DIGITALE GESELLSCHAFT

Ein Jahr Digitale Agenda:

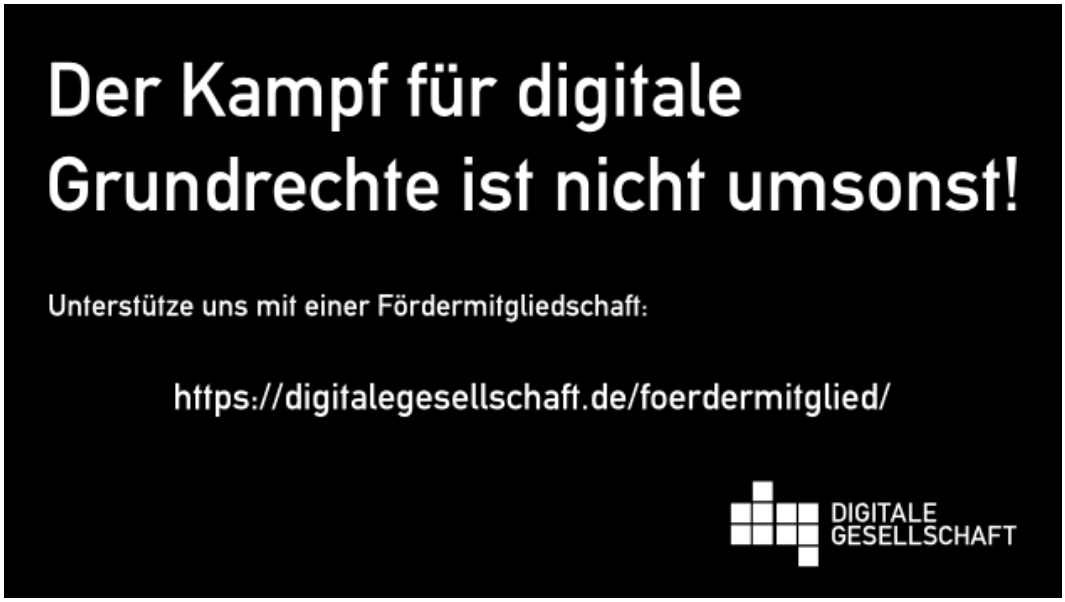
Kaum Fortschritt, viel Stillstand und verheerende Rückschritte

Parallel zur Vorstellung der Digitalen Agenda der Bundesregierung vor genau einem Jahr veröffentlichte der Digitale Gesellschaft e.V. eine alternative Digitale Agenda. Darin identifizierten wir sieben elementare netzpolitische Herausforderungen, erörterten diese vor dem Hintergrund der Regierungsagenda und unterbreiteten Vorschläge für menschen- und verbraucherrechtsfreundliche Lösungen.

Anlässlich des einjährigen Bestehens der Digitalen Agenda wenden wir uns erneut den aus unserer Sicht wichtigsten netzpolitischen Fragen zu und ziehen eine erste Bilanz: Was hat sich in der Zwischenzeit getan? Wo gab es Fortschritte, wo gab es Rückschritte und wo herrscht noch immer Stillstand? Gleichzeitig zeigen wir Alternativen zu den Antworten und Maßnahmen der Bundesregierung im Sinne einer offenen und freiheitlichen digitalen Gesellschaft auf.

Dass es in der Netzpolitik der Bundesregierung insgesamt so gut wie keine nennenswerten Fortschritte, dafür aber viel Stillstand und einige verheerende Rückschritte gab, ist angesichts des Eindrucks, den ihre Digitale Agenda bereits vor einem Jahr erweckte, wenig überraschend. Schon damals fiel auf, dass die Agenda über weite Strecken lediglich aus Prüfaufträgen besteht und Lösungsansätze in vielen Bereichen erst noch über Gesprächsrunden und Multistakeholder-Foren gefunden werden sollen. Ganz offensichtlich fehlen der Bundesregierung nach wie vor ein stimmiges und durchdachtes netzpolitisches Konzept ebenso wie eine echte Vision für eine digitale Gesellschaft.

Inhalt



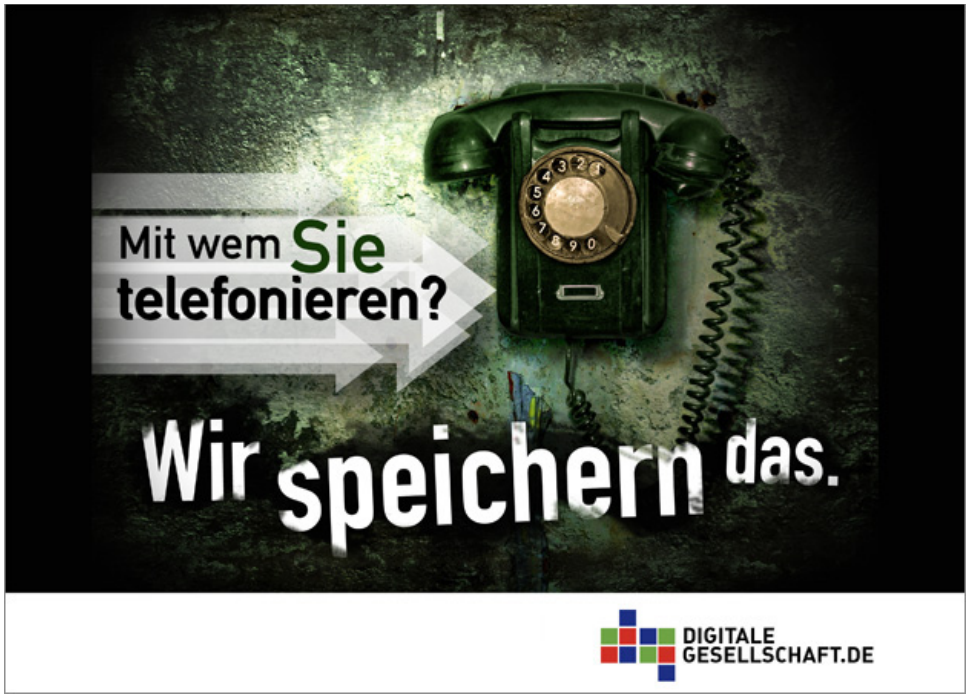
1. Überwachung/Geheimdienste: Grundrechte schützen, Dienste an die Leine legen.

Auch ein Jahr nach Vorstellung der Digitalen Agenda der Bundesregierung ist die geheimdienstliche Massenüberwachung noch immer eines der größten ungelösten Probleme. Sowohl durch die fortlaufende journalistische Auswertung der von Edward Snowden geleakten Dokumente als auch durch die Arbeit des NSA-Untersuchungsausschusses und die Veröffentlichungen von Wikileaks kommen immer wieder neue Details über die Spähaktionen deutscher und sogenannter befreundeter Dienste ans Licht.

Die US-amerikanische NSA fängt im Verbund mit ihren "Five Eyes" Partnerndiensten in Kanada, dem Vereinigten Königreich, Australien und Neuseeland weltweit sämtliche verfügbaren Daten der elektronischen Kommunikation ab, um diese sodann zu analysieren und in riesigen Datenbanken zu speichern. Der Dienst fördert zudem aktiv Sicherheitslücken in Verschlüsselungstechnologien, spioniert internationale Organisationen, deutsche und europäische Regierungsmitglieder sowie Unternehmen aus und zwingt Telekommunikationsdienstleister und Internetdienste zur heimlichen Weitergabe von Nutzerdaten. Auch auf die Gestaltung und Auslegung der gesetzlichen Befugnisse deutscher Nachrichtendienste soll die NSA mit Hilfe ihres britischen Partnerdienstes GCHQ nach Angaben von Edward Snowden aktiven Einfluss genommen haben.

Deutsche Dienste, allen voran der Bundesnachrichtendienst (BND) und das Bundesamt für Verfassungsschutz (BfV), sind – wenngleich als Partner zweiter Klasse – an der Spähmaschinerie der Five Eyes beteiligt. So führen insbesondere NSA und BND regelmäßig gemeinsame Mitarbeiterschulungen durch, betreiben eine gemeinsame operative Einheit namens Joint SIGINT Activity und beliefern sich gegenseitig mit Überwachungstechnologie. Des Weiteren füttert der BND die SMS-Datenbanken der NSA und hilft bei der Überwachung von Glasfaserkabeln. Am Netzknotenpunkt DE-CIX in Frankfurt fängt der BND die durchlaufende Kommunikation ab und durchsucht sie algorithmisch nach geheimdienstlich relevanten Informationen. Von 2004 bis 2008 hat der BND Daten aus dieser Überwachung massenhaft an die NSA weitergeleitet.

Die Totalausspähung der elektronischen Kommunikation entwertet nachhaltig Grundrechte, angefangen beim Recht auf Privatsphäre und der Telekommunikationsfreiheit über das Recht auf informationelle Selbstbestimmung und die Vertraulichkeit und Integrität informationstechnischer Systeme. Sie unterminiert verfassungsrechtliche Prinzipien wie Rechtsstaatlichkeit und Gewaltenteilung und erodiert das Vertrauen der Menschen in die Unabhängigkeit und Integrität politischer Institutionen wie auch die Sicherheit digitaler Technologien.



a. Maßnahmen der Bundesregierung

Wie schon die dürre Behandlung der Überwachungsthematik in der Digitalen Agenda vermuten ließ, hat die Bundesregierung keinerlei konkrete Maßnahmen zur Eindämmung oder Beendigung der geheimdienstlichen Ausspähung der Bevölkerung unternommen. Ganz im Gegenteil treibt sie den Ausbau der Überwachungsarchitektur aktiv voran, während sie sich öffentlich weiter in Beschwichtigungen und gespielter Empörung übt.

Eines der wenigen Vorhaben aus der Digitalen Agenda, welche die Bundesregierung bisher in die Tat umgesetzt hat, ist die massive Ausweitung der Mittel und Befugnisse des BfV. Vor einem Jahr kündigte die Bundesregierung an, die Behörde "strategisch und organisatorisch" aufzurüsten, "um den aktuellen Veränderungen bei Kommunikationsformen und -verhalten von Terroristen und Extremisten besser begegnen zu können"; dem Dienst sollten "eine sachgerechte Infrastruktur sowie technische Analysewerkzeuge" bereitgestellt werden, um die „Auswertung vorhandener Daten weiter zu verbessern und Kommunikationsmuster deutlich sichtbarer zu machen".

Diese Ankündigung wurde durch die Gründung der BfV-Einheit „Erweiterte Fachunterstützung Internet" (EFI) umgesetzt. 6 Referate mit insgesamt 75 Vollzeitstellen sollen sich darum kümmern, anhand von Metadaten die sozialen Netze und Bewegungsprofile einzelner Personen zu rekonstruieren, Chats in sozialen Netzwerken wie Facebook und Twitter zu überwachen und nicht öffentlich im Internet gespeicherte Informationen heimlich zu erheben. Um Zielpersonen, die mehrere unterschiedliche Endgeräte nutzen, lückenlos verfolgen zu können, soll die EFI-Einheit Daten möglichst nah am oder sogar direkt vom Server des jeweiligen Providers abgreifen können. Außerdem soll ein System zur automatisierten Gewinnung, Verarbeitung und Auswertung großer Datenmengen entwickelt werden, um bisher unbekannte und nicht offen

erkennbare Zusammenhänge zwischen Personen und Gruppierungen im Internet erkennen zu können.

Ein weiterer Schritt, mit dem die Bundesregierung die Überwachung der Bevölkerung massiv auszuweiten sucht, ist die Einführung der Vorratsspeicherung von Verbindungs- und Standortdaten aus der elektronischen Kommunikation. Obwohl Bundesjustizminister Maas nach der Aufhebung der EU-Richtlinie zur Vorratsdatenspeicherung durch den Europäischen Gerichtshof (EuGH) stets beteuert hatte, dass es mit ihm keinen neuen Anlauf in dieser Sache geben werde, legte er auf Druck von Bundesinnenminister Thomas de Maizière und Bundeswirtschaftsminister Sigmar Gabriel schließlich doch einen entsprechenden Gesetzentwurf vor. Danach ist vorgesehen, bei jeglicher elektronischer Kommunikation mit Ausnahme von Emails die Verbindungsdaten für zehn und die Standortdaten für vier Wochen anlasslos zu speichern. Polizei und Staatsanwaltschaft können zum Zwecke der Gefahrenabwehr und der Verfolgung bestimmter Straftaten auf diese Daten zugreifen. Behördliche, kirchliche und soziale Einrichtungen sind von der Speicherung gänzlich ausgenommen, während die Daten anderer Berufsgeheimnisträger wie Rechtsanwälte oder Journalisten aufgezeichnet, aber nicht abgerufen werden dürfen. Außerdem soll ein neuer Straftatbestand der „Datenhehlerei" eingeführt werden, der gerade für Whistleblower und Journalisten die Gefahr begründet, sich mit ihrem Tun strafbar zu machen.

