

Unsere rC3-Welt im Dezember 2020. Was das ist? Nachzulesen auf Seite 52



► Bibliographische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detailliertere bibliografische Daten sind im Internet über <https://www.dnb.de> abrufbar

► Rechteinweis:

Dieses Werk steht – soweit beim jeweiligen Text oder Bild nichts anderes vermerkt ist – unter der Creative Commons Lizenz cc by 4.0. Was das bedeutet, können Sie unter <http://de.creativecommons.org> nachlesen.

Bitte geben Sie bei Namensnennung (by) immer den Namen der Autorin oder des Autors eines Textes mit dem Hinweis „aus dem Buch ‚Digitalcourage für das Jahr 2022‘ “ an.

Wir danken allen Fotograf.innen, Karikaturist.innen und Grafiker.innen für freie Lizenzen oder freundliche Genehmigungen für den Abdruck. Insbesondere bedanken wir uns bei der Firma Panthermedia, die uns seit einigen Jahren mit Bildkontingenten unterstützt.

► Umschlagfotos:

Vorne oben: Matthias Hornung, cc by 4.0
(Künstlerische Gestaltung BigBrotherAwards: Angelika Höger)
Vorne unten: Stefanie Loos, cc by 4.0
Hinten: Digitalcourage, cc by 4.0

 Wir danken der Bewegungsstiftung für ihre Unterstützung.
Anstöße für soziale Bewegungen

► Impressum:

(cc by 4.0) 2022 Verlag Art d'Ameublement
Redaktionsschluss: November 2021
Digitalcourage e.V., Marktstraße 18, 33602 Bielefeld
Telefon: 0521 / 1639 1639
E-Mail: mail@digitalcourage.de
Internet: digitalcourage.de, bigbrotherawards.de
Mastodon: [@digitalcourage@digitalcourage.social](https://digitalcourage@digitalcourage.social)
Twitter: [@digitalcourage](https://twitter.com/digitalcourage)
Facebook, WhatsApp, Instagram: Nein.
Hrsg.: padeluun und Rena Tangens
Redaktionelle Zusammenstellung: [Claudia Fischer \(verstandenwerden.de\)](http://claudia.fischer@verstandenwerden.de)
Lektorat: [Claudia Fischer und Katrin Schwahlen \(katrinschwahlen.de\)](http://claudia.fischer@katrinschwahlen.de)
Layout und Design: [Isabel Wienold \(iwi-design.de\)](http://isabel.wienold@iwi-design.de)
ISBN 978-3-934636-29-3

padeluun und Rena Tangens (Hrsg.)

 **digitalcourage**

für das Jahr 2022

Vorwort	7
► Aktuelles und Begleitendes	9
Unser Auftrag an die neue Bundesregierung	10
Was wir alles tun Unser Motherboard	14
Schulen datenschutzfreundlich voranbringen!	22
Gemeinsam schaffen wir das: Das Netzwerk Freie Schulsoftware	26
Verbraucherschutz Digitalcourage ist jetzt Mitglied beim vzbv	28
Unsere Datenkrake im Haus der Geschichte	29
Aus hygienischen Gründen bargeldlos zahlen? Ist Quatsch.	30
Ein Etappensieg: Schufa zieht Pläne vorerst zurück	31
Nicht jammern – Klagen! Unsere Verfassungsbeschwerden	32
Warum der Kinderschutz nichts mit Vorratsdatenspeicherung zu tun hat	34
Digital Markets Act Europas historische Chance gegen Internetgiganten Warum Werbetacking schädlich und gefährlich ist	40 42
Lobbyismus live: Mit Facebook gegen Überwachung?!	45
Unterschreiben gegen Gesichtserkennung Worum geht es bei einer Europäischen Bürger.inneninitiative (EBI)?	46 48
Warum Digitalcourage?	49

Wir wollen ihn immer noch verhindern:	
Den Fingerabdruck im Perso	50
Der rC3: Ein Riesenspaß beim Chaos Communication Congress	52
Der Digitalzwangsmelder	54
kurz&mündig Digitales Wissen für die Hosentasche	56
Videoüberwachung bei Demonstrationen	60
Das Digitalcourage-Team Porträts	62
► Abgemahntes:	69
Vom Streaming her denken	
Backstage-Bericht von den BigBrotherAwards 2021	70
Rolf Gössner: Danke für 20 Jahre BigBrotherAwards-Jury!	72
Kategorie „Verkehr“ Frank Rosengart	
Die EU-Kommission	75
Kategorie „Bildung“ Prof. Dr. Peter Wedde	
Proctorio GmbH in München	79
Kategorie „Public Intellectual“ padeluun	
Prof. Dr. phil. Dr. h. c. Julian Nida-Rümelin	88
Kategorie „Was mich wirklich wütend macht“ Rena Tangens	
Google	97
Kategorie „Gesundheit“ Dr. Thilo Weichert	
Doctolib	108
► Aktivierendes	117
Digitale Selbstverteidigung	
Wie Sie Ihre Computer, Smartphones, E-Mails und Daten schützen können	118

Online Zusammenarbeiten in Homeoffice und Büro	119
Gemeinsam an Dateien arbeiten	120
Videokonferenzen	121
Telefonkonferenzen	122
Chatten, Koordinieren und Abstimmen	123
Termine finden	124
Umfragen	124
Daten teilen und austauschen	124
Post-It Tafeln, Bilder und Textschnipsel teilen	125
Daten und E-Mails verschlüsseln	126
CryptPad Für umfassende Teamarbeit	128
Fediverse So geht gutes Social Media	130
Der freie App-Store F-Droid und seine Apps	134
Kriterien für vertrauenswürdige Apps	138
OpenStreetMap	140
Gibt es ein Leben ohne Google? Der Europäische Suchindex	142
► Richtungweisendes	151
Public Domain vor 30 Jahren	152
Unsere Veranstaltungsreihe zu Technik, Kunst, Wissenschaft und Gesellschaft	152
40 Jahre Datenschutzbewegung in Deutschland	157
Geschichte und Geschichten	157
► Anhang	191
Preise und Auszeichnungen für Digitalcourage	192
Datenschutzrelevante Termine für 2022	194
Index	195



Gegen den Trend

Keine großen Veranstaltungen, keine Vorträge, keine Kongresse, keine Crypto-Cafés oder CryptoParties, keine Public Domains und keine ungeplanten Treffen. Schnell hatten wir eigene Videokonferenz-Server eingerichtet, aber das ist kein Ersatz für persönliche Begegnungen.

Es hat uns gebeutelt – die viele Zeit im Homeoffice, die häufigen Videokonferenzen haben uns gestresst, der Austausch mit anderen, die Aktionen, das gemeinsame Mittagessen im Team und die Gespräche nebenbei haben uns gefehlt. All das hat uns ganz schön mitgenommen.

Ja, Digitalcourage hat Corona überlebt – dank der Hilfe von vielen privaten Sponderinnen und Spendern, die uns unterstützt haben, und Fördermitgliedern, die ihren Beitrag erhöht haben, um die Ausfälle auszugleichen.

Und trotz Corona haben wir viel geschafft: Technik-Tipps fürs Homeoffice und Videokonferenzen, eine neue Buchreihe namens „kurz&mündig“ aufgelegt (mit mittlerweile 14 Titeln, ► Seite 56), rC3 - eine Art Online-Adventure-Welt beim Chaos Communication Congress gebaut (Seite 52), ein Bildungspaket herausgegeben und ein Netzwerk Freie Schulsoftware zur Selbsthilfe aufgesetzt (► Seite 22 und 26), eine freie Videoplattform namens PeerTube aufgebaut, einen weiteren Tor-Server zum unbeobachteten Surfen in Betrieb genommen (der inzwischen der viertgrößte weltweit ist), unser datenschutzfreundliches Terminvereinbarungstool „nuudel“ hat mittlerweile über 100.000 gleichzeitig laufende aktive Umfragen, wir haben eine Handreichung für

die nächste Bundesregierung erarbeitet mit Themen, die angepackt werden müssen (► Seite 10).

Und wir haben trotz Corona wieder eine BigBrotherAwards-Verleihung veranstaltet – mit einigen wegweisenden Preisträgern (► Seite 69). So der Arzttermindienst Doctolib, an denen wir auch weiter dranbleiben (► Seite 108). Und wir haben einmal das ganze Werbe-Tracking-Ökosystem seziiert, mit dem Google, Facebook & Co uns unserer persönlichsten Erfahrungen und Neigungen enteignen (► Seite 97). Und die mit ihren astronomischen Werbeeinnahmen jede Konkurrenz plattmachen und Macht über Institutionen, Politik und Medien, und damit auch über die Meinungsbildung gewinnen.

Während viele Firmen Arbeits- und Büroplätze abbauen, haben wir uns getraut, gegen den Trend zu handeln und haben, als sich die Gelegenheit bot, „zugeschlagen“ und weitere Räumlichkeiten vier Häuser weiter in der Marktstraße 26 angemietet. Damit wir auch mal einen Ruhearbeitsraum haben, in dem wir ungestört einen Text schreiben können. Und ein Studio, in dem wir Podcast- und Videoaufnahmen machen können. Und wo der Digitalcourage-Shop endlich aus dem Keller ins Erdgeschoß ziehen kann und im Schaufenster sichtbar wird. Der Shop wird zukünftig direkt mit dem Campaigning Hand in Hand arbeiten, und so werden wir bald viel häufiger auch „was zum Anfassen“ passend zu unseren politischen Themen haben.

Wir haben uns getraut, weitere Menschen einzustellen, denn es gibt so unendlich viele Themen zu bearbeiten. Wir schaffen viel, aber wir ärgern uns immer wieder, wenn wir etwas gerne tun würden, es aber nicht schaffen können. Wir müssen manchmal dann doch anerkennen, dass der Tag nur 24 Stunden hat.

Einmal mehr wollen wir „Danke“ sagen an alle Menschen, die uns so zuverlässig unterstützen. Ohne Sie und ohne Euch wäre all das nicht möglich. Dank der Hilfe unserer Mitglieder und Spender:innen finanziert Digitalcourage sich ohne staatliche Gelder und ohne Firmen-Sponsoring. Darauf sind wir stolz. Denn unsere Unabhängigkeit ist uns wichtig.

Wir sagen Danke an alle, die geholfen haben, Digitalcourage mit aufzubauen. Und wir sagen Danke an unser großartiges Team – wir sind glücklich, mit euch zusammen zu arbeiten! Und wir danken unseren aufgeweckten Praktikantinnen und Praktikanten, die immer wieder unsere Gedanken mit frischem Wind durchpusten.

Wohin das alles führt, können wir Ihnen einmal mehr in diesem Jahrbuch für das Jahr 2022 präsentieren.

Viel Spaß beim Lesen!
Rena Tangens & padeluum



Foto: Konstantin Macher, cc by-sa 4.0

Für ein Europa ohne Gesichtserkennung!



Foto: Till Rimmelle, cc by 4.0

Unser Auftrag an die neue Bundesregierung

Von Julia Witte und Konstantin Macher

Während dieses Jahrbuch in Druck geht, laufen in Berlin die Koalitionsverhandlungen für die neue Bundesregierung. Direkt nach der Wahl haben wir Handlungsempfehlungen zur Digitalpolitik formuliert und Anfang November 2021 an die Fachpolitikerinnen und Fachpolitiker übergeben (siehe Fotos). Einige haben sich bedankt – wir werden im Auge behalten, was davon wie umgesetzt wird und weiter Druck machen. Digitale Entwicklung braucht keinen Blockchain-Hype, keine Start-Up-Götter und kein „deutsches Google“ – sondern mutige politische Gestaltung.

Um Digitalisierung politisch zu verstehen, ist es erforderlich, Machtstrukturen, Geldströme und Souveränitäten zu verstehen. In den letzten Jahren wurde eine Digitalisierung vorangetrieben, die in erster Linie dazu dient, einen Anschein von Progressivität zu erwecken.

Gleichzeitig haben wir schon große Fortschritte auf dem Weg zu einer wirksamen Regulierung gemacht: Die europäische Datenschutzgrundverordnung (DSGVO) hat sich als richtungweisend erwiesen und ist – allen Unkenrufen zum Trotz – weltweit zum Vorbild geworden. Der anstehende Digital Markets Act und der Digital Services Act (► Seite 40) bieten wieder die Möglichkeit einer Weichenstellung für unsere Zukunft. Wir müssen es schaffen, das System Überwachungskapitalismus, das sich in den letzten zwanzig Jahren herausgebildet und immer weiter Fahrt aufgenommen hat, zu wandeln – hin zu Digitalisierung, die der Allgemeinheit dient, Kommunikationsgesellschaft fördert und Bildung und Wirtschaft in die Breite zurückbringt.

Wir verstehen Datenschutz nicht als Selbstzweck – denn so wie das Postgeheimnis nicht Briefumschläge schützt, schützt auch der Datenschutz nicht

Daten, sondern Menschen. Wir fordern deshalb die Politik auf, eine lebenswerte digital vernetzte Welt zu gestalten. Wir wollen nicht zu Datensätzen degradiert, technokratisiert und manipuliert und monetarisiert werden. Wir wollen auch im digitalen Zeitalter in einer freiheitlichen Demokratie leben und unser Grundrecht auf Privatsphäre lebendig erhalten.

Die neue Bundesregierung muss jetzt die Rahmenbedingungen für eine lebenswerte Welt im digitalen Zeitalter schaffen. **Digitalcourage fordert daher, folgende Prioritäten in den Koalitionsvertrag aufzunehmen:**

► **Machtkonzentration der Internetmonopole brechen**

Die Monopolstellung großer Internetkonzerne schadet unserer Demokratie. Monopolisten:innen nutzen ihren Zugriff auf Daten und Finanzkraft, um breiten Einfluss auf Politik, Wissen-

schaft, Bildung, Medien und die öffentliche Meinung zu nehmen. Die Bundesregierung wird ein wirksames Wettbewerbsrecht mit der Möglichkeit der Entflechtung schaffen und sich in der EU für einen starken Digital Markets Act einsetzen, der zu große Machtkonzentration effektiv verhindert, schon bevor eine konkrete Marktmanipulation nachgewiesen wurde. Um eine souveräne, dezentrale Infrastruktur zu ermöglichen, engagiert sich die Bundesregierung für einen Europäischen Suchindex als positives Gegenmodell. (► Seite 142)

► **Tracking, personalisierte Werbung und Dark Patterns verbieten**

Die Komplettüberwachung des Online-Verhaltens entmündigt Menschen und degradiert sie zu Objekten von technokratischen Prognosen und profitorientierter Beeinflussung. Verlage und Kreative bekommen einen immer geringe-

ren Anteil der Werbeeinnahmen. Die Bundesregierung wird darauf hinwirken, dass Tracking, personalisierte Werbung und manipulativ gestaltete Cookie-Banner (Dark Patterns) verbo-

ten werden und lenkt stattdessen Energie in Innovation für faire, datenschutz- und gesellschaftsfreundliche Geschäftsmodelle. (► Seite 106)

Foto: Stefanie Loos, cc by 4.0



Wiebke Esdar (SPD) nimmt unsere 15 Prioritäten für die Verhandler:innen entgegen.

Erhältlich im Digitalcourage-Shop!**Aufkleber
„Digitalcourage Bildungspaket“**

10 Motive gemischt, DIN A8 (5,2 x 7,4 cm)

Preis: 2,50 Euro zzgl. Versand

► shop.digitalcourage.de

► Nachhaltige digitale Bildung ermöglichen

Die Bundesregierung wird zusammen mit den Ländern Rahmenbedingungen dafür schaffen, dass IT-Fachpersonal, Datenschutzbeauftragte und Medienpädagog:innen Schulen unterstützen bei der Nutzung von Freier Software und eigener Infrastruktur. Digitale Bildung wird verpflichtender Teil der Lehrkräfteausbildung, um Verständnis zu fördern für Zusammenhänge von Technikgestaltung, Mediennutzung, Politik, Wirtschaft und Gesellschaft. Statt nur zu lernen, einzelne Programmsysteme zu bedienen, werden Kinder befähigt, mit digitaler Technik mündig und kompetent umzugehen. (► Seite 24)

► Biometrische Überwachung verbieten

Biometrische Überwachungstechnologien stellen eine Gefahr für Rechtsstaatlichkeit und unsere Grundfrei-

heiten dar und können Diskriminierungen verstärken. Die Bundesregierung wird sich für ein europaweites Verbot biometrischer Massenüberwachung einsetzen. Insbesondere der Einsatz automatisierter Gesichtserkennung im öffentlichen Raum wird staatlichen und privaten Stellen sofort verboten. (► Seite 46)

► Digitales anonymes Bargeld

Kryptowährungen auf Blockchain-Basis schaden durch ihren hohen Stromverbrauch dem Klima und damit der Allgemeinheit und stellen ein Datenschutzproblem dar. Die Bundesregierung wird sich für ein digitales Bargeld einsetzen, das den Schutz privater Daten gewährleistet und mit dem Währungsspekulationen und Geldwäsche nicht möglich sind. Es wird staatliches, digitales Bargeld geschaffen und derart gestaltet, dass nicht nachvollziehbar ist, wer es wann und wofür ausgibt. (► Seite 30)

► Moratorium für kommerzielle Überwachungstechnologien

Deutsche Behörden dürfen keine kommerziellen Staatstrojaner erwerben. Der Export von Überwachungstechnologien wird verboten. Der bisherige Einsatz solcher Software wird aufgeklärt.

(► Seite 32)



Foto: Stefanie Loos, cc by 4.0



Geheimdienste abschaffen! Unser Protest gegen das BND-Gesetz 2016

► **Verfassungsschutz abwickeln**

Der Verfassungsschutz wird aufgelöst und ersetzt durch eine transparent arbeitende, demokratisch kontrollierbare Behörde.

► **Chatkontrolle abwenden – Privatsphäre wahren (ePrivacy)**

Die Bundesregierung wird sich auf europäischer Ebene für einen Schutz der Privatsphäre einsetzen und sich Ausnahmeregelungen in der ePrivacy-Richtlinie entgegenstellen.

► **Public Money – Public Code**

Mit öffentlichen Geldern für öffentliche Verwaltungen entwickelte Software wird unter einer Freie-Software- und Open-Source-Lizenz veröffentlicht.

► **Vollautonome Waffensysteme international ächten**



Sticker: FIF

Waffen dürfen niemals selbstständig entscheiden, ob sie einen Menschen verletzen oder töten. Die Bundesregierung wird auf ein weltweites Verbot von autonomen Waffensystemen hinwirken.

► **Digitalzwang vermeiden – Menschen nicht ausschließen**

Die Teilhabe am öffentlichen Leben wird auch für Menschen gewährleistet, die bestimmte digitale Anwendungen oder Technologien nicht nutzen können oder wollen. (► Seite 54)

► **Meldepflicht für IT-Sicherheitslücken**

Um die Sicherheit von Privatpersonen und Unternehmen nicht fahrlässig zu gefährden, wird Behörden die Nutzung von IT-Sicherheitslücken verboten. Stattdessen werden sie verpflichtet, ihnen bekannte Schwachstellen zu melden und auf deren Schließung hinzuwirken.

► **Vorratsdatenspeicherung**

Vorratsdatenspeicherung verhindert keine Verbrechen, sondern missachtet die Grundrechte der Bürger:innen und schadet der Wirtschaft. Zukünftig gilt deshalb: Eine anlasslose Speicherung von Verbindungsdaten findet nicht statt. (► Seite 32)

► **Verschlüsselung als Grundrecht und Wirtschaftsmotor**

Die Bundesregierung wird das uneingeschränkte Recht auf Verschlüsselung als Grundrechtsschutz und Standortfaktor verteidigen.

► **Anonymes Reisen**

Die Möglichkeit des anonymen Reisens innerhalb Europas mit öffentlichen und individuellen Verkehrsmitteln wird gewährleistet.

Aktivcongress

Neue Ideen – Neue Möglichkeiten

Der Aktivcongress ist ein Treffen im Barcamp-Format für alle, die sich für Datenschutz, Grundrechte und freie Netze einsetzen und die nicht nur reden, sondern auch selber etwas tun wollen. Hier werden Themen vorgestellt, Inhalte diskutiert, Strategien erdacht und Aktionen geplant.

Digitale Selbstverteidigung

Techniktipps zur Selbsthilfe

Da weder Firmen noch Politik unsere Privatsphäre achten, müssen wir uns selbst schützen. Die gute Nachricht: Es gibt viele Möglichkeiten – technische und organisatorische – und nicht alle davon sind aufwändig oder kompliziert. Einige unserer Hinweise gibt es in diesem Jahrbuch. ► Seite 117

Recherche und Pressearbeit

Aufdecken, einordnen, veröffentlichen

Wir gehen den Dingen auf den Grund, und wir wollen selber verstehen, was läuft. Deshalb recherchieren wir viel und in Tiefe. Nicht nur bei der Recherche für die BigBrotherAwards, sondern auch zu Themen, die uns im Alltag erreichen. Und schließlich veröffentlichen wir: Als Pressemitteilung, im Digitalcourage-Newsletter, im Blog auf unserer Website, auf Twitter und im Fediverse. Wir haben eine große Reichweite und sind gefragt als Ansprechpartner:innen von Presse und Medien.

Demos organisieren

Gemeinsam sind wir stark!

Wir verteidigen unsere Demokratie! Egal, ob gegen Überwachung oder gegen Rechts – wir gehen für die Freiheit auf die Straße! „Freiheit statt Angst“, #unteilbar, #keinFußbreit und „Rettet die Grundrechte“ sind nur einige Großdemos, die wir in den vergangenen Jahren (mit)organisiert haben. Gemeinsam sind wir stärker! Wir möchten, dass viele Menschen es uns gleich tun und bieten daher auch Hilfestellungen an: Wir organisieren die Versendung von Plakaten, Flyern, Ordnerbinden, Warnwesten, Kreidespray, und kümmern uns um Verwaltung und Organisation. Mit unserer Infrastruktur möchten wir die Menschen unterstützen, die auf die Straße gehen und Zivilcourage und Gesicht zeigen!

Vorträge

Smart City, digitale Mündigkeit und Selbstverteidigung, Big Data, Polizeigesetze

Es gibt eine Menge Themen, mit denen wir uns auskennen. Wir haben was mitzuteilen und geben unser Wissen gerne weiter. Sie können uns einladen zu Vorträgen, Podiumsdiskussionen, Seminaren und Workshops. Unser Team ist in der ganzen Bundesrepublik – und darüber hinaus – unterwegs.

BIG BROTHER AWARDS

Die Oscars für Datenkraken

Die BigBrotherAwards sind ein Datenschutz-Negativpreis, den wir in Deutschland seit 2000 jährlich verleihen. Datenkraken bekommen so das, was sie am wenigsten mögen: Das Licht der Öffentlichkeit. Die Jury besteht aus renommierten Fachleuten von verschiedenen Bürgerrechtsorganisationen. Gemeinsam haben wir mit den BigBrotherAwards Missstände nicht nur aufgedeckt, sondern echte Verbesserungen erzielt und heikle Themen auf die politische Agenda gesetzt. (► Seite 69)

Tor-Server

Unbeobachtet surfen

Wer seine Privatsphäre auch im Internet schützen will, surft mit Tor. Die Abkürzung „Tor“ steht für „The Onion Router“ – ein Netzwerk, das in mehreren Schichten funktioniert, wie eine Zwiebel (englisch: Onion). Damit ist eine Rückverfolgung, wann welche Webseite aufgerufen hat, unmöglich. Digitalcourage betreibt einen Tor-Exit-Knoten, denn weil diese besonders gefährdet sind, gibt es davon besonders wenige. Unsere Tor-Knoten laufen ohne Virtualisierung auf einem nur von uns gepflegten dedizierten Server bei einem kleinen deutschen Anbieter, und natürlich speichern wir keinerlei Daten über deren Nutzer – wie es bei Tor-Relays üblich ist.

Mastodon-Instanz

digitalcourage.social

Mastodon ist ein verteilter Mikrobloggingdienst, der seit 2016 von Eugen Rochko entwickelt wird; einem deutschen Programmierer aus Jena. Im Gegensatz zu großen Plattformen wie Twitter ist Mastodon als dezentrales Netzwerk konzipiert. Benutzer:innen können einer beliebigen Instanz beitreten oder selbst eine eigene betreiben. Wir betreiben eine eigene Mastodon-Instanz. Wer möchte, kann einen Zugang zu unserer Instanz bekommen. (► Seite 131)

Freedom not Fear

Vernetzung europaweit

„Freedom not Fear“ (FnF) ist das europäische Datenschutz-Barcamp-Wochenende in Brüssel – voller Vorträge, Diskussionen, Workshops und Aktionen. FnF wird von und für Datenschutzaktivist:innen aus ganz Europa organisiert – und wir sind auch im Orga-Team mit dabei. Hier kommen Politiker:innen mit Aktivist:innen zusammen. Außerdem organisieren wir Gespräche mit Abgeordneten direkt im EU-Parlament. So entsteht ein großes Vernetzungstreffen mit Menschen aus ganz Europa, die gemeinsam für das Wohl der Bürger:innen in der EU kämpfen. freedomnotfear.org

Charmante Aktionen

Wir sind freundlich, aber wir lassen uns nicht veralbern!

Ob wir eine Million Aufkleber verteilen, die Asyl für Edward Snowden fordern, in Berlin gegen Überwachung auf die Straße gehen, gegen die Vorratsdatenspeicherung Unterschriften sammeln oder auf dem Kirchentag eine Resolution für besseren EU-Datenschutz durchboxen: Ein Großteil unserer Arbeit besteht darin, Aktionen zu organisieren und thematische Kampagnen durchzuführen. Da kann es schon mal passieren, dass wir allen Bundestagsabgeordneten Placebo-Pillen gegen Angst vor Terror zukommen lassen oder riesige Schilder in der Berliner U-Bahn mit ehrlichen Hinweisen auf Videoüberwachung überkleben. Diese Aktionen sind nur möglich, wenn wir von unseren Ortsgruppen, Ehrenamtlichen und anderen Menschen tatkräftig unterstützt werden.

Überwachungs- gesamtrechnung

1 + 1 + 1 = ZU VIEL

Eine einzelne Überwachungsmaßnahme mag für sich gesehen noch akzeptabel erscheinen. Doch ihre Bewertung muss immer im Kontext aller anderen Überwachungsmethoden stattfinden. Das hat das Bundesverfassungsgericht 2010 sinngemäß so formuliert.

Um zu belegen, wie viele Überwachungsmaßnahmen seit 2010 neu hinzugekommen sind, haben wir mehrere Jahre lang eine Liste „Überwachungs-gesamtrechnung“ auf digitalcourage.de gepflegt. Anfang 2021 hat nun die Friedrich-Naumann-Stiftung das Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht, Abteilung Öffentliches Recht in Freiburg i. Br. beauftragt, eine ähnliche Aufstellung zu machen und ein „Überwachungsbarometer“ zu entwickeln. Wir freuen uns, dass unsere Idee aufgegriffen wurde! (Links über die Jahrbuch-Webseite)

CryptoParties

Digitale Selbstverteidigung lernen

Gemeinsam mit unseren Digitalcourage-Hochschulgruppen und -Ortsgruppen bieten wir an vielen Orten CryptoParties und CryptoCafés an. Hier heißt es: eigenen Rechner mitbringen! Bei diesen Treffen kommen Selbstverteidigungs-Profis und Laien zusammen, um in geselliger Runde gemeinsam die eigenen Geräte unter die Lupe zu nehmen und Hilfestellung beim Verschlüsseln von E-Mails, beim Sicherer-Machen von Smartphones oder beim Installieren von Linux zu geben.

Online- Shop

Gadgets, Gimmicks, Bücher, Geschenkideen

In unserem Shop für Unterstützungsbedarf finden Sie Gadgets und Geschenkideen, Bücher und Informationsmaterial zum Verteilen: vom PrivacyDongle zum unbeobachteten Surfen über Wissenslektüre zum Weitergeben bis zum Buch „Qualityland“ von Marc-Uwe Kling. Die Einnahmen aus dem Shop kommen in voller Höhe unserer inhaltlichen Arbeit zugute. shop.digitalcourage.de

CiviCRM

Freie Software zur Adressen-, Mitglieder- und Spendenverwaltung

Für unsere Arbeit nutzen wir ein freies Kontaktmanagement-System namens „CiviCRM“. Wir haben die Software für die Anforderungen in Deutschland bei Banken und Steuerrecht angepasst, also z.B. Lastschriftmöglichkeit und Spendenquittungen eingebaut. So profitieren wir nicht nur von Freier Software, sondern wir tragen auch zu ihrer Entwicklung bei. Um diese Arbeit dauerhaft zu stemmen, haben wir mit anderen Organisationen gemeinsam den Verein „Software für Engagierte“ gegründet, der an „CiviCRM“ weiter arbeitet und Schulungen dazu anbietet.

