AmCham GERMANY

TIM Milestones 2018

Digitalisierung der Gesamtwirtschaft: Kernforderungen für den Innovationsstandort Deutschland

Empfehlungen des AmCham Germany Telecommunications, Internet, and Media (TIM) Committee für die Legislaturperiode 2017–2021

Februar 2018

Inhalt

Einleitung 4

1. Infrastrukturen für die Gigabit-Gesellschaft schaffen 5

2. Digitale Plattformen: Innovationspotenzial nutzen und Augenmaß bei der Regulierung walten lassen 6

3. Unklare Rechtslage der Providerhaftung beenden 8

4. Industrial Internet: Durch geeignete Rahmenbedingungen volles Potenzial heben 10

5. Intelligent mit künstlicher Intelligenz umgehen 11

6. Cybersicherheit durch klare und einheitliche europäische Regeln gewährleisten 12

7. Rahmenbedingungen für Ermittlungen im Cyberspace harmonisieren und modernisieren 14

8. Hürden für den Datenverkehr abbauen 15

9. Verbraucherschutz in der digitalen Welt sichern ohne Innovationen zu gefährden 16

10. Digitalisierung im Bildungsbereich 17

11. Arbeiten 4.0: Beschäftigung für eine digitale Zukunft sichern 18

Über das Telecommunications, Internet, and Media (TIM) Committee 20

Einleitung

Die Zukunft ist digital und die digitale Transformation der gesamten Wirtschaft mithin zentraler Faktor, um Deutschlands Position als führende Industrienation auch künftig zu sichern. Die Chancen, welche die Digitalisierung für den Standort Deutschland bietet, liegen auf der Hand. Um sie bestmöglich nutzen zu können, bedarf es der richtigen Weichenstellungen für den digitalen Wandel.

Mit der Digitalen Agenda 2014–2017 hat die Bundesregierung bereits Leitlinien zur Digitalpolitik vorgelegt. Eine der wichtigsten Aufgaben wird es auch in dieser Legislaturperiode sein, die digitale Transformation von Wirtschaft und Gesellschaft mitzugestalten und voranzutreiben.

Dazu möchte die American Chamber of Commerce in Germany e. V. (AmCham Germany) einen Betrag leisten und hat mit den „TIM Milestones 2018" [1] Empfehlungen zu elf Themenbereichen – von Infrastrukturen für die Gigabit-Gesellschaft über Bildung, die Zukunft der Arbeit bis zum Verbraucherschutz in der digitalen Welt – erarbeitet.

Ob es das Potenzial von Plattformen, künstlicher Intelligenz oder industriellem Internet zu nutzen gilt, gemeinsam ist den jeweiligen Rahmenbedingungen, dass sie innovationsoffen sein müssen. Um auch künftig weiter gesamtgesellschaftlich bedeutsame Innovationen zu stimulieren, muss der Rechtsrahmen Impulse für eine positive wirtschaftliche Entwicklung der Anbieter von Infrastrukturen, Inhalten und Dienstleistungen setzen und darf deren Handlungsspielraum nicht unverhältnismäßig einschränken. Notwendige Voraussetzungen für wirtschaftliches Wachstum sind darüber hinaus offene Grenzen für Fachkräfte und der zügige Abbau bestehender Handelsbarrieren.

Der Bedeutung der Digitalisierung wurde in der vergangenen Legislaturperiode bereits durch die Einsetzung des Ausschusses „Digitale Agenda" Rechnung getragen. AmCham Germany fordert, diesen Weg konsequent weiterzugehen. Dabei muss beachtet werden, dass Digitalisierung immer ausgehend von Themen und Ökosystemen gedacht und umgesetzt wird. Die Digitalisierung des Gesundheitswesens stellt uns vor andere Herausforderungen als die Digitalisierung der Justiz und diese unterscheidet sich vom Breitbandausbau. Neben unterschiedlichen Akteuren und Interessen spielt dabei der Grad der Digitalisierung eine Rolle. In einigen Bereichen (z.B. Landwirtschaft) ist sie weit fortgeschritten, in anderen sind Aufholjagden notwendig, so zum Beispiel in der Bildung. Deshalb ist die Digitalisierung eine Aufgabe der gesamten Politik, die zwar einer deutlich besseren Koordinierung bedarf, nicht aber einer Zentralisierung.

AmCham Germany fördert die globalen Handelsbeziehungen, die auf dem starken Fundament der amerikanisch-deutschen Partnerschaft stehen. Dabei unterstützen und fördern wir aktiv die Interessen unserer Mitglieder durch unser Netzwerk in Wirtschaft, Politik und der AmChams weltweit. AmCham Germany ermöglicht interkulturelles Verständnis, Zusammenarbeit und neue Investitionen durch die Grundsätze eines transparenten Dialogs, freien Handels und eines wettbewerbsfähigen und offenen Wirtschaftsklimas.

1 Aktualisierte Neuauflage der TIM Milestones 2017

1 Infrastrukturen für die Gigabit-Gesellschaft schaffen

Leistungsstarke digitale Infrastrukturen im Festnetz und Mobilfunk werden zum Rückgrat von Wirtschaft und Gesellschaft. Ihr weiterer Ausbau erfordert einen Regulierungsrahmen, der in erster Linie Anreize für private Investitionen setzt und den Wettbewerb möglichst vieler Infrastrukturen stärkt, und staatliche Interventionen auf Fälle des Missbrauchs von Marktmacht und Subventionen auf dauerhaft wirtschaftlich nicht versorgbare Gebiete beschränkt. Eine harmonisierte europäische Frequenzvergabe schafft Planungs- und Investitionssicherheit für die mobilen Netze der nächsten Generation.

Leistungsfähige Kommunikationsinfrastrukturen sind Grundvoraussetzung, um die Potenziale der Digitalisierung für Wirtschaft und Gesellschaft nutzbar machen zu können. Dies gilt gleichermaßen für die Anbindung gewerblicher wie privater Nutzer, für die Anbieterseite digitaler Dienste ebenso wie für die Nachfrage hiernach.

Notwendig sind leistungsfähige Anschlüsse sowohl im Festnetz als auch bei der mobilen Anbindung. Die Grenzen verschwimmen ohnehin, da künftige Mobilfunkstandards mit sehr hoher Leistungsfähigkeit, wie 5G, ein besonders engmaschiges Antennennetz erfordern. Dies seinerseits muss mit hochleistungsfähigen Festnetzleitungen angeschlossen sein, um die Datenverkehrsmengen überhaupt abführen zu können.

Bandbreite bleibt auch in Zukunft das zentrale, im Bedarf stetig steigende Qualitätsmerkmal für Internetanbindungen für die Breite der Anwender und Anwendungen. Ziel muss sein, möglichst vielen Haushalten und Unternehmen in den kommenden Jahren Zugang zum Internet mit Gigabit-Bandbreiten anbieten zu können. Jedoch treten daneben weitere Qualitätsparameter wie Latenz, Jitter oder Packet Loss, um bestimmte Anwendungen mit spezialisiertem Qualitätsbedarf realisieren zu können.

Weiterhin ist ein effektiver Infrastrukturwettbewerb in den Breitbandmärkten der zentrale Motor von Innovation, Investitionen und wirtschaftlichem Wachstum. Auch der notwendige Aufbau von Gigabit-Netzen wird ganz überwiegend nur mittels eigenwirtschaftlicher Investitionen der privaten Marktteilnehmer im freien Wettbewerb gelingen können. Führende Breitbandmärkte zeigen, dass der dauerhafte Infrastrukturwettbewerb zwischen mehreren Telekommunikationsnetzen auf Basis der unterschiedlichen Technologien (Glasfaser, HFC/Kabel, VDSL/Vectoring und Mobilfunk) gute Perspektiven für marktgetriebene Infrastrukturinnovationen und einen schnellen Ausbau der Fest- und Mobilnetze der nächsten Generation bieten.

Um das unverzichtbare private Investitionspotenzial zur Entfaltung zu bringen, ist für alle Beteiligten vor allem eine langfristig rechts- und planungssichere Perspektive essentiell. Für den weiteren Netzausbau müssen Investitionsanreize im Wettbewerb gesetzt werden; Investitionspotenziale können dabei auch durch ein Weniger an regulatorischen Eingriffen in den Markt erschlossen werden. Staatliche Intervention im Markt, insbesondere eigene Ausbauaktivitäten oder Fördermaßnahmen sollten zwingend eng auf solche Gebiete beschränkt bleiben, in denen ein eigenwirtschaftlicher Ausbau durch private Investoren absehbar nicht erfolgen kann. Eine Frustration privater Investition, etwa durch den Überbau bestehender Netze, muss verhindert werden.

