zu unterscheiden. So genannte **Cookies von Erstanbietern** werden von der besuchten Website selbst platziert und dienen im Wesentlichen dazu, die Effizienz und das Kundenerlebnis zu verbessern. **Drittanbieter-Cookies** werden hingegen von einer anderen als der besuchten Domäne

[10] Siehe Europäische Kommission SWD (2017).4, S. 2.

[11] SMART 2013/0071, Januar 2015.

[12] Daten und Informationen zur Umsetzung und Durchführung in den einzelnen Mitgliedstaaten finden Sie in Anhang 1 des Berichts sowie in einer Konkordanztabelle mit Verweis auf die Berichte der einzelnen Länder.

[13] Hier ist anzumerken, dass sich die Datenschutz-Grundverordnung noch in der Vorschlagsphase des ordentlichen Gesetzgebungsverfahrens befand, als der SMART 2013/0071-Bericht ausgearbeitet wurde. Dieser Teil des Berichts ist deshalb nicht Teil des vorliegenden Briefings.

behandelt werden. Einige Mitgliedstaaten (wie Deutschland und Finnland) haben bei der Umsetzung des Textes den Anwendungsbereich der Richtlinie bereits auf zusätzliche Dienste ausgeweitet.

Die in Artikel 5(1) festgelegten Bedingungen für die **Vertraulichkeit der Kommunikation** haben ihr Ziel, nationale Bestimmungen EU-weit zu harmonisieren, verfehlt. In vielen Mitgliedstaaten wurde dieser Aspekt bereits vor Annahme der e-Datenschutz-Richtlinie reguliert. Trotz der Umsetzung der Richtlinie in nationales Recht haben verschiedene Rechtstraditionen in der EU dazu geführt, dass verschiedene Definitionen, Bedingungen und Modalitäten zur Wahrung der Vertraulichkeit weiterhin bestehen und unterschiedliche Ausnahmen gelten – zum Beispiel mit Blick auf die Überwachung von Kommunikationsdaten zu Strafverfolgungszwecken oder zu beruflichen Zwecken. Auch bei der Durchsetzung der Rechte, die die Richtlinie bietet, wurde auf mögliche Problemfelder hingewiesen. Ein Grund für diese könnte sein, dass in den einzelnen Mitgliedstaaten unterschiedliche Behörden für die Umsetzung der e-Datenschutz-Richtlinie zuständig sind.[14] Dies kann in manchen Fällen zu Inkohärenzen und Unsicherheiten bei der Anwendung der geltenden Bestimmungen innerhalb eines Mitgliedstaates führen.

Dem Bericht zufolge wurde das Ziel von Artikel 5(3) zu **Cookies**, Spyware und anderen Techniken und zur Vorgabe, dass für diese zunächst die **Zustimmung des Nutzers** eingeholt werden muss, nicht in vollem Umfang erreicht. Die 2009 im Rahmen der Überarbeitung der Richtlinie eingeführten Änderungen zur Nutzung von Cookies scheinen zu Unsicherheit in Bezug auf die Anwendung vor Ort geführt zu haben. Die Überarbeitung erforderte des Weiteren eine Auslegung und Beratung seitens der Artikel 29 Datenschutzgruppe,[15] zum Beispiel in Bezug auf Browser-Einstellungen und die Art und Weise der Zustimmung zur Nutzung von Cookies. Zudem hat der übermäßige Einsatz von Cookies auf vielen Websites nicht nur zu Verunsicherung seitens der Verbraucher geführt, sondern auch das Ziel der Warnmeldungen, nämlich Informationen zum Einsatz von Cookies zu liefern, verwässert. Nutzer, die mit Cookies regelrecht „bombardiert" werden, werden nicht zwangsläufig verstehen (oder sich nicht die Zeit dafür nehmen, um zu verstehen), worin der Unterschied zwischen den verschiedenen Cookie-Typen besteht, z. B. was Drittanbieter-Cookies von solchen unterscheidet, die in Zusammenhang mit dem Zweck stehen, zu welchem der Nutzer die Website in erster Linie konsultiert (analytische Erstanbieter-Cookies).

Laut Bericht ist Artikel 6 der Richtlinie (**Verkehrsdaten**)[16] korrekt in nationales Recht umgesetzt worden. Bei der Durchsetzung bestehen jedoch weiterhin Bedenken. Probleme wurden auch bei der Nutzung von **Standortdaten** (Artikel 9) beobachtet.[17] Dies ist insbesondere der Fall, da einige standortbasierte Dienste, die Risiken für die Privatsphäre mit sich bringen, nicht unter die Richtlinie fallen, wenn sie in einem *privaten* Netzwerk genutzt werden. Die Richtlinie umfasst nämlich solche Dienste, die in *öffentlichen* Netzwerken genutzt werden, da diese in den Rahmen für elektronische Kommunikation und der darin enthaltenen Definition von elektronischen Kommunikationsdiensten fallen.[18] Mit Blick auf **unerbetene Nachrichten zu Werbezwecken** kommt der Bericht zu dem Schluss, dass die Mitgliedstaaten Artikel 13 der Richtlinie erfolgreich umgesetzt haben und automatische Anrufe und Kommunikationssysteme, die zu Zwecken des Direktmarketings und ohne vorherige Zustimmung durchgeführt werden, verboten wurden. Andere Formen des Direktmarketings können auf nationaler Ebene weiterhin auf unterschiedliche Weise behandelt werden. So haben einige Mitgliedstaaten eine Opt-out-Variante gewählt, während sich andere in ihrer Gesetzgebung für einen Opt-in-Ansatz entschieden haben.

[14] Gemäß Artikel 15a obliegt es den Mitgliedstaaten, zu entscheiden, welche nationalen Behörden für die Durchsetzung der Richtlinie 2002/58 zuständig sind.

[15] Siehe Fußnote 6.

[16] Dies gilt insbesondere für „Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden". Siehe Glossar, Anhang 14, SWD (2017)3.

[17] Bezieht sich auf „Daten, die in einem elektronischen Kommunikationsnetz oder von einem elektronischen Kommunikationsdienst verarbeitet werden und die den geografischen Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen elektronischen Kommunikationsdienstes angeben", SWD (2017)3, Anhang 14.

[18] Dies kann zu nicht eindeutigen Situationen führen. Der Bericht nennt das Beispiel von öffentlichen W-LAN-Verbindungen an Flughäfen. Sind diese als öffentlich oder privat einzustufen?

Aus den Ergebnissen des Berichts ergaben sich eine Reihe von Empfehlungen zu den fünf Schwerpunktthemen, zusammengefasst in Tabelle 1.

