EU WAHL
DIGITAL19
eco

EU Agenda für eine moderne Digitalpolitik

19 Kernforderungen des eco zur Europawahl 2019

eco
VERBAND DER INTERNETWIRTSCHAFT

Inhalt

EU Agenda für eine moderne Digitalpolitik

Die Digitalisierung und das Internet sind aus dem Alltag nicht mehr wegzudenken. Ob das Mobiltelefon, das Smart-TV, die Beleuchtung zu Hause oder das Auto – beinahe alles kann heute über das Internet vernetzt und darüber mit aktuellen Informationen, Videostreams oder Updates versorgt bzw. geöffnet oder gesteuert werden. Die Digitalisierung schreitet auch in der Wirtschaft weiter voran. Entwicklungen wie Connected Cars, Internet of Things, Künstliche Intelligenz oder der Mobilfunkstandard 5G sind nur Beispiele, die andeuten, wohin wir uns bewegen.

Die Digitalisierung ist eine große Herausforderung für alle. Internationale Industrieunternehmen müssen sich ebenso umstellen wie kleine und mittlere Unternehmen (KMU), und auch die Politik steht vor zahlreichen neuen Fragen. Der Strukturwandel betrifft nahezu alle Bereiche der Wirtschaft und wirkt sich auf bestehende und zukünftige Geschäftsmodelle aus. Dies eröffnet viele Chancen und Möglichkeiten, stellt uns aber auch vor zahlreiche neue Herausforderungen.

Um Europa auch in der Zukunft auf dem globalen Markt wettbewerbsfähig zu halten, braucht es einen starken digitalen Binnenmarkt, und damit der digitale Wandel in allen Wirtschaftsbereichen gelingt, müssen die entsprechenden Rahmenbedingungen für die Digitalisierung geschaffen werden. Ein einheitlicher Rechtsrahmen für die digitalen Märkte und die Betreiber digitaler Technologien bzw. Dienste fördert die Innovationskraft bestehender Industrien und Wirtschaftsakteure, ermöglicht neue Wertschöpfungsketten und Geschäftsmodelle und stärkt nicht zuletzt neue Unternehmen bzw. Start-ups.

Zahlreiche Vorschläge wurden in der Legislaturperiode 2014–2019 von der EU-Kommission präsentiert, um bestehende Regelungen anzupassen oder zu ersetzen. Die Bandbreite der adressierten Themen reichte dabei von IT-Sicherheit bis hin zu Urheberrecht. Trotz dieser Vielzahl von Initiativen ist die Entwicklung des digitalen Binnenmarktes noch lange nicht abgeschlossen. Im Gegenteil handelt es sich vielmehr um ein Projekt, das sich fortlaufend weiterentwickelt. Der nächste Schritt sollte den Übergang vom speziellen digitalen Binnenmarkt hin zum Bestandteil des allgemeinen Europäischen Binnenmarktes darstellen.

Aus Sicht von eco fehlte vielen politischen Vorhaben und Projekten das Verständnis für digitale Technologien, ihre Möglichkeiten und Herausforderungen, aber auch ihre praktischen Grenzen. Die Diskussion um die fortschreitende Digitalisierung wird bedauerlicherweise mit einer technik- und internetskeptischen Grundhaltung geführt und ist geprägt von den Interessen etablierter Industrien. Hier ist ein Ungleichgewicht entstanden. Den involvierten Stellen in der Kommission, den Ausschüssen im Parlament sowie dem Rat bzw. den Ministerien in den EU-Mitgliedstaaten fehlte es zudem teilweise an einer gemeinsamen Idee bzw. einem gemeinsamen Ziel. Hier sieht eco für die Zukunft Optimierungspotenzial.

Aber auch in verschiedenen Detailbereichen sollte sich die EU weiterentwickeln. Einzelne Schwerpunkte, Aktions- und Handlungsfelder möchte eco nachfolgend aufzeigen.

19 Kernforderungen des eco zur Europawahl 2019

IT-Sicherheit, Staatliche Überwachung und Strafverfolgung

1 Die EU muss ein gesamteuropäisches Vorgehen im Kampf gegen Cybergefahren sicherstellen, nationale Alleingänge von Mitgliedstaaten verhindern und auch Bürger/-innen einbinden.

2 Die EU muss flächendeckende und anlasslose staatliche Überwachungsmaßnahmen der europäischen Bevölkerung in allen Mitgliedstaaten unterbinden sowie Verschlüsselung und sichere Dienste stärker fördern.

3 Die EU muss ein einheitliches Vorgehen bei der Strafverfolgung von Cyberkriminalität finden sowie gerechte Regeln und Standards – im Hinblick auf kleinste, kleine und mittlere Unternehmen – für den grenzüberschreitenden Datenzugriff im Rahmen von Ermittlungsverfahren definieren.

Datenschutz und Privatsphäre Online

4 Die EU muss sicherstellen, dass die Mitgliedstaaten die Datenschutzgrundverordnung einheitlich sowie konsistent umsetzen und anwenden.

5 Der europäische Datenschutzausschuss muss die Internetwirtschaft stärker in seine Arbeit einbeziehen.

6 EU-Kommission und -Parlament müssen die Pläne zur E-Privacy-Verordnung in einem offenen Dialog mit der Wirtschaft diskutieren, um eine Fragmentierung des europäischen Datenschutzrahmens zu vermeiden.

7 Die EU-Mitgliedstaaten müssen sich klar gegen eine anlasslose Vorratsdatenspeicherung aussprechen.

Rechtsverletzungen und Haftung im Internet

8 Die EU darf den soliden und erprobten Rechtsrahmen für die Bereitstellung digitaler Dienste in Europa nicht durch inkonsistente Änderungen der E-Commerce-Richtlinie und des „Notice and Action"-Prinzips weiter aufweichen.

Fortsetzung 19 Kernforderungen des eco zur Europawahl 2019

Rechtsverletzungen und Haftung im Internet

9 Die EU muss einen kooperativen und gesamtgesellschaftlichen Ansatz zum Umgang mit Hate Speech und Fake News entwickeln, der Wirtschaft und Bevölkerung einbezieht und nicht allein auf technische Lösungen setzt.

10 Die EU muss zur Bekämpfung von Online-Kriminalität die Strafverfolgung sowie die Arbeit weltweit vernetzter Hotlines stärken und ausbauen.

