

Erwartungen an die ePrivacy-Verordnung aus Sicht des Verbraucherschutzes

in: vorgänge Nr. 221/222 (1-2/2018), S. 103-114

Die EU-Datenschutz-Grundverordnung klammert den Datenschutz im Zusammenhang mit der elektronischen Kommunikation aus. Für die Internetnutzung und andere Formen elektronischer Kommunikation hat die Europäische Kommission daher Anfang 2017 einen Vorschlag für eine ePrivacy-Verordnung vorgelegt, die eine EU-Richtlinie zu diesem Thema aus dem Jahr 2002 ablösen soll. Florian Glatzner analysiert diesen Vorschlag und die Debatten hierzu aus der Perspektive des Verbraucherschutzes.

Die Datenschutzrichtlinie für elektronische Kommunikation[1] (folgend ePrivacy-Richtlinie) spezifizierte und ergänzte die bisherige europäische Datenschutzrichtlinie[2], die ab Mai 2018 durch die europäische Datenschutz-Grundverordnung[3] (folgend DSGVO) abgelöst wird. In der Mitteilung "Strategie für einen digitalen Binnenmarkt für Europa" (COM(2015) 192 final) vom 6. Mai 2015 legte die EU-Kommission fest, dass die ePrivacy-Richtlinie überprüft werden sollte, sobald die DSGVO beschlossen wurde. Infolge dieser Überprüfung legte die EU-Kommission am 10. Januar 2017 einen Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation[4] (folgend ePrivacy-Verordnung) vor. Das Europäische Parlament stimmte nach kontroversen Verhandlungen seine Position am 23. Oktober 2017 ab. Die generelle Ausrichtung des Rats der Europäischen Union steht bisher noch aus.

Grundsätzliche Betrachtungen

Während die europäische Datenschutzrichtlinie und die ePrivacy-Richtlinie weitgehend aufeinander abgestimmt waren, wird das Zusammenspiel der DSGVO und der ePrivacy-Richtlinie ab Mai 2018 von Unklarheiten für alle Beteiligten geprägt sein. Dementsprechend ist eine Überarbeitung der ePrivacy-Richtlinie unausweichlich, um einen konsistenten Rechtsrahmen in Europa zu schaffen. Doch nicht nur Änderungen des europäischen Rechts, auch die schnell voranschreitenden technischen Entwicklungen im Bereich der elektronischen Kommunikation machen eine Novelle dringend erforderlich. Eine Modernisierung und die Entwicklung eines EU-weit einheitlichen Rechts ist also geboten, um den Schutz der persönlichen Daten und die Privatsphäre der Verbraucher_innen auch in Zukunft zu gewährleisten und gleichzeitig die Rechtssicherheit und Wettbewerbsfähigkeit der europäischen Unternehmen zu stärken.

Notwendigkeit einer sektorspezifischen Regelung

Ziel der kommenden ePrivacy-Verordnung ist, das Recht auf Privatsphäre und der Vertraulichkeit der elektronischen Kommunikation sicherzustellen. Dieses Ziel kann nur mit einer sektorspezifische Regelung erreicht werden. Die ab Mai 2018 geltende DSGVO ist dafür alleine nicht ausreichend. Aufgrund der spezifischen Risiken im Bereich der elektronischen Kommunikation müssen die abstrakten Vorschriften der DSGVO für diesen spezifischen Bereich konkretisiert werden. Insofern soll die ePrivacy-Verordnung in erforderlicher Weise die DSGVO detaillieren.

Ferner bildet die DSGVO lediglich Artikel 8 der EU-Grundrechtecharta (Schutz personenbezogener Daten) ab, während die ePrivacy-Verordnung darüber hinaus Artikel 7 der EU-Grundrechtecharta (Achtung des Privat- und Familienlebens) ausgestaltet. Dieser schreibt unter anderem das Recht auf vertrauliche Kommunikation fest. Vertrauliche Kommunikation ist nicht nur unerlässlich, um die Persönlichkeitsrechte Einzelner zu schützen, sondern auch um die Funktionsfähigkeit demokratischer Gesellschaften sicherzustellen. Allerdings steht die Vertraulichkeit der Kommunikation in Zeiten der Digitalisierung durch die neuen Möglichkeiten und Fortschritte bei der Datenverarbeitung unter starkem Beschuss. Daher sind weiterhin klare und strikte Regelungen notwendig, um diese Vertraulichkeit zu schützen.

