Tätigkeitsbericht 2017

Wir reden nicht nur, wir handeln. Nicht zuletzt Dank eurer Unterstützung haben wir 2017 gemeinsam viel geschafft. Wir haben uns vor und hinter den Kulissen erfolgreich für Grund- und Verbraucherrechte in der digitalen Welt eingesetzt. Unter anderem haben wir Erfolge bei der WLAN-Störerhaftung und der ePrivacy-Reform feiern können. Leider findet die Stimme der Nutzer*innen, Verbraucher*innen und Zivilgesellschaft in der Netzpolitik immer noch zu wenig Gehör. 2017 war deshalb auch das Jahr des Netzwerkdurchsetzungsgesetzes, der Umsetzung der Vorratsdatenspeicherung von Fluggastdaten und der Einführung von Zero-Rating-Angeboten in Deutschland.

Wir lassen uns davon jedoch nicht entmutigen, sondern machen weiter. Wir erklären in Presse, Radio und Fernsehen, vor Politiker*innen, vor Gerichten aber auch vor Schüler*innen, warum Verbraucher- und Grundrechte in der digitalen Gesellschaft wichtig sind und wie wir sie bewahren können. Aus diesem Grund freut es uns sehr, dass wir 2017 ein Projekt zur Aufklärung über die neuen Datenschutzregeln beim Bundesministerium der Justiz und für Verbraucherschutz einwerben konnten.

Es gibt mehr als genug zu tun und wir brauchen auch im neuen Jahr eure Unterstützung, damit wir noch mehr für eine nutzerfreundliche und demokratische Netzpolitik tun können. Deshalb vorneweg, wie auch zum Schluss die Aufforderung:

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

https://digitalegesellschaft.de/foerdermitglied/

https://digitalegesellschaft.de/unterstuetzen/

oder über betterplace:

https://www.betterplace.org/de/projects/19435-spende-fur-menschenrechts-und-verbraucherfreundliche-netzpolitik

1. Begleitung der neuen Datenschutzregeln aus Sicht der Grund- und Verbraucherrechte

1.1 Umsetzung der Datenschutzgrundverordnung in Deutschland

2017 wurde die Anpassung des Bundesdatenschutzgesetzes an die neue EU-Datenschutzgrundverordnung (DSGVO) beschlossen. Nach der Verabschiedung der DSGVO müssen die Mitgliedstaaten ihre nationalen Gesetze an die neuen EU-Bestimmungen anpassen. Da die DSGVO auch eine große Anzahl von Öffnungsklauseln enthält, können die Mitgliedstaaten in einigen Punkten von den EU-Vorschriften abweichen. Deutschland hat diese Möglichkeiten im Gesetzentwurf zur Anpassung des nationalen Datenschutzsystems umfassend genutzt. Bereits im Jahr 2016 hatten wir uns mit einer umfangreichen Stellungnahme in den Prozess eingebracht. Im Zentrum unseres Interesses stand der Versuch, die deutschen nationalen Gesetze so verbraucherfreundlich wie möglich zu gestalten.

Obwohl einige Kritikpunkte, die wir und andere Daten- und Verbraucherschützer vorgebracht hatten, am Ende berücksichtigt wurden, bleibt die deutsche Umsetzung der Datenschutzgrundverordnung ein gefährlicher Sonderweg für die Rechte der Verbraucher und die freiheitlich-demokratische Gesellschaft. Das Datenschutzanpassungsgesetz beschneidet nicht nur die Betroffenenrechte, sondern schafft zugleich die Voraussetzungen für die Ausweitung der Videoüberwachung öffentlich zugänglicher Orte und Verkehrsmittel. Unsere Kritikpunkte haben wir mehrfach öffentlich vorgebracht, u.a. in unserer wöchentlichen Radioshow beim Berliner Sender FluxFM.

Datenschutz: Deutscher Sonderweg mit Videoüberwachung - DigiGes @ FluxFM (04.05.2017): https://www.youtube.com/watch?v=sWzjUTKDlaQ

Datenschutz: Bundesrat stimmt über deutschen Sonderweg ab (12.05.2017): https://digitalegesellschaft.de/2017/05/datenschutz-bundesrat/

1.2 Informationsportal zur Datenschutzgrundverordnung: Deine Daten. Deine Rechte.

Doch wir bleiben dran an der DSGVO. Seit Herbst 2017 bereiten wir eine umfassende Aufklärungskampagne unter dem Titel „Deine Daten. Deine Rechte." zur Datenschutzgrundverordnung vor. Wir wollen die deutsche und europäische Öffentlichkeit über die Bedeutung des Datenschutzes aufklären, die Gründe für dessen Notwendigkeit verständlich machen und den Bürger*innen und Verbraucher*innen zeigen, welche Rechte sie als Betroffene haben und wie sie diese durchsetzen können.

Im Jahr 2017 haben wir hierfür wichtige Vorarbeiten geleistet, u. a. haben wir Recherchen und Hintergrundgespräche durchgeführt und das Konzept für die Informationsplattform „Deine Daten. Deine Rechte." entworfen. Diese soll Verbraucher*innen in die oftmals trockene Materie des Datenschutzrechts mit kurzen Erklärtexten, Videos und mittels eines Spiels einführen.

„Deine Daten. Deine Rechte." wird mit dem Anwendungsbeginn der Datenschutzgrundverordnung im Mai 2018 an den Start gehen. Das Projekt wird vom Bundesministerium der Justiz und für Verbraucherschutz (BMJV) vom 1. Juli 2017 bis 30. September 2018 finanziert.