11 EU-Kommission und -Parlament müssen ein modernes europäisches Urheberrecht entwickeln, das die berechtigten Interessen der Urheber/-innen, der Verwerter/-innen, der Internetwirtschaft sowie der Nutzer/-innen miteinander in Einklang bringt.

Infrastruktur und Netze

12 Die EU muss eine konsistente Strategie – auch bei Forschung, Aus- und Weiterbildung sowie bei Energiekosten – zur Sicherstellung digitaler Souveränität auf Basis leistungsfähiger digitaler Infrastrukturen entwickeln.

13 Die EU muss ihren ausgewogenen Regulierungsansatz zur Wahrung des freien Internets und der Innovationsfreundlichkeit beibehalten und weiterentwickeln.

Dienste und Wettbewerb

14 Die EU muss im Zuge der Medienkonvergenz einen konsistenten Regulierungsrahmen schaffen, der gleichartige Angebote auch den gleichen Regelungen unterwirft.

15 Die EU muss protektionistischen Bestrebungen, die eine Benachteiligung digitaler Dienste und Geschäftsmodelle darstellen, sowohl in einzelnen Mitgliedstaaten als auch auf europäischer Ebene entschieden entgegentreten.

16 Die EU muss Start-ups sowie kleine und mittlere Unternehmen bei Legislativvorschlägen stärker berücksichtigen und angemessene sowie gleichwertige Markt- und Wettbewerbsverhältnisse schaffen.

Digitale Wirtschaft und Digitalisierung

17 Der Europäische Rat sollte von seinen Plänen für eine Digitalsteuer Abstand nehmen und sich stattdessen für ein einheitliches Besteuerungssystem einsetzen, das alle Unternehmen nach denselben Maßgaben besteuert.

18 Die EU-Mitgliedstaaten müssen virtuelle Binnengrenzen abschaffen und Datenfreizügigkeit innerhalb der EU gewährleisten.

19 Die EU muss eine einheitliche europäische Strategie für die Stärkung der Entwicklung und des Einsatzes von Künstlicher Intelligenz und Blockchain-Technologien erarbeiten.

IT-Sicherheit, Staatliche Überwachung und Strafverfolgung

1 Die EU muss ein gesamteuropäisches Vorgehen im Kampf gegen Cybergefahren sicherstellen, nationale Alleingänge von Mitgliedstaaten verhindern und auch Bürger/-innen einbinden.

Mit der zunehmenden Vernetzung und Digitalisierung verändern sich die Bedrohungen für Unternehmen, Staaten und Bürger/-innen. Neben herkömmlichen Kriminellen werden auch immer häufiger Staaten oder deren Proxies als Urheber von Angriffen ausgemacht. Dieser zunehmenden Gefahr und diesen Herausforderungen müssen nicht nur Bürger/-innen, Unternehmen und Mitgliedstaaten gerecht werden; auch die EU steht hier in einer besonderen Verantwortung und muss Mitgliedstaaten zielgerichtet unterstützen. Ihre zentrale Aufgabe beim Schutz der Grundrechte darf sie dabei jedoch nicht außer Acht lassen.

Die Zusammenarbeit von europäischen Sicherheitsinstitutionen wie ENISA und Europol mit der Internetwirtschaft muss weiter intensiviert werden, um Herausforderungen effizient und effektiv zu begegnen. Grundrechte, Gefahrenabwehr und wirtschaftliche Handhabbarkeit müssen in Einklang gebracht werden. Für die Abwehr gemeinsamer Gefahren und Bedrohungen gilt es, überschießende Regelungen und vorschnelle Maßnahmen bei der Regulierung zu vermeiden. Zudem sind ausreichende operative Kapazitäten bei den EU- Behörden sowie bei den Strafverfolgungsbehörden in den Mitgliedstaaten bereitzustellen. IT-Sicherheit muss als gemeinsame Herausforderung verstanden werden, die Regierungsinstitutionen, Unternehmen und Anwender/-innen zusammen verantwortungsvoll und effizient adressieren können.

Ein zentraler Baustein für die Abwehr von Gefahren im Internet- und Technologiebereich ist der Rechtsakt zur Cybersicherheit. Mit ihm soll das Mandat für die europäische IT-Sicherheitsagentur ENISA perpetuiert werden – ein wichtiger Schritt für die IT-Sicherheit, den eco befürwortet. Zentrale erste Aufgabe von ENISA sollte die Koordination und Überprüfung der konsequenten und stringenten Umsetzung der NIS-Richtlinie in allen EU-Mitgliedstaaten sein. Die Handreichungen der EU-Kommission stellen hierfür eine sinnvolle Grundlage und einen Ausgangspunkt dar.

Eine Herausforderung wird der durch den Cybersicherheits-Rechtsakt vorgesehene Zertifizierungsrahmen bleiben, der auf der einen Seite transparente und nachvollziehbare Sicherheitsanforderungen definiert, auf der anderen Seite aber den speziellen Anforderungen der modernen Informationstechnologie und der offenen Plattformen sowie einer möglichst flächendeckenden Umsetzung Rechnung tragen muss. Dieser Spagat zwischen nötiger Abstraktheit und konkretem Sicherheitsbedarf kann bspw. durch Standardisierungsprozesse und nur in Zusammenarbeit mit der Internetwirtschaft bewältigt werden.

Seitens der EU und der ENISA ist dafür Sorge zu tragen, dass nationale Alleingänge der Mitgliedstaaten vermieden werden und ein notwendiges gesamteuropäisches Vorgehen stattfindet. Widrigenfalls wird dies negative Konsequenzen für den europäischen (digitalen) Binnenmarkt als Ganzes sowie für individuelle Mitgliedstaaten und deren Unternehmen haben.

2 Die EU muss flächendeckende und anlasslose staatliche Überwachungsmaßnahmen der europäischen Bevölkerung in allen Mitgliedstaaten unterbinden sowie Verschlüsselung und sichere Dienste stärker fördern.

Einen Beitrag zur Verbesserung der Sicherheit in Netzwerken müssen aber nicht nur Unternehmen und europäische Behörden leisten. Auch die EU-Mitgliedstaaten müssen ihre Bestrebungen, eingebaute Hintertüren für Behörden oder zentrale Verschlüsselungssysteme mit „Generalschlüssel" für Ermittlungsbehörden zu fordern, kritisch hinterfragen. Die Sammlung und Geheimhaltung von Schwachstellen in Diensten, Produkten und Geräten (sog. Zero Day Exploits) sind der allgemeinen Verbesserung der IT-Sicherheit nicht zuträglich. Entsprechende Maßnahmen untergraben zudem das Vertrauen der Nutzer/-innen in Dienste und Produkte sowie in die Nutzung des Internet generell.