So sehr die Bundesregierung sich beim Ausbau der Überwachung ins Zeug legt, so verzagt agiert sie, wenn es darum geht, die Spähexzesse der NSA und ihrer Partnerdienste aufzuklären und einzudämmen. Dem NSA-Untersuchungsausschuss legt sie nach wie vor so gut sie kann Steine in den Weg. Exemplarisch dafür ist der Umgang mit der Liste der als „Selektoren" bezeichneten Suchbegriffe, welche die NSA in die Überwachungssysteme des BND eingespeist hat, um auf diesem Weg Unternehmen und Regierungsangehörige europäischer Nachbarstaaten auszuspionieren. Die Verantwortlichen im Kanzleramt bestreiten schlicht jedes Mitwissen und schieben dem BND die alleinige Verantwortung in dieser Angelegenheit zu. Zugleich versucht die Bundesregierung, die Aufarbeitung der deutschen Beihilfe zur Spionage zu verhindern, indem sie dem NSA-Untersuchungsausschuss die Vorlage der Selektorenliste verweigert und diese stattdessen nur einem von ihr bestellten Sonderermittler zugänglich machen möchte.

Ein typisches Beispiel für die Beschwichtigungsversuche der Bundesregierung sind die angeblichen Verhandlungen mit der US-Administration um ein No-Spy-Abkommen. Obwohl Obama-Mitarbeiter schon früh signalisiert hatten, dass ein solches Abkommen für die Amerikaner nicht in Betracht komme, erweckte die Bundesregierung gegenüber der Öffentlichkeit noch monatelang bewusst wahrheitswidrig den Eindruck, dass die Verhandlungen fortgeführt würden.

b. Kritik

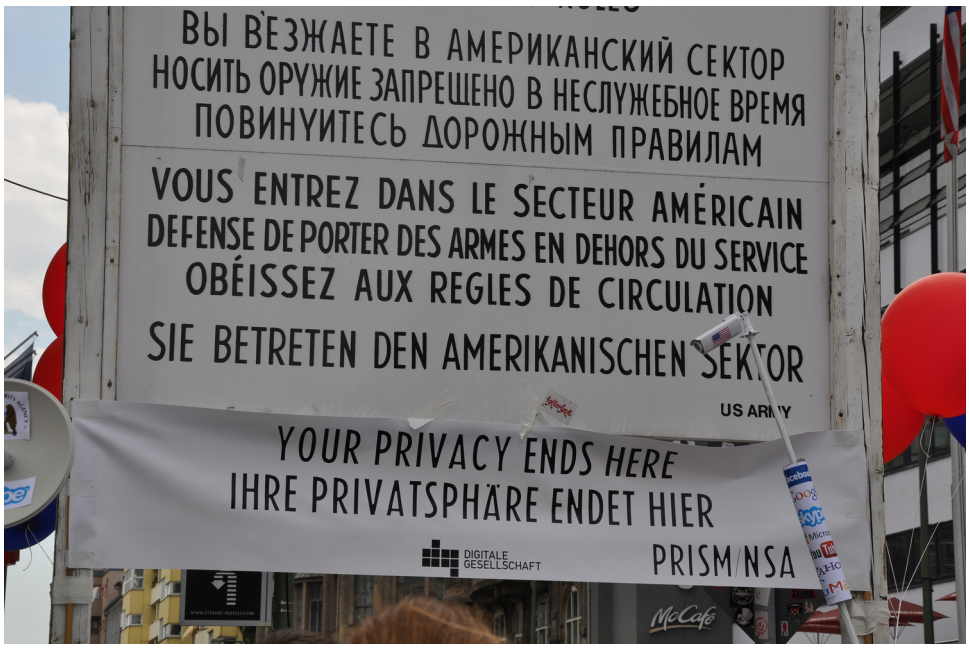
Die Maßnahmen und Unterlassungen der Bundesregierung im Bereich der Geheimdienste und der Kommunikationsüberwachung unterminieren die Grundrechte der Bevölkerung in Deutschland und tragen zur Aushöhlung rechtsstaatlicher Prinzipien bei. Durch die Aufrüstung mit Kapazitäten zur Massendatenauswertung und zur Analyse von Beziehungsgeflechten und Bewegungsprofilen verleiht die Bundesregierung dem BfV Möglichkeiten zur Ausspähung der eigenen Bevölkerung, die denen der NSA ähneln. Im Zuge solcher Analysen werden die personenbezogenen Daten unzähliger Menschen in Deutschland erhoben und in den Systemen des BfV verarbeitet, um auf diese Weise „Kontaktpersonen" und neue „Verdächtige" zu ermitteln. Zwar darf das BfV, anders als etwa der BND, nur einzelne Personen ins Visier nehmen, neben der eigentlichen Zielperson können davon aber auch ihre Kontakte und wiederum deren Kontakte betroffen sein. Auf diese Weise kann die Anzahl der Personen, deren Daten durch das BfV erhoben und ausgewertet werden, in jedem einzelnen Fall schnell auf mehrere Tausend anwachsen.

Zugleich ist die Bundesregierung offenbar bemüht, eine öffentliche Debatte über die massive Verschärfung der Überwachung der Bevölkerung in Deutschland zu vermeiden. Journalisten von netzpolitik.org, die über die Pläne zum Aufbau der EFI und die dazugehörigen Haushaltspläne berichteten, wurden mit einem Strafverfahren wegen Landesverrats überzogen. Zwar ist dieser Einschüchterungsversuch mit einem der schwersten Geschütze, die das deutsche Strafrecht zu bieten hat, aufgrund einer breiten öffentlichen Protestwelle grandios gescheitert; zugleich zeigt das Vorgehen jedoch, wie wenig die Bundesregierung dazu bereit ist, eine gesamtgesellschaftliche Diskussion um die Frage zu führen, ob und bejahendenfalls wie viel Geheimdienste und Überwachung in einem demokratischen und freiheitlichen Rechtsstaat akzeptabel sind. Mit welcher Geringschätzung die Bundesregierung den Freiheitsrechten der Bevölkerung ebenso wie der höchstrichterlichen Rechtsprechung gegenübersteht, lässt sich auch an der Wiedereinführung der Vorratsdatenspeicherung ablesen. Mit der anlasslosen Speicherung der Verbindungs- und Standortdaten ignoriert sie die klaren Voten des Bundesverfassungsgerichts und des EuGH. Die besonders schützenswerten Daten von Berufsgeheimnisträgern setzt sie durch die Speicherung einem hohen Missbrauchsrisiko aus. Durch den Straftatbestand der Datenhehlerei schafft sie zudem ein weiteres Instrument, mit dem gegen Whistleblower und unliebsame Journalisten vorgegangen werden kann. All diese grundrechtlichen Einschränkungen und Gefährdungen nimmt sie billigend in Kauf, obwohl der Nutzen der Vorratsdatenspeicherung für die Gefahrenabwehr und die Strafverfolgung bis heute noch nicht einmal mit Indizien belegt werden kann. Im Gegenteil kommen sämtliche bisher zu dieser Frage im In- und Ausland angestellten Untersuchungen zu dem Ergebnis, dass der Rückgriff auf Vorratsdaten nicht zu einer Verbesserung der Aufklärungsquoten geführt hat.

Auch rechtsstaatliche Prinzipien scheinen für die Bundesregierung eher störendes Beiwerk zu sein, was sich besonders deutlich an ihrer Abwehrhaltung bei der Aufklärung der geheimdienstlichen Spähexzesse zeigt. Sowohl nach dem Grundgesetz als auch nach den einfachgesetzlichen Regeln ist es das unveräußerliche Recht der Mitglieder des

Untersuchungsausschusses, Beweise selbst zu erheben und zu bewerten. Zwar kann der Ausschuss einen Ermittlungsbeauftragten bestellen, der besonders umfangreiche Beweismittel zunächst sichtet und nach Relevanz sortiert. Gleichwohl bleibt es auch in diesem Fall dabei, dass die Mitglieder des Untersuchungsausschuss selbst Zugriff auf die Beweismittel haben. Ein Sonderermittler, der anstelle der Ausschussmitglieder die Beweismittel erhebt und bewertet, beschneidet hingegen in unzulässiger Weise ihre verfassungsrechtlich garantierten Untersuchungsrechte.

Ebenso offenbart die Begründung der Bundesregierung für das Zurückhalten der Selektorenliste eine eigentümliche Auffassung rechtsstaatlicher Prinzipien. So behauptet die Bundesregierung, dass für eine Offenlegung der Liste gegenüber Abgeordneten des Bundestages die Zustimmung der US-Seite völkerrechtlich erforderlich sei. Damit bezieht sie sich auf die als „Memorandum of Agreement“ oder „Memorandum of Understanding“ bekannte Kooperationsvereinbarung zwischen den deutschen und den US-amerikanischen Geheimdiensten. Abgesehen davon, dass Vertreter des Weißen Hauses mittlerweile klargestellt haben, dass die USA sich nie explizit gegen eine Vorlage der Selektorenliste ausgesprochen hat, gehört die Vereinbarung als bloße Vereinbarung zwischen Behörden auch nicht zum Völkerrecht. Hinzu kommt, dass der Gewaltenteilungsgrundsatz, nach dem sich die unterschiedlichen Säulen der Staatsgewalt in ihrer Machtausübung gegenseitig kontrollieren und hemmen sollten, komplett ausgehebelt würde, wenn die Exekutive die Untersuchungsrechte des Bundestags durch beliebige Vereinbarungen mit ausländischen Behörden unterlaufen könnte. Schließlich entbehrt es auch nicht einer recht offenkundigen Ironie, dass die Bundesregierung sich mit Verweis auf die Interessen der NSA weigert, gewählten Volksvertretern Einblick in die Selektorenliste zu gewähren, während die NSA selbst sensible Daten und „Betriebsgeheimnisse“ privatwirtschaftlichen Unternehmen, den sogenannten Contractors, mit Tausenden von Mitarbeitern anvertraut.



c. Alternative

Zum Schutz der Grundrechte und des freiheitlichen Charakters der Gesellschaft müssen sämtliche anstehenden und bereits realisierten Vorhaben zum Ausbau der Massenüberwachung aufgegeben und rückgängig gemacht werden. Das betrifft die geplante Wiedereinführung der Vorratsdatenspeicherung ebenso wie die Kriminalisierung von investigativen Journalisten und Whistleblowern sowie die Aufrüstung des BfV mit Mitteln und Kapazitäten zur Internetüberwachung.

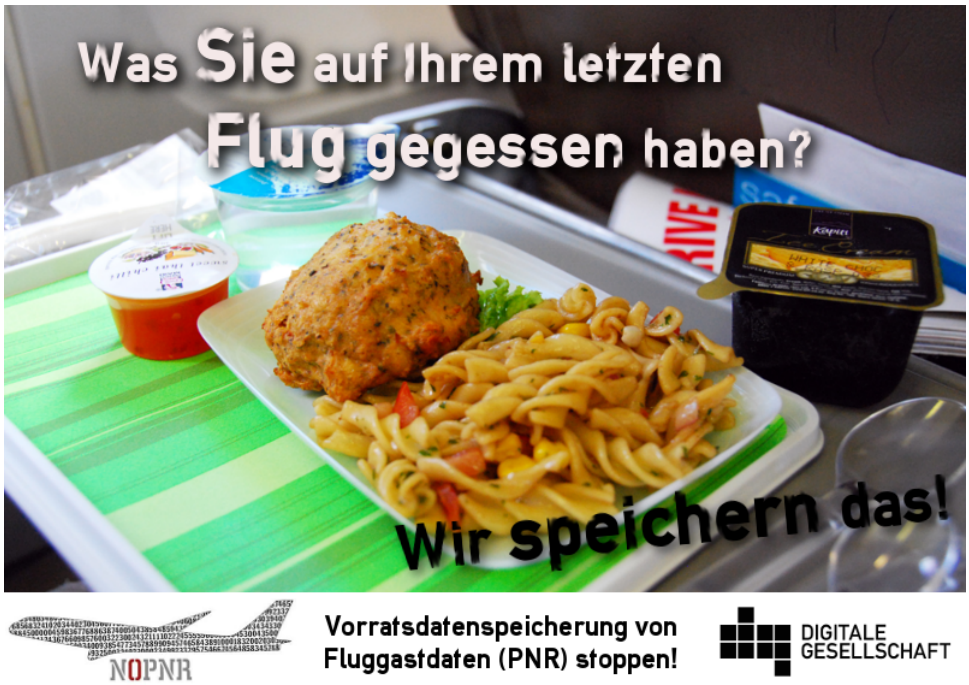
Zur Eindämmung der Spähexzesse deutscher und internationaler Geheimdienste muss die Bundesregierung des Weiteren ihre Blockadehaltung gegenüber dem NSA-Untersuchungsausschuss aufgeben und die Selektorenliste ebenso wie sämtliche weiteren Details zur Beteiligung deutscher Stellen an der weltweiten Überwachungsmaschinerie schonungslos offenlegen.