1.3 Kampagne zur Abstimmung des Europäischen Parlaments über die ePrivacy-Verordnung

Um Datenschutz und Privatsphäre unserer Kommunikation geht es auch bei der ePrivacy-Verordnung, die die EU-Kommission Anfang 2017 vorgestellt hat und die seit dem den europäischen Gesetzgebungsprozess durchläuft. Ziel der Reform ist es, Online-Kommunikationsdienste in den Anwendungsbereich des Gesetzes einzubeziehen, was bisher nicht der Fall ist.

Im Oktober 2017 hat das Europäische Parlament in seiner Abstimmung zur ePrivacy-Reform zugunsten der Verbraucher- und Grundrechte entschieden. Das EU-Parlament stärkt den Schutz vor Tracking, fordert verpflichtende datenschutzfreundliche Voreinstellungen bei Browsern und Endgeräten und votiert für ein Recht auf Verschlüsselung.

Diesen Erfolg haben wir mit unseren Unterstützer*innen und unseren europäischen Partnerorganisationen gemeinsam erkämpft. Wir haben dazu aufgerufen, die Mitglieder des EU-Parlaments zu kontaktieren und sie auf die Bedeutung einer starken ePrivacy-Reform aufmerksam zu machen. Wir haben dieses wichtige, jedoch medial wenig präsente, Thema zudem im Radio und auf unserem monatlichen netzpolitischen Abend erklärt.

Aufgrund unserer Expertise in diesem Themenbereich wurden wir bereits früher im Jahr vom Wirtschaftsministerium zu einem Hintergrundgespräch sowie zu einem schriftlichen Kommentar über die deutsche Position zur geplanten ePrivacy-Verordnung im Rat der Europäischen Union („Ministerrat") eingeladen.

Wir haben zudem auf akademischen und politischen Konferenzen, wie dem Langenburger Forum für Nachhaltigkeit, über die Bedeutung des Datenschutzes und der Privatsphäre gesprochen.

Stellungnahme des Digitale Gesellschaft e.V. zum Vorschlag der EU-Kommission für eine ePrivacy-Verordnung (21. März 2017):
https://digitalegesellschaft.de/wp-content/uploads/2017/03/Stellungnahme_DigiGes_ePVO.pdf

Kostenloser Anruf bei MEPs: Fordert euer Recht auf Privatsphäre ein! (04.10.2017):
https://digitalegesellschaft.de/2017/10/epriv-meps-call/

ePrivacy: Europäisches Parlament stimmt gegen Ausverkauf des Datenschutzes (26.10.2017):
https://digitalegesellschaft.de/2017/10/eprivacy-ep-abstimmung/

2. Einsatz für Meinungsfreiheit und Rechtsstaatlichkeit: Unsere Arbeit gegen das Netzwerkdurchsetzungsgesetz

Ein Hauptschauplatz unserer Arbeit im Jahr 2017 war das Netzwerkdurchsetzungsgesetz (NetzDG), das die Bundesregierung gegen den Rat zahlreicher Interessengruppen und Experten aus Zivilgesellschaft und Wirtschaft zum Ende der letzten Legislaturperiode verabschiedet hat. Gegen das Netzwerkdurchsetzungsgesetz (NetzDG), das Social Media-Unternehmen bestraft, wenn sie illegale Inhalte nicht schnell genug löschen, haben wir uns frühzeitig eingesetzt und das Gesetz bis zur Verabschiedung substantiell kritisiert.

Seit etwa zwei Jahren kündigt Justizminister Heiko Maas an, dass er Social-Media-Unternehmen für bestimmte illegale Inhalte verantwortlich machen will, die als Hassrede oder gefälschte Nachricht eingestuft werden. Nachdem seine Versuche, die Anzahl der bei der Benachrichtigung mit Hilfe einer Task Force gelöschten Inhalte zu erhöhen, gescheitert waren, legte der Justizminister einen Gesetzentwurf vor. Dieser droht Social-Media-Unternehmen mit Bußgeldern von bis zu 50 Millionen Euro, wenn sie „offensichtlich illegale" Beiträge nicht innerhalb von 24 Stunden und andere „illegale" Beiträge nicht innerhalb einer Woche nach Benachrichtigung löschen.

Das Gesetz hat viele Mängel, von den Kernideen bis hin zu technischen Fragen wie unklaren Definitionen. Das Kernproblem des Gesetzes aber ist, dass es die Last der Einstufung von Inhalten als illegal auf die Schultern von Social-Media-Unternehmen legt und ihnen mit einer Geldstrafe droht, wenn sie zu wenig löschen. Das muss zu einer strengen und proaktiven Löschpolitik in sozialen Netzwerken führen. Im Zweifel über die Rechtmäßigkeit eines Postings wird das soziale Netzwerk die Löschung wählen müssen, um eine Geldstrafe zu vermeiden. Der Gesetzentwurf stellt daher eine Bedrohung für

die Meinungsfreiheit dar. Das Gesetz führt zudem zu einer Privatisierung der Rechtsdurchsetzung. Im Rechtsstaat ist es eine Kernfunktion der Justiz, zu entscheiden, ob eine Äußerung rechtswidrig ist oder nicht.