Public Domain

Die Veranstaltungsreihe seit 1987

„Public Domain“ heißt einerseits „öffentlicher Raum“ – das bedeutet: „jede und jeder kann kommen“ und andererseits heißt es „öffentliche Angelegenheit“ – mit anderen Worten: „Da sollten wir uns drum kümmern!“ Seit 1987 veranstalten wir Vorträge, Vorführungen und Diskussionen unter diesem Titel. Die Veranstaltungsreihe hat sich zu einem wichtigen Treffpunkt im Spannungsfeld Zukunft und Gesellschaft, Technik, Wissenschaft, Kunst und Kultur entwickelt. Fun Fact: Auf einer frühen PUBLIC DOMAIN hat sich der Digitalcourage (damals unter dem Namen FoeBuD e. V.) gegründet. (► Seite 152)

Zensurfreier DNS-Server

Alternativer Domain Name Service

DNS-Server sind praktisch das Telefonbuch im Internet. DNS steht für „Domain Name Service“ – eine Datenbank, die Domainnamen in die zugehörigen Zahlen umsetzt. Digitalcourage betreibt einen öffentlichen zensurfreien DNS-Server. Damit die DNS-Abfragen nicht (wie üblich) im Klartext gestellt und beantwortet werden, unterstützt unser neuer Server nur noch verschlüsselte Kommunikation (bisher nur) via DNS-over-TLS. Dann können auch alle Provider den Verkehr nicht mehr mitlesen. Gleichzeitig bieten wir mit unserem Server eine Alternative zum DNS von Google. **Der Server hat die IP 5.9.164.112 (IPV4) bzw. 2a01:4f8:251:554::2 (IPV6)**

Advocacy

Lobbyarbeit im Sinne der Allgemeinheit

Advocacy ist die Einflussnahme auf die Politikgestaltung – aber anders als beim Lobbying arbeiten wir nicht für Einzelinteressen, sondern im Interesse der Allgemeinheit. Wir mischen uns ein, begleiten laufende Gesetzgebungsprozesse, sprechen mit Politikerinnen und Politikern und verfassen Stellungnahmen für Anhörungen zu Gesetzentwürfen. Damit verleihen wir Freiheitsrechten und Privatsphäre Nachdruck – für eine starke Demokratie.

Datenschutz an Schulen

Eine Investition in die Zukunft

Kinder steuern ihre Bildungsinhalte nicht selbst. Das machen Eltern und Schulen. Wir geben Nachhilfe: In unserem **Bildungspaket** voller Infomaterialien, helfen wir Eltern, Schulen und Politiker:innen mit Ideen, wie digitaler Unterricht frei, nachhaltig und datenschutzfreundlich gelingen kann. Und in unserem **Netzwerk Freie Schulsoftware** stellen Schulen ihre Erfahrungen mit grundrechtewahrender Software für andere, die gerade einsteigen wollen, zur Verfügung. (► Seite 22)

Termine und Umfragen

Schnell Termine finden, an denen die meisten Interessierten Zeit haben? Einfach eigene Umfragen machen? Dafür bieten wir das datenschutzfreundliche Terminfindungstool nuudel.digitalcourage.de an – frei von Google Analytics und sonstigen Trackern.



Lesen gegen Überwachung

Belletristik, Science Fiction und Sachbücher

Es gibt eine Menge spannender Texte, die sich mit Überwachung, Konsum und dem Leben in totalitären Gesellschaften auseinandersetzen und unterschiedliche Facetten beleuchten. Bei „Lesen gegen Überwachung“ wird vorgelesen – im Cafe, auf der Straße oder in einem Salon – und es gibt Zeit für Fragen und Diskussion, und Raum für eigene Texte und Ideen. Die Aktion lässt sich mit einfachen Mitteln veranstalten, auch umsonst und draußen während der Corona-Zeit, sobald das Wetter mitspielt. Organisieren auch Sie in Ihrer Stadt ein „Lesen gegen Überwachung“. Wir unterstützen Sie bei den Vorbereitungen!



Gemeinsam an Dokumenten arbeiten

Mit der freien Software CryptPad können nicht nur Texte, sondern auch Tabellen, Präsentationen und Umfragen im Browser erstellt und gleichzeitig bearbeitet werden, während man sich zeitgleich im integrierten Chat-Fenster dazu bespricht. Der Kniff bei CryptPad: Alle Daten liegen verschlüsselt auf dem Server - nicht mal die Admins können mitlesen. Falls gewünscht, kann auch ein Account erstellt werden, um Dokumente in einem eigenen Speicher langfristig zu organisieren. Das geht nicht nur allein, sondern auch für Gruppen. Mehr erfahren? ► Seite 120 und 128 Ausprobieren? Hier entlang: cryptpad.digitalcourage.de

Ortsgruppen / Hochschulgruppen

Mitmachen vor Ort!

Unsere Arbeit lebt vom Engagement und der Courage vieler Menschen. Ob durch Spenden, im Praktikum, in AGs zum Texten, Korrigieren, Fotografieren, Übersetzen oder in der AG Digitale Selbstverteidigung (ab Seite 118). Sie können auch in einer unserer unserer Ortsgruppen (derzeit Braunschweig, Bremen, Kiel, Köln und München) oder Hochschulgruppen (Bayreuth und Bielefeld) aktiv mitmachen. Das ist dann mehr als Kaffeetrinken: Die OG Braunschweig hat gerade ein Dossier zur Netzpolitik für die Niedersächsische Landeszentrale für politische Bildung geschrieben (Link über die Jahrbuch-Website) und die OG Bremen hat maßgeblich dabei geholfen, den Staatstrojaner in Bremen zu verhindern. Sie wollen etwas tun? Hier entlang: digitalcourage.de/helfen

PeerTube

Plattformfreie Videos

Unser Online-Videos liegen jetzt nicht mehr bei Datenkraken wie YouTube oder Vimeo, sondern wir betreiben einen eigenen PeerTube-Kanal. PeerTube ist freie und quelloffene Software, die Videos dezentral lagert und ein eigenes Netzwerk aus verschiedenen Instanzen bildet. Für themenähnliche und befreundete Organisationen bieten wir mit digitalcourage.video die Möglichkeit, unsere trackingfreie Instanz ebenfalls zu nutzen. Seitdem gehen unser Filme nicht mehr in der Masse der Katzen- und Böldkstoff-Videos unter und die großen Datenkraken gucken in die Röhre.

Nicht jammern – klagen!

Wir tun es nicht gern, aber manchmal sind Grundrechts-

verletzungen und Überwachungswahn der Politik nur auf dem juristischen Weg zu stoppen. Wir reichen Verfassungsbeschwerden ein (► Seite 32), klagen gegen Fingerabdrücke im Personalausweis (► Seite 50) oder erstatten Strafanzeigen, wenn nötig. Auf diese Weise haben wir schon das erste Gesetz zur Vorratsdatenspeicherung und ELENA (den elektronischen Entgeltnachweis) erfolgreich gekippt. Bei vielen juristischen Aktionen bieten wir die Möglichkeit, mit zu unterzeichnen und sich daran zu beteiligen. Regelmäßig stellen wir außerdem Anfragen auf Akteneinsicht bei Behörden nach dem Informationsfreiheitsgesetz (IFG) und veröffentlichen die befreiten Dokumente.

**Juristisches:
Verfassungsbeschwerden & Co****KURZ&MÜNDIG****Wissen kompakt**

Damit der Weg in eine lebenswerte Welt im digitalen Zeitalter (Motto von Digitalcourage) für alle einfacher verständlich wird, schreiben und drucken wir kompaktes Wissen im Hosentaschenformat. In der Booklet-Reihe „kurz&mündig“ geht es um Sicherheitstipps für Computer und Handy, um digitale Bildung, faire Website-Programmierung, Versammlungsfreiheit oder digitale Mündigkeit. (► Seite 56)

**Podcasts****Digitalcourage auf die Ohren**

Seit 2018 sendet Digitalcourage – genauer gesagt unsere Ortsgruppe München – im Rahmen des Formats „Forum aktuell“ bei Radio Lora. Alle zwei Monate spricht Moderator Lars Tebelmann jeweils eine Stunde lang über aktuelle Digitalcourage-Themen und lädt Gäste ein. Im Live-Programm kann man auch anrufen und mitdiskutieren. Später sind die Folgen dann als Podcasts auf unserer Website abrufbar:

digitalcourage.de/podcast

Schulen datenschutz- freundlich voranbringen!

Von Jessica Wawrzyniak

Foto: Fabian Kurz, cc by-sa 4.0



Jessica Wawrzyniak, Medienpädagogin bei Digitalcourage, mit ihrem Lexikon #Kids #digital #genial

Im September 2020 haben wir Susanne Eisenmann, die damalige Ministerin für Kultus, Jugend und Sport des Landes Baden-Württemberg (CDU), mit einem unserer BigBrotherAwards ausgezeichnet. Ausschlaggebend waren ihre Bestrebungen, wesentliche Dienste der digitalen Bildungsplattform des Landes von Microsoft betreiben zu lassen. Zeitgleich zu der Verleihung der „Oscars für Datenkraken“ bildete sich ein Bündnis gegen das Vorhaben. Die Kampfansage: Wir wollen die Daten von Kindern

nicht Microsoft in den Rachen werfen!
(unsere-digitale-schule.de)

► **Feierstimmung!**

Es war ein langer Weg, aber im Mai 2021 konnten wir mit Freuden einen Erfolg vermelden: Stefan Brink, der Landesbeauftragte für Datenschutz und Informationsfreiheit (LfDI), schätzte Microsoft 365 an Schulen als **nicht zulässig** ein. Frau Eisenmann, die bei der baden-württembergischen Landtagswahl 2021 als CDU-Spitzenkandidatin antrat, hatte sich nach niederschmetternden Wahlergebnissen inzwischen aus der Politik zurückgezogen und die amtierende Kultusministerin Theresa Schopper (Bündnis 90/Die Grünen) möchte den Job offensichtlich besser machen als ihre Vorgängerin. Sie verkündete im Juli 2021, dass Microsoft 365 nicht in die Digitale Bildungsplattform des Landes integriert wird.

► **Was in der Zwischenzeit geschah:**

Herbst 2020: Der verliehene BigBrotherAward sorgte nicht nur für eine erhöhte Aufmerksamkeit in der Presse, sondern Teile aus der BBA-Laudatio fanden auch ihren Weg in den Bildungsausschuss des Landtags. Trotz aller Kritik aber ging im Oktober ein Pilotprojekt mit Microsoft 365 an einigen Berufsschulen in Baden-Württemberg los.

Foto: Cord Santeimann, cc by-sa 4.0



Winter 2020/21: Viele Eltern, Lehrkräfte, Datenschützer und zivilgesellschaftliche Organisationen – auch Digitalcourage – haben sich zum Bündnis „Unsere digitale Schule“ zusammengeschlossen, um das Kultusministerium in Baden-Württemberg zu einer Umkehr zu bewegen.

Es wurden Gespräche mit dem Landesdatenschutzbeauftragten aufgenommen, der eine gründliche Prüfung der Datenflüsse an Microsoft versprach. Das Bündnis veröffentlichte im Januar 2021 eine gemeinsame Stellungnahme mit der Forderung, kommerzielle Cloud-Software durch Open-Source-Lösungen zu ersetzen.

März/April 2021: Im März verkündete Ministerin Eisenmann ihren Rückzug, und dann wurde es richtig spannend: Ralf Armbruster, Leiter der Stabstelle Digitale Bildungsplattformen, zeigte sich optimistisch und erklärte am 1. April bei Twitter, dass für den Start der Bildungsplattform mit Microsoft 365 alles vorbereitet sei. Leider kein April-Scherz. Die datenschutzrechtliche Auswertung des vorausgegangenen Pilotprojekts liege aber noch beim LfDI und die Frage, ob die Software tatsächlich eingebaut würde, in der Hand des zukünftigen Kultusministers bzw. der künfti-

Pressekonferenz des Bündnisses „Unsere Digitale Schule“: Lennard Indlekofer (Landesschülerbeirat Baden-Württemberg), Michael Mittelstaedt (Vorstand des Landeselternbeirats), Stefan Leibfarth (Chaos Computer Club Stuttgart)

gen Bildungsministerin. Zu diesem Zeitpunkt war Eisenmanns Nachfolge nicht geklärt, aber es wurde bekannt, dass das Ministerium an die Grünen übergeht. Das Bündnis erfasste die Gelegenheit und mischte sich mit einem Positionspapier in die Koalitionsverhandlungen der neuen Regierung ein. Ende April die große Erleichterung: Der LfDI sprach sich gegen den schulischen Einsatz von Microsoft 365 aus und kündigte eine Duldung bis nach den Sommerferien 2021 an. Danach würde die Nutzung datenschutzrechtliche Konsequenzen mit sich ziehen.

Mai 2021: Wir hofften also auf frischen Wind in der Bildungspolitik unter Kultusministerin Theresa Schopper und ein Verbot von Microsoft 365 an Schulen – so nah schien das Sommermärchen mit Aussicht auf ein Happy End. Doch im Mai sorgten zunächst noch Meldungen des Landeshochschulnetzes „BeiWü“ für Aufruhr. Der IT-Dienstleister, der für

das Lernmanagement-System Moodle und andere schulischen Softwarelösungen sowohl Serverplatz als auch das Hosting bereitstellt, gab bekannt, dass er einen Großteil dieser Dienste zukünftig nicht mehr für Schulen anbieten wird. Genau die Programme, die als Ersatz für Microsoft 365 so wichtig sind. BelWü hatte dem Kultusministerium schon Monate vorher angekündigt, dass ihre Personal- und Server-Ressourcen an Grenzen stoßen. Da das Kultusministerium offensichtlich verpasst hat, frühzeitig auf BelWüs Ausstieg zu reagieren und nur schwammige neue Lösungen parat hatte, kamen schnell Zweifel an der erhofften Abkehr von Microsoft auf.

Währenddessen hatten sich auch Pro-Microsoft-Lager gebildet: Schüler:innen,

Eltern und Lehrkräfte, die durch den Wegfall von Microsoft-Software den Erhalt von Bildung gefährdet sehen. (Was natürlich hanebüchener Unsinn ist, um es an dieser Stelle noch einmal zu betonen. Vor allem wäre es ein Skandal, wenn unser Bildungssystem tatsächlich derart abhängig von einem Großkonzern wäre.)

Juli 2021: Erleichterung! Im Juli 2021 wurde das endgültige Aus für Microsoft 365 als Teil der Digitalen Bildungsplattform verkündet. Was für ein Erfolg! Mit einem kleinen Dämpfer: Der LfDI will die Nutzung von Microsoft 365 nicht generell verbieten, bis landeseigene Softwarelösungen zur Verfügung stehen. Und das kann lange dauern. Zum Zeitpunkt des Redaktionsschlusses dieses Artikels (Spätsommer 2021), gehen in Baden-Württemberg die Ausschreibungen für landeseigene Software-Lösungen los und Digitalcourage hat ein Papier mitgezeichnet, das der neuen Ministerin die Dringlichkeit für gute Alternativen verdeutlicht.

Wir hoffen also weiterhin auf das „happy“ auf dem holprigen, langen Weg zum Ende: Funktionierende, freie Schulsoftware, die sowohl die Grundrechte als auch die Privatsphäre von Kindern und Lehrkräften achtet.

- Aktuelle Entwicklungen zum Thema Datenschutz an Schulen finden Sie auf digitalcourage.de/kinder-und-jugendliche/schulen.

Erhältlich im Digitalcourage-Shop!

„#KIDS #DIGITAL #GENIAL

Schütze dich und deine Daten!

Das Lexikon von App bis .zip“



Hardcover, 1. Auflage, 68 Seiten

Mengenrabatt bei Klassensätzen:

Einzelpreis: 12 € ISBN 978-3-934636-18-7

ab 11 Stk: 11,04 €, ab 26 Stk: 10,80 €

Softcover, 2. erweiterte Auflage, 96 Seiten

Mengenrabatt bei Klassensätzen:

Einzelpreis: 3,85 € ISBN 978-3-934636-20-0

ab 11 Stk: 3,54 €, ab 26 Stk: 3,47 €

Jeweils versandkostenfrei

► shop.digitalcourage.de



Das Digitalcourage-Bildungspaket

Digitalcourage verfolgt das bildungspolitische Geschehen überall im Land. Baden-Württemberg ist nur ein Beispiel, das öffentlich stark diskutiert wurde und zeigt, wie viel Stress und Ärger die Wahl der falschen Schulsoftware mit sich bringen kann. Auch andere Bundesländer und Städte haben Nachholbedarf bei der Gestaltung freier, grundrechtewahrender und nachhaltiger digitaler Bildung. Schulen, die zwischen verschiedenen Anforderungen zerrissen werden und gleichzeitig die Verantwortung für ihre Schüler:innen tragen, brauchen Orientierung.

Daher haben Medienpädagogin Jessica Wawrzyniak und Netzphilosophin Leena Simon ein Informationspaket zusammengestellt, das Eltern, Schulen und Politiker:innen aufklärt: über datenschutzrechtliche Bestimmungen an Schulen, bildungspolitische Versäumnisse, die ausgeräumt werden müssen, und konkrete Lösungen für Schulen. Dank unserer Unterstützer:innen haben wir bereits über 800 der Infopakete – bestehend aus Büchern, Broschüren, Flyern und (weil wir nicht anders können ;-)) thematisch passenden Aufklebern – verteilt.

Mit dem Digitalcourage-Bildungspaket möchten wir Aufmerksamkeit für das Thema Datenschutz an Schulen schaffen: Sowohl im

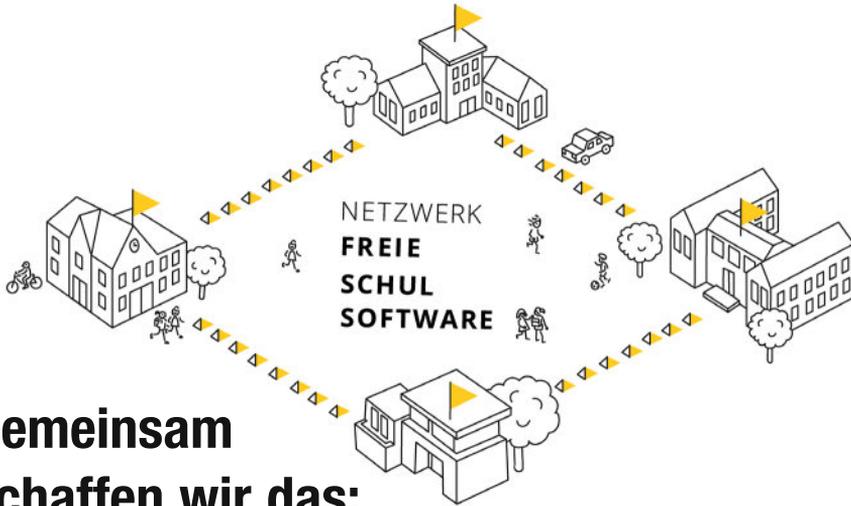
Umgang mit den Daten von Schülerinnen und Schülern, als auch bei der Vermittlung von Datenschutzthemen in der Lehre.

Das Paket kann nach wie vor im Digitalcourage-Shop bestellt werden und es gibt auch eine Basisversion (ohne die gedruckten Hefte, aber mit einer Zusammenfassung der wichtigsten Informationen), die als PDF heruntergeladen und an Interessierte verteilt werden kann. Alle, die ein Bildungspaket bestellen und weitergeben, tragen einen Teil zur Aufklärung an Schulen bei.

Sie haben selbst Kinder oder kennen Eltern schulpflichtiger Kinder? Sie kennen Lehrerinnen und Lehrer oder beteiligen sich an der Regionalpolitik Ihrer Stadt? Dann helfen Sie mit!

digitalcourage.de/bildungspaket





Grafik: Ann Kathrin Damme, Digitalcourage cc by 4.0

Gemeinsam schaffen wir das:

Das Netzwerk Freie Schulsoftware

Was wir während unserer Kampagne gelernt haben: Viele Schulen und Lehrkräfte haben sich in Software-Alternativen reingefuchst und bieten richtig gute Lösungen an. Seit dem Sommer 2021 bieten wir deshalb auch ein Netzwerk für konkrete Hilfestellungen in der Praxis an.

Es gibt viele Schulen, die bereits einen Weg gefunden haben, Freie Software an Ihrer Schule einzusetzen und damit gute

Erfahrungen machen. Diese Erfahrungen sind ein wichtiger Schlüssel, denn sie können anderen schnell helfen, während Entscheidungen auf bildungspolitischer Ebene in langen Diskussionen ausgehandelt werden.

So geht's: Schulen, die sich bereits mit dem ein oder anderen freien Programm auskennen, können andere Schulen zum Erfahrungsaustausch einladen oder

So können Sie mitmachen

1. Formular (Biete/Suche)



Formular ausfüllen:

Welche Freie Software nutzen Sie? Wo können Sie helfen? Wo benötigen Sie Hilfe?

2. Hilfe finden & anbieten



Austausch finden & anbieten:

Schauen Sie nach, welche Schule in der Nähe Hilfe anbietet und zu welchen Themen noch Expertise gesucht wird.

3. Informationen



Informationen & Aufklärung:

Hier finden Sie Informationen zu digitaler Bildung und Datenschutz an Schulen.

screenshot Projektseite

ihnen weitere Hilfe anbieten (z.B. bei der Installation der Software). Wer Hilfe sucht, kann sich die passenden Ansprechpartner:innen auf der Webseite heraussuchen und diese direkt kontaktieren – ohne Umwege. Natürlich gibt es auch einen Infobereich, in dem erklärt wird, was Freie Software ist und wofür wir sie an Schulen brauchen.

digitalcourage.de/netzwerk-freie-schulsoftware

Das Netzwerk soll vor allem Schulen anregen, sich untereinander zu helfen,

denn sie wissen am besten „wie der Hase läuft“. Aber natürlich können auch Privatpersonen und Vereine Hilfsangebote eintragen, um Schulen zu unterstützen.

► Und wer auf andere Weise helfen möchte, kann weiterhin fleißig die Digitalcourage-Bildungspakete verteilen, um auf die grundsätzlichen Problematiken hinzuweisen, oder Digitalcourage mit einer Spende unterstützen. Die Vernetzungsarbeit kostet uns viel Mühe und Zeit, aber wir machen weiter, solange unsere Arbeit hilft.

Jessica Wawrzyniak berichtet begeistert:

„Vier Wochen nach Projektstart wurden bundesweit schon 700 Hilfsangebote zu weit über 100 freien Programmen eingetragen, die sich für den Einsatz an Schulen eignen. Und das während der Ferienzeit! Das zeigt: Schulen können auch datenschutzfreundlich. Freie Software bringt Schulen enorme Vorteile, viele Menschen haben das erkannt und sind zudem bereit, anderen zu helfen. Mir persönlich bereitet dieses Projekt große Freude und ich hoffe, dass es sich schnell herumspricht, damit viele Schulen die angebotene Hilfe annehmen.“

Aber neben all der Freude

ist Jessica auch ein wenig verärgert:

„Wir haben trotz begrenzter Mittel und Reichweite in kurzer Zeit so ein großes Hilfsnetzwerk geschaffen. Wieso kom-



Foto: Fabian Kurz, cc by-sa 4.0

men von „oben“, von den Ministerien, keine ähnlichen Projekte? Und wieso müssen Bildungsprojekte immer Millionen kosten, statt erstmal das zu nutzen, was die Schulen sich schon selbst erarbeitet haben? Die Digitalisierung von Schulen könnte schon so viel weiter und besser sein.“

Verbraucherschutz: Digitalcourage ist jetzt Mitglied beim vzbv

Von Rena Tangens und Claudia Fischer

Seit Januar 2021 ist Digitalcourage Mitglied im vzbv, dem Dachverband der 16 Verbraucherzentralen und 28 weiterer verbraucherpolitischer Verbände. Er streitet für starke Verbraucherrechte, faire Märkte sowie unbedenkliche Produkte und Dienstleistungen. Die Einladung, vzbv-Mitglied zu werden, hat uns sehr gefreut – wir fühlen uns geehrt! Wir bringen gerne unsere Kompetenz ein und wollen uns aktiv an Themenfindung und Diskussionen beteiligen.

Wer hätte das gedacht:

Anfang der 2000er-Jahre wurde uns noch vom Wirtschafts-/Verbraucherministerium beschieden, dass Datenschutz mit Verbraucherschutz nichts

zu tun hätte. Seitdem haben wir knapp zwei Dutzend BigBrotherAwards in der Kategorie Verbraucherschutz vergeben. (bigbrotherawards.de)

In einer vernetzten Welt ist Datenschutz der Schlüssel zur Verteidigung unserer Grundrechte. Wer im Internet Waren bestellt oder auch nur betrachtet, mit Karte bezahlt, nach Informationen sucht oder ein Online-Video guckt, hinterlässt eine Datenspur über sein Verhalten, seine Vorlieben, seine Tagesabläufe, biometrische Informationen, Kontakte und vieles mehr. Viele Angebote im Netz und auf dem Smartphone gibt es nur, um „im Nebenbei“ unsere Verhaltensdaten abzugreifen.

All diese Informationen werden gespeichert, kombiniert, ausgewertet und genutzt. Von wem, für welche Zwecke und nach welchen Kriterien – das haben wir nicht mehr in der Hand. Denken wir einfach mal an Versicherungen, Pharmakon-

Foto: unbekannt? xy, cc by 4.0



2015 erhielt Rena Tangens die Auszeichnung „Persönlichkeit des Verbraucherschutzes“ von der Deutschen Stiftung Verbraucherschutz. (► Seite 192)

zerne, PR-Agenturen und Lobbyisten – die sind vielfältig interessiert... Und die Deutungsmacht liegt in den Händen der Digitalkonzerne.

Die Machtasymmetrie zwischen einzelnen Menschen und den weltweit tätigen Digitalkonzernen ist riesig. „Der Kunde ist König“ gilt schon lange nicht mehr. Zumal wir, wenn wir die vorgeblichen Gratis-Angebote im Netz konsumieren, eben keine „Kund.innen“ sind, sondern der Rohstoff für das Geschäftsmodell des ÜberwachungsKapitalismus. (► Seite 40).

Datenschutz ist Verbraucher-schutz. Machen Sie uns stark!

► digitalcourage.de/mitglied

Aufklärung und Information der Verbraucher:innen alleine reichen deshalb nicht – wir brauchen Gesetze, die die Macht der Digitalkonzerne einschränken. Geltendes Recht muss wirksam durchgesetzt werden und alternative Angebote müssen aktiv aufgebaut werden.

Digitalcourage legt viel Energie in Aufklärung, erarbeitet praktische Tipps für die Digitale Selbstverteidigung und tritt deutlich ein für die Rechte der einzelnen Menschen gegenüber den Digitalkonzernen.

Unsere Datenkrake im Haus der Geschichte

Normalerweise begleitet uns unsere kleine Datenkrake (ja, es gibt mehrere Modelle...) auf Demos – 2020/21 haben wir sie aber ans Haus der Geschichte in Stuttgart ausgeliehen. Dort hatte sie eine eigene Vitrine ganz für sich allein – auch mal schön, wenn man sonst mit Demoschildern und anderen Aktionsmaterialien im Keller lebt!

Die Ausstellung hieß „Gier“ und wird mit den Teilen „Hass“ und „Liebe“ 2022 fortgesetzt – das gemeinsame Motto ist „Was uns bewegt“.

Wir haben uns sehr gefreut, dass das Haus der Geschichte auch die Gier nach Daten berücksichtigt hat. Für unsere kleine Krake war das nicht die erste große Fahrt: Wir hatten sie auch



dabei, als wir z. B. 2008 vor dem Bundesverfassungsgericht in Karlsruhe gegen die Vorratsdatenspeicherung protestiert haben.

Aus hygienischen Gründen bargeldlos zahlen?

Ist Quatsch.

Von Kerstin Demuth

Seit den ersten Corona-Tagen werden wir häufig „aus Infektionsschutzgründen“ um bargeldlose Zahlung gebeten. Was aber hat Bargeld mit einer möglichen Ansteckungsgefahr zu tun? Und welche Datenspuren legen wir, wenn wir Kredit- oder EC-Karten benutzen?

1. Kaum Schmierinfektionen nachweisbar

Bislang ist Tröpfcheninfektion über die Atemluft der Hauptinfektionsweg für SARS-CoV-2. Auf Oberflächen überlebt das Virus nur sehr kurze Zeit und die Virenlast ist gering.



2. PIN oder Unterschrift statt Bargeld? Bringt gar nichts.

Ob Sie eine PIN eingeben oder unterschreiben: Auch beim Zahlen mit Plastikkarten kommen Sie mit Oberflächen in Berührung. Tastaturen und Stifte werden in Supermärkten selten desinfiziert. Diese könnten ebenso gut kontaminiert sein wie der Geldscheine, Münzen oder jede Ware im Regal. Das Zahlen mit PIN oder Unterschrift verbindet das Schlechte aus beiden Welten: Sie fassen häufig genutzte Tasten oder Stifte an und hinterlassen eine Datenspur bei

Ihrem Kreditinstitut und in der Ladenkasse.

3. Kontaktlos zahlen? Spart keine Zeit und sicher auch keine Daten.

Nur beim Bezahlen mit dem NFC-Funkchip vermeiden Sie Oberflächen, wenn Sie die PIN dann mit der Ecke der Karte eintippen. Vielleicht verringert sich so auch geringfügig die Zeit, die wir im Supermarkt verbringen und mit anderen die Atemluft teilen. Zeit sparen tut eigentlich nur der Händler, der abends das Geld nicht mehr zählen muss.

Dem steht gegenüber, dass diese Funkchips unsicher sind und digitale Zahlung auf lange Sicht große Risiken birgt. Allein die Standortdaten, die Sie bei der Kartenzahlung hinterlassen, sprechen Bände über Ihr Leben. **Wo** waren Sie **wann** und haben **was** gekauft?

► Lassen Sie sich nicht unter Druck setzen!

Sie sind nicht unsolidarisch, wenn Sie weiter bar bezahlen. Im Gegenteil: Bargeld ist die einzige Möglichkeit, anonym einzukaufen. Das sollten wir nicht leichtfertig aufgeben.

Ein Etappensieg: Schufa zieht Pläne vorerst zurück

Von Claudia Fischer

Foto: Philip Eichler, cc by 4.0



Kalt, aber erfolgreich: Eingepackt in Sandwich-Plakate von Nackedeis haben wir im Februar 2021 zusammen mit Campact vor der Schufa-Zentrale in Wiesbaden protestiert. 380.000 Unterschriften wollten wir übergeben gegen die Pläne der Wirtschaftsauskunftei Schufa, sich mit dem Produkt „CheckNow“ Einsicht in private Kontoauszüge zu verschaffen. Aber die Schufa nahm die Unterschriften zunächst nicht an – angeblich „wegen Corona“. **Wenig später aber zog sie das Projekt „CheckNow“ dann doch zurück** – die kritische Berichterstattung, unsere Aktion gemeinsam mit Campact und die Kritik von Landesdatenschützer:innen hatten also Erfolg.