Statt Journalisten, welche die Öffentlichkeit über die Kapazitäten der geheimdienstlichen Überwachung informieren, strafrechtlich zu verfolgen, muss die Bundesregierung selbst eine öffentliche Debatte über die Frage anstoßen, ob und gegebenenfalls in welchem Maß eine freie und offene Gesellschaft bereit ist, geheimdienstliche Überwachung zu tolerieren. Dazu muss sie auch gegenüber der Öffentlichkeit sämtliche Vereinbarungen zur Zusammenarbeit deutscher Behörden mit ausländischen Nachrichtendiensten offenlegen und Klarheit über die Tätigkeit der eigenen Dienste schaffen.

Des Weiteren gehört das gesamte bundesdeutsche Geheimdienstwesen auf den Prüfstand. Eine solche grundlegende Neuordnung muss mindestens die Befugnisse der Dienste zur Datenerhebung, -verarbeitung und -weitergabe sowie ihre parlamentarische Kontrolle umfassen. Ein Datenaustausch mit ausländischen Diensten darf nur stattfinden, wenn auf beiden Seiten ein verfassungsgemäßer und strikt dem Grundrechtsschutz unterworfener Umgang mit den Daten zweifelsfrei gewährleistet ist. Dienste wie die NSA, welche die von deutschen Stellen gelieferten Mobilfunkdaten zu gezielten willkürlichen Tötungen im Drohnenkrieg oder in sonst menschenrechtsswidriger Weise verwenden, müssen als Kooperationspartner ausscheiden.

Die parlamentarische Kontrolle der bundesdeutschen Dienste muss überdies deutlich verbessert werden. Neben einer personellen Aufstockung des Parlamentarischen Kontrollgremiums einschließlich der Bereitstellung eines eigenen Mitarbeiterstabs bedarf es außerdem einer Ausweitung seiner Kontrollbefugnisse. Dazu gehören Rechte zur Durchsuchung von behördlichen Räumlichkeiten und zur Analyse der von den Diensten eingesetzten Software und Systeme ebenso wie die Möglichkeit, als vertrauliche Anlaufstelle für Whistleblower zu dienen. Unterstützt werden sollte die Arbeit des Gremiums außerdem durch einen Expertenbeirat, der aus Fachleuten unterschiedlicher Disziplinen besteht und den notwendigen technischen, operativen und juristischen Sachverstand beisteuern kann.

Auf internationaler Ebene muss die Bundesregierung den Druck insbesondere auf die Dienste des “Five Eyes” Programms erhöhen. Zu diesem Zweck muss sie vor dem EuGH ein Vertragsverletzungsverfahren gegen das Vereinigte Königreich wegen der Überwachung der Unterseekabel durch den GCHQ einleiten. Außerdem muss sie in den betreffenden EU-Gremien für eine Aussetzung von Safe Harbor sowie von Datenaustauschabkommen mit den USA, namentlich PNR und TFTP (SWIFT), stark machen.



2. IT-Sicherheit: Dezentralisierung vorantreiben, Open Source fördern.

Ständige Sicherheitslücken in IT-Systemen und Meldungen über gigantische Datendiebstähle gehören mittlerweile zum Alltag. Immer wieder lesen wir von Hacks, bei denen Millionen von Nutzerinnen und Nutzern betroffen sind. Ob Kreditkartendaten oder Adressdaten von Flirtportalen, die gestohlen und in Umlauf gebracht werden, ob Angriffe auf Sicherheitszertifikate von Banken oder Attacken auf Atomkraftwerke - kein System scheint wirklich sicher zu sein. So wurde erst kürzlich die IT des Bundestags gehackt und auch die Erinnerungen an Stuxnet sind noch nicht verblasst. Gleichzeitig zeigen die Snowden-Enthüllungen, dass Geheimdienste mit einem gigantischen Datenhunger alle Daten absaugen und auswerten, die sie in die Finger bekommen können. Befeuert wird diese Gier nach Informationen auch durch Äußerungen wie etwa die Forderung von Bundesinnenminister Thomas de Maizière, dass Verschlüsslung für Geheimdienste knackbar sein solle. Diese Entwicklungen führen zu einer zunehmenden Verunsicherung der Nutzerinnen und Nutzer von Online-Diensten und befördern gleichzeitig deren Wunsch nach mehr Sicherheit im digitalen Raum. Sowohl bei der Wahrnehmung ihrer demokratischen Freiheitsrechte als auch bei Alltäglichkeiten wie dem Onlinebanking sind die Menschen auf sichere Infrastrukturen angewiesen. Ist diese Sicherheit nicht gewährleistet, so erodiert dies die sozialen und wirtschaftlichen Grundlagen unserer Gesellschaft.

a. Maßnahmen der Bundesregierung

Das Thema IT-Sicherheit spielt in der Digitalen Agenda der Bundesregierung eine verhältnismäßig große Rolle. Besondere Aufmerksamkeit erfährt die Erhöhung der Sicherheit der Bundes-IT. Sie soll unabhängiger von „globalen IT-Konzernen“ – gemeint sind wohl US-amerikanische Unternehmen – werden. Die „Daten der Bundesverwaltung“ sollen durch eigene „Netzwerkstrukturen unter Verwendung vertrauenswürdiger Komponenten“ fließen. Auf Nutzerseite will die Bundesregierung die Einführung der De-Mail vorantreiben sowie die Entwicklung, den Einsatz und die Zertifizierung von Verschlüsselung fördern. Zudem ist eine „Meldepflicht für erhebliche IT- Sicherheitsvorfälle“ angedacht. Zugleich sollen die Polizeibehörden, Nachrichtendienste und das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Stärkung erfahren, um für mehr „Sicherheit im Cyberraum“ zu sorgen.

Die Bundesregierung hat sich zunächst der Meldepflicht bei IT-Sicherheitsvorfällen und der Stärkung von Nachrichtendiensten und Ermittlungsbehörden bzw. dem BSI zugewandt.

Mitte dieses Jahres wurde das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, auch bekannt als IT-Sicherheitsgesetz, auf den Weg gebracht. Mit dem Gesetz sollte der große Wurf gelingen: Zum einen soll die IT-Sicherheit in Unternehmen, zum anderen der Schutz der Bürgerinnen und Bürger gewährleistet werden. Dafür werden beispielsweise die Betreiber kritischer Infrastrukturen sowie Telekommunikationsanbieter dazu verpflichtet, eine

„IT-Sicherheit nach dem Stand der Technik zu gewährleisten“. Gleichzeitig soll eine anonyme „Meldepflicht erheblicher IT-Sicherheitsvorfälle“ zu mehr Sicherheit führen. Auf Grundlage der so gewonnenen Informationen sollen anschließend Lagebilder erstellt und Aufsichtsbehörden unterrichtet werden. Eine Information derjenigen, die von Sicherheitsvorfällen betroffenen sind, ist jedoch nicht vorgesehen. Durch der Einführung eines Sanktionsmechanismus soll gewährleistet werden, dass sich die Unternehmen auch an die Vorschriften halten.

Um Cyberattacken nachvollziehen zu können, werden Anbietern von Telemedien und Telekommunikationsdiensten Speicherbefugnisse eingeräumt. Sie dürfen Bestands- und Verkehrsdaten ihrer Kundinnen und Kunden erheben und verwenden. Auf diese Weise ermöglicht das IT-Sicherheitsgesetz diesen Anbietern eine fakultative Verkehrsdatenspeicherung.

Gleichzeitig werden Ermittlungsbehörden, Geheimdienste und das Bundesamt für Sicherheit in der Informationstechnik (BSI) gestärkt. So sollen bis zu 78 neue Stellen beim Bundeskriminalamt (BKA), 48,5 Stellen beim BfV und bis zu 30 Stellen beim BND geschaffen werden, um gegen Cybercrime vorgehen zu können. Das BSI wird vor allem durch den Zugewinn an Kompetenzen, etwa die Auswertung der Meldungen über sicherheitsrelevante Vorgänge und das Erstellen der Lagebilder, aufgewertet. Für die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) ist nur die Schaffung von maximal sieben neuen Stellen vorgesehen.

b. Kritik

Dass die Bundesregierung ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme auf den Weg gebracht hat, ist zunächst positiv zu bewerten. Die Ausgestaltung des Gesetzes erweist sich jedoch als mangelhaft und teilweise widersprüchlich. Bereits die Ausrichtung des Gesetzes auf kritische Infrastrukturen ist viel zu eng gefasst. Was eine kritische Infrastruktur ist, wird durch das Bundesministerium des Innern (BMI) durch Rechtsverordnung bestimmt. Seitens der Regierung geht man von etwa 2.000 Betreibern kritischer Infrastrukturen aus. Wie genau man auf diese Anzahl kommt und nach welchen Kriterien man die Betreiber kritischer Infrastruktur identifizieren will, bleibt nebulös. Die Begrenzung bleibt nicht nur vermeintlich willkürlich, sondern bringt auch ein großes Restrisiko mit sich. Angriffe auf IT-Systeme gehen häufig in die Breite, richten sich also gegen eine Vielzahl von Unternehmen gleichzeitig. Selbst wenn diese Unternehmen einzeln betrachtet nicht als kritische Infrastruktur anzusehen sind, kann ein konzentrierter Angriff in der Summe ebenso kritische Situationen hervorrufen ein Angriff auf einen einzelnen Betreiber einer kritischen Infrastruktur.

Problematisch erscheint des Weiteren, dass IT-Sicherheitsvorfälle anonym gemeldet werden können. Für die Öffentlichkeit besteht damit kaum eine Möglichkeit, die betroffenen Unternehmen unter Druck zu setzen. Da die Anonymität Schutz vor lästigen öffentlichen Debatten gewährt, dürften betroffene Unternehmen in der Regel nicht motiviert sein, einem aufgrund eines IT-Sicherheitsmangels verursachten Imageschaden durch entsprechende Investitionen vorzubeugen. Zwar wird gleichzeitig ein Sanktionsmechanismus eingeführt, der Strafen zwischen 50.000 und 100.000 Euro vorsieht. Doch inwieweit eine Strafe von maximal 100.000 Euro bei milliardenschweren Unternehmen tatsächlich zu einem Umdenken im Bereich IT-Sicherheit führt, muss bezweifelt werden. Zielführender wäre ein Sanktionsmechanismus, der sich am Jahresumsatz der Unternehmen orientiert.

Dass mit der Einführung einer freiwilligen Verkehrsdatenspeicherung das Prinzip der Datensparsamkeit vollständig umgekehrt wird, passt zur absurden Grundausrichtung dieses Gesetzes. Daten, die nicht gespeichert werden, können auch nicht gestohlen oder manipuliert werden. Mit jeder Datenspeicherung steigt auch die Wahrscheinlichkeit für Angriffsversuche, um an die Daten zu gelangen. Die Bundesregierung befördert mit dem Gesetz daher gerade die Begehrlichkeiten von Kriminellen, welche sie mit dem Gesetz zu unterbinden sucht. Zugleich setzt sie dadurch sensible Daten der Kundinnen und Kunden von Telekommunikationsanbietern erheblichen Missbrauchsrisiken aus.