Tabelle 1: Empfehlungen zu ausgewählten Themen

Gegenstand	Empfehlung
Anwendungsbereich	Artikel 3 sollte abgeändert und in Bezug auf die Verarbeitung personenbezogener Daten „in Zusammenhang mit den Bestimmungen zu öffentlich zugänglichen Diensten *in öffentlichen oder öffentlich zugänglichen privaten Kommunikationsnetzen* in der Union" Anwendung finden.
Vertraulichkeit	Artikel 5(1) sollte abgeändert und in Bezug auf die Vertraulichkeit von Kommunikation und die damit zusammenhängende Nutzung von Verkehrsdaten über *öffentliche oder öffentlich zugängliche private Kommunikationsnetze* Anwendung finden. Der Anwendungsbereich von Artikel 5(2) sollte mit Blick auf „Ausnahmen in der Geschäftspraxis" eindeutiger gestaltet sein, damit eine einheitliche Umsetzung und Durchsetzung in der gesamten EU sichergestellt werden können.
Cookies und Ähnliches	Die bestehenden Ausnahmen gemäß Artikel 5(3) sollten deutlicher formuliert sein. Weitere Ausnahmen sollten in den Artikel aufgenommen werden. Es sollten Bedingungen für die „spezifische, aktive und vorherige Einwilligung in allen Fällen, in denen Cookies oder ähnliche Techniken zu Direktmarketing-Zwecken zum Einsatz kommen" aufgestellt werden.
Verkehrs- und Standortdaten	Die Artikel 6(1) und 9(1) sollten geringfügig abgeändert werden, damit deren Anwendbarkeit auf alle Dienste in öffentlichen und öffentlich zugänglichen privaten Kommunikationsnetzen, in Einklang mit den für Artikel 3 genannten Änderungen, sichergestellt werden kann.
Unerbetene Nachrichten zum Zweck der Direktwerbung	Artikel 13 sollte an die für Artikel 3 vorgeschlagene Änderung angepasst werden, damit die in Artikel 13 vorgesehene Opt-out-Regelung auch in Bezug auf E-Mail-Nachrichten, die über Dienste der Informationsgesellschaft versandt werden, Anwendung findet. Die Mitgliedstaaten sollten weiterhin selbst entscheiden dürfen, ob sie ein Opt-in- oder Opt-out-Modell für Nachrichten zum Zwecke des Direktmarketings anwenden wollen.
Verbindung zur Datenschutz-Grundverordnung	Die e-Datenschutz-Richtlinie sollte in eine Verordnung umgewandelt werden.

Quelle: Ausführungen der Verfasserin auf Grundlage der Studie SMART 2013/0071, S. 7-18.

REFIT-Bewertung der Richtlinie

In der Folgenabschätzung der Anfangsphase der Europäischen Kommission zur Überarbeitung der Richtlinie wurde bereits darauf hingewiesen, dass die Bewertung weiterer Elemente, die im oben genannten Bericht nicht berücksichtigt wurden, Teil einer gesonderten REFIT-Bewertung sind.[19] Letztere wurde zeitgleich zur Folgenabschätzung durchgeführt. Beide Dokumente wurden zeitgleich mit dem Vorschlag am 10. Januar 2017 veröffentlicht.

Die Daten der REFIT-Bewertung betreffen die EU28 sowie den Zeitraum 2009-2016.[20] In Einklang mit den Leitlinien für bessere Rechtsetzung der Kommission orientiert sich der Bericht an den fünf **Bewertungskriterien** Effizienz, Wirksamkeit, Bedeutung, Kohärenz und EU-Zusatznutzen, welche auf die fünf wichtigsten Bereiche der Richtlinie angewandt werden: 1) die Sicherheit von elektronischer Kommunikation; 2) die Vertraulichkeit von Kommunikation und damit verbundenen Verkehrsdaten; 3) die Vertraulichkeit von Informationen, die auf Endgeräten gespeichert werden; 4) Verbraucherschutz bei unerbetenen Nachrichten, und 5) weitere Bestimmungen zum Schutz der Privatsphäre von Nutzern und den berechtigten Interessen von Teilnehmern.[21]

Zudem wurde in der Bewertung auch auf **zwei horizontale Fragestellungen** eingegangen (nämlich auf den Anwendungsbereich der Richtlinie und die Entscheidungsfreiheit der zuständigen Behörden), da diese direkte Auswirkungen darauf haben, wie wirksam beim Erreichen der durch den Gesetzgeber gesetzten Ziele sind. In diesem Zusammenhang kam die REFIT-Bewertung zu dem Schluss, dass mit der Definition von

[19] Europäische Kommission, SWD(2017)5. Hierbei ist zu beachten, dass in der REFIT-Bewertung unter anderem auch auf zwei weitere externe Studien zurückgegriffen wurde: Deloitte (2016), Bewertung und Überprüfung der Richtlinie 2002/58 über den Schutz der Privatsphäre in der elektronischen Kommunikation (SMART 2016/0080) und ECORYS, TNO und Andere (2016), Study on future trends and business models in communication services, (SMART 2013/0019). Die in Deloitte (2016) angestellten quantitativen Abschätzungen finden Sie in der Folgenabschätzung SWD (2017)3, Anhang 8 zum neuen Vorschlag.

[20] Wie bereits erwähnt, wurde die Richtlinie zuletzt im Jahr 2009 überarbeitet. Wenn weitere ältere Daten einschlägig und zugänglich waren, wurden auch diese mit einbezogen.

[21] SWD (2017) 5, Abschnitt 3 und S. 22.

elektronischen Kommunikationsdiensten, welche die Grundlage der Richtlinie darstellt, **deren Anwendungsbereich zu begrenzt und/ oder überholt** sei. Hinzukommt, dass der derzeitige Anwendungsbereich als nicht eindeutig eingestuft wurde, was zu **Rechtsunsicherheiten** führen kann. Dadurch wurde die Wirksamkeit der Rechtsvorschriften letztlich beeinträchtigt. Weitere Probleme sind auch darauf zurückzuführen, dass es mit der Richtlinie nicht möglich ist, zu bestimmen, welches nationale Gesetz, insbesondere in grenzüberschreitenden Situationen, Anwendung findet und welche Behörden der verschiedenen Mitgliedstaaten, aber auch innerhalb eines einzigen Mitgliedstaates, für die Durchführung zuständig sind.

Aus den verschiedenen Themen, die mit den Fragen der Bewertung abgedeckt wurden, ging hervor, dass die Anforderungen an die **Betriebssicherheit der elektronischen Kommunikation** (Artikel 4) als weiterhin relevant und als „grundlegende Voraussetzung" gesehen werden, um die Ziele der Richtlinie zu erreichen, gerade mit Blick auf die steigende Zahl der sicherheitsrelevanten Vorfälle, die Einfluss auf die Privatsphäre der Nutzer haben. Da sich ähnliche Bestimmungen auch in anderen Rechtsakten wie der Datenschutz-Grundverordnung finden, kam die Bewertung zu dem Schluss, dass **einige Teile der e-Datenschutz-Richtlinie redundant geworden** seien. Trotz der Verbesserungen, die durch die Überarbeitung der Richtlinie im Jahr 2009 erreicht worden sind, scheint Artikel 4 weiterhin nur teilweise wirksam zu sein. Der derzeitige Wortlaut des Artikels lässt weiterhin Raum für Unsicherheiten, zum Beispiel hinsichtlich der verschiedenen Arten von Sicherheitsrisiken, die unter die Verpflichtung, Teilnehmer zu informieren, fallen, sowie mit Blick auf mögliche abmildernde Maßnahmen, die in solchen Fällen Anwendung finden können. Dies hat dazu geführt, dass die Anforderungen in den verschiedenen Mitgliedstaaten **in unterschiedlichen Graden und Formen umgesetzt** wurden. Dies ist nicht auf eine gescheiterte oder unvollständige Umsetzung, sondern vielmehr auf die Unklarheit des Textes zurückzuführen.

