Tätigkeitsbericht 2016

Ein ereignisreiches netzpolitisches Jahr geht zu Ende und wir möchten allen, die uns unterstützt haben, Danke sagen! Nur durch Eure Unterstützung können wir uns tagein, tagaus für eine bessere Netzpolitik einsetzen. Damit meinen wir: Mündigkeit und Kompetenz in der Nutzung digitaler Technologien, den Erhalt demokratischer Mitbestimmung und Grundrechte in der digitalen Transformation sowie die Reflektion dieser Entwicklungen in Wissenschaft und Bildung.

2016 war aus netzpolitischer Sicht ein ereignisreiches Jahr. Ob Datenschutz, Überwachung, Zugang zu Netzen oder Urheberrecht – überall gab es weitreichende Änderungen. Der Datenaustausch mit den USA wurde auf eine neue rechtliche Grundlage gestellt, ohne jedoch die massenhafte Überwachung von Europäerinnen und Europäern zu stoppen. Mit der Einführung einer Vorratsdatenspeicherung von Reisedaten wird der Weg für eine Total-Überwachung des Reiseverkehrs geebnet. Zugleich müssen Fortschritte auf dem Gebiet des Zugangs zu Netzen und Inhalten, wie bei der WLAN-Störerhaftung, mühsam erkämpft werden. Fehlende Medienkompetenz bleibt ein Problem, während neue Themen wie individualisierte Preise für Verbraucherinnen und Verbraucher beim Online-Handel aufkommen. Es bleibt viel zu tun und wir brauchen einen langen Atem.

Deshalb vorneweg, wie auch zum Schluss die Aufforderung:

Werde / werden Sie Fördermitglied oder unterstützen Sie uns mit einer Spende, damit wir die Arbeit fortführen können.

https://digitalegesellschaft.de/foerdermitglied/

https://digitalegesellschaft.de/unterstuetzen/

1. Überwachung: Einsatz für Grund- und Freiheitsrechte, informationelle Selbstbestimmung und Rechtsstaatlichkeit

1.1 Kampagne gegen die BND-Reform

In Reaktion auf den NSA-Skandal und massenhafte Rechtsverstöße des Bundesnachrichtendienstes (BND) kündigte die Bundesregierung an, dass die Berechtigungen des Auslandsnachrichtendienstes durch eine neue Reform verschärft werden sollten. Die Reform läuft auf eine großzügige Legalisierung und Ausweitung der bislang rechtswidrigen Spähexzesse des BND und seiner Zusammenarbeit mit ausländischen Diensten hinaus. Gleichzeitig sollte die parlamentarische Kontrolle deutlich geschwächt werden.

Im Zentrum der Reform steht die sogenannte Ausland-Ausland-Fernmeldeaufklärung. Damit sind Abhörmaßnahmen gemeint, mit denen vom bundesdeutschen Inland aus die Kommunikation von Ausländern im Ausland erfasst wird. Im Rahmen einer Anhörung im NSA-Untersuchungsausschusses gingen führende Verfassungsrechtler wie der frühere Präsident des Bundesverfassungsgerichts, Hans-Jürgen Papier, sogar so weit, die Auslandsaufklärung des BND als „insgesamt rechtswidrig" zu bewerten.

Gegen diese weitgehenden Eingriffsbefugnisse in Grundrechte war fundamentaler Protest notwendig.

a) Telefonaktion: Unser kostenloses Anruf-Tool

Durch das Anruftool haben wir die Menschen kostenlos mit einem Abgeordneten verbunden, ihnen damit eine Stimme gegeben und den Dialog zwischen Bürger*innen und Abgeordneten zum Thema Grundrechte und Rechtsstaatlichkeit befördert.

b) Online-Petition: Wir wollen keine deutsche NSA!

Wir haben gemeinsam mit der Aktivistin Katharina Nocun, der Humanistischen Union und dem Whistleblower-Netzwerk sowie Dr. Rolf Gössner von der Internationalen Liga für Menschenrechte eine Online-Petition gegen das geplante BND-Gesetz gestartet. Unter dem Titel „BND-Gesetz verhindern: Wir wollen keine deutsche NSA!" forderten wir Bundeskanzlerin Angela Merkel, Bundesinnenminister Thomas de Maizière, Bundesjustizminister Heiko Maas sowie die Mitglieder des Bundestages dazu auf, das Gesetz nicht zu verabschieden.

c) Demonstration

Am 26. September und am 20. Oktober haben wir unseren Protest auf die Straße gebracht. Wir haben am Brandenburger Tor auf dem Pariser Platz und vor dem Gebäude des Reichstags in Berlin gegen den BND protestiert. Mit den Initiatoren Katharina Nocun (Netzaktivistin), Amnesty International, Reporter ohne Grenzen, Deutscher Journalisten-Verband sowie dem Deutschen Anwaltverein haben wir versucht, dem Aufbau einer deutschen NSA entgegenzuwirken.

d) Blogbeitrag

Durch unseren Blogbeitrag haben wir die gravierenden Folgen der BND-Reform in Bezug auf die Geltung der Menschenrechte vermittelt. Die Eingriffe des BND würden ohne gesetzliche Grundlage geschehen. Zudem haben wir thematisiert, dass die parlamentarische Kontrolle der Reform weiterhin zu Bruch gehen wird, weil die Überprüfung dieser Reform nicht vorgesehen ist.

Trotz der vielen Proteste wurde das Gesetz verabschiedet, welches die Befugnisse des deutschen Auslandsgeheimdienstes völlig neu regelt. Das Gesetz ermöglicht dem BND die massenhafte Überwachung elektronischer Kommunikation aufgrund von Kriterien, deren vage Formulierung dem Geheimdienst nahezu ungehinderten Zugriff auf die Telekommunikation der Bürgerinnen und Bürger im Ausland erlaubt. Folglich wird uns das Thema der BND-Reform weiter im Jahr 2017 beschäftigen.