Vor diesem Hintergrund erklärt sich auch, dass auf Basis der ePrivacy-Verordnung eine Verarbeitung von Daten der elektronischen Kommunikation nur auf Grundlage eines gesetzlichen Erlaubnistatbestands oder mit Einwilligung der Nutzer_innen möglich sein soll und eine Verarbeitung auf Basis einer Interessenabwägung für diesen besonders sensiblen Bereich ausgeschlossen wird. Eine solche Abwägung zwischen den berechtigten Interessen eines Unternehmens und den Interessen oder Grundrechten einer betroffenen Person ist in der DSGVO als eine mögliche Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten vorgesehen.

Darüber hinaus werden wesentliche Verbraucherschützende Vorschriften der ePrivacy-Verordnung durch die DSGVO nicht abgedeckt. Dazu gehören beispielsweise Regelungen zum Schutz von Informationen, die auf den Kommunikationsgeräten der Nutzer_innen gespeichert sind sowie Vorschriften zu unerbetener Kommunikation, wie beispielsweise telefonischer Direktwerbung. Somit detailliert die ePrivacy-Verordnung nicht nur die DSGVO, sondern ergänzt sie auch.

Darüber hinaus ist eine Überarbeitung der ePrivacy-Richtlinie notwendig, um das verlorene Vertrauen der Menschen in die digitale Wirtschaft wieder herzustellen. Im Jahr 2015 vertrauten lediglich 32 Prozent der Deutschen den Internet- und Telefonanbietern, nur 19 Prozent vertrauten der Internetwirtschaft (Europäische Kommission 2015:66). 70 Prozent der Deutschen zeigten sich besorgt, dass ihre Daten zu anderen Zwecken verwendet werden, als sie ursprünglich erhoben wurden (wie Direktmarketing, Profilbildung oder interessenbezogene Werbung) (Europäische Kommission 2015:69). 42 Prozent der deutschen Internetnutzer_innen vermeiden sogar bestimmte Webseiten, weil sie befürchten, dass ihre Onlineaktivitäten beobachtet werden (Europäische Kommission 2016:39).

Auch in einer breit angelegten Umfrage des Vodafone Instituts für Gesellschaft und Kommunikation vom Januar 2016 spiegelt sich das geringe Vertrauen der Verbraucher_innen in datenverarbeitende Dienste wider. Beispielsweise vermeiden es 56 Prozent der deutschen Befragten, in E-Mails oder Textnachrichten über sehr persönliche Dinge zu schreiben, da sie befürchten, dass Dritte auf diese zugreifen könnten (Vodafone Institut 2016:53). Außerdem gaben 36 Prozent der Deutschen an, gänzlich auf soziale Netzwerke zu verzichten, um ihre Daten zu schützen (Vodafone Institut 2016:76). Und selbst wenn ihre Daten anonymisiert wären, würden sich nur 42 Prozent der deutschen Befragten damit wohl fühlen, diese Daten an die Gesundheitsforschung zu geben (Vodafone Institut 2016:122). Dies zeigt, dass sogar die Erfolgchancen vorbildlicher oder datenschutzfreundlicher Dienste durch das mangelnde Vertrauen der Verbraucher_innen in Mitleidenschaft gezogen werden können. Im Gegensatz dazu wirken Privatsphäre und Vertraulichkeit der Kommunikation vertrauensbildend, da sie Risiken für die Nutzer_innen verringern. Das Vertrauen der Verbraucher_innen ist eine Grundbedingung für den Erfolg datenintensiver Geschäftsmodelle in Europa.

Europaweite Harmonisierung

Ein weiteres Ziel der ePrivacy-Verordnung ist es, eine europaweite Harmonisierung des Rechts auf Privatsphäre und der Vertraulichkeit der elektronischen Kommunikation auf einem hohen Niveau sicherzustellen. Dieses Ziel wurde zwar schon bisher durch die ePrivacy-Richtlinie verfolgt, konnte in der

Vergangenheit jedoch nicht erreicht werden. Die Mitgliedsstaaten nutzten nicht nur die ihnen eingeräumten Spielräume, sondern setzten auch einzelne Vorschriften höchst unterschiedlich um, wie beispielsweise Regelungen zu Cookies und ähnlichen Tracking-Technologien (DLA Piper 2016). In Folge dessen konnten zum Beispiel deutsche Verbraucher_innen in der Vergangenheit ihre europarechtlich vorgesehenen Rechte zum Schutz ihrer Privatsphäre nur unzureichend wahrnehmen (DSK 2015).

Vor diesen Hintergrund ist es positiv, dass die EU-Kommission in ihrem Vorschlag die Form einer Verordnung gewählt und in diesem entsprechend der DSGVO das Marktortprinzip festgelegt hat. Demnach ist einheitlich jede Bereitstellung elektronischer Kommunikationsdienste für Verbraucher_innen und die Nutzung dieser Dienste in der EU erfasst, unabhängig davon, ob eine Bezahlung verlangt wird und unabhängig davon, ob ein Unternehmen in der EU niedergelassen ist oder nicht. So kann die europaweite Harmonisierung und eine hohe Konsistenz zur DSGVO erreicht werden.