Um den Motor des Wettbewerbs nicht ins Stocken geraten zu lassen, muss in Fällen von missbräuchlicher Marktdominanz auch weiterhin ein regulierender Eingriff den Wettbewerb sowohl auf den bestehenden als auch auf neu entstehenden Märkten sichern. Sofern Marktdominanz von Unternehmen festgestellt wird, bleibt weiterhin ein diskriminierungsfreier Zugang zu wesentlichen Leistungen (Vorprodukten) erforderlich. Zwar sind nach dem Grundsatz geringstmöglicher Regulierungsintensität wettbewerbskonforme Vereinbarungen grundsätzlich vorzuziehen, und die Erfahrungen der letzten Jahre haben gezeigt, dass kommerzielle Regelungen zunehmend an Bedeutung gewinnen, um die Interoperabilität von Dienstleistungen sowie Planungs- und Rechtssicherheit über Schnittstellen und Netzübergabepunkte zu garantieren. Allerdings

muss im Fall des Scheiterns einer Einigung der Regulierer auch weiterhin die Möglichkeit haben, zur Sicherung des Wettbewerbs Unternehmen mit beträchtlicher Marktmacht zur Bereitstellung technologieneutraler und nachfragegerechter Vorleistungsprodukte zu verpflichten.

Dies gilt vor allem auch dann, wenn bei Inanspruchnahme von Investitionsanreizen durch ein marktbeherrschendes Unternehmen ein wettbewerblich orientiertes Umfeld für alternative Anbieter andernfalls der Re-Monopolisierung anheim zu fallen droht.

Speziell für die weitere Entwicklung mobiler Breitbanddienste muss auch hier eine effiziente Regulierung ein wettbewerbliches Umfeld gewährleisten, das geeignet ist, gleichermaßen flächendeckend entsprechende Infrastrukturen und innovative Dienste durch die verschiedenen Marktbeteiligten zu ermöglichen. Insbesondere muss eine vorausschauende Frequenzstrategie verfolgt werden, die die erforderliche Planungs- und Investitionssicherheit für den Ausbau hochbitratiger Netze bietet. Neben einer planungssicheren Zukunftsperspektive für die GSM-Netze, ist vor allem das Angebot von Netzen im Bereich 5G zur Weiterentwicklung mobiler Breitbanddienste essentiell. Der 5G-Netzausbau sollte dabei so gering wie möglich durch zusätzliche Kosten und bürokratische Hürden beim Aufbau von Small Cells und neuen Funkstandorten belastet werden. Ein erleichterter Zugang für die Marktbeteiligten zu öffentlichem Grund, Gebäuden und Einrichtungen wie Lampen, Masten etc. an Straßen vereinfacht dabei die Netzausbau-Aktivitäten der Anbieter.

Als Innovations- und Wirtschaftsstandort muss Deutschland deswegen frühzeitig durch eine vorausschauende, europaweit harmonisierte Frequenzvergabe den infrastrukturellen Grundstein für mobile Breitbanddienste auch im Bereich des Internet of Things (IoT) und speziell der Machine-to-Machine-Kommunikation (M2M) legen.

2 Digitale Plattformen: Innovationspotenzial nutzen und Augenmaß bei der Regulierung walten lassen

Plattformregulierung darf Innovation, Wachstum und Wohlstand für Wirtschaft und Gesellschaft nicht verhindern. Entsprechend gilt es Augenmaß bei der Plattformregulierung walten zu lassen: Der Fokus sollte auf die Anwendung bestehender Gesetze gelegt, Selbst- und Ko-Regulierung – zumindest auf europäischer Ebene – zur ersten Wahl werden, missbrauchsabhängig ex-post reguliert und nationale oder gar regionale Alleingänge vermieden werden.

Informations- und Kommunikationstechnologie (IKT) hat das Wirtschaftsleben in den letzten 20 Jahren grundlegend verändert. Diese Entwicklung wird sich in den nächsten Jahren und Jahrzehnten mit hoher Geschwindigkeit fortsetzen. Eine zentrale Rolle werden dabei digitale Plattformen einnehmen. Immer mehr Marktsegmente werden von „Pipeline"- zu Plattformmärkten umgestaltet, und zwar sowohl im Endkonsumenten-, als auch im Industrie 4.0-Kontext. Die Ausgestaltung der rechtlichen Rahmenbedingungen für digitale Plattformen muss ihrer standortpolitischen Bedeutung gerecht werden. Plattformregulierung darf Innovation, Wachstum und Wohlstand für Wirtschaft und Gesellschaft nicht verhindern. Andererseits soll sie einen fairen Wettbewerb zwischen etablierten und neuen Plattformen ermöglichen.

„Digitale Plattformen" werden sehr unterschiedlich definiert. Aufgrund ihrer vielfältigen Ausprägungen je nach Aktivität, Branche, Geschäftsmodell oder Größe ist der Begriff als solcher nicht als Grundlage für eine rechtssichere und praxistaugliche Regulierung geeignet. Ein solcher „One Size Fits All"-Ansatz würde zu Rechtsunsicherheit und negativen Folgen für Verbraucher und Wachstum in Deutschland führen – in den meisten Fällen lassen sich digitale Plattformen durch geltendes Recht in Bereichen wie dem Schutz geistigen Eigentums, Datenschutz, IT-Sicherheit oder Verbraucherschutz ohne weiteres einordnen.

Leider hat sich die politische Diskussion zu Plattformen stark verengt. Digitale Plattformen werden sich jedoch nicht nur in vielen Endkunden-Märkten als überwiegende Marktstruktur etablieren, sondern auch im Industrie 4.0-Kontext oder in der Sharing Economy. Regelungen zur Haftung von Plattformbetreibern werden nicht nur B2C-, sondern auch B2B-Plattformen betreffen. Hier gilt es demnach Augenmaß walten zu lassen – andernfalls wird aus der Plattformregulierung ein Innovationskiller.

Plattformregulierung sollte sich an den folgenden fünf Grundsätzen orientieren:

Erstens: Verhältnismäßigkeit und Fokus auf Anwendung existierender Gesetze. Wie das Grünbuch „Digitale Plattformen" des BMWi richtig feststellt, ist der Beitrag digitaler Plattformen zu Wirtschaftswachstum, Beschäftigung und Innovation beträchtlich und darf nicht durch unverhältnismäßige Regulierung behindert werden. Die Erfahrung der letzten Jahre zeigt, dass Deutschland durch derartige Regulierungsansätze digitale Wachstumspotentiale vergeben hat. Digitale Plattformen sind bereits heute Gegenstand zahlreicher verbraucherschutz-, datenschutz- und wettbewerbsrechtlicher Vorschriften auf nationaler und EU-Ebene. Bevor die Politik über neue Regulierungen nachdenkt, die Gefahr laufen, künftige Innovationen im Keim zu ersticken, sollte sie zunächst die Durchsetzung der geltenden Vorschriften sicherstellen. Dort wo Regulierung angepasst oder neue Regeln geschaffen werden ist es wichtig, diese klar und verständlich zu formulieren. Innovationen sollten nicht durch Unsicherheit bei Verbrauchern und Wirtschaft über die geltenden Rahmenbedingungen ausgebremst werden.

Zweitens: Wettbewerb ist das beste Korrektiv. Plattformbetreiber stehen unter großem Druck, den Bedürfnissen aller Kundengruppen Rechnung zu tragen, um im Wettbewerb mit anderen Plattformen zu bestehen. Da sie sich im Wettbewerb um das Vertrauen ihrer Kunden befinden, haben sie in der Regel auch ohne Regulierung genügend Anreize, deren Nachfrage beispielswese nach Transparenz und Datenschutz zu erfüllen.

Drittens: Selbst- und Ko-Regulierung als erste Wahl, zumindest auf europäischer Ebene. Falls sich nach eingängiger Untersuchung herausstellt, dass im Zusammenhang mit einer bestimmten Art oder Aktivität von digitalen Plattformen ein Marktversagen vorliegt, sollte die Präferenz der Politik zunächst bei freiwilligen Maßnahmen wie Selbst- oder Ko-Regulierung – flankiert durch angemessene Kontrollmechanismen – liegen. Falls das identifizierte Problem darin besteht, dass Wettbewerber mit klassischen Geschäftsmodellen stärker reguliert sind als digitale Plattformen, ist zunächst zu hinterfragen, ob der bestehende Rechtsrahmen für herkömmliche Geschäftsmodelle immer noch angemessen ist und nicht vielmehr eine De-Regulierung letzterer anzudenken ist. Dies entspricht ebenfalls dem Ansatz der EU-Kommission über Online-Plattformen im digitalen Binnenmarkt [2] sowie der Monopolkommission. Die Monopolkommission stellte zudem in ihrer Mitteilung von September 2016 zu Sharing Economy fest, dass von Verboten solcher Plattformen aus wettbewerbspolitischer Sicht abzuraten sei. Wichtig sei eine „angemessene Regulierung" [3], die wir auch jetzt schon sehen.

Viertens: Missbrauchsabhängige ex-post- statt ex-ante-Regulierung. Digitale Plattformen werden zum Teil als „essential facilities" bezeichnet, die einer ex-ante-Regulierung unterliegen sollten. Eine pauschale Gleichsetzung digitaler Plattformen mit physischen Infrastrukturen ist grundfalsch und unterschätzt die Innovations- und Wettbewerbsdynamiken der digitalen Welt. Was heute wie eine unangreifbare, dominante Plattform aussieht, kann morgen schon ein „alter Hut" sein. Deswegen ist im Wettbewerbsrecht die missbrauchsorientierte Einzelfallbetrachtung ex-post der richtige Ansatz.