BND-Reform verhindern: Telefonaktion und Petition gegen Massenüberwachung (15.09.2016): https://digitalegesellschaft.de/2016/09/bnd-reform-verhindern

1.2 Öffentliche Begleitung der Verhandlungen zur EU-Anti -Terror-Richtlinie

In der EU gab es keine einheitlichen Straftatbestände für Handlungen mit terroristischem Hintergrund. Jeder Mitgliedstaat hat selbst definiert, welche Handlungen sanktioniert werden und welche nicht. Insbesondere bei Reisen für die Vorbereitung terroristischer Akte, der Verbreitung von terroristischer Propaganda und der Finanzierung von Terrorismus gab es keinen gemeinsamen europäischen Weg. Am 2. Dezember 2015 hat die EU-Kommission daher, insbesondere als Reaktion auf die vorausgegangenen Anschläge, eine Richtlinie zur Terrorismusbekämpfung veröffentlicht. Ziel sollte es sein, gemeinsame europäische Standards zu entwickeln, wie bestimmte mit Terrorismus in Verbindung stehende Handlungen sanktioniert werden sollen. So wurde etwa definiert, unter welchen Voraussetzungen eine Reise als Vorbereitung einer terroristischen Straftat gelten sollte. Zudem wollte der Ausschuss auch die vom Rat vorgeschlagenen Überwachungsmaßnahmen einführen.

Wiederum haben wir unser kostenloses Telefontool für eine Telefonaktion genutzt, um die Bürger und Bürgerinnen in den Protest einzubeziehen. Auf vielfältige Weise haben wir über unsere Kritik informiert: in einem Beitrag auf unserem Netzpolitischen Abend, in einer Stellungnahme auf unserer Internetseite und über unsere Social-Media-Accounts.

Verhindert die EU-Überwachungsfantasien (07.06.2016): https://digitalegesellschaft.de/2016/06/verhindert-ueberwachungsfantasien/

1.3 Öffentliche Begleitung und Stellungnahme zur Ausweitung der Videoüberwachung

Medienberichten zufolge wollte Bundesinnenminister Thomas de Maizière die Videoüberwachung an privatrechtlich betriebenen öffentlichen Orten wie Einkaufszentren, Sportstätten und Parkplätzen sowie in Bussen und Bahnen deutlich ausweiten. Dabei sollten künftig auch vermehrt Techniken zur automatischen Gesichtserkennung zum Einsatz kommen. Dies sollte, so de Maizière, mit Verweis auf die Taten von Ansbach und München im Sommer 2016, der Vorbeugung von Terroranschlägen dienen.

Umsetzen wollte der Innenminister seine Pläne durch eine Änderung des Bundesdatenschutzgesetzes. Dort sollte festgeschrieben werden, dass die „Sicherheit der Bevölkerung" bei Entscheidungen über den Einsatz von Überwachungstechnik „besonders zu berücksichtigen" ist. Über die Verwendung von Überwachungsinstrumenten in den öffentlich zugänglichen Bereichen privat betriebener Einrichtungen haben die Landesdatenschutzbehörden zu entscheiden. Diese standen bislang insbesondere der Videoüberwachung aus guten Gründen skeptisch bis ablehnend gegenüber. Mit seinem Vorstoß wollte de Maizère also offenkundig diese behördliche Entscheidungspraxis ins Gegenteil verkehren.

Im November wollte die Bundesregierung das Gesetz auf den Weg bringen. Zum Referentenentwurf haben wir eine schriftliche Stellungnahme verfasst. Darin lehnten wir das Vorhaben als unverhältnismäßigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung ab. Denn obwohl es keine Belege dafür gibt, dass durch Videoüberwachung Straftaten effektiv verhindert werden, zielt der

Entwurf darauf ab, möglichst viele öffentlich zugängliche Orte rund um die Uhr per Kamera zu beobachten.

Wiederum haben wir durch Veröffentlichungen auf unserem Blog, auf den Social-Media-Kanälen und im Radio auf FluxFM zur Verbreitung unserer Einschätzungen beigetragen.

Ausweitung der Videoüberwachung: Nicht mehr Sicherheit, sondern weniger Grundrechte (27.10.2016): https://digitalegesellschaft.de/2016/10/videoueberwachung-weniger-grundrechte/

Stellungnahme des Digitale Gesellschaft e.V. zum Referentenentwurf des Bundesministeriums des Innern eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes (Videoüberwachungsverbesserungsgesetz) (10.11.2016): https://digitalegesellschaft.de/wp-content/uploads/2016/11/Stellungnahme_DigiGes_Video%C3%BCberwachungsverbesserungsG.pdf

1.4 Vorratsdatenspeicherung: Wegweisendes Urteil und Brief an die EU-Kommission

Der EuGH stellte bereits 2014 in seinem Urteil zur europäischen Richtlinie zur Vorratsdatenspeicherung (VDS) klar, dass eine anlasslose Bevorratung von Kommunikationsdaten gegen europäische Grundrechte verstößt. Nun musste sich der EuGH mit den nationalen Gesetzen zur VDS in Großbritannien und Schweden befassen. In erfreulicher Klarheit führte das Gericht aus, dass auch mitgliedstaatliche Regelungen, die eine Speicherung von Kommunikationsdaten vorschreiben, den Vorgaben der EU-Grundrechte genügen müssen. Des Weiteren stellte der Luxemburger Richter deutlich heraus, dass anlass- und verdachtsunabhängige Speicherverpflichtungen stets gegen den Verhältnismäßigkeitsgrundsatz verstoßen, weil sie niemals auf das absolut notwendige Maß begrenzt sind. Eine Bevorratung von Kommunikationsdaten kann danach nur zulässig sein, wenn sie zeitlich und örtlich beschränkt ist und auf Personen abzielt, bei denen konkrete Hinweise für die Verwicklung in schwere Straftaten vorliegen. Damit verbietet das Gericht klar die auch hierzulande immer wieder fälschlich als Allheilmittel propagierte Behandlung der gesamten Bevölkerung als Verdächtige. Daher musste Deutschland das erst Ende 2015 verabschiedete Gesetz zur Wiedereinführung der Vorratsdatenspeicherung nun unverzüglich aufheben und von weiteren Anläufen für anlasslose Datensammlungen endgültig Abstand nehmen.