Ausweitung des Anwendungsbereiches

Zwar war die ePrivacy-Richtlinie schon bisher ein wichtiges Instrument, um das Recht auf Privatsphäre und Vertraulichkeit in der elektronischen Kommunikation sicherzustellen, jedoch konnte ein umfassender Schutz aufgrund des eingeschränkten Anwendungsbereichs der Richtlinie auf klassische Telekommunikationsanbieter nicht gewährleistet werden. Dem ökonomischen, sozialen und politischen Bedeutungszuwachs von Over-The-Top-Kommunikationsanbietern[5] (folgend OTTs) wurde die ePrivacy-Richtlinie bisher nicht ausreichend gerecht.

Während noch vor wenigen Jahren der Großteil der elektronischen Kommunikation über traditionelle Telekommunikationsanbieter geführt wurde, kommunizieren Verbraucher_innen heute in erster Linie über diese OTT-Dienste. Beispielsweise sendeten die deutschen Verbraucher_innen im Jahr 2012 – als die ePrivacy-Richtlinie in Deutschland umgesetzt wurde – noch über 160 Millionen SMS-Nachrichten und 20 Millionen WhatsApp-Nachrichten am Tag. Im Jahr 2015 hatten sich diese Zahlen umgekehrt: die Deutschen sendeten weniger als 40 Millionen SMS-Nachrichten pro Tag, aber über 660 Millionen WhatsApp-Nachrichten (Statista 2015). Diese Nachrichten stehen jedoch nicht unter einem vergleichbaren Schutz wie klassische SMS-Nachrichten.

Diese Unterscheidung ist für viele Verbraucher_innen im höchsten Maße irritierend. So glauben 62 Prozent der Deutschen fälschlicher Weise, dass per Gesetz Instant-Messaging- und VoIP-Telefonate vertraulich seien und niemand auf diese ohne ihre Einwilligung zugreifen dürfe (Europäische Kommission 2016:27). Für sie ist nicht verständlich, weshalb eine Nachricht die per SMS versendet wird, einen höheren Schutz genießt als eine Nachricht, die sie – möglicherweise sogar über dieselbe Smartphone-Applikation – über das Internet versenden. So verstehen sie beispielsweise nicht, warum Anbieter von OTT-Diensten derzeit die Inhalte von Nachrichten auslesen und auswerten dürfen.

Damit einhergehend ist auch aus grundrechtlicher Perspektive die bisherige Unterscheidung heutzutage nicht mehr nachvollziehbar. Denn würde das Schutzniveau nicht an die heutigen Kommunikationsgegebenheiten angepasst werden, würde sich das allgemeine Schutzniveau durch die Verlagerung der Kommunikation massiv verringern. Daher ist es richtig, dass der Anwendungsbereich der ePrivacy-Verordnung auf alle Kommunikationsdienste ausgeweitet werden soll, wenn diese äquivalent zu klassischen Telekommunikationsdiensten sind und diese substituieren.

Die Regelungen im Einzelnen

Aber was sehen nun die einzelnen Regelungen der ePrivacy-Verordnung vor? Schon der Vorschlag der EU-Kommission enthielt aus Verbrauchersicht viele gute Ansätze, aber auch kritische Punkte und offene Detailfragen. Das Europäische Parlament führte diesen grundsätzlich verbraucherfreundlichen Ansatz fort und schärfte ihn weiter. Aus dem EU-Rat und den Mitgliedsstaaten sind bisher nur wenige konkrete Vorschläge an die Öffentlichkeit gedrungen.

Besonders strittig wird derzeit die Frage diskutiert, auf welchen Rechtsgrundlagen elektronische Kommunikationsdaten verarbeitet werden dürfen. Außerdem stehen die Regelungen zum Schutz von Informationen, die mit den Kommunikationsgeräten der Nutzer_innen in Verbindung stehen, sowie Vorgaben zur datenschutzfreundlichen Voreinstellung von Kommunikationssoftware im Zentrum der kontroversen Debatte.

Schutz der Kommunikation

Die ePrivacy-Verordnung soll regeln, unter welchen Bedingungen und auf Basis welcher gesetzlichen Grundlagen elektronische Kommunikationsdaten verarbeitet werden dürfen. Demnach soll eine Verarbeitung von elektronischen Kommunikationsdaten künftig nur auf Grundlage eines gesetzlichen Erlaubnistatbestands oder mit Einwilligung der Nutzer möglich sein. Zu diesen elektronischen Kommunikationsdaten gehören sowohl die Inhalte elektronischer Kommunikation, als auch Metadaten. Grundsätzlich ist es also untersagt, Verbindungsdaten und Inhalte von Nachrichten abzufangen oder zu überwachen, außer wenn die betroffenen Nutzer_innen eingewilligt haben oder es dafür eine gesetzliche Ermächtigung gibt.