Fünftens: Keine nationalen oder regionalen Alleingänge. Schließlich sind nationale, regionale oder gar lokale Insellösungen kontraproduktiv für den Aufbau einer erfolgreichen Plattformwirtschaft in Deutschland und Europa. Ohne einen einheitlichen und wettbewerbsfähigen Rechtsrahmen ist es darüber hinaus nur schwer denkbar, erfolgreiche neue Akteure herauszubilden oder dem vorhandenen Mittelstand die notwendige digitale Transformation zu erleichtern. Ein einheitlicher

2 https://ec.europa.eu/transparency/regdoc/rep/1/2016/DE/1-2016-288-DE-F1-1.PDF
3 http://www.monopolkommission.de/images/HG21/HGXXI_Kap5.pdf

Rechtsrahmen im digitalen Binnenmarkt anstatt 28 verschiedener Regelwerke wäre sowohl zum Nutzen der Unternehmen als auch der Verbraucher. Harmonisierte Vorschriften auf EU-Ebene beschleunigen die Einführung innovativer Angebote und erleichtern das Wachstum digitaler Plattformen in den europäischen Märkten. Der European Digital Single Market sollte nicht nur in rechtlicher, sondern auch in technischer Hinsicht (Standards) gefördert werden.

Innovationen lassen sich selten durch eine Verschärfung des nationalen Ordnungsrahmens herbeiführen. Vielmehr sollte der Ordnungsrahmen so gestaltet sein, dass in Deutschland und Europa grundsätzlich Innovationen möglich sind und möglich bleiben. Die Einführung von Experimentierklausel um Innovationen zeitlich und/oder örtlich begrenzt von Regulierung auszunehmen wäre zielführend. Dort, wo Regulierung heute Innovationen verhindert (z. B. Personenbeförderungsrecht), sollte diese modernisiert werden. Das schafft neue wirtschaftliche und gesellschaftliche Chancen hierzulande. Im Fokus sollte dabei immer ein problemorientierter Ansatz stehen, bei dem die „harte" Regulierung von Plattformen die letzte Lösung darstellt. Um die Vision eines europäischen digitalen Binnenmarktes auch für die Plattformwirtschaft zu verwirklichen, sollten nationale Alleingänge möglichst vermieden und die Harmonisierung eines innovationsfreundlichen Rechtsrahmens in der EU unterstützt werden.

Im Zuge der fortwährend dynamischen, weltweiten Technologieentwicklung wird es für viele etablierte Geschäftsmodelle ein Existenzrisiko geben, welches auch durch einen schärferen Ordnungsrahmen nicht vermeidbar sein wird. Dies ist nicht zuletzt auch Teil eines funktionierenden Wettbewerbs. Gleichwohl sollten regulatorische Anpassungen zum Ausgleich von Wettbewerbsnachteilen ausgewogen und nicht zum Nachteil einzelner oder speziell ausländischer IKT-Anbieter vorgenommen werden. AmCham Germany wird sich auch weiterhin für einen fairen und ausgewogenen Wettbewerb in Deutschland und Europa einsetzen.

3 Unklare Rechtslage der Providerhaftung beenden

Angesichts der zentralen Rolle der Providertätigkeit bei der Gestaltung und Entwicklung des Internets, sind klare Regeln zur Verantwortlichkeit von Service Providern hinsichtlich fremder Inhalte dringend notwendig. Während die europäische E-Commerce-Richtlinie für viele Bereiche sinnvolle Verantwortungszuweisungen enthält, lässt die Umsetzung in deutsches Recht die notwendige Klarheit vermissen. Überdies bestehen auch große Unterschiede in der europaweiten Umsetzung der Richtlinie. Dies hat zu Rechtsunsicherheit und damit verbunden zu widersprüchlicher und zum Teil praxisferner Rechtsprechung geführt. Hierdurch wird die Entwicklung des gesellschaftlichen und wirtschaftlichen Nutzens des Internets gehemmt.

Ein gutes Beispiel, um den Ansatz für eine progressive Plattformregulierung und die Gefahr nationaler Alleingänge zu illustrieren, ist die sogenannte „Providerhaftung", also die Frage, inwieweit ein Anbieter einer digitalen Plattform für Rechtsverletzungen, die durch die Plattformnutzer begangen werden, in Haftung genommen werden kann. Angesichts der zentralen Rolle der Plattformanbieter bei der Gestaltung und Entwicklung des Internets, sind klare Regeln zur Verantwortlichkeit von Diensteanbietern hinsichtlich fremder Inhalte dringend notwendig.

In dem Fall, in dem Nutzer automatisiert Inhalte einstellen können, etwa bei Online-Marktplätzen, haben die Betreiber der Plattformen, sogenannte Host-Provider, keinerlei Kenntnis von den nutzergenerierten Angeboten. Die fremden Inhalte auf ihre Rechtmäßigkeit zu kontrollieren, ist angesichts der Menge der verarbeiteten Daten in der Praxis kaum realisierbar. Die Providertätigkeit erfordert daher klare Regeln zu ihrer Verantwortlichkeit hinsichtlich der fremden Inhalte.

Die europäische E-Commerce-Richtlinie gibt hier einen ausgewogenen Rechtsrahmen vor, in dem sie Host-Provider grundsätzlich solange von juristischer Verantwortung freistellt, wie sie nicht tatsächliche Kenntnis von einem rechtswidrigen Inhalt haben und ab Kenntnisnahme umgehend die Beseitigung oder Sperrung dieses Inhalts betreiben. Eine Pflicht zu einem allgemeinen Monitoring der gespeicherten fremden Inhalte gibt es hingegen nicht. Dies ist auch zu begrüßen, da eine

entsprechende Verpflichtung technisch kaum möglich und wirtschaftlich nicht zumutbar ist und ansonsten der Nutzen der Plattformen für den Verbraucher gefährdet und jedwede Innovation, die durch die Plattformwirtschaft erfolgt, verhindert werden würde.

Während die E-Commerce-Richtlinie also sinnvolle Verantwortungszuweisungen enthält, lässt die Umsetzung in deutsches Recht die notwendige Klarheit vermissen. Dies hat zu Rechtsunsicherheit und damit verbunden zu widersprüchlicher und zum Teil praxisferner Rechtsprechung geführt. Erfreulicherweise – aber lediglich für einen Teilbereich, nämlich für die Frage, ob Anbieter öffentlich zugänglicher WiFi-Hotspots für Rechtsverletzungen Dritter haften – wurde durch das Dritte Gesetz zur Änderung des Telemediengesetzes im Herbst 2017 die „Störerhaftung" für diesen Bereich abgeschafft. Ein Problem bleibt jedoch, dass der Host-Provider selbst zwischen den eigentlich streitenden Parteien steht. In der Regel fehlen ihm die Informationen, um die Tatsachen- und Rechtslage abschließend einschätzen zu können. Dennoch wird er durch eigene Prüfpflichten in die Rolle eines Richters gedrängt, ohne hierfür über die fachliche, geschweige denn institutionelle Kompetenz zu verfügen. Schon allein die Bandbreite der möglichen Rechtsverletzungen, etwa Regelungen aus dem Bereich der Produktsicherheit, des Umwelt- und Verbraucherschutzes, des Wettbewerbs- und des Steuerrechts, Urheber- und Markenrechte etc., zeigt die Unmöglichkeit eines solchen Unterfangens, insbesondere da für den Plattformanbieter zunächst nur die Angaben der Nutzer vorliegen.

Wünschenswert wäre daher, statt Unterlassungs- und Monitoring-Pflichten auszuweiten, ein Notice-And-Take-Down-Verfahren einzuführen, in dem ein Provider aufgrund bestimmter formaler Kriterien Inhalte entfernen kann, ohne selbst in den Streit zwischen Rechteinhaber und Verletzer hineingezogen zu werden. Selbstverständlich sollte die Rechtsordnung aber auch Möglichkeiten bereithalten, gegen solche Provider vorzugehen, deren Tätigkeit gerade auf das Hosten von rechtsverletzenden Inhalten abzielt.

Der praktische Wert solcher Verfahren zur effektiven Bekämpfung von Rechtsverletzungen ist bereits in verschiedenen Jurisdiktionen erprobt; der Vorteil liegt insbesondere in der schnellen vorläufigen Unterbindung einer vermeintlichen bzw. behaupteten Rechtsverletzung, indem auf die Information vom Regelverstoß (Notice) im Vertrauen auf deren Richtigkeit als Regelmaßnahme die umgehende Sperrung des Inhalts folgt (Takedown). Wesentlicher Anreiz eines solchen Regimes wäre die Haftungsfreistellung für den Provider im Fall von ungerechtfertigten Maßnahmen aufgrund der Angaben des Rechteinhabers.