Anlässlich des Urteils haben wir die EU-Kommission in einem Brief um die Prüfung gebeten, ob ein Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland eingeleitet werden muss. Diese Prüfung war von hoher Relevanz, denn im Zuge eines Vertragsverletzungsverfahrens werden die Mitgliedstaaten gezwungen, Verstöße gegen das EU-Recht abzustellen.

Wiederum haben wir auf vielen Wegen dazu beigetragen, die Öffentlichkeit über die Gefahren für die Grund- und Menschenrechte durch die Vorratsdatenspeicherung zu informieren.

Sieg der Grundrechte: Europäischer Gerichtshof verbannt Vorratsdatenspeicherung auf den Müllhaufen der Geschichte (21.12.2016): https://digitalegesellschaft.de/2016/12/eugh-vds-muellhaufen/

Brief an EU-Kommission: Deutschland muss Gesetz zur Vorratsdatenspeicherung aufheben (22.12.2016): https://digitalegesellschaft.de/2016/12/brief-kommission-vds/

1.5 Videokampagne gegen die Vorratsdatenspeicherung von Reisedaten: PNR

Fünf Jahre nachdem die EU-Kommission ihren Vorschlag zur Einführung einer Vorratsdatenspeicherung von Reisedaten („Passenger Name Record", kurz: PNR) vorgelegt hat, stand die finale Abstimmung im EU-Parlament bevor. Bis zu 60 Einzeldaten, etwa Kreditkarteninformation, Essenswünsche und Angaben über den gesundheitlichen Zustand von Reisenden, sollten fünf Jahre lang auf Vorrat gespeichert werden. Die Datensammlung werde für den Kampf gegen Terrorismus und schwere Kriminalität benötigt, hieß es. Beweise für den Nutzen der Datensammelwut gab es nicht.

Dennoch stand die Einführung dieser mit massiven Grundrechtsverletzungen einhergehende Dauerüberwachung kurz bevor. Die im Ministerrat vertretenen Mitgliedstaaten der EU und das EU-Parlament hatten sich bereits Ende 2015 auf einen Kompromiss für die Einführung der Vorratsdatenspeicherung von Reisedaten verständigt. Allein die finale Abstimmung im Plenum des EU-Parlaments, die Ende April 2016 stattfand, stand noch aus.

Wir haben eine Videokampagne ins Leben gerufen, in der Menschen ihre Meinung zur Vorratsdatenspeicherung von Reisedaten preisgeben konnten. In den Videos drücken #noPNR Unterstützer ihre Kritik an der Überwachung von Passenger Name Records aus. Beispielsweise erläutern sie ihren Zweifel daran, dass PNR eine effektive Lösung zur Bekämpfung des Terrorismus ist und ihr Unbehagen damit, dass sich alle Reisenden wie Verbrecher behandeln lassen müssen. Diese Videos haben wir an die EU Parlamentarier geschickt und sie somit aufgefordert, gegen die Einführung der Massenüberwachung des europäischen Flugreiseverkehrs zu stimmen.

Video-Kampagne NoPNR: https://www.youtube.com/playlist?list=PLMoiP4YfunXJnmsmLaPm66QTCs57Mo8ix

Richtlinie zur Fluggastdatenspeicherung: EU-Parlament winkt Massenüberwachung des Reiseverkehrs durch (14.04.2016): https://digitalegesellschaft.de/2016/04/eupnr-fin-vote/

1.6 Safe Harbour & Privacy Shield: Offener Brief für rechtskonformen Datenverkehr in die USA

Auf Basis der EU-Datenschutzrichtlinie von 1995 war es Unternehmen in Europa nicht gestattet, personenbezogene Daten in Drittländer zu transferieren, wenn dort ein Datenschutzniveau vorliegt, welches nicht mit europäischen Standards vergleichbar ist. Da das Datenschutzniveau in den USA generell niedriger anzusiedeln ist, erließ die EU-Kommission im Jahr 2000 die sogenannte „Safe Harbor" Entscheidung, um den ungehinderten transatlantischen Datenaustausch weiter gewährleisten zu können. „Safe Harbor" sieht eine Selbstverpflichtung der datenverarbeitenden Unternehmen gegenüber der US-Handelskommission vor, bestimmte Datenschutzprinzipien einzuhalten. Ob und inwieweit die Unternehmen ihre Versprechen tatsächlich einhalten, wurde von der EU-Kommission allerdings gar nicht und von der zuständigen Handelskommission lediglich unzureichend kontrolliert. Hinzu kam, dass die Selbstverpflichtung der Unternehmen sich gerade nicht auf Datenübermittlungen in den Bereichen der nationalen Sicherheit und der Strafverfolgung erstreckt. Nicht zuletzt aus diesem Grund kritisierten Datenschutzbehörden, zivilgesellschaftliche Organisationen und das EU-Parlament die „Safe Harbor" Entscheidung bereits seit Jahren.

Vor dem Hintergrund des faktisch unbegrenzten Zugriffs des US-amerikanischen Geheimdienst NSA auf die von den großen US-amerikanischen Internetunternehmen gespeicherten Daten wollte der österreichische Datenschutzaktivist Max Schrems von der zuständigen irischen Datenschutzbehörde prüfen lassen, ob die Überführung von persönlichen Daten in die USA durch Facebook nach geltendem Recht zulässig war. Da sich die irische Datenschutzbehörde mit Verweis auf „Safe Harbor" geweigert hatte, die Prüfung durchzuführen, verwies der Irish High Court den Fall letztlich an den Europäischen Gerichtshof. Dieser entschied am 6. Oktober 2015, dass die Safe-Harbor-Entscheidung der EU mit den

USA, auf der der Datenexport basierte, ungültig war, da sie gegen europäische Grundrechte verstieß. Die „Safe Harbor" Entscheidung der EU-Kommission war damit ungültig.

