Digitale Agenda und Cybersicherheit

Annegret Bendiek*

Im grenzüberschreitenden Waren-, Dienstleistungs- und Personenverkehr spielen digitale Informationssysteme, allen voran das Internet, eine wesentliche Rolle. Die fortschreitende Vernetzung macht es notwendig, gemeinsame datenschutzrechtliche und sicherheitspolitische Regelungen zu treffen. Dauerhaftes Vertrauen der Bevölkerung in Technologie und Rechtssicherheit ist unabdingbar. Fehlende Akzeptanz hätte negative wirtschaftliche Konsequenzen zur Folge. So schätzt die Europäische Kommission, dass die Vollendung des digitalen Binnenmarkts das europäische Bruttoinlandsprodukt um fast 500 Mrd. Euro steigern könnte.[1] Estland mit nur 1,3 Mio. Einwohner gilt als Vorreiter der Digitalisierung in Europa. Die nationale ‚e-ID'-Infrastruktur wird von nahezu allen Bürgern genutzt. Das Land hat weltweit acht Duplikate der eigenen digitalen Staatsverwaltung aufgebaut, die von den estnischen Botschaften betreut werden. Die IT-Infrastruktur dieser ‚Daten-Botschaften' wird mit Hilfe von privaten Unternehmen in befreundeten Staaten wie Großbritannien, Deutschland, den USA, Kanada, Südafrika und Japan betrieben.

Legt man das Konzept der positiven und negativen Integration (Fritz W. Scharpf) zugrunde, so gibt es zwei grundsätzliche Handlungsoptionen staatlicher (De-)Regulierung als Antwort auf die Erweiterung des Wirtschaftsraums über nationalstaatliche Grenzen hinaus. Negative Integration bedeutet, dass Beschränkungen des freien Handels (zum Beispiel Zölle) beseitigt werden. Diese Maßnahmen wirken marktschaffend. Positive Integration bedeutet den Einsatz wirtschaftspolitischer und regulatorischer Kompetenzen auf EU-Ebene, um Marktergebnisse zu korrigieren und Marktversagen zu überwinden. Maßnahmen der positiven Integration wirken marktkorrigierend. Die digitale Integration ist analog zur wirtschaftlichen Integration als der Ausbau einheitlicher gesellschaftlicher Handlungsräume zu verstehen, die gemeinsamen Regeln unterliegen und durch die Aufhebung von institutionellen Grenzen zwischen den Mitgliedstaaten gekennzeichnet sind. Die Regulierung des Marktes setzt grundsätzlich auf verschiedenen Ebenen an. Die globale Standardsetzung sollte in internationalen Foren erfolgen, der Datenschutz sollte einheitlich auf der EU-Ebene geregelt sein, und die Verfolgung digitaler Straftaten gehört auch auf die nationale Ebene (gegebenenfalls EU-weite Koordinierung). Daraus ergibt sich, dass die digitale Regulierung als eine Mehrebenenstruktur zu verstehen ist. Die Europäische Union ist aufgrund des Binnenmarkts nicht nur ein wichtiger Ort der Regulierung, sondern gleichzeitig auch ein starker wirtschaftlicher Akteur mit einer globalen Ambition zur digitalen Selbstbehauptung. Normen wie MP3, SMS, Halbleiter etc., die sich europäisch durchsetzen konnten, haben automatisch einen Anpassungsdruck auf nicht-europäische Marktteilnehmer entfalten können. Durch den Gemeinschaftsrahmen werden staatliche und nicht-staatliche Akteure in die Lage versetzt, globale Standardsetzung in einem Ausmaß zu beeinflussen, das einzelstaatlichem und privatem Handeln verwehrt bleibt.

* Die Autorin dankt Christoph Berlich und Tobias Metzger für die vielfältige Zuarbeit.

1 Europäische Kommission: Digital Agenda Review: Frequently Asked Questions, 18.12.2012, abrufbar unter: http://europa.eu/rapid/press-release_MEMO-12-1000_en.htm (letzter Zugriff: 16.6.2015).

Herausforderungen des digitalen Binnenmarkts

Die Herausforderungen bei der Schaffung eines digitalen Binnenmarkts lassen sich anhand des Datenweges einer E-Mail illustrieren. Mit welcher (1) Hard- beziehungsweise Software wird eine E-Mail geschrieben, über welche (2) Routinginfrastrukturen über das Internet übertragen, auf welchen (3) Datenservern und bei welchen Cloud-Anbietern gespeichert, dabei mittels welcher (4) Techniken verschlüsselt und durch welche (5) datenschutzrechtlichen und wettbewerbsrechtliche Vorgaben geschützt? Am Beispiel der digitalen Wegmarken lässt sich sowohl zeigen, dass es einen Regulierungsbedarf gibt als auch, dass die Europäische Union der angemessene Ort der Regulierung ist:

Erstens ist Europa in der Soft- und Hardware-Branche mit wenigen Ausnahmen wie SAP oder Alcatel-Lucent kaum noch ein relevanter Spieler. Die europäische Industrie ist zu einem so hohen Maß von US-amerikanischen und chinesischen Komponenten abhängig, dass ein vollkommen eigenständiger europäischer Markt nicht vorstellbar ist. Viele der Branchen wie Suchmaschinen befinden sich derzeit im Zustand eines Quasi-Monopols, indem sie von Microsoft, Google, Cisco oder Huawei dominiert werden. Zu den führenden PC-Herstellern zählen Apple, DELL, HP (alle USA), MSI, ASUS, Acer (alle Taiwan), Samsung (Südkorea), Lenovo (China) und Toshiba (Japan). Gleichzeitig sind einige dieser Hersteller auch beim Verkauf von Smartphones in der Weltspitze vertreten, wobei Huawei (China) und LG (Südkorea) hinzukommen. Die Hardwarekomponenten eines Heimnetzwerks kommen weltweit hauptsächlich aus dem Hause Cisco (USA) oder Huawei (China). Bei Server-Hardware der Rechenzentren wiederum liegt HP vor Dell und IBM. Durch den Rückgang des Marktanteils europäischer Anbieter (Siemens, Nokia) besteht de facto eine Duopolstellung zwischen US-amerikanischen und asiatischen Anbietern (Huawei, ZTE).