Behörden gaben auch an, dass es zu **Schwierigkeiten kam, die Pflicht zur Meldung von Verstößen durchzusetzen**. Diese Aussage wird durch die relativ geringe Zahl an angezeigten Verstößen in den Mitgliedstaaten, die Teil einer der zugrunde liegenden Studien waren, erhärtet.[22] Hinsichtlich der Kohärenz kam die Bewertung zu dem Schluss, dass die jüngst verabschiedete Datenschutz-Grundverordnung und deren Bestimmungen zu Meldungen von Verletzungen des Schutzes personenbezogener Daten (Artikel 33 und 34) dazu führen kann, dass zwei verschiedene Ansätze gefahren werden, wenn die e-Datenschutz-Richtlinie nicht abgeändert wird. Da der durch die Datenschutz-Grundverordnung eingeführte Ansatz wirksamer zu sein scheint, kommt die Bewertung zu dem Schluss, dass nur Artikel 4(2) der e-Datenschutz-Richtlinie weiterhin von Bedeutung sei, da die darin enthaltenen Bestimmungen nicht von anderen Rechtsvorschriften abgedeckt werden. Diese Überschneidung wurde auch bei der Bewertung der Wirksamkeit von Artikel 4, der als einer der kostspieligsten der Richtlinie galt, deutlich. Obwohl bestätigt wurde, dass Bestimmungen zu Verletzungen des Schutzes personenbezogener Daten, besonders in grenzüberschreitenden Situationen, einen EU-Zusatznutzen haben, kam die Bewertung abermals zu dem Schluss, dass die jeweiligen Bestimmungen der Datenschutz-Grundverordnung ausreichend seien.

Mit Blick auf die **Vertraulichkeit der Kommunikation und damit verbundene Verkehrsdaten** (Artikel 5(1), 6 und 9) bestätigte die Bewertung, wie wichtig diese Bestimmungen sind, da diese in keinen der anderen EU-Gesetzen enthalten sind. Dies wurde auch im Fazit der Bewertung zur Kohärenz zwischen diesen Bestimmungen und dem übrigen *Besitzstand* der EU deutlich. Dennoch scheint die Richtlinie **beim Schutz der Vertraulichkeit nicht in vollem Umfang wirksam gewesen zu sein**. Verschiedene Faktoren, wie zum Beispiele Probleme hinsichtlich der Formulierung und Umsetzung von Artikel 5(1), oder auch die Tatsache, dass einige Bestimmungen durch die Entwicklungen in der elektronischen Kommunikation bereits veraltet sind, können ein Grund dafür sein. Zudem gibt es auf nationaler Ebene weiterhin verschiedene Ansätze zum Umgang mit Inhalten und Standortdaten. Die Tatsache, dass OTTs derzeit nicht unter die Richtlinie fallen, hat den Schutz, den diese tatsächlich bietet, beeinträchtigt und zu „ungleichen Rahmenbedingungen" für Marktteilnehmer geführt. Von der Möglichkeit, dass Mitgliedstaaten aus Gründen der nationalen Sicherheit von der Richtlinie

[22] SWD (2017) 5, S. 27-28 zu Deloitte (2016), S. 68.

abweichen dürfen, wurde in unterschiedlichem Maße Gebrauch gemacht, was zu einer gewissen Fragmentierung geführt hat.

Da zu wenig quantitative Daten zur Verfügung standen, - ein durchgängiges Problem bei der Bewertung - konnten keine endgültigen Schlüsse zur Wirksamkeit dieser Artikel gezogen werden. Die Meinungen zur Wirksamkeit gingen bei Verbraucherschutz- und Branchenvertretern auseinander, worauf in Abschnitt 4 dieses Briefings noch näher eingegangen wird. Die Bewertung hat bestätigt, dass die Bestimmungen zur Vertraulichkeit der Kommunikation und der damit verbundenen Verkehrsdaten einen **EU-Zusatznutzen darstellen**, und zwar nicht nur, weil Kommunikation immer mehr auch grenzüberschreitend stattfindet, sondern auch aufgrund der **Vorteile für die Harmonisierung der Konzepte und Definitionen** (z. B. von Verkehrs- und Standortdaten), die durch die Richtlinie entstanden sind.

Die Wichtigkeit der Anforderungen an die **Vertraulichkeit von Informationen, die bereits im Endgerät gespeichert sind** (Artikel 5(3)), wurde durch die Bewertung bestätigt, obwohl ebenso festgestellt wurde, dass der Artikel zu viele Aspekte, wie Praktiken, die nicht in die Privatsphäre eingreifen, mit einbezieht. Der EU-Zusatznutzen blieb unbestritten und auch die Kohärenz mit der Datenschutz-Grundverordnung wurde hervorgehoben. Die Wirksamkeit der Bestimmungen scheint jedoch durch die verschiedenen in diesem Briefing bereits genannten Gründe geschmälert worden zu sein. Dazu zählt zum Beispiel der übermäßige Einsatz von Cookies, der dazu führt, dass Nutzer diese satt haben und ihre Einwilligung automatisch geben, oder auch das Phänomen der sogenannten „Cookie-Walls“, einem Alles-oder-nichts-Ansatz, der Nutzern den Zutritt zur Website verwehrt, wenn diese die Nutzung von Cookies abgelehnt haben. Hinzukommt, dass die Wirksamkeit, wie auch bei anderen Bestimmungen, durch die unterschiedliche Art und Weise der Um- und Durchsetzung in den verschiedenen Mitgliedstaaten beeinträchtigt wurde. Den quantitativen Schätzungen zufolge können für die Erfüllung der in Artikel 5(3) genannten Anforderungen Kosten in Höhe von 300 € pro Website pro Jahr entstehen und sich die Befolgungskosten in der gesamten EU demnach auf rund 1,8 Milliarden € im Jahr 2015 belaufen.[23] Die Bewertung hat gezeigt, dass auch wirksamere Wege zur Einhaltung der Richtlinie gefunden werden können.

Mit Blick auf den **Schutz gegen unerbetene Nachrichten** (Artikel 13) wird in der Bewertung erläutert, dass die Kosten für solche Praktiken in den letzten Jahren immer weiter zurückgegangen sind, was die Ausmaße des Problems verschärfen könnte und wodurch nochmals bestätigt wurde, wie wichtig diese Bestimmung ist. Hinsichtlich der **verschiedenen Schutzmöglichkeiten, die die Richtlinie liefert, gingen die Meinungen der Interessenvertreter jedoch auseinander**. Zum einen lassen die gesammelten Informationen vermuten, dass Artikel 13 teilweise wirksam ist, da die Bürger den zuständigen Behörden der jeweiligen Mitgliedstaaten eine große Zahl an belästigenden Anrufen gemeldet haben. Zum anderen berichteten die für die Bewertung und die zugrunde liegenden Studien befragten Branchenvertreter von Schwierigkeiten, sowohl beim Verständnis als auch bei der Umsetzung der jeweiligen Bestimmungen. Auch hier kam es also aufgrund der unterschiedlichen Umsetzungspraktiken in den Mitgliedstaaten zu Fragmentierung und Rechtsunsicherheit innerhalb der EU. Auch die Bewertung der Wirksamkeit in quantitativer Hinsicht erwies sich als schwierig. An dieser Stelle muss jedoch angemerkt werden, dass die durch Artikel 13 entstehenden Kosten aus Sicht der Unternehmen vor allem Opportunitätskosten darstellen, die durch den Marketing- und Umsatzverlust entstehen. Der EU-Zusatznutzen der Bestimmungen wurde bestätigt. Abschließend ließ sich aus der Bewertung der Schluss ziehen, dass sich Artikel 13, die Datenschutz-Grundverordnung, die Richtlinie 2000/31 über den elektronischen Geschäftsverkehr und die Verbraucherrechte-Richtlinie 2011/83 ergänzen, was auf eine Kohärenz zwischen den verschiedenen Gesetzgebungsakten in diesem Punkt hindeutet.