Anlässlich einer Expertenanhörung des Justizministeriums konnten wir einen schriftlichen Kommentar zum NetzDG abgeben. Wir haben es geschafft, in den Medien eine öffentliche Debatte über das geplante Gesetz anzuregen. Wir haben uns auch an die Europäische Kommission gewandt und argumentiert, dass das Gesetz gegen die in der E-Commerce-Richtlinie festgelegten Haftungsregeln sowie das dort ebenfalls geregelte Herkunftslandprinzip verstößt.

Schließlich haben wir eine große Allianz aus Wirtschaftsverbänden, netzpolitischen Organisationen, Gegenredeninitiativen, zivilgesellschaftlichen Organisationen und renommierten Rechtsexperten initiiert. In einer gemeinsamen „Deklaration für die Meinungsfreiheit" kritisiert das Bündnis, dass das NetzDG den Grundfreiheiten und der öffentlichen Diskurskultur schadet und fordert gleichzeitig einen umfassenderen Lösungsansatz. Dieser muss mit einer gründlichen wissenschaftlichen Analyse der Phänomene Hassrede und gefälschte Nachrichten beginnen.

Wir haben auf allen unseren Kommunikationskanälen (Blog, Radiosendung auf FluxFM, wöchentliche Kolumne in der Berliner Zeitung und mehrere Konferenzen) immer wieder über das NetzDG gesprochen, um die öffentliche Aufmerksamkeit für das Thema zu erhalten. Wir haben auch eine E-Mail-Kampagne organisiert, mit der wir Menschen dazu ermutigt haben, ihre Kritik am NetzDG gegenüber den Abgeordneten des Bundestages zu kommunizieren.

Zur Verabschiedung des Gesetzes kommentierten wir: „Wir bedauern, dass die Große Koalition sich dazu entschlossen hat, das hoch umstrittene Netzwerkdurchsetzungsgesetz durch den Bundestag zu bringen. Die Art und Weise, wie dieses Vorhaben allen Bedenken zum Trotz durchgesetzt wurde, hat dem Ansehen des Rechtsstaates eher geschadet als genützt. Das Ergebnis ist ein mit heißer Nadel gestricktes Regelwerk, das schwerwiegende handwerkliche Mängel aufweist und außerdem gegen das Europarecht verstößt."

Aufgrund unserer öffentliche Positionierung zum NetzDG und weiteren unter dem Eindruck der US-Wahlen intensiv diskutierten Themen rund um den politischen Einfluss von Social Media, wurden wir zu einer Expertenanhörung über die möglichen Gefahren von Social Bots im Ausschuss Digitale Agenda des Bundestages eingeladen.

Stellungnahme des Digitale Gesellschaft e.V. zu den Referentenentwürfen für ein Netzwerkdurchsetzungsgesetz (30. März 2017):
https://digitalegesellschaft.de/wp-content/uploads/2017/03/Stellungnahme_DigiGes_NetzDG.pdf

Stellungnahme des Digitale Gesellschaft e.V. zur TRIS-Notifizierung des Entwurfs für ein Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) (07.04.2017):
https://digitalegesellschaft.de/wp-content/uploads/2017/04/Stellungnahme_TRIS_NetzDG_DigiGes.pdf

Deklaration für die Meinungsfreiheit (18.05.2017): https://deklaration-fuer-meinungsfreiheit.de/

3. Erfolg für Verbraucher*innen: Abschaffung der WLAN-Störerhaftung

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*innen: Sie werden für vermeintliche Urheberrechtsverstöße, die Dritte über ihre Netze begehen, abgemahnt. Das Risiko, eine Abmahnung zu erhalten, hat dazu geführt, dass private und gewerbliche WLAN-Betreiber in Deutschland ihre

Netzwerke kaum öffnen. Schon 2012 haben wir deshalb einen ersten Formulierungsvorschlag für ein entsprechendes Gesetz vorgelegt.

Im Sommer 2017 konnte sich die Große Koalition in letzter Minute nun doch noch auf die Abschaffung der WLAN-Störerhaftung einigen. Dem voraus ging die auf halber Strecke stehen gebliebene gesetzliche Abschaffung der Störerhaftung der Bundesregierung im Jahr 2016. Nach der Verabschiedung des Gesetzes forderten wir immer wieder Änderungen, da wir das Gesetz im Hinblick auf das Ziel, Rechtssicherheit für WLAN-Eigentümer zu schaffen, für unzureichend hielten. Die Entscheidung des Europäischen Gerichtshofs (EuGH) im Fall McFadden vs. Sony Music hat nur wenige Monate später unsere Einschätzung bestätigt. Wir haben die Entscheidung genutzt, um öffentlichen Druck auf die Bundesregierung und insbesondere auf das Wirtschaftsministerium auszuüben, um Änderungen am kurz zuvor verabschiedeten Gesetz vorzunehmen.

Als das Ministerium im Frühjahr 2017 einen neuen Gesetzentwurf zur Abschaffung der Störerhaftung vorlegte, haben wir diesen neuen Entwurf kommentiert und mehrere Änderungen gefordert. Das Ministerium hat viele der von uns vorgeschlagenen Änderungen aufgenommen, bevor das Kabinett und schließlich das Parlament zustimmte. Das im Sommer 2017 verabschiedete Gesetz zur Abschaffung der WLAN-Störerhaftung bringt spürbare Verbesserungen für die Anbieter offener WLAN-Zugänge und Verbraucher*innen. Kostenpflichtige Abmahnungen wegen Rechtsverletzungen Dritter sind nun effektiv ausgeschlossen. Rechtsunsicherheiten bleiben jedoch insbesondere im Hinblick auf den neu eingeführten Sperranspruch der Rechteinhaber gegenüber WLAN-Betreibern bestehen.