Was war CheckNow? Menschen, die von der Schufa bisher eine schlechte Bewertung bekommen haben, sollten der Schufa Zugang zu ihren Kontoauszügen gewähren und so ihren Score verbessern können. Natürlich „ganz freiwillig“. Für uns aber fing der Skandal viel früher an: 2001 haben wir der Informa-

Unternehmensberatung GmbH (heute Bertelsmann Arvato Financial Solutions) einen BigBrotherAward für ihr Scoring übergeben.

Scoring ist „vollautomatische Vorurteilsbildung“. Über einen Algorithmus wird die Bonität eines Menschen bewertet und in einem Score-Wert zusammengefasst. Mietvertrag, Bankkredit – vieles gibt es nur mit Scoring-Abfrage. Da Verbraucher:innen nicht erfahren, wie ihr Wert zustande gekommen ist, können sie ihn auch nicht korrigieren. Das bleibt Geschäftsgeheimnis der Auskunfteien. Mehr als ein Girokonto? Mehrfach umgezogen? Schon sehr wenige, banal erscheinende Informationen können zu einem schlechten Score-Wert führen. Bei fast 25 % der Personen beruht die Bewertung auf höchstens drei Informationen, haben Spiegel Online und der Bayerische Rundfunk auf Basis von Daten der Initiative OpenSchufa berichtet.

Einsicht in die Kontoauszüge wäre für die Schufa ein Schatz gewesen. Gehalt, Miete und Konsumgewohnheiten wären automatisch erfasst worden, ebenso die Zahlung an den Psychotherapeuten. **Digitalcourage fordert, dass Scoringunternehmen endlich ihre Formeln für die Scorewerte offenlegen und dass Scoringssysteme gesetzlich verboten werden!**

Nicht jammern – klagen!

Unsere Verfassungsbeschwerden

Von Konstantin Macher

Aufmerksam beobachten wir verschiedene Gesetzgebungsverfahren, in denen es um Freiheit, Datenschutz-, Verbraucher- und Menschenrechte geht. Fällt uns etwas auf, versuchen wir, unsere Sichtweisen in das Verfahren einzubringen und mitzudiskutieren. Aber wenn Sachargumente nicht gehört werden, und wir der Meinung sind, dass ein beschlossenes Gesetz gegen geltendes Recht verstößt, bleibt uns leider manchmal nur noch der Gang zum Bundesverfassungsgericht nach Karlsruhe.

Aktuell haben wir drei Verfassungsbeschwerden eingereicht. In allen Fällen müssen wir einen langen Atem beweisen und begleiten die Themen auch weiter politisch. Dies ist der Sachstand aus dem Herbst 2021:

► **Seit 2016:** **Verfassungsbeschwerde gegen die Vorratsdatenspeicherung**

Aktenzeichen: 1 BvR 141/16, 1 BvR 229/16, 1 BvR 2023/16, 1 BvR 2683/16

Nein, auch 2020 und 2021 hat das Bundesverfassungsgericht – entgegen unserer Hoffnungen im letzten Jahrbuch – nicht über unsere Verfassungsbeschwerde entschieden. Aber inzwischen wird gegen den Überwachungs-

zombie „Vorratsdatenspeicherung“ auf vielen Ebenen geklagt. Das Bundesverfassungsgericht (BVerfG) wartet anscheinend eine Entscheidung des Europäischen Gerichtshofes (EuGH) in ähnlicher Beschwerde ab. Bis dieser sein Urteil verkündet, können nach Redaktionsschluss dieses Jahrbuches noch einige Monate vergehen.

Darin sehen wir aber auch eine Chance: Der EuGH könnte der Vorratsdatenspeicherung nämlich europaweit einen Riegel verschieben. Wenn das Gericht aber dem zunehmenden politischen Druck der Mitgliedsstaaten nachgibt, dann wird unsere Verfassungsbeschwerde umso wichtiger.

Unterstützen Sie uns mit Ihrer Unterschrift:

aktion.digitalcourage.de/weg-mit-vds

Mehr zur Vorratsdatenspeicherung finden Sie auf Seite 34.

► **Seit August 2018: Verfassungsbeschwerde gegen Staatstrojaner**

Aktenzeichen: 2 BvR 897/18, 2 BvR 1797/18, 2 BvR 1838/18, 2 BvR 1850/18, 2 BvR 2061/18

Der Einsatz von Staatstrojanern ist ein unverhältnismäßiger Eingriff in unsere

Foto: Mischä Burmester, cc by 4.0



Kerstin Demuth, Jan Roggenkamp und padelun auf dem Platz der Menschenrechte in Karlsruhe. Sie haben eben die Verfassungsbeschwerde gegen das Polizeigesetz NRW beim Bundesverfassungsgericht eingereicht.

Grundrechte. Und die Erfahrung der letzten Jahre zeigt, dass keine ordentliche demokratische Kontrolle stattfindet (z. B. durch das Parlament). In einem Urteil vom Juli 2021 (1 BvR 2771/18) hat das Bundesverfassungsgericht klargestellt, dass die Nutzung geheim gehaltener Sicherheitslücken für Staatstrojaner ein Sicherheitsrisiko darstellt und es eine konkrete staatliche Schutzpflicht gibt. Das stimmt uns optimistisch, denn das gehört zu den Punkten, die wir in unserer Verfassungsbeschwerde angreifen.

Staatliche Behörden sollten sich nicht länger am kommerziellen Markt für Sicherheitslücken beteiligen, z. B. durch

den Erwerb der Pegasus-Staatstrojaner für BKA und BND, und damit Bürger:innen und Unternehmen gefährden. Stattdessen kämen die Behörden ihrer staatlichen Schutzpflicht nach, wenn sie ihnen bekannte Sicherheitslücken an die Hersteller melden müssten, damit diese geschlossen werden.

Aber nein: Im Sommer 2021 hat die große Koalition die Überwachung durch Staatstrojaner sogar noch ausgeweitet. Wir hoffen, dass das BVerfG in unserer Verfassungsbeschwerde die neuen Verschärfungen dann gleich mitberücksichtigt – und kippt.

Unterstützen Sie uns mit Ihrer Unterschrift:

aktion.digitalcourage.de/

[kein-staatstrojaner](https://aktion.digitalcourage.de/kein-staatstrojaner)

► Seit Oktober 2019: Verfassungsbeschwerde gegen die Telekommunikationsüberwachung im Polizeigesetz NRW

Aktenzeichen: 1 BvR 2466/19

Wir warten auf eine Entscheidung. In der Zwischenzeit unterstützen wir Proteste gegen Bemühungen der NRW-Landesregierung (CDU/FDP), auch noch das Versammlungsgesetz in NRW bis zur Verfassungswidrigkeit hin zu verschärfen und der Polizei z. B. umfassende Rechte auf Videoüberwachung von Demonstrationen einzuräumen. (► Seite 60)

Unterstützen Sie uns mit Ihrer Unterschrift:

aktion.digitalcourage.de/polg-nrw

Warum der Kinderschutz nichts mit Vorratsdatenspeicherung zu tun hat

Von Friedemann Ebel

Diesen Text haben wir im Sommer 2020 veröffentlicht. Da die Koalitionsverhandlungen der neuen Bundesregierung auch wieder Vorratsdatenspeicherung mit Verbrechensbekämpfung gleichsetzen, drucken wir ihn hier noch einmal ab: **Überwachung verhindert keine Verbrechen!**

Wir vermeiden nach Möglichkeit die Begriffe „Missbrauch“ oder „Kinderpornografie“, weil diese Wortwahl nicht angemessen für Gewalttaten ist. Hier tauchen die Worte trotzdem auf, weil es sich um Zitate aus dem Bericht des NRW-Innenministeriums handelt.

Drei der größten aktuell diskutierten Netzwerke zur sexualisierten Gewalt gegen Kinder wurden in Nordrhein-Westfalen aufgedeckt: Lügde, Münster und Bergisch Gladbach. Nach den Ermittlungspannen in Lügde hat NRW-Innenminister Herbert Reul das Personal bei Polizei und Staatsanwaltschaften dafür mehr als verdoppelt. Im Sommer 2020 legte das Innenministerium NRW einen Bericht vor (verlinkt über die Jahrbuch-Webseite), der auflistete, was gegen sexualisierte Gewalt an Kindern getan werden muss. **Überraschung:** Anlasslose Vorratsdatenspeicherung ist dafür nicht nötig.

Stattdessen wird als Grund für die Ermittlungserfolge in NRW die „Ausrichtung der NRW-Polizei auf den kriminalpolitischen und kriminalstrategischen Schwerpunkt ‚Bekämpfung des sexuellen Missbrauchs/der Kinderpornografie‘“ benannt, also das, was Beratungsstellen und Fachleute schon seit langem fordern: Die Ermittlungsbehörden müssen das Thema endlich ernst nehmen und gut ausgestattet werden. Nur so kann sexualisierte Gewalt gegen Kinder beendet werden. Der Bericht benennt Schwachstellen, erreichte Verbesserungen und weiteres Handlungspotenzial für diese Ermittlungen:

- ▶ Ein Problem sei die „vergleichbar nur **geringe Anzeigebereitschaft bei sexuellem Missbrauch**“.
- ▶ Aufgrund von „**exponentiell steigenden Datenmengen** (Massendaten) im Deliktsbereich“ ist eine computergestützte „Auswertung von Darstellungen des sexuellen Missbrauchs von Kindern“ notwendig.
- ▶ Die Stabsstelle hat festgestellt, dass „die NRW-Polizei über **keine leistungsfähige und landesweite Auswertefrastruktur** verfügt“, woraufhin entsprechende Verbesserungen beschlossen wurden.

Illustration: Isabel Wienold, cc by 4.0



Die Polizei muss für ihre Arbeit gut ausgestattet werden.

- ▶ **Hoch problematisch sind Bearbeitungsrückstände** von Fällen: „Zum Stichtag 31.03.2019 ... in den Kreispolizeibehörden ... 557 nicht vollstreckte Durchsuchungsbeschlüsse, davon 85 älter als drei Monate“ (Anmerkung von Digitalcourage: Der 31.3.2019 war zu Beginn der Ermittlungen in Lügde. Der Missbrauchsskandal in Bergisch Gladbach wurde erst im November 2019 aufgedeckt, der in Münster erst 2020. Die Zahlen dürften heute also deutlich höher sein.)
- ▶ Der Bericht bemängelt eine „**grundsätzlich defizitäre Personalsituation**“ und erläutert, in welchem Rahmen bereits Personal aufgestockt wurde.
- ▶ Mangelhaft ist ebenso: „in Teilen zu **wenig Betreuungs- und Begleitungsangebote** (z. B. Supervision)“, die „**defizitären Raumsituationen** sowie **unzureichende Technik**.“
- ▶ **Die polizeilichen Kapazitäten bewertet der Bericht als unzureichend:** Die Folge von Personal- und

Sachmittelknappheit ist, „dass die seit Jahren zunehmende Anzahl an Verfahren und insbesondere exponentiell zunehmenden Datenmengen

zu deutlich verlängerten Verfahrenslaufzeiten führen und damit das möglichst frühzeitige Erkennen von ggf. anhaltenden Missbrauchstaten und deren Beendigung erschweren. Das ist aus Opfersicht und unter fachlichen Gesichtspunkten nicht hinnehmbar.“

- ▶ **Hinweistelefon:** „Das LKA NRW ist beauftragt, ein Konzept für eine ergänzende zentrale Anzeigenaufnahme in Fällen von sexuellem Missbrauch/ Kinderpornografie über eine zentrale Rufnummer („Hinweistelefon“) vorzulegen.“
- ▶ „In Verfahren wegen Kinderpornografie treten **zunehmend Kinder und im besonderen Maße Jugendliche als Täterinnen und Täter** in Erscheinung.
- ▶ **Welche Rolle spielt die Vorratsdatenspeicherung?**

Am Ende des Berichtes waren wir erstaunt: Es hängt ein Absatz über Vorratsdatenspeicherung hinter den Ermittlungserfahrungen, der wenig Zusammenhang zum vorherigen Teil hat, was z. B. den Zeitraum des Zahlenmaterials angeht. Es wirkt, als wäre er wie ein Textbaustein eingeschoben worden. Zum Beispiel bezieht er sich nicht auf



Foto: Felix Kindermann, cc by 4.0

konkrete Erfahrungen bei der Ermittlungsarbeit, sondern fußt lediglich auf einer Zahl des Bundeskriminalamtes von 2017.

„Dazu hat das BKA veröffentlicht, dass alleine im Jahr 2017 insgesamt 8.400 Verdachtshinweise von NCMEC ‚National Center for Missing & Exploited Children‘ nicht aufgeklärt werden konnten, da die jeweiligen deutschen IP-Adressen mangels Umsetzung der Vorratsdatenspeicherung keinen konkreten Personen mehr zugeordnet werden konnten.“

Es folgt ein Fazit des NRW-Berichtes, das diesen Absatz nicht weiter beachtet, sondern sich nur auf die vorherigen Ermittlungserfahrungen bezieht. Für uns ist das ein weiteres Indiz dafür, dass dieser Absatz eher eingeschoben wurde und nicht zur Kernaussage des Berichtes gehört.

Die 8.400 nicht aufklärbaren Ermittlungsverfahren werden immer wieder in Podiumsdiskussionen und Texten des BKA angeführt. Dabei bleibt vieles unklar:

- ▶ Es wird nicht erläutert, wie viele dieser 8.400 Verdachtshinweise auf Grund von mangelnden personellen und

Zusammen mit Campact, der Digitalen Gesellschaft und dem AK Vorrat haben wir 100.000 Unterschriften an Mitglieder des Europarlaments übergeben.

technischen Ressourcen nicht weiter verfolgt werden konnten.

- ▶ Es ist unklar, auf wie viele und auf welche Art von Fällen sich die Hinweise beziehen und wie viele seit 2017 später ermittelt werden konnten.
- ▶ Es wird nicht darüber aufgeklärt, dass IP-Adressen in vielen Fällen gar keine Rückschlüsse auf konkrete Personen erlauben.
- ▶ Es liegen keine Informationen darüber vor, ob in allen 8.400 Fällen alle möglichen Ermittlungswege systematisch ausgenutzt wurden.
- ▶ Es wird nicht erklärt, wie viele dieser 8.400 Verdachtshinweise mit Hilfe eines Quick-Freeze-Verfahrens (siehe Jahrbuch-Webseite) hätten aufgeklärt werden können.

Stattdessen heißt es im Bericht:

„Das Innenministerium NRW sieht die derzeit nicht umgesetzte gesetzliche Pflicht zur Vorratsdatenspeicherung vorrangig in Fällen von Kinderpornografie und Rechtsextremismus als höchst problematisch an.“

Diese Aussage lässt sich nicht aus dem vorherigen Erfahrungsbericht in NRW herleiten oder begründen. Vorratsdatenspeicherung ist anlasslose Massenüberwachung aller Menschen in Deutschland. Dadurch wird kein Kind geschützt.

► Was wirksam wäre

Folgende wirksame und rechtsstaatlich vertretbare Kinderschutz-Maßnahmen listet der Bericht auf:

- Maßnahmen zur „Prävention, zum Schutz vor und Hilfe bei sexualisierter Gewalt gegen Kinder und Jugendliche“
- Mehr Personal
- Verbesserung der Arbeitsbedingungen für Ermittler:innen: psychologische Betreuung, Supervision, Erschwerniszulagen
- Optimierung der technischen Auswertung von Audio/Videomaterial
- Optimierung von Prozessabläufen
- Weiterbildung und Unterstützung von damit befassten Personen (u.a. technische Ermittlungsberatung, IT-fachliche Beratung, Förderung von Kompetenzen zur Sicherung und Aufbereitung von IT-Daten, zur Auswertung von IT-Daten, zur Anhörung von Kindern, zu Supervision, zur Auswertung von IT-Massendaten etc.)
- Fortbildungskapazitäten massiv ausbauen
- „Konzentration von spezialisierten Ermittlungskräften über die Behörden Grenzen hinaus“
- Abbau offener Durchsuchungsbeschlüsse (Stand in NRW im März 2020: 540 offene Durchsuchungsbeschlüsse)

- Standards/Handlungsleitlinien (Kinderanhörungszimmer)
- verbesserte Anzeigenaufnahme (Not-Telefon-Nummer)
- verbesserte Zusammenarbeit mit Jugendämtern, Schulen, Kindergärten etc. („Förderung des Informationsaustausches und Stärkung eines gemeinsamen Verständnisses und Vorgehens zum Schutz von Kindern und Jugendlichen vor (sexueller) Gewalt“; „Mechanismen zum frühzeitigen Erkennen der Taten und die Weitergabe der Informationen“)

► Unser Fazit

Der Bericht liefert genug Ansätze, wie die Polizei dabei unterstützt werden kann, Kinder zu schützen und Verbrechen gegen Kinder aufzuklären. Vorratsdatenspeicherung gehört nicht dazu.

Politiker:innen und alle anderen, die anlasslose Vorratsdatenspeicherung zur Strafverfolgung bei sexualisierter Gewalt fordern, sollten umdenken und sich mit diesem Erfahrungsbericht der Ermittler:innen in NRW auseinandersetzen. Es gibt eine Menge zu tun – die Vorratsdatenspeicherung löst keines der aufgezeigten Probleme.

Im Gegenteil: **Die ewige Wiederholung der Forderung nach Vorratsdatenspeicherung lenkt ab davon, wirklich wirksame Maßnahmen zum Kinderschutz in Angriff zu nehmen.**

FEB MÄRZ 2022 JUNI

MONTAG
DIENST
MITTWA
D
F
S
S
↑
L
€
MITTWOCH
DONNERSTAG
FREITAG
SAMST
SONNT
MONT
DIENST
MITT
DONN
FREIT
SAMST
SONNT
MONTAG
DIENSTAG



Zensus 2022

2022 findet in Deutschland wieder ein Zensus statt. Mit dieser statistischen Erhebung wird ermittelt, wie viele Menschen in Deutschland leben, wie sie wohnen.

Viele politische Entscheidungen beruhen auf Bevölkerungs- und Wohnungszahlen. In früheren Volkszählungen waren noch Zähler von Haus zu

Haus mit Fragebögen unterwegs. In Deutschland ist der Zensus 2022 eine registergestützte Bevölkerungszählung, die durch eine Stichprobe ergänzt und mit einer Gebäude- und Wohnungszählung kombiniert wird. Informationen dazu auf zensus2022.de.

Siehe Seite 162



To Do

- Firmenfeier nächste Woche:
- Buttons bestellen
- photos ok / no photos
-
- shop.digitalcourage.de
-



GUTE LAUNE-TIPP:
DIE DATENSCHUTZ-KARIKATUREN
VON CHRISTIANE PFOHLMANN!
(PFOHLMANN.DE)
UND NICHT VERGESSEN:
LUCA-APP LÖSCHEN!

AUG Wandplaner 2022 bestellen: shop.digitalcourage.de

NOV

1
2 31

1

DEZ 2023



Sensible Fracht: Christian holt den neuen Digitalcourage-Server mit dem Lastenrad ab.



MAN SIEHT NUR MIT DEM HERZEN GUT.
DAS WESENTLICHE IST FÜR DAS DIGITALE UNSICHTBAR.

Digital Markets Act

Europas historische Chance gegen Internetgiganten

Von Rena Tangens und Andrea Neunzig

Die Macht der großen Internetmonopolisten (Google, Amazon, Facebook & Co.) gefährdet unsere Demokratie. Sie muss beschränkt und Wettbewerb wieder ermöglicht werden. Das fordert Digitalcourage seit langem.

Die Erkenntnis ist offenbar auch in anderen Kreisen angekommen. So auch bei Andreas Schwab (CDU), dem Berichterstatter im Europäischen Parlament für den Digital Markets Act.

Er sagt: „Die Vermachtung von Wirtschaft führt am Ende politisch zu sehr negativen Auswirkungen.“ Und begründet

damit, warum es harter regulativer Interventionen bedarf. Nun haben wir in Europa endlich die Chance dazu, denn die EU-Kommission hat im Dezember 2020 einen ambitionierten Gesetzentwurf auf den Weg gebracht: den „Digital Markets Act“, kurz DMA.

Die Regulierungen des DMA zielen auf die sogenannten „Gatekeeper“. Das sind diejenigen Plattformen, die als „Torwächter“ den Zugang zu digitalen Märkten beherrschen und die Regeln auf diesen Märkten diktieren. Wird

eine Internetplattform als Gatekeeper eingestuft, gelten für sie die im DMA genannten verbindlichen Regeln (Ge- und Verbote).

Der Entwurf der EU-Kommission muss noch mit dem EU-Parlament und dem Rat der Europäischen Union abgestimmt werden. In den sogenannten Trilog-Verhandlungen bringen Parlament und Rat Änderungen über sogenannte Berichterstatter ein. Die Verhandlungen

dazu sind im vollen Gange. Auf Hochtouren läuft auch die Lobbyarbeit der betroffenen großen Konzerne, die mit allen

Mitteln versuchen, die Gesetzgebung zu verhindern oder abzuschwächen und damit wirkungslos zu machen.

Aber auch Digitalcourage hat sich frühzeitig in die Verhandlungen eingebracht:

► Wir haben gemeinsam mit Lobbycontrol im Mai 2021 einen Brief an EU-Abgeordnete geschickt, in dem wir den Vorschlag begrüßen, Verhaltensregeln für große Internetmonopolisten einzuführen. Gleichzeitig zeigen wir, wo wir Umsetzungsprobleme sehen und fordern dringend Nachbesser-

► „Die Vermachtung von Wirtschaft führt am Ende politisch zu sehr negativen Auswirkungen.“ ◀

Foto: Jan Schötteldreier, cc by 4.0



Im Sommer 2021 hat uns Alexandra Geese, MdEP für Bündnis 90/Die Grünen, in Bielefeld besucht. Sie ist Verbraucherschutz-Politikerin auf Europa-Ebene.

rungen. Dieser Brief wurde sehr gut aufgenommen.

- ▶ Wir haben direkte Gespräche mit EU-Abgeordneten und Berichterstattern geführt.
- ▶ Zusammen mit 27 NGOs haben wir einen zivilgesellschaftlichen Aufruf verfasst und strukturelle Maßnahmen gefordert, die deutlich über die Verhaltensvorgaben im bisherigen Entwurf des DMA hinausgehen: Wir fordern rechtliche Mittel zur Fusionskontrolle und Entflechtung der großen Unternehmen.

Digitalcourage stellt zwei zentrale Forderungen auf, die im Digital Markets Act verankert werden sollen:

1. Verbot von personalisierter Werbung insgesamt.

Denn personalisierte Werbung ist die Ursache vielen Übels: Sie erfordert die Dauerüberwachung der Nutzer:innen und Profilbildung, verteilt detaillierte persönliche Daten der Nutzer:innen bei Online-Auktionen um Werbeplätze wahllos weiter an alle, die behaupten, Werbung schalten zu wollen, und ermöglicht gezielte manipulative Beeinflussung (▶ Seite 98). Mittlerweile ist klar: Das Konzept personalisierter Werbung (wir könnten sie treffender auch „überwachungsbasierte Werbung“ nennen) hat sehr negative Auswirkungen auf Wirtschaft und Gesellschaft. Deshalb sollte personalisierte Werbung verboten werden.

Dafür fordern wir konkret das Verbot der Zusammenführung von personenbezieharen Daten zu Werbezwecken oder zur Profilbildung in Artikel 5a des DMA.

Oft wird bisher die Zustimmung der Nutzer:innen zu dieser Datenverarbeitung mit unlauteren Mitteln (Dark Patterns) erschlichen. Diese Hintertür muss geschlossen werden.

2. Verbot von Dark Patterns im DMA

„Dark Patterns“ (dunkle Muster) sind unfaire und manipulative Benutzungsoberflächen, mit denen Verbraucher.

innen zu Entscheidungen gedrängt werden, die nicht ihrem wahren Willen entsprechen. Bekanntestes Beispiel für Dark Patterns sind die derzeit genutzten Cookie-Banner, die uns dazu verleiten wollen, „freiwillig“ dem Tracking und der Weitergabe unserer persönlichen Daten zuzustimmen. (► Seite 97)

Dark Patterns müssen im Digital Markets Act explizit verboten werden. Denn ansonsten könnten Gatekeeper die Entscheidungen der Verbraucher:innen durch manipulative Methoden lenken und damit wichtige Verpflichtungen nach Art. 5 und 6 des DMA aushebeln und umgehen.



Foto: Ingo Jürgensmann, cc by 4.0

Dark Patterns kommen nicht nur im Zusammenhang mit personalisierter Werbung zum Einsatz, sondern sie erschleichen die Zustimmung, mit der Nutzer:innen ihre Rechte aufgeben, zum Beispiel das Recht vorinstallierte Software von ihrem eigenen Gerät zu entfernen (Art. 6b) und nicht künstlich in einem Dienst eingeschlossen zu werden (technischer Lock-In, Art. 6e).

► **Wir fordern, dass Dark Patterns explizit gesetzlich verboten werden – stattdessen brauchen wir eine Pflicht zu fairem Design.**

Beim Digital Markets Act ist viel in Bewegung – wir bleiben dran!

Warum Werbettracking schädlich und gefährlich ist

Bei unserer Kritik des Werbetrackings und der personalisierten Werbung geht es uns keineswegs nur um Datenschutz, sondern um die vielfältigen schädlichen Auswirkungen auf Wirtschaft, Gesellschaft und letztendlich die Demokratie.

Die Werbewirtschaft setzt personalisierte Werbung ein, weil Anbieter von Produkten und Dienstleistungen das angeblich so wollen. Aber tatsächlich schadet das Modell auch der Wirtschaft.

Personalisierte Werbung setzt Tracking (also Verfolgung, Überwachung, Profilerstellung) der Nutzer:innen voraus. Alle Konzerne, die dem Geschäftsmodell „pseudo-gratis gegen Verhaltensüberwachung“ folgen, bedienen sich an den

Informationen über unsere Verhaltensweisen, Vorlieben und Eigenarten, als ob sie herren-

loses Gut wären, das sie sich einfach aneignen können. Die Ausforschung und Verfolgung, sprich: Überwachung der Netznutzer:innen zur Profitmaximierung wird immer lückenloser und detaillierter. Shoshana Zuboff nennt dieses Wirtschaftsmodell „Überwachungskapitalismus“.

Werbung im Internet ist ein hoch konzentrierter Markt. Einige wenige de facto Monopole wie Google, Facebook und inzwischen auch Amazon kontrollieren den Werbemarkt mit personalisierter Werbung. Insbesondere der Zugriff auf Nutzer:innen-Daten führt zu einer massiven Wettbewerbsverzerrung zu Gunsten der großen Plattformen, weil sie aus vielen eigenen Quellen Informationen über die Nutzer:innen sammeln. Dies geht zu Lasten aller anderen Unternehmen.

Inhalte im Netz sollen durch Werbung finanziert werden. Doch vom Werbekuchen bleibt immer weniger zur Finanzierung übrig. Während die Werbeausgaben von Firmen im Internet erheblich steigen,



sinken die Einnahmen bei Medien und Kreativen. (Grafik ► Seite 101) Wo bleibt dieses

Geld? Inzwischen kommen die Werbe-Einnahmen überwiegend nicht mehr bei den Inhaltelieferanten (Verleger, Journalistinnen, Rechercheure, Fotografinnen etc.) an, sondern bleiben zu 50-70% bei den Werbeplattformen, Targeting-Profil-datenbanken etc. hängen.

Intransparenz für die Werbetreibenden: Plattformen agieren undurchsichtig. Werbetreibende Firmen können kaum noch überprüfen, ob und welche Werbung von ihnen wo tatsächlich geschaltet ist und welche wie wirksam ist.

Betrug und Manipulation: Große Firmen sehen sich deshalb inzwischen zu umfangreichen Kontrollmaßnahmen genötigt. Doch insbesondere kleine und mittlere Unternehmen können sich das nicht leisten und werden zunehmend durch betrügerische Werbepraktiken ausgetrickst.

Die Wirtschaft leidet unter diesen Praktiken: Der Wettbewerb bleibt auf der Strecke. Monopole, Intransparenz und Betrug behindern Wachstumspotentiale der digitalen Wirtschaft.



Der Werbekuchen – Die Plattformen haben ihn unter sich aufgeteilt...

Dieses Werbemodell schadet nicht nur anderen Marktteilnehmer:innen, sondern es hat auch enorm gefährliche Auswirkungen auf die Gesellschaft.

Manipulation und Desinformation: Die detaillierten Profile der Netznutzer:innen werden für politisches Microtargeting genutzt. Parteien und Wirtschaft, Lobbyisten und PR-Firmen, ausländische Geheimdienste und Kriminelle können diese Informationen ausnutzen, um Menschen gezielt zu beeinflussen. Es geht also keineswegs nur um Werbung im engeren Sinne, sondern auch um das Nutzen von psychologischen Analysen, um Desinformation zu verbreiten.

Kampf um Zeit und Aufmerksamkeit: Um attraktiv für Werbekunden zu sein, versuchen Plattformen, Nutzer:innen dazu zu bringen, dass sie möglichst viel Zeit auf ihrer Plattform verbringen. Dazu spielen die Plattform-Algorithmen gezielt emotionale, kontroverse



... und für die, die spannende Inhalte ins Netz liefern, bleiben nur die Krümel.

und immer radikalere Inhalte zu. Dieses Ausnutzen von Emotionen wie Empörung, Scha-

denfreude und Hass, um Menschen zu fesseln, führt zu einer Verzerrung der Weltwahrnehmung und zu einer gefährlichen Polarisierung der Gesellschaft.

Verlust der selbstbestimmten Zukunft:

Die gesammelten Nutzer:innen-Daten werden nicht nur für personalisierte Werbung verwendet, sondern auch für Verhaltensprognosen, die großen Einfluss auf unsere Zukunftsgestaltung haben.