Inhalte der elektronischen Kommunikation können hochsensible Informationen über die daran beteiligten natürlichen Personen offenlegen, von persönlichen Erlebnissen und Gefühlen oder Erkrankungen bis hin zu sexuellen Vorlieben und politischen Überzeugungen, was zu schweren Folgen im persönlichen und gesellschaftlichen Leben oder zu wirtschaftlichen Einbußen führen kann. Daher war es Telekommunikationsanbietern bisher nicht gestattet, überhaupt die Inhalte elektronischer Kommunikation zu verarbeiten. Künftig soll die Verarbeitung von Inhalten jedoch für die Betreiber elektronischer Kommunikationsdienste erlaubt sein, wenn alle betroffenen Nutzer_innen ihre Einwilligung zur Verarbeitung ihrer elektronischen Kommunikationsinhalte für bestimmte Zwecke gegeben haben.

Wären diese Regelungen also für Telekommunikationsunternehmen neue Verarbeitungsmöglichkeiten eröffnen, stellen sie für die OTT-Dienste eine aus Verbrauchersicht begrüßenswerte Einschränkung dar. So war es beispielsweise bei vielen vermeintlich kostenlosen E-Mail-Anbietern bisher üblich, die Nachrichteninhalte der Nutzer_innen zu analysieren, um diesen dann maßgeschneiderte Produktinformationen anzuzeigen (vzbv 2016). Da auch OTT-Dienste künftig von der ePrivacy-Verordnung erfasst werden, wird nach den bisherigen Vorschlägen die Einwilligung aller beteiligten Kommunikationspartner_innen notwendig sein, wenn beispielsweise ein E-Mail-Anbieter die Inhalte von Nachrichten zu Werbezwecken verarbeiten möchte.

Wichtig ist jedoch, dass sich der besondere Schutz der ePrivacy-Verordnung nicht nur auf elektronischen Kommunikationsdaten während ihrer Übertragung erstrecken darf, sondern sich auch auf Kommunikationsdaten, die auf den Servern der Anbieter gespeichert sind. Ansonsten würden die engen Ausnahmen für die Verarbeitung ins Leere laufen. Würde sich der Schutz nur auf die Übertragung erstrecken, könnten die Anbieter künftig unter anderem Inhaltsdaten auf Basis der DSGVO verarbeiten.

Diese Ausweitung der Verarbeitungsmöglichkeiten könnte das derzeitige Schutzniveau massiv verringern und würde dem Recht auf vertrauliche Kommunikation nach Artikel 7 der EU-Grundrechtecharta entgegenstehen.

Auch hinsichtlich der Kommunikationsmetadaten ist es kritisch, dass die Möglichkeiten der Verarbeitung durch die Telekommunikationsanbieter ausgeweitet werden sollen. Zu diesen Metadaten gehören unter anderem angerufene Nummern, der geografische Standort, Uhrzeit, Datum und Dauer eines getätigten Anrufs. Deren Verarbeitung war für Telekommunikationsunternehmen bisher auf Dienste beschränkt, für die Betroffene einwilligten und die gleichzeitig einen Mehrwert für diese Betroffenen boten. Nach den Vorschlägen der EU-Kommission und des EU-Parlaments soll die Verarbeitung künftig zu jedem Zweck möglich sein, zu dem die Betroffenen einwilligen. Auf der anderen Seite ist es hier ebenso zu begrüßen, dass in Zukunft somit auch andere Anbieter von OTT-Diensten die Metadaten der Nutzer_innen nur mit deren Einwilligung verarbeiten dürfen.

Besorgniserregend sind jedoch vor allem aktuelle Debatten – besonders in der Wirtschaft aber auch innerhalb der Bundesregierung und des EU-Rats – die diese grundlegende Stoßrichtung der Verordnungsvorschläge in Frage stellen und weitere Verarbeitungsbefugnisse fordern. Nach diesen Vorschlägen sollen in Zukunft auch ohne Einwilligung der Betroffenen Kommunikationsmetadaten auf der Rechtsgrundlage der Interessenabwägung von Betreibern elektronischer Kommunikationsdienste genutzt oder sogar "für kompatible Zwecke" weiterverarbeitet werden dürfen. Andere Forderungen lauten, dass es grundsätzlich gestattet sein sollte, pseudonymisierte Metadaten auch ohne Einwilligung der Betroffenen zu verarbeiten.