Bis zur Abschaffung der Störerhaftung war es ein weiter Weg, aber wir haben einen langen Atem für Verbraucherrechte und besseren Zugang zum Netz bewiesen. Allein im Jahr 2017 haben wir mehrere Stellungnahmen verfasst, Hintergrundgespräche geführt, sprachen in einer Anhörung zum Thema im Bundestag und haben das Thema wie immer auch öffentlich eingeordnet.

Neuer Vorstoß zu offenen Netzen: Ministerium muss nachbessern (10.03.2017): https://digitalegesellschaft.de/2017/03/offene-netze-nachbessern/

Stellungnahme des Digitale Gesellschaft e.V. zum Referentenentwurf des Bundesministeriums für Wirtschaft und Energie für ein Drittes Gesetz zur Änderung des Telemediengesetzes (neues WLAN-Gesetz – 3. TMGÄndG) (09.03.2017): https://digitalegesellschaft.de/wp-content/uploads/2017/03/Stellungnahme_DigiGes_Drittes_TMG%C3%84ndG.pdf

Stellungnahme des Digitale Gesellschaft e.V. zum Gesetzentwurf der Bundesregierung eines Dritten Gesetzes zur Änderung des Telemediengesetzes (BT-Drs. 18/12202) sowie zur Stellungnahme des Bundesrates und zur Gegenäußerung der Bundesregierung (BT-Drs. 18/12496) (22.06.2017): https://digitalegesellschaft.de/wp-content/uploads/2017/06/Stellungnahme_DigiGes_Drittes_TMG%C3%84ndG.pdf

Anhörung im Ausschuss für Wirtschaft und Energie zum Zugang zu öffentlichen WLAN-Angeboten (26.06.2017): https://www.youtube.com/watch?v=4U4W3aywj78

Offene Netze: Rechtssicherheit mit Schönheitsfehlern (30.06.2017): https://digitalegesellschaft.de/2017/06/wlan-schoenheitsfehler/

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

Kritik der Umsetzung der Vorratsdatenspeicherung von Fluggastdaten in Deutschland

Im Jahr 2017 haben wir gegen die Umsetzung der EU-Richtlinie zur Speicherung von Passagiergastdaten (PNR) in deutsches Recht gekämpft.

Bei jeder Flugbuchung speichern die Fluggesellschaften bis zu 60 individuelle Informationen pro Passagier und Flug in sogenannten PNR-Systemen. Die EU-Kommission präsentierte 2011 einen ersten Entwurf für eine PNR-Richtlinie. Die Richtlinie zwingt die Mitgliedstaaten, nationale Gesetze zu erlassen, die es den Fluggesellschaften verbindlich vorschreiben, PNR-Daten zu speichern und den Sicherheitsbehörden Zugang zu den Daten zu gewähren. Diese Behörden können die Daten dann mit Fahndungslisten abgleichen und sie mithilfe mustererkennender Verfahren durchsuchen, um vermeintliche Sicherheitsrisiken, also Verdächtige, zu erkennen. Das Projekt wurde mehrfach verschoben und verändert, bis das Europäische Parlament im Februar 2016 doch die Richtlinie verabschiedete. Nach der Verabschiedung der Richtlinie haben die Mitgliedstaaten mit der Umsetzung in nationales Recht begonnen – so auch Deutschland.

Durch unsere kontinuierliche Arbeit konnten wir uns als Experten zum Thema Fluggastdatenspeicherung positionieren und in den politischen Prozess zur Umsetzung der PNR-Richtlinie in Deutschland einbringen. Unter anderem haben wir als Sachverständige an der Anhörung zur Fluggastdatenspeicherung im Innenausschuss des Deutschen Bundestages teilgenommen und eine kritische Stellungnahme verfasst. Wir betrachten die Vorratsdatenspeicherung von Reisedaten als grundrechtswidrig. Ihr Nutzen für die Sicherheit ist zudem nicht belegt. Die Umsetzung der PNR-Richtlinie in Deutschland sollte daher unterbleiben. Leider folgte der Deutsche Bundestag unserer Empfehlung nicht und verabschiedete das grundrechtswidrige Fluggastdatengesetz.

Später im Jahr hat der EuGH unsere Auffassung in seinem Gutachten zum geplanten Fluggastdatenabkommen mit Kanada bestätigt. Das Gericht stellte klar, dass verdachtsunabhängige Vorratsdatenspeicherungen gegen die Grundrechte auf Privatsphäre und den Schutz personenbezogener Daten verstoßen. Wir haben das EuGH-Gutachten erklärt und klargestellt, dass hieraus die Aufhebung der EU-Richtlinie zur Fluggastdatenspeicherung und ihrer deutschen Umsetzung folgen muss.

Stellungnahme des Digitale Gesellschaft e.V. zum Entwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz – FlugDaG) (20.04.2017): https://digitalegesellschaft.de/wp-content/uploads/2017/04/FlugDaG-Stellungnahme.pdf

Bundestag stimmt für Vorratsdatenspeicherung von Reisedaten (26.04.2017): https://digitalegesellschaft.de/2017/04/bundestag-fuer-pnr/

Verstoß gegen Grundrechte: Gerichtshof kippt geplantes Fluggastdatenabkommen mit Kanada (26.07.2017): https://digitalegesellschaft.de/2017/07/eugh-pnr-kanada/

Einordnung der Nicht-Umsetzung der Vorratsdatenspeicherung von Telekommunikationsdaten

Gegen die Grundrechte auf Privatsphäre, Datenschutz und informationelle Selbstbestimmung verstößt auch die Vorratsdatenspeicherung von Telekommunikationsdaten.