Es gibt eine Lösung: Eine bessere Alternative wäre **kontextabhängige Werbung**, also Werbung passend zum redaktionellen Umfeld. Denn diese braucht die Nutzer:innen nicht auszuforschen und zu tracken. Und sie nützt

auch den Medien, die den Werbepplatz anbieten, weil sie nicht mehr für die Tracking- und Profilingdienste bezahlen müssen. So bleibt mehr vom Werbekuchen bei ihnen hängen.



Lobbyismus live:

Mit Facebook gegen Überwachung?!

Von Claudia Fischer

Dinge gibt's, die gibt's gar nicht. Wie diese Mail an Rena Tangens im Mai 2021, in der ein Facebook-Lobbyist um Kontaktaufnahme bittet. Weil Facebook gerne mit uns gemeinsam gegen Überwachung protestieren möchte. Gegen **staatliche** Überwachung. Um es genau zu sagen: Gegen das geplante „Gesetz zur Anpassung des Verfassungsschutzrechts“. Da würde nämlich die verschlüsselte Kommunikation bedroht. Und das macht Facebook Sorgen. Sieh an. Deshalb würde man gerne einen Brief dagegen an Bundestagsabgeordnete schreiben. Ob wir da nicht mitzeichnen wollen.

► **Nö, Facebook, wollen wir nicht. Nicht mit Euch.** Die Gründe könnt Ihr auf digitalcourage.de oder bigbrotherawards.de nachlesen.

Spaß beiseite: Eigentlich ist diese Mail eine ernste Sache.

Klar setzt sich Digitalcourage gegen staatliche Überwachung von Messengern und für Verschlüsselung ein. Hey – wir haben schon für Verschlüsselung gekämpft, da gab es weder Google noch Facebook. Wir haben 1990 in der Zerberus-MailBox-Software verschlüsselte Postfächer eingeführt, so dass auch wir Systembetreiber die Post nicht mitlesen konnten. Wir haben 1993 das erste

deutsche Handbuch für das Verschlüsselungsprogramm PGP herausgegeben und 12.000 Exemplare unter die Leute gebracht.

Internet-Konzerne geben sich gerne als Freiheitskämpfer, die unsere Privatsphäre, die freie Meinungsäußerung und das Internet an sich verteidigen. Das tun sie aber nur, wenn es sich gegen staatliche Maßnahmen richtet. Ihre eigene, wesentlich umfassendere Nutzerüberwachung ist zentraler Bestandteil ihres Geschäftsmodells und wird nicht thematisiert. Perfide, wie Facebook mit dieser Mail Organisationen der Zivilgesellschaft (NGOs) für seine PR einspannen will.

Unter der Mail hat Facebook den Chaos Computer Club (CCC), Netzwerk Recherche, Reporter ohne Grenzen, Digitale Gesellschaft etc. so geschickt als Quellen platziert, dass man denken könnte, dass die bereits Kooperationspartner dieser Aktion wären. Wir warnen deshalb:

NGOs aufgepasst – lasst euch nicht für Facebooks Greenwashing einspannen!

Update: Die Digitale Gesellschaft hat die Unterschrift ebenso klar abgelehnt wie wir. Die Stiftung Neue Verantwortung und der CCC haben den Facebook-Brief mit unterschrieben.

Unterschreiben gegen Gesichtserkennung

Von Konstantin Macher

Die Uhr tickt: Bis zum 1. August 2022 sammeln wir Unterschriften in ganz Europa, weil wir im Bündnis mit vielen anderen Grundrechtsgruppen biometrische Massenüberwachung verhindern wollen. Unter dem Motto #ReclaimYourFace („Hol Dir Dein Gesicht zurück“) geht es darum, Technologien wie die biometrische Gesichtserkennung in Europa zu verbieten.



Im Sommer 2021 hat Konstantin Macher für Digitalcourage und das ReclaimYourFace-Bündnis bei der „unteilbar“-Demonstration in Berlin erklärt, worum es dabei geht (Alle Hintergründe verlinken wir über die Jahrbuch-Webseite):

„**H**allo, ich bin Konstantin von Digitalcourage und dem Bündnis **#ReclaimYourFace**. Wir setzen uns für **ein europaweites Verbot biometrischer Massenüberwachung** ein und ich will kurz erklären, was das bedeutet und wie jede und jeder von euch hier mithelfen kann. Denn wir brauchen dabei eure Unterstützung!

*Vielleicht kennt ihr noch das Projekt zur automatisierten Gesichtserkennung am Bahnhof Südkreuz in Berlin. Da zeichnet eine Kamera dein Gesicht auf, wenn du durch den Bahnhof gehst, sei es morgens auf dem Weg zur Arbeit oder wenn du, so wie ich, nach Berlin kommst, um an einer Demo teilzunehmen. **Das System macht dann aus deinem Gesicht kontinuierlich einen Datensatz** und versucht damit festzustellen, ob die Polizei gerade nach dir fahndet. Andere Systeme versuchen zu bewerten, ob du dich gerade auffällig verhältst und ob du vielleicht doch kriminell bist.*

*Das ist nicht nur mega creepy, es ist auch **ein Eingriff in unsere Grundrechte**. Wir werden unter Generalverdacht gestellt und selbst wenn wir unschuldige Leute sind, kann uns das System plötzlich als Verbrecher.in bewerten. Denn solche Systeme sind fehleranfällig, und so war das auch am Südkreuz.*

Insbesondere, wenn du nicht weiß und männlich bist, dann ist so ein System fehleranfällig. Diese vermeintlich „intelligenten“ Systeme sind nämlich meist trainiert mit Daten aus einem verzerrten Bild einer weißen Mehrheitsgesellschaft und reproduzieren dann diesen Rassismus in der Technik.

Leider werden solche biometrischen Systeme zur Massenüberwachung immer mehr eingesetzt, und wir bei **#ReclaimYourFace** wollen dem etwas entgegenstellen. Jede.r einzelne hier kann dabei helfen. Wir nutzen das Werkzeug einer Europäischen Bürger.inneninitiative (EBI), um unser Anliegen von der Straße in die Politik zu tragen. Wenn wir Erfolg haben, muss die EU-Kommission uns zuhören und ist gezwungen, sich mit unserer Forderung auseinanderzusetzen.

Auf dem Weg dorthin versuchen wir der Politik immer wieder, dass **wir uns unteilbar für unser aller Grundrechte einsetzen**. Egal, ob ein biometrisches Überwachungssystem gegen Sportfans im Stadion eingesetzt wird, gegen Studierende bei der Prüfung am Rechner (► Seite 79) oder gegen Geflüchtete an den EU-Außengrenzen, um ihnen ihr Recht auf Schutz zu verwehren:

Solche Systeme schaffen keine Sicherheit. Stattdessen wird ein Gefühl der kontinuierlichen Unsicherheit konst-



Foto: Sebastian Marg (e-punc) cc by 4.0

Konstantin Macher (rechts) auf der #unteilbar-Demo in Berlin 2021

ruiert. Wenn ich weiß, dass so ein biometrisches System mich die ganze Zeit bewertet, nach meinem Aussehen und meiner Gangart, oder wenn es jede plötzliche Bewegung als ein Indiz für eine Gefährdung ansieht, dann kann es sein, dass ich mein Verhalten anpasse (► Seite 165). Vielleicht versuche ich möglichst „normal“ zu handeln beziehungsweise so, dass mich das System für normal hält. Oder ich meide dann diese Orte, gehe nicht mehr zur Demo und werde aus dem öffentlichen Raum verdrängt.

► **Wir stellen uns dem entschieden entgegen!**

Wir fordern mit dem Bündnis **#ReclaimYourFace** ein Verbot biometrischer Massenüberwachung und ich hoffe, ihr **unterstützt uns dabei**, indem ihr online auf ReclaimYourFace.eu/de unterschreibt. Gemeinsam können wir das schaffen. Danke!“

Worum geht es bei einer Europäischen Bürger.inneninitiative (EBI)?

Eine EBI ist das einzige offiziell anerkannte Verfahren, mit dem EU-Bürger.innen und Bürger die EU-Kommission zwingen können, sich mit einem Thema zu befassen, das sie bewegt. Um eine EBI zu starten, müssen sich viele Menschen aus der ganzen EU zusammentun und gemeinsam ein neues Gesetz vorschlagen. „Viele“ heißt in diesem Fall: mehr als eine Million.

Unsere EBI für ein Verbot der massenhaften biometrischen Gesichtserkennung wurde Anfang 2021 zugelassen. Jetzt gilt's: **Bis Sommer 2022 müssen wir mindestens eine Million Unterschriften von EU-Bürger.innen sammeln.** Außerdem brauchen wir **eine Mindestanzahl an Stimmen in mindestens sieben Mitgliedsstaaten der EU.** Auf der Jahrbuch-Webseite verlinken wir eine ständig aktualisierte Übersicht, wie weit wir sind.

Wenn unsere EBI Erfolg hat,

- ▶ muss sich die **Europäische Kommission mit uns treffen** und den Vorschlag diskutieren.
- ▶ muss die Kommission eine „Kommunikation“ (ein offizielles politisches Instrument) verabschieden, in der sie erklärt, welche Maßnahmen sie ergreift (oder sein lässt).
- ▶ kann das Europa-Parlament das Thema auf die Tagesordnung setzen, darüber diskutieren und eine eigene Antwort vorschlagen.

Bisher haben erst sechs EBIs die Grenze von einer Million Unterschriften überschritten. Manche davon haben greifbare Änderungen an EU-Gesetzen erreicht.

Bei #ReclaimYourFace gibt es eine besondere Herausforderung für das Erreichen unseres Ziels: **Wir verzichten ganz bewusst auf personalisierte Werbung in sozialen Medien.** Daher ist es für uns besonders schwer, die nötigen Stimmen zu sammeln – und **darum sind wir umso mehr auf unsere Unterstützer.innen angewiesen,** die unterschreiben und es weitersagen. Besonders helfen Sie mit, wenn Sie Freund.innen und Bekannte in anderen EU-Ländern auf #ReclaimYourFace aufmerksam machen, damit auch dort die notwendigen Stimmen zusammenkommen. Auf ReclaimYourFace.eu sind die Informationen in 15 Sprachen verfügbar.

Darüber hinaus können viele Unterschriften in einem einzigen Land auch dafür sorgen, dass einzelne Regierungen Dinge tun, um Menschen vor biometrischer Massenüberwachung zu schützen. Es gibt also viele Wege, wie Ihre Unterschrift ganz viel bewirken kann.

- ▶ **Die EBI kann online und auf Papier unterschrieben werden. Alle nötigen Informationen, auch zum Datenschutz bei dieser Unterschriftensammlung, gibt es auf ReclaimYourFace.eu/de.**

Warum Digitalcourage?

Foto: Fabian Kurz, cc by 4.0



Luisa Baltik verbucht unsere Spenden und bearbeitet Mitgliedsanträge. Manchmal verbinden Menschen ihre Spende mit einer Rückmeldung an uns. Und Luisa reicht dieses Lob dann an das Team weiter, als Motivationsspritze und zur Versüßung des Arbeitsalltags. Das tut immer gut! Vielen Dank, an alle Unterstützer:innen!

„Ich finde es gut, dass ihr neben den klassischen IT- Themen die Themen staatliche Überwachung mit im Blick habt. Vielen Dank für eure Arbeit und auch dafür, dass ihr das Thema zwar ernsthaft und sachlich, aber durchaus auch spielerisch und lustig adressiert. Das halte ich für den richtigen Weg!“

„Weiter so!
Digitalen Daten-
schutz brauchen
wir mehr denn je!“

„Danke für
jeden digitalen
Mutmacher!“

„Ich kenne euch schon länger. Wenn man sich mit dem Thema Datenschutz und Digitaler Selbstbestimmung auseinandersetzt, kann man euch zum Glück kaum übersehen.“

„Für mich seid ihr ein ganz elementarer Teil der letzten Bastion gegen die Gleichgültigkeit gegenüber der alltäglichen Privatspionage.“

„Ich finde genial, was Ihr macht, und bin dankbar für Eure Arbeit! Eine kleine Spende von mir, aber Kleinvieh macht ja bekanntlich auch Mist. Liebe Grüße von einem Fan“

„Ich habe bereits in den 1987 ein Monatsgehalt meines Azubihilohnes als Strafe bezahlt für meine Weigerung, bei der Volkszählung 1987 mitzumachen. Heute browse ich gerne mit Tor über ein VPN, meine Prepaid-Handykarte ist seit 10 Jahren aktiviert von Daisy Duck, Teichstraße 69 in 96669 Entenhausen, und ich meide Social Media wie der Abgeordnete das Lobbyregister. Als Mitglied bei Ihrem Verein mit einer winzigen monatlichen Spende möchte ich andere auf dem Weg in ein selbstbestimmtes digitales Leben unterstützen.“

„Ich finde es wichtig, für digitale und sonstige Rechte einzustehen. Mit der Fingerabdruckpflicht in Personalausweisen ist für mich erneut eine rote Linie überschritten worden. Daher unterstütze ich Sie gerne bei Ihren Aktionen und angestrebten rechtlichen Schritten. Ich wünsche Ihnen noch einen angenehmen Tag. Bleiben Sie gesund!“

„Danke für
euren tollen
Nuudel-Service!“

Wir wollen ihn immer noch verhindern:

Den Fingerabdruck im Perso

Von Konstantin Macher



Grafik: Digitalcourage, cc by 4.0

Seit dem 2. August 2021 gilt in Deutschland eine Pflicht zur Speicherung von Fingerabdrücken im neuen Personalausweis. Wir sind überzeugt, dass es sich hier um einen ungerechtfertigten Eingriff in unsere Grundfreiheiten handelt. Biometrische Merkmale haben eine besondere Dimension, denn sie ermöglichen lebenslange Kontrolle: Menschen können, wenn es sein muss, Passwort, Namen und Wohnort wechseln, um sich beispielsweise vor Verfolgung oder Bedrohung zu schützen. Biometrische Daten wie Fingerabdrücke können wir niemals ändern. Und wenn sie in falsche Hände geraten, wie im vergangenen Sommer, als den Taliban nach der Machtübernahme in Afghanistan die technische Infrastruktur der NATO für die biometrische Erfassung der Bevölkerung in die Hände fiel, dann kann niemand mehr irgendeine Sicherheit garan-

tieren. Faustregel: Am sichersten sind die Daten, die gar nicht erst erfasst und gespeichert werden (Grundsatz der Datensparsamkeit).

Außerdem sehen wir es als einen Angriff auf unsere Würde, wenn wir wie Verbrecher:innen behandelt werden. Die zwangsweise und anlasslose Abgabe von biometrischen Daten entspricht nicht den Werten von Rechtsstaaten und Demokratien, sondern der Kontrollsucht von Polizeistaaten, in denen alle Menschen unter Generalverdacht stehen.

Wir waren begeistert von dem Zuspruch, den unsere „PersoOhneFinger“-Kampagne seit Sommer 2020 erhalten hat: Über 12.300 Menschen haben bei uns online unterschrieben, viele haben uns auch Kommentare geschickt. Daher wissen wir: Nicht nur wir sagen „Wenn der Staat uns nicht vertraut – warum soll-

ten wir dann staatlichen Behörden vertrauen?“ Sondern viele fragen sich: Selbst wenn wir dem deutschen Staat gute Absichten unterstellen, trauen wir ihm wirklich zu, die Sicherheit unserer biometrischen Daten zu garantieren? Viele haben uns geschrieben, dass sie unserer Aufforderung gefolgt sind und noch vor dem 2. August 2021 einen Personalausweis ohne diese Überwachungsfunktion beantragt haben.

Und das ist wichtig, denn damit haben wir Zeit gewonnen, um die Pflicht doch noch zu kippen. Wir haben juristische Schritte auf den Weg gebracht, denn wir glauben, einer ordentlichen Prüfung hält das neue Gesetz nicht stand.

Die verpflichtende Abgabe von Fingerabdrücken ist **nicht zielführend**, da sie auf Dauer die Fälschung von Ausweisdokumenten nicht verhindern wird. In einem stetigen Katz- und Mausspiel zwischen Dokumentenfälscher:innen und (Un-)Sicherheitsbehörden werden ständig neue (und zunehmend teurere) Merkmale verwendet, um einen kurzen technischen Vorsprung zu erhalten. Und sie ist **nicht verhältnismäßig**, da hier unsere persönlichen Daten massenhaft in die Waagschale geworfen werden, um gegen eine geringe Anzahl von Fällen vorzugehen. Seit 2007 wird bereits im deutschen Reisepass der Abdruck des rechten und linken Zeigefingers gespeichert. Seinerzeit wurde damit argumentiert, dass das ja nicht schlimm sei, weil es mit dem Personalausweis noch ein anderes Ausweisdokument ohne Fingerabdruck gäbe.

Der Weg durch die Instanzen, den wir jetzt einschlagen, kann sich aber über eine lange Zeit hinziehen. Wir sind gewillt, mit Hilfe des juristischen Sachverständes unserer Anwälte bis zu einer höchstrichterlichen Entscheidung zu kämpfen, um die neue Fingerabdruckpflicht im Personalausweis wieder zu Fall zu bringen. Dabei hoffen wir weiterhin auf couragierte Unterstützung: Mit Ihrer Unterschrift kann unserer Klageposition mehr Gewicht verliehen werden. Und wie alles, kostet auch das Geld: Jede Spende hilft uns, diesen langen Klageweg zu bezahlen. Denn wir wollen gemeinsam nicht locker lassen und unser aller Grundrechte durchsetzen.

Hier können Sie unterschreiben
(und gerne auch spenden):

aktion.digitalcourage.de/

[perso-ohne-finger](#)

Erhältlich im Digitalcourage-Shop!

Stempel: Schäubles Fingerabdruck



Einige Zeit lang sammelte der der Chaos Computer Club die Fingerabdrücke von Politikern. Hier der Fingerabdruck von Dr. Wolfgang Schäuble: ein Stempel mit hohem Symbolwert.

Stück: 7,50 Euro zzgl. Versand

► shop.digitalcourage.de

Foto: Panthermedia

Der rC3: Ein Riesenspaß beim Chaos Communication Congress

Von Jens Reimerdes



„Hallo Jens, hast Du schon gehört, dass der Chaos-Congress in diesem Jahr keine Präsenzveranstaltung, sondern ein Computerspiel werden soll? Hast Du Lust, das mit uns zu entwickeln?“ – „Nein, davon habe ich noch nicht gehört. Klingt aber super – wie viel Zeit haben wir noch?“ – „Äh... drei Wochen...“

Mit diesem Telefonat fing es für mich an: Der alljährliche Chaos Congress, also das große Jahrestreffen vom Chaos Computer Club (CCC) und allen Gruppen und Vereinen aus dessen Umfeld, konnte 2020 – wie so viele andere Veranstaltungen – leider nicht in Präsenz stattfinden. Aber ein Chaos-Congress wäre unterfordert (und unterfordernd), wenn er auf eine Abfolge von Video-Vorträgen wie andere Veranstaltungen umschwenken würde. Nein, hier würde etwas wirklich Neues geplant – und davon hatte ich genauso wenig Ahnung wie viele andere.

Was wir brauchten, war eine Map. Das ist ein Grundriss, auf dem sich die Teilnehmer:innen mit kleinen Figürchen/Avataren zweidimensional bewegen und Attraktionen besuchen können.

Freundlicherweise gab es vom CCC ein kleines HowTo für alle angehenden Map-Architekt:innen. Blöd allerdings: Nach

dessen Lektüre waren die Fragezeichen noch viel größer als vorher. Unser kleines Digitalcourage-Team stürzte sich in die Arbeit – ohne zu wissen, wie das Ergebnis denn überhaupt aussehen soll.

„Wege entstehen dadurch, dass man sie geht“, hat der Lyriker Antonio Machado gesagt. Und sobald wir die ersten Hürden genommen hatten, ist etwas Bemerkenswertes passiert: Die anfängliche Ratlosigkeit wurde Schritt für Schritt durch eine spielerische Neugier und Faszination ersetzt, herauszufinden, was mit der gegebenen Technik alles möglich ist.

„Wenn wir dieses so machen können, geht dann auch jenes? Komm, wir probieren es einfach mal.“ – „An welchen Stellen könnten transparente Elemente oder Animationen neue Effekte schaffen?“ – „Wie übersetzen wir nicht nur die Inhalte, sondern auch den Charme von Digitalcourage in diese Computerwelt?“



Eine meiner persönlichen Lieblings-Herausforderungen war das Motherboard. Beim Chaos-Congress 2019 hatten wir bereits die Aktionen und Aktivitäten von Digitalcourage an einer Pinwand im Look einer Computer-Platine dargestellt – das



PADELUUN



musste jetzt auf eine interaktive Online-Map übertragen werden (seit 2021 gibt es das Motherboard ja auch schon im Jahrbuch, ► Seite 14). Wir fingen an mit einem winzig kleinen Bild, hinter dem eine kleine Website verlinkt sein sollte. Das wuchs dann mit der Zeit immer weiter, bis wir am Ende eine eigene Map dafür geschaffen haben, ein raumfüllendes Motherboard, das man durch ein Wandbild in unserer Hauptmap betreten und auf dem man als Spielfigur herumlaufen und die Elemente der Karte spielerisch entdecken konnte.

Wir konnten es selbst kaum glauben: Pünktlich zum Congress-Start kurz nach Weihnachten hatten wir eine Map, auf der man sich Digitalcourage virtuell „erlaufen“ konnte (zu besichtigen vorne in diesem Buch). Auch während der Congressstage haben wir laufend gefeilt, programmiert, daran gefummelt und die Map erweitert. Eine wiederkehrende Tradition übrigens, die ich bis dahin noch nicht kannte, da ich selber vorher noch keinen Congress besucht hatte. Denn auch im realen Leben ist der Aufbau mit Congressbeginn noch längst nicht abgeschlossen, sondern auch in der realen Welt wird noch bis zum letzten Veranstaltungstag ständig entwickelt und umgebaut. Und das gilt und galt nicht nur für Digitalcourage, sondern auch für die anderen Maps auf dem rC3 Congress 2021: Viele hundert Welten, die

eigens für diesen Congress geschaffen wurden, wurden auch während der Veranstaltungstage noch laufend weiterentwickelt.



Dazu gehörte beispielsweise auch unser Floh-Netzwerk. Angelehnt an die Bücher von Harry Potter haben wir kleine Kamine gebaut, durch die man direkt in die Welten befreundeter Organisationen hüpfen konnte, ohne die eigentlichen – teilweise sehr langen – Wege nutzen zu müssen. Mit dabei waren bspw. die Haecksen, das CERT, die Privacy Week, der Computertruhe e.V., FifF, Open-StreetMap, c-base, cyber4EDU und Moin.

Ja, der rC3-Congress 2021 hat mich und andere, allen voran Leena, Jan, Sebastian und Georg aus dem Digitalcourage-Team, viele (häufig auch nächtliche) Stunden gerade in der Weihnachtszeit (28.-30.12.2020) gekostet. Aber wir hatten auch wunderbare, herzliche Momente, viel Spaß und insgesamt tolle kreative Erfahrungen, die ich auf keinen Fall missen möchte. Ich freue mich schon auf das nächste Abenteuer.

**DNS-SERVER
(ZENSURFREI)**

Der Digitalzwangmelder

Von Melanie Lübbert, Julia Witte, Claudia Fischer,
Leena Simon und Andrea Neunzig

Illustration: Digitalcourage cc by 4.0



Wir lieben Technik. Und gleichzeitig finden wir es nicht in Ordnung, zur Technik-Nutzung gezwungen und davon abhängig gemacht zu werden. Denn meist werden – so ganz nebenbei und unerwähnt – dabei sehr viele Daten erhoben. Um sein Leben zu organisieren, sollte es auch immer möglich sein, auf digitale Technik zu verzichten und analoge Wege zu nutzen. Das gehört zur digitalen Mündigkeit.

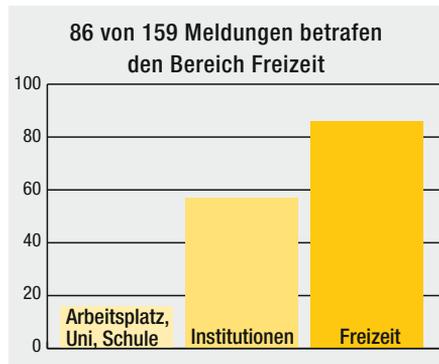
Im Juni 2021 startete unser neues Projekt „Digitalzwangmelder“. Wir riefen Menschen auf, uns Situationen zu melden, in denen sie sich zu digitalen Handlungen gedrängt fühlen.

Der Rücklauf war überwältigend. Uns erreichten die unterschiedlichsten Eingaben – manche auf digitalem Weg, andere als analoger Brief. Die große Mehrheit davon kam von Menschen,

die keineswegs Digitalmuffel sind. Sie kamen von Menschen, die sich in ihrem Alltag bedrängt fühlen und ein Unrechtsbewusstsein dafür haben.

► Die Ergebnisse:

Von Anfang Juni bis Mitte August 2021 sind bei uns 159 Meldungen eingegangen. Wir haben sie kategorisiert in die Themenfelder Arbeit/Uni/Schule, Institutionen (Behörden, Banken, Post, Versicherungen usw.) und Freizeit (Gastronomie, Freibäder, Kultureinrichtungen, Produkte). Auf Freizeiteinrichtungen kann man vielleicht verzichten, wenn einem der Digitalzwang nicht gefällt, auf Arbeit, Bildungseinrichtungen und Institutionen meistens nicht.

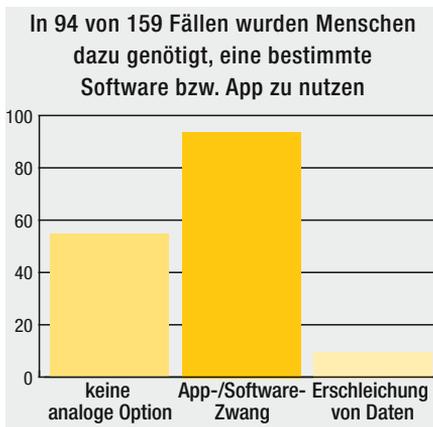


Wie erwartbar war im Sommer 2021, bezog sich mehr als ein Drittel aller Meldungen auf den Einsatz der umstrittenen und aus Datenschutzsicht nicht empfehlenswerten Luca-App. Außerdem

erhielten wir häufiger Meldungen zu Themen, die wir sowieso im Blick haben, wie z. B. Doctolib (► Seite 108). Das hat uns sehr gefreut – eine Bestätigung unserer Arbeit.

Drei verschiedene Formen von Digitalzwang konnten wir ausmachen:

- Vorgänge, die früher analog möglich waren, können nur noch online oder sogar nur noch mit Smartphone genutzt werden (oder die analoge Form wird sehr teuer).
- Die Nutzung einer bestimmten Software oder App wird vorgeschrieben.
- Daten werden unnötigerweise erhoben (z. B. muss man bei manchen „Click and Collect“-Bestellungen seine Adresse eingeben, obwohl man die Ware doch abholen kommt – ein Verstoß gegen das Datensparsamkeits-Gebot).



Viele Menschen meldeten Situationen, in denen sie durch den Digitalzwang von wichtiger gesellschaftlicher Teilhabe

ausgeschlossen wurden. Kitas, die Infos an die Eltern nur noch per Smartphone-App verteilen. Behörden, die nicht mehr telefonisch, sondern nur noch per Mail erreichbar sind. Museen, Zoos oder Freibäder, die man nur noch mit Online-Terminbuchung besuchen kann.

An anderen Stellen erschleichen sich digitale Dienste bei „ganz normaler Nutzung“ nebenbei noch persönliche Daten, wie hier zum Beispiel: *„Das Kopieren der Fotos von MEINER Kamera auf MEIN Handy via Wifi ist nur möglich, wenn GPS aktiviert ist. Das erscheint mir ziemlich unverschämt, weil es für den Vorgang definitiv nicht nötig ist.“*

So etwas wäre vielen Menschen wahrscheinlich gar nicht aufgefallen – bleiben Sie wachsam, was die Berechtigungen Ihrer Apps und Software angeht! Wenn Ihnen irgendwo Digitalzwang sauer aufstößt – Melden Sie ihn uns gerne, per Post oder auf unserer Website. Diese Meldungen liefern uns sehr wertvolle Informationen, auch wenn wir leider nicht jeder Meldung im einzelnen nachgehen und etwas dagegen machen können – das würde unsere Kapazitäten völlig sprengen. Aber die Meldungen fließen oft in unsere täglich Arbeit ein, zeigen, wo grade etwas in eine falsche Richtung läuft und geben uns Hinweise, wo wir Druck machen müssen.

- Wir geben Ihnen eine Stimme!

Digitalcourage wirkt, wirken Sie mit!

► digitalcourage.de/spende



Digitales Wissen für die Hosentasche

Von Katrin Schwahlen

Das Digitale – wir lieben es und möchten es menschenfreundlich und freiheitlich gestalten. Doch Digitales ist nicht immer leicht zu verstehen. Deswegen haben wir von Digitalcourage **kurz&mündig** erfunden: eine Broschüren-Reihe für mündige Menschen und solche, die es werden wollen. Im Hosentaschen-Format, grafisch überraschend gestaltet, immer mit einer klaren Haltung.

Die Themen reichen von Digitalisierung und Grundrechten über digitale Selbstverteidigung und politische Arbeit bis zu gesellschaftlichen Aspekten, Justiz und Technik.

Genauso vielfältig sind die Autorinnen und Autoren – Expert:innen für IT natürlich, für Bildung, Netzphilosophie, Medienpädagogik, Rechtskritik, Journalismus und viele andere Bereiche.

Über die Themen entscheiden wir mit hohem Anspruch an uns selbst und an das Selbstverständnis von Digitalcourage: Wir lassen uns nicht verdaten und verkaufen.