Fraglich erscheint zudem, ob das BMI in der Lage sein wird, seine vorgesehenen besonderen Kompetenzen bei der Bewertung und Analyse von IT-Angriffen ohne Zielkonflikte wahrzunehmen. So war das BSI zuvor etwa an der Entwicklung des Staatstrojaners beteiligt. Zudem befindet es sich im Geschäftsbereich des BMI, mithin eines Ministeriums, aus dem immer wieder Forderungen nach systematischen Schwächungen von Verschlüsselungstechniken zu vernehmen sind.

Am Ende bleibt ein Gesetz der Bundesregierung, was allenfalls dazu taugt IT-Sicherheit zu simulieren und gleichzeitig dafür genutzt wird, um die Sicherheitsbehörden mit weiteren Ressourcen auszustatten.

In anderen Bereichen der IT-Sicherheit bleibt die Bundesregierung ebenfalls weit hinter den nötigen Fortschritten zurück. So sind die Vorschläge der Bundesregierung bei den Themen Vergabe- und Beschaffungspolitik bemerkenswert unkonkret. Es wird nicht klar, wie eine „innovationsorientierte Vergabepolitik" konkret ausgestaltet sein und zu mehr IT-Sicherheit beitragen soll. Das gleiche gilt für die Förderung von Verschlüsselungstechniken und -produkten. Das Ziel der „Chancengleicheit" von Open-Source-Software in der Beschaffungspolitik halten wir für nicht ausreichend, um die gewachsenen Pfadabhängigkeiten hinsichtlich proprietärer Systeme aufzubrechen. In der Koalitionsvereinbarung sprach sich die Bundesregierung an dieser Stelle noch proaktiv für eine Förderung von Open-Source-Lösungen aus.

Als widersprüchlich und unvereinbar mit den in der Digitalen Agenda genannten IT-Sicherheitszielen (u.a. Schutz vor Angriffen, Verschlüsselung und Autonomie), erscheint das Vorhaben, die De-Mail zu stärken. Eine derart zentralisierte, nicht hinreichend verschlüsselte und unter Beteiligung US-amerikanischer Unternehmen entwickelte Kommunikationsinfrastruktur zu verbreiten, wäre für die Sicherheit digitaler Kommunikation desaströs.

Zudem erkennen wir in der Digitalen Agenda der Bundesregierung eine kontraproduktive Polizeiisierung und Militarisierung von „Cyber-Sicherheit" anstelle des nötigen Paradigmenwechsels hin zu einer transparenten, evidenzbasierten und effektiven IT-Sicherheitspolitik. Polizeiliche, militärische und geheimdienstliche Stellen lösen die – zuvorderst technischen – Probleme der IT-Sicherheit nicht und verursachen dabei untragbar hohe gesellschaftlichen Kosten. Die Stärkung der Ressourcen staatlicher Stellen wie des BfV, die auf Eingriffsmöglichkeiten in IT-Systeme und den Zugriff auf Datenvorhaltungen angewiesen sind, verhindert ein Mehr an IT-Sicherheit.

c. Alternative

Den einleitend geschilderten Quellen der Verunsicherung der Nutzerinnen und Nutzer lässt sich gezielt durch eine Umgestaltung der IT-Sicherheitspolitik begegnen. Dabei hätte bereits im IT-Sicherheitsgesetz dafür gesorgt werden müssen, dass nicht nur die ca. 2.000 Betreiber kritischer Infrastrukturen angehalten werden, für mehr Sicherheit zu sorgen. Vielmehr muss das Ziel darin bestehen, in der Breite für robuste Systeme zu sorgen. Dazu gehören neben öffentlichen Mitteilungen über IT-Sicherheitslücken auch die Einführung innovativer Lösungen. So könnten etwa durch das Ausloben von Prämien für das Finden und Beseitigen von Sicherheitslücken Anreize geschaffen werden, die zu einer schnellen Beseitigung der Sicherheitsrisiken führen, anstatt dies auf intransparente Weise durch das BSI realisieren zu lassen. Zudem sollten Schutzmaßnahmen für Whistleblower geschaffen werden, um zu gewährleisten, dass Sicherheitslücken auch auf diesem Weg kommuniziert werden können.

In der Beschaffungs- und Vergabepolitik sollten Open Source, Dezentralisierung und Ende-zu-Ende-Verschlüsselung zu den leitenden Prinzipien gehören. Ferner ist bei der Begünstigung europäischer und deutscher Unternehmen in der Vergabepolitik darauf zu achten, dass hier mittelständische Unternehmen gegenüber großen Akteuren bevorzugt werden. Zudem müssen IT-Systeme und Software regelmäßig und verpflichtend auditiert werden.
Problemtisch ist auch die derzeitige Nähe des BSI zum BMI. Diese Behörde muss umgehend aus dem Geschäftsbereich des Bundesministeriums des Inneren ausgegliedert werden, um ihre Unabhängigkeit zu gewährleisten. Statt der vorgeschlagenen Stärkung von BfV, BND und BKA ist die Ressourcen- und Personalausstattung von BfDI und BSI zunächst auf Augenhöhe mit den Sicherheitsbehörden zu bringen. Zudem ist zu prüfen, welche Aufgaben im Bereich der IT-Sicherheit derzeit in nachrichtendienstlichen Behörden angesiedelt sind und besser in ein unabhängiges BSI bzw. zur BfDI ausgegliedert werden sollten.

3. Datenschutz: Datensammelwut von Unternehmen eindämmen, Datensouveränität für Verbraucher/innen stärken.

In einer vernetzten Welt hinterlässt beinahe jede menschliche Handlung auch eine Datenspur. Besonders deutlich wird das im sogenannten „Internet der Dinge". Nicht mehr nur die „virtuelle" Benutzung von Onlineangeboten wie sozialen Netzwerken oder Einkaufsportalen, sondern auch all jene Praktiken, die vormals als Teil der „Offline-Welt" galten, werden verdatet. Dazu zählen Dinge wie der Energieverbrauch oder auch die körperliche Bewegung im Rahmen der Erfassung von Gesundheitsdaten. Ob im sozialen Netzwerk oder gegenüber der Krankenkasse: Daten sind nicht das Abfallprodukt, sondern zunehmend auch der Treibstoff der digitalen Gesellschaft. Einzelpersonen stehen dabei zumeist privaten Unternehmen gegenüber, von deren, auf Datenverarbeitungen beruhenden, Leistungen sie abhängen – das gilt für Freemailer ebenso wie für Autoversicherungen mit fahrverhaltensbasierten Tarifen. In Anbetracht dieser Abhängigkeitsverhältnisse wird man dem Problem nicht dadurch gerecht, eine angebliche „digitale Sorglosigkeit" (Thomas de Maizière) der Nutzerinnen und Nutzer zu monieren.

Datenschutz hilft dabei, Grundprinzipien von Selbstbestimmung und Fairness zu erhalten. Kreditwürdigkeit sollte nicht vom Facebook-Freundeskreis abhängen und der neue Job nicht von der Krankenakte. Wo nicht nötig, sollten Daten nicht länger vorgehalten, verbunden oder weitergegeben werden. Die Einhaltung dieser Regeln muss nachvollziehbar sein und Abweichungen müssen geahndet werden.

Seit Jahren arbeitet Europa an einer Reform seiner Datenschutzregeln. Die Bundesregierung hat diesen Reformprozess verschlafen, da sie es nicht vermochte, starke und zugleich den Realitäten der neuen Datenschutzherausforderungen entsprechende Vorschläge in diesen Prozess einzubringen. Die Bundesregierung hat die Überarbeitung der Datenschutzregeln während der Verhandlungen im EU-Ministerrat zugleich immer wieder verzögert. Nicht zuletzt trägt sie Mitschuld an der Verwässerung der Position der EU-Mitgliedsstaaten und damit der kommenden Datenschutzverordnung. So ist es politisch höchst unwahrscheinlich, dass in den finalen Trilogverhandlungen zwischen den europäischen Institutionen der Graben zwischen den akzeptablen Positionen des Europäischen Parlaments und der unzureichenden Vorschläge des Rates in zufriedenstellender Weise überbrückt wird.

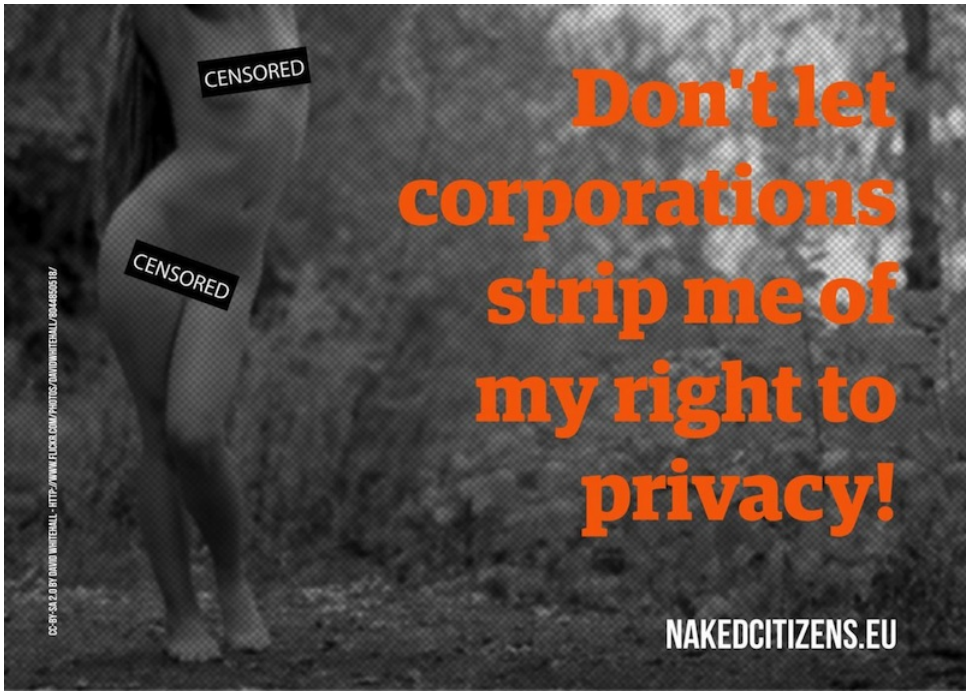
Deutschland muss auf der Zielgeraden des Ringens um die Datenschutzverordnung als starke Stimme an der Seitenlinie der Verhandlungen nun zumindest das Schlimmste verhindern, um zugleich im Sinne eines „nach der Reform ist vor der Reform" neu an den Herausforderungen der Datengesellschaft zu arbeiten.

a. Maßnahmen der Bundesregierung

Im Mittelpunkt der Maßnahmen der Bundesregierung stand die erwähnte Datenschutzverordnung. Im Juni 2015 einigten sich die EU-Mitgliedsstaaten nach mehr als drei Jahren Verhandlungszeit auf eine Position. Zumindest was den in der Digitalen Agenda avisierten Zeitplan angeht, hat die Bundesregierung also Wort gehalten. Die erste Lesung im Europäischen Parlament erfolgte bereits 2014. Beide Institutionen müssen sich nun im Trilogverfahren zusammen mit der Europäischen Kommission auf einen finalen Rechtsakt einigen, worauf die Bundesregierung nur noch bedingt Einfluss hat.

Formal Wort gehalten hat die Bundesregierung auch bei der Einführung eines Verbandsklagerechts für Datenschutzverstöße auf nationaler Ebene. Das Bundeskabinett hat einen entsprechenden Gesetzesentwurf beschlossen.

Nicht Bestandteil der Digitalen Agenda war die Herauslösung der Bundesdatenschutzbeauftragten aus dem Innenministerium auf Druck eines Urteils des Europäischen Gerichtshofes. Damit ist die Dienststelle nun formal unabhängig.



b. Kritik

Der Standpunkt des EU-Ministerrats zur Datenschutzverordnung war ein herber Rückschlag für den Datenschutz. Der Rat schwächte den Entwurf der Europäischen Kommission in allen wichtigen Punkten: technisch-organisatorische Maßnahmen wie die Bestellung eines Datenschutzbeauftragten sollen nicht mehr verpflichtend sein, Sanktionen für Datenschutzverstöße fallen zu gering aus und Grundprinzipien des Datenschutzes wie Zweckbindung und Datensparsamkeit weichte der Rat auf. Aus den Verhandlungsdokumenten

wird ersichtlich, dass sich die deutsche Bundesregierung insbesondere für die Abschwächung der Zweckbindung und Datensparsamkeit eingesetzt hat. Das von den deutschen Verhandlern ausgegebene Ziel „internettauglicher" Regeln lief somit auf eine simple Streichung vermeintlich veralteter Regeln hinaus. Wirklich innovativ wäre dagegen die Beibehaltung dieser Regeln bei gleichzeitigem Auftrag zur Konkretisierung und Operationalisierung in Standardisierungsverfahren gewesen.