Auch sind flächendeckende und anlasslose staatliche Maßnahmen zur Überwachung der europäischen Bevölkerung, wie die immer wiederkehrende Vorratsdatenspeicherung, in allen Mitgliedstaaten zu unterbinden. Der EuGH hat hier eine klare Rechtsprechung vorgelegt. Ein Bekenntnis zu dieser Rechtslage muss seitens des EU-Parlaments und der EU-Kommission flankierend erbracht werden.

Der Reputationsverlust, der durch die beschriebenen Maßnahmen, deren Mehrwert für tatsächliche Polizeiarbeit und Ermittlungen zumindest als fragwürdig eingestuft werden kann, ist für die Internetwirtschaft nicht hinnehmbar.

Ein Bekenntnis zu starker Verschlüsselung, die Förderung der Entwicklung und Nutzung von einfach anzuwendender Verschlüsselung und der explizite Verzicht auf jegliche Form der Schwächung bzw. Untergrabung von Verschlüsselungsverfahren stärkt das allgemeine Vertrauen in Netze und Dienste, fördert das Vertrauen in die Digitalisierung und stärkt Europa als digitalen Binnenmarkt.

Fortsetzung IT-Sicherheit, Staatliche Überwachung und Strafverfolgung

Datenschutz und Privatsphäre Online

3 Die EU muss ein einheitliches Vorgehen bei der Strafverfolgung von Cyberkriminalität finden sowie gerechte Regeln und Standards – im Hinblick auf kleinste, kleine und mittlere Unternehmen – für den grenzüberschreitenden Datenzugriff im Rahmen von Ermittlungsverfahren definieren.

Eine zunehmend vernetzte Welt bringt bedauerlicherweise auch Cyberkriminalität in verschiedensten Ausprägungen und Formen hervor, die auch die Strafverfolgungsbehörden in den Mitgliedstaaten vor Herausforderungen stellt. Hier gilt es, innerhalb der EU ein gemeinsames Vorgehen zu finden sowie Regeln und Standards für einen raschen grenzüberschreitenden Datenzugriff für die Ermittlung und Verfolgung von Cyberkriminalität zu etablieren und zu gewährleisten.

Die EU hat – nach der 2014 verabschiedeten Europäischen Ermittlungsanordnung – mit der E-Evidence-Verordnung bereits nach sehr kurzer Zeit einen neuen, zusätzlichen Vorschlag präsentiert. In diesem Bereich gilt es, die teilweise hohen Schutz- und Sicherheitsstandards einzelner Mitgliedstaaten zu erhalten bzw. sie EU-weit an dieses hohe Niveau anzupassen und zu übernehmen. Darüber hinaus gilt es, die Missbrauchsgefahr zu minimieren und die Haftungsrisiken für Internetdiensteanbieter zu eliminieren.

Eine höhere Effizienz beim Datenaustausch mit der Strafverfolgung ist generell zu begrüßen, darf aber – insbesondere mit unrealistischen Reaktionszeiten und impraktikablen Verifikationsmaßnahmen – nicht zu Lasten von KMU oder betroffenen Bürgerinnen und Bürger gehen. Dabei darf die Wahrnehmung und Verantwortung hoheitlicher Aufgaben nicht auf die Privatwirtschaft abgewälzt werden.

4 Die EU muss sicherstellen, dass die Mitgliedstaaten die Datenschutzgrundverordnung einheitlich sowie konsistent umsetzen und anwenden.

Mit der Datenschutzgrundverordnung (DSGVO) wurde die Basis für einen einheitlichen Datenschutz in Europa geschaffen. Ihre Grundprinzipien und Maßgaben gelten nun in allen EU-Mitgliedstaaten. Der institutionelle Rahmen, der mit der DSGVO geschaffen werden soll, beginnt mit der Einsetzung des Europäischen Datenschutzausschusses ebenfalls konkret Gestalt anzunehmen.

Jetzt gilt es, bei der EU-weiten Implementierung der DSGVO darauf zu achten, dass diese konsistent und im Sinne der Verordnung erfolgt.

5 Der europäische Datenschutzausschuss muss die Internetwirtschaft stärker in seine Arbeit einbeziehen.

Die bisherigen Beschlüsse der Artikel-29-Datenschutzgruppe (welche infolge der DSGVO im Europäischen Datenschutzausschuss aufging) lassen jedoch Zweifel an einer systematischen und zweckmäßigen Umsetzung aufkommen, wenn nebensächliche Themen (wie bspw. die Übertragung von Playlists von Musikdiensten) in den Fokus rücken.

Daher fordert eco eine zielgerichtete Strukturierung der Arbeit des Europäischen Datenschutzausschusses und die stärkere Einbeziehung der Kompetenz der Internetwirtschaft. Dadurch soll auch eine erhebliche Beschleunigung der notwendigen praktischen Konkretisierung zur Anwendung der DSGVO erreicht werden.

Darüber hinaus gilt es anzuerkennen, dass das Internet nicht vor Landesgrenzen haltmacht und z. B. die konsistente Umsetzung und Anwendung der DSGVO eine Herausforderung für Webseitenbetreiber in der ganzen Welt darstellen kann.

Die Reaktion zahlreicher amerikanischer Nachrichtenanbieter – nämlich die Unterbindung europäischer Zugriffe auf deren Webseiten – ist wohl das prominenteste Beispiel der weltweiten Auswirkungen der DSGVO und bedeutet für Nutzer/-innen aus der EU eine Einschränkung der Informationsmöglichkeiten.

Solchen Entwicklungen sollte durch proaktive Maßnahmen seitens der EU, wie z. B. einen Dialog mit Webseitenbetreibern in Drittstaaten für ein besseres Verständnis und eine einfachere Umsetzung der neuen Vorgaben, entgegengetreten werden.

Auf der anderen Seite bietet das EU-US Privacy Shield aus Sicht von eco eine Grundlage für die Ausgestaltung von Datenverkehr mit Drittstaaten. Entsprechende Vereinbarungen oder die Anerkennung von Adäquanz im Datenschutz müssen aber auch mit Großbritannien und anderen Regionen der Welt erfolgen.