Der Safe-Harbor-Nachfolger „Privacy Shield" sollte die neue rechtliche Grundlage für den Datenverkehr zwischen Europa und den USA werden. Anfang Februar 2016 wurde zunächst ein vorläufiges Verhandlungsergebnis zwischen der EU-Kommission und den USA präsentiert, aus dem nur wenige Details ersichtlich wurden. Später veröffentliche die EU-Kommission schließlich die Dokumente. Die Befürchtungen bestätigten sich, dass es sich bei dem Wechsel von „Safe Harbor" zu „Privacy Shield" lediglich um kosmetische Änderungen handelte, welche die Kernprobleme der alten Regelung nicht lösen konnten.

Gemeinsam mit fast zwei Dutzend weiteren Organisationen haben wir uns in einem offenen Brief an die verschiedenen EU-Institutionen gewandt und weitreichende Nachbesserungen des Privacy Shield gefordert. In dem Schreiben legen wir dezidiert dar, dass das Privacy Shield weder den Vorgaben der Safe-Harbor-Entscheidung des EuGH (Europäischer Gerichtshof) noch den Bedingungen genügt, welche der Zusammenschluss der europäischen Datenschutzbehörden (Artikel-29-Gruppe) für eine rechtskonforme Vereinbarung aufgestellt hatte.

Privacy Shield: Zivilgesellschaftliche Koalition fordert erhebliche Nachbesserungen (16.03.2016): https://digitalegesellschaft.de/2016/03/privacy-shield-offener-brief/

1.7 Verschlüsselung: Weltweiter offener Brief für den Erhalt verschlüsselter Kommunikation

Regierungen, Strafverfolgungsbehörden und Geheimdienste in aller Welt wünschen sich uneingeschränkten Zugriff auf verschlüsselte Daten. Nur wenn staatliche Stellen in der Lage seien, kryptographische Sicherungen zu umgehen, seien sie auch in der Lage, Kriminalität und Terrorismus wirksam zu bekämpfen, so das gebetsmühlenartig wiederholte Credo; die Privatsphäre der Nutzerinnen und Nutzer, die Vertraulichkeit ihrer Kommunikation und die Integrität informationstechnischer Systeme müssten im Zweifel hinter der nationalen Sicherheit zurückstehen.

Dementsprechend versuchten Regierungen in der EU, den USA und vielen anderen Staaten auf der Welt, Online-Unternehmen zur Offenlegung verschlüsselt gespeicherter Daten zu verpflichten oder kryptographische Verfahren durch den Einbau von Hintertüren zu schwächen. Damit würden sie jedoch genau denjenigen in die Hände spielen, um deren Bekämpfung es vorgeblich geht: Kriminelle und Terroristen könnten Schwachstellen in Verschlüsselungsverfahren ebenso für ihre Zwecke ausnutzen, wie dies für staatliche Stellen möglich wäre.

Gemeinsam mit anderen Organisationen, Unternehmen und Einzelpersonen haben wir uns in einem offenen Brief an die Regierungen in aller Welt gewandt und sie dazu aufgefordert, den bisher eingeschlagenen Kurs in Sachen Verschlüsselung zugunsten echter IT-Sicherheit aufzugeben.

Offener Brief an Regierungen: Verschlüsselung stärken statt schwächen (12.01.2016): https://digitalegesellschaft.de/2016/01/offener-brief-verschluesselung/

2. Datenschutz: Schutz von informationeller Selbstbestimmung und Verbrauchern im Internet

2.1 Analyse zum Kommissionsvorschlag zur Reform der E-Privacy-Richtlinie

Seit 2002 schützte die sogenannte ePrivacy-Richtlinie die Grundrechte und die Privatsphäre von EU-Einwohnern bei der elektronischen Kommunikation. Zuletzt wurde sie 2009 durch die Cookies-Richtlinie geändert. Seitdem haben sich die Kommunikationsmittel und -kanäle erheblich und nachhaltig gewandelt. Messenger-Dienste, Video-Telefonie, Kurznachrichtendienste oder Photosharing-Apps treten

zunehmend an die Stelle des klassischen Telefonanrufs, der E-Mail oder der SMS. Im Internet der Dinge kommunizieren außerdem auch immer mehr Maschinen untereinander. Dementsprechend schlug die EU-Kommission eine Reform der ePrivacy-Richtlinie vor. Diese soll das Recht an die veränderten Bedingungen anpassen und fit für die digitale Gegenwart machen. Wir haben den Kommissionsvorschlag umfassend analysiert.

Analyse: Entwurf der ePrivacy-Verordnung stärkt Rechte von Endnutzerinnen und Endnutzern (15.12.2016): https://digitalegesellschaft.de/2016/12/analyse-entwurf-eprivacy-verordnung/

2.2 EU-Datenschutzreform: Stellungnahme zur Anpassung des Bundesdatenschutzgesetzes

Seit dem 25. Mai 2016 sind die europäische Datenschutzgrundverordnung (DSGVO) sowie die Datenschutz-Richtlinie (DSRL) in Kraft. Die Regelungen sollten das bislang geltende Datenschutzrecht der EU, das noch aus den 90er Jahren stammt, ablösen und fit für das digitale Zeitalter machen. Während eine Richtlinie noch der Umsetzung in nationales Recht bedarf, hat eine Verordnung in den Mitgliedstaaten grundsätzlich unmittelbare Geltung. Die Datenschutzgrundverordnung enthielt allerdings zahlreiche Öffnungsklauseln, die es den einzelnen Mitgliedstaaten erlauben, von den EU-Vorgaben abzuweichen und nationale Sonderwege einzuschlagen.