Der Entwurf des Rates konterkariert zudem das geplante Verbandsklagerecht auf nationaler Ebene. Die kollektive Rechtewahrnehmung durch Verbraucher- und Datenschutzorganisationen strichen die EU-Staaten aus dem Entwurf. Die Schuld hierfür liegt sicherlich nicht bei der Bundesregierung, weshalb sie nun um so lauter Partei für eine europäische Verankerung des Verbandsklagerechts bei Datenschutzverstößen eintreten muss. Nur kollektive Interessenvertretung vermag es, Unternehmen grundlegende Schutzprinzipien zum Wohle des Individuums abzuringen. Man denke an die Verbesserung der Arbeitsbedingungen durch Gewerkschaften im 20. Jahrhundert. Kollektive Interessenvertretung kann allerdings nichts bewirken, wenn Grundprinzipien wie Zweckbindung und Datensparsamkeit sich nicht einfordern lassen, weil sie nicht mehr existieren.

Die formale Unabhängigkeit der Bundesdatenschutzbeauftragten begrüßen wir – jedoch darf es dabei nicht bleiben. Es bedarf mehr Stellen, Mittel und Zuständigkeiten, etwa durch verpflichtende Konsultation der Behörde in Gesetzgebungsverfahren, um der Bundesdatenschutzbeauftragten angemessene Bedeutung einzuräumen.

c. Alternative

Neben den bereits angedeuteten Maßnahmen ergeben sich für die Bundesregierung eine Fülle von Aufgaben, aber auch Gestaltungsmöglichkeiten, im Datenschutz. Zu den verpflichtenden Aufgaben gehört es, mit starker Stimme auf das Trilogverfahren einzuwirken und das Verhandlungsgleichgewicht in Richtung der – zumindest akzeptablen – Position des Europäischen Parlaments zu verschieben. Bedauerlicherweise wird auch der Kompromiss zur Datenschutzverordnung eine Reihe von nationalen Umsetzungsspielräumen mitbringen. Es gilt, diese Öffnungsklauseln zu evaluieren und auf nationaler Ebene sogleich bestmöglich auszugestalten. Die Bundesregierung kann dabei auf die Expertise einer starken deutschen Datenschutzcommunity vertrauen.

Bereits angedeutet hat die Europäische Kommission die Überarbeitung der E-Privacy-Richtlinie. Diese Richtlinie regelt derzeit unter anderem die Verwendung von sogenannten „unique identifiers", also den Zugriff von auf Nutzergeräten gespeicherten Informationen zur Identifizierung gegenüber bestimmten Diensten. Nutzer werden durch derlei Informationen über verschiedene Dienste hinweg wiederidentifiziert, d.h. getrackt. Es entstehen Profile über Nutzer auf deren Basis sie diskriminiert werden können. Der gesamte Bereich der Onlinewerbung basiert auf diesem Mechanismus. Die Zahl der unique identifiers ist seit Verabschiedung der Richtlinie enorm angestiegen, vor allem durch die Verbreitung von Smartphones. Das „Internet der Dinge" potenziert die Zahl der unique identifiers noch einmal

um ein Vielfaches und macht Nutzungsweisen weit über Werbung hinaus denkbar, etwa bei der Preis- und Tarifdiskriminierung. Das Phänomen des Tracking ist schon nach derzeitigem Stand der Technik unreguliert und weitgehend außer Kontrolle. Hier besteht Handlungsbedarf, den die Bundesregierung so noch nicht kommuniziert hat.

Weiterhin möchten wir noch einmal auf unsere Vorschläge aus dem Jahr 2014 hinweisen. Dazu zählen:

- Stärkung und informationstechnische Qualifikation der Datenschutzbehörden
- mehr Transparenz über Datenverarbeitungen im privaten und öffentlichen Bereich durch obligatorische und öffentlich einsehbare Verfahrensverzeichnisse
- Dezentralisierung von Datenvorhaltungen und -verarbeitungen

Darüber hinaus darf Datenschutz nicht länger als ein One-Size-Fits-All-Ansatz verstanden werden. Ein einziges Datenschutzgesetz wie die EU-Datenschutzverordnung kann den vielfältigen Herausforderungen des Datenschutzes nicht gerecht werden. Etwa im Bereich Profiling und Diskriminierung sind zielgenauere, und wahrscheinlich auch bereichsspezifische Regeln, erforderlich. Ob etwa das derzeitige Datenschutzrecht mit seinem Bezug auf das Individuum Phänomene wie Profilbildungen von Gruppen zu erfassen vermag, ist fraglich. Ein weiteres Regulierungsfeld, das in unseren Forderungen von 2014 bereits anklang, ist Algorithmentransparenz. Algorithmen haben bereits heute weitreichenden Einfluss auf gesellschaftliches Zusammenleben. Sie dürfen nicht länger ein Geschäftsgeheimnis bleiben. Weiterhin kann die Datenschutzpolitik aus anderen Feldern wie der Umweltpolitik lernen. Diese versteht Umweltschutz schon lange als bereichsübergreifende Gestaltungsaufgabe und wirkt daher auch stark in die Bildungs- und Forschungspolitik, die Subventions- und Vergabepolitik und sogar Steuerpolitik hinein. In diesem Sinne könnten etwa Modell- und Infrastrukturprojekte im öffentlichen Sektor eine Nische darstellen, in der sich Datenschutzlösungen entwickeln und praxisfähig werden.

4. WLAN-Störerhaftung: Offenes WLAN ermöglichen, Providerprivileg für Alle.

Offene WLAN-Zugänge haben in Deutschland noch immer Seltenheitswert. Nur in wenigen Cafés, Bars oder Kneipen gibt es freies WLAN, bei Privatpersonen (z.B. den Nachbarn) in der Regel gar nicht. Bekommt man es in Cafés, muss man sich immer häufiger registrieren und die Betreiber sind gezwungen, das WLAN zu überwachen. Nur so können sie der sogenannten WLAN-Störerhaftung entgehen, die bis heute einem freien Netzzugang für alle im Weg steht.

Im "Sommer unseres Lebens" Urteil hatte der Bundesgerichtshof entschieden, dass Funknetzbetreiber als sogenannte Störer verschuldensunabhängig für Rechtsverletzungen haften, die Dritte über ihre WLANs im Internet verüben. Daher lässt sich ein offenes WLAN bislang nicht betreiben, ohne Abmahnungen oder langwierige, kostenintensive Rechtsstreitigkeiten zu riskieren. Für klassische Zugangsprovider wie etwa die Deutsche Telekom hingegen gibt es eine Haftungserleichterung, die als Providerprivileg bezeichnet wird. Danach ist ein Zugangsprovider nicht haftbar, wenn seine Kunden über den von ihm angebotenen Internetzugang beispielsweise Urheberrechtsverstöße begehen.

Diese Rechtslage verhindert eine flächendeckende, allgemein verfügbare und kostengünstige Versorgung mit mobilem Internet für alle. Die Vielzahl neuer Möglichkeiten zur demokratischen Teilhabe, zur Fortbildung und zum zivilgesellschaftlichen Engagement, welche die Informationsgesellschaft eröffnet, bleiben daher zahlreichen Menschen in Deutschland verschlossen. Insbesondere Personen mit geringem Einkommen und solche, die auf staatliche Transferleistungen angewiesen sind, können sich häufig keinen Internetzugang leisten. Die bestehende Rechtslage ist daher weder zukunftsorientiert noch sozial ausgewogen.

a. Maßnahmen der Bundesregierung

Die Pläne der Bundesregierung zur Abschaffung der WLAN-Störerhaftung waren bereits im Ansatz wenig ambitioniert. In der Digitalen Agenda wurde lediglich das Ziel formuliert, „Rechtssicherheit für die Anbieter solcher WLANs im öffentlichen Bereich, beispielsweise Flughäfen, Hotels, Cafés" zu schaffen. Diese Betreiber sollten nach dem Willen der Bundesregierung "grundsätzlich nicht für Rechtsverletzungen ihrer Kunden haften". Rein private Funknetzbetreiber fanden in der Digitalen Agenda hingegen keine Berücksichtigung.

Nach monatelangen Ankündigungen präsentierte die Bundesregierung schließlich im März 2015 einen ersten Gesetzentwurf zum Thema WLAN-Störerhaftung. Danach kommen Funknetzbetreiber in den Genuss der Haftungsfreistellung, wenn sie ihr WLAN verschlüsseln und den Zugang nur solchen Personen ermöglichen, die zuvor eingewilligt haben, keine Rechtsverletzungen zu begehen. Rein private Betreiber müssen darüber hinaus auch die Namen der jeweiligen Nutzerinnen und Nutzer kennen.

Nachdem dieser Entwurf auf massive Kritik aus Zivilgesellschaft, Wirtschaft und Wissenschaft gestoßen war, legte die Bundesregierung schließlich eine überarbeitete Fassung vor. Darin wird

keine Unterscheidung zwischen unterschiedlichen Anbietern von WLAN-Zugängen mehr vorgenommen. Stattdessen wird die Haftungsfreistellung nun allgemein davon abhängig gemacht, dass die Betreiber zumutbare Maßnahmen ergriffen haben, um eine Rechtsverletzung durch Nutzer zu verhindern. Laut Gesetzestext ist dies insbesondere der Fall, wenn Betreiber ihr Drahtlosnetzwerk mit angemessenen Maßnahmen gegen unberechtigte Zugriffe gesichert haben und nur solchen Personen den Zugang gewähren, die zuvor erklärt haben, im Rahmen der Nutzung keine Rechtsverletzungen zu begehen.

Am 15. Juni notifizierte die Bundesregierung den überarbeiteten Entwurf bei der EU-Kommission. Ändert ein Mitgliedstaat, wie hier im Fall der WLAN-Störerhaftung, gesetzliche Vorschriften über Dienste der Informationsgesellschaft, so muss er den Gesetzentwurf vor dessen Verabschiedung der EU-Kommission vorlegen. Diese überprüft die Vereinbarkeit der geplanten Änderung mit dem Unionsrecht und dem EU-Binnenmarkt. Währendessen darf der betreffende Mitgliedstaat das Gesetz nicht weiter vorantreiben oder in Kraft setzen. Im Falle des Regierungsentwurfs zur Abschaffung der WLAN-Störerhaftung wird das Notifizierungsverfahren voraussichtlich am 15. September enden.

b. Kritik

Mit ihrem Gesetzentwurf verfehlt die Bundesregierung ihr selbst gestecktes Ziel, rechtssichere Bedingungen für den Betrieb offener WLAN-Netze zu schaffen. Im Gegenteil würde damit der gegenwärtige rechtsunsichere Zustand zementiert und die Verbreitung offener Drahtlosnetze weiter verhindert.

So lässt der Entwurf offen, was genau unter „angemessenen Sicherungsmaßnahmen gegen unberechtigten Zugriff" zu verstehen ist. Mangels näherer Definition bleibt damit zunächst einmal unklar, welche Maßnahmen als angemessen im Sinne des Gesetzes anzusehen sind. Für Betreiber von Drahtlosnetzen besteht daher weiter keine Rechtssicherheit, falls sie ihre Netze für Dritte öffnen.

Unverständlich ist zudem, wie bei einem offenen WLAN überhaupt ein unberechtigter Zugriff erfolgen soll – schließich sind offene Netze gerade dadurch gekennzeichnet, dass sie von jeder beliebigen Person ohne Registrierung oder Eingabe eines Passwortes genutzt werden können. Diese Passage des Gesetzestextes kann daher nur so verstanden werden, dass die Bundesregierung entweder gerade keine genuin offenen Netze in Deutschland zulassen möchte oder das Thema offenes WLAN sachlich schlicht nicht richtig durchdrungen hat.