Zweitens setzt ein verlässliches europäisches Kommunikationsnetz voraus, dass es im öffentlichen Interesse betrieben und verwaltet wird und dass Einzelinteressen nur dort ihren Platz finden, wo sie das allgemeine Interesse nicht verletzen. In Europa ist heute genau das Gegenteil der Fall. Das Netz setzt sich zusammen aus nationalen Teilnetzen mit Kontrolleuren, die jeweils partikulare Interessen verfolgen. In der Theorie besteht das Internet aus den Netzen verschiedener Internetdienstanbieter (ISPs), welche an neutralen Stellen (Internetknotenpunkten) zum Gesamtnetz, dem Netz von Netzen, zusammengeschlossen sind. In der Praxis kann von Neutralität keine Rede sein. DE-CIX ist der größte der weltweit 321 Internetknotenpunkte und gehört dem Verband der deutschen Internetwirtschaft eco. Er wird in einer Weise betrieben, die dem Bundesnachrichtendienst Zugriffsmöglichkeiten erlaubt, wobei auch die Daten nicht-deutscher Akteure betroffen sind. Ob hier das europäische Interesse gewahrt bleibt, kann bezweifelt werden.

Drittens stellen sich im Bereich des Cloud Computing, der verteilten Bearbeitung und des Speicherns von Daten vielfältige neue Anforderungen. Für wichtige Fragen der positiven Regulierung im Bereich des EU-Konsumenten- und Datenschutzes entsteht das Problem des Auseinanderfallens von rechtlichen und ökonomischen Räumen. Europäische Gesetze greifen dort ins Leere, wo Daten und Zugriffe auf Daten an Orten jenseits der Gültigkeitsreichweite des EU-Rechts liegen. Daten, die auf Cloud-Plattformen abgelegt werden, können dort unerlaubt abgegriffen werden. Gefahren lauern etwa bei außereuropäischen Servern im großangelegten Datendiebstahl oder in Geschäftsbedingungen, die dritten Akteuren Zugriffsrechte auf Inhalte einräumen können. Die Rechtsunsicherheit brachte bereits einige von staatlicher Überwachung betroffene amerikanische Internetfirmen beziehungsweise Cloud-Anbieter in Schwierigkeiten. Demnach müssen amerikanische Anbieter die auf europäischen Servern gespeicherten Kundendaten auf Anfrage

herausgeben (Streitfall irische Tochtergesellschaft von Microsoft versus US-Regierung), aber auch europäische Firmen, die in den USA tätig sind, unterliegen dieser Verpflichtung.

Viertens hat die Digitalisierung der Kommunikation dazu geführt, dass das Recht auf Privatheit nicht mehr in dem nötigen Umfang gewährleistet ist. Die Snowden-Veröffentlichungen haben gezeigt, dass staatliche Sicherheitsbehörden in der Lage sind, unverschlüsselte E-Mails zu jedem Zeitpunkt auszuwerten. Die Güter der Privatheit und Freiheit sind eine wichtige Voraussetzung für den Markt selber, und diese zu schützen liegt im eigenen Interesse desselben. Für liberale Gesellschaften ist das Recht auf Privatheit allerdings konstitutiv. Ohne Privatheit kann es auch keine Freiheit geben. Es bedarf einer europäischen Antwort auf die Gefährdung privater Daten und damit der gesellschaftlichen Freiheit. Da sich die Telekommunikationsinfrastruktur in privatwirtschaftlichem Besitz befindet und Netze Ländergrenzen überschreiten, liegt derzeit der Fokus auf verbesserten Verschlüsselungsverfahren. Voraussetzung ist jedoch, dass die Verschlüsselungstechnologie keine derartigen Zugriffsmöglichkeiten bereithält, welche zuletzt nicht nur von der chinesischen, sondern auch von den US-amerikanischen und britischen Regierungen für Ermittlungszwecke gefordert wurden. Doch auch aus verschlüsselten E-Mails lassen sich viele Infos ablesen. Die Metadaten, quasi der Briefumschlag einer E-Mail, verraten wer mit wem, wann und wie häufig in Kontakt steht, ja sogar den Betreff der Nachricht.

Fünftens sind Quasi-Monopolstellungen großer Unternehmen grundsätzlich problematisch. Kartellbildungen oder andere Formen der Marktbeherrschung führen bekanntermaßen zu Missbrauch, höheren Preisen, schlechteren Produkten und anderen gravierenden Abweichungen vom Ideal des freien Marktes. Es gibt zwar Fusionskontrollen, jedoch reagiert das EU-Wettbewerbsrecht erst dann mit Sanktionen, wenn Marktbeherrschung auch faktisch zu Missbrauch führt. Anders ausgedrückt: Europa reagiert erst dann, wenn ‚das Kind in den Brunnen gefallen ist'. Trotzdem wird die Frage einer marktbeherrschenden Stellung des US-Unternehmens Google im europäischen Markt durch die bevorzugte Listung eigener Angebote in seinen Suchergebnissen prominent diskutiert. Der ehemalige Wettbewerbskommissar Joaquín Almunia hat schon vor mehr als vier Jahren ein Verfahren gegen Google eingeleitet. Seine Nachfolgerin Margrethe Vestager hat es nun wiederbelebt. Nach ihrer Auffassung sprechen viele Fakten dafür, dass Google bei der allgemeinen Internetrecherche systematisch eigene spezialisierte Einkaufs-Suchdienste gegenüber Konkurrenzprodukten bevorzugt. Zudem geht die Wettbewerbskommissarin gegen mehrere Staaten vor, weil diese möglicherweise Konzerne wie Amazon oder Apple durch Steuervorentscheide (‚tax rulings') bevorzugen. Diese sind zumindest dann wettbewerbswidrig, wenn einzelne Unternehmen auf Kosten ihrer Konkurrenten bevorzugt werden.