Fortsetzung Datenschutz und Privatsphäre Online

6 EU-Kommission und -Parlament müssen die Pläne zur E-Privacy-Verordnung in einem offenen Dialog mit der Wirtschaft diskutieren, um eine Fragmentierung des europäischen Datenschutzrahmens zu vermeiden.

Wenn es nach den Plänen von EU-Kommission und -Parlament geht, ist die Regulierung des Datenschutzes im Netz mit der DSGVO noch nicht abgeschlossen. Mit der E-Privacy-Verordnung ist ein weiter Legislativakt in Arbeit. Dieser könnte weitreichende Auswirkungen auf die Netze und Dienste und im Weiteren auch auf digitale Geschäftsmodelle in Europa haben.

Nachdem bereits die DSGVO für Einschnitte bei Webseitenbetreibern und digitalen Diensten gesorgt hat, ist mit einer erneuten Verschärfung der Datenschutzvorschriften über dieses allgemeine Maß hinaus eine Benachteiligung des europäischen Standortes zu erwarten. Von einer solchen Regulierung würden letzten Endes Produkte und Dienste profitieren, die vor allem außerhalb Europas Nutzerdaten generieren und verarbeiten sowie basierend darauf ihre Geschäftsmodelle entwickeln.

Mit den inkonsistenten Anforderungen und Vorgaben der E-Privacy-Verordnung würde eine Stärkung des europäischen Digitalstandortes hingegen untergraben und durch unklare Begriffsdefinitionen die Problematik der Akzeptanz und Umsetzung europäischer Datenschutzinitiativen verschärft werden.

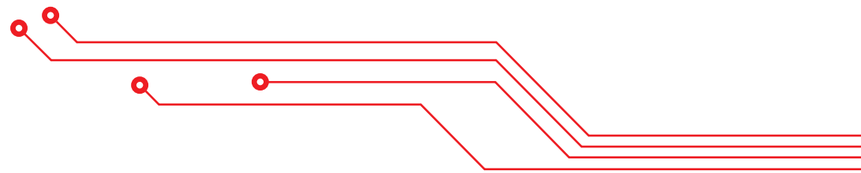
Die E-Privacy-Verordnung sollte in einem offenen Dialog mit Politik und Wirtschaft diskutiert werden, der ein europäisches Verständnis der Zielrichtung und potenzieller Probleme ermöglicht.

7 Die EU-Mitgliedstaaten müssen sich klar gegen eine anlasslose Vorratsdatenspeicherung aussprechen.

Eine vom EuGH untersagte anlasslose Vorratsdatenspeicherung ist Nutzerinnen und Nutzern nur schwer zu erklären und wird von eco nicht nur deshalb grundsätzlich abgelehnt. In Deutschland haben die betroffenen Unternehmen der Internet- und Telekommunikationsbranche bedauerlicherweise nun bereits zwei Mal erheblichen Aufwand betrieben und entsprechende personelle und finanzielle Mittel zur Umsetzung der rechtswidrigen Vorratsdatenspeicherung aufgewendet. Deren Nutzen konnte bisher weder belegt werden, noch wurden Anstrengungen unternommen, einen Nutzen empirisch zu belegen.

Die für eine Vorratsdatenspeicherung notwendigen technischen Vorkehrungen sowie der administrative und personelle Aufwand belasten die betroffenen Unternehmen massiv. Sie stellt Eingriffe sowohl in deren Grundrechte als auch in die der betroffenen Nutzer/-innen dar.

In der Konsequenz fehlen insbesondere den KMU die finanziellen Mittel, welche zur Umsetzung der Vorratsdatenspeicherung erforderlich sind, für die Entwicklung innovativer Telekommunikationsdienste sowie für den Auf- und Ausbau hochleistungsfähiger Telekommunikationsnetze und Gigabitinfrastrukturen. Zudem führen solche Gesetzesvorhaben, die vor dem EuGH wie auch vor den nationalen Gerichten angegriffen werden und keinen Bestand haben, dazu, dass es betroffenen Unternehmen an der absolut notwendigen Investitions-, Planungs- und Rechtssicherheit mangelt.



Rechtsverletzungen und Haftung im Internet

8 **Die EU darf den soliden und erprobten Rechtsrahmen für die Bereitstellung digitaler Dienste in Europa nicht durch inkonsistente Änderungen der E-Commerce-Richtlinie und des „Notice and Action"-Prinzips weiter aufweichen.**

Die E-Commerce-Richtlinie (EC-RL) war und ist seit nunmehr fast 20 Jahren einer der zentralen Eckpfeiler für die Bereitstellung digitaler Dienste in Europa und die Basis nationaler gesetzlicher Regelungen. Sie ermöglichte damit die Entstehung des Internets und seiner zahlreichen Dienste in der Form, wie wir sie heute kennen. Damals einigte man sich auf Pflichten und Haftungsregeln für Internetdiensteanbieter. Mit dem Providerprivileg wurde dabei sichergestellt, dass Inhalte einer nachträglichen Kontrolle unterliegen und Internetdiensteanbieter bei fehlender Konsequenz für Rechtsverletzungen Dritter unmittelbar haftbar werden können („Notice and Action" bzw. „Safe Harbour").

Die im Internet angebotenen Dienste und die Nutzungsgewohnheiten haben sich seither verändert und nicht zuletzt deshalb wurden verstärkt Rufe nach einer Änderung der EC-RL und des „Notice and Action"-Prinzips laut. Mit Verhaltenskodizes wurden große Anbieter zunächst in die Pflicht genommen, aktiver gegen unerwünschte Inhalte vorzugehen. Maßnahmen in den beiden Themenbereichen Kindesmissbrauchsdarstellungen (sog. CSAM) sowie terroristische Inhalte senkten dabei die Hemmschwelle für weitere Schritte und die Ausweitung von Maßnahmen (bspw. Einsatz von Filter- und KI-Technologien) auf andere Inhalte.