Auch **weitere Bestimmungen** wie das Recht, Rechnungen ohne Einzelgebührennachweis zu erhalten (Artikel 7) und das Recht zu entscheiden, ob ein Eintrag ins Teilnehmerverzeichnis erfolgen soll (Artikel 12) wurden von den Bürgern und der Zivilgesellschaft als wichtig eingestuft. Die Industrie hingegen forderte die Streichung oder Anpassung dieser Artikel an den technologischen Wandel. Die Bewertung ergab, dass die Bestimmungen insgesamt **ihr jeweiliges Ziel wirksam erreichen und einen EU-Zusatznutzen mit sich**

[23] SWD (2017)5, S. 47.

brachten. Da nicht ausreichend quantitative Daten zur Verfügung standen, erwies es sich als schwierig zu bewerten, wie wirksam solche Anforderungen sind. Der Bewertung zufolge sind die betreffenden Bestimmungen und andere relevante Bereiche des *Besitzstands* der EU im Allgemeinen kohärent.

3. Standpunkt des Europäischen Parlaments/Anfragen von MdEP

3.1. Entschließungen des Europäischen Parlaments

Entschließung des Europäischen Parlaments vom 19. Januar 2016 zu dem Thema „Auf dem Weg zu einer Akte zum digitalen Binnenmarkt“

In seiner Entschließung hat das Europäische Parlament hervorgehoben, dass Grundrechte, insbesondere die Datenschutzvorschriften, geachtet werden müssen und gefordert, die Richtlinie 2002/58 zu überarbeiten, um diese „an die einschlägigen Bestimmungen des Datenschutzpakets anzupassen, noch bevor es in Kraft tritt“ (Mai 2018). Das Parlament stellte auch fest, dass elektronische Massenüberwachung das Vertrauen der Bürger in digitale Dienste und den wirksamen Schutz ihrer Privatsphäre erschüttert hat und hat erneut betont, dass „bei der Verarbeitung personenbezogener Daten für kommerzielle Zwecke oder Strafverfolgungszwecke die geltenden Datenschutzvorschriften strikt eingehalten werden müssen“. Das Parlament betonte, dass das Vertrauen der Bürger und Unternehmen in digitale Dienste eine notwendige Grundlage für Innovation und Wachstum sowie für die Schaffung eines wettbewerbsfähigen Binnenmarkts darstellt.

In ihren Folgemaßnahmen zur Entschließung bestätigte die Europäische Kommission, dass sie mit dem Überprüfungsverfahren der e-Datenschutz-Richtlinie bereits begonnen habe. Zudem hat sie mitgeteilt, dass sie beabsichtige, bis zum Ende 2016 einen Vorschlag vorzulegen. Die Kommission gab ferner an, auch die Bedeutung von Datenverschlüsselung inhaltlich mit in Betracht zu ziehen, um die Privatsphäre der Verbraucher und deren personenbezogene Daten in der elektronischen Kommunikation zu schützen, wie es das Parlament in seiner Entschließung betont hatte.

3.2. Schriftliche Anfragen von Mitgliedern des Europäischen Parlaments

Schriftliche Anfrage von Morten Messerschmidt (ECR, Dänemark), 15. April 2016

Der Abgeordnete nimmt Bezug auf Artikel 5(3) der e-Datenschutz-Richtlinie, welcher vorsieht, dass nach Inkenntnissetzung zunächst eine Einwilligung erfolgen muss, bevor Informationen auf dem Endgerät eines Nutzers gespeichert oder auf diese zugegriffen werden darf. Der Abgeordnete weist darauf hin, dass es an der Zeit sei, zu bewerten, ob die Bestimmung ihr angestrebtes Ziel erreichen konnte und ob sie im Verhältnis zur Belastung für die Nutzer stehe. Auf der einen Seite irritiere es Nutzer, ständig Cookies akzeptieren zu müssen. Auf der anderen Seite werde die Einwilligung zur Nutzung von Cookies oftmals gegeben, ohne dass sich die Nutzer der Konsequenzen dessen in vollem Umfang bewusst seien, wodurch die Sicherheit nicht verbessert werden könne. Der Abgeordnete möchte deshalb wissen, ob die Europäische Kommission gewillt wäre, diese besondere Bestimmung, die mehr Belastungen als Vorteile mit sich zu bringen scheint, zu streichen.

Antwort von Günther Oettinger im Namen der Kommission, 14. Juni 2016

Der Kommissar erinnert daran, dass die Einwilligung bei einer technischen Speicherung oder dem Zugang, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn es sich, soweit dies unbedingt erforderlich ist, um einen vom Teilnehmer oder Nutzer ausdrücklich gewünschten Dienst der Informationsgesellschaft handelt, nicht notwendig ist. Der Kommissar fügt hinzu, dass es oft möglich sei, eine Einwilligung für eine bestimmte Website einmalig zu erteilen oder Browser-Einstellungen zu diesem Zwecke vorzunehmen. Er betont jedoch auch, dass die Artikel29Datenschutzgruppe zu dem Schluss gekommen war, dass viele Websites noch immer unnötige Cookies verwenden, oftmals, um Nutzer zu erfassen und ein Profil ihres Lebens bzw. ihrer Gewohnheiten zu erstellen. Er verweist darauf, dass diese Fragen in der öffentlichen Konsultation und in der Bewertung für eine Überarbeitung der Richtlinie 2002/58 angesprochen worden seien.

Schriftliche Anfrage von Santiago Fisas Ayxelà (EPP, Spanien), 27. April 2016
Nutzer, die auf ihrem Computer Pop-up-Blocker installiert haben, werden von einigen Websites vermehrt daran gehindert, auf den Inhalt dieser Seiten zuzugreifen. Der Abgeordnete betont, dass solche Mechanismen, die den Zugang zu Inhalten verhindern möglicherweise Artikel 5(3) der e-Datenschutz-Richtlinie verletzen, da diese nicht die ausdrückliche Einwilligung des Nutzers benötigen.[24] Er möchte deshalb wissen, wie die Kommission sicherzustellen gedenkt, dass die Privatsphäre der Nutzer angesichts solcher Praktiken gewahrt bleibt, und fragt, inwieweit es möglich wäre, ein Gleichgewicht zwischen dem Schutz der Nutzer auf der einen und der Tragfähigkeit der Websites mit Blick auf Werbemaßnahmen auf der anderen Seite herzustellen.

Antwort von Günther Oettinger im Namen der Kommission, 8. Juli 2016
Der Kommissar erklärt, dass es von der Technologie, die die Websites nutzt, um den Einsatz von Pop-up-Blockern festzustellen, abhängig sei, ob Artikel 5(3) der Richtlinie 2002/58 in einer bestimmten Situation greife oder nicht. Er betont auch, dass die nationalen Aufsichtsbehörden und Gerichtshöfe dafür zuständig seien, die Überwachung und Durchsetzung der geltenden Rechtsvorschriften sicherzustellen. Dies beinhalte auch die Beurteilung, ob die Bestimmung der Richtlinie bei den von Websites genutzten Mechanismen zur Erkennung von Pop-up-Blockern Anwendung findet. Er weist ebenfalls darauf hin, dass die jüngst verabschiedete Datenschutz-Grundverordnung das Vertrauen der Nutzer in digitale Dienste stärken soll. Abschließend betont er, dass die e-Datenschutz-Richtlinie mit Blick auf ihre Effizienz und Wirksamkeit bewertet werde und diese Bewertung auch eine Kosten-Nutzen-Analyse beinhalte.