Die digitale Gesamtstrategie

Regulatorische Herausforderungen, wie jene, die am Beispiel der digitalen Wegmarken veranschaulicht wurden, haben in der europäischen Geschichte oft zu qualitativ anspruchsvollen Integrationssprüngen wie zum Beispiel dem Deutschen Zollverein oder der gemeinsamen Handelspolitik beigetragen. Mit dem Amtsantritt der neuen Juncker-Kommission haben der für diesen Bereich zuständige Vizepräsident und Kommissar, Andrus Ansip, und sein Kollege Günther Oettinger, der die digitale Wirtschaft und Gesellschaft betreut, Anfang Juni 2015 ihre Gesamtstrategie zur Schaffung eines digitalen Binnenmarkts vorgestellt. Ziel ist es letztlich, die Vorzüge des europäischen Binnenmarkts auf den digitalen Raum auszuweiten. Man könne von den technischen Neuerungen rund um Big Data, Cloud-Computing und das Internet der Dinge (IoT) nur dann profitieren, wenn jüngst

erklärte Ideen einer technologischen Souveränität zugunsten einer Harmonisierung von nationalen Märkten überwunden werden. Die Strategie der Kommission für einen digitalen Binnenmarkt beruht auf drei Säulen: (1) besserer Zugang für Verbraucher und Unternehmen zu digitalen Waren und Dienstleistungen in ganz Europa, (2) Schaffung der richtigen Bedingungen und gleichen Voraussetzungen für florierende digitale Netze und innovative Dienste und (3) bestmögliche Ausschöpfung des Wachstumspotenzials der digitalen Wirtschaft. Die jüngsten Gesetzesinitiativen beziehen sich auf den grenzüberschreitenden E-Commerce und eine Reform der Richtlinie über audiovisuelle Mediendienste mit neuen Vorgaben vor allem für Video-Plattformen im Internet.

1. Säule

Mithilfe der Maßnahmen der ersten Säule sollen Unternehmen gegenüber dem nationalen Handel künftig keinen beziehungsweise nur kleinstmöglichen Hemmnissen im digitalen Binnenmarkt unterliegen. Hierzu sollen das Vertragsrecht oder Mehrwertsteuer-Regelungen harmonisiert oder grenzübergreifende Paketlieferdienste verbessert werden. Die Kommission will so gegen „Diskriminierung auf Basis von Wohnort, Niederlassung oder Nationalität im Binnenmarkt" vorgehen. Durch den entsprechenden Verordnungsentwurf werden grenzüberschreitende Paketzustelldienste preislich transparenter und stärker beaufsichtigt. Zudem zielt die Initiative darauf ab, Zugriffseinschränkungen (Geo-Blocking) zu entfernen, indem urheberrechtliche Fragestellungen auf EU-Ebene vereinheitlicht beantwortet werden. An den Vertrieb von urheberrechtsgeschützten Online-Inhalten wie Musik, Filme oder E-Books soll gemäß eines bereits im Rat behandelten Rechtsaktes das Geo-Blocking zunächst erst einmal für die begrenzte Mitnahme legal erworbener Dienste auf Reisen in andere EU-Staaten gelockert werden. Der Verordnungsentwurf zum grenzüberschreitenden E-Commerce verpflichtet Händler, Kunden aus anderen EU-Staaten nicht mehr den Zugang zu ihren Online-Plattformen zu verwehren. Angebote dürfen demnach auch nicht mehr abhängig von der Herkunft beziehungsweise der IP-Adresse ihrer Kunden unterschiedlich gepreist werden. Die Kommission will zudem die Europäische Cloud-Initiative umsetzen und hierzu folgende Maßnahmen ergreifen:[2]

(1) Ab 2016: Schaffung einer Europäischen Cloud für Forscher und ihre weltweiten Wissenschaftspartner durch die Integration und Konsolidierung von e-Infrastruktur-Plattformen, die Verknüpfung bereits vorhandener wissenschaftlicher Clouds und Forschungsinfrastrukturen durch die Unterstützung der Entwicklung cloudgestützter Dienste.

(2) 2017: Alle wissenschaftlichen Daten, die im Rahmen des mit 77 Mrd. Euro ausgestatteten Forschungs- und Innovationsprogramms Horizont 2020 generiert werden, sollen standardmäßig offen zugänglich werden.

(3) 2018: Start der Flaggschiff-Initiative, um die neuen Entwicklungen im Bereich der Quantentechnologie zu beschleunigen.

(4) Bis 2020: Entwicklung und Einführung einer europäischen Großinfrastruktur für Hochleistungsrechner, Datenspeicher und Netze, der Erwerb von zwei Prototypen von Hochleistungsrechnern sowie der Aufbau eines europäischen Big-Data-Zentrums und die Modernisierung des Kernnetzes für Forschung und Innovation (GEANT).

2 Europäische Kommission: Mitteilung an die Presse. Die Europäische Cloud-Initiative – damit Europa in der Datenwirtschaft weltweit führend wird, 19. April 2016.

2. Säule

Mit den Maßnahmen der zweiten Säule „Regulatorische Klarheit" setzt die Kommission auf neue Gesetzgebungsakte zur positiven, das heißt eine dem EU-Binnenmarkt einen politischen Ordnungsrahmen gebende Integration. Doch diese Akte erfordern die Zustimmung einer großen Zahl politischer Akteure mit unterschiedlichsten Interessen und Zielen, die angesichts verschiedener nationaler Politikmodelle oft nur schwer zu erreichen sein werden. Um den Wettbewerb anzukurbeln, muss Klarheit darüber bestehen, welche Handlungen gesetzlich verpflichtend beziehungsweise zu unterlassen sind. Mit der Initiative zu den audiovisuellen Mediendiensten sollen geltende Bestimmungen für TV-Sender auf neue Dienste wie YouTube und Video-on-Demand-Angebote ausgedehnt werden. Auflagen für Kinder- und Jugendschutz sollen freiwillig auf Video-Plattformen erweitert werden. Verfahren, mit denen rechtswidrige Inhalte im Netz gelöscht werden, will die Europäische Union ebenfalls vereinheitlichen. Damit sind „Informationen, die dem öffentlichen Interesse zuwiderlaufen" und terroristische Propaganda, Kinderpornographie und Urheberrechtsverstöße, gemeint. Im Dezember 2015 hat die Kommission ein neues Urheberrecht vorgeschlagen, um das Leistungsschutzrecht, die Panoramafreiheit und eine stärkere Copyright-Durchsetzung EU-weit anzugleichen. Mit dem Entwurf zur Reform von Verbraucherschutzregeln sollen nationale Behörden mehr Befugnisse erhalten, betrügerische Webseiten sofort zu blockieren. Beim Verkauf gefälschter Tickets sollen Aufsichtsbehörden Sanktionen verhängen dürfen. Nicht zuletzt hat die Kommission ihr Wettbewerbsverfahren gegen Google erweitert. Unter anderem schränke der Konzern die Möglichkeiten von Unternehmen ein, auf ihren Webseiten Suchmaschinenwerbung von Googles Wettbewerbern anzuzeigen. In dem Verfahren geht es ferner um Shopping-Angebote und das weltweit dominierende Smartphone-Betriebssystem Android. Bei Wettbewerbsverfahren drohen dem Konzern von bis zu 10 Prozent des Jahresumsatzes an Strafzahlungen.