Unklarheiten bestehen ferner bei der Frage, wann „tatsächliche Kenntnis" einer Rechtsverletzung vorliegt. Dies führt zur rechtlichen Unsicherheit, ob z. B. stichprobenartige Monitoring-Aktivitäten zur Kenntnis und damit in der Folge zu einer Haftung für entdeckte illegale Inhalte führen könnten. Hier sollte das Recht klare Regeln vorsehen, die eine Schlechterstellung durch freiwillige Sicherheitsmaßnahmen verhindern, wie sie etwa im anglo-amerikanischen Rechtskreis als „Good Samaritan Principle" bekannt sind.

Soziale Plattformen stehen an dieser Stelle vor besonderen Herausforderungen. Hier stellt die Prüfung aller eingehenden Meldungen aufgrund ihrer bloßen Menge eine Herausforderung dar, der sich die Anbieter mit hohem Ressourcenaufwand stellen. Die E-Commerce-Richtlinie verpflichtet die Plattformanbieter, rechtswidrige Inhalte unverzüglich nach Kenntnis zu löschen. Dies bedeutet allerdings nicht, unverzüglich nach Kenntnis des Inhalts, denn die Kenntnis über die Rechtswidrigkeit kann erst später – nach einer rechtlichen Prüfung – vorliegen. Insbesondere bei schwierigen Abwägungsentscheidungen, wie im Bereich der Meinungsfreiheit, kann die juristische Einschätzung komplex und zeitaufwändig sein. Plattformen eine sehr restriktive Zeitauflage vorzugeben, ist daher kontraproduktiv. Vor diesem Hintergrund sehen wir das zum 1. Januar 2018 in Kraft getretene Netzwerkdurchsetzungsgesetz kritisch. Eine Evaluierung durch die neue Bundesregierung ist notwendig. Die im Gesetz verankerten kurzen, starren Löschfristen in Verbindung mit hohen Bußgeldandrohungen können im Zweifelsfall dazu führen, dass Inhalte vorsorglich und schneller entfernt werden, ohne die im Grundgesetz garantierte Meinungsfreiheit abzuwägen. Eine Abgrenzung zwischen verbotener Beleidigung und erlaubter Satire kann in Folge teilweise wegfallen. Dies ist in den ersten Tagen seit Inkrafttreten auch bereits zu beobachten, praktische Probleme bei der Umsetzung werden gänzlich bei den Anbietern abgeladen.

Wie oben dargelegt, bieten Instrumente der Selbst- und Ko-Regulierung gute Ansätze für eine Plattformregulierung. Hierbei sollten alle relevanten Interessengruppen, etwa Verbände, Rechteinhaber und Organe der Rechtsdurchsetzung mit eingebunden werden. Ein gutes Beispiel für einen „Stakeholder"-Ansatz ist das 2011 geschlossene Memorandum of Understanding über den Internethandel mit gefälschten Waren, das von der EU-Kommission unterstützt wurde und die Zusammenarbeit der relevanten Interessengruppen massiv verbessert hat.

4 Industrial Internet: Durch geeignete Rahmenbedingungen volles Potenzial heben

Damit Deutschland seine starke Stellung im Industrial Internet weiter ausbauen kann, bedarf es leistungsfähiger industrieller Plattformen und geeigneter politischer Rahmenbedingungen, die die Erfassung, Verarbeitung, Speicherung und Übertragung von Daten ermöglichen, ohne Abstriche beim Schutz personenbezogener Daten und der Sicherheit informationstechnischer und industrieller Systeme zu machen.

Seit einiger Zeit erfasst die Digitalisierung aller Lebensbereiche auch die Kernbereiche industrieller Wertschöpfung. Das hat allergrößte Bedeutung für Wohlstand und Beschäftigung in Deutschland, wo der Anteil des verarbeitenden Gewerbes an der Bruttowertschöpfung mit etwa 23 Prozent sehr hoch ist. Die „Vierte Industrielle Revolution" ist in vollem Gange: Im industriellen Internet der Dinge werden Maschinen mit Sensoren ausgestattet und senden Daten, die mit internetbasierenden Anwendungen gesammelt und ausgewertet werden. In der industriellen Fertigung, in Energie, Transport und Logistik lassen sich Abläufe und Verfahren dank dieser Datenanalytik effizienter, kostengünstiger und sicherer gestalten.

Bei Internetanwendungen für Konsumenten (B2C) spielen deutsche Unternehmen heute nur eine untergeordnete Rolle. Anders im industriellen Internet (B2B): Hier wird Deutschland mit seiner starken industriellen und mittelständischen Basis weltweit führend sein und kann seine wirtschaftliche Stellung behaupten und ausbauen. Dazu bedarf es leistungsfähiger industrieller Plattformen, die es wie ein Betriebssystem ermöglichen, unterschiedliche Applikationen etwa in der internetgesteuerten Produktion (Industrie 4.0) und im vorausschauenden Betrieb von Maschinen und Anlagen (Asset Performance Management) einzusetzen. Und es bedarf geeigneter politischer Rahmenbedingungen, die die Erfassung, Verarbeitung, Speicherung und Übertragung von Daten ermöglichen, ohne Abstriche beim Schutz personenbezogener Daten und der Sicherheit informationstechnischer und industrieller Systeme zu machen.

Die Produktivitätsgewinne stellen sich bereits heute ein und werden weiter wachsen; allerdings kommen mit der Digitalisierung sowie dem Einsatz von Robotern und autonomen Systemen auch altgewohnte Fähigkeiten und Fertigkeiten auf den Prüfstand. Für manche Befürchtungen vor größeren Arbeitsplatzverlusten gibt es dabei weder aufgrund aktueller Beobachtungen noch unserer historischen Erfahrungen Anlass. Dennoch werden sich Tätigkeitsprofile verändern, wird die laufende Qualifizierung und ganz generell die Bildung und Ausbildung von Beschäftigten in allen industriellen Sektoren weiter an Bedeutung gewinnen. Unternehmen und Staat tragen hierfür gemeinsam Verantwortung.

5 Intelligent mit künstlicher Intelligenz umgehen

Durch künstliche Intelligenz können die großen gesellschaftlichen Herausforderungen besser bewältigt werden. Dabei werden menschliche Fähigkeiten ergänzt und gestärkt, ohne sie zu ersetzen. Entscheidungsprozesse müssen dennoch nachvollziehbar sein, ohne dass Unternehmen Geschäftsgeheimnisse aufgeben.

Der vermehrte Einsatz von technisch immer versierteren Assistenzsystemen führt zu einer Debatte über den generellen Umgang mit und den Einsatz von künstlicher Intelligenz. Diese Debatte ist innovationsoffen und differenziert zu führen, was schon damit beginnt, dass unterstrichen werden muss, dass es nicht eine Art der künstlichen Intelligenz gibt. So reicht die Spannbreite von ausgereiften Data Analytics Lösungen über begrenzt selbstlernende Systeme bis hin zu neuronalen Netzwerken, die menschliche Synapsen nachbilden.

Allen Systemen inhärent ist die Zielrichtung, den Nutzer zu besseren Entscheidungen kommen zu lassen, sei es den Arzt bei der Auswahl der erfolgversprechendsten Therapie, den Autofahrer bei der Wahl der sichersten Strecke und Fahrweise, den Bankkunden bei der richtigen Anlagestrategie oder den Konsumenten bei einer zielgerichteten Produktauswahl.

Wenn künstliche Intelligenz aber vermehrt die Entscheidungsfindung prägt, kommt den Programmierern eine besonders verantwortungsvolle Rolle zu. Algorithmen brauchen ein Mindestmaß an Transparenz oder Interpretierbarkeit: Dabei muss ein Ausgleich zwischen dem Schutz von Geschäftsgeheimnissen und dem Informationsbedürfnis der Nutzer gefunden werden. Privacy by Design, wie es die Datenschutzgrundverordnung vorsieht, sollte zu Ethics by Design weiterentwickelt werden und ethische Aspekte müssen Bestandteil der Ausbildung von Programmierern und Ingenieuren sein.

Wir starten hier nicht von Null. Überall im Bereich Datenverarbeitung gibt es ethisch begründete Verfahren (Verhältnismäßigkeit, Einwilligung, Zweckbindung, etc.). Grundsätzlich sollten alle Systeme künstlicher Intelligenz nach denselben Werten funktionieren wie menschliche Interaktionen – das ist gerade bei Mensch-Maschine-Interaktion zentral. Hierbei sind einige Branchen (Gesundheit, Finanzsektor) schon sehr weit fortgeschritten. Das zeigt auch, dass Ethik in den einzelnen Bereichen (Domains) gedacht und durch dynamische Anpassung entwickelt wird. Eine verallgemeinerte Ethik für künstliche Intelligenz ist daher nicht zielführend.

Dabei darf nicht unterschlagen werden, dass der vermehrte Einsatz intelligenter Systeme auch dazu führen wird, dass bestimmte Qualifikationen weniger nachgefragt werden (insbesondere solche, die automatisiert werden können). Die befürchtete massenhafte Jobvernichtung ist aber höchst unwahrscheinlich, da Maschinen und Menschen über sich ergänzende Fähigkeiten verfügen. Historisch ist technologischer Fortschritt nicht nur von höherer Produktivität begleitet worden, sondern auch von insgesamt höheren Beschäftigungszahlen. Hoch qualifizierte Berufe wie Ingenieure, Architekten oder Richter werden weiterhin stark nachgefragt sein, ebenso solche, die ein hohes Maß an sozialer und emotionaler Kompetenz erfordern.