In dieser Tendenz zu technologischen Lösungsansätzen sieht eco eine bedenkliche Entwicklung. Deren Fehleranfälligkeit und technische Grenzen bedeuten eine Gefährdung der Grundrechte von Nutzerinnen und Nutzern sowie Unternehmen (insbesondere freie Meinungsäußerung und unternehmerische Freiheit). Außerordentlich schwer wiegt, dass sich Maßnahmen oft an den Gegebenheiten der größten Martktteilnehmer orientieren und KMU sowie (die gewünschten europäischen) Start-ups außen vor gelassen werden. Diese Entwicklung ist vor allem deshalb problematisch, da der Großteil der europäischen IKT-Unternehmen mittelständische Unternehmen sind.

9 **Die EU muss einen kooperativen und gesamtgesellschaftlichen Ansatz zum Umgang mit Hate Speech und Fake News entwickeln, der Wirtschaft und Bevölkerung einbezieht und nicht allein auf technische Lösungen setzt.**

Im Laufe der Zeit haben sich im Internet Plattformen und Dienste herausgebildet, die nicht nur große Bekanntheit erlangten, sondern auch tagtäglich vom Großteil der Internetnutzer/-innen in Anspruch genommen werden – allen voran soziale Medien wie Facebook, Twitter, LinkedIn oder Instagram. Nutzer/-innen teilen dort (persönliche) Informationen und Unternehmen (z. B. Medienunternehmen) nutzen diese Plattformen, um auf ihre Inhalte und Artikel hinzuweisen oder diese dort direkt verfügbar zu machen.

Infolge der letzten US-Präsidentschaftswahlen erlangten bedauerlicherweise vermeintlich neue Phänomene wie Filterblasen und Fake News eine prominente Rolle. Ein weiterer Begriff dieser Kategorie ist Hate Speech, welche insbesondere eine Folge der Flüchtlingsbewegungen 2015/16 war. Doch keines dieser Phänomene ist gänzlich neu. Allein der digitale Verbreitungsweg ist in der heutigen Zeit einfacher zu nutzen und ist eine kostengünstige und unkomplizierte Möglichkeit zur raschen, breiten Streuung bzw. zu anonymen Angriffen oder solchen unter Verwendung eines Pseudonyms.

Diesen Entwicklungen darf jedoch nicht mit unbedachten Maßnahmen begegnet werden. Die Lösung kann nur über eine Kooperation der betroffenen Gruppen – Bürger/-innen, Unternehmen, Staat – erreicht werden. Es wäre illusorisch zu glauben, dass Technik allein diese gesamtgesellschaftlichen Herausforderungen meistern könnte.

10 **Die EU muss zur Bekämpfung von Online-Kriminalität die Strafverfolgung sowie die Arbeit weltweit vernetzter Hotlines stärken und ausbauen.**

Eine ähnliche Entwicklung – hin zu mehr technologischen Ansätzen und Automatisierung – zeigt sich auch bei der Bekämpfung der Verbreitung von Terrorismus- und Kindesmissbrauchsmaterial im Internet. Dabei gilt es jedoch zu beachten, dass es sich sowohl in der Art als auch bezüglich der Schwere von Straftaten in diesen Gebieten um eine Besonderheit handelt. Denn es herrscht weltweit eine vergleichsweise einheitliche Rechtslage vor und die einschlägigen Inhalte sind relativ eindeutig zu identifizieren. Eine entsprechende technische Unterstützung kann hier – in diesem begrenzten Anwendungsbereich und in einem gewissen Ausmaß – gegebenenfalls sinnvoll sein.

Doch auch hier können technologische Ansätze allein nichts verhindern. Viel mehr Erfolg verspricht die Arbeit von spezialisierten und weltweit vernetzten Hotlines sowie Kooperationen mit Internet Service Providern. Dabei darf nicht außer Acht gelassen werden, dass eine konsequente Ermittlung der Täter und eine Strafverfolgung für die Bekämpfung und Verfolgung der Verbreitung von Terrorismus- und Kindesmissbrauchsmaterial im Internet elementar sind.

eco fordert eine konsequente Unterstützung dieses international erfolgreichen und kooperativen Modells. Sein Erfolg wird durch die hohen Löschquoten bestätigt und zeigt, dass es auch zukünftig in seiner Form fortbestehen muss, damit der Kampf gegen diese illegalen Inhalte auch weiterhin erfolgreich sein kann.

Fortsetzung Rechtsverletzungen und Haftung im Internet

11 EU-Kommission und -Parlament müssen ein modernes europäisches Urheberrecht entwickeln, das die berechtigten Interessen der Urheber/-innen, der Verwerter/-innen, der Internetwirtschaft sowie der Nutzer/-innen miteinander in Einklang bringt.

Moderne Technologien und vor allem das Internet haben die Verbreitung digitaler Inhalte in Form von Nachrichten und Texten, Bildern und Fotos, Musik, Videos etc. so einfach, kostengünstig und schnell wie nie zuvor gemacht. Dies brachte viele Vorteile mit sich. Journalistinnen und Journalisten sowie Bloggerinnen und Blogger fanden einen direkteren Zugang zu Leserinnen und Leser; junge Künstlerinnen und Künstler konnten einfacher ins Rampenlicht treten und vom YouTube- zum internationalen Popstar werden; „YouTube-Nutzer/-in" und „Instagram-Influencer/-in" wurden Berufsbezeichnungen. Was mit dieser Entwicklung nicht Schritt gehalten hat und sich kaum weiterentwickelt hat, ist jedoch das Urheberrecht.

Das Internet bietet europäischen Unternehmen und Nutzerinnen und Nutzer viel Potenzial, das es auszuschöpfen gilt. Dabei dürfen Künstlerinnen und Künstler, Autorinnen und Autoren, Journalistinnen und Journalisten etc. jedoch nicht außen vor bleiben. Ein modernes Urheberrecht sollte die Bereitstellung digitaler Inhalte und deren angemessene Vergütung sowie eine unkomplizierte Anwendung nicht gegeneinander ausspielen. Dabei muss auch der Schutz von Grundrechten einbezogen werden und die technischen Möglichkeiten sind zu beachten. Zu einem modernen Urheberrecht gehört zwingend auch die technologieneutrale Ausgestaltung von Rechten und Pflichten.

eco unterstützt die Aufbruchsstimmung in diesem Rechtsgebiet, fordert aber dazu auf, gemeinsam zeitgemäße Regelungen zu finden, um die berechtigten Interessen der Urheber/-innen, der Verwerter/-innen, der Internetwirtschaft sowie der Nutzer/-innen miteinander in Einklang zu bringen und die Potenziale der Digitalisierung auszuschöpfen.