Der Regierungsentwurf verstößt außerdem gegen das EU-Recht. So überschreitet das Erfordernis, zumutbare Maßnahmen gegen Rechtsverletzungen durch Nutzer zu ergreifen, die Vorgaben des Artikels 12 der E-Commerce-Richtlinie. Dort sind abschließend die Bedingungen aufgezählt, unter denen sich Zugangsprovider auf die Haftungsfreistellung berufen können. Maßnahmen zur Vorbeugung gegen Rechtsverletzungen der Nutzer gehören nicht dazu.

Die vorgesehenen Regelungen des Regierungsentwurfs verletzen des Weiteren das EU-Grundrecht auf unternehmerische Freiheit aus Artikel 16 EU-Grundrechtecharta. Wird die unternehmerische Freiheit zum Schutz anderer Grundrechte eingeschränkt, so müssen die Einschränkungen nach ständiger Rechtsprechung des EuGH hinreichend wirksam sein, um einen wirkungsvollen Schutz der betreffenden Grundrechte sicherzustellen. Die beispielhaft in dem Entwurf aufgeführten Maßnahmen (Sicherung gegen unberechtigten Zugriff, Rechtstreueerklärung) sind offensichtlich ungeeignet, um Grundrechte Dritter vor Verletzungen durch WLAN-Nutzer zu schützen.

c. Alternative

Das Providerprivileg muss unterschiedslos auf sämtliche Personen ausgeweitet werden, die Dritten Zugang zum Internet vermitteln. Die Haftungsfreistellung darf ferner nicht von der Erfüllung besonderer Pflichten oder dem Ergreifen bestimmter Maßnahmen abhängig sein.

Bereits in der letzten Legislaturperiode hat der Digitale Gesellschaft e.V. eine Gesetzesänderung vorgeschlagen, um die bestehenden Hindernisse zu beheben und eine flächendeckende Versorgung mit offenen Funknetzzugängen effektiv zu fördern. Der Muster-Gesetzesentwurf sieht eine Änderung des Telemediengesetzes (TMG) vor. Das Providerprivileg des § 8 TMG, welches bisher nur klassische Zugangsprovider von der Haftung für Rechtsverletzungen ihrer

Kundinnen und Kunden freistellt, muss unterschieds- und vorbehaltlos auf sämtliche Betreiberinnen und Betreiber von Drahtlosnetzen ausgeweitet werden.

Konkret muss § 8 TMG um zwei Absätze mit folgendem Wortlaut ergänzt werden:

Absatz 3:
Der Ausschluss der Verantwortlichkeit (Absatz 1) umfasst auch gewerbliche und nichtgewerbliche Betreiberinnen und Betreiber von Funknetzwerken, die sich an einen nicht im Voraus namentlich bestimmten Nutzerkreis richten (öffentliche Funknetzwerke).

Absatz 4:
Der Ausschluss der Verantwortlichkeit (Absatz 1) umfasst auch Ansprüche auf Unterlassung.

5. Urheberrecht: Recht auf Remix einführen, offene Lizenzen bevorzugen.

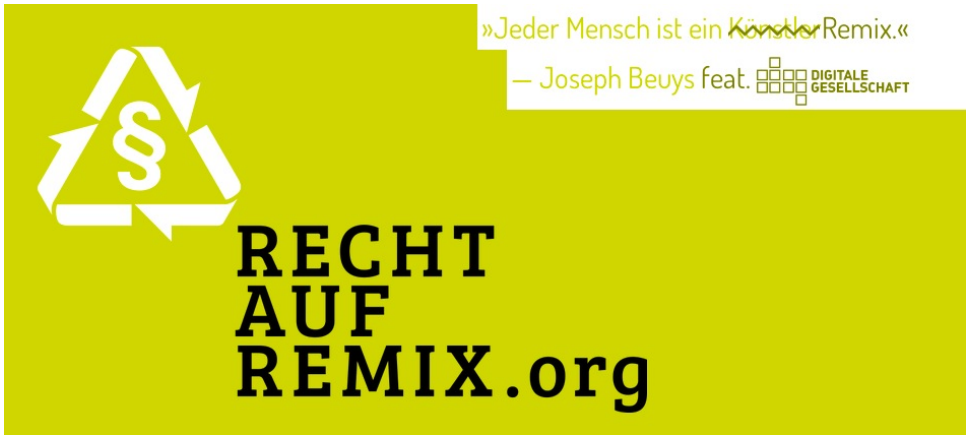
Die zentrale Bedeutung des Urheberrechts im digitalen Zeitalter war auch in der Digitalen Agenda der Bundesregierung zu erkennen - und zwar vor allem daran, dass es an verschiedenen Stellen der digitalen Agenda thematisiert wurde. Die Bandbreite reicht vom Urheberrecht als "Ordnungsrahmen für die digitale Wirtschaft" über die Forderung nach einer allgemeinen "Bildungs- und Wissenschaftsschranke" im Urheberrecht bis hin zu Fragen des "Verbraucherschutzes in der digitalen Welt".

a. Maßnahmen der Bundesregierung

Zwar wird auf Ebene der Fachabteilungen des Bundesministeriums für Justiz an punktuellen Reformmaßen im Urheberrecht gearbeitet, öffentlich bekannt oder gar in Umsetzung begriffen ist bislang jedoch noch kein einziger konkreter Reformvorschlag. In einem Interview im März 2015 skizzierte Justizminister Heiko Maas (SPD) zwar eine Reihe von Reformprojekten, konkrete Gesetzesinitiativen gibt es bislang jedoch keine.

Die einzige gesetzliche Maßnahme der Bundesregierung im Urheberrecht war bislang die Entfristung der Ausnahmeregelung des § 52a Urheberrechtsgesetz, der Schulen und Universitäten die Bereitstellung von Inhalten in Intranets erlaubt. Es wurde also eine ohnehin bereits seit Jahren bestehende Regelung verlängert.

Neben Justizminister Maas präsentierte Monika Grütters (CDU), Staatsministerin für Kultur in Medien bei der Bundeskanzlerin, Ideen zum Urheberrecht in Form eines Katalogs an, „Kulturpolitische[n] Forderungen für das Urheberrecht im digitalen Umfeld“. Anlass von Grütters Einlassungen war, den ohnehin sehr vagen und zurückhaltenden Reformbestrebungen ihres Parteikollegen und EU-Kommissars Günther Oettinger entgegenzutreten. Dieser hatte ein Ende von Geoblocking in der EU gefordert sowie Überlegungen hinsichtlich eines einheitlichen EU-Urheberrechts angestellt. Das Grütters-Papier lehnt beides vehement ab und sieht abgesehen von Verschärfungen bei der Rechtsdurchsetzung keinen Reformbedarf im Urheberrecht.



b. Kritik

Die Vorhaben der Bundesregierung im Bereich des Urheberrechts waren alles andere als ambitioniert - auch unter Berücksichtigung der eingeschränkten nationalen Regulierungsspielräume. Weder eine Modernisierung und Ausdehnung des Zitatrechts um Remix und Mashups zu erleichtern noch wirksame Eindämmung von Abmahnunwesen oder offene Lizenzen für öffentlich finanzierte Inhalte standen am Programm der Regierung.

Bislang wurden aber nicht einmal in den aus- und selbstgewählten Bereichen, in denen Urheberrecht in der digitalen Agenda Thema war, konkrete Fortschritte erzielt. Im Gegenteil, die Einlassungen von Staatsministerin Grütters legen nahe, dass die Regierung auch bei noch so zaghaften EU-Reformbestrebungen auf der Bremse stehen wird.

c. Alternative

Hier hat sich seit unserer Analyse der digitalen Agenda nichts geändert, die Probleme und Lösungswege sind dieselben geblieben. Während in Deutschland also in Sachen Urheberrecht stillsteht, scheint auf europäischer Ebene durchaus etwas in Bewegung zu geraten.

Stärkstes Indiz für Reformwillen auf EU-Ebene ist der mit großer Mehrheit angenommene Bericht zur EU-Urheberrechtsrichtlinie, für den die deutsche Piratenabgeordnete Julia Reda verantwortlich zeichnet. Der Bericht könnte insofern einen Wendepunkt in der Urheberrechtsdebatte darstellen, weil er eine Abkehr von Ausdehnung und Verschärfung von Urheberrechten hin zu Stärkung von Schranken und Nutzungsrechten empfiehlt. Gleichzeitig haben es wichtige Punkte wie ein EU-weit einheitliches Urheberrecht, eine offen Schranke nach Vorbild des US-Fair-Use oder ein Recht auf Remix nicht in den finalen Bericht geschafft.

6. Netzneutralität: Diskriminierungsfreies Internet erhalten, Spezialdienste klar definieren.

Ein diskriminierungsfreier Internetzugang ist für die Verwirklichung der Meinungs- und Informationsfreiheit ebenso wie für die demokratische Teilhabe im digitalen Raum von zentraler Bedeutung. Zudem sichert ein solcher Zugang die Innovationsoffenheit des Netzes, da er die Markteintrittsschwelle für die Anbieter neuer elektronischer Dienste niedrig hält.

Für ein freies und offenes Netz bedarf es daher der Gewährleistung der Netzneutralität. Nach diesem Grundsatz werden sämtliche Datenpakete im Internet unabhängig von Absender, Empfänger oder Inhalt in gleicher Qualität und Geschwindigkeit übermittelt. Große Telekommunikationsunternehmen lobbyieren seit Jahren für eine Aufweichung dieses Prinzips und fordern die Zulassung sogenannter Spezialdienste, über die besonders attraktive und beliebte Internetangebote nur noch gegen gesonderte Bezahlung verfügbar sein sollen. Dringen die Provider mit ihrem Verlangen durch, so droht eine Zerschlagung des Internet in ein Zwei-Klassen-Netz, in dem sich Verbraucherinnen und Verbraucher mit einem Tarif- und Paketdschungel konfrontiert sehen und für Start-Ups und nichtkommerzielle Anwendungen Markteintrittsbarrieren und Wettbewerbsnachteile entstehen.

Das EU-Parlament hat diese Gefahren weitestgehend erkannt und bei der Abstimmung über eine europäische Telekommunikationsmarktverordnung im April 2014 eine vergleichsweise netzneutralitätsfreundliche Gesetzesfassung beschlossen. Leider stimmte der EU-Ministerrat, in dem die Regierungen der Mitgliedstaaten vertreten sind, für eine fast diametral entgegengesetzte Position. In den anschließenden Trilog-Verhandlungen, in denen ein Kompromiss zwischen den Fassungen von Rat und Parlament gefunden werden soll, einigten sich die Unterhändler von Ministerrat und EU-Parlament auf eine gemeinsame Position. Auch diese Kompromissfassung der geplanten Gesetzgebung sichert die Netzneutralität keineswegs, sondern lässt aufgrund erheblicher Rechtsunsicherheiten große Schlupflöcher für die Errichtung eines Zwei-Klassen-Netzes. Unklar bleibt nach dem gegenwärtigen Text etwa, ob Praktiken wie das Zero-Rating zulässig sind und unter welchen Voraussetzungen bestimmte Daten priorisiert sowie optimierte Dienste (früher: Spezialdienste) angeboten werden dürfen.

Die erforderliche Zustimmung des Parlaments zum Trilog-Kompromiss steht zum gegenwärtigen Zeitpunkt noch aus.

a. Maßnahmen der Bundesregierung

Schon in der Digitalen Agenda wurde die Netzneutralität nur kursorisch behandelt, was der herausragenden Bedeutung des Themas weder in quantitativer noch in qualitativer Hinsicht gerecht wurde. Die Bundesregierung versprach dort lediglich pauschal, die Gewährleistung der Netzneutralität als Ziel gesetzlich zu verankern und dafür auch auf europäischer Ebene einzutreten.

Das tatsächliche Engagement der Bundesregierung beschränkte sich darauf, im Rahmen des EU-Gesetzgebungsverfahrens zur Netzneutralität Mitte Dezember 2014 ein Positionspapier beim Ministerrat einzubringen. Anders als von der Bundesregierung beworben, handelte es sich dabei jedoch nicht um einen ausgewogenen Kompromiss zwischen den Interessen der Netzgemeinde und denen der Wirtschaft. Vielmehr kam sie damit weitestgehend den Forderungen der Telekommunikationslobby nach der Legalisierung von Spezialdiensten und wettbewerbsfeindlichen Praktiken wie dem Zero-Rating nach. Gleichwohl vermochte sich die Bundesregierung mit ihrer Position im Ministerrat nicht durchzusetzen. Der schließlich dort verabschiedete Regulierungsvorschlag erwies sich sogar als noch netzneutralitätsfeindlicher und providerfreundlicher als der Entwurf der Bundesregierung.

b. Kritik

Von dem Versprechen der Bundesregierung, sich auch auf europäischer Ebene für eine gesetzliche Verankerung der Netzneutralität einzusetzen, ist ein Jahr nach Vorstellung der Agenda wenig Greifbares geblieben.