Schriftliche Anfrage von Kathleen Van Brempt (S&D, Belgien), 13. April 2015
In einem Bericht der belgischen Kommission zum Schutz der Privatsphäre wurde festgestellt, dass Facebook die Online-Aktivitäten von
Personen aufgezeichnet hat, die weder die Dienste des sozialen Netzwerks nutzten noch dessen Seite besuchten. Dies geschah laut Bericht ohne deren Wissen oder Einwilligung. Die Abgeordnete will deshalb wissen, ob die Europäische Kommission von dieser Nutzung von Langzeit-Cookies zur Erkennung und Verfolgung der Aktivitäten nicht angemeldeter Nutzer wusste und ob mit dieser Praxis gegen die e-Datenschutz-Richtlinie verstoßen wurde. Sie fragte auch, welche Aktionen die Kommission plane, um die rechtswidrige Verfolgung von Nutzeraktivitäten zu unterbinden und Internetnutzer über das Tracking durch Drittanbieter zu informieren.

Antwort von Günther Oettinger im Namen der Kommission, 7. Juli 2015
Der Kommissar bestätigt, dass der Kommission Informationen zu der von der Abgeordneten erwähnten Praxis vorlägen und betont, dass der Einsatz von Cookies zu Verfolgung der Nutzeraktivitäten in Einklang mit den nationalen Maßnahmen zur Umsetzung der e-Datenschutz-Richtlinie und insbesondere mit der Überarbeitung des Artikels 5(3) aus dem Jahr 2009 zur Einwilligung der Nutzer in voller Sachkenntnis stehen müsse. Er erinnert auch daran, dass es die Aufgabe der Mitgliedstaaten ist, diese Bestimmungen durchzusetzen. Mit ihren Untersuchungsbefugnissen seien also die zuständigen nationalen Behörden die geeignete Anlaufstelle, bei welcher betroffene Nutzer ihre Bedenken mitteilen können. Abschließend betont er, dass die Kommission die Bemühungen der Branche unterstütze, das Bewusstsein der Nutzer hinsichtlich ihrer Rechte gemäß Richtlinie 2002/58 durch Systeme wie die Do-Not-Track-Software oder den Einsatz von Dialogfeldern mit Informationen über Cookies und zahlreiche andere Mechanismen zur Einwilligung zu schärfen.

4. Öffentliche Konsultationen der Kommission

Eurobarometer-Umfrage zum Datenschutz in der elektronischen Kommunikation
Auf Anfrage der Europäischen Kommission wurden im Sommer 2016 knapp 27 000 Unionsbürger kontaktiert, um eine Studie zum Thema Schutz der Privatsphäre durchzuführen.[25] In der Befragung ging es um die folgenden Themen: Wie nutzen die Bürger Kommunikationstechnologien? Wie wichtig sind ihnen der Schutz

[24] An dieser Stelle sei anzumerken, dass Bedenken zur verpflichtenden Annahme von Cookies, um Zugang zu bestimmen Websites zu erhalten, und zum Zugang zu personenbezogenen Daten (einschließlich zu Verkehrs- und Standortdaten) in den vergangenen zwei Jahren bereits in Form von Anfragen beim Referat Bürgeranfragen des Europäischen Parlaments (AskEP) eingegangen sind.
[25] Flash Eurobarometer 443, Juli 2016.

der Privatsphäre im Internet und die Vertraulichkeit ihrer Kommunikation? Welche Schritte unternehmen Bürger, um ihre Privatsphäre im Internet zu schützen? Kennen sie die geltenden Rechtsvorschriften? Wie gehen sie mit unerbetenen E-Mail-Nachrichten oder Anrufen zu Marketingzwecken um?

Die Studie hat gezeigt, dass mehr als 70 % der befragten Bürgerinnern und Bürger ihre Mobiltelefone täglich oder beinahe täglich für Anrufe und das Versenden von Textnachrichten, zur Internetnutzung (60 %) sowie zum Versenden von E-Mails (46 %) nutzen. Die Hälfte der Befragten nutzen wöchentlich Online-Dienste zum Versenden von Sofortnachrichten. Nur 8 % der Befragten nutzen das Internet täglich für Anrufe oder Videoanrufe.[26]

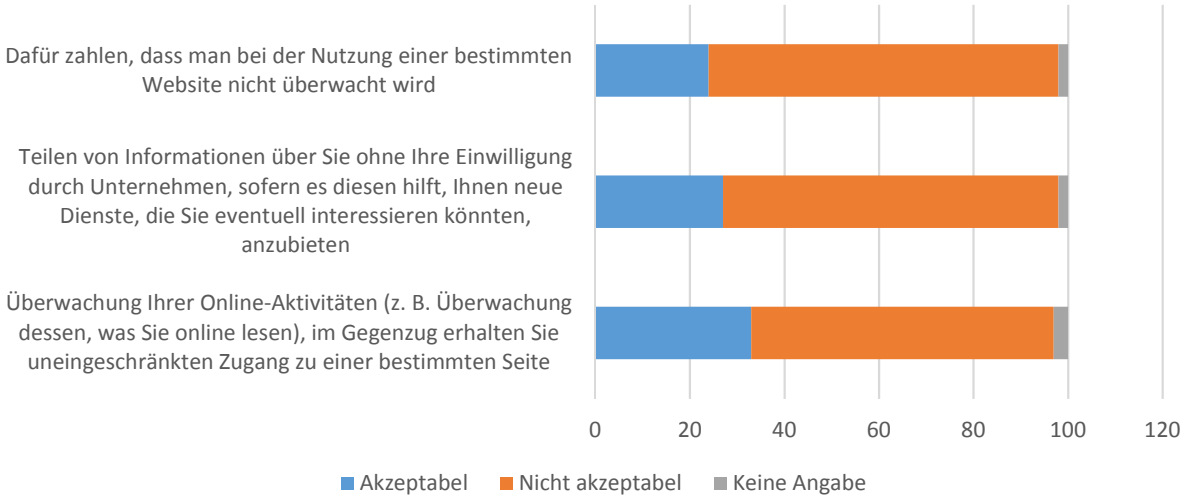
Bei der Frage, wie vertraut die Bürger mit den geltenden Rechtsvorschriften zum e-Datenschutz sind, gab die Mehrheit (67 %) an, sich bewusst darüber zu sein, dass der Zugang zu personenbezogenen Informationen wie Fotos oder Anruflisten, die auf ihrem Endgerät gespeichert sind, nur mit einer Einwilligung erfolgen kann. 58 % der Befragten waren auch die Bestimmungen bekannt, die für das Speichern von Informationen (wie zum Beispiel durch Cookies) auf ihren Endgeräten ohne ihre Einwilligung gelten. An dieser Stelle ist anzumerken, dass es bei dem zweiten Punkt zwischen den verschiedenen Mitgliedstaaten größere Unterschiede gab als bei dem ersten. Nur 37 % der Befragten waren sich der Tatsache bewusst, dass Sofortnachrichten und Sprachnachrichten nicht zwangsläufig vertraulich sind. 58 % der Befragten nahmen irrtümlich an, dass auf diese Kommunikation nur mit deren Einwilligung zugegriffen werden kann. Während die Antworten zeigten, dass es beider Sensibilisierung der Bürger geografische Unterschiede gab, schien die soziodemografische Verteilung keine Auswirkungen auf die Sensibiilisierung der Befragten zu haben.