Der aktuelle Stand der Diskussion und die vorgelegten Entwürfe für die Novellierung des Urheberrechts sind für die Internetwirtschaft unbefriedigend und werden sich innovationshemmend auswirken. Urheberrecht darf nicht zum Schutz althergebrachter Geschäftsmodelle instrumentalisiert werden und neue Geschäftsmodelle einseitig und unausgewogen benachteiligen.

Infrastruktur und Netze

12 Die EU muss eine konsistente Strategie – auch bei Forschung, Aus- und Weiterbildung sowie bei Energiekosten – zur Sicherstellung digitaler Souveränität auf Basis leistungsfähiger digitaler Infrastrukturen entwickeln.

Für die weitere Digitalisierung und die Wettbewerbsfähigkeit des europäischen Standortes ist die europaweite Verfügbarkeit hochleistungsfähiger Gigabitnetze, gigabitfähiger Anschlüsse sowie modernster Mobilfunknetze notwendig. Zu einem funktionierenden Ökosystem digitaler Infrastrukturen gehören auch Rechenzentren, Co-Location-Anbieter und Cloudinfrastrukturanbieter sowie zuverlässige und performante Internet-Austauschknoten.

Nach Angaben der EU-Kommission werden nur sechs Prozent der weltweit verfügbaren Daten in Europa physisch in Rechenzentren gespeichert (gehostet). Daher ist eine strategische Betrachtung dieses Teilsegments digitaler Infrastrukturen als Rückgrat der Digitalisierung maßgebend für das Gelingen europäischer digitaler Leistungsfähigkeit und digitaler Souveränität.

Aus Sicht von eco bedarf es einer konsistenten Strategie, die u. a. die Forschung und deren Förderung in diesem Bereich, Aus- und Weiterbildung sowie nicht zuletzt eine wettbewerbsfördernde Gestaltung der Energiekosten umfassen muss. Da die Themen und Zuständigkeiten bei unterschiedlichen staatlichen Institutionen liegen, ist ein interdisziplinärer und ressortübergreifender Ansatz notwendig.

Im Hinblick auf den Ausbau von Hochgeschwindigkeitsnetzen ist bei der notwendigen Anpassung der Beihilferegelungen darauf zu achten, dass die bisherige Schwelle von 30 Mbit/s deutlich angehoben wird. Dies ist nicht zuletzt deshalb notwendig, weil damit die Ziele der Gigabitstrategie 2025 der EU-Kommission erreicht werden können.

eco ist überzeugt, dass der Ausbau vorrangig privatwirtschaftlich erfolgen soll und dass eine wettbewerbsverzerrende Wirkung von Beihilfen verhindert werden muss. Unter den Gesichtspunkten der sozialen Teilhabe, der Forschung, der Wirtschaft im Allgemeinen und der Internetwirtschaft im Besonderen sollte dafür Sorge getragen werden, dass schnellstmöglich alle weißen und später auch grauen Flecken gigabitfähig erschlossen werden.

Die damit einhergehenden positiven Effekte für die Volkswirtschaft, die Gesellschaft und den Staat liegen auf der Hand. Insbesondere die Internetwirtschaft wird davon profitieren und kann ihren Kundinnen und Kunden dadurch Dienste effizienter anbieten. In diesem Sinne kann man die europäischen Institutionen nur dazu ermutigen, solche Initiativen aufzunehmen, die zur Verwirklichung des digitalen Binnenmarktes beitragen und mit dem privaten Wettbewerb in Einklang stehen.

Fortsetzung Infrastruktur und Netze

13 Die EU muss ihren ausgewogenen Regulierungsansatz zur Wahrung des freien Internets und der Innovationsfreundlichkeit beibehalten und weiterentwickeln.

Das Internet ermöglicht ein digitales Ökosystem, das sich durch einen niedrigschwelligen Marktzugang, geringe Marktzutrittskosten sowie Skalierungseffekte auszeichnet. Es ermöglicht damit die Bereitstellung innovativer neuer Dienste und Geschäftsmodelle gerade auch durch kleinere und noch unbekannte Unternehmen sowie Start-ups.

eco erachtet das Prinzip der Netzneutralität als einen wertvollen Baustein für die Internetwirtschaft und deren Verankerung in der Telekom-Binnenmarkt-Verordnung und die Konkretisierungen durch GEREK als einen wichtigen Schritt. In der Anwendung zeigt sich, dass die nationalen Regulierungsbehörden geeignete Instrumente an die Hand bekommen haben, die sie überwiegend maßvoll anwenden. Dadurch werden Interessen von Internetzugangs-, Inhalte- und Applikationsanbietern sowie Endnutzerinnen und Endnutzer in Ausgleich gebracht.

Für die Zukunft gilt es, diese Ausgewogenheit zu bewahren und weiterzuentwickeln, bspw. beim Mobilfunkstandard 5G, um dadurch einerseits Innovationen zu fördern und andererseits ein freies Internet zu erhalten. Aus Sicht von eco ist die Kodifizierung der Netzneutralität nicht zuletzt auch ein Wettbewerbsvorteil für Europa im internationalen Vergleich.

Dienste und Wettbewerb

14 Die EU muss im Zuge der Medienkonvergenz einen konsistenten Regulierungsrahmen schaffen, der gleichartige Angebote auch den gleichen Regelungen unterwirft.

Die Audiovisuelle-Mediendienste(AVMD)-Richtlinie ist maßgebend für die regulatorische Behandlung verschiedener Medienarten im Zeitalter zunehmend konvergierender Medienformen. Sie unterscheidet dafür auch in ihrer aktualisierten Fassung weiterhin anhand des technischen Merkmals der Linearität (klassische TV- und Rundfunkangebote) bzw. Nichtlinearität (Online-Angebote wie Videoportale oder sog. Video-on-Demand-Dienste). Dies führt in der praktischen Umsetzung der Richtlinie in den Mitgliedstaaten (z. B. in Deutschland) dazu, dass versucht wird, die Vorstellungen der Rundfunkregulierung auf das Internet zu übertragen. Dies ist jedoch nicht im Sinne einer Modernisierung des Rechtsrahmens. Das Internet ist sowohl technisch als auch durch seine verschiedenen Zugangsformen grundsätzlich vom Rundfunk zu unterscheiden.