Spezifische Regelungen (Maschinensteuer, Versicherungen gegen „falsche Berufswahl") sind zum jetzigen Zeitpunkt nicht notwendig. Wir brauchen einen innovationsoffenen und wettbewerbsfreundlichen Rahmen, der auf die technische Gestaltung von Innovationen zielt und weniger auf die rechtlichen Detailfragen. Neue Gesetze bzw. Sanktionierungen sind daher nicht zielführend, es bedarf vielmehr IT-Anwendungen, die den geltenden Vorgaben Rechnung tragen und damit die eigentliche Voraussetzung für die legale Verarbeitung von Daten darstellen.

6 Cybersicherheit durch klare und einheitliche europäische Regeln gewährleisten

Es bedarf einer zielgerichteten Sicherheitspartnerschaft zwischen Staat und Wirtschaft sowie einer strikt einheitlichen europäischen Kodifizierung und Durchsetzung der bestehenden Regulierungen. Nationale Sonderwege, die zu widersprüchlichen Regelungen und Doppelregulierungen führen, müssen vermieden werden. Der Schlüssel zur Erhöhung von Sicherheit in der digitalen Welt liegt dabei vor allem in technologischen Innovationen von Schutzmechanismen.

Die Digitalisierung in Staat, Wirtschaft und Gesellschaft hat Deutschland in nur wenigen Jahren grundlegend verändert. Vernetzte elektronische Geräte prägen verstärkt den Lebens- und Arbeitsalltag der Menschen. Durch die zunehmende maschinelle Erzeugung von Daten sowie die zunehmende Verbreitung von intelligenten Zählern und Sensoren entstehen riesige Datenmengen. Selbstlernende Maschinen können immer komplexere Aufgaben übernehmen. Abläufe, Verfahren und Produktionsprozesse werden zunehmend vernetzt. Der grenzüberschreitende Cyberraum erfordert neue Ansätze.

Für die Cybersicherheitspolitik ist dies Neuland. Wie bei anderen modernen Bedrohungsformen gilt auch hier: Das Territorialprinzip und die Fixierung auf territoriale Grenzen verlieren an Bedeutung. Mit der NIS Richtlinie ist auf EU-Ebene ein erster regulativer Ansatz für ein harmonisiertes IT-Sicherheitsregime in Kraft. Im Rahmen des EU-Cybersecurity Packages soll dies unter anderem um einen Rahmen für harmonisierte Zertifizierungsverfahren ergänzt werden. AmCham Germany unterstützt diese Bestrebungen, sowohl im Bereich der materiellen IT-Sicherheitsregulierung als auch im Bereich von Standards und Zertifizierungen zu EU-einheitlichen Regeln und Prozessen zu gelangen nachdrücklich.

Zum einen bedarf es einer zielgerichteten Sicherheitspartnerschaft zwischen Staat und Wirtschaft, insbesondere unter partnerschaftlichem Einbezug der Innovations- und Wissensbasis der IKT-Anbieter. Die Cybersicherheitsstrategie der Bundesregierung sollte insbesondere unter diesem Aspekt in dieser Legislaturperiode weiterentwickelt und angepasst werden. Im Sinne eines top-down, bottom-up-Verfahrens unter Einbindung der industriellen Expertise gilt es für einen besseren Schutz und eine höhere Akzeptanz in Wirtschaft und Gesellschaft zu wirken.

Die zweite Dimension betrifft die europäische und internationale Perspektive. Es bedarf zwingend eines integrierten und abgestimmten europäischen Ansatzes, der auch eine flexible Gesprächsbereitschaft der Bundesregierung erfordert. Aktuell zeigen insbesondere die Herausforderungen bei der Abstimmung zwischen Europäischer NIS-Richtlinie und dem Deutschen IT-Sicherheitsgesetz, welchen Wert ein abgestimmtes Vorgehen haben kann. Mittelfristig gilt es, einen vollständig harmonisierten EU-Regulierungsrahmen mit abschließender Wirkung anzustreben.

Europäisch agierende Unternehmen betreiben meist Dienste in mehreren Staaten der EU, bieten Dienste aus verschiedenen Staaten für verschiedene Staaten an und beziehen Dienste aus verschiedenen Mitgliedsstaaten. Eine nicht harmonisierte Umsetzung der NIS-Richtlinie in den einzelnen EU-Mitgliedstaaten darf nicht zu unterschiedlichen oder gar widersprüchlichen Umsetzungen führen, die gegebenenfalls nicht realisierbar sind. Ein entsprechender Austausch mit dem Ziel der Harmonisierung in den Mitgliedsstaaten ist unbedingt erforderlich. Beispielsweise würde im Hinblick auf die Regelung zur örtlichen Zuständigkeit der Aufsichtsbehörden, die vorgeschlagene Umsetzung in Deutschland diesen Ansatz praktisch kodifizieren. So droht die Gefahr, dass die betroffenen Dienstanbieter gegenüber mehreren Behörden (im EU-Sitzland und in Deutschland) berichtspflichtig wären.

Betreiber von KRITIS-Anlagen müssen sich künftig darauf einstellen, eine regelmäßige Überprüfung durch BSI-Vertreter vor Ort zu begleiten und zu unterstützen. Dies widerspricht jedoch gänzlich dem bislang gewählten kooperativen Ansatz, wonach sich KRITIS-Betreiber in eigener Verantwortung nach dokumentierten Standards schützen und ausdrücklich keine BSI-Überprüfung der einzelnen Anlagen vorgesehen war. Auch ist fraglich, ob diese Praxis der Erhöhung von Sicherheitsstandards dienlich ist.

Mit der jetzt von der Richtlinie übernommenen Definition der Cloud-Dienste, die bislang so im deutschen Recht nicht existiert, entsteht ein Überschneidungsbereich mit den nach IT-Sicherheitsgesetz und der darauf aufbauenden Verordnung erfassten Betreibern von Rechenzentren, die auch der entsprechenden Meldepflicht unterliegen. Hier ergeben sich Fragen in Bezug auf etwaige Doppelregulierungen. Zur Vermeidung von Doppelregulierungen sollte eine Klarstellung erfolgen, dass die im Zuge der Umsetzung der NIS-Richtlinie geschaffenen Verpflichtungen (etwa Meldepflichten) nicht gelten, wenn entsprechende oder strengere Pflichten für den konkreten Anbieter bereits aus Regelungen für die Betreiber kritischer Infrastrukturen folgen.

Vergleichbares gilt auch für internationale Ansätze. Die sehr lange geführte Debatte rund um den Nachfolger von Safe Harbor, die daraus resultierende Unsicherheit bei Kunden und Wirtschaft sowie die teilweise bestehenden Unsicherheiten bezüglich der Rechtsverbindlichkeiten, darf sich im Cybersicherheitsbereich nicht wiederholen. Hier sind alle Akteure gefordert, Rechtssicherheit und internationale Anschlussfähigkeit zu jedem Zeitpunkt der Debatte sicherzustellen. Gerade der auf internationalen Standards aufbauende konstruktive Diskussionsprozess zwischen UP-KRITIS und dem BSI, sollte als Blaupause für weitere Prozesse dienen.

Es ist unbestritten, dass der Staat die Pflicht hat, im Interesse der Bürgerinnen und Bürger sowie der Wirtschaft die Sicherheit im Cyberraum aktiv zu gestalten und Rahmenbedingungen zu schaffen, um Sicherheit zu gewährleisten und dennoch diese Veränderungsprozesse chancenorientiert weiterzuentwickeln. Wirtschaft, Bürgerinnen und Bürger müssen auch zukünftig sicher, frei und selbstbestimmt im digitalen Kosmos agieren können. Unternehmen müssen ihr Know-how auch im Zeitalter der Digitalisierung vor einem unerlaubten Zugriff schützen und die Produktionsprozesse auch dann beherrschen, wenn dabei selbstlernende Maschinen zum Einsatz kommen oder ihre Daten durch die Nutzung von Cloud-Lösungen verteilt sind. Ein Schlüssel zur Erhöhung von Sicherheit in der digitalen Welt liegt dabei in technologischen Innovationen von Schutzmechanismen.