Die Regierungskoalition hat das Gesetz zur Speicherung der Telekommunikationsdaten im Jahr 2015 in Rekordzeit durch das Parlament getrieben. Nach dem Gesetz müssen Telekommunikations-unternehmen Verkehrsdaten, also Informationen darüber wer wann mit wem kommuniziert hat, für zehn Wochen speichern. Standortdaten der elektronischen Kommunikation müssen vier Wochen

gespeichert werden. Das Kernproblem des Gesetzes ist, dass es eine grundrechtswidrige, da massenhafte und anlasslose Datenspeicherung vorschreibt, die noch nicht einmal auf ein bestimmtes geografisches Gebiet, eine bestimmte Region, eine bestimmte Zeitspanne, eine bestimmte Gruppe von Personen oder bestimmte Personen begrenzt ist.

Das Gesetz zur Vorratsdatenspeicherung war im Dezember 2015 verabschiedet worden und trat im Juli 2017 offiziell in Kraft. Allerdings wurde es nicht umgesetzt. Im Juni 2017, also kurz vor Umsetzungsbeginn, erklärte das Oberverwaltungsgericht (OVG) Nordrhein-Westfalen die deutsche Regelung zur Vorratsdatenspeicherung für unvereinbar mit einen Urteil des EuGH, in dem einer anlasslosen Vorratsdatenspeicherung eine klare Absage erteilt wurde. Der klagende Provider Spacenet musste die Vorratsdatenspeicherung daraufhin nicht umsetzen. Andere Provider konnten sich auf das Urteil berufen. Ende Juni 2017 schloss sich die Bundesnetzagentur dem Urteil an. Sie entschied, dass sie das Gesetz aufgrund schwerwiegender rechtlicher Bedenken nicht umsetzen wird. Konkret heißt das, dass die Bundesnetzagentur die Vorratsdatenspeicherung nicht gegenüber den Telekommunikations-unternehmen anordnet oder Sanktionen verhängt.

Wir haben diese erfreulichen rechtlichen Entwicklungen für die Öffentlichkeit eingeordnet und die politischen Konsequenzen daraus verdeutlicht: Die Vorratsdatenspeicherung von Telekommunikationsdaten ist damit Geschichte. Die Bundesregierung muss das Gesetz aufheben.

Vorratsdaten: OVG-Beschluss markiert Anfang vom Ende der Speicherpflicht (22.06.2017): https://digitalegesellschaft.de/2017/06/vds-ovg/

Ende auf Raten: Bundesnetzagentur setzt Vorratsdatenspeicherung aus (28.06.2017): https://digitalegesellschaft.de/2017/06/ende-vds-bnetza/

EU-Anti-Terror-Richtlinie und deutsche Anti-Terror-Gesetzgebung

Nach den Terroranschlägen von Paris 2015 hat die EU-Kommission einen Vorschlag für eine Anti-Terror-Richtlinie vorgelegt. Der Vorschlag enthält eine Vielzahl von grundrechtlich fragwürdigen Maßnahmen, die die Mitgliedstaaten ergreifen sollen. Dazu zählte auch die Blockierung „terroristischer" Inhalte im Internet, die Durchsuchung von Privatcomputern, die verdeckte elektronische Überwachung sowie Video- und Audioaufnahmen von Personen in privaten und öffentlichen Fahrzeugen. Im Februar 2017 hat das Europäische Parlament die Anti-Terror-Richtlinie durchgewunken.

Das deutsche Anti-Terror-Gesetz wurde im Juni 2017 im Eilverfahren verabschiedet. Es ermöglicht dem Bundesamt für Verfassungsschutz, sich an gemeinsamen Datenbanken mit ausländischen Nachrichtendiensten zu beteiligen, ohne dass konkrete Vorkehrungen für den Schutz personenbezogener Daten getroffen werden. Das Gesetz verbietet es zudem, Prepaid-Karten für Mobiltelefone an Personen zu verkaufen, die sich nicht mit einem gültigen Personalausweis identifizieren können.

Wir haben in beiden Gesetzgebungsprozessen wiederholt auf die Verletzung von Grund- und Menschenrechten unter der Maßgabe des Kampfes gegen den Terrorismus hingewiesen. Besonders im deutschen Fall haben wir zudem auch das Verfahren selbst kritisiert: Die Verabschiedung des Anti-Terror-Gesetzes nur zwei Wochen nach der ersten Lesung im Bundestag wird der Tragweite der dort beschlossenen Grundrechtseingriffe nicht gerecht. Der öffentliche Diskurs, Rechtsstaatlichkeit und nicht zuletzt die Einbeziehung der Zivilgesellschaft blieben bei der Verabschiedung des Anti-Terror-Gesetzes auf der Strecke.