Und: Man muss nicht alles wissen, aber man sollte wissen, wovon man keine Ahnung hat.

HOLEN SIE EINSCHÄTZUNGEN VON EXPERT.INNEN EIN

Sie müssen das Rad nicht neu erfinden. Haben andere bereits etwas über diesen Anbieter oder das Angebot herausgefunden?

Aber verlassen Sie sich nicht auf Kundenrezensionen oder Sternebewertungen, denn die sind oft gefälscht – zumindest die guten Bewertungen. Geben Sie stattdessen zum Namen des Webdienstes Schlagworte wie „Datenschutz“, „Sicherheit“ und „Bewertung“ in die Suchmaschine ein. Schauen Sie nach Expertisen von Verbraucherzentralen, Datenschutzbehörden, Juristinnen und Informatikern. Auch IT-Magazine und techniknahe Nachrichtenportale veröffentlichen oft Bewertungen einzelner Angebote und Anbieter.



Digitale Mündigkeit (Band 1) ist dabei eine der wichtigsten Kompetenzen, die Sie trainieren können. Digitale Mündigkeit bedeutet, Verantwortung für das eigene Handeln im digitalen Raum zu übernehmen.

► Websites, Tools und Apps

Die Broschüre **Faire Websites** (Band 3) erklärt zum Beispiel, was Sie dafür tun können, damit keine Daten von Nutzer:innen an Dritte abfließen. Sie und vor allem Ihre Programmierer:innen bekommen jede Menge Tipps für IT-Sicherheit, für Ihre eigene private Website oder als Organisation mit sensiblem Beratungsanspruch.

Um Datenschutz und freie Software geht es im siebten kurz&mündig-Band **Homeoffice**. Das ist wichtig für alle, die auch im Homeoffice Videokonferenzen starten, Verzeichnisse verwalten und Firmengeheimnisse schützen wollen.

Mal ehrlich, lesen Sie jedes Mal das Kleingedruckte, wenn Sie eine App installieren? In Band 13 erfahren Sie, wie Sie in fünf Minuten **Webangebote und Apps** einfach selbst auf Vertrauenswürdigkeit prüfen können.

► Digitale Bildung und Datenschutz

Digitalisierung in Schulen ist auch und gerade nach Corona ein wichtiges Thema. Band 4 der k&m-Broschüren rückt Schüler:innen, Lehrkräfte und Eltern in den Mittelpunkt und stellt zehn Leitlinien auf, damit Lernen demokratisch, nachhaltig und digital funktionieren kann.

Band 2 gibt Eltern und Lehrkräften Tipps, wie sie **Datenschutzrechte durchsetzen** und andere zum Mitmachen bewegen können.

Lernen verändert sich, lebenslanges Lernen wird zentral, digitale Kompetenzen werden zu Grundkompetenzen für den digitalen



Verbreiten Sie keine Fakes
oder Verschwörungsideologien

FACT



BEISPIEL CYBERMOBBING

Material zum Thema Cybermobbing erfüllt oft nicht die inhaltlichen Anforderungen, wenn wichtige Lerneinheiten fehlen, z.B. über gesellschaftliche Konsequenzen der Social-Media-Nutzung, die schnelle Verbreitung von Nachrichten und die Funktionsweise von Ranking-Algorithmen (siehe 4.).

In die Lerneinheiten müssen außerdem Module zur Wiederholung und Reflexion eingebaut werden.



Wandel. Deswegen braucht es auch in der **Erwachsenenbildung** hochwertige und zeitgemäße digitale Bildungsangebote. Wie Sie diese Schritt für Schritt selbst erstellen können, zeigen wir Ihnen in Band 8.

Datenschutz ist Ihnen egal, weil Sie **nichts zu verbergen** haben? Quatsch, wir alle haben Geheimnisse. In Band 12 finden Sie elf starke Argumente, die helfen, wenn jemand Ihr Grundrecht auf Privatsphäre vom Tisch fegen will.

► Digitale Angriffe und Gewalt

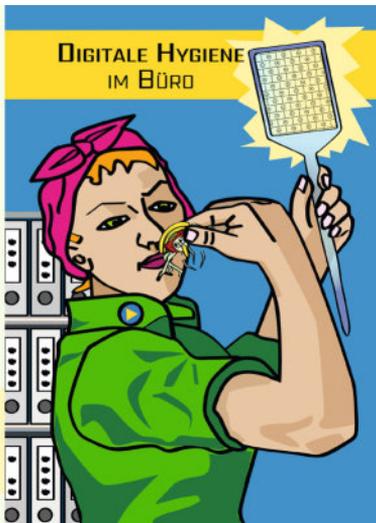
Woran erkennen Sie, ob Ihre Geräte gehackt wurden? Was können Sie tun, um Angreifer:innen nicht hereinzulassen? Wie gehen Sie mit Hatespeech um? Band 6 zeigt Ihnen, wie Sie **digitale Gewalt und Stalking** erkennen und beenden können.

Sie sind Anwalt, Ärztin, Journalist, Pastorin oder Berater? Alle Menschen, die beruflich die Geheimnisse anderer wahren müssen, finden in **Digitale Angriffe im Büro** (Band 9) konkrete Tipps und Hinweise, was technisch möglich ist und wie sie sich schützen können.

Apropos Beraterinnen: Vor allen in **Frauenhäusern** spielt (digitale) Sicherheit eine extrem große Rolle. Doch IT-Sicherheit für diese Organisationen steckt oft noch in den Kinderschuhen, dort ist noch viel Pionierinnenarbeit zu leisten. Band 10 fasst zusammen, welche Software genutzt werden sollte und was ein guter Umgang mit Social Media ist.

► Demokratie und Gesellschaft im digitalen Raum

Demokratie braucht lebendige Demonstrationen. Die **Versammlungsfreiheit** durch verschärfte Gesetze einzuschränken und Aktionsformen zu kriminalisieren, ist ein Angriff auf die Zivilgesellschaft. Band 11 gibt Ihnen



einen Überblick über die Versammlungsgesetze in Deutschland, die Rolle von Polizei und Behörden, Videoüberwachung und Ordnungswidrigkeiten.

Wie wollen wir als Gesellschaft umgehen mit Fake News, Gewalt, verletzten Persönlichkeitsrechten usw.? Immer wieder werden „Uploadfilter“ als eine Lösung präsentiert – gegen den Willen vieler Internetnutzer:innen, die den Algorithmen nicht die Entscheidung über ihre Inhalte überlassen wollen. Band 5 erklärt leicht verständlich, wie Uploadfilter funktionieren und warum sie der Demokratie schaden.

In Band 14 erklären wir, wie das **chinesische Sozialkreditsystem** funktioniert. An Überwachungskameras haben wir uns gewöhnt. Fahrtrouten von der App berechnen zu lassen, ist so bequem, und wie praktisch ist es doch, dass Algorithmen beim Buchen und Shoppen helfen. Doch was, wenn jene Algorithmen gleichzeitig das Verhalten kontrollieren und dafür Plus- oder Minuspunkte vergeben? Was dystopisch klingt, ist in China längst Realität.

► Hinterher ist man immer schlauer.

Schon oft haben Leser:innen die kurz&mündig-Hefte liebevoll als „Pixibücher für Erwachsene“ bezeichnet. Wir hoffen, dass sie genauso viel Spaß bringen und genauso oft gelesen werden wie die Kinderbücher. Sie können die Broschüren im Digitalcourage-Shop bestellen oder in jeder gut sortierten Buchhandlung kaufen. Falls Ihre Lieblingsbuchhandlung sie noch nicht führt, geben Sie gerne unsere Adresse weiter. Wir gewähren Buchhandelsrabatt und haben auch schicke Kassendisplays im Programm.

Und wenn Sie ein digitales Thema haben, über das unbedingt berichtet werden sollte, melden Sie sich. Wir freuen uns immer über neue Ideen und Autor:innen und helfen gerne bei der journalistischen Umsetzung.



Ein Umerziehungsinstrument wie das chinesische Sozialkreditsystem kann nur so gut sein wie die daran gekoppelte Künstliche Intelligenz. Künstliche Intelligenz aber ist nur so gut, wie es die menschliche Forschung zulässt. Ob diese Forschung also vorangetrieben werden sollte, ob der Menschheit wirklich daran gelegen sein sollte, solch ein gruselig-umfangreiches und effizientes Überwachungswerkzeug zu perfektionieren – das ist die entscheidende Frage, die wir eindeutig mit „Nein“ beantworten.



Videoüberwachung bei Demonstrationen:

Wie dürfen Kameras eingesetzt werden?



Bild und Text sind in der kurz&mündig-Broschüre 11 „Versammlungsfreiheit“ erscheinen. Viel Spaß mit diesem Wimmelbild! Es gibt viel – insbesondere viele Kameras - zu entdecken!

Videoaufnahmen werden von den Gerichten grundsätzlich als Einschränkung der Versammlungsfreiheit gesehen, weil sie potentiell einschüchternd wirken. Für die Anfertigung von

Bild- und Tonaufnahmen sind deshalb Rechtsgrundlagen in den Versammlungsgesetzen erforderlich.

1 Das Bundesversammlungs-gesetz erlaubt lediglich **Aufnahmen von konkreten Teilnehmer:innen**, wenn erhebliche Anhaltspunkte dafür sprechen, dass die Personen Straftaten oder Ordnungswidrigkeiten begehen (werden).

2 Die Versammlungsgesetze der Länder (Ausnahme: Sachsen-Anhalt) weiten die Überwachungsbefugnisse mittels Videoaufnahmen aus, indem sie **Übersichtsaufnahmen** erlauben. Dies muss zwar „wegen der Größe oder Unübersichtlichkeit“ erforderlich sein – aber mal ehrlich, welche Demo ist denn klein und übersichtlich? Man wird in Zukunft davon ausgehen müssen, dass jede Versammlung, die kein Reinfall ist und eine Größe von ca. 100 Teilnehmer:innen erreicht, durch Übersichtskameras gefilmt wird. Und das, obwohl das Bundesverfassungsgericht explizit „exzessive Observationen“ verbietet. Es gibt in den Ländergesetzen unterschiedliche Regelungen, inwiefern die Identifikation einzelner Teilnehmer:innen möglich und erlaubt ist. Und ob, wie und wie lange die Aufnahmen gespeichert werden dürfen.

3 Besonders problematisch ist die geplante NRW-Regelung, die **verdeckte Aufzeichnungen** erlaubt – Versammlungsteilnehmer:innen müssen in NRW

also zukünftig befürchten, auf Versammlungen von staatlichen Stellen, ggf. sogar von verdeckten Ermittler:innen, gefilmt zu werden - ohne dass sie hiervon Kenntnis haben. Es ist zudem kaum möglich, hiergegen Rechtsschutz vor den Gerichten zu erlangen, da man ja nicht mal weiß, ob man gefilmt wurde.

4 Zur Verfolgung von Straftaten und Ordnungswidrigkeiten darf die Polizei auch **Videobilder, die privat aufgenommen wurden**, z.B. von Smartphones oder Ladenkameras, beschlagnahmen und auswerten.

5 Ebenfalls problematisch sind die möglichen **Weiterverarbeitungen** der Videoaufnahmen. Auch wenn eine automatisierte Analyse beispielsweise durch Gesichtserkennungs- und andere Datenbanksoftware zurzeit (noch) unzulässig ist, wecken einmal erhobene Daten Begehrlichkeiten. Es gibt inzwischen Beispiele von rechtswidriger Weiterverarbeitung polizeilicher Videoaufnahmen z. B. aus Hamburg, Hessen und NRW.

Versammlungsfreiheit – Gelebte Demokratie

k&m Band 11

3,50 Euro

zzgl. Versand

Online bestellbar unter:

digitalcourage.de/kum



Das Digitalcourage-Team

Porträts

Von Claudia Fischer

Digitalcourage lebt von den vielen Menschen, die haupt-, neben- und ehrenamtlich für eine lebenswerte Welt im digitalen Zeitalter arbeiten. Die Interessen sind vielfältig, genau wie die Tätigkeitsfelder und die Menschen selbst. Das wollen wir zeigen. In unseren Jahrbüchern präsentieren wir darum immer einige Gesichter und Namen, die zum Team gehören und sonst nicht immer sichtbar werden.

► Der Anpacker

Damien Jeske

„So richtig hellhörig wurde ich zum Jahreswechsel 2013/2014, als Facebook für viele, viele Milliarden US-Dollar den Messengerdienst WhatsApp gekauft hat“, beschreibt Damien Jeske seinen Digitalcourage-Werdegang. „Da habe ich mir gedacht, wenn die so viel Geld dafür auf den Tisch legen, dann haben die wirklich was Großes vor und versprechen sich viel Gewinn davon. Das können ja nur die Daten sein. Das hat mich sehr misstrauisch gemacht.“

Und wenn Damien etwas anpackt, dann macht er das konsequent. „Ich habe damals meine Social-Media-Konten gelöscht und bin von WhatsApp auf freie Messenger umgestiegen. Das war viel Aufwand, denn ich musste ja meinen ganzen Familien- und Bekanntenkreis davon überzeugen, mit mir nun über

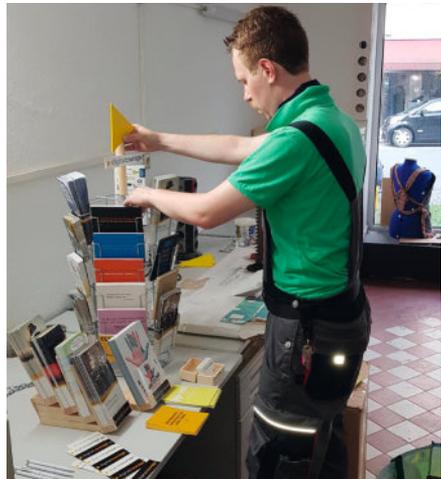


Foto: Damien Jeske, cc by 4.0

Infostand im TransitionHaus Bayreuth

andere Messenger in Kontakt zu bleiben. Wie oft habe ich gehört ‚Och nöö, das ist so umständlich, ne Extra-App, muss das denn sein?‘ Dafür fehlt mir manchmal das Verständnis – wie Leute aus reiner Bequemlichkeit ihre Privatsphäre riskieren.“

In Kontakt mit Digitalcourage kam Damien bei einer Demo „Freiheit statt Angst“. „Das war meine erste Demo überhaupt, und da war dieser Infostand von Digitalcourage mit der großen Krake, das hat mich angezogen. Die Website kannte ich schon aus dem Netz.“ Nach der Demo fragte er per Mail in Bielefeld an, ob er nicht in Bayreuth als Student eine Hochschulgruppe gründen

könnte. Und nach einigen persönlichen Kontakten beim Jahreskongress des Chaos Computer Clubs in Leipzig kam dann ein Anruf aus dem Büro in Bielefeld: „Ja, lass uns das mal machen mit der Hochschulgruppe.“ Und als nächster Schritt stand dann ein Einführungspaket mit Roll-Up-Banner, Infomaterial, T-Shirts etc. vor seiner Tür. „Das war genial, so viel Wertschätzung für meine Initiative zu erhalten.“ Seit 2019 ist Damien also die zentrale Person in der DC-Hochschulgruppe Bayreuth und engagiert sich per Fern-Kontakt in der AG Digitale Selbstverteidigung.

Die Vortragsreihe der – von der Uni Bayreuth und dem StuPa (Studierenden-Parlament) bestätigten – Hochschulgruppe Bayreuth hat einen weiten Einzugsbereich: Aus bis zu 100 km Entfernung kamen Menschen vor Corona zu den Infoabenden rund um digitale Selbstverteidigung. „Teilweise haben wir noch Stadtführungen in Bayreuth vorgeschaltet, damit sich die Anreise für unsere Referent:innen auch lohnt“, schmunzelt er. Mit Beginn der Pandemie hat Damien dann sehr kurzfristig zusammen mit dem Hackspace „Imaginärraum“ für einen seiner geplanten Veranstaltungsorte, das TransitionHaus Bayreuth, und die dortigen Initiativen einen BigBlueButton-Server für Videokonferenzen eingerichtet. „Seitdem haben wir online sogar Gäste aus Österreich bei unseren Veranstal-



Damien beim Vortrag über Phishing 2019

Foto: Damien Jeske, cc by 4.0

tungen dabei.“ Teilweise schalten sich deutlich über 100 Leute zu. Seit 2021 haben manche Vorträge schon wieder als Hybrid-Veranstaltungen stattfinden können. Bei den Videovorträgen packte ein Filmstudent tatkräftig mit an, aber auch Technik-Ausstattung und -Unterstützung aus dem Digitalcourage-Büro in Bielefeld haben geholfen, dass die Arbeit in Bayreuth während der Pandemie nahtlos weiter ging.

Mit seinem BWL-Studium ist Damien nun fertig, aber egal, wie es für ihn persönlich weitergeht: Digitalcourage in Bayreuth soll bleiben. „Es stehen mehrere Ideen im Raum“, sagt Damien zum Redaktionsschluss des Jahrbuches, „Genaueres werden wir erst 2022 entscheiden können. Klar aber ist: In Bayreuth und Umgebung soll Digitalcourage vertreten bleiben, denn es gibt hier sonst wenige Angebote für digital- und netzpolitisch denkende Menschen.“

Kontakt: zur Hochschulgruppe bayreuth: digitalcourage.de/hsg-bt

▶ digitalcourage
Hochschulgruppe
Bayreuth ◀

► Die Wort-Jongleurin Julia Witte

Julia kommt aus dem Großraum rund um Bielefeld, hat ihren Weg zu Digitalcourage aber über Bayern genommen. „Ich habe in Passau Wirtschaft und Kulturwissenschaften mit Schwerpunkt Südostasien studiert und ein Auslandssemester in Südchina gemacht. Die Entstehung von Nationen, das Verhältnis von Bürger:innen zu ihrem Staat und die Frage, wie Regierungen Menschen dazu bringen, sich auf eine bestimmte Weise zu verhalten – das hat mich damals sehr beschäftigt. 2011 hat mir ein Bekannter in Passau von Digitalcourage (damals noch FoeBuD e.V.) in Bielefeld erzählt. Und das passte zu meinen Interessen, also habe ich mich für ein Praktikum beworben.“

Während ihres Praktikums 2011 war die Einführung der elektronischen Gesundheitskarte ein großes Thema und Julia hat damals die Kampagne dazu mit angeschoben. „Dabei ist mir ein Mechanismus immer wieder aufgefallen: Die Bevorteilung einer bestimmten Gruppe ist immer auch die Benachteiligung aller anderen. Oder konkret in diesem Fall: Wenn eine Krankenkasse einen günstigeren Tarif anbietet für alle, die einen sogenannten gesunden Lebensstil pflegen, dann heißt das eben auch: Alle, die in den Augen der Krankenkasse nicht gesund genug leben – oder die nicht einsehen, warum sie das nachweisen sollten – all diejenigen müssen die Vergünstigungen für die anderen ausgleichen.“

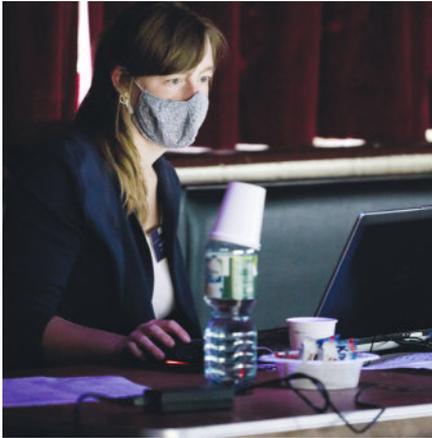
Nach drei Monaten ging sie zurück nach Passau und wieder ihrem Studium nach. Wobei sie sich schmunzelnd erinnert, dass sie eigentlich mehr Zeit beim Uniradio Campus Crew verbracht hat als im Hörsaal. Deshalb hat sie dieses Hobby nach dem Studium gleich zum Beruf gemacht – und sechs Jahre lang in Rosenheim als Hörfunkjournalistin und Radiomoderatorin gearbeitet. Für einen lokalen Radiosender und den Bayerischen Rundfunk hat sie über Kunst und Kultur, gesellschaftspolitische Themen, aber auch über bayrisches Brauchtum und altes Handwerk berichtet.



Foto: Fabian Kurz, cc by 4.0

Digitalcourage war zumindest räumlich weit weg – nicht aber die Themen und Gedanken, die Julia von ihrem Praktikum mitgenommen hat: „Wie automatische Bewertungssysteme Menschen benachteiligen und die Gesellschaft spalten, das hat mich weiter sehr bewegt. Auch weil ich selber mal Probleme durch die Schufa hatte. Es hat sich damals herausgestellt, dass meine einzigen ‚Vergehen‘ waren, dass ich jung war und in meiner Studien- und Praktikazeit ab und zu

Foto: Jens Reimerdes, cc by 4.0



Pressearbeit im Hintergrund:
Julia am Social-Media-Rechner
während der BigBrotherAwards

umgezogen bin. Ich konnte das dann recht schnell regeln, aber da habe ich gedacht: Das kann doch nicht sein, dass Leute durch Umstände, die total unbedeutend waren, in schlechte Bewertungen reinrutschen und dann kaum noch eine Chance haben, da wieder rauszukommen.“

Viele Jahre war sie „stille Sympathisantin“ – als Fördermitglied bei Digitalcourage und Leserin des Newsletters. Direkten Kontakt zum DC-Büro in Bielefeld hatte sie lange Zeit nicht mehr. Bis 2020 eine Stellenanzeige im Newsletter stand: Redakteurin gesucht. Da war Julia gerade mit Mann und Baby nach Ostwestfalen auf den Bauernhof ihrer Eltern gezogen. „Ich habe sofort gedacht: Das ist mein neuer Job! Ich habe Rena angerufen und war überrascht, dass die sich noch sehr gut an mich erinnern konnte.“ Weil ihre kleine Tochter aber gerade erst auf der Welt war, stand Julia kurzfristig erstmal nur

stundenweise zur Verfügung. Inzwischen ist sie mit 30 Stunden pro Woche fest angestelltes Teammitglied, betreut den Newsletter und die Website, koordiniert Arbeitsgruppen und Kampagnen-Aktionen.

„Digitalcourage war in den ersten Monaten super-flexibel mit meinen Arbeitszeiten, das hat in der Baby-Zeit total gut gepasst“, freut sie sich. „Der Verein und alle im Team haben die Arbeitsbedingungen quasi um mich herum gebaut, das weiß ich sehr zu schätzen! Es hieß immer: Was du schaffst, das schaffst Du, und was nicht, das nicht.“ Und – das wissen wir im Verein wiederum zu schätzen – Julia schafft eine Menge!

Sie sieht sich selbst oft als Übersetzerin: Das Fachwissen der Spezialist:innen im Verein erkennen, sammeln und übersetzen für die Menschen, die sich nicht so intensiv mit Digitalthemen oder Netzpolitik beschäftigen können.

Momentan tut sie das noch schriftlich, bald hoffentlich auch per Podcast und Video. Das Studio ist im Bau.

**Bewerben Sie sich
für ein Praktikum!**



► bewerbung@digitalcourage.de

► Der Möglich-Macher Gunther Pflüger

Viele lachen über den Begriff „Facility-Management“, der angeblich als Verballhornung von Hausmeister verwendet wird. Dabei kann man „Facility“ auch mit „Möglichkeit“ oder „Leichtigkeit“ übersetzen, und das gefällt Gunther Pflüger so richtig gut. „Ich verstehe mich als jemand, der Ideen und Wünsche umsetzt“, sagt er, und das ist so ziemlich das Gegenteil vom Hausmeister-Klischee als der „Verhinderer im grauen Kittel“. „Projektrealisation“ ist das, was er für sich als treffendste Beschreibung empfindet. „Die Kreativität von kreativen Menschen braucht jemanden, der dafür sorgt, dass das auch entsteht. Und das bin ich“, bringt er sein Selbstverständnis auf den Punkt.



Im Escape-Room in Osaka reagiert Gunthers Steuerung interaktiv auf die Spieler:innen.

Bei Digitalcourage wurde er für die Organisation und Leitung von Veranstaltungen eingestellt. Die Verleihung der BigBrotherAwards 2021 war seine Feuerprobe (► Seite 70), die Vorbereitung für den BBA 2022 läuft bereits, die nächsten Großdemos werden kommen, und damit ihm nicht langweilig wird, hat Digitalcourage ein paar Häuser neben dem „Hauptquartier“ in der Marktstraße 18 noch weitere Räume angemietet, in denen Gunther gerade jede freie Minute verbringt. Ein Audio-Video-Aufnahme-

studio für Vorträge, Podcasts und kleine Talkrunden soll es geben, der Shop bekommt dort ein neues Zuhause, die Server werden umziehen und Büros und Aufenthaltsräume sollen für gesundes Arbeiten gestaltet werden. Lichtkonzepte, Kabelverbindungen, Klimatisierung – Gunther ist vielfältig gefordert und voll in seinem Element.

Wo hat er das alles gelernt? Gunthers Antwort ist eine Rückfrage: „Wo soll ich anfangen?“ Zirkusartist wollte er mal werden, als Jugendlicher lernte er nähen und entdeckte seine Leidenschaft für Technik beim Auseinandernehmen alter Geräte. „Neugier ist meine Triebfeder. Ich wollte schon immer

wissen, wie die Dinge funktionieren.“ Während Zivildienst und Studium kamen dann Flipper- und Videospieleautomaten, aber auch die Computer- und Videotechnik dazu. Später dann hat er große, aufwändige Messestände und Tagungen für Technik-Firmen wie IBM realisiert, zusammen mit seinem Bruder in dessen Firma CPP, die seit zwei Jahren auch die BigBrotherAwards filmt und streamt. Wirtschaftsmarketing, Kunst und Kultur, gemeinnützige Vereine – keine Branche ist ihm fremd. Zuletzt hat er dann

Foto: Gunther Pflüger, cc by 4.0

Foto: Gunther Prüfer, cc by 4.0



Schwarzlicht-Minigolf in Frankfurt:
Ein Fest der Neonfarben.

Escape-Rooms in Japan und Schwarzlicht-Minigolf in Frankfurt gebaut.

„In internationalen Projekten finde ich es faszinierend, wie unterschiedlich Arbeitskultur und -methoden sein können“, schwärmt er. Mal arbeitete er in einem basisdemokratischen Betrieb mit Einheitsgehältern, war Dienstleister bei internationalen Projekten und hatte mehrere Subunternehmer zu managen, dann wieder arbeitete er im Schulterchluss mit Künstler:innen und Ehrenamtlichen. Gunther hört zu, saugt Ideen auf, zieht sich zum Basteln zurück und verblüfft mit seinen Lösungen. „Ich liebe es, an die Grenzen dessen zu gehen, was gerade noch so machbar ist.“ Und das nicht nur technisch, sondern vor allem auch in der Zusammenarbeit mit Teams.

„Das Beste ist immer, wenn ich reisen kann“, erzählt er mit funkelnden Augen.

► „Ich liebe es, an die Grenzen dessen zu gehen, was so gerade noch machbar ist.“ ◀

Er ist nämlich auch begeisterter Online-Spieler und hat sowohl über jahrzehntelanges Gaming als auch über die LGB-TQI-Gemeinschaft Freunde und Kontakte in aller Welt. „Es ist so großartig, wenn man für eine Messe mal eine Woche in Stockholm oder Osaka ist, und die Chance nutzen kann, um Freunde zu treffen, die man seit Jahren online kennt.“ Und auch virtuell ist da viel möglich: In den beiden Escape-Rooms in Japan, die er mitgebaut hat, kann er vom Bielefelder Sofa aus das Licht ein- und ausschalten (macht er aber nur nach Absprache.)

Und dann kam der März 2020. Für Gunther war mit der Corona-Pandemie von einem Tag auf den anderen alles vorbei. Keine Reisen, keine Messen, keine Veranstaltungen, Kultureinrichtungen weltweit zu, Logistik-Wege unkalkulierbar. „Ich war wirklich am Rätseln, wie es für meine Projekte weitergehen soll“, erinnert er sich. Und dann rief sein Bruder Gernot an und sagte „Digitalcourage hat eine Stelle frei, für die wärst Du perfekt!“

„Das war wie nach Hause kommen“, sagt Gunther heute. Gernot und er kennen nämlich Rena Tangens und

padeluun schon seit CeBIT-Zeiten, also aus den 1990er-Jahren. „Wir haben uns in der Straßenbahn in Hannover kennengelernt, auf dem Heimweg vom Messegelände. Ins Gespräch kamen wir über Technik, und dann stellte sich heraus, dass Gernot padeluun als Musiker kannte und eine Platte von ihm hatte.“

Den Kontakt haben sie eher locker gehalten, ab und zu brachten Diskussionen über technische Neuheiten, Mailboxen, Netzentwicklung und Digitaltechnik sie wieder zusammen. „Es muss so um das Jahr 2000 herum gewesen sein, dass wir den Faden mit Rena und padeluun wieder aufgenommen haben“, vermutet Gunther. Beim Umzug der BigBrotherAwards aus dem Bunker Ulmenwall in die Industriehallen der Ravensberger Spinnerei in Bielefeld haben Gernot und Gunther den FoeBuD (bis 2012 hieß Digitalcourage so) technisch unterstützt. Später haben die Brüder Vorträge bei Public Domains gehalten und wurden Fördermitglieder.