Im Zuge der Medienkonvergenz – die es ermöglicht, das TV- und Rundfunkprogramm linear im Internet zu übertragen oder es dort auch nichtlinear in einer Mediathek oder einem Katalog auf Abruf bereitzuhalten – erachtet eco das technische Merkmal der Linearität nicht mehr als sinnvolles Unterscheidungskriterium für eine Regulierung. Ziel sollte vielmehr sein, einen konsistenten und vergleichbaren Regulierungsrahmen zu schaffen, der gleichartige Angebote auch den gleichen Regelungen unterwirft.

Unabhängig von der Art des Anbieters und der Übertragung oder der Nutzungspräferenz sollte für miteinander unmittelbar im Wettbewerb stehende Angebote ein gleichartiges Regulierungsniveau herrschen, um Wettbewerbsverzerrungen zu vermeiden. Dabei sind auch die Möglichkeiten zur Rechtsdurchsetzung zu beachten und die Deregulierung ist – wo immer möglich – einer nicht effektiv durchsetzbaren Regulierung vorzuziehen.

Vorrangig ist auch generell zu überprüfen, wo und wie eine Deregulierung möglich ist. So sind nach der deutschen Rundfunkregulierung vor allem Plattformen und Plattformanbieter einem strengen Regelungsrahmen unterworfen, der insgesamt zu weitgehend und detailliert erscheint. Auch in der AVMD-Richtlinie sollte in Zukunft darauf geachtet werden, dass sie keine zu engen Vorgaben hinsichtlich der Ausgestaltung von Plattformen und Benutzeroberflächen macht, damit die Verfügbarkeit und die Bereitstellung neuer Dienste sowie die Angebote und der Wettbewerb im europäischen Binnenmarkt weiter gefördert werden.

Neue Produkte und Dienste – z. B. smarte Lautsprecher und Fernseher oder das Internet of Things, Künstliche Intelligenz, Blockchain bzw. Distributed Ledger oder Big Data – ermöglichen nicht nur einen Paradigmenwechsel in der Interaktion zwischen Menschen und Internettechnologien, sondern bieten auch Potenziale

Fortsetzung Dienste und Wettbewerb

für technologische Entwicklungen und Unternehmen. Gerade der zukünftigen Anwendung von Künstlicher Intelligenz wird eine umfangreiche Querschnittsfunktion im Bereich der Digitalisierung und der Neuausrichtung von Industrie- und Dienstleistungsprozessen zukommen und dies wird innovative Geschäftsmodelle ermöglichen. Gleichzeitig wächst die Sorge um die Anforderungen an diese Produkte.

Sicherheitsbedenken spielen hier ebenso eine Rolle wie Fragen nach Produktgestaltung und -anforderungen. Sinnvolle Grundsätze müssen bewahrt werden. Gleichzeitig bedarf es einer profunden Analyse zusätzlich sinnvoller Regeln und der Frage, inwieweit diese Regeln auch digitalen Vertriebskanälen und Geschäftsmodellen Rechnung tragen. Die Digitalisierung darf nicht als Vorwand dienen, die Geschäftsmodelle und Abschöpfungsmechanismen etablierter Wirtschaftszweige durch fehlgeleitete Regulierung zu zementieren.

15 Die EU muss protektionistischen Bestrebungen, die eine Benachteiligung digitaler Dienste und Geschäftsmodelle darstellen, sowohl in einzelnen Mitgliedstaaten als auch auf europäischer Ebene entschieden entgegentreten.

Die Internetwirtschaft und die Digitalisierung werden gerne als „disruptiv" bezeichnet, da sie mit innovativen Diensten und Angeboten den Markt der eingesessenen Unternehmen aufwirbeln. Dabei wird teilweise versucht, die Dienste (wie bspw. bei den AVMD) in bestehende Formen zu zwängen, ohne auf die Eigenheiten zu achten, die neue Technologien mit sich bringen. Auf der anderen Seite wird versucht, neue Maßstäbe an die Internetwirtschaft zu legen, um deren Vorteile aufzuwiegen und so einen Nachteil der „Old Economy" zu reduzieren (z. B. Digitalsteuer).

Die Internetwirtschaft selbst ist mit einer Vielzahl von verschiedenen Geschäftsfeldern und Produkten überaus heterogen. Deshalb ist eco der Auffassung, dass für sie keine Sonderregelungen im allgemeinen Wettbewerbsrecht geschaffen werden dürfen und etwaige Regelungen differenziert sein müssen, um der Heterogenität gerecht zu werden und dem Internet als Innovationsmotor der europäischen Wirtschaft den notwendigen Raum zu geben. Die teilweise sowohl in einzelnen Mitgliedstaaten als auch auf europäischer Ebene aufkommenden protektionistischen Bestrebungen stellen hingegen eine Benachteiligung digitaler Dienste und Geschäftsmodelle dar, hemmen und verzögern die Digitalisierung in Europa und stehen der Verwirklichung des digitalen Binnenmarktes entgegen.

16 Die EU muss Start-ups sowie kleine und mittlere Unternehmen bei Legislativvorschlägen stärker berücksichtigen und angemessene sowie gleichwertige Markt- und Wettbewerbsverhältnisse schaffen.

Ein weiteres Beispiel im Wettbewerbsrecht ist die Regulierung digitaler Plattformen im Zuge der Stärkung des digitalen Binnenmarktes, welche im Jahr 2018 zentraler Baustein der europäischen Politik geworden ist. Vor diesem Hintergrund ist die Vorstellung der sog. P2B-Verordnung (Verordnung zur Förderung von Transparenz und Fairness für gewerbliche Nutzer von Online-Vermittlungsdiensten) als ein weiterer Versuch zu sehen, digitalen Plattformen zusätzliche Pflichten aufzuerlegen.

Dabei sollte allerdings berücksichtigt werden, dass diese Regelungen nach dem derzeitigen Stand nicht nur marktmächtige Akteure, sondern auch kleinere Plattformen und KMU betreffen würden. Diese könnten durch die zusätzlichen Auflagen in ihrer Entwicklung maßgeblich gehemmt werden, was eine noch stärkere Konzentration bei den digitalen Plattformen zur Folge haben könnte.

eco fordert entsprechend das EU-Parlament und den Europäischen Rat auf, den Anwendungsbereich, die konkreten einzelnen Auflagen sowie die Adressaten im Verordnungsentwurf kritisch zu überprüfen. Darüber hinaus sollten auch die technische Machbarkeit der Auflagen und der Umstand berücksichtigt werden, dass hier eine Regelung zur Gestaltung von Geschäftsbeziehungen und keine Verbraucherschutzregelung geschaffen wird.