Statt die netzneutralitätsfreundliche Position des EU-Parlamentes im Ministerrat und in der Öffentlichkeit zu stützen und zu verteidigen, fielen insbesondere Bundeskanzlerin Merkel und Bundeswirtschaftsminister Gabriel durch Äußerungen auf, die Zweifel an ihrem Engagement für die Netzneutralität sowie an ihrer Sachkunde aufkommen lassen. Beide sprachen sich wiederholt für die Einführung von Spezialdiensten mit der Begründung aus, dass diese für Anwendungen wie das automatisierte Fahren oder die Telemedizin unabdingbar seien. Tatsächlich können derartige Echtzeit-Anwendungen weder über das offene Internet noch über Spezialdienste mit der nötigen Ausfallsicherheit angeboten werden. So bedürfen die derzeit etwa bei BMW oder Google entwickelten autonomen Fahrzeuge keines Internetzugangs, da die

Firmen aus Gründen der Qualitätssicherung auf eigene Kommunikationsnetze setzen. Die Äußerungen von Merkel und Gabriel entpuppen sich damit als bloßes Propaganda-Sprech der Telekommunikationslobby.

Auf einer Vodafone-Konferenz Anfang Dezember 2014 sagte die Bundeskanzlerin außerdem: „Wir brauchen uns über Netzneutralität nicht zu unterhalten, wenn die Kapazitäten nicht zur Verfügung stehen.“. Tatsächlich ist das genaue Gegenteil richtig. Das Prinzip der Netzneutralität sichert die diskriminierungsfreie Verteilung der knappen Ressource Bandbreite. Sind hingegen Leitungskapazitäten im Überfluss vorhanden, so verliert die Frage, welche Daten schneller und welche langsamer übermittelt werden, an Bedeutung und Brisanz.

Es verwundert daher wenig, dass auch das von der Bundesregierung in den EU-Ministerrat eingebrachte Positionspapier weitestgehend den Wünschen der Providerlobby entsprach. Spezialdienste, Zero-Rating, Blockierungen und Drosselungen der Zugänge zum offenen Internet – all das wäre damit legalisiert worden. Es wird deutlich, dass die Bundesregierung entgegen ihrer Beteuerungen in der Digitalen Agenda die Netzneutralität bislang eher als ein Hindernis für die Einführung von Spezialdiensten als ein elementares Prinzip zur Sicherung eines freien, offenen und diskriminierungsfreien Internet betrachtet.

c. Alternative

Zahlreiche Chancen für eine gesetzliche Absicherung der Netzneutralität hat die Bundesregierung bereits verspielt. Um zu verhindern, dass der nunmehr ausgehandelte Trilog-Kompromiss mit seinen erheblichen Rechtsunsicherheiten geltendes Unionsrecht wird, muss die Bundesregierung die konservativen und sozialdemokratischen Abgeordneten im Europäischen Parlament dazu aufrufen, die verbleibenden Lücken durch Änderungsanträge und ein entsprechendes Abstimmungsverhalten zu schließen.

Bleiben die Rechtsunsicherheiten des Trilog-Kompromisses hingegen bestehen, so wäre damit vor allem den großen Telekommunikationsunternehmen und Netzwerkbetreibern ein Gefallen getan, da diese über die nötigen Mittel verfügen, um langwierige Verfahren durchzustehen und sich die gewünschte Auslegung auf dem Rechtsweg zu erstreiten. Schaden würden hingegen die Rechte und Interessen von Verbraucherinnen und Verbrauchern sowie der europäischen Online-Wirtschaft nehmen, da eine echte Sicherung der Netzneutralität normenklare und eindeutige Regeln braucht.

Das Parlament muss daher die bislang noch bestehenden Unklarheiten beseitigen und durch explizite Regelungen ersetzen. Dazu gehört ein ausdrückliches Verbot wettbewerbsfeindlicher Praktiken wie Zero-Rating ebenso wie eine Verschärfung der Kriterien für optimierte Dienste und für Maßnahmen des Verkehrsmanagements. Die entscheidenden Regelungen sollten zudem in den eigentlichen Artikeln und nicht lediglich wie bislang vorgesehen in den Erwägungsgründen untergebracht werden, um ihnen das nötige Gewicht zu verleihen.

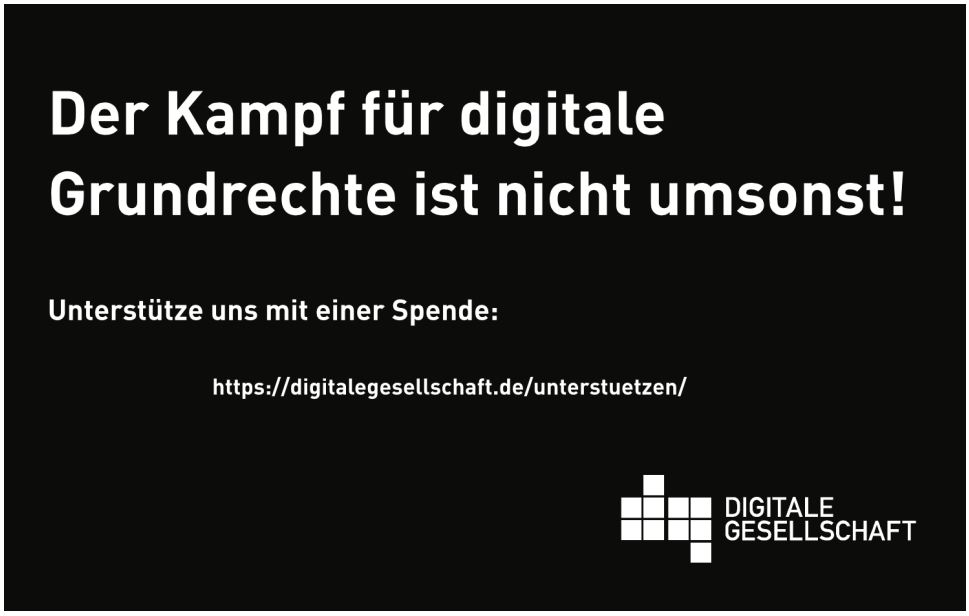
7. Breitbandausbau: Schnelle Netze schaffen, Daseinsvorsorge wahrnehmen.

Bei der flächendeckenden Versorgung mit schnellen Internetanschlüssen befindet sich Deutschland im europäischen und internationalen Vergleich noch immer im Hintertreffen. Noch nicht einmal vier Prozent der bundesdeutschen Haushalte sind derzeit an das Glasfasernetz angebunden und bei Weitem nicht alle der verfügbaren Anschlüsse werden überhaupt genutzt. Der Bandbreitenbedarf wird mit der Fortentwicklung digitaler Technologien, Anwendungen und Diensten in den kommenden Jahren stetig steigen. Ohne eine breite Abdeckung mit leistungsfähigen Netzanschlüssen bleibt Deutschland der Weg in eine digitalisierte Gesellschaft, in der demokratische Teilhabe, Meinungs- und Informationsfreiheit, Innovation und Wettbewerb gewährleistet sind, versperrt.

a. Maßnahmen der Bundesregierung

Auch ein Jahr nach der Veröffentlichung der Digitalen Agenda hält die Bundesregierung an ihrem Ziel fest, „mittels eines effizienten Technologiemix eine flächendeckende Breitbandinfrastruktur mit einer Downloadgeschwindigkeit von mindestens 50 Mbit/s bis 2018“ zu schaffen. Dabei soll der Breitbandausbau primär „marktgetrieben“, also im Wege privatwirtschaftlicher Investitionen, verwirklicht werden. Die Bundesregierung beabsichtigt daher, “eine investitions- und innovationsfördernde Regulierung” zu unterstützen und “in den Verhandlungen zur Weiterentwicklung des europäischen Rechtsrahmens” darauf zu achten, “dass der Regulierungsrahmen den Wettbewerb zwischen den Unternehmen wahrt und die notwendige Planungssicherheit für Investitionen geschaffen wird”.

Schätzungen der Bundesregierung zufolge liegt der Investionsbedarf für den Breitbandausbau bei insgesamt etwa 10 Milliarden Euro. Entsprechend ihrer oben skizzierten Ausbaustrategie sollen 80% dieser Summe, also rund 8 Milliarden Euro, von großen Telekommunikationsunternehmen aufgebracht werden. Deren Ausgaben für den Breitbandausbau werden über die sogenannte „Netzallianz Digitales Deutschland“, ein vom Bundesministerium für Verkehr und Digitale Infrastruktur ins Leben gerufenes Forum, koordiniert. Weitere 1,1 Milliarden Euro sollen über Förderprogramme des Bundes bereitgestellt werden. Eine dritte Säule der Finanzierung bilden die Erlöse aus der Versteigerung der mobilen Breitband-Frequenzen („Digitale Dividende II“). Anders als von der Bundesregierung prognostiziert, brachte die zwischen Ende Mai und Mitte Juni 2015 durchgeführte Versteigerung jedoch nicht eine weitere Milliarde, sondern lediglich 665 Millionen Euro für den Breitbandausbau ein.



b. Kritik

Bereits das von der Bundesregierung ausgegebene Fernziel des Breitbandausbaus, nämlich die Schaffung einer flächendeckenden Versorgung mit einer Downloadgeschwindigkeit von mindestens 50 Mbit/s, erweist sich als zu unbestimmt und nicht zukunftstauglich.

Zunächst ist offen, worauf sich die Datenübertragungsrate von 50 Mbit/s überhaupt bezieht. Erfolgt der Netzzugang beispielsweise über eine Funktechnologie wie LTE, so teilen sich sämtliche Nutzer einer Funkzelle die insgesamt darüber zur Verfügung stehende Bandbreite. Bezieht sich die Vorgabe von 50 Mbit/s also nur auf den LTE-Zugang in seiner Gesamtheit, so ist damit nichts über die im Einzelfall tatsächlich nutzbare Bandbreite gesagt.

Des Weiteren dürfte eine Datenübertragungsrate von 50 Mbit/s schon deutlich vor dem Jahr 2018 nicht mehr ausreichend sein, um dem ständig wachsenden Bandbreitenbedarf gerecht zu werden. Neben der zunehmenden Verbreitung von hochauflösendem Videostreaming werden auch Entwicklungen wie das Internet der Dinge, die Digitalisierung der Industrie („Industrie 4.0“) sowie zurzeit noch nicht absehbare Innovationen zusätzlichen Traffic verursachen. Der jüngsten Breitbandstudie des Bundesverbandes Breitbandkommunikation (BREKO) zufolge wird der Bandbreitenbedarf eines durchschnittlichen Netzzugangs im Jahr 2018 bei 100 Mbit/s in Wohngebieten und bei 240 Mbit/s in Gewerbegebieten liegen. Vor diesem Hintergrund erscheint die Zielvorgabe von 50 Mbit/s weder sinnhaft noch nachhaltig. Hinzu kommt, dass sich diese Vorgabe explizit nur auf die Downloadgeschwindigkeit bezieht. Die gerade für die Industrie besonders wichtige Uploadgeschwindigkeit hingegen findet weder in den Planungen noch in den Umsetzungsmaßnahmen der Bundesregierung irgendeine Berücksichtigung.