Von dieser Möglichkeit wollte Deutschland reichlich Gebrauch machen. Das Bundesinnenministerium hatte Ende November einen Referentenentwurf für die Anpassung des deutschen Datenschutzrechts an die neuen EU-Regeln vorgelegt und dazu verschiedene Interessenvertreter und Verbände angehört. Im Zentrum des Vorhabens stand die Neufassung des Bundesdatenschutzgesetzes. Neben Vorschriften zur Umsetzung der Datenschutz-Richtlinie sollten auch eine Reihe von Bestimmungen auf Grundlage der Öffnungsklauseln der Datenschutzgrundverordnung in das Gesetz aufgenommen werden.

Zum Referentenentwurf haben wir eine Stellungnahme erarbeitet. Unsere Kritik richtete sich vorrangig gegen die vorgesehene Regelung der Videoüberwachung, die Bestimmungen zur Zweckbindung sowie die Vorschriften zu den Betroffenenrechten. Wir haben thematisiert, dass der Entwurf gerade bei der Zweckbindung und den Betroffenenrechten sowohl hinter das Niveau der Verordnung (EU) 2016/679 (Datenschutzgrundverordnung) als auch das Niveau des bislang geltenden deutschen Datenschutzrechts zurückfiel. Auch unsere Kritik an einem weiteren Entwurf haben wir öffentlich gemacht.

Stellungnahme des Digitale Gesellschaft e.V. zum Referentenentwurf des Bundesministeriums des Innern eines Gesetzes zur Anpassung des Datenchutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (E) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) (07.12.2016):
https://digitalegesellschaft.de/wp-content/uploads/2016/12/Stellungnahme_Digitale_Gesellschaft_DSAnpUG-EU-1.pdf

2.3 Öffentliche Begleitung der CETA-Verhandlungen

CETA ist die Kurzform für das Comprehensive Economic and Trade Agreement, welches seit 2009 zwischen der kanadischen Regierung und der Europäischen Union (vertreten durch die EU-Kommission) ausgehandelt wurde. Offizielles Ziel der Verhandlungen war die Reduzierung von Zöllen und der Abbau von sogenannten „nicht-tarifären Handelshemmnissen". Faktisch bedeutet dies vor allem, dass Normen und Vorschriften entweder angeglichen oder gegenseitig anerkannt werden sollten.

CETA würde eine höchst undemokratische und intransparente Gerichtsbarkeit für Unternehmen schaffen und zugleich ein völlig veraltetes Urheberrecht zementiert und für potentielle Einfallstore sorgen, die den europäischen Datenschutz in Frage stellen könnten. Auf diversen Wegen haben wir unsere Kritik öffentlich gemacht.

CETA: Ein gewichtiger Präzedenzfall: https://digitalegesellschaft.de/mitmachen/ceta/

3. Netzneutralität: Aktivitäten für eine verbraucherfreundliche Umsetzung der EU-Regeln zur Netzneutralität

Das Prinzip der Netzneutralität besteht darin, dass sämtliche Daten unabhängig von Absender, Empfänger oder Inhalt stets nach der Reihenfolge ihres Eintreffens in gleicher Qualität und gleicher Geschwindigkeit von den Providern weitergeleitet werden. Es gibt danach also keine Daten, Dienste oder Nutzer erster und zweiter Klasse, keine wichtigen und weniger wichtigen Inhalte. In der Vergangenheit gab es immer wieder prominente Fälle, bei denen dieses Prinzip unterlaufen wurde.

Im Juni 2015 wurden die Dreiecksverhandlungen zwischen der EU-Kommission, dem Rat der Europäischen Union und dem Europäischem Parlament über eine Verordnung für einen einheitlichen digitalen Binnenmarkt mit einem Kompromiss abgeschlossen. Dabei konnte sich die netzneutralitätsfreundliche Position des Europäischen Parlaments in den Verhandlungen kaum gegen die stark an den Wünschen der Telekommunikationslobby orientierten Positionen von Ministerrat und Kommission durchsetzen. Ende Oktober 2015 wurde der Kompromiss im Rahmen der „Telecom Single Market" Verordnung im Plenum des EP verabschiedet und damit die Netzneutralität begraben. Obwohl sie bereits seit April 2016 dieses Jahres in Kraft ist, war bislang unklar, wie sie in der Praxis umgesetzt werden sollte. Das Gremium der europäischen Telekom-Regulierer (BEREC) sollte diese Unwägbarkeiten beseitigen, indem es Leitlinien zur Auslegung und Anwendung der Verordnung aufstellt.

Den Leitlinien-Entwurf haben wir fundamental kritisiert. Wir haben dazu aufgerufen, an der BEREC-Konsultation teilzunehmen und Verbesserungsvorschläge zu den Leitlinien vorzuschlagen. Am 9. August 2016 fand außerdem die Übergabe der Stimmen für Netzneutralität in Bonn statt. Durch die „Save the Internet" Kampagne, welche eine gemeinsame Kampagne von 23 europäischen Nichtregierungsorganisationen ist, war es uns möglich 100.000 Stimmen einzusammeln, um die Freiheiten des Internets zu schützen. In einem gemeinsamen offenen Brief haben wir uns zusammen mit 71 anderen zivilgesellschaftliche Organisationen aus 31 Ländern an die europäischen Telekom-Regulierer gewandt. Darin forderten wir eine starke Absicherung der Netzneutralität bei der Umsetzung der EU Telekommunikationsmarkt-Verordnung.

Auch an der Expertenanhörung zur Änderung des Telekommunikationsgesetzes (TKG) – also dem Gesetz, das die neue Netzneutralitätsverordnung ans deutsche Telekommunikationsrecht anpasst – im Ausschuss für Wirtschaft und Energie des Deutschen Bundestages nahmen wir teil und trugen unsere Kritik vor.