Digitale Wirtschaft und Digitalisierung

17 **Der Europäische Rat sollte von seinen Plänen für eine Digitalsteuer Abstand nehmen und sich stattdessen für ein einheitliches Besteuerungssystem einsetzen, das alle Unternehmen nach denselben Maßgaben besteuert.**

Der Rat der Europäischen Union hatte sich des Projekts einer Digitalsteuer angenommen, womit insbesondere Unternehmen, die ihre Umsätze nicht im Steuersitzland generieren, adressiert werden sollen. Eine solche Digitalsteuer ist jedoch schädlich für alle Unternehmen, die digital Waren oder Dienstleistungen anbieten, und diskriminiert diese gegenüber anderen (klassischen) Anbietern. Stattdessen sollten die bestehenden Besteuerungsmaßgaben grundsätzlich überprüft und in vernünftiger Art und Weise an eine vernetzte und globalisierte Wirtschaft angepasst werden. Dies würde eine einheitliche Besteuerung aller Unternehmen nach denselben Maßgaben und Grundsätzen bedeuten, sie gleichermaßen belasten, wodurch die Steuergerechtigkeit gewahrt würde – unabhängig von Geschäftsmodellen oder Vertriebskanälen. Besteuerungsmodelle, bei denen Sonderabgaben auf Online-Werbung (im Vergleich zu Print) bzw. auf online erworbene Software (im Vergleich zu Software auf Trägermedien) zu entrichten sind, bedeuteten hingegen einen nicht gerechtfertigten massiven Wettbewerbsnachteil für digitale Geschäftsmodelle und Internetunternehmen.

18 **Die EU-Mitgliedstaaten müssen virtuelle Binnengrenzen abschaffen und Datenfreizügigkeit innerhalb der EU gewährleisten.**

In einem vernetzten europäischen digitalen Binnenmarkt ist es essenziell, Marktzugangshürden und -hemmnisse abzubauen. Dazu zählen auch virtuelle Beschränkungen über die Lokalisation von Diensten und Daten. Innerhalb der EU sollte es möglich sein, Dienste – auch bei öffentlichen Aufträgen sowie bei der Nutzung von nicht personenbezogenen Daten aus der öffentlichen Verwaltung – grundsätzlich aus jedem Mitgliedstaat anbieten zu können. Spätestens seit dem Inkrafttreten der Datenschutzgrundverordnung und mit den flankierenden gesetzlichen Sicherheitsvorgaben ist es nicht mehr zu rechtfertigen, dass bspw. die physische Speicherung bzw. Verarbeitung oder Nutzung von Daten und Internetdiensten auf den jeweiligen Mitgliedstaat beschränkt werden.

Mit einer Datenfreizügigkeit wird Internetunternehmen z. B. ermöglicht, Standorte nach Kriterien wie Sicherheit und Effizienz sowie Verfügbarkeit auszuwählen und dieselben Dienste grenzüberschreitend anzubieten.

19 **Die EU muss eine einheitliche europäische Strategie für die Stärkung der Entwicklung und des Einsatzes von Künstlicher Intelligenz und Blockchain-Technologien erarbeiten.**

Die EU-Kommission hat im April 2018 ihren Vorschlag für eine Strategie für künstliche Intelligenz (KI) in Europa vorgelegt. Maßgeblicher Eckpfeiler dieser Strategie ist die Stärkung der Forschung. Daneben erhofft sich die Kommission eine Verbreiterung des Einsatzes von KI im Rahmen des digitalen Binnenmarktes. Beide Ansätze sind grundsätzlich begrüßenswert, bedürfen aber einer weiteren Konkretisierung. Insbesondere die wirtschaftstaugliche Anwendung von KI-Lösungen sollte auch von der EU stärker in den Fokus genommen werden.

Die Frage nach einem vereinfachten Zugang zu Daten für das Trainieren künstlicher Intelligenz ist dabei ein zentraler Eckpfeiler. Wichtig ist auch, dass die ambitionierten Ziele, welche die EU-Kommission mit 1,5 Mrd. Euro fördern möchte, nicht durch Regulierung an anderer Stelle konterkariert werden, wie es bspw. mit der E-Privacy-Verordnung passieren könnte.

Die Kommission hat die Beobachtungsstelle und das Forum der EU für die Blockchain-Technologie auf den Weg gebracht. Deren Ziel ist es, auf wichtige Entwicklungen der Blockchain-Technologie aufmerksam zu machen, europäische Akteure zu fördern und das europäische Zusammenwirken mit den verschiedenen an Blockchain-Aktivitäten beteiligten Interessenträgern zu intensivieren.

Die Blockchain-Technologie, bei der Informationspakete dezentral im Netz gespeichert werden, gilt als wichtiger Durchbruch, da sie bei Online-Geschäften ein hohes Maß an Rückverfolgbarkeit und Transparenz gewährleistet. Sie hat das Potenzial, digitale Dienstleistungen und Geschäftsmodelle in einer Vielzahl von Bereichen zu verändern (z. B. im Gesundheits-, Versicherungs- und Finanzwesen oder im Energiesektor, in der Logistik und im Rechtemanagement).

eco würde eine einheitliche europäische Strategie für die Stärkung des Einsatzes von KI sowie der Entwicklung und des Einsatzes von Blockchain-Technologien sehr begrüßen. In diesem Kontext sollte auch berücksichtigt werden, dass die Stärkung von auf KI oder entsprechenden Systemen basierenden digitalen Diensten und Produkten sowie die pauschale Regulierung von Algorithmen – insbesondere in Form einer Ex-ante-Regulierung, wie sie derzeit diskutiert wird – der gewünschten Stärkung wichtiger Zukunftstechnologien und Innovationen abträglich ist.

eco – Verband der Internetwirtschaft e.V.
Hauptstadtbüro
Französische Straße 48
10117 Berlin
Tel: 030 20 21 56 7-0
Fax: 030 20 21 56 7-11

E-Mail: berlin@eco.de

www.eco.de

Geschäftsführer: Harald A. Summa & Alexander Rabe