3. Säule

In der dritten Säule zu „Industrie 4.0 und die europäische digitale Wirtschaft" geht es sowohl um den Ausbau der europäischen digitalen Wirtschaft, das heißt derjenigen Unternehmen, deren Geschäftsbasis das Internet ist, als auch um die Nutzung von Digitaltechnik in der herkömmlichen Industrie. In Bezug auf Anbietern von Informations- und Kommunikationstechnik (IKT) legt die Strategie ein besonderes Augenmerk auf mittelständische Unternehmen (SME) und Neugründungen (Start-Ups). Das Angebot an IKT-Sicherheitsprodukten und -diensten im Binnenmarkt ist nach wie vor geografisch stark zersplittert. Darum ist es für europäische Unternehmen schwierig, auf diesem Feld international wettbewerbsfähig zu sein. Die Zertifizierung ist entscheidend für Vertrauen in IT-Produkte und Dienste und deren Sicherheit. Verstärkte nationale Initiativen zeigen zwar, dass die Bedeutung einer Zertifizierung anerkannt wird, unterschiedliche Standards im Binnenmarkt können aber Interoperabilitätsprobleme verursachen. Nur in wenigen EU-Staaten gibt es wirksame Zertifizierungsprogramme für die Sicherheit von IKT-Produkten. IKT-Anbieter müssen daher unter Umständen mehrere Zertifizierungsverfahren durchlaufen, um ihre Produkte gleichzeitig in mehreren EU-Staaten verkaufen zu können. Die Schaffung eines IKT-Sicherheitszertifizierungsrahmens auf EU-Ebene bleibt ein langfristiges Ziel.

EU-Strategie zur Cybersicherheit

Die Digitalisierung von Infrastruktur, Wertschöpfungsketten und Lebenswelt eröffnet nicht nur Chancen, sondern birgt auch Risiken. Immer wieder lässt sich beobachten, wie anfällig

zum Beispiel kritische Infrastrukturen sind. Nach Untersuchungen der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) nehmen Sicherheitsvorfälle im Cyberraum mit alarmierender Geschwindigkeit zu. Die Zahl der Sicherheitsvorfälle in der gesamten Wirtschaft nahm 2015 weltweit im Vergleich zum Vorjahr um 38 Prozent zu.

Die Angreifer können die Bereitstellung grundlegender Dienste wie Wasserversorgung, Gesundheitsfürsorge, Strom oder Mobilfunk stören oder sabotieren. Sicherheit im Cyberraum lässt sich nur durch konzertiertes Handeln von Wirtschaft, Politik und Gesellschaft erreichen.[3] Die erste EU-Cybersicherheitsstrategie[4], die im Februar 2013 präsentiert wurde, und die im Dezember 2015 vom Rat angenommene EU-Richtlinie für Netz- und Informationssicherheit (NIS) folgen diesem Multi-Stakeholder-Ansatz.[5] Zusammen mit dem Anfang 2013 eröffneten, bei EUROPOL angesiedelten Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3) legen diese Initiativen den Grundstein, gegen Cybergefahren vorzugehen.[6] Ziel ist es, europaweite Sicherheitsstandards zu gewährleisten und die bestehenden Grundrechte und -werte zu wahren. Die Kommission hat hierzu einen Aktionsplan angekündigt, um die Abwehrfähigkeit der Europäischen Union weiter zu stärken und die europäische Cybersicherheitsbranche zu fördern. Zu den Maßnahmen zählen:[7]

> „(1) Ausbau der europaweiten Zusammenarbeit: Die Kommission bestärkt die Mitgliedstaaten darin, die Kooperationsmechanismen, die im Rahmen der künftigen Richtlinie über Netz- und Informationssicherheit (NIS) geschaffen werden, bestmöglich zu nutzen und die Art und Weise, wie sie zusammenarbeiten und sich auf einen großen Cybervorfall vorbereiten, zu verbessern. Dazu gehören auch verstärkte Bemühungen um die Aus- und Weiterbildung und Übungen zur Cybersicherheit (wie die CyberEurope-Übungen der ENISA).
>
> (2) Förderung des entstehenden Binnenmarkts für Cybersicherheitsprodukte und -dienste in der EU: Die Kommission wird beispielsweise die Möglichkeit der Schaffung eines Zertifizierungsrahmens für IKT-Produkte und -Dienste ausloten, der durch ein freiwilliges und handliches Kennzeichnungssystem für die Sicherheit von IKT-Produkten ergänzt werden soll. Außerdem schlägt sie mögliche Maßnahmen für mehr Investitionen in die Cybersicherheit in Europa und Unterstützungsmaßnahmen für auf diesem Markt tätige KMU vor.
>
> (3) Einrichtung einer vertraglichen öffentlich-privaten Partnerschaft (cPPP) mit der Branche für den Ausbau der Kapazitäten der Cybersicherheitsbranche und die Innovationsförderung in der EU."

In Deutschland wurde mit dem IT-Sicherheitsgesetz im Juli 2015 eine Meldepflicht für verschiedene privatwirtschaftliche Branchen im kritischen Infrastrukturschutz eingeführt.[8] Mit seinen wegweisenden Regelungen hat das deutsche IT-Sicherheitsgesetz eine Vorreiterrolle in der Europäischen Union inne und setzt wichtige Akzente für die Ausgestaltung der EU-Richtlinie zur NIS. Diese soll die IT bei Betreibern kritischer Infrastrukturen und großen Online-Dienstleistern sicherer machen und wird die betroffenen Firmen

3 Europäische Kommission: Mitteilung an die Presse. Kommission als ehrlicher Mittler bei künftigen internationalen Verhandlungen über die Internet-Governance, 12. Februar 2014.

4 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Europäischen Ausschuss der Regionen. Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum, JOIN (2013) 1 final.

5 European Commission: Proposal for a directive of the EP and the Council concerning measures to ensure a high common level of Network and Information Security across Europe, COM (2013) 48 final.

6 Europol: Combating Cybercrime in a Digital Age, abrufbar unter: https://www.europol.europa.eu/ec3 (letzter Zugriff: 16.6.2015).

7 Europäische Kommission: Factsheet. Kommission gibt Impulse für Cybersicherheitsbranche und verstärkt Bemühungen zur Bewältigung von Cyberbedrohungen, MEMO/16/2322.