Rettet das Internet: BEREC-Leitlinien lassen Schlupflöcher zur Aushöhlung der Netzneutralität (15.06.2016): https://digitalegesellschaft.de/2016/06/rettet-das-internet-berec-leitlinien-lassen-schlupfloecher-zur-aushoehlung-der-netzneutralitaet/

Stellungnahme des Digitale Gesellschaft e.V. zu einem Dritten Gesetz zur Änderung des Telekommunikationsgesetzes (Anhörung im Ausschuss für Wirtschaft und Energie des Deutschen Bundestages (07.11.2016): https://digitalegesellschaft.de/wp-content/uploads/2016/11/Stellungnahme_Digitale_Gesellschaft_BT-Drs_18-9951.pdf

4. Mehr offene Internetzugänge und Rechtssicherheit für Verbraucher: Kampagne zur Abschaffung der WLAN Störerhaftung

Das Problem der WLAN-Störerhaftung begleitet uns bereits seit mehreren Jahren. Störerhaftung bedeutet hier, dass der Betreiber eines öffentlich zugänglichen WLANs für die Rechtsverletzungen, insbesondere Urheberrechtsverletzungen verantwortlich ist, die von Dritten über sein Funknetz begangen werden. Dieses Risiko scheuen viele potentielle Anbieter offener WLANs, da sie kostenpflichtige Abmahnungen fürchten. Im Gegensatz dazu verfügen die klassischen Access-Provider (z.B. Deutsche Telekom) über ein sogenanntes Providerprivileg, wodurch diese von dem Haftungsrisiko ausgenommen sind.

Wir setzen uns seit langem für die Abschaffung der WLAN-Störerhaftung ein. Die Störerhaftung ist nicht nur der Grund für das Fehlen offener WLAN-Netze in Deutschland, sondern auch für zahlreiche Abmahnungen gegen unwissende Verbraucher. Schon 2012 haben wir einen ersten Formulierungsvorschlag für ein entsprechendes Gesetz vorgelegt.

Aus diesem Grund begrüßten wir auch grundsätzlich, dass die Große Koalition die Abschaffung der WLAN-Störerhaftung plane und WLAN-Betreiber Access-Providern grundsätzlich gleich stellen will. Bei genauerem Hinsehen entpuppten sich die Pläne jedoch als unzureichend: Das Problem der Abmahnungen adressierte der Minimalkonsens der Großen Koalition gerade nicht. Wir haben auf das Problem aufmerksam gemacht und den politischen Prozess um die Abschaffung der Störerhaftung aktiv begleitet. Wir haben dazu aufgerufen, eine Petition zur Abschaffung der WLAN-Störerhaftung ohne Hintertüren für die Abmahnindustrie zu unterzeichnen. Leider blieb die Große Koalition trotzdem auf halber Strecke stehen. Die Störerhaftung wurde auch 2016 noch nicht abgeschafft.

Abschaffung der WLAN-Störerhaftung: Koalition darf nicht auf halber Strecke Halt machen (12.05.2016) https://digitalegesellschaft.de/2016/05/wlan-koalition-halbe-strecke/

WLAN-Störerhaftung: Petition fordert Abschaffung ohne Hintertüren für Abmahnindustrie (30.05.2016): https://digitalegesellschaft.de/2016/05/wlan-stoererhaftung-petition/

5. Erfolg für Kunstfreiheit und Verbraucher: Bundesverfassungsgericht schafft Recht auf Sampling

Vor dem Bundesverfassungsgericht (BverfG) fand Ende November 2015 eine Verhandlung zum Musik-Sampling statt. Konkret ging es dabei um die ungefragte Verwendung einer kurzen Rhythmussequenz aus einem Kraftwerk-Stück in einem Lied von Sabrina Setlur. Gegen diese Verwendung hatte Kraftwerk geklagt. Die Entscheidung des BVerfG könnte Grundsatzwirkung haben: Sollte das Gericht der Linie von Kraftwerk folgen, wäre Sampling – zumindest so wie es heute praktiziert wird – quasi unmöglich. Die zentrale Fragestellung bei dem Verfahren war, ob und unter welchen Voraussetzungen es erlaubt ist, kleinste Tonausschnitte aus einer fremden Tonaufnahme zu entnehmen und sie in eigene Aufnahmen einzubauen. In der rechtlichen Auseinandersetzung ging es dabei nicht um das Urheberrecht, sondern um das vom Inhalt der Aufnahme unabhängige Recht des Tonträgerherstellers und die Reichweite des Rechts auf freie Benutzung. Das Bundesverfassungsgericht hat letztlich sein Urteil in einem seit nunmehr 18 Jahren andauernden Rechtsstreit verkündet. Die Übernahme einzelner Teile aus einer fremden Tonaufnahme in ein eigenes Werk unter bestimmten Voraussetzungen ist nun ohne Erlaubnis des Rechteinhabers möglich.

Im Juli 2015 waren wir beim Bundesverfassungsgericht als sachkundige Dritte eingeladen und hatten bereits im Vorfeld der Verhandlung eine schriftliche Stellungnahme abgegeben. Darin haben wir die bisherige Rechtsprechung des Bundesgerichtshofes als Hindernis für die soziokulturelle Fortentwicklung kritisiert.

Metall auf Metall: Bundesverfassungsgericht schafft Recht auf Sampling (31.05.2016): https://digitalegesellschaft.de/2016/05/bverfg-recht-auf-sampling/

6. Verbändegespräch zu Preisen im digitalen Zeitalter

Die Preise im digitalen Zeitalter sind oft individualisiert und ihre Erstellung ist vollkommen intransparent und für die Verbraucherinnen und Verbraucher nicht nachvollziehbar. Doch nur wer weiß, dass und nach welchen Kriterien Preise flexibel gestaltet werden, kann sich darauf einrichten. Wer seine Privatsphäre schützen will muss oft mit erheblichen Mehrkosten rechnen. Auch die Gewährleistung der Datensicherheit dieser erhobenen Daten ist fraglich.