Die Ergebnisse der Umfrage zeigten auch, dass es breite Zustimmung zur Vertraulichkeit von persönlichen Informationen, E-Mails und Sofortnachrichten gab. 65 % der Befragten gaben an, aktive Schritte zum Schutz ihrer Privatsphäre zu unternehmen, zum Beispiel indem sie Änderungen an den Privatsphäreeinstellungen auf ihren Endgeräten vornehmen oder bestimmte Websites meiden, damit ihre Aktivitäten nicht verfolgt werden.[27] Aktive Schritte unternehmen vor allem die Befragten in der Altersgruppe der 15 bis 39-Jährigen sowie mit dem höchsten Bildungsniveau. Fast 70 % der Befragten unterstützten in vollem Maße die Aussage, dass die Standardeinstellungen von Browsern „das Teilen von Informationen verhindern sollten“. Weitere 65 % gaben an, die Verschlüsselung von Anrufen und Nachrichten in vollem Maße zu unterstützen, damit nur der vorgesehene Empfänger Zugang zur Kommunikation erhält. Bei der Frage, wie oft Websites Anfragen stellen sollten, um Zugang zu Daten zu erhalten, gingen die Meinungen auseinander. 60 % der Befragten gaben an, zu viele unerbetene Anrufe zu Werbezwecken zu erhalten, und sprachen sich für die Möglichkeit aus, dass solche Anrufe immer mit einer bestimmten Vorwahl gekennzeichnet sein sollten. Mit steigendem Bildungsniveau der Befragten stieg auch deren Befürwortung dieser Möglichkeit. Die Umfrage holte auch Rückmeldungen zu einer Reihe von Szenarien ein. Siehe Grafik. Bei der Befürwortung der letzten beiden Szenarien gab es große Unterschiede zwischen den Mitgliedstaaten. Je älter die Befragten waren, desto weniger sprachen sie sich für diese zwei Optionen aus.

[26] Die Verteilung der Antworten nach Mitgliedstaat, Altersgruppe, Bildungsniveau sowie Daten zur Nutzung von sozialen Netzwerken, Fetstnetzanschlüssen u. a. finden Sie im Eurobarometer 443, S. 8-21.

[27] Es war festzustellen, dass in allen Mitgliedstaaten nur eine Minderheit der Befragten angab, spezielle Software zu nutzen, um Online-Werbung zu umgehen oder um zu verhindern, dass ihre Online-Aktivitäten verfolgt werden: Eurobarometer 443, S. 39-40.

Bild 1: In wie weit halten Sie die folgenden Praktiken für akzeptabel (% EU)?



Quelle: Ausführungen der Verfasserin auf Grundlage des Flash Eurobarometers 443 (Juli 2016), S. 55.

Offene öffentliche Konsultation

Von April bis Juli 2016 hat die Europäische Kommission eine offene öffentliche Konsultation durchgeführt. Themen waren sowohl die Bewertung als auch die geplante Überarbeitung der e-Datenschutz-Richtlinie.[28]

Der erste Teil des **Konsultationsfragebogens** bezog sich auf die REFIT-Bewertung der Richtlinie und inwieweit Letztere ihre drei Hauptziele wirksam erreichen kann. Dabei ging es um mögliche Probleme beim Verständnis und der Anwendung bestimmter Bestimmungen sowie darum, welche beobachteten Auswirkungen die Tatsache, dass verschiedene Behörden der einzelnen Mitgliedstaaten für diese Richtlinie zuständig sind, mit sich bringt. Im Fragebogen ging es auch darum, welche Bedeutung die Richtlinie hat, insbesondere mit Blick auf die Möglichkeit, zusätzlich zu den anderen Rechtsvorschriften besondere Regelungen für den e-Datenschutz einzuführen. Ein weiterer Schwerpunkt des Fragebogens war die Übereinstimmung mit bestimmten Artikeln anderer EU-Gesetze sowie der EU-Zusatznutzen der Richtlinie. Wie im Abschnitt zur REFIT-Bewertung bereits erwähnt, verfolgte die Konsultation auch das Ziel, qualitative und quantitative Informationen zu den Kosten und Nutzen der Richtlinie zu sammeln, um deren Wirksamkeit beurteilen zu können. Im zweiten Teil des Fragebogens ging es mehr um die künftigen Perspektiven und Prioritäten, die mögliche künftige Instrumente für Privatsphäre und Datenschutz in der elektronischen Kommunikation verfolgen sollten. Des Weiteren ging es darum, ob die Richtlinie durch eine Verordnung ersetzt oder inwieweit ihr Anwendungsbereich erweitert werden sollte. Außerdem wurden die Interessenvertreter nach ihrer Meinung zu verschiedenen Ansätzen befragt, zum Beispiel, wie Sicherheit und Vertraulichkeit in der Kommunikation gestärkt oder wie die Erfahrung der Nutzer mit Cookies verbessert werden können. Sie wurden aber auch zu den bestehenden Ausnahmen der Einwilligung bei der Verarbeitung von Verkehrs- und Standortdaten sowie zu Opt-in- und Opt-out-Regelungen für unerbetene Nachrichten zu Marketingzwecken befragt. Den Abschluss bildeten verschiedene Fragen zur uneinheitlichen Um- und Durchsetzung.

Im Rahmen der Konsultation gingen **421 Antworten** von verschiedenen Interessenvertretern, wie Bürgern (39 %), Branchenvertretern (44 %), Behörden (10 %) sowie von Verbänden der Zivilgesellschaft und Verbraucherorganisationen (8 %) ein. Insgesamt kamen 26 % der Antworten aus Deutschland, 14 % aus dem Vereinigten Königreich, 10 % aus Belgien und 7 % aus Frankreich. Die eingegangenen Antworten[29] lassen sich grob in drei Gruppen einteilen (Antworten von Bürgern, Verbraucherorganisationen und Verbänden der

[28] Zur gleichen Zeit hat die Kommission über die REFIT-Plattform und gemeinsam mit der Artikel 29 Datenschutzgruppe und dem Netz für Zusammenarbeit im Verbraucherschutz zusätzliche Konsultationstätigkeiten sowie zwei Workshops mit Interessenvertretern durchgeführt. Die Ergebnisse dieser Aktivitäten sind in SWD (2017) 3, Anhang 3 zusammengefasst.

[29] Sämtliche Beiträge, unterteilt nach den jeweiligen befragten Gruppen, finden Sie hier.

Zivilgesellschaft; Antworten aus den Branchen und Antworten von Behörden)[30], deren Meinungen bei den Hauptthemen der Konsultation stark auseinandergingen. An dieser Stelle sei anzumerken, dass **diese Kategorien nicht so einheitlich sind, wie sie zunächst möglicherweise erscheinen**: So zählen zu Branchenvertretern zum Beispiel sowohl traditionelle Telekommunikationsanbieter als auch OTTs, die unterschiedliche Auffassungen mit Blick auf zentrale Themen der Richtlinie, wie zum Beispiel hinsichtlich deren Anwendungsbereich, vertreten.

Da viele Ergebnisse der Konsultation direkt in die eingangs erwähnte REFIT-Bewertung eingeflossen sind, soll in diesem Abschnitt vor allem auf eine Reihe ausgewählter Themen der Konsultation eingegangen werden. Mit Blick auf die **fünf Kriterien der Bewertung** war die große Mehrheit der Bürger, Verbraucher- und zivilgesellschaftlichen Organisationen nicht der Auffassung, dass die aktuelle Version der Richtlinie einen vollständigen Schutz der Privatsphäre und Vertraulichkeit der Kommunikation wirksam sicherstellen könne. Dabei verwiesen sie auf den begrenzten Anwendungsbereich und die Tatsache, dass bei der Einwilligung zur Nutzung von Cookies keine echte Wahlmöglichkeit bestehe. Bei den Branchenvertretern teilten elektronische Kommunikationsdienstleister die Auffassung der Bürger in diesem Punkt. 57 % der Industrieakteure gaben jedoch an, dass die Richtlinie wirksam sei. Diese positivere Auffassung vertraten auch die Behörden.