Anti-Terror-Richtlinie: EU-Parlament stimmt für Netzsperren und gefährdet zivilgesellschaftlichen Protest (16.02.2017): https://digitalegesellschaft.de/2017/02/anti-terror-rl-ep/

Anti-Terror-Gesetz: Rechtsstaatliches Fiasko und demokratischer Offenbarungseid (24.06.2017): https://digitalegesellschaft.de/2016/06/anti-terror-fiasko/

5. Öffentlicher Einsatz für ein modernes Urheberrecht: Für ein Recht auf Remix und gegen Geoblocking

Für eine Liberalisierung und Modernisierung des Urheberrechts im Sinne der Verbraucher*innen braucht es ein Recht auf Remix. Zudem sollten Inhalte überall in Europa verfügbar sein: Mindestens muss deshalb Schluss sein mit dem sogenannten Geoblocking innerhalb der EU, noch besser wäre eine umfassende Harmonisierung des europäischen Urheberrechts in zeitgemäßer Art und Weise.

Weder das europäische noch das deutsche Urheberrecht erlauben derzeit kreative Adaptionen bestehender Werke. Die transformative Nutzung eines Werkes ist strengstens untersagt, es sei denn, der ursprüngliche Autor stimmt dieser Nutzung ausdrücklich zu. Diese Rechtslage ist kaum mit einer digitalen Realität vereinbar, die jedem die Werkzeuge an die Hand gibt, neue kreative Werke aus bestehenden Werken zu erstellen und sie weltweit zu teilen. Auf allen unseren Kommunikationskanälen haben wir deshalb auch im Jahr 2017 weiter für ein Recht auf Remix geworben. Aufhänger hierfür war die von uns bereits im Vorjahr intensiv begleitete Rechtssache „Metall auf Metall".

Weiterhin haben wir die EU-Vorschläge zur Abschaffung des Geoblockings eingeordnet. Geboblocking meint das Sperren von Online-Inhalten aus lizenzrechtlichen Gründen entlang nationaler Grenzen. Die neue EU-Verordnung schafft Geoblocking leider nur für Bezahldienste und unter engen Voraussetzungen ab. Während man also seinen Account bei einem kommerziellen Streaminganbieter zukünftig auch auf Reisen innerhalb der EU ohne Einschränkungen nutzen können wird, unterliegen Gratisdienste und die Mediatheken öffentlich-rechtlicher Programme weiter dem Geoblocking. Die Verordnung steht damit gegen Verbraucherinteressen und konterkariert die Idee einer europäischen digitalen Öffentlichkeit.

Begrenzt grenzenlos: Geoblocking in der EU (23.02.2017): https://digitalegesellschaft.de/2017/02/begrenzt-grenzenlos-geoblocking-eu/

Begrenzt grenzenlos: EU-Parlament stimmt für Lockerung bei Geoblocking (18.05.2017): https://digitalegesellschaft.de/2017/05/ep-geoblocking/

Metall auf Metall: Remix-Kultur vor dem EuGH (08.06.2017): https://www.youtube.com/watch?v=zocIGtLHNEs

6. Öffentlichkeitsarbeit und Stakeholder-Beteiligung für mehr IT-Sicherheit

Smart und sicher im Netz (SuSi)

Grundbedingung für Datenschutz, Privatsphäre sowie Verbraucherschutz ist die Sicherheit unserer vernetzten Infrastruktur, Geräte und Anwendungen. In dem Projekt „Digitale Gesellschaft: smart & sicher" (SuSi) geht es darum, eine interdisziplinäre wissenschaftliche Herangehensweise zu entwickeln, um die Herausforderungen im Bereich der Informationssicherheit exakt benennen zu können. In mehreren Schritten sollen relevante Stakeholder identifiziert und zentrale Fragestellungen in Bezug auf die sichere und smarte Informationsgesellschaft formuliert werden. Ein besonderes Augenmerk liegt auf der Einbeziehung der Zivilgesellschaft.

Im Jahr 2017 haben wir gemeinsam mit unseren Projektpartnern mehrere Denkwerkstätten mit Expert*innen auf dem Gebiet der IT-Sicherheit durchgeführt sowie ein Impulspapier und eine Studie erarbeitet. Die Ergebnisse der Erhebungen und die gemeinsam herausgearbeiteten Impulse wurden am 7. September 2017 der Öffentlichkeit vorgestellt.

Die Digitale Gesellschaft führt das Projekt „Smart und sicher im Netz" gemeinsam mit dem Berliner Institut nexus im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) durch.

Digitale Gesellschaft: smart & sicher (SuSi):
https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/Digitale_Gesellschaft/SuSI/susi_node.html

Sicherheitslücken verhindern

Um ein akzeptables Maß an IT-Sicherheit für Bürger*innen und Verbraucher*innen aufrechtzuerhalten, wollen wir die Einführung von Hintertüren und anderen gezielten Schwächungen von Verschlüsselung verhindern. Darüber hinaus sollte es den staatlichen Behörden nicht gestattet sein, Zero-Day-Exploits, also das Wissen über Softwarefehler, die das Eindringen in IT-Geräte und digitale Kommunikation erlauben, auf Schwarz- oder Graumärkten zu kaufen. Stattdessen sollte der Staat verpflichtet werden, jede Schwachstelle, die ihm bekannt wird, zu veröffentlichen. Die staatlichen Behörden sollten auch Techniken der digitalen Selbstverteidigung fördern, wie beispielsweise den Einsatz von AdBlockern gegen Malvertising oder den Einsatz von Verschlüsselung, wo immer dies möglich ist. Außerdem fordern wir eine besondere Haftung von IT-Herstellern für Sicherheitslücken in ihren Produkten.