Während eines Verbändegesprächs mit dem Thema „Durchblick unerwünscht?" haben wir uns für stärkere Rechte für Verbraucherinnen und Verbraucher bei der Preisdifferenzierung ausgesprochen. Hier setzten wir uns mit individualisierten und dynamischen Preisen und deren Risiko für die Verbraucher auseinander.

Veranstaltung zu Preisen im digitalen Zeitalter (November Newsletter der Digitalen Gesellschaft (02.12.2016): https://digitalegesellschaft.de/2016/12/newsletter-november-2/#5

7. Medienkompetenz für Kinder und Jugendliche: Informationsbroschüre Digitale Defender

Die Broschüre „Digital Defenders vs. Data Intruders" soll Kinder und Jugendliche dabei unterstützen, sichere und gut informierte Entscheidungen darüber zu treffen, was sie online teilen. Sie enthält Kapitel darüber, was Privatsphäre eigentlich ist, wie man sichere Messenger nutzen kann und wie man die Datensicherheit auf Smartphones verbessern kann.

Broschüre Digitale Defender (Dezember 2016): https://digitalegesellschaft.de/wp-content/uploads/2016/12/defenders_v_intruders_de_web.pdf

8. Öffentliche Begleitung der Einigung zwischen Youtube und GEMA

Die bei Nutzerinnen und Nutzern der Videoplattform YouTube wenig geschätzten „GEMA-Sperrtafeln" dürften der Vergangenheit angehören. Es wurde verkündet, dass YouTube und die deutsche Verwertungsgesellschaft GEMA, sich auf eine Vergütung für Musikvideos geeinigt haben. Mit der außergerichtlichen Einigung legten die beiden Akteure einen jahrelangen Streit über die Frage bei, ob und in welcher Höhe YouTube für Musikuploads seiner User Entgelte an die GEMA zu entrichten hat. Über die Details der Vereinbarung bewahrten beide Seiten Stillschweigen. Die Einigung im Streit zwischen YouTube und GEMA setzte zwar den ärgerlichen Sperrtafeln ein Ende, warf jedoch zugleich zahlreiche neue Fragen auf.

Mit unseren Veröffentlichungen haben wir zur öffentlichen Auseinandersetzung mit dem Thema beigetragen, dass Fragen der Voraussetzungen für Kulturproduktion auf digitalen Plattformen ebenso berührt wie Rechtssicherheit für Verbraucher..

YouTube vs GEMA: Ein Ende kann ein Anfang sein (02.11.2016): https://digitalegesellschaft.de/2016/11/youtube-vs-gema/

10. Gefahr für die Demokratie? Aufklärung zu Social Bots

So genannte „Social Bots“ kommen immer häufiger zum Einsatz. Sie können Wettervorhersagen kommunizieren oder Produktempfehlungen verbreiten. Aber auch im politischen Alltag werden sie zunehmend eingesetzt. Im US-Wahlkampf etwa setzten sie Millionen Tweets für oder gegen die Präsidentschaftskandidaten ab. In Deutschland betreiben immer mehr Bots rechte Hetze im Netz. So beeinflussen sie die öffentliche Meinung und damit die demokratische Mitbestimmung. Wir haben das Zukunftsthema in unserem Podcast erklärt.

Social Bots: Wenn Maschinen Meinung machen - DigiGes @ FluxFM (24.11.2016): https://youtu.be/l2XPlpPk1fY?list=PLMoiP4YfunXJcELmvFy9cdxx2d6mN0s3Q

11. Kampagne zur EU-Geschäftsgeheimnis-Richtlinie

Während der ursprüngliche Zweck dieser Richtlinie die Verhinderung von Industriespionage war, ging die jetzige Fassung jedoch weit darüber hinaus: Sie gab Unternehmen das Recht, jeden zu verklagen, der auf ihre internen Informationen zugreift, sie verwendet oder – wie etwa im Fall der Panama Papers – veröffentlicht (Whistleblowing). Unternehmen versuchen, unabhängige Überprüfungen ihrer Produkte (z.B. Medikamente, Pestizide, Kfz-Emissionen) mit dem Hinweis, es handele sich dabei um Geschäftsgeheimnisse, zu verhindern. Durch die Richtlinie würde ihnen zusätzliche rechtliche Instrumente in die Hand gegeben, um missliebige Personen zu verklagen und Missstände zu vertuschen. Insbesondere Whistleblower haben sich in den vergangenen Jahren als zentrale Kontrollinstanz und Unterstützung für die Rechtsstaatlichkeit und den Grundrechteschutz etabliert. Die EU-Geschäftsgeheimnis-Richtlinie droht, Whistleblower zu gefährden.

Um der Richtlinie entgegen zu wirken, haben wir ein kostenloses Anruftool zur Verfügung gestellt. Damit konnten Bürger*innen mit den Abgeordneten in Kontakt treten und ihre Kritik vorbringen. Die wichtigsten Argumente haben wir auf unserem Blog veröffentlicht.

Geschäftsgeheimnis-Richtlinie: Kostenlose Telefonaktion gegen die Gefährdung von Pressefreiheit und Whistleblowern (13.04.2016): https://digitalegesellschaft.de/2016/04/geschaeftsgeheimnis-rl-telefonaktion/

12. Aufklärung zu Fake News und Hate Speech

Die Sorge um den Einfluss von gefälschten Nachrichten, irreführenden Zitaten und hetzerischen Kommentaren auf die politische Meinungs- und Willensbildung erschient zunächst durchaus nachvollziehbar. Teile der Bevölkerung in Deutschland hatten offenbar das Vertrauen in etablierte Medien und Politik verloren und sich stattdessen einer geschlossenen medialen Parallelwelt, bestehend aus sozialen Medien, Blogs und sogenannten „alternativen“ Nachrichtenportalen, zugewandt. Entscheidend ist dort weniger, ob eine Meldung tatsächlich der Wahrheit entspricht; vielmehr soll sie Ressentiments befördern, bestehende Feindbilder bedienen und den politischen Gegner diffamieren.