Bürger und Vertreter der Zivilgesellschaft bestätigten, dass gesonderte Regelungen für die elektronische Kommunikation wichtig seien, um die Ziele der Privatsphäre und Vertraulichkeit erreichen zu können. Auch 90 % der Behörden vertraten diese Auffassung. Branchenvertreter hingegen sahen in den sektorspezifischen Bestimmungen keine Vorteile, da viele der Anforderungen der e-Datenschutz-Richtlinie auch durch die Datenschutz-Grundverordnung oder andere Rechtsrahmen abgedeckt werden könnten.[31] Den Antworten der Bürger und zivilgesellschaftlichen Vertreter zufolge stehen die Richtlinie und andere Rechtsinstrumente nur bedingt miteinander in Einklang. Branchenvertreter hingegen sahen eine größere Kohärenz zwischen der e-Datenschutz-Richtlinie und der Datenschutz-Grundverordnung, der Rahmenrichtlinie über elektronische Kommunikationsnetze und der Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen. Auch die Antworten der Behörden gingen in diese Richtung. Wie eingangs bereits erwähnt, erwies sich die Erhebung von quantitativen Informationen zur Bewertung der Wirksamkeit der Richtlinie als schwierig. Während Branchenvertreter angaben, dass die durch die Richtlinie entstehenden Befolgungskosten sehr hoch (62 %) oder moderat (21 %) und allgemein unverhältnismäßig seien, gaben 57 % der Bürger, Verbraucher und Vertreter zivilgesellschaftlicher Organisationen an, dass die Kosten im Verhältnis zu den zu erreichenden Zielen stünden. Diese Meinung teilten auch die Befragten in Behörden (73 %). Bürger und Akteure der Branche waren sich jedoch einig, dass die Richtlinie und die nationalen Bestimmungen zur Umsetzung der Richtlinie nicht zu mehr Vertrauen seitens der Verbraucher geführt haben. Die Behörden kamen in diesem Punkt zu einer positiveren Einschätzung. Knapp 87 % der Bürge, Verbraucher und zivilgesellschaftlichen Vertreter gaben an, dass die Richtlinie einen EU-Zusatznutzen erbringe. 65 % der Behörden teilten diese Auffassung. 50 % der Branchenvertreter und sogar 60 % der elektronischen Kommunikationsdienstleister beantworteten die Frage, ob die Richtlinie einen EU-Zusatznutzen mit sich bringe, jedoch mit Nein.

Auch mit Blick auf die **anstehende Überarbeitung der Richtlinie** gingen die Meinungen der Interessenvertreter auseinander. Eine detaillierte Auswertung würde den Rahmen dieses Briefings sprengen. Ein Vergleich, wie die drei Kategorien der Umfrageteilnehmer die verschiedenen Optionen zur Überarbeitung des derzeitigen Textes einschätzen (siehe Tabelle 2) ist jedoch sehr aufschlussreich. Wie hoch der Anteil derer ist, die eine jeweilige Option befürworten, steht in Klammern.[32]

Die Idee eines möglichen überarbeiteten Instruments, das die derzeitige Richtlinie durch eine Verordnung ersetzt, wurde von den Bürgern Verbrauchern und zivilgesellschaftlichen Vertretern (66 %) sowie den

[30] Diese Unterteilung findet sich auch im vollständigen Bericht der Kommission über die Konsultation.
[31] Hierbei ist jedoch zu beachten, dass einige Branchenvertreter der Auffassung waren, dass einige bestimmte Regelungen für Direktmarketing und Teilnehmerverzeichnisse weiterhin notwendig seien. Vollständiger Bericht über die Konsultation, S. 5.
[32] Eine detaillierte Auswertung der hier zusammengefassten Positionen finden Sie auf den Seiten 9-18 des vollständigen Berichts zur Konsultation.

Befragten in Behörden (67 %) befürwortet. Die Branchenvertreter hingegen bevorzugten andere Optionen, wie die Aufhebung der Richtlinie 2002/58 und die Anwendung anderer Rechtsvorschriften, wie der Datenschutz-Grundverordnung.

Die Bürger, die zivilgesellschaftlichen Organisationen und die Akteure der Branche waren sich weitgehend einig, dass die **Governance-Struktur verschlankt** und eine einzige Einrichtung, am besten eine der nationalen Datenschutzbehörden, mit der Durchsetzung der Richtlinie beauftragt werden sollte. Diese Auffassung teilten nur 39 % der Befragten in Behörden. 50 % sprachen sich gegen diese Option aus.[33]

Tabelle 2: Höchste Prioritäten bei der Überarbeitung nach befragten Gruppen

Bürger, Verbraucher und Zivilgesellschaft	Branche	Behörden
Änderung der Bestimmungen zur Vertraulichkeit der Kommunikation und Endgeräte (69 %)	Bestimmungen nicht mehr erforderlich (56 %)	Erweiterung des Anwendungsbereichs auch auf OTTs (72 %)
Erweiterung des Anwendungsbereichs auch auf OTTs (63 %)	Erweiterung des Anwendungsbereichs auch auf OTTs umfassen (29 %)	Änderung der Bestimmungen zu unerbetenen Werbenachrichten (59 %)
Änderung der Bestimmungen zur Governance (62 %)	Änderung der Bestimmungen zu unerbetenen Werbenachrichten (23 %)	Änderung der Bestimmungen zur Vertraulichkeit (52 %)
Änderung der Bestimmungen zu unerbetenen Werbenachrichten (58 %)	Änderung der Bestimmungen zur Governance (23 %)	Änderung der Bestimmungen zur Sicherheit (41 %)
Änderung der Bestimmungen zur Sicherheit (56 %)	Änderung der Bestimmungen zur Vertraulichkeit der Kommunikation und Endgeräte (20 %)	Änderung der Bestimmungen zur Governance (41 %)
Bestimmungen nicht mehr erforderlich (4 %)	Änderung der Bestimmungen zur Sicherheit (17 %)	Andere Optionen (7 %)

Quelle: Ausführungen der Verfasserin auf Grundlage des Berichts zur Konsultation, S. 9.

5. Europäischer Wirtschafts- und Sozialausschuss

Eine jüngst abgeschlossene Studie zur Ethik von Big Data[34], die im Namen des Europäischen Wirtschafts- und Sozialausschusses durchgeführt wurde, widmet sich der schwierigen Frage, wie ein Gleichgewicht zwischen den Grundrechten wie Privatsphäre und Vertraulichkeit und den wachsenden wirtschaftlichen Chancen, die Big Data bietet, gefunden werden kann. Im Rahmen der Studie wurden **fünf Ausgleichsmaßnahmen** identifiziert, die in politische Maßnahmen umgesetzt werden könnten. Obwohl die empfohlenen Maßnahmen eng mit der Datenschutz-Grundverordnung verbunden sind, könnten sich die Maßnahmen Nummer 1, 2 und 5 definitiv auch auf Bereiche auswirken, die derzeit durch die e-Datenschutz-Richtlinie abgedeckt sind.