Und nun saß Gunther im Herbst 2020 im Vorstellungsgespräch. Worüber spricht man da, wenn man sich schon so lange kennt? „Naja“, räumt Gunther ein, „ich habe immer gedacht, ich eigne mich nicht für politische Arbeit. Ich bin nicht gut in Diplomatie, mir ist Politik oft zu komplex, ich bin mehr so geradeaus. Aber das war ja bekannt, und die Wünsche hier treffen schon sehr meinen Bereich, nämlich die Visionen von anderen aufzunehmen und auf den Punkt umzusetzen. Und dann haben wir

im Gespräch gemerkt, dass wir gar nicht so weit auseinander liegen: Wir wollen ja nicht die Welt erklären. Wir fragen uns: Wie gibt man Menschen genau die richtigen Hinweise, dass sie selbst eine Lösung finden, um ihr Leben in der digitalen Welt zu verbessern? Das ist der Ansatz von Digitalcourage, und da ist meine Grundhaltung ganz ähnlich. Auch im Escape-Room muss ich die Hinweise geben, die Menschen brauchen, um die Rätsel zu lösen.“

Und woran bastelt Gunther im Moment? „Sag ich noch nicht“, grinst her. „Könnte was mit Kugelbahnen zu tun haben. Oder mit Flipper-Automaten.“ Die sammelt er nämlich seit vielen Jahren. Noch stehen sie in seinem Haus in Frankfurt, aber wer weiß...



Industriemesse für ABB in China: Die LED-Wand reagiert auf den Roboter.

Foto: Gunther Pflüger, cc by 4.0

Die

BIG BROTHER AWARDS

2021

Die Oscars für Datenkraken



Foto: Matthias Hornung, cc by 4.0

Vom Streaming her denken

Backstage-Bericht von den BigBrotherAwards 2021

Von Gunther Pflüger

„Wir möchten Sie nochmals besonders auf die Einhaltung der Hygienemaßnahmen und die Gewährleistung der besonderen Nachverfolgbarkeit bei Ihrer Veranstaltung hinweisen!“ – Dieser Satz aus einer E-Mail der Stadt Bielefeld klingt nicht besonders freundlich, aber für uns war es die Erlösung: Endlich Sicherheit! Die BigBrotherAwards können wie geplant stattfinden! Sogar mit Publikum! Wenn auch mit starken Auflagen.

Vorausgegangen waren Wochen und Monate der Unsicherheit bei der Planung der BBA, in denen wir Inzidenzen verfolgten und neue Verordnungen analysierten. Sogar einen Ausweichtermin im September hatten wir in Reserve, aber eigentlich wollte niemand verschieben.

Auf mich als Neuling im Digitalcourage-Team kam eine große Aufgabe zu: Durch die Corona-Auflagen sollte aus unserer heißgeliebten „Präsenzveranstaltung“ eine hybride „Livestream“-Veranstaltung werden. Das hat Konsequenzen für Beleuchtung, Platzierung der Personen, Möbel, Deko und organisatorische Details, die ich mit vielen kreativen und flexiblen Menschen zusammen entwickeln und umsetzen konnte.

Gestreamt haben wir schon ein paar Jahre lang und die Aufzeichnungen online bereitgestellt, aber der Fokus lag doch immer auf der Veranstaltung und dem Publikum vor Ort. Dies war nun anders! Diesmal haben Podeste mit Kameras, Schienen mit Kameradolly und Kameralenten den Raum domi-

niert. Dazwischen saßen auf streng nach Abstandsregeln platzierten Stühlen die geladenen Gäste. „Besondere Nachverfolgbarkeit“ stand in der E-Mail – wir erinnern uns.

Der technische Aufwand war in diesem Jahr dann auch entsprechend höher, und wir mussten uns einige Gedanken machen, um das neue Format an unsere eigenen Ansprüche an Interaktivität mit den Zuschauern, die ja nun mehrheitlich

nicht mehr vor Ort waren, anzupassen. Wer sich hier noch einmal ein eigenes Bild machen möchte, findet die Videoaufzeichnung der BBA 2021 über die Jahrbuch-Webseite.

► Ohne die Hilfe der Firmen CPP Studios, Freiraum erleben, BlueSound, das VOC-Team des Chaos Computer Clubs sowie vieler weiterer Helfer:innen wäre das nicht möglich gewesen – herzlichen Dank.

Foto: Matthias Hornung, cc by 4.0



► Die Jury der BigBrotherAwards 2020

(von links nach rechts):

Dr. Thilo Weichert, DVD, Netzwerk Datenschutzexpertise. Die Deutsche Vereinigung für Datenschutz e.V. (DVD) ist eine unabhängige Bürger:innen-rechtsvereinigung, die sich für Datenschutzbelange in Deutschland und Europa einsetzt.

Frank Rosengart, CCC. Der Chaos Computer Club e.V. (CCC) ist die

größte europäische Hackervereinigung und seit 1981 Vermittler im Spannungsfeld technischer und sozialer Entwicklungen.

Rena Tangens und padeluun, Digitalcourage

Prof. Dr. Peter Wedde ist Professor für Arbeitsrecht und Recht der Informati- onsgesellschaft an der Frankfurt Uni- versity of Applied Sciences, wissen- schaftlicher Leiter der Beratungsge- sellschaft d+a consulting GbR in Wies- baden sowie Herausgeber und Autor zahlreicher Bücher und Fachveröffent- lichungen.

Dr. Rolf Gössner, Rechtsanwalt und Publizist, hat sich in diesem Jahr aus der Jury verabschiedet – unser Dank folgt auf der nächsten Seite.

Rolf Gössner: Danke für 20 Jahre BigBrotherAwards-Jury!

Von Rena Tangens, padeluun und Claudia Fischer

Rolf Gössner, Jurymitglied der ersten Stunde bei den deutschen BigBrotherAwards, hat sich im Juni 2021 nach 20 Jahren aus der Jury verabschiedet. Wir danken ihm von Herzen für seinen Scharfsinn, seine unbeugsame Haltung, seine meisterliche Reden und viele spannende Diskussionen in der Jury.

Seit der ersten BigBrotherAwards-Verleihung im Jahr 2000 war Rolf Gössner festes Mitglied in unserem Jury-Team. Als engagierter Strafverteidiger und Publizist wie auch als Vorstand der Internationalen Liga für Menschenrechte hatte sein Wort Gewicht bei unseren Jury-Entscheidungen. Rolf sezierte kenntnisreich Überwachungsgesetze und tadelte treffsicher besonders überwachungsafine Politiker:innen und Behörden. Otto Schily, Wolfgang Schäuble – die Innenminister von Bund und Ländern haben mittlerweile so etwas wie ein Abo auf den BigBrotherAward – dazu BKA, BND und der Verfassungsschutz.

Eigentlich hoffte Rolf Gössner wie wir alle in der Jury, dass nach zehn Jahren BigBrotherAwards das Ziel erreicht sein würde: Dann wäre alles gesagt, unsere guten Argumente hätten sich durchgesetzt und es würden nur noch demokratie- und rechtsstaatsverträgliche Digital-

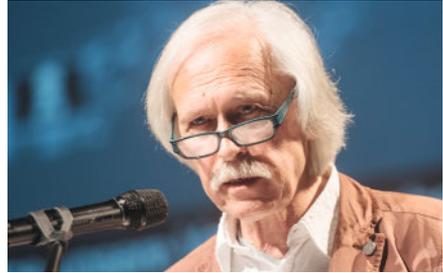


Foto: Matthias Hornung, cc by 4.0

und Sicherheitsgesetze beschlossen. Diesem Traum standen leider sowohl das Beharrungsvermögen als auch der Überwachungsideenreichtum von Behörden und Politik entgegen. Doch auch wir sind beharrlich. Rolf Gössner war 20 Jahre Mitglied der BigBrotherAwards-Jury. 20 Preisträger hat er in Tiefe recherchiert, pointiert bewertet und hinreißend laudiert.

Was unsere Zeitplanung oft auf eine harte Probe stellte: Rolf kämpfte um jede zusätzliche Minute Redezeit – er hatte aber auch etwas zu sagen! Und mit welcher Wortgewalt und Emphase er die Laudationes vortrug – zugleich strahlte er stets Seriosität und Gelassenheit aus. Das Publikum dankte es ihm regelmäßig mit der Wahl des Publikumspreises.

Von den staatlichen Akteur:innen hatte niemand je die Größe, den Preis persönlich entgegenzunehmen – obwohl wir sie stets zur Preisverleihung einladen. Einen

allerdings hat Rolf überlistet: Der ehemalige niedersächsische Innenminister Uwe Schünemann bekam 2011 den Award live vor laufender Fernsehkamera bei Sat 1. Dieses Video (verlinkt über die Jahrbuch-Webseite) macht uns immer wieder Freude!



Foto: Tom Kohler, cc by 4.0

Rolf mit Patrick Breyer, MdEP, zur Verfassungsbeschwerde gegen Vorratsdatenspeicherung 2016

Kein Artikel über Rolf Gössner sollte ohne den Hinweis auskommen, dass er selbst 40 Jahre lang in unrechtmäßiger Weise vom Verfassungsschutz beobachtet wurde. Den juristischen Kampf gegen diese Repressalien hat er Ende 2020 nach 15 Jahren Prozessführung gegen das Bundesamt für Verfassungsschutz endgültig gewonnen. Niemand wusste also besser als er, was staatlicher Überwachungswahn bedeutet.

Passend zum Abschied hat Rolf Gössner ein neues Buch „Datenkraken im öffentlichen Dienst“ herausgebracht – darin

finden sich Rückblick und Updates auf „seine“ BBA-Preisträger. „Ich will Wiederholungen vermeiden“, ist eines von Rolf Gössners Motiven, nach 20 Jahren die BigBrotherAward-Jury zu verlassen. Denn – siehe oben – mit Wiederholungstätern ist gerade bei Behörden und Politik leider zu rechnen.

► Lieber Rolf, wir danken dir von Herzen! Die Zusammenarbeit mit dir war eine große Freude für uns, du hast uns beflügelt, wir haben viel von dir gelernt, der Austausch und die Diskussion bei unseren gemeinsamen Jury-Sitzungen waren für uns stets ein Highlight des Jahres. Wir wünschen dir, dass du nun etwas mehr Zeit für Ruhe, Entspannung und die angenehmen Seiten des Lebens haben wirst. Du hast uns am Ende deiner Abschiedsrede den Auftrag mit auf den Weg gegeben, dass weiterhin noch viel, eher immer mehr zu tun sein wird im Einsatz für Grundrechte und eine lebendige Demokratie. Wir bleiben dran, lieber Rolf – versprochen. Und wir freuen uns, wenn wir hin und wieder von dir hören und einen Rat von dir einholen dürfen.

Erhältlich bei uns im Shop Datenkraken im öffentlichen Dienst



von Rolf Gössner
Verlag: Neue Kleine Bibliothek
ISBN 13:
978-3-89438-753-2
Paperback
366 Seiten
Preis: 19,90 EUR
versandkostenfrei

► shop.digitalcourage.de

Alle Preisträger.innen von Rolf Gössner in 20 Jahren BigBrotherAwards:

Jahr	Kategorie	Preisträger.innen
2000	Politik	Der Innensenator von Berlin Dr. Eckart Werthebach
2001	Politik	Der Bundesinnenminister Otto Schily für sein Überwachungs-gesetze-Paket, die sogenannten „Otto-Kataloge“
2002	Behörden und Verwaltung	Das Bundeskriminalamt für drei präventive Datenbanken mit Verdächtigen
2003	Politik	Die Innenminister und Regierungen von Bayern, Niedersachsen, Rheinland-Pfalz und Thüringen
2004	Behörden und Verwaltung	Die Bundesanstalt für Arbeit für ihre inquisitorischen Fragebögen für Erwerbslose
2005	Lebenswerk	Abermals Bundesinnenminister Otto Schily, siehe 2001
2006	Politik	Die Bundeskonferenz der Innenminister.innen und -senator.innen für die „Anti-Terror-Datei“
2007	Behörden und Verwaltung	Die Generalbundesanwältin Monika Harms für die Maßnahmen gegen die Protestierenden gegen den G8-Gipfel 2007
2008	Europa/EU	Der EU-Ministerrat für die EU-Terrorliste
2009	Lebenswerk	Wolfgang Schäuble, damals Bundesinnenminister
2010	Kein BBA	Veranstaltung verlegt von Herbst 2010 ins Frühjahr 2011
2011	Politik	Der niedersächsische Innenminister Uwe Schönemann
2012	Politik	Der Bundesinnenminister Dr. Hans-Peter Friedrich (CSU) für die Einrichtung von Cyber-Abwehrzentren und Verbunddateien
2013	Behörden und Verwaltung	Die Bundespolizei für Racial Profiling
2014	Politik	Das Bundeskanzleramt für die deutschen Verstrickungen in den NSA-Überwachungsskandal
2015	Behörden und Verwaltung	Der Bundesnachrichtendienst (BND) für seine ausufernde Rolle in Geheimdienstskandalen und Überwachungsexzessen
2016	Lebenswerk	Der Verfassungsschutz für seine gesamte 65jährige Geschichte
2017	Behörden	Die Bundeswehr, geleitet von Ursula von der Leyen, für die Vorbereitungen auf einen Cyber-Krieg
2018	Politik	Die hessische Landesregierung aus CDU und Grünen für das neue Polizeigesetz
2019	Behörden und Verwaltung	Der hessische Ministerpräsident Peter Beuth für die Beauftragung der US-Firma Palantir mit der Ausforschung von Social Media- und Polizeidateien
2020	Politik	Die Bundesregierung für die Untätigkeit gegen die US-Militärbasis in Ramstein

mächtigen Bordcomputer für die Steuerung und sind – dank dem BigBrotherAward-Preisträger von 2014 („e-Call“) – auch bereits mit einem Mobilfunkmodul ausgestattet, welches diese ganzen Daten sogar in Echtzeit übermitteln kann. Sowas nennt sich „Telemetrie“ (oder weniger technisch: „nach Hause telefonieren“). Für Telemetrie in Windows 10 hat Microsoft im Jahr 2018 einen BigBrotherAward bekommen. Und wenn das Auto das alles sowieso kann, braucht man gar keine Laborwerte mehr, die womöglich geschönt und frisiert werden.

Gut, bei der Übertragung per Mobilfunk könnte man jetzt denken: Puh, tja, ist der Echtzeit-Anspruch nicht etwas übertrieben? Könnte man die Daten nicht einfach sammeln und beim nächsten Werkstattaufenthalt auslesen? Klar, das ginge, aber neue Autos müssen erst nach drei Jahren zum TÜV, so lange müsste die EU-Kommission auf die Daten warten. Mit Blick auf den fortschreitenden Klimawandel ist das eine lange Zeit.

Für die nun laufende Testphase von fünf Jahren hat sich die EU-Kommission bei der Umsetzung der Verordnung 2019/631² dafür entschieden, die Hersteller mit der Datensammlung zu beauftragen.

² Link zur EU-Verordnung auf Jahrbuch-Website

Aha. Die Autohersteller. Die bisher sooo „ehrlich“ bei den Angaben zu Schadstoffen und Verbrauchswerten waren. Ernsthaft?

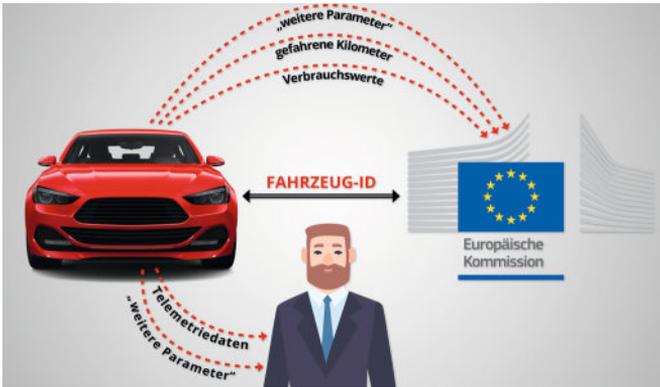
Das hat sich die EU-Kommission wohl auch gefragt – und möchte deswegen detailliert, für jedes Auto mit seiner Fahrzeugidentifikationsnummer, in dichten Abständen, die Verbrauchswerte, gefahrene Kilometer und ggf. weitere Parameter übermittelt bekommen, damit soll eine Schummelei seitens der Hersteller unterbunden werden.

► **Die Autohersteller. Die bisher sooo „ehrlich“ bei den Angaben zu Schadstoffen und Verbrauchswerten waren. Ernsthaft? ◀**

Kleiner Schönheitsfehler: Die Hersteller sind immer noch im Boot. Mehr noch: Sie bekommen die umfangreichen individuellen Telemetriedaten frei Haus geliefert, die sie sonst nur mit ausdrücklicher Einwilligung des Halters erheben dürften. Und nicht nur das, sondern darüber hinaus nicht genauer von der Verordnung spezifizierte „weitere Parameter“. Eine höchst willkommene weitere Datenquelle für die Hersteller.

Zwar steht in der EU-Verordnung, dass die Fahrzeug-Identifizierungsnummern „lediglich für die Zwecke dieser Datenverarbeitung verwendet und nicht länger als dafür notwendig gespeichert“ werden sollen, aber wie lange das ist, da möchte sich lieber niemand so genau festlegen. Fest steht: So lange die Motordaten mit der Fahrzeug-ID verknüpft bleiben, sind

Grafik: Dennis Blomeyer, cc by 4.0



Die EU-Verordnung ist eine willkommene Datenquelle für die Autohersteller.

auf jeden Fall umfangreiche Einblicke in das individuelle Fahrverhalten möglich.

Laut einer Antwort auf eine parlamentarische Anfrage der FDP³ ist sich die Bundesregierung sicher, dass mit dieser Technik keine Bewegungsprofile erstellt werden können, und abgesehen von der Datenbank beim Kraftfahrzeug-Bundesamt und denen der Versicherungen gäbe es auch keine Verknüpfung zwischen den Fahrzeugnummern und Halter:innen. Aber wie wir aus der Vergangenheit wissen, gerade wenn es um Bewegungsdaten geht: Wo ein Trog ist, kommen die

Grafik: Dennis Blomeyer, cc by 4.0



„Wo ein Trog ist, da kommen die Schweine.“ (Frank Rosengart)

3 Link zur FDP-Anfrage auf Jahrbuch-Website

Schweine. Wenn die Daten erstmal gesammelt sind, findet sich auch schnell ein Bedarf mit einem „berechtigten Interesse“ dafür.

Und nicht nur die EU-Kommission, auch die Bundesregierung hätte solche Daten gerne. Sie plant die Initiative „Datenraum-Mobilität“. Dort sollen vor allem die deutschen Autohersteller und Mobilitätsanbieter ihre Daten „teilen“, so das Ziel des Projektes. Wer da was mit wem teilt, ist aber noch reichlich unklar. Es gibt bestimmt sinnvolle Anwendungen für so einen Datenpool. Aber es lässt auch erahnen, wie zukünftig die Autofahrer:innen darum kämpfen müssen, dass ihre Bewegungsdaten nicht zum Freiwild werden.

Mit der elektronischen Verbrauchsdatenerfassung und -übermittlung (die englische Abkürzung dieses Verfahrens ist „OBFCM“) wird ein weiteres Mosaiksteinchen in Richtung gläserne Autofahrer:innen gelegt, obwohl dies gar nicht notwendig wäre. Wir sehen mit Sorge, wie Telematikdienste ihren Weg in die Autos finden und der Datenschutz dabei auf der Strecke bleibt.

Deshalb sagen wir für diese EU-Verordnung 2019/631: Herzlichen Glückwunsch, zum BigBrotherAward 2021, liebe EU-Kommission.

Wie es weiter ging

Von Claudia Fischer

Kommentare unseres Publikums via Twitter und Mastodon:

- ▶ „Danke, Uschi!“
- ▶ „Frage an das BigBrother Live-Team: Wo kann man die neugierigen Fahrzeuge denn stumm schalten lassen?“
- ▶ **Läuft... nicht gut.**

Die EU-Kommission hat uns angerufen. „Eine sehr freundliche, aber hartnäckige Pressesprecherin hat versucht, mich davon zu überzeugen, dass eigentlich der Europäische Rat und das EU-Parlament für OBFCM zuständig seien, vielleicht auch noch der deutsche Verkehrsminister Andreas Scheuer, aber nicht die Kommission“, erklärte pade luun während der Live-Gala. „Ich habe daraufhin Staatsrechtler, das Parlament und andere sachkundige Menschen kon-

taktiert und muss sagen: Wir liegen richtig. Die Kommission hat die Verordnung eingebracht. Parlament und Rat haben mitgearbeitet und dürfen sich mit abgemahnt fühlen. Aber letztendlich ist aus unserer Sicht die Kommission hauptverantwortlich. Und letztendlich bekommt die Kommission auch die Daten aus dem OBFCM.“

Frank Rosengart wurde während der Gala gefragt, seit wann diese Datensammlung eigentlich läuft. „Seit Anfang 2021 bereits wird die Verordnung auf alle Neuwagen angewandt. Die Daten werden also bereits gesammelt.“ Was noch unklar ist, sind die technischen Standards für die Übermittlung an die EU-Kommission. Das heißt: Bislang (Sommer 2021) sitzen die Autohersteller noch auf dem Datenschatz.

Bei der Social-Media-Frage danach, wie man Autos rooten oder stumm schalten könne (siehe oben), musste er schmunzeln. „Naja, wir haben ja bei Rena Tangens in der Laudatio (▶ Seite 97) gehört, wie das läuft. Es soll – wie in der DSGVO vorgeschrieben – die Möglichkeit geben, das OBFCM stumm zu schalten (Opt-Out). In der Realität sind das dann wahrscheinlich 77 Schieberegler, komplizierte Texte mit viel Kleingedrucktem und schlecht zu bedienen. Und wenn man dann alles abgewählt hat, bekommt man eine Meldung, dass einem womöglich wichtige Funktionen des Autos nach dieser Entscheidung nicht mehr zur Verfügung stehen. Und wer macht das dann noch?“



Leena Simon berichtet von Reaktionen bei Twitter und Mastodon

Foto: Infiac, cc by 4.0

Kategorie Bildung

Proctorio GmbH in München

Von Prof. Dr. Peter Wedde

Foto: Matthias Hornung, cc by 4.0



Laudator: Prof. Dr. Peter Wedde,
Frankfurt University of Applied
Sciences

Der BigBrotherAward 2021 in der Kategorie Bildung geht an die **Proctorio GmbH in München-Unterföhring**, für ihre KI-basierte Prüfungssoftware, die auch Proctorio heißt.

Der Name Proctorio leitet sich aus dem englischen Wort „Proctoring“ ab, das sich mit „beaufsichtigen“ übersetzen lässt. Proctorio geht es um „Online-Proctoring“, das heißt um die Beaufsichtigung von Prüflingen im Hochschulbereich per Internet.

Mit Blick auf dieses Geschäftsmodell war der Ausbruch der Corona-Pandemie Anfang 2020 für die Firma aus Marketingsicht ein absoluter Glücksfall:

Lehrende mussten aufgrund umfassender Lockdown-Maßnahmen und „Shut-downs“ geplante Präsenzprüfungen von einem Tag auf den anderen einstellen. Anreisen zu Klausuren mit öffentlichen Verkehrsmitteln stellten ebenso eine Gesundheitsgefahr dar wie der stundenlange Aufenthalt in einem Hörsaal. Studierende machten sich berechnete Sorgen um die Fortsetzung oder um den Abschluss ihres Studiums.

In dieser Situation wurden funktionierende technische Möglichkeiten für die Durchführung von Online-Prüfungen fast schon ebenso herbeigesehnt wie ein wirksamer Impfstoff gegen das SARS-CoV-2-Virus. Der optimale Zeitpunkt für das Angebot der Proctorio Software, die „vollautomatische und sichere Prüfungsaufsicht für Online Prüfungen“ ermöglichen soll, und die dabei laut Marketing-

Text „skalierbar, kostengünstig und DSGVO-konform“ (siehe Kasten) ist. Die Software soll nach Aussagen auf der Firmenwebsite eine täuschungsgeschützte Durch-

führung von Online-Prüfungen in den eigenen vier Wänden von Studierenden mit deren eigenen Geräten ermöglichen, ohne dass noch eine unmittelbare menschliche Aufsicht notwendig ist.

Aber für welchen Preis?

Die Software Proctorio greift tief in die Integrität der privaten Geräte der Studierenden ein. Um an Prüfungen teilnehmen zu können, müssen sie die Software auf ihren Computern installieren und Proctorio für die Dauer einer Prüfung die Kontrolle über ihr Gerät überlassen.



Foto: Frau: Panthermedia, cc by 4.0
Grafik: Dennis Blomeyer, cc by 4.0;

Während der Corona-Pandemie sahen viele Studierende die Fortsetzung ihres Studiums gefährdet.

Die Verwendung von Proctorio setzt zudem voraus, dass auf den Computern der Studierenden Google Chrome als Browser installiert ist. Dort werden von der Proctorio-Software zudem Drittanbieter-Cookies aktiviert, „um einen proaktiven Chat-Support“ anbieten zu können – über die US-amerikanische Firma OLARK.¹

¹ Quelle: „Proctorio FAQ für Studenten“, Seite 8, verlinkt über Jahrbuch-Webseite

An der „DSGVO-Konformität“ gibt es zahlreiche berechtigte Zweifel:

So ist beispielsweise an die Abgabe einer wirksamen freiwilligen Einwilligung der Studierenden in die Verarbeitung ihrer Daten mit der Software Proctorio angesichts der bestehenden „Zwangsprüfungssituation“ nicht zu denken.

Die Verarbeitung personenbezogener Daten von Studierenden für Zwecke der „Produktentwicklung“ als Auftragnehmer ist ohne ausreichende datenschutzrechtliche Grundlage.

Der Verweis auf ein „berechtigtes Interesse“ des Unternehmens Proctorio für die Verarbeitung von personenbezogenen Daten nach Art. 6 Abs. 1 lit. f) DSGVO verkennt das Überwiegen entgegenstehender Interessen, Grundrechte und Grundfreiheiten der Studierenden jedenfalls in den Fällen, in denen die Verwendung der Proctorio-Software für sie ohne Alternative ist.

An einer Onlineprüfung teilnehmen kann nur, wer Proctorio den Zugriff auf seine Videokamera ermöglicht. Diese muss während der gesamten Prüfungszeit eingeschaltet sein. Prüfende können entscheiden, ob sie Studierende während der Prüfung persönlich beobachten, oder ob die Software dies für sie erledigt. Und die Prüfenden können Proctorio den Start von Anwendungen und Downloads blockieren lassen oder Erweiterungen und individuelle Einstellungen sperren. Sogar „Copy and Paste“ kann grundsätzlich unterbunden werden. Und wenn Prüfende das wollen, muss zu Beginn der Prüfung ein „Raum-Scan“ durchgeführt werden, bei dem Prüflinge der Videokamera ihren gesamten Arbeitsraum vorführen müssen. Dieser „Raum-Scan“ muss auf Aufforderung während der Prüfung wiederholt werden.

► „Das System erkennt Anomalien durch vermehrte Blicke in eine Richtung und markiert diese Vorfälle als potenziell verdächtig.“ ◀

Und es kommt noch schlimmer: Hochschulen und Lehrende als potentielle Kunden werden von Proctorio mit dem Argument umworben, dass bei der

Klausurdurchführung eine „vollautomatische Kontrolle“ möglich ist. Die Software wertet dafür die eingehenden Videoinformationen mit „künstlicher Intelligenz“

aus und soll auf dieser Grundlage erkennen können, ob sich eine weitere Person im Raum aufhält.

Hinzu kommt eine von Proctorio als „Gesichtserkennung“² bezeichnete Analyse der Augenbewegungen. Hierzu schreibt die Firma: „Das System erkennt Anomalien durch vermehrte Blicke in eine Richtung und markiert diese Vorfälle als potenziell verdächtig.“³ Weiter heißt es dort wenig später: „Das bedeutet nicht, dass Sie bei Denkpausen nicht wegsehen dürfen. Solange Sie keine Hilfsmittel verwenden, müssen Sie keine Bedenken haben.“⁴

Wie gnädig, dass die Proctorio-Software Denkpausen

Foto: Adobe Stock



Auf Verlangen müssen Studierende den Prüfenden per Webcam ihre privaten Räume zeigen.

2 Quelle: „Proctorio FAQ für Studenten“, Seite 5.

3 Ebenda, Seite 5.

4 Ebenda, Seite 5.

erlaubt! Allerdings tragen die Studierenden auch hier das volle Risiko, falls die Software das doch irgendwie verdächtig findet.

Im Automatikmodus wird das beobachtete Verhalten der Prüflinge mit den Mustern abgeglichen, die in der Software als „Normverhalten“ hinterlegt sind. Findet sie das beobachtete Verhalten in Ordnung – was immer das bedeutet – werden die vorhandenen Aufzeichnungen im Regelfall nach dreißig Tagen durch Proctorio gelöscht. Gibt es hingegen Auffälligkeiten, können die Prüflenden sich die entsprechenden Videos

► **Automatisierte
Bewertungen des menschlichen Verhaltens sind
immer bedenklich.** ◀

anschauen. Damit entscheidet im Automatikmodus allein die sogenannte „Künstliche Intelligenz“ von Proctorio darüber, ob ein Täuschungsverdacht besteht. Ganz selbstständig.

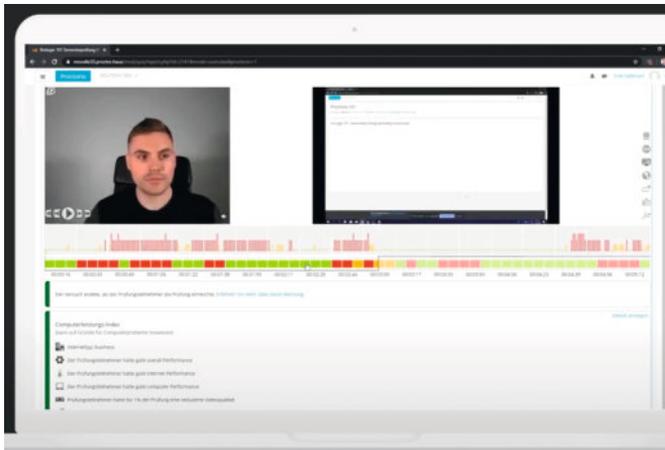
Derartige automatisierte Bewertungen des menschlichen Verhaltens sind immer bedenklich. Im Schul- und Hochschul-

bereich sollte die Aufhebung der Unschuldsvermutung durch Formen der „automatisierten Verdachtsbeurteilung“ schon

mit Blick auf die hier verfolgten pädagogischen Ziele und auf die zu vermittelnden Grundwerte vollständig tabu sein. Und für viele Studierende trägt es zur

Erhöhung ihres persönlichen Klausurstresses bei, wenn sie stundenlang Auge in Auge mit einer Kamera arbeiten müssen, ohne zu wissen, ob ihr aktuelles Verhalten gerade den Argwohn eines Prüfers oder einer Software erregt.