In den Phänomenen Fake News und Hate Speech kommen die Themen Grundrechte und Öffentlichkeit mit der Medienkompetenzbildung zusammen. Wir haben über Fake News und Hate Speech informiert und auf andere Möglichkeiten der Problemlösung verwiesen.

Fake News und Hate Speech: Was hilft gegen Propagandalügen? (21.12.2016): https://digitalegesellschaft.de/2016/12/was-hilft-gegen-propagandaluegen/

13. Für mehr freies Wissen: Wahlprüfsteinaktion Mecklenburg-Vorpommern

Wir haben uns mit dem Bündnis Freie Bildung, Freifunk, die Free Software Foundation Europe, die Open Knowledge Foundation und Wikimedia Deutschland zur Koalition Freies Wissen zusammengeschlossen, um anlässlich der Landtagswahl in Mecklenburg-Vorpommern am 04. September 2016 die Parteien zu Themen aus den Bereichen Freie Software, Offene Daten, Freies Wissen, Digitale Bildung und Grundrechten im und Zugang zum Digitalen Raum zu befragen.

Wahlprüfsteinaktion Mecklenburg-Vorpommern 2016 (23.08.2016): https://digitalegesellschaft.de/2016/08/wahlpruefsteinaktion-mv-2016/

14. Netzpolitische Abende der Digitalen Gesellschaft

Jeden ersten Dienstag im Monat konnten wir auf unseren Netzpolitischen Abenden auf der c-base in Berlin über Mündigkeit und Kompetenz in der Nutzung digitaler Technologien, den Erhalt demokratischer Mitbestimmung und Grundrechte in der digitalen Transformation und der Reflektion dieser Entwicklungen in Wissenschaft und Bildung informieren. Zugleich bieten die Netzpolitischen Abende Gleichgesinnten und Initiativen die Möglichkeit, sich zu vernetzen. Der Livestream ermöglicht es auch denen, die nicht in Berlin sind, die Veranstaltungen zu verfolgen. Die Videos werden danach jeweils auf unserer Internetseite ins Netz gestellt und bleiben so der Öffentlichkeit erhalten.

Netzpolitischer Abend auf der Webseite der Digitalen Gesellschaft:
https://digitalegesellschaft.de/portfolio-items/netzpolitischer-abend/

15. Wöchentlicher Radiobeitrag und Podcast: „In digitaler Gesellschaft“ auf FluxFM

Seit Januar 2016 berichten wir in der Reihe „In digitaler Gesellschaft“ beim Berliner Radiosender FluxFM über das netzpolitische Thema der Woche. In kurzen Gesprächen erläutern wir aktuelle Entwicklungen im Feld der Netzpolitik. Das Themenspektrum reicht von tagespolitischen Ereignissen auf lokaler sowie globaler Ebene bis hin zu längerfristigen Projekten, welche wir als DigiGes kritisch begleiten. Als gemeinnütziger Verein, der sich für Grundrechte und Verbraucherschutz im digitalen Raum einsetzt, möchten wir nicht zuletzt auch die Fragen aufwerfen, warum die angesprochenen Themen uns alle betreffen und welchen Beitrag jeder einzelne zum Erhalt und zur Fortentwicklung einer freien und offenen digitalen Gesellschaft leisten kann.

„In digitaler Gesellschaft“ auf der Website der Digitalen Gesellschaft:
https://digitalegesellschaft.de/portfolio-items/in-digitaler-gesellschaft-bei-flux-fm/

Unterstütze uns!

Liebe Freundinnen und Freunde des Digitale Gesellschaft e.V.,

Engagement kostet viel Zeit und auch Geld. Auch in diesem Jahr haben wir für eine moderne Netzpolitik und Bürgerrechte gekämpft. Wir haben uns für die gesetzliche Verankerung der Netzneutralität eingesetzt, wir haben gegen die ausufernde Massenüberwachung mobil gemacht, für ein modernes Urheberrecht gestritten und vieles mehr.

Für unsere Arbeit sind wir auf Spenden angewiesen. Nur so können wir die vielen Kampagnen stemmen, unsere Meinung professionell in die Parlamente tragen und für unsere Ziele kämpfen. In Zukunft wird unsere Aufgabe nicht leichter: eine große Koalition braucht eine starke außerparlamentarische Opposition. Damit wir auch in den kommenden Jahren die digitalen Bürgerrechte verteidigen können, brauchen wir eure Unterstützung.

Um uns zu helfen, könnt ihr zum Beispiel Fördermitglied werden. Fördermitglieder leisten einen wesentlichen Beitrag, dass wir noch besser gegen Industrielobby-Interessen und für mehr Bürgerrechte eintreten können. Übrigens: Ab einem Spendenbetrag von 10 Euro pro Monat gibt es einen schicken Digiges-Jutebeutel und ein Digiges-T-Shirt in einer gewünschten Größe als Willkommensgeschenk. Hier könnt ihr Fördermitglied werden: https://digitalegesellschaft.de/foerdermitglied/

Wir freuen uns aber auch über klassische Spenden. Dafür gibt im Moment zwei Möglichkeiten: Einerseits per Banküberweisung, und sehr viel einfacher über unser Spendenformular: https://digitalegesellschaft.de/spenden/

Unsere Kontodaten sind:

Digitale Gesellschaft e.V.

Konto-Nr: 1125012800

BLZ: 430 609 67

IBAN: DE88430609671125012800

BIC: GENODEM1GLS (44789 Bochum)

Alle wichtigen Infos, etwa wie ihr Spenden steuerlich absetzen könnt, findet ihr hier.

https://digitalegesellschaft.de/unterstuetzen/spenden-faq/

Wir freuen uns auf eure Unterstützung.

Eure Digiges

==========

V.i.S.d.P.: Alexander Sander, Digitale Gesellschaft e.V., Singerstraße. 109, 10179 Berlin