IT-Sicherheit ist in Zeiten des Internet of Things keine exklusive Domäne reiner IT-Unternehmen mehr. Wenn mehr und mehr Gegenstände des Alltags vernetzt sind, wird IT-Sicherheit zur Querschnittsanforderung für fast jeden Produktionssektor. Erste Botnetzangriffe unter Ausnutzung von IoT-Endgeräten belegen, dass die Gefahr schon heute keine theoretische mehr ist. Es bedarf daher einer Diskussion, auf welchem Wege die IT-Sicherheit über die künftige, nahezu unüberschaubare Breite vernetzter Geräte, die auch in den Alltag der Verbraucher einziehen, erhöht werden kann. Hier stellt sich die Frage neuer, flexibler Mindeststandards bzw. der Etablierung von IoT-Sicherheitslabeln. Auch die schon im Gange befindliche Diskussion zu etwaigen Anpassungen im Haftungssystem sollte im Kontext dieser Standardisierungsfrage diskutiert werden, weil Haftungsadressaten Rechtssicherheit benötigen, welche Maßnahmen vorzunehmen sind. Anders als in der bisherigen standardbezogenen Regulierung von IT-Sicherheit, die mit BSI-Grundschutz und ISO-Standards auf kritische oder zumindest besonders relevante Einzelsektoren zielt, muss für die Zukunft ein Weg gefunden werden, Sicherheitsmindeststandards für Massenmarktprodukte zu etablieren. Dies setzt voraus, dass weniger komplexe Standards entwickelt werden, die Implementierung auch für kleine Unternehmen und Startups kostenmäßig handhabbar bleibt und für die vor allem keine monatelangen Zertifizierungsprozesse erforderlich sind. In Bezug auf die aufkommende Diskussion um eine Reform der Produkthaftung ist überdies zu berücksichtigen, dass Haftungsrisiken versicherbar sein müssen. Auch sollten offene Entwicklungs- und Distributions-Ansätze, wie Open Source nicht durch Haftungsregelungen infrage gestellt werden.

7 Rahmenbedingungen für Ermittlungen im Cyberspace harmonisieren und modernisieren

Ermittlungsarbeit im Cyberspace bedarf einer stärkeren Harmonisierung der Rechtsgrundlagen staatlicher Zugriffsbefugnisse, einer Modernisierung der bestehenden Rechtshilfeabkommen sowie größtmöglicher Transparenz.

Innere Sicherheit wird eines der zentralen Themen dieser Legislaturperiode. Die grundlegende Herausforderung der Gewährleistung effektiver Ermittlungsarbeit bei gleichzeitiger Wahrung der hohen rechtsstaatlichen Standards und dem Schutz der Grundrechte des Einzelnen ist dabei aktueller denn je. An der bereits im Gang befindlichen Diskussion zeigt sich, dass die Ermittlungsarbeit im Cyberspace eine besondere Rolle spielt. Ermittlungsbehörden weisen auf die Notwendigkeit einer „Waffengleichheit" hin, um Straftaten und terroristische Bedrohungen frühzeitig zu erkennen. Gleichzeitig besteht ein gesellschaftlicher Konsens, dass eine flächendeckende Überwachung der Bevölkerung nicht mit den Verfassungswerten Deutschlands in Einklang zu bringen ist. Dazu kommt, dass Ermittlungen im Cyberspace immer öfter internationalen bis globalen Charakter haben. Es bedarf daher einer grundlegenden Diskussion zu den Befugnissen von Ermittlungsbehörden im Netz und in diesem Zusammenhang auch der Zusammenarbeit mit Telekommunikations- und Internetdienstleistern im Bereich staatlicher Zugriffsbefugnisse.

Momentan fehlt es weitgehend an harmonisierten Rahmenbedingungen für den Zugriff auf digitale Beweismittel, wenn dieser grenzüberschreitend erfolgen muss. Der Fortschrittsbericht der EU-Kommission zu den Schlussfolgerungen des EU-Rates in Bezug auf Ermittlungen im Cyberspace sieht daher die Notwendigkeit vereinheitlichter und modernisierter rechtlicher Grundlagen vor. Die neue Bundesregierung sollte diese Initiative aufgreifen und sich für eine stärkere Harmonisierung der rechtlichen Grundlagen staatlicher Zugriffsbefugnisse einsetzen.

Es muss insbesondere vermieden werden, dass es zu einem Wettrüsten der Staaten in Bezug auf einseitige extraterritoriale Zugriffe von Strafverfolgungsbehörden kommt. Deshalb bedarf es entlang der Empfehlungen der EU-Kommission einer grundlegenden Modernisierung der bestehenden Rechtshilfeabkommen, um diese in der Praxis zu revitalisieren.

Soweit die Politik über eine Ausdehnung der Zugriffsbefugnisse im Cyberspace nachdenkt, muss im Sinne der Sicherung rechtsstaatlicher Balance der Aspekt der Transparenz stärker hervorgehoben werden. Ziel muss ein größtmögliches Maß an Transparenz sein, solange diese nicht den Ermittlungserfolg im Einzelfall gefährdet. Daher sollten die bestehenden gesetzlichen Regelungen in Bezug auf Zugriffsbefugnisse von Behörden für Kommunikationsanbieter präzisiert und insbesondere festgelegt werden, unter welchen Umständen und in welchem Umfang Unternehmen, die aufgrund gesetzlicher Vorschriften zur Herausgabe von Informationen an Behörden verpflichtet sind, hierüber die betroffenen Kunden unterrichten dürfen.

Flankierend muss es Unternehmen weiterhin möglich sein, im Wege statistischer Transparenzberichte ein Mindestmaß an Transparenz in Bezug auf den Umfang der Zusammenarbeit mit Behörden auf Basis der entsprechenden rechtlichen Pflichten herzustellen. Transparenzberichte haben sich in den vergangenen Jahren zu einem wichtigen Instrument der Vertrauensbildung gegenüber Bürgern und Kunden sowohl bezüglich der Arbeit der Sicherheitsbehörden als auch in Bezug auf die von Bürgern genutzten Telekommunikations- und Internetdienste, entwickelt. Anzustreben ist, dass diese Form der öffentlichen Information künftig ausgebaut wird.

Die neue Bundesregierung sollte außerdem an der eingeschlagenen Linie in Bezug auf Verschlüsselung festhalten. Wirksame und einfach nutzbare Verschlüsselung ist und bleibt die zentrale digitale Vertrauenstechnologie der digitalisierten Welt. Daher darf das Grundprinzip einer Ablehnung jeder Form der „Krypto-Regulierung" nicht aufgeweicht werden. Denn jedwede regulatorisch erzwungene Schwächung kryptografischer Systeme schwächt das Grundprinzip und damit auch das Vertrauen der Nutzer.

8 Hürden für den Datenverkehr abbauen

Um die enormen Wachstumspotenziale der Datenwirtschaft voll auszuschöpfen, muss der möglichst ungehinderte Datenverkehr im europäischen Binnenmarkt sowie mit unseren wichtigsten Handelspartnern, einschließlich der USA, gesichert werden. Die Bundesregierung sollte diesbezügliche Initiativen auf europäischer und internationaler Ebene unterstützen und Beschränkungen des freien Datenverkehrs in Deutschland einer strengen Prüfung unterziehen. Der verbesserte Zugang zu und Austausch von maschinengenerierten Daten zwischen verschiedenen Unternehmen und Sektoren kann am besten erreicht werden, indem die Politik internationale, industriegetriebene Normen fördert und davon absieht, die Vertragsfreiheit unnötig einzuschränken.

Die Verarbeitung und Weitergabe von digitalen Daten ist heute fester Bestandteil moderner Geschäftsmodelle. Der freie Datenverkehr über Landesgrenzen hinweg ermöglicht es Unternehmen, auf globale Wertschöpfungsketten zurückzugreifen und ihre Cloud-basierten Dienste sicherer und günstiger anzubieten. Insbesondere kleine und mittlere Anbieter digitaler Dienste können auf diese Weise schneller wachsen und neue Märkte erschließen. Zugleich wächst das Angebot kostengünstiger Dienstleistungen für Unternehmen und Verbraucher. Im Internet der Dinge sind zudem viele Millionen Geräte miteinander verbunden und nutzen grenzüberschreitende Datenübertragung, etwa in den Bereichen vernetztes Fahren, Logistik und industrielles Internet.

Mit einem Volumen von gut 70 Milliarden Euro machte die Datenwirtschaft im Jahr 2015 2,3 Prozent des deutschen Bruttoinlandsprodukts aus. Dieser Anteil könnte bis 2020 auf bis zu sieben Prozent anwachsen, wenn die richtigen politischen und rechtlichen Rahmenbedingungen gegeben sind.[4] Die Gewährleistung des freien Datenverkehrs im europäischen Binnenmarkt sowie mit unseren wichtigsten Handelspartnern, einschließlich der USA, gehört hierbei zu den wesentlichen Voraussetzungen.