Ich bin seit rund fünfundzwanzig Jahren Hochschul-lehrer und habe in dieser Zeit sehr viele Klausuren beaufsichtigt und viele mündliche Prüfungen abgenommen. Deshalb



Screenshot: youtube-Video

Screenshot: Proctorio kennzeichnet in rot die Strecken des Prüfungsvideos, in denen die KI „verdächtige“ Verhaltensweisen erkannt haben will.

und deshalb

Foto: Matthias Hornung, cc by 4.0



„Hochschullehrer können Druck rausnehmen und Brücken bauen. Maschinen erkennen kein Lampenfieber.“ (Peter Wedde)

weiß ich, dass Prüfungs- und Klausursituationen für viele Studierende unabhängig vom fachlichen Leistungsstand sehr anstrengend und vielfach angstbesetzt sind. Bei einer Präsenzklausur können Prüfende Stress und Ängste von Studierenden oft durch ein paar freundliche aufmunternde Worte abbauen. Und ich finde es nie verdächtig, wenn jemand beim Nachdenken den Blick schweifen lässt – solange das Ziel nicht der Text von Sitznachbarn ist. Gleiches gilt in mündlichen Prüfungen, wo schnell zu erkennen ist, ob Studierende eine Antwort nicht wissen, oder ob ihnen vor Aufregung nur die Worte fehlen. Prü-

fende können in Präsenzsituationen Druck rausnehmen, Brücken bauen oder mit einer zulässigen Andeutung ermuntern. Eine Maschine kann hingegen nur Algorithmen abarbeiten und erkennt nicht, ob jemand seinen Blick nachdenklich schweifen lässt oder mit der Intention, eine Lösung abzuschreiben.

Auf der Grundlage dieses Wissens hätte ich vor der Corona-Pandemie der massenhaften Durchführung von beaufsichtigten Online-Klausuren ebenso wie viele meiner Kolleginnen und Kollegen vehement widersprochen. Dass wir trotz großer grundsätzlicher Bedenken in dieser besonderen Situationen Online-Klausuren zugelassen haben, heißt aber nicht, dass das jetzt ein Normalfall geworden ist. Für alle Standardfälle müssen Hochschulen „nach Corona“ wieder zurück zu Präsenzsituationen kommen. Und wo



Online-Prüfungen mit Rundum-Überwachung sind ein großer Stressfaktor für Studierende.

Collage : Dennis Blomeyer, cc by 4.0 (Panthermedia, Wikimedia)

Online-Klausuren oder Online-Prüfungsgespräche sinnvoll sind, müssen sie unter der Aufsicht von Menschen stattfinden, die Blicke nicht nur erfassen, sondern auch verstehen können.

Eine Software wie Proctorio hat kein Verständnis für Studierende, sondern prüft, ob ihr Verhalten dem entspricht, was andere Menschen als „normal“ definiert haben. Studierende in den USA, wo Proctorio an einer Reihe von Hochschulen im Einsatz ist, berichteten in der *Washington Post*⁵, das Programm habe bereits Verdacht geschöpft, wenn sie während einer Prüfung ungewöhnlich oft den Kopf, die Augen oder die Maus bewegt haben. Verdächtig war auch, dass sie „zu oft“ gescrollt, geklickt oder Fenstergrößen verändert hatten. Was immer diese Erkenntnisse auch aussagen sollen. Als „abweichend“, „abnormal“ und „auffällig“ hat die Software auch bewertet, dass Studierende früher oder später als andere fertig waren. Manche Studierende haben berichtet, dass sie sich aus Angst, dafür einen Betrugsversuch vorgeworfen zu bekommen, nicht getraut hätten, den Raum für eine Toilettenpause zu verlassen. In ihren eigenen vier Wänden.

Und wer zudem das Pech hatte, die Prüfung in einem Raum durchzuführen, in dem es viele Außengeräusche, eine langsame Internetverbindung, schlechtes Licht oder eine flackernde Kamera gab, über den generierte die Software ebenfalls einen Hinweis an die Prüfenden. Um derartige Einflussfaktoren auszuschließen, rät Proctorio Studierenden bezüglich der Auswahl eines geeigneten Raums in seinen „FAQ für Studierende“ übrigens: „Überlegen Sie sich im Vorfeld, welchen Raum Sie für die Prüfung verwenden möchten. Sie können Ihre Prüfung auch an einem Ort absolvieren, bei dem sie genügend Ruhe gewährleisten können (z. B. Büro).“⁶ Mit Blick auf die schwierige finanzielle Situation, in der viele Studierende sich seit Beginn der Pandemie befinden, ist das schon ziemlich zynisch.



Foto: K. Ijaaa, cc by-sa 3.0

In der Pandemie ist Protest von Studierenden auf der Straße nicht zu erwarten – nicht zuletzt fehlt es an Alternativen zu Online-Prüfungen.

⁵ Link zum Artikel auf der Jahrbuch-Website

⁶ Quelle: „Proctorio FAQ für Studenten“, Seite 3.

In Normalzeiten wäre zu erwarten, dass Studierende gegen die Planung einer solchen „Rundum-Totalkontrolle“ protestieren und auf die

Straße gehen würden. Aber wir haben eine Pandemie. Proteste und Versammlungen sind deshalb schwierig zu organisieren. Zudem geht es Studierenden verständlicherweise vor allem darum, mit ihrem Studium irgendwie voran und durch zu kommen. Da nehmen sie Online-Prüfungen in Kauf, zumal, wenn es keine Prüfungsalternativen gibt.

Aber vielleicht sind uns die Studierenden in den USA ja nur etwas voraus. Dort hagelte es Proteste bei Proctorio und in den sozialen Medien. In Deutschland erweckt hingegen unser Preisträger, die Proctorio GmbH in München, den Eindruck, Hochschulen, Lehrende und Studierende seien einhellig voll des Lobes. Glaubt man den Pressemitteilungen des Unternehmens, muss es Scharen von online-prüfwilligen Studierenden geben, die im Chor rufen „Aber das ist doch alles gut so. Dann werden doch ehrliche Studierende belohnt und die unehrlichen von der Software entdeckt.“

Ich will als Hochschullehrer auch gar nicht in Abrede stellen, dass Online-Klausuren von zu Hause aus für Studierende attraktiver und bequemer sein können als in einem Hörsaal in der Hochschule. Wer aber Online-Klausu-

**„abweichend“
„abnormal“
„auffällig“**

zu viele Kopf-, Augen-,
Mausbewegungen

zu oft gescrollt, geklickt,
Fenstergrößen verändert

früher oder später als
andere fertig



viele Außengeräusche

langsames Internet

schlechtes Licht

flackernde Kamera

**Hinweis an die
Prüfenden**

Keine Bewegung,
kein Umgebungsereignis bleibt
unbemerkt.

Foto: HAL9000: Wikimedia cc by 3.0 Grafik: Dennis Blomeyer, cc by 4.0;

ren zum Standardfall macht, der nimmt in Kauf, dass Bildungsgerechtigkeit und Chancengleichheit auf der Strecke bleiben. Wer Online-Prüfungen in einem kleinen WG Zimmer auf seinem altersschwachen Notebook schreibt und dabei mit lauter Musik aus dem Nachbarzimmer beschallt wird, dessen Erfolgchancen sind in der Regel schlechter als die eines Studierenden, der über ein technisch gut ausgestattetes Arbeitszimmer in einer ruhigen Wohngegend verfügt. Dies gilt erst recht, wenn die Proctorio-Software genervtes Umherblicken oder laute Nebengeräusche verdächtig findet und Prüfende veranlasst, hier noch einmal genauer hinzusehen.

Wir halten fest

- ▶ Die Nutzung von Proctorio für die Beaufsichtigung von Online-Prüfungen führt zu einem schweren Eingriff in die Integrität der privaten Geräte der Studierenden.
- ▶ Die permanente Videoüberwachung der Prüflinge während der Prüfungs-



Grafik: Dennis Blomeyer, cc by 4.0;
Laptop: Pixabay / Cookies: „Icon made by Freepik from
www.flaticon.com

zeit ist ein schwerer Eingriff in ihre Privatsphäre und in ihre privaten Räume – insbesondere, wenn ein Raum-Scan stattfindet.

- ▶ Die von der „KI“-Software durchgeführten automatischen Analysen ihres Verhaltens sind für die betroffenen Studierenden nicht transparent. Die allgemeine Unschuldsvermutung, die für alle Bürger gilt, wird durch die verwendeten Algorithmen und die hieraus folgende intransparente Kontrolle außer Kraft gesetzt.
- ▶ Die Gestik und insbesondere Augenbewegungen werden permanent erfasst und ausgewertet. Die Software kann hieraus negative Schlussfolgerungen ziehen, was den Druck und den Stressfaktor für die Studierenden erhöht.
- ▶ Online-Prüfungen zu Hause finden manche Studierende sicher angenehm. Sie gefährden aber aufgrund

ungleicher Wohn- und Lebensverhältnisse die Chancengleichheit, die bei der Ablegung von „Präsenzprüfungen“ hergestellt werden soll.

- ▶ Das Einsparpotential, das Proctorio für automatisierte Prüfungsaufsichten verspricht, macht die Software für kostenbewusste Hochschulen attraktiv. Diese Einsparung geht aber auf Kosten der Studierenden, die mit klassischen Präsenzprüfungen besser zurechtkommen als mit Online-Prüfungen unter den Augen einer Software.
- ▶ Die Datenschutzkonformität ist schon deshalb zweifelhaft, weil belastbare Aussagen zur Rechtsgrundlage fehlen und eine „freiwillige Zustimmung“ der Studierenden in Prüfungssituationen wohl eher nicht gewährleistet ist.

Gründe genug für den BigBrother-Award in der Kategorie Bildung. Herzlichen Glückwunsch, Proctorio GmbH.

Wie es weiter ging

Von Claudia Fischer

Kommentare unseres Publikums via Twitter und Mastodon:

- ▶ „Da kann man sowas von froh sein, das Studium schon lange hinter sich zu haben. Und auch als Lehrende hätte ich auf keinen Fall mit meinem Gewissen vereinbaren können, sowas wie Proctorio einzusetzen.“
- ▶ „Frage mich, wie sich Studierende eigentlich wehren können. Eine Software mit so vielen Zugriffen auf den Rechner heißt doch Malware.“

▶ In bester Gesellschaft

Wir sind nicht die einzigen, die Proctorio für extrem bedenklich halten. Der Datenschutzbeauftragte des Landes Baden-Württemberg, Dr. Stefan Brink, bezeichnete Proctorios Versprechen, Betrugsversuche an der Mimik der Studierenden zu erkennen, als „Hokuspokus“ (Quellen verlinkt über die Jahrbuch-Webseite).

Die Gesellschaft für Freiheitsrechte hat beim IT-Sicherheitsexperten Mike Kuketz ein Gutachten über Proctorio in Auftrag gegeben, das im Juli 2021 veröffentlicht wurde. Demnach bestehen erhebliche Sicherheitsrisiken durch den Zugriff der Proctorio-Software auf die Rechner der Studierenden. Zum Beispiel kann die Zwischenablage ausgelesen werden – in der Studierende womöglich noch kurz vor der Prüfung Passwörter und Zugangsdaten abgelegt haben, um sich in ihr Online-Banking einzuloggen. Die

Gesellschaft für Freiheitsrechte hat die Fernuni Hagen bereits für den Einsatz der Proctorio-Software verklagt.

Während der BBA-Gala fragte ein Social-Media-Nutzer, ob man die Software nicht einfach austricksen könne. „Ja sicher kann man das“, antwortete Peter Wedde. „Eine Möglichkeit ist zum Beispiel, den Laptop vorab mit einem Bildschirm im Nebenraum zu verbinden, so dass kluge Menschen im Nebenraum die Aufgaben sehen und Lösungen nachschlagen können. Über einen kleinen Knopf im Ohr können sie dann unbemerkt soufflieren. Einen anderen Trick kennen wir aus Krimis: Man zeichnet sich selbst in konzentrierter Haltung einige Zeit auf, während der Prüfung fällt ein Stift runter, man bückt sich und spielt dem System die Aufzeichnung vor. Ist die Aufzeichnung vorbei, fällt der Stift nochmal runter und das Live-Bild ist wieder da. Und ich wette, findigen Menschen fällt noch viel mehr dazu ein.“

„Liebe Studis,
bitte nicht
nachmachen!“



Bild: public domain

Kategorie „Public Intellectual“

Prof. Dr. phil. Dr. h. c. Julian
Nida-Rümelin

Von padeluun



Foto: Infliac, cc by 4.0

Laudator padeluun, Digitalcourage

Der BigBrotherAward in der Kategorie „Public Intellectual“ geht an

den Philosophen und stellvertretenden Vorsitzenden des Deutschen Ethikrats, Prof. Dr. phil. Dr. h. c. Julian Nida-Rümelin, für seine öffentlich mehrfach geäußerte unhaltbare Behauptung, dass „der Datenschutz“ die Bekämpfung von Corona erschwert und Tausende von Toten zu verantworten habe.

Natürlich benötigen die Missklänge um die Corona-Pandemiebekämpfung einen Widerhall bei den BigBrotherAwards. Und ich habe lange gebraucht, um zu entscheiden, welchen Namen ich hier

als Preisträgerin oder Preisträger nennen möchte. Über Coronapolitik, Sinn und Unsinn gibt es eine Menge zu sagen – was leider auch viele tun. Da komme ich auch noch zu.

Aber erst einmal meine Begründung, warum ich über Herrn Nida-Rümelin wirklich erzürnt bin.

Er sagte und wiederholte die Ansicht, dass (ich fasse da mal zusammen) „in Deutschland der Datenschutz eine vernünftige Warn-App verhindere. Anders als in Südkorea, wo man die Pandemie mit Apps ohne Datenschutz super in den Griff bekommen habe“.

Der Journalist Markus Bekkedahl bezeichnete diese Sichtweise als „Talkshow-Mythos“¹. Demnach wird die App in Südkorea nämlich vor allem dazu eingesetzt, um die Quarantänebestimmungen einzuhalten, weniger dazu, um Infektionsketten nachzuverfolgen und zu unterbrechen. Und der Blogger Linus Neumann, der hier an dieser Stelle auch schon einmal eine Laudatio gehalten hat, ergänzt²: „Die südkoreanische App hatte Ende Juli ein schweres Datenleck und Südkorea kämpft gerade mit der zweiten Welle. Einen Ausbruch im August hat Korea hingegen unter Kontrolle gebracht – mit einem Lockdown. Auch dieser ‚Erfolg‘ kann also nicht als argumentative Grundlage dienen für das, was Nida-Rümelin behauptet.“

Auch sonstige Behauptungen Nida-Rümelins zerpfückt Linus Neumann genüsslich in seinem Blog³.

Was treibt einen anscheinend klugen Mann wie Nida-Rümelin dazu, sich im



Screenshot: ardmediathek.de

► „Leider hat der Denker diese Chance nicht zum Denken genutzt.“ ◀

Fernsehen, Radiosendungen, in Zeitungen dazu auszulassen, dass der Datenschutz „Tausende Corona-Tote zu verantworten hätte“? Wie klein muss sein großer Geist sein, damit der ihm nicht noch mal eine Warnung zuflüstert, bevor er so eine offensichtliche Dummheit in die Welt hinausruft?

Herr Nida-Rümelin ist Philosoph, Politiker, ehemaliger Kulturstaatsminister, stellvertretender Vorsitzender des Ethikrats. Dortselbst ist er Pressesprechpartner für Digitalisierung.

Schon im Mai letzten Jahres ließ er sich auf SWR1⁴ aus. Im September 2020 haben wir das für die BigBrotherAwards noch ignoriert. „Don’t make stupid views famous.“ Leider hat der Denker Nida-Rümelin diese Chance nicht zum Denken genutzt. Bei der Unterhaltungssendung „Anne Will“⁵ im Dezember 2020 wieder-

1 Quelle: SWR-Podcast 14.12.2020

2 Quelle: Linus-Neumann.de 23.12.2020

3 Quelle: ebenda

4 Quelle: SWR1 Leute, 15.5.2020

5 Quelle: Anne Will, ARD, 13.12.2020

holte er seine falschen Parolen gegen den Datenschutz.

Und dann, im März 2021 – da waren alle Fakten, auf die er sich gestützt hatte, längst komplett widerlegt – verbreitete er seine alternativen Meinungen erneut, diesmal über die Deutsche Presseagentur. Da dachte ich dann wirklich: Ach, Philosoph, hättest Du doch geschwiegen ...

Nein, Julian Nida-Rümelin und Ihr anderen „Anti-Datenschutz“-Apologeten: Datenschutz tötet nicht. Datenschutz ist die dünne Membran, die uns alle vor der Barbarei staatlicher und kommerzieller Übergriffigkeiten schützt.

Datenschutz, beziehungsweise ‚Informationelle Selbstbestimmung‘, beziehungsweise „Menschenschutz“, vom Bundesverfassungsgericht 1983 aus den ersten zwei Artikeln des Grundgesetzes abgeleitet (► Seite 164), seit der Inkraftsetzung der Datenschutzgrundverordnung ein weltweiter Innovationsmotor, ist ein Thema, das wie kein anderes das geschulte philosophische Denken fordert, weil diese verdammte



Foto: Panthermedia, cc by 4.0

„Ach, Philosoph, hättest Du doch geschwiegen...“ (padeluun)

► **Datenschutz ist die dünne Membran, die uns alle vor der Barbarei staatlicher und kommerzieller Übergriffigkeiten schützt.** ◀

digital vernetzte Welt nun mal nicht mit Hämmern und Nägeln vergleichbar und nicht mit mechanischen Modellen darstellbar ist. Wir haben in den vergange-

nen 4 Jahrzehnten die Darstellung unserer Welt und unsere Kommunikation darüber in Nullen und Einsen zerlegt. Es sind Stromschwankungen, die potenziell

an Millionen und Milliarden Orten bis hinein in den erdnahen Orbit und das Universum gleichzeitig kopiert werden – völ-

lig ohne dass das an der Ursprungsstelle erfahrbar ist.

Was das fürs Menschsein bedeutet, haben Sie, Herr Nida-Rümelin – genauso wie die anderen Schwachmaten, die zurzeit ein digitales Pro-Terrorgesetz nach dem anderen verabschieden – noch lange nicht durchdrungen. Darüber muss man nachdenken, bevor man den Erwachsenen reinredet. Da muss man zuhören, wenn die Erwachsenen drüber reden. Da muss man seinen Verstand gebrauchen, wenn man der Gesellschaft weiter helfen will.

(Ich bitte die Arroganz der vorstehenden Sätze zu entschuldigen: Sie sind meiner Verzweiflung geschuldet.)

Digitaler Menschen- und Gesellschaftsschutz braucht Präzision.

Ja, ich benenne das Wort Datenschutz jetzt mal zum besseren Verständnis um. Denn Datenschutz bedeutet nicht, dass Daten geschützt werden müssen – das wäre Datensicherheit – sondern, dass Menschen und Gesellschaft Schutz brauchen.

Also nochmal:

- ▶ Digitaler Menschen- und Gesellschaftsschutz braucht Präzision.
- ▶ Digitaler Menschen- und Gesellschaftsschutz braucht geschultes Denken.
- ▶ Digitaler Menschen- und Gesellschaftsschutz braucht Philosophie.
- ▶ Das denkt sich nun mal nicht so schnell zwischen Häppchen und Interview.



Bild: Panthermedia, cc by 4.0

Die digitale Welt ist nicht mehr unmittelbar erfahrbar

Ich erwarte von einem studierten und lehrenden Philosophen, dass er nicht einfach wie jeder andere dahergelaufene Verschwörungsheini undurchdachten Blödsinn in die Welt hinausbläst. Oder erwarte ich da einfach zu viel? Hat mir mein gefährliches Halbwissen von Platons Traum der „Philosophenherrschaft“ schon selbst den Ver-

stand vernebelt, so dass ich jetzt enttäuscht bin über meine Vorstellung von einer Denk-Elite, die nicht mehr als ungare Plattitüden ‚raushaut‘?

Ich möchte hier auf gar keinen Fall einer keimenden Intellektuellenfeindlichkeit das Wort reden. Im Gegenteil. Natürlich gehört es zum Beruf eines Philosophen, steile Thesen zu proklamieren – aber es gehört auch dazu, sich dem Diskurs zu stellen und diese Thesen prüfen und angreifen zu lassen, und aus dem Diskurs zu lernen. Und das Gelernte muss dann anschließend in neue Thesen eingebaut werden. Und dann, wenn man in vielen nervigen und beflügelnden Diskursen Festigkeit in seiner These erlangt hat, dann erst strebt man zu der großen Bühne und gibt das in die Gesellschaft, was die Gesellschaft als Gesamtes weiterbringt. Man wiederholt auf der großen Bühne nicht ein Jahr lang dumme Behauptungen – und schon gar nicht, wenn deren Faktenbasis inzwischen Stück für Stück komplett widerlegt worden ist.

Wumms.

Und jetzt frage ich mich, was mich selbst denn so von Herrn Nida-Rümelin unterscheidet (abgesehen davon, dass ich meinen Beruf als Künstler bezeichne). Ich stelle mich auch auf mehr oder

weniger große Bühnen und postulierte Erkenntnisse. Aber auch, wenn ich das nicht wahrhaben will, bin ich auch nur ein älterer Herr, der ab und an ganz schön sauer ist und durchaus das Mitteilungsbedürfnis hat, andere an dieser Mißstimmung – mit dem Ziel der Verbesserung – teilhaben zu lassen.

Wenn ich mich in der Corona-Diskussion umgucke, sehe ich eine Kakophonie von vielen Herren und ein paar Damen, die einem ihre Erkenntnisse und Ansichten mit Kraft der von ihnen genutzten Medien um die Ohren hauen möchten. Schulen auf? Ja! Schulen zu? Ja! Lockdown? Ist doch gar kein Lockdown! Alles zumachen! Alles aufmachen? Spahn macht alles falsch! Datenschutz stinkt! Die Luca-App ist Betrug! Du genderst falsch! IP-Nummern sind keine personen-ziehbaren Daten! Doch, sind sie! Corona ist eine Absprache des

World Economic Forums. Die wollen nur ID2020 durchbringen. Und Billionen über Impfungen einsacken. Putin ist ein lupenreiner Demokrat. Versammlungen sind grundsätzlich verboten. Das war doch nur satirisch gemeint!

In dieser Kakophonie hat Julian Nida-Rümelin als Denker mitgemacht. Und um es ganz schlicht auszudrücken: Er war nicht hilfreich.

► **Es gehört zum Beruf eines Philosophen, steile Thesen zu formulieren. Aber auch: Aus dem Diskurs zu lernen.** ◀

► **Wir können uns nicht in
Feuersbrünste werfen und
heldenhaft Frauen und
Kinder retten. Wir sind dazu
verdonnert, zur Seite zu
gehen und Fachleute
machen zu lassen.** ◀

Sollte ich Mitleid mit ihm haben, Verständnis zeigen? Ich kann es mal versuchen. Da stehen wir armen Toren, und ohne, dass es blitzt und donnert oder Asche regnet, bricht da eine Pandemie aus. Wir können sie nicht riechen, nicht schmecken. Wir können uns nicht in Feuersbrünste werfen und heldenhaft Frauen und Kinder retten. Wir sind dazu verdonnert, zur Seite zu gehen und Fachleute machen zu lassen.

Er und ich sind keine Pandemiefachleute.

Deshalb interessiert sich auch niemand für uns. Wir sind gar nicht gefragt. Das einzige, was ich Leuten hätte sagen können, war: Ich habe wissenschaftlich arbeitende Menschen in meinem Freundeskreis, die können Statistik verstehen und die sagten mir zu Beginn der Pandemie: Bunker Dich erst mal ein. Zumindest, bis weitere Informationen da sind.

Und dann hat man ein bisschen Zeit, um das Seuchenschutzgesetz zu lesen. Dann versteht man den gesetzlichen Auftrag des RKI. Versteht plötzlich den Unterschied

zwischen Katastrophen- und Bürgerschutz. Man weiß dann, dass Seuchenschutz Länderrecht ist. Und dann entdeckt man, dass die Gesundheitsämter überhaupt nicht für die Bewältigung einer Pandemie aufgestellt sind. Dass in den vielen Jahren Gesetzgebung nichts getan wurde, um einer Pandemie zu begegnen. Aber es wurde ein schwach-sinniges Gesetz nach dem anderen für



„Und dann entdeckt man, dass die Gesundheitsämter überhaupt nicht für die Bewältigung einer Pandemie aufgestellt sind.“ (padelun)

Foto: Matthias Hornung, cc by 4.0

► „Aber der Datenschutz ist schuld? Ja?! Echt mal!“ ◀

den Fetisch „für mehr Sicherheit“ gemacht. In den Gesundheitsämtern sitzen sie mit Papier und Bleistift, Faxgeräten und Wählscheibentelefonen und schaffen es nicht, die Informationsmengen und Anforderungen, die auf sie einströmen, zu bewältigen. Hier blicken wir auf mindestens 30 Jahre Staatsversagen. Und dann kam noch der Kanzlerkandidatsmachtkampf der CDU dazu, der nicht hilfreich war. Weil unter dem Eindruck dieses Machtkampfes nie klar war, welche Maßnahme wirklich sinnvoll war und welche nur den Gockeleien geschuldet war ...

Aber der Datenschutz ist schuld? Ja?! Echt mal!

Ich weiß nicht, ob jemand hier im Raum mal auf einer „Corona-Leugner“-Demo

war. Ich war es. Ich habe meinen Presseausweis eingesteckt, meinen

Mundschutz aufgesetzt, und ich habe dort mit vielen Leuten gesprochen. Menschen, wie du und ich. Menschen, bei denen ich mir auch vorstellen konnte, dass sie auf einer unserer Demos mitlaufen könnten. Aber auch Menschen, denen geistige Führung fehlt, um eigenständig sein zu können. Die durch das, von dem sie denken, dass es Korruption sei, dieses Haudrauf-Gesetzemachen ohne Sinn und Verstand, so verunsichert sind, dass sie zu der nächstbesten wohlfeilen Erklärungsalternative greifen.

Ich kann es ihnen nicht wirklich verdenken. Zumal immer mehr Verwirrprofis Morgenluft wittern und nicht nur die dummen Klugen, sondern nun auch die

bösen Schlaun mitspielen im Verwirrspiel. Die Leute da sind (mal von den komplett Verstrahlten abgesehen) wirklich überzeugt von ihren Einstellungen, von ihren Zweifeln und den ‚alternativen‘ Informationen, die sie sich einver-

leibt haben. Das sind die Menschen, die von denen, die fürs Denken bezahlt werden, allein gelassen worden sind. Nicht nur allein gelassen: Sie wurden dem



Corona-Maßnahmen-Kritiker:
„Menschen, bei denen ich mir auch vorstellen konnte, dass sie auf einer unserer Demos mitlaufen könnten.“
(padeluun)

strukturellen Populismus⁶ der sozialen Hetzwerke ausgeliefert. Allein gelassen nicht nur von Herrn Nida-Rümelin, sondern auch von den anderen Herren (und Damen) seines Kalibers.

Deshalb haben wir auch die Kategorie „Public Intellectual“ eingeführt – weil wir eigentlich so dringend Menschen brauchen, die denken können und anderen damit Wege weisen. Wie bitter, wenn Menschen wie Herr Nida-Rümelin diesen Auftrag so schändlich für billigen Populismus verraten.

Viele haben in dieser verfluchten Corona-Pandemie mit den notwendigen Einschränkungen von Freizügigkeit und existenzbedrohenden finanziellen Verlusten hier und da Dinge von sich gegeben, die man bei klarem Verstand so nicht gesagt hätte. All denen gegenüber müssen wir Barmherzigkeit walten lassen. Den Schauspielern, die sich jetzt für ihre komische Aktion schämen. Und den Leuten, die als Querdenker:innen ein paar gewissenlose Hetz-Trolle reich gemacht haben. Und die dabei nicht gemerkt haben, dass der Gebrauch ihres eigenen Verstandes eine Zeitlang in die Irre geführt hat. Ihnen allen – auch Herrn Nida-Rümelin – möchte ich zurufen: Wer A sagt, muss nicht immer wieder A sagen. Man kann auch erkennen, dass A falsch war.

In diesem Sinne: Herzlichen Glückwunsch, Julian Nida-Rümelin, zum BigBrotherAward 2021.

⁶ FAZ, 14.3.2021

Wie es weiter ging

Von Claudia Fischer

Kommentare unseres Publikums via Twitter und Mastodon:

- ▶ „Ein hochverdienter Preisträger in der Kategorie „Intellectual Impropriety“ (man verzeihe die Verballhornung) und die Laudatio beim BBA21 ein Juwel. Chapeau. Gucken.“
- ▶ „padeluum, diese Leidenschaft, ich krieg Gänsehaut!“
- ▶ „Für Nida-Rümelin hätte ich auch eine neue Kategorie ins Leben gerufen.“
- ▶ „Überragende Rede von padeluum... Spitze!“
- ▶ „Echt klasse und sehr gut, padeluum, dass Du den Ver(w)irrten die Hand gereicht hast. <3 Das ist super, denn zu ihnen sollten Brücken aufgebaut werden.“

▶ Eine Antwort per Video

Prof. Julian Nida-Rümelin überraschte uns mit einer Videobotschaft. Und ein paar Tage nach der Preisverleihungsgala diskutierte er mit padeluum live im Radio bei Bayern 2.

padeluum: „Ich freue mich ganz grundsätzlich, dass Herr Nida-Rümelin anders als viele andere BBA-Preisträger:innen die Größe hat, mit mir in einen Dialog zu treten. Auch wenn er – leider, leider – von seiner Position nicht abrückt und auch auf meine Argumente wenig eingeht.“ Das Video, dass Herr Nida-Rüme-

ling uns geschickt hat, können Sie sich auf digitalcourage.video in voller Länge ansehen – bis zum Redaktionsschluss des Jahrbuches haben das schon über 200 Menschen getan.