Seit einigen Jahren wirbt jedoch vor allem das Innenministerium für die Idee der gezielt eingebauten Lücken in kryptographischen Produkten. Dies soll ihnen helfen, die verschlüsselte Kommunikation von Terroristen und anderen Kriminellen zu untersuchen. Das Ministerium lehnt es auch ab, bekannte Sicherheitslücken zu veröffentlichen, anstatt sie für staatliche Behörden wie Nachrichtendienste und Polizei zu nutzen. Während das Innenministerium immer wieder behauptet, dass sie eine sichere IT für alle wollen, sieht die Praxis ganz anders aus. So schreibt das Ministerium den elektronischen Personalausweis (der eine Reihe von Sicherheitsrisiken mit sich bringf) verbindlich vor und wirbt für Hintertüren in IoT („Internet of Things")-Produkten und vernetzten Autos.

Obwohl derzeit noch keine konkreten Gesetzesvorschläge in Vorbereitung sind, hielten wir es für wichtig, dem verschlüsselungskritischen Diskurs der Bundesregierung entgegenzuwirken, die Öffentlichkeit frühzeitig über dieses wichtige Thema zu informieren und uns im Hinblick auf anstehende politische Vorhaben auf diesem Gebiet zu positionieren.

Gestörter Hausfrieden, Netzwelt-Kolumne, Berliner Zeitung (16.08.2017)

WannaCry: Das gefährliche Geschäft mit Sicherheitslücken (18.05.2017): https://www.youtube.com/watch?v=03Vdk8nch1w&index=34

Backdoor-Debatte: Tausendmal geführt ... (07.12.2017): https://www.youtube.com/watch?v=36cgod84ynI

7. Medienkompetenzvermittlung: Jugendprojekte „Dein Netz – Digitale Mündigkeit für Berlin" und „Sicher & bewusst im Netz"

Wir wollen insbesondere junge Menschen darüber aufklären, wie sie das Netz sicher, respektvoll und selbstbestimmt nutzen können. Sie sollen verstehen, wie Internet und Smartphone funktionieren, warum Datenschutz wichtig ist und welche Möglichkeiten sie haben, Programme so einzustellen, dass Informationen über sie besser geschützt sind. Deshalb sind wir auch im Jahr 2017 an Schulen und

Jugendzentren gegangen, um jungen Menschen und Pädagogen das nötige Grundwissen für das Leben in der digitalen Gesellschaft zu vermitteln.

In Zusammenarbeit mit der Medienanstalt Berlin-Brandenburg („Dein Netz – Digitale Mündigkeit für Berlin“) und dem Bezirksamt der Stadt Berlin und dem Quartiersmanagment Pankstraße („Sicher und bewusst im Netz“) organisierten wir Veranstaltungen in Berliner Schulen und Jugendzentren für Schüler im Alter von 10 bis 18 Jahren. In diesen Veranstaltungen erläutern wir die Geschäftsmodelle von Social-Media-Plattformen und anderen Online-Diensten, weisen auf deren rechtliche, technische und psychologische Fallstricke hin und geben Tipps für eine sicherere und bessere Nutzung.

Nachdem das Projekt „Sicher und bewusst im Netz“ seit drei Jahren erfolgreich läuft, haben wir in 2017 unseren Vertrag mit der Stadt Berlin um weitere zwei Jahre verlängert. Mit der Medienanstalt Berlin-Brandenburg ist es uns zudem gelungen, einen Förderer für ein weiteres Jugendprojekt namens „Dein Netz – Digitale Mündigkeit für Berlin“ zu gewinnen. Im Gegensatz zu „Sicher und bewusst im Netz“, das auf den Berliner Stadtteil Wedding beschränkt ist, umfasst das Projekt mit der Medienanstalt Berlin-Brandenburg die gesamte Stadt Berlin.

Projekt-Webseite „Dein Netz“: https://dein-netz.org/

8. Für echte Netzneutralität: Kampagne gegen das Zero-Rating-Angebot „StreamOn“

Bereits bei der Verabschiedung der EU-Verordnung zur Netzneutralität haben wir vor den Schlupflöchern in den neuen Regeln gewarnt – insbesondere durch sogenanntes Zero Rating. Zero Rating bedeutet, dass der Datenverkehr bestimmter Internetdienste nicht auf das Datenvolumen des Telekommunikationsvertrages (meist handelt es sich um Mobilfunkverträge) angerechnet wird, was diese Dienste aufgrund knapper und teurer Datenvolumina für die Kund*innen besonders attraktiv macht. Durch Zero Rating werden jene Dienste bevorteilt, die in der Lage sind, mit den Telekommunikationsunternehmen entsprechende Vereinbarungen einzugehen und Dienste entsprechend der Vorgaben der Telekommunikationsanbieter bereitzustellen. Das bevorteilt große Online-Dienste, schränkt die Wahlfreiheit der Verbraucher*innen sowie die Vielfalt und Kommunikationsfreiheit im Netz ein. Beim Zero Rating handelt es sich um einen klaren Verstoß gegen die Netzneutralität: Die Inhalte der Zero-Rating-Partner werden gegenüber anderen Inhalten im Internet diskriminiert.

Die Leitlinien des Gremiums der europäischen Telekom-Regulierer (BEREC) und die Anpassungen des deutschen Rechts an die Netzneutralitätsregeln der EU haben das Schlupfloch Zero Rating nicht geschlossen. Das haben wir bereits im Jahr 2016 kritisiert. Umso vorhersehbarer war es, dass die Deutsche Telekom mit StreamOn in 2017 ein Zero Rating Angebot in Deutschland gestartet hat.