8 Deutscher Bundestag: Bundestagsbeschlüsse am 11. und 12. Juni, 12. Juni 2015, abrufbar unter: http://www.bundestag.de/dokumente/textarchiv/2015/kw24_angenommen_abgelehnt/377456 (letzter Zugriff: 16.6.2016).

verpflichten, Sicherheits- und Datenschutzvorfälle sowie IT-Angriffe zu melden. Die Auflagen sollen für sämtliche Betreiber und Anbieter ‚essentieller Dienste' gelten, etwa in den Bereichen Energie, Wasserversorgung, Transport, Finanzwesen, Gesundheit und Internet. Im Entwurf werden Verkehrsknoten, Domain-Regierungsstellen, Online-Marktplätze und Suchmaschinen aufgeführt, nicht aber soziale Netzwerke. Kleine Digitalfirmen sollen ebenfalls außen vor bleiben. Sobald die Richtlinie in Kraft getreten ist, müssen alle EU-Staaten nationale Meldesysteme aufbauen und Informationen untereinander austauschen.

Durch die kommende NIS-Richtlinie werden zwei Koordinierungsmechanismen geschaffen: Erstens eine Kooperationsgruppe, die den Informationsaustausch über Cybervorfälle zwischen den EU-Staaten unterstützen soll, und zweitens ein Netzwerk der IT-Noteinsatzteams (CSIRT), um die operative Zusammenarbeit bei konkreten Cybersicherheitsvorfällen und den Informationsaustausch über Risiken zu erleichtern. 2017 will die Kommission ein Konzept vorstellen, in dem sie einen koordinierten Ansatz für die Krisenzusammenarbeit im Fall eines großen Cybervorfalls darlegen wird. Darin würden EU-Einrichtungen wie ENISA, das IT-Notfallteam der Europäischen Union (CERT-EU) und das bei Europol angesiedelte Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3) ebenso eine Rolle spielen wie das CSIRT-Netzwerk.

Die ENISA spielt für die Cybersicherheit in der Europäischen Union eine zentrale Rolle, indem sie bei der Bewältigung, Abwehr und Vorbeugung von NIS-Problemen eng mit den Mitgliedstaaten, den EU-Organen und dem Privatsektor zusammen arbeitet. Hierzu zählt etwa die Leitung europaweiter Übungen zur Cybersicherheit, die Bereitstellung wichtiger Informationen über NIS-Probleme, ihr jährlicher Bericht über die Bedrohungslage im Cyberraum sowie die Ausbildung. Die Kommission muss bis Juni 2018 eine Bewertung der ENISA vornehmen, um die Änderung oder Erweiterung ihres Mandats, das im Jahr 2020 ausläuft, zu beurteilen. Angesichts der derzeitigen Cybersicherheitslage und der Implementierung der Richtlinie über Netz- und Informationssicherheit soll die Bewertung zeitlich vorgezogen werden. Kontinuierliche Zusammenarbeit zwischen öffentlichen und privaten Akteuren beim Austausch von Sicherheitsvorfällen ist wichtig, um angemessen auf Bedrohungen aus dem Cyberraum reagieren zu können. Hierzu wurde am 13. Juni 2016 die Europäische Cybersicherheitsorganisation (ECSO) in Brüssel gegründet. Die ECSO ist eine Vereinigung ohne Gewinnerzielungsabsicht nach belgischem Recht. Sie steht unter der Federführung der Branche. Zu den Mitgliedern zählen europäische Großunternehmen, KMU und Startups, Forschungszentren, Hochschulen, Cluster und Vereinigungen sowie lokale, regionale und nationale Verwaltungen in der Europäischen Union und dem Europäischen Wirtschaftsraum (EWR), der Europäischen Freihandelsassoziation (EFTA) und den mit Horizont 2020 assoziierten Ländern. Die Gründungsmitglieder sind die Europäische Organisation für Sicherheit (EOS), die Alliance pour la Confiance Numérique (ACN), Guardtime (im Namen des Estnischen IKT-Verbands) und Teletrust.[9] Die Europäische Union wird 450 Mio. Euro in diese Partnerschaft investieren, und zwar im Rahmen von Horizont 2020. Von den Akteuren des Cybersicherheitsmarkts, vertreten von der ECSO, wird erwartet, dass sie ihrerseits die dreifache Summe investieren.

Datenschutz als Standortvorteil

Der Schutz vertraulicher Daten, die aufgrund mangelnder Sicherheitsvorkehrungen oder nachteiliger rechtlicher Rahmenbedingungen in die Hände Dritter gelangen können, gilt

9 Weitere Informationen über ESCO ist abrufbar unter: http://www.ecs-org.eu/ (letzter Zugriff: 25.8.2016).

als Hauptaugenmerk der EU-Regulierungen. Restriktive Gesetze zum Datenstandort oder zu Verschlüsselungsverfahren will sie vereinheitlichen. Ein Vorschlag plädiert für eine Infrastruktur des Schengen-Routing, damit alle europäischen Marktteilnehmer in jeder Hinsicht gleich behandelt werden. Denn die Verteilung von Datenpaketen (Routing) – beispielsweise Kommunikation zwischen Estland und Italien – kann durchaus über US-amerikanische Server erfolgen. Die Implikation einer solchen Datenverbindung für den Datenschutz riefen daher vermehrt Verfechter eines Schengen-Routing auf den Plan. Dies ist allerdings aus Gesichtspunkten der Ausfallsicherheit und Ökonomie problematisch. Die US-Handelsbehörde USTR sieht darin – trotz vergleichbarer Regelungen in den USA – eine Verletzung internationaler Handelsvereinbarungen. Überzeugender ist ein Vorschlag der ENISA. Sie hat Möglichkeiten der Ende-zu-Ende-Verschlüsselung für verschiedene Anwendungen sowie Verschleierungsmethoden für Metadaten mit Hilfe von ‚Virtual Privat Network'-Verbindungen (VPN) oder Onion-Routing vorgestellt. Eine E-Mail würde beispielsweise in einer sogenannten ‚Dark Mail' mehrfach verschlüsselt. Die verschiedenen Verschlüsselungsschichten legen sich dann wie Briefumschläge um die eigentliche Nachricht und jede beteiligte Stelle kann nur auf diejenigen Informationen zugreifen, die sie unbedingt benötigt, um die Nachricht weiterzuleiten.