Da Kommunikationsmetadaten eine besondere Aussagekraft haben, können durch sie sehr sensible und persönliche Informationen offengelegt werden - wie es auch der Europäische Gerichtshof ausdrücklich feststellte.[6] Daher sollten entsprechende Informationen grundsätzlich nur mit Einwilligung der betroffenen Nutzer_innen oder auf Basis einer rechtlichen Grundlage verarbeitet werden dürfen. Eine Datenverarbeitung auf Basis einer durch die Unternehmen vorgenommenen Abwägung zwischen ihren berechtigten Interessen und den schutzwürdigen Interessen der Verbraucher_innen sowie eine Weiterverarbeitung für „kompatible Zwecke“ wäre im besonders sensiblen Kommunikationsbereich nicht akzeptabel.

Schutz der mit den Geräten der Nutzer_innen in Verbindung stehenden Informationen

Kommunikationsgeräte können – wie es der verstorbene Vizepräsident des Bundesverfassungsgerichts Winfried Hassemer formulierte – so etwas wie ein ausgelagertes Gehirn der Nutzer_innen sein. Entsprechend relevant sind die mit den Kommunikationsgeräten verbundenen Informationen für die Persönlichkeit und Privatsphäre ihrer Nutzer_innen. Daraus ergibt sich ein hohes Schutzbedürfnis für diese Geräteinformationen.

Gleichzeitig ist es heutzutage nahezu unmöglich, auf moderne Kommunikationsmittel oder Dienste der Informationsgesellschaft zu verzichten, wenn man am sozialen Leben oder am gesellschaftlichen Diskurs teilnehmen möchte. Jedoch speichern viele dieser Dienste und Anwendungen Informationen auf den Kommunikationsgeräten, rufen bereits gespeicherte Informationen von diesen Geräten ab oder nutzen deren Verarbeitungsmöglichkeiten. So legen nahezu alle Webseiten oder Applikationen Cookies auf den Rechnern oder Smartphones der Verbraucher ab oder verwenden Technologien wie das Device- oder Browser-Fingerprinting, um die Anwender zu identifizieren (Artikel-29-Datenschutzgruppe 2014).

Der Einsatz dieser Technologien kann zu vielen Zwecken erfolgen, beispielsweise zur Reichweitenmessung von Inhalten oder zur Individualisierung von Preisen. Häufigster Anwendungsfall dürfte aber sein, das Verhalten der Nutzer_innen über Webseiten, Apps oder Endgeräte hinweg zu erfassen bzw. Profile zu

erstellen, um diesen anschließend personalisierte Werbung anzeigen zu können. Viele Verbraucher_innen empfinden ein solches "Tracking" als Eingriff in ihre Privatsphäre und die Vertraulichkeit ihrer Kommunikation. Nach einer Studie der EU-Kommission fühlen sich lediglich 29 Prozent der Deutschen damit wohl, dass Internet-Unternehmen Informationen über ihre Online-Aktivitäten nutzen, um Werbung an ihre Interessen anzupassen (Europäische Kommission 2015:66).

Problematisch ist, dass sich das Tracking im Internet und auf dem Smartphone kaum umgehen lässt. Im Jahr 2014 untersuchte das Fraunhofer SIT 1.600 Webseiten und fand auf diesen über 600 verschiedene Tracking-Dienste eingebunden (Schneider et al. 2014). Die Top-3-Tracker wurden auf 994, 780 und 474 Seiten verwendet. Auf den Top-3-Seiten fand das Fraunhofer SIT jeweils über 70 verschiedene Tracker, die Top-25-Seiten hatten alle über 50 Tracker eingebunden.

Auf mobilen Geräten sieht die Lage nicht besser aus. Das Australia's Information and Communications Technology Research Centre of Excellence untersuchte im Jahr 2015 die Top-100 Android-Apps (Seneviratne et al. 2015). Über 85 Prozent der kostenlosen Apps beinhalteten mindestens ein Tracking-Framework, 30 Prozent mehr als fünf. Bei kostenpflichtigen Apps beinhalteten über 60 Prozent einen Tracker, etwa 20 Prozent drei oder mehr. Über 50 Prozent der Smartphones waren mit mehr als 25 Trackern in Kontakt, 20 Prozent der Telefone sogar mit über 40 Trackern. Diese Tracker übertrugen eine Vielzahl von personenbezogenen Daten und Identifikationsnummern (inklusive des Standorts, der Kontakte oder der Kalender).