Mit StreamOn verspricht die Deutsche Telekom ihren Kund*innen unbegrenztes und obendrein kostenloses Video- und Audio-Streaming. Wer bereits einen der höherwertigen „Magenta“-Tarife der Telekom gebucht hat, kann ohne zusätzliche Kosten die StreamOn-Option hinzubuchen. Solange das monatliche Datenvolumen des Magenta-Tarifs noch nicht aufgebraucht ist, wird der durch Audio- und Videostreams verursachte Traffic dann nicht auf das monatliche Datenvolumen angerechnet. Die theoretische Möglichkeit für Anbieter, kostenlos an StreamOn teilzunehmen, ändert nichts daran, dass es sich bei StreamOn um eine nach der Netzneutralitätsverordnung verbotene Beschränkung der Wahlfreiheit der Kund*innen handelt. Denn praktisch kann oder will nicht jeder Inhalteanbieter an StreamOn teilnehmen.

Wir haben den Vorstoß der Telekom detailliert analysiert und erklärt, warum dieser nicht vereinbar mit den EU-Netzneutralitätsregeln ist. Darüber hinaus haben wir auf kreative Art und Weise auf die intransparenten und ungleichen Teilnahmebedingungen bei StreamOn für Anbieter hingewiesen: Wir

haben eine Video-Website mit einem Video zu StreamOn erstellt und versucht, selbst Streaming-Partner der Telekom zu werden. Was wir dabei erlebt haben, haben wir öffentlich diskutiert und damit auf den Irrweg Zero-Rating aufmerksam gemacht. Im Sinne der Netzneutralität, des Verbraucherschutzes und der Kommunikationsfreiheit fordern wir ein Verbot von StreamOn durch die Bundesnetzagentur.

Netzneutralität kaputt?, Netzwelt-Kolumne, Berliner Zeitung (13. Oktober 2017)

Tricks der Netzanbieter, Netzwelt-Kolumne, Berliner Zeitung (6. Dezember 2017)

SchemeOn: Wie die Telekom die Netzneutralität verletzt (20.04.2017): https://www.youtube.com/watch?v=1QUEFIFme3w

StreamOn: Zero-Rating auf dem Prüfstand (01.06.2017): https://www.youtube.com/watch?v=HrHtkbOd5o8

Entscheidung zu StreamOn: Netzneutralität kaputt (12.10.2017): https://www.youtube.com/watch?v=INUbMmHx4o4

9. Netzpolitik in Massenmedien: Radioshow und Podcast „In digitaler Gesellschaft" auf FluxFM und Kolumne in der Berliner Zeitung

Seit Januar 2016 berichten wir in der Reihe „In digitaler Gesellschaft" beim Berliner Radiosender FluxFM über das netzpolitische Thema der Woche. Bis einschließlich Dezember 2017 haben wir 100 Folgen für das Format produziert. 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 Digitale Gesellschaft 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 jede*r zum Erhalt und zur Fortentwicklung einer freien und offenen digitalen Gesellschaft leisten kann.

Nicht zuletzt konnten wir der wöchentlichen Netzwelt-Kolumne in dem Printmedium „Berliner Zeitung" unsere Themen platzieren.

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

10. Wissensaustausch und Vernetzung: Monatlicher Netzpolitischer Abend

Jeden ersten Dienstag im Monat konnten wir mit unserem Netzpolitischen Abend auf der c-base in Berlin netzpolitische Themen einer interessierten Öffentlichkeit vorstellen. Unsere netzpolitischen Abende sind seit Jahren ein wichtiger Anlaufpunkt für die digitale Zivilgesellschaft in Berlin und verzeichneten auch im Jahr 2017 konstant hohe Besucherzahlen.

In kurzen Vorträgen werden netzpolitische Themen, Projekte, Initiativen und Kampagnen vorgestellt. Die netzpolitischen Abende dienen der Vernetzung und dem Wissensaustausch. Die Vorträge werden live gestreamt und später auf unserem Youtube-Kanal öffentlich zur Verfügung gestellt. Über die Jahre ist so ein umfangreiches, frei verfügbares Wissensarchiv zu netzpolitischen Themen entstanden. Auch 2017 haben wir mit den netzpolitischen Abenden zahlreichen Initiativen und wichtigen Anliegen für Verbraucher- und Grundrechte eine Plattform gegeben.

Netzpolitischer Abend auf der Webseite der Digitalen Gesellschaft:

https://digitalegesellschaft.de/portfolio-items/netzpolitischer-abend/

Unterstütze uns!

Liebe Freunde und Freundinnen der Digitalen Gesellschaft,

Engagement kostet viel Zeit und auch Geld. Auch in diesem Jahr haben wir für eine moderne Netzpolitik und Bürgerrechte gekämpft.

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 Grund- und Verbraucherrechte verteidigen können, brauchen wir eure Unterstützung.

Deshalb vorneweg, wie auch zum Schluss die Aufforderung: Werde / werden Sie Fördermitglied oder unterstützen Sie uns mit einer Spende.

Um uns zu helfen, könnt ihr zum einen 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 oder 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.

IBAN: DE88430609671125012800

BIC: GENODEM1GLS (44789 Bochum)

Spenden sind ebenfalls über betterplace möglich:

https://www.betterplace.org/de/projects/19435-spende-fur-menschenrechts-und-verbraucherfreundliche-netzpolitik

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.: Elke Steven, Digitale Gesellschaft e.V., Groninger Str. 7, 13347 Berlin