Abgesehen davon ist auch das Vorhaben, eine flächendeckende Versorgung mit schnellem Internet über einen „effizienten Technologiemix“ herzustellen, im Hinblick sowohl auf die

Zukunftsfestigkeit als auch auf die Verbraucherinteressen problematisch. Statt den konsequenten Ausbau von Glasfaseranschlüssen bis zum Gebäude zu forcieren, soll es den Telekommunikationsunternehmen nach dem Willen der Bundesregierung freigestellt sein, die Netzzugänge auch über Funktechnologien wie LTE sowie über optimierte Datenübertragungen wie VDSL2-Vectoring zu verwirklichen. Dies nützt vor allem den Telekommunikationsunternehmen, welche die erheblichen Investionen in den Glasfaserausbau scheuen und deshalb kostengünstigere, aber für den Endverbraucher nachteilige Varianten bevorzugen. Während der Kernbereich des Netzes auf Glasfaserverbindungen beruht, treten Flaschenhalseffekte nämlich vor allem auf der Strecke zwischen Hauptverteiler und Teilnehmeranschluss („letzte Meile") auf. Die meisten Haushalte in Deutschland sind mit der nächsten Verteilerstelle derzeit über Kupferleitungen verbunden, was die verfügbaren Bandbreiten empfindlich limitiert. Zwar können die Bandbreiten bei Kupferleitungen im Wege einer optimierten Datenübertragung per VDSL2-Vectoring theoretisch auf bis zu 500 Mbit/s erhöht werden. Mit zunehmender Entfernung zwischen Verteilerstelle und Hausanschluss nimmt dieses Optimierungpotential jedoch kontinuierlich ab, so dass schon bei einem Abstand von 200 Metern nur noch maximale Bandbreiten von 100 bis 120 Mbit/s erzielt werden können. Hinzu kommen die wettbewerbsfeindlichen Auswirkungen dieser Technologie. An einem Hauptverteiler kann stets nur ein Anbieter VDSL2-Vectoring betreiben, während dessen Konkurrenten parallel dort allenfalls nicht optimierte und daher langsamere Zugänge anbieten können. Mit der Verlegung eines Glasfaseranschlusses bis ins Gebäude können diese Nachteile weitestgehend vermieden werden. Zwar müssten auch hier die letzten Meter bis zum Teilnehmer per Kupferleitung überbrückt werden. Da diese Strecke jedoch deutlich kürzer ist, fallen die limitierenden Effekte der Kupferleitung dabei allerdings deutlich schwächer aus als bei VDSL2-Vectoring.

Der schwerwiegendste Fehler des Ausbaukonzepts der Bundesregierung liegt nach wie vor darin, die flächendeckende Versorgung mit schnellen Internetanschlüssen im Wesentlichen den Telekommunikationsunternehmen zu überlassen. In einer digitalisierten Gesellschaft stellt der Breitbandausbau jedoch eine zentrale Infrastrukturaufgabe dar, die als Teil der Daseinsvorsorge zunächst dem Staat zufällt. Für die Grundversorgung mit schnellem Internet ist neben großer Bandbreite vor allem die technische und inhaltliche Diskriminierungsfreiheit des Netzzugangs von essentieller Bedeutung. Nur ein Netz, an dem Alle unter den gleichen Bedingungen teilhaben können und in dem sie selbst entscheiden, welche Inhalte, Dienste und Anwendungen sie nutzen, kann als infrastrukturelle Grundlage einer demokratisch verfassten Gesellschaft dienen. Diese Chancengleichheit bei Zugang und Nutzung des Internet gewährleistet das Prinzip der Netzneutralität. Folgerichtig wäre es also, auf eine konsequente gesetzliche Absicherung der Netzneutralität hinzuwirken.

Der bisherige Ansatz der Bundesregierung geht allerdings genau in die entgegengesetzte Richtung. Nach ihrer Vorstellung sollen primär große Telekommunikationsunternehmen die flächendeckende Versorgung mit schnellem Internet vorantreiben. Um für diese Unternehmen neue Quellen für Investitionsmittel zu eröffnen, ist sie bereit, Einschnitte bei der Netzneutralität

und die Einführung kostenpflichtiger Überholspuren im Internet („Spezialdienste“ oder „Qualitätsklassen“) zu hinzunehmen. Anders als immer wieder seitens der Bundesregierung kommuniziert, würden diese Sonderzugänge nicht nur Anwendungen wie das fahrerlose Auto oder die Telemedizin ermöglichen. Vielmehr könnten auch beliebte Dienste des offenen Internet ohne Weiteres auf Spezialzugänge ausgelagert werden, welche Verbraucherinnen und Verbraucher ebenso wie die Anbieter von Online-Diensten gesondert bezahlen müssten. Neben einem neuen Dickicht aus Zugangspaketen und Tarifen drohen damit auch Markteintrittshürden und Wettbewerbsnachteile für Startups, die nicht die Finanzkraft etablierter Player wie Google, Facebook oder Microsoft besitzen. Sie könnten ihre Nutzerinnen und Nutzer nur über das „Best Effort“ Internet erreichen, während die zahlungskräftigere Konkurrenz sich einen besseren Kundenzugang schlicht erkaufen könnte.

Die Pläne der Bundesregierung beschädigen daher die Innovationskraft des Netzes und leisten der digitalen Spaltung der Gesellschaft weiteren Vorschub. Hinzu kommt, dass der ökonomische Anreiz für Investitionen in den Erhalt und die Fortentwicklung des offenen Internet aus Sicht der Telekommunikationsunternehmen immer weiter sinkt, je mehr Umsatz sie mit Spezialdiensten machen. Die Legalisierung dieser Überholspuren führt daher nicht nur geradewegs in ein Zwei-Klassen-Netz, sie setzt auch langfristig die falschen Impulse beim Breitbandausbau.

c. Alternative

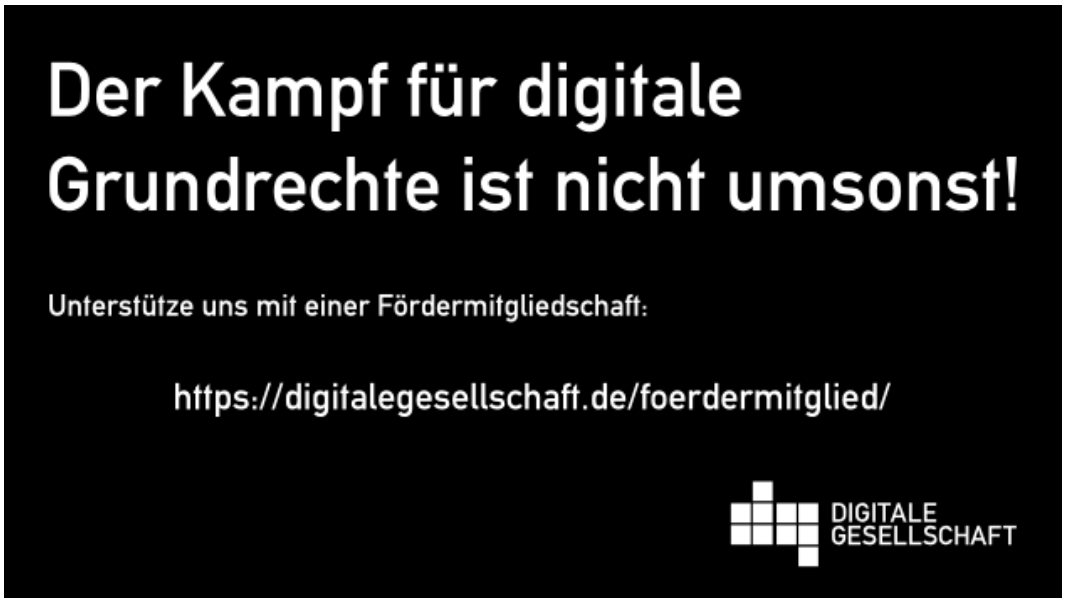
Zunächst muss der konsequente Ausbau von Glasfaseranschlüssen bis zum Gebäude oberste Priorität haben. Dies bietet die Aussicht, eine der kritischsten Schwachstellen bei der flächendeckenden Versorgung mit schnellem Internet dauerhaft und zukunftssicher zu schließen. Zudem würden sich damit auch Vorgaben zur verfügbaren Bandbreite erübrigen.

Darüber hinaus erscheint eine Universaldienstverpflichtung für Telekommunikationsdienstleister als überaus wünschenswert. Als infrastrukturelle Grundlage einer digitalen Gesellschaft ist das Internet ein öffentliches Gut. Es ermöglicht politische Partizipation, öffnet Räume für die Betätigung von Meinungs-, Informations- und Kunstfreiheit und befördert Wettbewerb und Innovationen. Damit entspricht es in seiner gesamtgesellschaftlichen Tragweite bereits heute anderen Elementen der Daseinsvorsorge wie Wasser- und Energieversorgung, öffentlichen Straßen oder Gesundheitswesen. Diese Bedeutung wird weiter zunehmen, je tiefer digitale Technologie unseren Alltag durchdringt. Um der digitalen Spaltung der Gesellschaft vorzubeugen, muss der Staat im Rahmen der Grundversorgung daher gewährleisten, dass allen Teilen der Bevölkerung der Zugang zum Internet offen steht. Andere Länder haben diesen Schritt bereits getan. So ist in der Schweiz bereits seit 2008 eine entsprechende Universaldienstverpflichtung in Kraft. In den USA wiederum hat die dortige Regulierungsbehörde FCC kürzlich angekündigt, Telekommunikationsunternehmen künftig als „common carrier“ einzustufen, was der hiesigen Einordnung als Grundversorger entspricht.

Nicht zuletzt aufgrund der Einordnung des Internet als öffentliches Gut wäre es sinnvoll, mehr

Bundesmittel als bisher für den Breitbandausbau bereitzustellen. Das bislang verfolgte Breitband-Konzept des „marktgetriebenen Ausbaus“ erweist sich, wie oben dargestellt, im Hinblick auf die Qualität der Daseinsvorsorge als kontraproduktiv. Richtig wäre es vielmehr, den Ausbau soweit wie möglich von den ökonomischen Interessen der Telekommunikationsunternehmen zu entkoppeln, um die oben beschriebenen Zielkonflikte zu vermeiden. Dass dies keineswegs den völligen Abzug privater Investitionsmittel aus dem Breitbandausbau bedeuten würde, zeigte sich kürzlich in den USA. Nachdem die dortige Regulierungsbehörde FCC angekündigt hatte, Telekommunikationsunternehmen künftig als „common carriers“ zu kategorisieren, erklärte der drittgrößte US-Provider Sprint Corp, weiterhin unverändert in den Netzausbau investieren zu wollen. Zudem äußerte das Unternehmen die Erwartung, dass seine Konkurrenten sich ebenso verhalten werden. Diese Einschätzung entspricht der Dynamik eines wettbewerbsgetriebenen Marktes, in dem derjenige Marktanteile verliert, der Investitionen in Servicequalität und -umfang verabsäumt.

Statt sich beim Breitbandausbau in die Abhängigkeit einiger weniger Telekommunikationskonzerne zu begeben und aus fiskalischen Überlegungen heraus die Diskriminierungsfreiheit des Netzes zu opfern, wäre es im Sinne der Daseinsvorsorge oberste Aufgabe der Bundesregierung, alternative, netzneutralitätsfreundliche Finanzierungskonzepte beim Breitbandausbau zu erarbeiten und umzusetzen. Die Bereitstellung zusätzlicher Bundesmittel kann ein Baustein eines solchen alternativen Finanzierungskonzeptes sein. Daneben wären aber auch andere Ansätze, etwa ein bürgerfinanzierter und staatlich abgesicherter Fond oder genossenschaftliche Modelle, denkbar. Auf diese Weise könnte die Bevölkerung nicht nur unmittelbar am Breitbandausbau mitwirken und von dem späteren Netzbetrieb profitieren; zusätzlich könnte auch nachhaltig sichergestellt werden, dass bei der Fortentwicklung der Netzinfrastruktur die Belange des Gemeinwohls nicht aus dem Blick geraten.



Der Digitale Gesellschaft e.V. ist ein gemeinnütziger Verein, der sich seit seiner Gründung im Jahr 2010 für Grundrechte und Verbraucherschutz im Netz einsetzt. Zum Erhalt und zur Fortentwicklung einer offenen digitalen Gesellschaft engagiert sich der Verein gegen den Rückbau von Freiheitsrechten im Netz und für die Realisierung digitaler Potentiale bei Wissenszugang, Transparenz, Partizipation und kreativer Entfaltung.

Spendenkonto:
BIC: GENODEM1GLS
IBAN: DE88 4306 0967 1125 0128 00

Kontakt:
Digitale Gesellschaft e. V.
Sophienstraße 5
10178 Berlin
Tel.: 030/68916575
info@digitalegesellschaft.de

Twitter: @digiges
Youtube: youtube.com/user/digitalegesellschaft
Facebook: facebook.com/DigitaleGesellschaft
Flickr: flickr.com/photos/digitalegesellschaft/