Darüber hinaus versäumte die Werbeindustrie jahrelang die Gelegenheit, wirksame Selbstverpflichtungen einzurichten. So wird seit dem Jahr 2007 der Do-Not-Track-Standard entwickelt, der inzwischen von allen Webbrowsern unterstützt wird.[7] Von der Werbeindustrie wird der Standard jedoch nicht anerkannt. Die Do-Not-Track-Liste enthält gerade einmal 21 eingetragene Unternehmen, Google, Facebook, Yahoo etc. fehlen (Mayer, Narayanan 2018). Auch andere "Selbstverpflichtungen" und Widerspruchssysteme gelten als wirkungslos (BEUC 2011). Insofern gibt es derzeit kaum eine Möglichkeit, sich dem umfassenden Tracking zu entziehen, außer keine modernen Kommunikationsmittel zu nutzen und damit auf Teilhabe am sozialen Leben und der politischen Willensbildung zu verzichten.

Schon nach der bisherigen ePrivacy-Richtlinie war eigentlich eine Einwilligung der Nutzer_innen notwendig, wenn Daten auf ihren Kommunikationsgeräten gespeichert oder von diesen abgerufen wurden. Jedoch muss in den meisten Fällen bezweifelt werden, dass diese Einwilligungen frei, informiert und unmissverständlich erteilt wurden. So wurde bisher beispielsweise die schlichte Nutzung einer Webseite als eine Einwilligung zum Tracking gewertet. Darüber hinaus wurde die ePrivacy-Richtlinie in Deutschland nach Ansicht von Daten- und Verbraucherschützer_innen nicht richtlinienkonform umgesetzt, da das Telemediengesetz lediglich eine Widerspruchslösung vorsieht (DSK 2015).

Die kommende ePrivacy-Verordnung soll die bisherigen Regelungen EU-weit vereinheitlichen, konkretisieren und der Datenschutzaufsicht Mittel zur effektiven Durchsetzung des Rechts an die Hand geben. Unternehmen sollen nach den Vorschlägen der EU-Kommission und des EU-Parlaments weiterhin nur mit Einwilligung der Betroffenen Informationen von den Endgeräten nutzen oder darauf speichern dürfen – es sei denn diese Verarbeitung ist notwendig, um einen von den Nutzer_innen gewünschten Dienst zu erbringen. Diese Einwilligung soll den strengen Vorgaben der Datenschutz-Grundverordnung entsprechen.

Beide Vorschläge sehen außerdem eine Ausnahme für die Reichweitenmessung vor, die vom Parlament nochmals etwas klarer gefasst wurde. Demnach ist eine solche Reichweitenmessung bzw. Webseitenanalyse auch ohne Einwilligung erlaubt, wenn sie durch den Anbieter oder im Rahmen einer Auftragsverarbeitung vorgenommen wird, lediglich einer statistischen Zählung dient, die Daten aggregiert werden, Sicherheitsmaßnahmen (wie Pseudonymisierung der Daten) getroffen werden und die Daten nach Erreichen des Zwecks gelöscht werden. Außerdem sollen die Nutzer_innen über die Verarbeitung und ihre Zwecke informiert werden und über eine Widerspruchsmöglichkeit verfügen.

Darüber hinaus sollen Verbraucher_innen ihren Widerspruch zum Tracking künftig über die Einstellungen ihrer Softwareprogramme ausdrücken können, also beispielsweise über ihren Webbrowser oder innerhalb

einer App. Die Software soll den Wunsch der Nutzer den Diensteanbietern signalisieren. Dieses Signal soll rechtlich verbindlich sein.

Der Parlamentsentwurf sieht darüber hinaus ein Kopplungsverbot vor, so dass Nutzer_innen der Zugang zu einem Dienst nicht mit der Begründung verweigert werden darf, sie hätten ihre Einwilligung in die Verarbeitung personenbezogener Daten nicht gegeben, die für die Erbringung des Dienstes nicht notwendig ist. Ein solches Kopplungsverbot ist ein wichtiger Baustein, um die Freiwilligkeit der Einwilligung sicherstellen.

Eine Datenverarbeitung auf Basis einer durch die Unternehmen vorgenommenen Abwägung zwischen ihren berechtigten Interessen und den schutzwürdigen Interessen der Verbraucher_innen, wie Teile der Wirtschaft fordern, wäre auch hier nicht akzeptabel und würde hinter dem geltenden Recht zurück bleiben. Dementsprechend sind auch reine Widerspruchslösungen für das Tracking von Nutzer_innen abzulehnen.

Datenschutzfreundliche Voreinstellungen

In ihrem Vorschlag konnte sich die EU-Kommission leider nicht zu einer Regelung durchringen, dass Kommunikationssoftware stets datenschutzfreundlich voreingestellt sein muss. Sie schlug lediglich vor, dass die Software bei der Installation die Nutzer_innen über die Einstellungsmöglichkeiten zur Privatsphäre informieren soll. Die Installation ließe sich dann nur fortsetzen, wenn die Nutzer_innen sich für eine Privatsphäreneinstellung entschieden haben.