Die erste EU-Datenschutzrichtlinie aus dem Jahr 1995 verfolgt die gleichberechtigten Ziele, einerseits für den „Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten" und andererseits für den „freien Datenverkehr" zu sorgen. In der Folge wurden nationale Datenschutzgesetze insbesondere in den neuen EU-Staaten verabschiedet und bestehende Grundlagen der alten an die EU-Anforderungen angepasst. Im Jahr 2002 folgte die Datenschutzrichtlinie für elektronische Kommunikation (ePrivacy-Richtlinie) sowie 2009 die ergänzende Cookie-Richtlinie, doch werden mit beiden keine ausreichenden Schutzbestimmungen für ‚Big Data'-Analysen geschaffen. Hier werden allein Bestimmungen zum Schutz personenbezogener Daten wie durch entsprechende Cookies erhobene Daten bei der individuellen Internetnutzung festgelegt. Mit dem richtungsweisenden Urteil des Gerichtshofes der Europäischen Union (EuGH) zu Facebook aus dem Jahr 2013, zur Vorratsdatenspeicherung vom April 2014 und zum Recht auf Vergessenwerden vom Mai 2014 hat eine grundlegende Überprüfung aller Vorgaben in Bezug auf die Angemessenheit ihrer Vorkehrungen zu Datensicherheit und Datenschutz begonnen. Im Lichte des ‚Safe Habor'-Urteils des EuGH vom Oktober 2015 wurde bestimmt, dass Standardvertragsklauseln, verbindliche Unternehmensregeln sowie Einwilligungen derjenigen Personen, deren Daten übermittelt werden, alle zu überprüfen sind.

Mitte Dezember 2015 haben sich Parlament, Rat und Kommission auf eine neue Datenschutz-Grundverordnung (DS-GVO) der Europäischen Union geeinigt. Der Innen- und Justizausschuss hat diese Einigung mit großer Mehrheit von 48 Ja-Stimmen bei vier Nein-Stimmen und vier Enthaltungen angenommen. Der Rat und das Plenum des Parlaments müssen noch final zustimmen. Damit wird die erste umfassende Reform des EU-Datenschutzrechts seit 1995 in Kraft treten. In über 700 Sitzungsstunden der drei Jahren andauernden Verhandlungen wurden unter dem Berichterstatter des Europäischen Parlaments, Jan-Philipp Albrecht, mehr als 2.000 Änderungsvorschläge diskutiert; im Bundesinnenministerium war eine rund 340-köpfige Task Force mit der DS-GVO befasst. Mit Zustimmung von Rat und Parlament wird die Verordnung Anfang 2018 in Kraft treten und unmittelbar in nationales Recht umzusetzen sein. Die Verordnung wird damit den Flickenteppich vorheriger Regelungen in den 28 Mitgliedstaaten ablösen. Sie gilt für den gesamten privaten und öffentlichen Bereich. Ausgenommen ist lediglich der Bereich von Polizei und Justiz, für den gleichzeitig eine neue Datenschutzrichtlinie verhandelt wurde. Verordnung

und Richtlinie werden auch richtungsweisend für die Verhandlungen mit den USA über ein neues Abkommen zum Datentransfer und Datenschutz sein.

Mit der DS-GVO wird es erstmals ein einheitliches und verbindliches EU-weites Schutzniveau geben. So soll die Wettbewerbskonkurrenz um die niedrigsten Schutzbestimmungen in der Europäischen Union vermieden werden. ‚Europäisches Recht auf europäischen Boden' lautet das Leitmotiv der Kommission. Die Neuregelung sieht grob vor, dass Internetkonzerne in Zukunft die ausdrückliche Zustimmung der Nutzer einholen müssen, wenn sie deren Daten verwenden wollen. Nutzer erhalten zudem das Recht, gespeicherte Informationen leichter wieder löschen zu lassen (Recht auf Vergessenwerden) und Daten von einem Anbieter zum nächsten mitzunehmen (Portabilität). Unternehmen müssen ihre Produkte datenschutzfreundlich voreinstellen (Privacy by Design und by Default). Wettbewerbsverzerrungen im Binnenmarkt durch Monopolbildungen sollen durch neue Anforderungen an ‚Privacy by Design' und ‚Security by Design' verringert werden, indem IT-Produkte gefördert werden sollen, die durch ihre technologische Ausgestaltung die Einhaltung des Datenschutzes erleichtern. Anerkannte Prüfverfahren und Datenschutzgütesiegel wie das European Privacy Seal von EuroPriSe existieren bereits und sollen gerade mittelständische Unternehmen auf dem hart umkämpften Markt vor allem gegenüber der übermächtigen amerikanischen und auch asiatischen Konkurrenz gestärkt werden.

An die neuen Regeln müssen sich nicht nur europäische Unternehmen halten, sondern auch Firmen aus Drittstaaten wie den USA. Wenn Anbieter dagegen verstoßen, drohen hohe Strafen von bis zu 4 Prozent des weltweiten Jahresumsatzes eines Unternehmens. Hat ein Verbraucher ein Problem mit dem Anbieter in einem anderen EU-Land, soll er sich künftig in seiner Sprache an die heimische Beschwerdestelle wenden können. Datenschutzbehörden nehmen als Beschwerde und Kontrollstelle eine immer wichtigere Funktion wahr, weil sie darauf achten, wie mit personenbezogenen Daten in der Informationsgesellschaft umgegangen wird und Sanktionen veranlassen können. Umso wichtiger ist es, deren Unabhängigkeit zu stärken und Einflussnahme seitens privatwirtschaftlicher Unternehmen zu begrenzen. Der EuGH hat in zwei Urteilen (2010, 2012) die Notwendigkeit der ‚völligen Unabhängigkeit' von Datenschutzbeauftragten und ihren Behörden betont.

Die derzeitige Rechtslage verbietet es, personenbezogene Daten aus EU-Staaten in Länder zu übertragen, die nicht über einen mit dem EU-Recht vergleichbaren Datenschutz verfügen. Daten-Portabilität ist ein wichtiges Thema, da das europäische Verfassungsverständnis nicht identisch mit dem der USA ist. Ihr Fokus ist nicht primär auf den Schutz der Menschenwürde, sondern auf Freiheit im Sinne von ‚liberty' als Bürgerrecht des Individuums, das „frei sein will von gesetzlicher Regulierung". Die neue DS-GVO soll aber Garantierechte für EU-Bürger bei der Rechtsbeihilfe durchsetzen und wird daher Auswirkungen auf alle derzeit zu verhandelnden bilateralen Abkommen mit den USA zum Datentransfer im Sicherheits- und Wirtschaftsbereich (unter anderem Safe Harbor, Rahmenabkommen zum Datenschutz, bilaterales Rechtshilfeabkommen, Austausch von Fluggastdaten) haben.