Dennoch besteht heute noch kein europäischer Binnenmarkt für Daten. Zwar soll die Datenschutz-Grundverordnung mit EU-weit einheitlichen Vorschriften ab Mai 2018 die datenschutzbedingten Hindernisse für den Verkehr personenbezogener Daten im Binnenmarkt abschaffen. Viele faktische oder rechtliche Beschränkungen des Datenverkehrs, die allein die deutsche Volkswirtschaft geschätzt pro Jahr zwischen 0,05 und 0,06 Prozent des Bruttoinlandprodukts kosten, bleiben hiervon jedoch unberührt.[5] Neben den rechtlichen Beschränkungen ist zudem die Fehleinschätzung verbreitet, dass die lokale Speicherung von Daten grundsätzlich sicherer sei als eine Speicherung in anderen EU-Mitgliedstaaten. Diese Annahme darf die Regierung nicht zu fehlgeleiteten nationalen Alleingängen führen, die den digitalen europäischen Binnenmarkt verhindern und damit Wachstumsperspektiven für die deutsche Wirtschaft beschränken. Es müssen bestehende legislative und formal gelebte Lokalisierungsregelungen im Sinne der Verwirklichung eines digitalen europäischen Binnenmarktes nachhaltig beseitigt werden. In diesem Sinne sollte die Bundesregierung die EU-Kommission in ihrer Initiative zur Durchsetzung der Binnenmarktregeln im Sinne eines freien Datenverkehrs unterstützen und jegliche Beschränkungen des freien Datenverkehrs in Deutschland einer strengen Prüfung hinsichtlich ihrer Zweckmäßigkeit und Verhältnismäßigkeit unterziehen.

Mindestens genauso wichtig ist der internationale Datenverkehr mit wichtigen Handelspartnern wie den USA. Für den Transfer personenbezogener Daten bietet die Datenschutz-Grundverordnung vielfältige Werkzeuge, auf denen auch das Privacy Shield-Abkommen zwischen der EU und den USA beruht. Die Bundesregierung sollte die EU-Kommission darin bestärken, auf dieser Basis die Gespräche zur „Feststellung eines angemessenen Datenschutzniveaus" auch mit anderen wichtigen Handelspartnern in Ost- und Südost-Asien sowie mit interessierten Ländern in Lateinamerika und den Nachbarländern zügig voranzutreiben und Freihandelsabkommen zu nutzen, um den freien Datenverkehr zu fördern und neue Formen des digitalen Protektionismus zu überwinden. Zudem sollte Deutschland sich in internationalen Organisationen wie dem Europarat, den G20 und den Vereinten Nationen für eine Konvergenz hin zu hohen Datenschutzstandards einsetzen, um den freien Datenverkehr weltweit zu erleichtern.

4 European Data Market Study, SMART/0063, IDC, 2016.

5 ECIPE, Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States, 2016.

Neben grenzüberschreitenden Datenflüssen muss auch der Zugang zu und Austausch von maschinengenerierten Daten zwischen verschiedenen Unternehmen und Sektoren gefördert werden. Eine gesetzlich erzwungene Öffnung des Zugangs zu privat gehaltenen Daten oder die Schaffung eines neuartigen Eigentumsrechts für Daten, wie sie die EU-Kommission zur Diskussion gestellt hat, wären jedoch nicht nur unnötig, sondern würden auch den Innovationsstandort Europa ernsthaft gefährden. Das bestehende Kartell- und Vertragsrecht bietet zugleich die benötigte Flexibilität in einem sich dynamisch verändernden Umfeld und ausreichende Grundlagen, um missbräuchlichen Praktiken dominanter Marktteilnehmer Einhalt zu gebieten und einen fairen Interessenausgleich zwischen Anbietern und Kunden zu erzielen. Vielmehr sollte die Politik die Industrie dabei unterstützen, gemeinsame technische Normen zu entwickeln, um die Datenübertragung und Interoperabilität zwischen verschiedenen Systemen zu fördern. Dabei gilt es, nationale Insellösungen zu vermeiden und möglichst von Beginn an auf europäische bzw. internationale Lösungen zu setzen.

9 Verbraucherschutz in der digitalen Welt sichern ohne Innovationen zu gefährden

Entscheidende Kriterien für den Verbraucherschutz sollten einheitliche, verständliche sowie praxistaugliche Regeln sein. Die Durchsetzung des Verbraucherschutzes in der digitalen Welt bedarf einer kompetenten Aufsicht und konsequenter Rechtsdurchsetzung. Die jeweiligen (Rechts-) Instrumente müssen jedoch mit Bedacht angewandt und ausgelegt werden, um die Innovationsfähigkeit des Standorts Deutschland nicht zu gefährden.

Für den Verbraucher vereinfachen neue digitale Geschäftsmodelle alltägliche Dinge wie den wöchentlichen Supermarkteinkauf oder das Abwickeln von Finanzgeschäften radikal. Immer mehr Supermarktketten beispielsweise ermöglichen es dem Verbraucher, bequem von Zuhause oder unterwegs frische Lebensmittel zu bestellen und flexibel einen Liefertermin nach den eigenen Verfügbarkeiten zu wählen – unabhängig von starren Ladenöffnungszeiten. Auf Online-Marktplätzen kann der Verbraucher aus Sortimenten wählen, die die Größe und das Angebot klassischer Warenhäuser bei weitem übertreffen. Suchmaschinen und Vergleichsportale erlauben es dem Verbraucher gleichzeitig, eine Vielzahl unterschiedlicher Anbieter schnell und ohne großen Aufwand untereinander zu vergleichen und das beste Angebot zu finden.

Verbraucher profitieren dabei auch von neuen Möglichkeiten innovativer Datenanalyse: Die verbesserte Vergleichbarkeit von Preisen erhöht die Transparenz im Markt und erleichtert es so dem Kunden, den günstigsten Preis zu finden. Dies verstärkt den Preisdruck auf Unternehmen, die darauf unter anderem mit der Implementierung von Algorithmen reagieren, die im Falle einer Unterbietung durch Konkurrenten die eigenen Preise automatisch absenken. Eine häufig geäußerte Befürchtung ist dabei, dass Unternehmen mit Hilfe der Metadaten der Konsumenten die Zahlungsbereitschaft ihrer Kunden ermitteln und darauf aufbauend individualisierte Preise für die einzelnen Kunden anbieten. Wie Untersuchungen, zum Beispiel vom „Sachverständigenrat für Verbraucherfragen" zeigen, ist eine solche angebliche „Preisdiskriminierung" in der Praxis in Deutschland jedoch nicht zu beobachten.

Als informierter Verbraucher ist der Bürger im Gegenteil bestens dafür gewappnet, diese neue Markttransparenz für sich zu nutzen, sprich: Bewertungen zu lesen, Angebote zu vergleichen, Nutzungsbedingungen zu berücksichtigen und auch zu Wettbewerbern zu wechseln, um von besseren Konditionen zu profitieren. Die entscheidenden Kriterien für den Verbraucherschutz sollten deshalb einheitliche, verständliche sowie praxistaugliche Regeln sein. Hierzu gehört die effektive Gewährleistung der Informationspflichten, d. h. eine Offenlegung beispielsweise der Bewertungskriterien durch Vergleichsportale oder der Preisentwicklung. Hierzu gehört jedoch nicht die Veröffentlichung der von Anbietern genutzten Algorithmen. Sie sind wettbewerbsrelevante Geschäftsgeheimnisse, deren Preisgabe weitere Innovationen behindern würde.

Gleichzeitig dürfen zu weitreichende Transparenzvorgaben nicht zu einer Bevormundung der Verbraucher führen. Dadurch können Innovationen ausgebremst werden, die von den Verbrauchern nachgefragt werden, da sie schlussendlich davon profitieren. Hier sollte die Politik dem Verbraucher zutrauen, dass dieser in der Lage ist, die zahlreichen Möglichkeiten zur Information in Anspruch nehmen zu können und ggf. von seinem Widerrufsrecht Gebrauch zu machen.

Die Durchsetzung des Verbraucherschutzes in der digitalen Welt bedarf einer kompetenten Aufsicht und konsequenter Rechtsdurchsetzung. Der Ausbau der Kompetenzen der Datenschutzaufsichtsbehörden im Rahmen der Datenschutz-Grundverordnung und die Einführung eines Verbandsklagerechts im Datenschutz verbessern beide Bereiche zu Gunsten des Verbrauchers. Mit der Einrichtung des Marktwächters Digitale Welt sowie den Plänen zur Einführung einer Musterfeststellungsklage und der Erweiterung der Zuständigkeiten des Bundeskartellamts hin zu einer Verbraucherschutzbehörde im Internet werden weitere Maßnahmen ergriffen, um einen hohen Verbraucherschutzstandard durchzusetzen. Allerdings darf es hier nicht zu doppelten Zuständigkeiten kommen, da dies kein geeignetes Instrument ist, um die Rechtsdurchsetzung zu verbessern. Um die Digitalisierung der deutschen Wirtschaft und die Innovationsfähigkeit des Standorts nicht zu gefährden, müssen diese (Rechts-)Instrumente zudem immer mit Bedacht angewandt und ausgelegt werden. Gleichzeitig laufen sie Gefahr, politisch opportun für ordnungspolitische Eingriffe in den Wettbewerb zweckentfremdet zu werden, die das Wettbewerbsrecht aus guten Gründen nicht zulässt. Eine Kernaufgabe der nächsten Legislaturperiode wird es sein, die Gefahr eines solchen Missbrauchs zu unterbinden.

10 Digitalisierung im Bildungsbereich

Die Ausrichtung des Bildungswesens auf die Vermittlung digitaler Kompetenzen ist eine der dringendsten Aufgaben der Politik. Dies schließt technische Fähigkeiten ebenso wie kritischen Umgang mit Medien ein. Bildungseinrichtungen aller Art sollen daher konkrete Anreize und Zielvorgaben für den Einsatz digitaler Technologien und Medien erhalten. Nur so wird Deutschland seine Wettbewerbsfähigkeit auch in Zukunft sichern. Die Bundesregierung muss auch in einem föderalen Bildungssystem ihren Beitrag zur Verbesserung der digitalen Bildung leisten.