Dabei zeigt das Flash Eurobarometer 443 der EU-Kommission, dass sich die Verbraucher_innen datenschutzfreundliche Voreinstellungen ihrer Kommunikationssoftware wünschen. 90 Prozent der deutschen Internetnutzer_innen sprachen sich für solche Voreinstellungen in ihren Webbrowsern aus (Europäische Kommission 2016:46). Gleichzeitig zeigt die Studie auch, dass besonders Ältere, Personen mit niedrigerer Bildung sowie Menschen, die das Internet wenig verwenden, seltener Änderungen der Datenschutzeinstellungen ihrer Software vornehmen (Europäische Kommission 2016:37). Datenschutzfreundliche Voreinstellungen schützen also in erster Linie diese besonders vulnerablen Verbrauchergruppen.

Das EU-Parlament griff diese Kritik auf und schlägt vor, dass Hersteller von Kommunikationssoftware Datenschutz und Datensicherheit durch technische Gestaltung der Systeme und entsprechende Voreinstellungen gewährleisten müssen. Nach der Installation der Software sollen Nutzer_innen dann entscheiden können, ob sie die datenschutzfreundlichen Voreinstellungen beibehalten oder abändern wollen.

Ausblick

Die Zeit drängt. Nach den ursprünglichen Plänen der EU-Kommission sollte die ePrivacy-Verordnung gemeinsam mit der Datenschutz-Grundverordnung ab dem 25. Mai 2018 angewendet werden. Inzwischen hat sich jedoch herauskristallisiert, dass dieser Termin nicht zu halten ist. Zwar hat das Europäische Parlament seine Position bereits im Oktober 2017 abgestimmt, die Verhandlungen im EU-Rat waren aber bis März 2018 noch nicht sehr weit fortgeschritten. Auch innerhalb der Bundesregierung gab es zu den oben genannten Punkten bis März 2018 noch keine abgestimmte Position. Die bulgarische Ratspräsidentschaft kündigte zwar an, eine allgemeine Ausrichtung des Rates bis Juni 2018 anzustreben, um anschließend in die Trilog-Verhandlungen mit dem EU-Parlament und der EU-Kommission eintreten zu können. Aber es ist

fraglich, ob die Verhandlungen im Rat zu diesem Zeitpunkt abgeschlossen sein werden.

Diese Situation ist für alle Beteiligten höchst unbefriedigend. Das Nebeneinander von Datenschutz-Grundverordnung und ePrivacy-Richtlinie führt vor allem zu Rechtsunsicherheit. Diese Rechtsunsicherheit wird voraussichtlich noch einige Jahre aufrechterhalten bleiben. Selbst optimistische Prognosen gehen inzwischen davon aus, dass die Trilog-Verhandlungen bis Ende 2018 andauern werden. Außerdem ist derzeit eine Übergangsfrist von einem Jahr vorgesehen, so dass die ePrivacy-Verordnung voraussichtlich Ende 2019 in Kraft treten könnte.

Es ist zu hoffen, dass die europäischen Gesetzgeber und die Mitgliedsstaaten eine schnelle Lösung finden. Gleichzeitig dürfen sie den Datenschutz und die Vertraulichkeit elektronischer Kommunikation nicht den Versprechungen und Wünschen der Telekommunikations- und Werbeindustrie opfern, die oftmals auf Mythen und fehlgeleiteten Argumenten basieren und gesellschaftlichen Interessen entgegen stehen können (vgl. Dachwitz 2017). Der Entwurf des Parlaments bietet eine gute Grundlage, der der EU-Rat folgen sollte.

Wohin die Reise gehen wird, ist derzeit aber noch nicht absehbar. Klar ist: Ein Rückschritt hinter das Schutzniveau der bisherigen ePrivacy-Richtlinie wäre nur in eng begrenzten Fällen unter strengen Voraussetzungen tragbar. Viele der derzeit diskutierten Vorschläge sind dies aber nicht. Besonders Bestrebungen, das Schutzniveau der Datenschutz-Grundverordnung durch die ePrivacy-Verordnung abzuschwächen, sind aus Verbrauchersicht inakzeptabel. Ob die ePrivacy-Verordnung zu einer Verbesserung des Datenschutzes und der Vertraulichkeit der Kommunikation führen wird oder ob der unbefriedigende Status Quo erhalten bleibt, hängt nun stark von den Mitgliedsstaaten im Rat der EU – und damit auch von der deutschen Bundesregierung – ab.