Europa in der digitalen Welt

Die EU-Regelsetzung lässt sich zwangsläufig nicht unabhängig vom Rest der Welt und damit dem Rahmen des EU-Binnenmarkts denken. Die europäische Informations- und Kommunikationswirtschaft ist hochgradig verflochten mit anderen Märkten. Um diesen wechselseitigen Abhängigkeiten der europäischen und globalen Standard- und Regelsetzung Rechnung zu tragen, sind die Kommission und einzelne EU-Staaten in internationalen Gremien zu den zentralen Themen Internet Governance und Cybersicherheit aktiv.

Die digitale Integration umfasst daher auch die außenpolitischen Dimensionen staatlicher Politik, die nicht nur auf die Erweiterung des digitalen Binnenmarkts über nationale Grenzen hinaus, sondern auch auf die Cyberaußen- und Sicherheitspolitiken der EU-Staaten gerichtet sind. In diesem Sinne wird sich in den Ratsschlussfolgerungen zur Internet Governance vom November 2014 sowie in denen zur Cyberdiplomatie vom Februar 2015 für den Multistakeholder-Ansatz ausgesprochen, nach welchem Regierungen, Vertreter der Wirtschaft und der technischen Community, der Wissenschaft und der Zivilgesellschaft gleichermaßen Berücksichtigung finden sollen, und eine enge Cyberdiplomatie mit den USA, zum Beispiel in Bezug auf die Group of Governmental Experts (GGE) auf Ebene der Vereinten Nationen (VN), stattfinden soll.

Unter Internet Governance wird sinngemäß die Entwicklung und Anwendung gemeinsamer Prinzipien, Normen und Vorgehensweisen bei der globalen Kommunikation verstanden. Sie wird mit der NETmundial-Konferenz 2014 und mit dem IANA-Transitionsprozess, der künftigen Ausgestaltung von Top-Level-Internetdomänen durch eine unabhängige Instanz verbunden. Grundlegend spalten sich die Regierungen in das Lager derer, die den derzeit praktizierten Multistakeholder-Ansatz unter Einbeziehung der Wirtschaft, Wissenschaft und Zivilgesellschaft bei der Ausgestaltung des künftigen Internets befürworten, und das Lager derer, die eine multilaterale, intergouvernementale Regelung in den VN fordern. Seit Juni 2011 verfolgt die Kommission das Ziel der Schaffung eines „einzigen, offenen, freien und unfragmentierten Netzwerkes von Netzwerken, welches denselben Gesetzen und Normen unterliegt, die offline gelten".[10] Das Akronym hierfür lautet COMPACT (Civic responsilities, One unfragmented resource, Multistakeholder approach to Promote democracy and Human Rights, sound technological Architecture, Confidence and Transparent governance). Die Europäische Union hebt hierbei die Rolle des Internet Governance Forums (IGF) hervor, um eine staatliche Einflussnahme zu Lasten des Multistakeholder-Ansatzes zu verhindern. Die Fortsetzung des oft kritisierten Formats über 2015 hinaus hängt von der Entscheidung der VN-Generalversammlung Ende 2016 ab. Zudem fordert die Europäische Union Gremien wie ICANN (Internet Corporation for Assigned Names and Numbers) und IANA (Internet Assigned Numbers Authority), die unter einer starken US-Dominanz operieren, dazu auf, sich zu internationalisieren. Komplementär hierzu setzte die einmalige NETmundial-Konferenz im Jahr 2014 ihren Schwerpunkt auf Menschenrechte und das Recht auf Privatheit im Internet. Europa bestellt seit Anfang Juli 2015 mit dem Joseph Cannataci den Posten des VN-Sonderberichterstatters zum Recht auf Privatheit im VN-Menschenrechtsrates. Die auf Anstoß des Weltwirtschaftsforums (WEF), des brasilianischen Internet-Lenkungsausschusses CGI und der ICANN im Januar 2015 eingerichtete NETmundial-Initiative (NMI) wird wiederum von den europäischen Teilnehmenden aufgrund ihrer Zusammensetzung und mangelnder Abgrenzung zum IGF kritisiert und hat sich bisher nicht als Ergänzung des Internet Governance-Ökosystems etablieren können.

Die Europäische Union tritt auf VN-Ebene nicht als einheitlicher Block auf. In einem offenen Schreiben vom April 2015 weisen Federica Mogherini und der niederländische Außenminister Bert Koenders auf die Notwendigkeit hin, Staaten für Angriffe aus ihrem nationalen Cyberraum verantwortlich zu machen und darauf, dass ein unzureichender

10 Europäische Kommission: Mitteilung der Kommission an das Europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Internet-Politik und Internet-Governance. Europas Rolle bei der Mitgestaltung der Zukunft der Internet-Governance, COM(2014) 72, S. 12.

Schutz der zentralen Infrastrukturelemente nicht nur eine Bedrohung für die nationale, sondern auch für die internationale Sicherheit darstellt. Derzeit sind fünf EU-Staaten auf der VN-Ebene engagiert. In der vierten Runde der Regierungsexperten zur Cybersicherheit (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, GGE) verhandelten insgesamt 20 Staaten, darunter fünf EU-Staaten. Die GGE wurde 2004 auf Initiative Russlands gegründet. Ihre Mitglieder analysieren bestehende und zukünftige Sicherheitsrisiken des Cyberraums und entwickeln internationale Ansatzpunkte. Im Fokus ihrer Arbeit liegt die Auseinandersetzung mit Themen der Informations- und Cybersicherheit. Die letzte Sitzung der bereits vierten GGE-Runde fand Ende Juni 2015 in New York statt. Als Konfliktpunkt bleibt die konkrete Anwendung des Völkerrechts auf den Cyberraum. Grundsätzlich unterschiedliche Auffassungen verschiedenster Aspekte der Informationssicherheit machen eine tiefer gehende, substanzielle und inhaltliche Auseinandersetzung auf VN-Ebene nahezu unmöglich. Strittige Punkte sind etwa der Umfang des Themenfelds, die Bedrohungswahrnehmung, Rolle der VN und der Regierungen gegenüber privatwirtschaftlichen und zivilgesellschaftlichen Akteuren. In der Cybersicherheit zeigen sich Trennlinien zwischen den Lagern der rechtsstaatlich-demokratischen Gleichgesinnten, der Gruppe der autoritären Staaten und der sogenannten ‚Swing-States', welche themenabhängig Positionen beider Lager unterstützen. Eine engere Absprache gibt es unter den ‚Großen Drei' Europas sowie mit der Gruppe westlicher Gleichgesinnter. Weitere GGE-Beratungen in einer fünften Runde sollen ab Herbst 2016 stattfinden. Vieles spricht dafür, dass hier die künftig vertretenen EU-Staaten stärker denn je das europäische Interesse im Auge behalten.