Der Einsatz digitaler Lernmittel soll dort gefördert werden, wo sich ein Mehrwert für Medienkompetenz, Eigenständigkeit und Lernmotivation ergibt. Rahmenbedingung hierfür ist eine leistungsfähige und sichere Infrastruktur: Breitbandinternet, WLAN, mobile Endgeräte. Außerdem brauchen Bildungseinrichtungen klare Leitlinien und professionelle Beratung, um den reibungslosen Betrieb ihrer Systeme und den verantwortungsvollen Umgang mit ihren Daten sicherzustellen.

Die Bundesregierung kann hier klare Zielvorgaben setzen, die Bundesländern und Bildungsträgern noch genügend Flexibilität in der Ausgestaltung lassen. Um diese Ziele flächendeckend effektiv umzusetzen, müssen Anreize für mehr Zusammenarbeit zwischen den Bundesländern geschaffen werden, auch durch eine Ausweitung der im Grundgesetz vorgesehenen Förderungsmöglichkeiten. Deutschlands Ausgaben für schulische Bildung müssen auf fünf Prozent BIP erhöht werden, um das Bildungswesen an die europäische Spitze zu bringen. Der digitalpakt#D ist eine gute Grundlage und sollte als Priorität umgesetzt werden. Digitalisierung darf dabei nicht gegen andere notwendige Investitionen, wie etwa in bauliche Modernisierung oder Betreuungsausbau, aufgerechnet werden.

Digitale Bildung beginnt mit der Förderung digitaler Kompetenzen in der Aus- und Weiterbildung von Lehrern. Lehrer sind am besten in der Lage zu beurteilen, wo digitale Lernmittel im Unterricht pädagogisch und didaktisch sinnvoll sind. Auch die Rolle des Lehrers und der Unterrichtsaufbau verändern sich durch den Einsatz digitaler Lernkonzepte. Es ist daher eine drängende Herausforderung für Bildungsträger, Lehrer unterschiedlicher Fachrichtungen, Berufserfahrung und persönlicher Motivation in die Lage zu versetzen, selbst digitale Kompetenzen zu vermitteln und digitale Technologien im Unterricht zu nutzen.

Der Einsatz digitaler Lernkonzepte und mobiler Endgeräte kommt vor allem denjenigen zugute, die mit konventionellen Bildungsmethoden und Materialien besondere Schwierigkeiten haben. Hierzu gehören nicht nur Menschen mit Körper- oder Lernbehinderungen oder fremdem Sprachhintergrund, sondern auch Kinder aus bildungsferneren Gesellschaftsgruppen. Digitale Lernkonzepte können individuelle Hilfestellung bieten, so dass jeder Lernende den gemeinsamen Lernstoff auf einem eigenen Weg erarbeitet. Dies verbessert den Lernerfolg, erhöht die Motivation und verringert Stigmatisierung und Ausgrenzung. Zudem wird ein erfolgreicheres Berufsleben und Selbstständigkeit in der Gesellschaft ermöglicht. Die Bundesregierung sollte daher in Leitlinien und Förderprogrammen insbesondere solche Konzepte fördern, die auf Integration und Inklusion bauen.

Coding ist eine Grundlagenkompetenz, die ermöglicht, sich in die Zusammenhänge der digitalen Kommunikation hineinzudenken – unabhängig davon ob diese Kompetenz später passiv oder aktiv genutzt wird. Die Entwicklung der Plattformwirtschaft hat bereits eine neue wirtschaftliche Dimension geschaffen, samt neuen Anforderungen an den Arbeitsmarkt. IT-Spezialisten, Programmierer und App Developer leisten sowohl als interne Angestellte, externe Dienstleister oder Selbständige wesentliche Beiträge zum Erfolg vieler Unternehmen. Angesichts der Fülle digitaler Medienformate wird auch eine grundlegende Medienkompetenz für jeden Bürger immer wichtiger. Einblicke in Grundlagen von Informatik und Algorithmen begünstigen die Fähigkeit zur Analyse, Bewertung und kritischen Rezeption digitaler Medien. Die Bundesländer sollten daher Grundlagen in Coding oder Computational Thinking in ihre Lehrpläne aufnehmen.

11 Arbeiten 4.0: Beschäftigung für eine digitale Zukunft sichern

Als bedeutende Industrienation besitzen Deutschland und die hier tätigen Unternehmen eine große Verantwortung, die Digitalisierung der Arbeitswelt in wirtschaftlicher und sozialer Hinsicht nachhaltig zu gestalten. Der digitale Wandel erfordert ein Umdenken bei allen Akteuren in der Arbeitswelt und einen grundlegenden Paradigmenwechsel in der Art und Weise, wie wir arbeiten.

Die heutige Wirtschaftskraft Deutschlands beruht in hohem Maße auf einem leistungsstarken, exportorientierten Industriesektor. Gleichzeitig haben die vergangenen industriellen Revolutionen gezeigt, dass Automatisierung vor allem im produzierenden Sektor ein extrem hohes Potential besitzt. Daraus ergeben sich zahlreiche Herausforderungen, wie die fortschreitende Digitalisierung der Arbeitswelt erfolgreich gestaltet werden kann: die bestehenden Arbeitsmarktstrukturen mit den neuen Berufsbildern und Unternehmensformen verzahnen, die Weiterbildung der heutigen Erwerbstätigen für die neuen Tätigkeitsprofile sicherstellen und die Arbeitskräfte von morgen richtig qualifizieren. Die Schaffung geeigneter Aus- und Weiterbildungsangebote für den digitalen Wandel ist ein entscheidender Schritt, um Deutschland global eine Vorreiterrolle in der Digitalisierung zu sichern. Diese müssen jedoch sowohl zeitlich als auch örtlich flexibel nutzbar sein.

Flexibilität zur Sicherung der Wettbewerbsfähigkeit des Standortes Deutschland kann durch die Politik in den kommenden vier Jahren aktiv befördert werden: Zum einen sollte das Arbeitszeitrecht modernisiert werden mit dem Ziel nicht unbedingt mehr, aber flexibel arbeiten zu können (Tageszeiten, Pausen, Wochenend- und Feiertage etc.). Aufgrund der zunehmenden Bedeutung projektbasierten Arbeitens sollten flexibel Beschäftigungsverhältnisse weiter möglich sein, wenn auch für die Beschäftigten sozialversicherungsrechtlich besser abgesichert.

Grundsätzlich sollte stets die Möglichkeit für Beschäftigte und ihre Auftrag- bzw. Arbeitgeber Vorrang haben ihre Leistungen und Pflichten zu regeln statt kollektiv für einen One-Size-fits-all-Ansatz zu versuchen, der die Möglichkeit von Flexibilität und Innovationskraft hemmt. Allgemein sollte – auch durch die Entwicklung digitaler Beteiligungsmöglichkeiten – die Beschäftigten individueller in Entwicklungs- und Entscheidungsprozesse eingebunden werden. Die unmittelbare Partizipationsmöglichkeit von Beschäftigten und Betrieben sollte im Vergleich zur traditionellen, kollektiven Rechtewahrnehmung der Sozialpartner oder einer komplexen Gesetzgebung gestärkt werden.

Über das Telecommunications, Internet, and Media (TIM) Committee

Das Telecommunications, Internet, and Media (TIM) Committee der Amerikanischen Handelskammer in Deutschland (AmCham Germany) vertritt als zentraler Ansprechpartner die Interessen der AmCham-Mitglieder der IKT-Branche. Die bearbeiteten Themen erstrecken sich vom Ausbau leistungsfähiger Kommunikationsinfrastrukturen über digitale Plattformen, künstliche Intelligenz und Cybersicherheit bis hin zum Abbau von Hürden für den Datenverkehr. Das TIM Committee repräsentiert derzeit mehr als 80 Mitgliedsunternehmen aus allen bedeutenden Bereichen der Telekommunikations-, Internet-, und Medienmärkte. Am Standort Deutschland umfasst der IKT-Sektor gegenwärtig rund 1,03 Millionen Beschäftigte, die Umsätze belaufen sich auf mehr als 160 Milliarden Euro pro Jahr.

Kontakt AmCham Germany Telecommunications, Internet, and Media (TIM) Committee

Chairs

Dr. Gunnar Bender
Director Public Policy DACH,
Amazon Deutschland Services GmbH

Mike Cosse
Vice President Government Relations, SAP SE

Dr. Nikolaus Lindner, LL.M.
Director, Head of Government Relations DE & EEC,
eBay Corp. Services GmbH

Staff Contact

Constanze Krüger
Manager, Government Relations
American Chamber of Commerce in Germany e. V.
Charlottenstrasse 42, 10117 Berlin
T +49 30 2130056-27
F +49 30 2130056-11
E ckrueger@amcham.de