FLORIAN GLATZNER *Jahrgang 1980, Politikwissenschaftler (M.A.), Referent im Team Digitales und Medien des Verbraucherzentrale Bundesverbands e.V. (vzbv) in Berlin, begleitet den Gesetzgebungsprozess zur ePrivacy-Verordnung aus Verbrauchersicht. Wichtigste Buchveröffentlichung: "Die staatliche Videoüberwachung des öffentlichen Raumes: Spielräume und Grenzen eines Instruments der Kriminalitätsbekämpfung" (2008).*

Literaturverzeichnis:

Artikel-29-Datenschutzgruppe 2014: Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting; abrufbar unter

https://collections.internetmemory.org/haeu/20170615232552/http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf

BEUC - Bureau Européen des Unions de Consommateurs 2011: EASA - IAB Best Practice Recommendations; abrufbar unter <http://www.beuc.eu/publications/2011-09975-01-e.pdf>

DLA Piper 2016: EU Law on Cookies; abrufbar unter https://www.dlapiper.com/~media/Files/Other/EU_Cookies_Update.pdf

Europäische Kommission 2015: Special Eurobarometer 431; abrufbar unter http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf

Europäische Kommission 2016: Flash Eurobarometer 443; abrufbar unter https://data.europa.eu/euodp/en/data/dataset/S2124_443_ENG

Dachwitz, Ingo 2017: ePrivacy-Mythen unter der Lupe: "Eine der schlimmsten Lobby-Kampagnen, die wir

je erlebt haben" ; abrufbar unter <https://netzpolitik.org/2017/eprivacy-mythen-unter-der-lupe-eine-der-schlimmsten-lobby-kampagnen-die-wir-je-erlebt-haben/>

DSK - Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder 2015: Keine Cookies ohne Einwilligung der Internetnutzer; abrufbar unter

https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/Entschliessung_Co

Mayer, Jonathan et al. 2018: Do Not Track: Implementations; abrufbar unter <http://donottrack.us/implementations>

Schneider, Markus et al. 2014: Web-Tracking-Report 2014; abrufbar unter <https://www.sit.fraunhofer.de/de/wtr/>

Seneviratne, Suranga 2015: Short: A Measurement Study of Tracking in Paid Mobile Applications; in: WiSec '15 Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks, Article No. 7; abrufbar unter <https://dl.acm.org/citation.cfm?id=2766523>

Statista 2015: Anzahl gesendeter SMS-Nachrichten pro Tag in Deutschland bis 2015; abrufbar unter <http://de.statista.com/statistik/daten/studie/3624/umfrage/entwicklung-der-anzahl-gesendeter-sms--mms-nachrichten-seit-1999/> vzbv - Verbraucherzentrale Bundesverband e.V. 2016: vzbv mahnt Datenschutzerklärung von Google erneut ab; abrufbar unter <https://www.vzbv.de/pressemitteilung/vzbv-mahnt-datenschutzerklaerung-von-google-erneut-ab>

Vodafone Institut für Gesellschaft und Kommunikation 2016: Big Data – A European Survey on the Opportunities and Risks of Data Analytics; abrufbar unter <http://www.vodafone-institut.de/wp-content/uploads/2016/01/VodafoneInstitute-Survey-BigData-en.pdf>

Anmerkungen:

1 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) in der Fassung der Richtlinie 2009/136/EG vom 25. November 2009

2 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

3 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

4 Vorschlag für eine Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG, COM (2017) 10 final vom 10. Januar 2017. 113 Glatzner: Erwartungen an die ePrivacy-Verordnung vorgänge #221/222

5 OTTs sind Dienste, die über einen Internetzugangsdienst angeboten werden, ohne jedoch dafür eine eigene Telekommunikationsinfrastruktur zu verwenden. Darunter fallen zum Beispiel Voice-Over-IP-Telefonate oder Instant Messaging.

6 Siehe verbundene Rechtssachen C-293/12 und C-594/12 Digital Rights Ireland und Seitlinger und andere,

ECLI:EU:C:2014:238; verbundene Rechtssachen C-203/15 und C-698/15 Tele2 Sverige AB und Secretary of State for the Home Department, ECLI:EU:C:2016:970

7 Do Not Track (DNT; englisch für "nicht verfolgen") ist ein HTTP-Header-Feld und signalisiert einer Website oder Webanwendung den Wunsch, dass diese über die Aktivitäten des Besuchers kein Nutzungsprofil erstellt

<https://www.humanistische-union.de/publikationen/vorgaenge/221-222/publikation/erwartungen-an-die-eprivacy-verordnung-aus-sicht-des-verbraucherschutzes-1/>

Abgerufen am: 16.08.2026