Ausblick

Die digitale Gesamtstrategie der Europäischen Union gilt vielen als zu wenig ambitioniert, um die digitale Selbstbehauptung Europas gegenüber den USA und China vorantreiben zu können. Selbst ein großer EU-Staat wie Deutschland kann nur im Kontext der EU-Institutionen und in Zusammenarbeit mit den anderen EU-Staaten hinreichend global wirken. Die Gruppe der Friends of Presidency on Cyber Issues (FoP Cyber) leistet zur Unterstützung der jeweiligen EU-Ratspräsidentschaft relevante innereuropäische Koordinierungsaufgaben, die durchaus auch in internationalen Organisationen zur Geltung kommen sollten.

Die digitale Selbstbehauptung der Europäischen Union bedarf einer internationalen Flankierung der digitalen Integration mit dem Ziel, die Werte der Freiheit und der Demokratie in Europa zu stabilisieren und ihnen global weiter Geltung zu verleihen. Vertreter der Wissenschaft kritisieren, „der Diskurs zu Industrie 4.0 [verlaufe] häufig zu technisch und national".[11] Daher sei dieser Diskurs stärker als bisher mit der EU-Ebene zu verzahnen, denn bei diesen zum Teil kritischen Infrastrukturen werden Lösungen zu Datensicherheit, Betriebssicherheit und Datenschutz nicht zusammengeführt.

Marktschaffende, marktregulierende und distributive Politiken sollen nach Ansicht der Kommission möglichst zügig auf den Weg gebracht werden. Das geforderte Tempo ist jedoch ein Problem, denn die Kommission muss die Rechtspolitiken sämtlicher 28 EU-Staaten harmonisieren. Als wichtige Wegmarken einer europäischen beziehungsweise transatlantischen Verständigung in Datensicherheits- und Datenschutzpolitik gelten einige Grundsatzurteile des EuGH von 2014 und 2015, nämlich zur Illegalität der Vorratsdaten-

11 Sabine Pfeiffer: Industrie 4.0 und die Digitalisierung der Produktion – Hype oder Megatrend?, in: Bundeszentrale für politische Bildung (Hrsg.): Aus Politik und Zeitgeschichte 31-32/2015, S. 6-12, hier S. 8.

speicherung, zum Recht auf Vergessen und zur Unwirksamkeit des Safe-Harbor-Abkommens. Dessen Nachfolgevereinbarung zwischen Europäischer Union und USA, der sogenannte ‚Privatsphäre-Schutzschirm' (Privacy Shield), ist hier ebenfalls hervorzuheben.

Des Weiteren haben sich Parlament, Rat und Kommission Ende Dezember 2015 auf die NIS-Richtlinie sowie auf eine DS-GVO geeinigt. Industrievertreter hingegen ziehen mit Blick auf die EU-Harmonisierung eine kritische Bilanz. In den EuGH-Urteilen und den Gesetzesinitiativen der Kommission sehen sie eine protektionistische Politik, das heißt eine „Inanspruchnahme von Politikfeldern für eine digitale Industriepolitik"[12].

Schließlich gilt es der Versuchung zu widerstehen, auf die wachsende Zahl digitaler Angriffe mit dem Aufbau einer digitalen Rüstungsindustrie und damit Cyber-Offensivwaffen zu reagieren. Die Globale Strategie zur Außen- und Sicherheitspolitik vom Juni 2016 enthält die Vorgabe, dass die Europäische Union in der Cyberverteidigung möglichst eng mit der NATO kooperieren soll und ein breites Fähigkeitsspektrum abdecken muss. Militärisch wird der Cyberraum als ‚operative Domäne' qualifiziert, vergleichbar mit Land, Luft, See oder Weltraum. Derartige Strategieentscheidungen bergen die Gefahr, dass der Cyberraum versicherheitlicht oder gar militarisiert wird und so eine neue Bedrohungskulisse entsteht. Anschaulich wird diese Gefahr auf Konferenzen zur Cyber-Außen- und Sicherheitspolitik: Zwischen Herstellern von gepanzerten Fahrzeugen, ferngesteuerten Drohnen und Funkgeräten treffen Teilnehmende auf IT-Firmen wie McAfee, FireEye, Kaspersky, Symantec, Microsoft und einschlägige Startups, die hochspezialisierte Dienstleistungen anbieten. So ist es nicht verwunderlich, dass die private IT-Sicherheitsindustrie laut Schätzungen des Beratungsunternehmens Frost & Sullivan bis 2020 rund 155 Mrd. US-Dollar im Jahr umsetzen wird. Hier entwickelt sich relativ eigenständig ein Markt, nämlich ‚security as a service', dessen Kehrseite ‚crime as a service' ist.

Weiterführende Literatur

Frank Schirrmacher (Hrsg.): Technologischer Totalitarismus. Eine Debatte, Berlin 2015.

Annegret Bendiek: Sorgfaltsverantwortung im Cyberraum. Leitlinien für eine deutsche Cyber-Außen- und Sicherheitspolitik, in: SWP-Studie 3/2016.

Annegret Bendiek: Die Globale Strategie für die Außen- und Sicherheitspolitik der EU, in: SWP-Aktuell 44/2016.

Annegret Bendiek/Evita Schmieg: EU-Außenhandel und Datenschutz. Wie lässt sich beides besser vereinabren?, in: SWP-Aktuell 10/2016.

Annegret Bendiek/Christoph Berlich/Tobias Metzger: Die digitale Selbstbehauptung der EU, in: SWP-Aktuell 71/2015.

Bundesregierung: Digitale Agenda 2014 – 2017, abrufbar unter: https://www.digitale-agenda.de/Webs/DA/DE/Home/home_node.html.

Jerin Lanier: Wenn Träume erwachsen werden. Ein Blick auf das digitale Zeitalter, Essays und Interviews 1984-2015, Hoffmann und Campe 2015.

12 Ansgar Baums: Der weiße Elefant: Industriepolitik durch die Hintertür des Datenschutzes?, 10.3.2015, abrufbar unter: http://plattform-maerkte.de/der-weisse-elefant-industriepolitik-durch-die-hintertuer-des-datenschutzes/ (letzter Zugriff: 13.10.2016).