Die erste mögliche Maßnahme sieht vor, eine EU-Plattform für Datenschutzmanagement zu schaffen, eine zentrale Anlaufstelle bzw. ein zentrales Portal der EU, das es natürlichen Personen ermöglicht, zu kontrollieren, wie deren personenbezogene Daten genutzt werden. Die zweite Maßnahme zielt darauf ab, ein Protokoll für ethisches Datenmanagement in Form eines europäischen Zertifizierungssystems zu erarbeiten, welches dazu beitragen würde, Marktakteure ausfindig zu machen, die den Datenschutz achten. Die fünfte Maßnahme betrifft die digitale Bildung und soll dazu dienen, ein besseres Verständnis von Big Data und dessen Folgen für Einzelpersonen zu schaffen. Alle fünf Aktionslinien wurden den Interessenvertretern vorlegt, unter anderem, damit diese die Umsetzbarkeit der Maßnahmen bewerten können. Einige der Vorschläge, wie die Einrichtung einer zentralen Anlaufstelle bzw. eines zentralen Portals gelten als verfrüht,

[33] Hierbei gilt zu beachten, dass die verschiedenen Beweggründe für die gegebenen Antworten nicht erfasst sind und dass insgesamt 21 % der Befragten eine andere als die vorgestellten Optionen vorziehen. Dazu gehört unter anderem die Aufhebung der Richtlinie. Einige der Befragten gaben auch zu bedenken, dass nicht mit dem Datenschutz in Verbindung stehenden Belangen womöglich weniger Aufmerksamkeit geschenkt werde, wenn Datenschutzbehörden mit der Durchführung der Richtlinie beauftragt würden.

[34] „The ethics of Big Data: Balancing economic benefits and ethical questions of Big Data in EU policy context", Studie für den EWSA, durchgeführt von Evodevo Srl (2017). Die Studie soll Anfang Februar auf der Homepage der Kommission veröffentlicht werden.

oder, angesichts der derzeitigen Situation, als nicht angebracht. Andere Maßnahmen, wie Investitionen in Bildung und Aufklärung und die Einrichtung eines europäischen Zertifizierungssystems für Unternehmen fanden bei den Interessenvertretern jedoch Anklang.

6. Schlussfolgerungen

Seit Annahme der Richtlinie 2002/58 über Datenschutz in der elektronischen Kommunikation haben sich die technologischen, wirtschaftlichen und sozialen Bedingungen stark verändert. Trotz der gezielten Änderungen aus dem Jahr 2009 wird der aktuelle Text der Richtlinie den Entwicklungen im Sektor und in Bezug auf Verbrauchergewohnheiten nicht mehr in vollem Maße gerecht. Wesentliche Veränderungen in diesem Bereich entstanden unter anderem durch neuartige Akteure auf dem Markt und die verbreitete Nutzung von Online-Diensten, zum Beispiel zum Versenden von Direktnachrichten. Diese können möglicherweise auch Auswirkungen auf die Wirksamkeit der bestehenden e-Datenschutz-Bestimmungen mit sich bringen. Zudem wurde durch die Annahme der Datenschutz-Grundverordnung im Jahr 2016 der Rechtsrahmen zum Datenschutz verändert, wodurch infrage gestellt werden könnte, welche Bedeutung die e-Datenschutz-Richtlinie noch hat und inwieweit sie in Einklang mit den neuen Rechtsvorschriften steht.

Die zur Bewertung der Wirksamkeit, Effizienz, Kohärenz, Bedeutung und des EU-Zusatznutzens der Richtlinie 2002/58 erhobenen Daten, das Feedback, dass die Kommission in ihren zielgerichteten Workshops erhielt, die öffentliche Online-Konsultation und die Umfrage des Eurobarometers haben gezeigt, dass es noch eine Reihe verschiedener Herausforderungen gibt. Diese wurden auch im Rahmen einer vom Europäischen Parlament im Jahr 2015 durchgeführten Sonderkonferenz angesprochen.[35] So führen einige der grundlegenden Bestimmungen der Richtlinie noch nicht in vollem Maße dazu, dass die vom Gesetzgeber beabsichtigten Grade an Vertraulichkeit und Schutz erreicht werden. Dies ist zum Beispiel der Fall von Artikel 5(3) zu Cookies und anderen Techniken, mit denen Informationen auf dem Endgerät der Nutzer gespeichert und zugänglich gemacht werden. Dieser Punkt wurde mehrfach, auch von den Mitgliedern des Europäischen Parlaments, angesprochen. Zudem scheinen einige Teile der Richtlinie 2002/58 aus technischer Sicht überholt oder es wurden zwischenzeitlich bereits bessere rechtliche Vorgehensweisen unternommen. Eine Bewertung der Umsetzung der e-Datenschutz-Richtlinie in den Mitgliedstaaten zeigte, dass in unterschiedlichem Umfang regulatorische Fragmentierungen, unterschiedlich hohe Schutzniveaus innerhalb der EU und komplizierte Governance-Strukturen festzustellen sind, bei welcher Behörden unterschiedlicher Art, teilweise sogar im selben Mitgliedstaat, für die Durchsetzung der Richtlinie zuständig sind. Dies hat insgesamt zu mangelnder Rechtssicherheit, unzureichender Klarheit und ungleichen Rahmenbedingungen innerhalb der EU geführt. Dennoch wurde auch immer wieder betont, dass spezielle Bestimmungen zum Schutz der Privatsphäre und zur praktischen Anwendung des Artikels 7 der Charta der Grundrechte der Europäischen Union nicht nur einen EU-Zusatznutzen mit sich bringen, sondern auch insgesamt von Bedeutung sind. Die Modernisierung der bisherigen Bestimmungen ist deshalb ein zentraler Punkt der EU-Strategie für einen digitalen Binnenmarkt. So soll das Vertrauen der Verbraucher und der Unternehmen in das digitale Umfeld wieder hergestellt und verbessert werden.

Am 10. Januar 2017 hat die Europäische Kommission einen Vorschlag zur Aufhebung der Richtlinie 2002/58 vorgelegt. Die Richtlinie soll durch eine Verordnung ersetzt werden, in der auf eine Reihe der eingangs erwähnten Problematiken eingegangen werden soll und mit welcher geltende Bestimmungen vereinfacht und zukunftsfähig gemacht werden sollen. Die Mitgesetzgeber haben nun die Aufgabe, ein Gleichgewicht zwischen den zahlreichen gegensätzlichen Positionen und Erwartungen zu finden, die im Laufe des Prozesses, der zur Überarbeitung der Richtlinie geführt hat, aufgekommen sind.

[35] Protecting online privacy by enhancing IT security and strengthening EU IT capabilities, Hochrangige Konferenz, gemeinsam vom LIBE-Ausschuss des Europäischen Parlaments, der STOA-Lenkungsgruppe und der Luxemburgischen Ratspräsidentschaft organisiert, 8. Dezember 2015.

7. Weitere Quellen zu Referenzzwecken

Carey, P. (2015), Data protection: a practical guide to UK and EU law, Oxford University Press.

Davies, R., Regulating electronic communications: A level playing field for telecoms and OTTs?, Briefing, Wissenschaftlicher Dienst des Europäischen Parlaments, 31. August 2015.

Leith, P. (2015), Privacy in the Information Society - The library of essays on law and privacy, Band II, Aldershot, Ashgate Publishing Group.

Luzak, J. (2013), Much Ado about Cookies: The European Debate on the New Provisions of the ePrivacy Directive regarding Cookies 21 European Review of Private Law, Ausgabe 1, S. 221–245.

REFIT-Plattform, Opinion on the submission by the Danish Business Forum on the E-Privacy directive and the current rules related to 'cookies', 27. -28. Juni 2016.

Das Referat Politikzyklus erreichen Sie per E-Mail unter: EPRS-PolicyCycle@ep.europa.eu

Redaktionsschluss: Januar, 2017.