Herr Nida-Rümelin bittet in seinem Video um Entschuldigung, dass er nicht kurzfristig selbst nach Bielefeld anreisen konnte, stellt sich kurz vor und nimmt zu padeluuns Kritik Stellung:

„Was jetzt hier inkriminiert wird, ist in der Tat meine Einschätzung, dass sich die Datenschutzpraxis, nicht die Gesetzgebung, in dieser Pandemie-Krise als dysfunktional erwiesen hat. Dass es uns nicht gelungen ist, die Gesundheitsämter durch digitale Aufrüstung instand zu setzen, das Infektionsgeschehen zurückzuverfolgen und damit den zweiten, dritten und möglicherweise weitere Lockdowns zu verhindern. Und dass die Verhältnismäßigkeit nicht beachtet worden ist. Wir haben Artikel 1, Menschenwürde, eingeschränkt, als wir alte Menschen sterben ließen, ohne dass sie noch besucht werden konnten. Wir haben Menschen ihren Job genommen, ihren Beruf genommen. Wir haben Eigentum vernichtet. Das war alles notwendig, weil nur mit Shutdown- und Lockdown-Maßnahmen eine Steuerung noch möglich war. Mir wäre es lieber gewesen, wir hätten die Gesundheitsämter digital auferüstet, hätten



Foto: Matthias Hornung, cc by 4.0

Prof. Julian Nida-Rümelin schickte uns vor der Gala eine Videobotschaft.

eine Corona-App etabliert, die nun wirklich nützlich ist für die Gesundheitsämter, hätten weniger Misstrauen gegenüber den Gesundheitsämtern gehabt und mehr gegenüber den ‚Big Five‘ aus dem Silicon Valley.“

padeluun:

„Herr Nida-Rümelin stellt hier Beziehungen zwischen Dingen her, die nichts miteinander zu tun haben. Ich kann mich nur wiederholen: Die Datenschutzpraxis ist nicht das Problem, sondern die nicht für eine Pandemie geeignete Ausstattung der Gesundheitsämter. Da geht es um ausreichend Computer und Bandbreite, um Software, Know-How und Menschen, nicht um die Datenschutzpraxis. Auch die Altenheime hatten kein Datenschutzproblem.

Zugegeben: Als Herr Nida-Rümelin die Videobotschaft schickte, kannte er den Wortlaut der Laudatio noch nicht. Aber auch nach der Gala, bei meinem Zusammentreffen mit ihm im Radio, muss ich sagen: Ich fürchte, er will immer noch nicht verstehen, worum es geht.“

Kategorie „Was mich wirklich wütend macht“

Von Rena Tangens



Foto: Matthias Hornung, cc by 4.0

Laudatorin: Rena Tangens,
(Digitalcourage)

Die Kategorie für diesen BigBrother-Award ist neu.

Sie heißt: „Was mich wirklich wütend macht!“

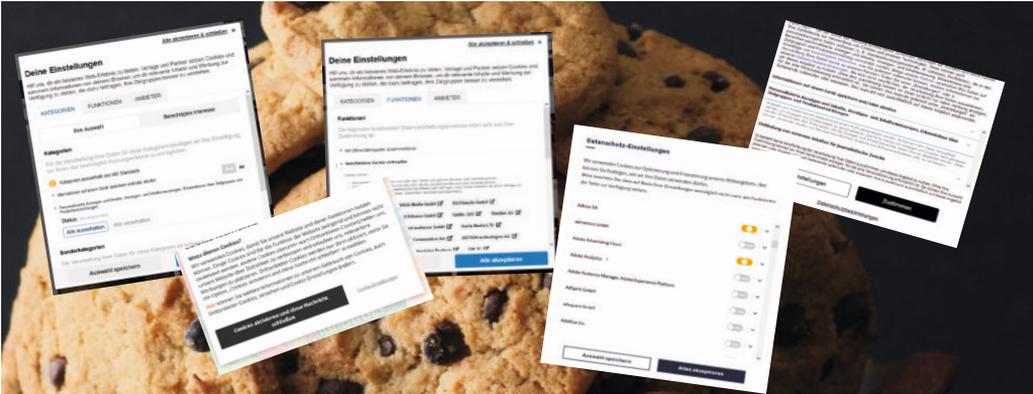
Und der diesjährige Preis geht an..... – ja, an wen eigentlich?

Das ist diesmal nicht so einfach. Werden Sie gleich sehen.

Also: Was mich wirklich wütend macht:

Cookie-Banner! Diese Pest! Sie kennen das: Sie rufen eine Webseite auf und – zack! – schon schiebt sich dieser Kasten mit unsäglich schlechtem Design über das, was Sie eigentlich sehen wollen. Dann müssen Sie sich entscheiden: Wollen Sie einfach nur schnell an die gewünschte Webseite, dann klicken Sie einfach auf den großen bunten Button „Okay“. Doch wenn Sie das mit Ihren Rechten ernst nehmen, dann wird es kompliziert. Augen zusammenkneifen, kleine graue Schrift auf weißem Grund lesen, und minutenlang alles einzeln wegeklicken, was Sie nicht wollen. Und das ist verdammt viel: 470 Tracker zum Beispiel alleine bei der Süddeutschen Zeitung. „Will ich alles nicht!“ wird Ihnen gar nicht erst angeboten. Und wenn Sie alle Tracker einzeln in mühsamer Handarbeit wegeklickt haben, dann passen Sie bloß auf, denn der nächste freundlich-bunte Button heißt „Alles zulassen“ und nicht „Meine Auswahl abspeichern“. Der ist grau. Aber Vorsicht – auch da sollten Sie nicht draufklicken. Denn vorher müssen Sie noch die meist gut verborgene Kategorie „Berechtigtes Interesse“ finden. Dort steht nämlich auch

Grafik: Isabel Wienold, cc by 4.0;
Cookies: Kiko Camaciang on Unsplash



alles auf „aktiviert“, und Sie müssen es wegklicken. Haben Sie's gewusst?)

Was mich daran wirklich wütend macht:

Diese Cookie-Dialoge sind nach den neuesten Erkenntnissen über menschliche Wahrnehmung, Psychologie und Webdesign für ergonomisch ansprechende Webseiten gestaltet. Also:

- ▶ Wichtige Handlungsoptionen werden im Fließtext versteckt, während das „ok“ auf einem fetten Button thront.
- ▶ Sie werden in unlesbaren Farben und Schriftgrößen angezeigt.
- ▶ Der „Alles zulassen“-Button steht unten rechts – wo wir eigentlich die Bestätigung unserer Auswahl erwarten.
- ▶ Bei vielen Schaltern ist die rechts-links-Position vertauscht: Wenn ich dort klicke, wo ich vorher Tracker deaktiviert habe, werden mit dem Zentral-Schalter plötzlich alle wieder aktiviert.
- ▶ Und dann gibt es noch sprachliche

„Cookie-Banner sind eine Pest!“
(Rena Tangens)

Ungetüme, komplizierte Formulierungen und mehrfache Verneinungen, um uns maximal zu verwirren.

Diese Art der Trickserei bei der Gestaltung wird „Dark Patterns“ genannt – wörtlich: „dunkle Muster“. Man könnte sie auch „betrügerisch“, „unethisch“ oder „Manipulation by Design“ nennen.

Wenn wir gute Laune haben – und viel Zeit – können wir das Ganze auch als schräges Spiel betrachten – ein Dark-Pattern-Adventure: Schaffe ich, durch



Grafik: Dennis Blomeyer, cc by 4.0;



Grafik: Isabel Wienold, cc by 4.0;
Cookies: Mae Mu on Unsplash;
Labyrinth: Panthermedia

das Labyrinth zu kommen und alle Tracker abzulehnen? Was versuchen sie jetzt noch, um mich auszutricksen? Und wenn ich durchgekommen bin: Was war eigentlich nochmal der Artikel, den ich gerne lesen wollte? Ach egal...

Cookie-Banner sind kein Spiel. Sie sind armselig und niederträchtig. Sie klauen mir meine Lebenszeit. Dieses Design will mich ermüden und zermürben. Es will, dass ich aufgebe und schließlich „ok“ drücke.

Und jetzt einmal zum Mitschreiben: Nein, der Datenschutz ist nicht schuld! Nein, diese nervenden Abfragen sind vom Gesetz keineswegs so vorgeschrieben

Schaffe ich es, durch das Labyrinth zu kommen und alle Tracker abzulehnen?

– vielmehr ist ein Großteil der Cookie-Banner schlicht illegal. Die von Max Schrems¹ initiierte Datenschutzorganisation noyb.eu² hat Ende Mai 2021 mehr als 500 Beschwerden an Unternehmen verschickt, die auf ihrer Website rechtswidrige Cookie-Banner verwenden. Es könnten eine Menge mehr werden. Danke dafür! Ebenso Dank an die EU-Abgeordneten, die die Initiative „trackingfreeads.eu“³ gegen personalisierte Werbung gestartet haben.

Dabei sind Cookie-Banner nur die sichtbare Materialisierung davon, wie wir im Internet ausgespäht werden.

Neben Cookies gibt es nämlich noch etliche andere Ausspäthmethoden. Das Facebook-Pixel zum Beispiel, das

Foto: Matthias Hornung, cc by 4.0



Max Schrems bei den BigBrotherAwards 2015

1 Max Schrems hat schon 2015 hier bei den BigBrotherAwards auf der Bühne gestanden und hat als Gastlaudator unseren Innenministern die Leviten gelesen, weil sie – während sie eifrig das Gegenteil behaupteten – versuchten, das europäische Datenschutzrecht zu schwächen.

2 noyb.eu – none of your business noyb.eu/de

3 Quelle: trackingfreeads.eu

► „Es beginnt eine Auktion um Ihre Aufmerksamkeit. Sie sind die Ware.“ ◀

unsichtbar auf vielen Medienseiten⁴ eingebunden ist und unser Klickverhalten an Facebook verpetzt. Den Browser-Fingerabdruck, der Informationen über Betriebssystem, Browser, Plugins und installierte Schriften nutzt, um uns ganz ohne Cookies wiederzuerkennen.

Was mich wirklich wütend macht:

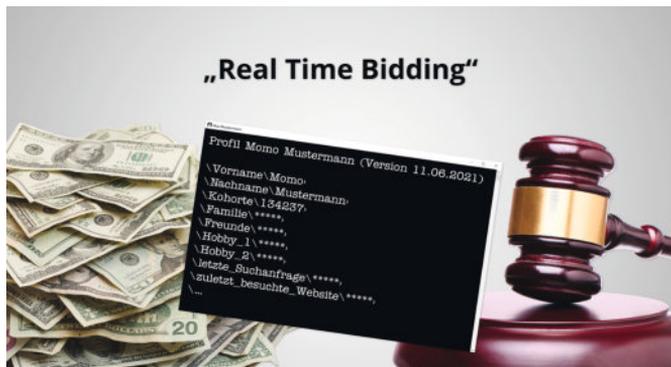
Wissen Sie, was im Hintergrund passiert, wenn Sie eine Website „betreten“? Während die ersten Teile der Webseite laden, wird im Hintergrund Ihr persönliches Profil auf dem Werbemarkt feilgeboten. Es beginnt eine Auktion um Ihre Aufmerksamkeit. Sie sind die Ware. Das nennt sich „Real-Time-Bidding“, geschieht in Millisekunden. Verschiedene Gruppen von Online-Werbefirmen identifizieren, analysieren und kategorisieren Sie anhand Ihres Online-Profiles, das wieder andere Werbefirmen verwalten. Nehmen wir mal an: Sie sind ein Mann, Mitte 40, mögen teure Uhren? Schwupps, zeigt Spiegel Online Ihnen BMW-Werbung. Oder die Studentin, die

eben nach WG-Zimmern gesucht hat, versucht man direkt mit nur vermeintlich günstigen Kreditangeboten zu ködern.

Beim „Real-Time-Bidding“ zockt ein ganzes Ökosystem von Werbefirmen darum, wer Ihnen seine Werbung zeigen darf. Ein gigantisches Netzwerk von Dienstleistern und Mit-Verdienern. Und die, die das Internet interessant machen, die Zeitungsverlage, Blogs, Inhalte-Lieferanten, bekommen am wenigsten vom Kuchen ab.

Was mich dann noch wirklich wütend macht, ...

... sind die Leute, die rufen: Aber dafür sind doch die ganzen Inhalte gratis. Gratis? Hm – Ausforschung und Manipulation im Netz ist ein ziemlich hoher Preis für dieses „Gratis“, finde ich. Dann



Beim Real-Time-Bidding zockt ein ganzes Ökosystem von Werbefirmen um Ihre Daten.

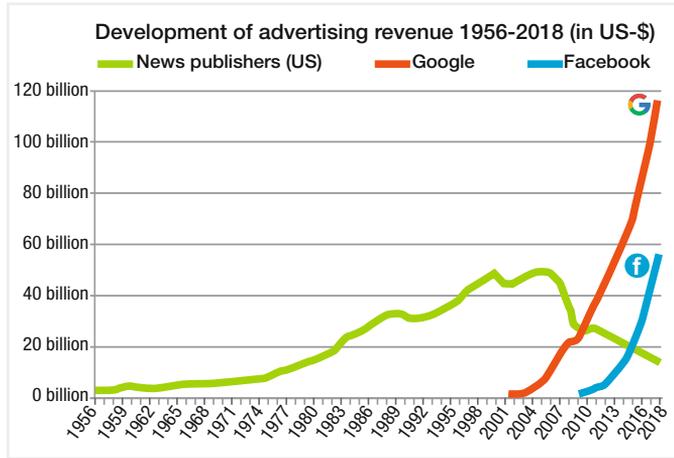
Gratifik: Dennis Blomeyer, cc by 4.0;
Fotos: Panthermedia

⁴ Wie zum Beispiel Zeit Online – unser BigBrother-Awards-Preisträger des Jahres 2019. Link zur Laudatio siehe Jahrbuch-Webseite

wird behauptet: Die Medien, die die interessanten Inhalte produzieren, könnten ohne personalisierte Werbung gar nicht existieren. Das müssten wir doch einsehen und deshalb Tracking und personalisierte Anzeigen akzeptieren.

Das ist Quatsch. Medien haben auch früher schon Anzeigenplatz verkauft. Allerdings haben sie dabei bis in die 1990er-Jahre den größten Teil der Einnahmen auch tatsächlich selber erhalten und konnten damit Journalisten, Fotografinnen, Zeichner, Rechercheurinnen etc. korrekt bezahlen. Seit den 2000er-Jahren sind die Einnahmen der Medien im freien Fall. Denn inzwischen kommen 50-70% (!) des Geldes, das die Anzeigenkunden ausgeben, gar nicht mehr bei den Verlagen an, sondern landen bei den Dienstleistern und Werbepattformen, die sich dazwischen geschaltet haben.⁵

Und wo ist das Geld, das nicht mehr bei den Medien ankommt? Schauen Sie mal auf diese Grafik⁶ (oben rechts). Inzwi-



Gratik: mit freundlicher Genehmigung von trackingfreeds.eu

Und wo ist der ganze Gewinn, den die Nachrichtenseiten in den letzten 15 Jahren verloren haben?

► „Die Nutzer werden ausgehört – die Medien werden ausgehungert.“ ◄

schen im Wesentlichen bei Google. Und bei Facebook. Ich fasse zusammen: Personalisierte Werbung bedeutet: Die Nutzer werden ausgehört – die Medien werden ausgehungert.⁷

Was mich wirklich wütend macht:

Nun kommt Google als Ritter auf dem weißen Pferd daher und kündigt an: Chrome, der Google-eigene Browser, wird ab 2022 Third-Party-Cookies blockieren. Jubel im Netz und in den Medien: Google erlöst uns von den Cookie-Bannern!

Doch das Blockieren von Dritt-Party-Cookies heißt mitnichten, dass das Tracking und die Ausforschung im Netz auf-

⁵ Quelle für Zahlen: trackingfreeds.eu

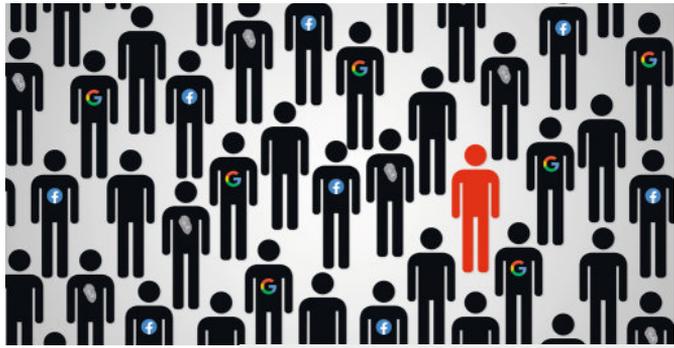
⁶ Quelle: trackingfreeds.eu

⁷ Quelle: Wall Street Journal, 29.5.2019

hören würde. Nein, Google will dafür einfach nur eine neue Technik einführen namens „FLoC“ – Federated Learning of Cohorts. FLoC

bedeutet: Wir werden nach unserem Browsing-Verhalten der letzten Woche einer Gruppe von ein- bis fünftausend Individuen zugeschlagen, die ähnliche Websites besucht haben. Die Zugehörigkeit zu der jeweiligen Kohorte speichert Chrome auf unserem eigenen Rechner.

Wer jetzt denkt, dann zumindest in der Gruppe der tausend anderen untertauchen zu können, irrt sich. Zum Beispiel ist eine Person, die sich auf einer Website einloggt, natürlich nicht mehr anonym. Und ihre persönlichen Informationen können mit der aktuellen FLoC-Kohorte verknüpft werden. Dasselbe gilt für alle, die einen Google- oder Facebook-Account haben und aus Bequemlichkeit ständig eingeloggt bleiben – auch die sind identifizierbar. Und schließlich können wir an unserem Browser-Fingerabdruck wiedererkannt werden. So sorgt FLoC dafür, dass wir in Zukunft noch genauer analysiert werden als bisher schon. Und der Chrome-Browser hat inzwischen einen Marktanteil von etwa 70% weltweit.



Grafik: Dennis Blomeyer, cc by 4.0;

Auch in einer ganzen Gruppe (Kohorte) von Menschen sind wir leicht eindeutig identifizierbar.

► „Eher glauben wir Piranhas, dass sie Veganer werden wollen.“ ◀

FLoC ist keine datenschutzfreundliche Technik. Es beendet keineswegs unsere Verfolgung im Netz – eher im Gegenteil⁸.

Aber wer könnte das auch ernsthaft von Google erwarten – einem Konzern, der 99% seines Umsatzes mit Werbung macht.

Eher glauben wir Piranhas, dass sie Veganer werden wollen.

Willkommener Nebeneffekt von FLoC und dem Blockieren von Third Party Cookies: Google bootet damit konkurrierende Werbeplattformen aus. Nicht, dass wir denen besonders nachweinen würden. Aber der Effekt wird sein, dass die

⁸ Die EFF fasst es so zusammen: „FLoC ist das Gegenteil einer datenschutzfreundlichen Technik. Während Ihnen heute noch Tracker durchs Web folgen, in den digitalen Schatten herumschleichen, um zu erraten, was für eine Art Person Sie wohl sind, werden die sich in Googles Zukunft zurücklehnen, entspannen und den Browser auf Ihrem Rechner die Arbeit für sich machen lassen.“ Übersetzung Rena Tangens, Quelle siehe Jahrbuch-Webseite

► „Was man als Big Tech-Konzern will, ist ein Monopol.“ ◀

Konzentration auf dem Werbemarkt noch weiter vorangetrieben wird.

Google ist dort schon die Nummer eins, dann folgt Facebook und inzwischen auch Amazon. Und dann kommt lange nichts mehr. „Competition is for losers“ – „Wettbewerb ist was für Verlierer.“⁹ Freier Markt? Ach was. Was man als Big-Tech-Konzern will, ist ein Monopol.

Was mich wirklich wütend macht:

Wie diese Konzerne mit uns umgehen. Wie sie Menschen nur noch als Rohstoff ansehen, den sie ausbeuten und deren persönliche Erfahrungen sie sich aneignen können. Die Verachtung für die Menschen, die Skrupellosigkeit und der Wille, sie über den Tisch zu ziehen. Die Verachtung fürs Steuerzahlen und für staatliche Infrastruktur. Und die Verachtung für geltendes Recht. Shoshana Zuboff hat ein Wort dafür gefunden: „Überwachungskapitalismus“.¹⁰

Es ist nicht nur eine einzelne Datenkrake – es ist ein ganzes krakiges Ökosystem. Dazu gehören die Versicherungen, die möglichst jedes Risiko für sich selber ausschließen wollen, die Scoring-Unternehmen, die uns geheime Noten geben, nach denen sich unsere Chancen im Leben richten, die Lobbyisten, die Think Tanks, die PR-Agenturen, die Anwalts-

kanzleien, die diese Enteignung möglich machen, und die Geheim-

dienste, die davon profitieren und selbst gern im Trüben fischen.

Und an wen geht denn nun dieser BigBrotherAward?

An die Cookie-Bäckereien? An die Internet-Werbewirtschaft? An die großen Plattform-Monopolisten? An die Nudging-Psychologen und die Dark-Pattern-Designer? Die Zeitdiebe und Nervenräuber? Die Profil-Dealer und Real-Time-Bidding-Casinobetreiber? Die Smarten, die Gewissenlosen und die Mitläufer bei den Medienhäusern? Die Karrieristen und die Blauäugigen unter den Digital-Politikern?¹¹

Die Wahl fiel schwer.

Aber dann passierte etwas.

Was mich wirklich amüsiert hat.

Denn Google hat sich quasi selbst nominiert.

Wir wissen nicht, ob es ein menschliches Versehen, die Heldentat eines Whistleblowers oder eine KI war, die digitales Wahrheitsserum genascht hatte...

Die Geschichte geht so: Zehn US-Bundesstaaten unter der Führung von Texas

9 Zitat von Peter Thiel, Gründer von Paypal und Palantir, Investor bei Facebook

10 Shoshana Zuboff, Quellen siehe Jahrbuch-Webseite

11 Oder doch die Werbefachleute, Marktforscher, Unternehmensberater, Versicherungsvertreter und Telefonesinfizierer – die, wie wir aus Douglas Adams' „Per Anhalter durch die Galaxis“ wissen – vom Planeten Golgafirinham evakuiert wurden und auf der Erde gelandet sind?

haben Ende 2020 Klage gegen Google eingereicht. Der Vorwurf: Google nutze seine Marktmacht, um Preise für Internetwerbung zu kontrollieren, ein Kartell zu bilden und

Werbe-Auktionen zu manipulieren. Dafür nutze Google seine Mehrfachfunktion als Werbepattformbetreiber, zugleich selber Werbeanbieter und seinen Zugriff auf Nutzerdaten hemmungslos aus. Der texanische General-Staatsanwalt Ken Paxton erklärte den Sachverhalt mit einem Bild aus dem Baseball: Google ist Werfer, Fänger und Schiedsrichter zugleich.¹²

Google schickte also Dokumente an das Gericht

in Texas. Die waren zum Beweis seiner Unschuld gedacht. Die eingereichten Dokumente waren überaus relevant zu diesem Thema – allerdings so gar nicht in Googles Sinne. Denn die Dokumente wurden unredigiert eingereicht, also ohne die wirklich interessanten Stellen wirksam zu schwärzen.

Einige Stunden später bemerkte man bei Google den Irrtum und bat das Gericht, die Dokumente austauschen zu dürfen. Doch zu spät – ein paar flinke Gerichts-



Foto: Matthias Hornung, cc by 4.0

reporter des Jura-Portals MLex¹³ hatten die unredigierte Fassung gelesen und flugs erkannt, was ihnen da für ein Schatz zugeflogen war:

Die Dokumente beschreiben, wie Google seit 2013 als Auktionsplattform seine Kenntnis von vorangegangenen Auktionen nutzt, um die voraussichtlich gerade ausreichenden Preise vorherzusagen.

► „An der Börse heißt so etwas ‚Insiderhandel‘.“ ◀

Damit konnten sie in ihrer zweiten Rolle als Werbevermittler aktuelle

Anzeigenauktionen gewinnen, und zwar zu einem möglichst geringen Preis¹⁴. An der Börse heißt so etwas „Insiderhandel“. Vermutet wurde so etwas schon lange – nun steht es genau so in Googles eigenen Dokumenten.

Mit diesem Trick verschafft sich Google nicht nur einen Vorteil vor den anderen Werbevermittlern, sondern drückt auch den Preis, den Publisher für ihren Werbeplatz erhalten. Nutzer werden ausgeforscht – Medien ausgehungert.

¹² Quelle für Paxton-Zitat: siehe Jahrbuch-Webseite

¹³ Quelle MLex: siehe Jahrbuch-Webseite

¹⁴ Quelle Businessinsider: siehe Jahrbuch-Webseite

Was mich wirklich wütend macht:

Dieses Verfahren hat Google firmenintern „**Project Bernanke**“ getauft – nach Ben Bernanke, dem ehemaligen Chef der US-Zentralbank. Dieser Codename bedeutet nichts anderes als „Googles Lizenz zum Gelddrucken“. Welch eine Arroganz.

Damit aber nicht genug: 2018 hat Google mit Facebook, der Nummer 2 im Werbemarkt, eine geheime Abmachung geschlossen – interner Codename „**Jedi Blue**“. Darin sichert Google seinem Konkurrenten Facebook zu, dass sie 10% der Anzeigenauktionen, an denen sie auf Googles Plattform teilnehmen, gewinnen. Wie soll das gehen in einem Markt mit angeblich freiem Wettbewerb?

Nun: Google liefert Facebook dafür Informationen über Netznutzer:innen, anhand derer Facebook 60% der Desktopnutzer

und 80% der Mobilnutzer eindeutig identifizieren kann. Damit weiß Facebook, bei wem es sich lohnt, in Anzeigen zu investieren. Facebook sagt im Gegenzug zu, dass sie eine bestimmte Summe für Anzeigen investieren und dass sie ein geplantes Verfahren namens „Header Bidding“, das anderen Werbenetzwerken neben Google bessere Chancen gegeben hätte, nicht weiter verfolgen. Wenn das keine Wettbewerbsmanipulation ist, was dann?

Aber: Erwischt!

Was mir Mut macht!

► Die Klagen und Bußgeldverfahren gegen Big Tech wegen Datenschutz- und Wettbewerbsverstößen häufen sich, sowohl von einzelnen Ländern (aktuell in Frankreich) wie auch von der EU und in den USA. Jawoll – geltendes Recht durchsetzen!¹⁵

► Kalifornien – ja, der US-Bundesstaat, in dem auch Silicon Valley liegt – hat ein Datenschutzgesetz beschlossen. Vorbild war das europäische Datenschutzrecht – doch das kalifornische Gesetz ist tatsächlich strenger!¹⁶

Grafik: Dennis Blomeyer, cc by 4.0;



¹⁵ Quelle Bundeskartellamt

¹⁶ Quelle ionos.de: siehe Jahrbuch-Webseite

- ▶ Die New York Times hat 2018 (nach Inkrafttreten der DSGVO) beschlossen, für ihre internationale Ausgabe auf

Tracker und personalisierte Werbung zu verzichten und schaltet Anzeigen nun wieder kontextabhängig. Neben dem Plus an Datenschutz ist diese Entscheidung auch ein finanzieller Erfolg: Denn weil die Tracking-Dienstleister nun außen vor sind, bleibt mehr vom Werbegeldkuchen für die Zeitung übrig.¹⁷

- ▶ Die britische Tageszeitung The Guardian hat 2019 nach schwierigen Jahren zum ersten Mal mit einem satten Plus abgeschlossen – ganz ohne Paywall, mit Spenden der Leserinnen und Leser.¹⁸
- ▶ Die EU bereitet zwei wichtige Verordnungen vor, die in das Geschäft der Internet-Riesen eingreifen: Den Digital Services Act (DSA) und den Digital Markets Act (DMA). Die Lobbyisten und die Anwaltskanzleien von Big Tech sind schon am Rotieren.¹⁹
- ▶ Was uns extra Schwung geben sollte: In den USA entwickelt sich tatsächlich eine überparteiliche Bewegung, die die Macht der großen Digitalkonzerne beschneiden will. Wir freuen uns

¹⁷ Quelle digiday.com, 19.1.2019

¹⁸ Quelle Meedia.de, 2.5.2019

¹⁹ Quelle Lobbycontrol, 15.12.2020



Foto: Panthermedia

Die EU bereitet zwei wichtige Verordnungen vor, die in das Geschäft der Internet-Riesen eingreifen: Den Digital Services Act (DSA) und den Digital Markets Act (DMA)

auf Lina Khan²⁰, die von Joe Biden für die Federal Trade Commission (FTC, die Verbraucher- und Wettbewerbsbehörde) nominiert wurde – eine kompetente Kritikerin von Big Tech.

- ▶ Und: Google erhält den BigBrother-Award 2021 für jüngst offenbar gewordene massive Manipulation des Internet-Werbemarktes, Aushungern von Kreativen und Medien sowie Enteignung unserer digitalen Persönlichkeiten.

Vielleicht ist das alles schon mal der Anfang von etwas, was Google wirklich wütend macht.

Herzlichen Glückwunsch, Google.

Weiterlesen: Auf der Jahrbuch-Webseite finden Sie viel weiterführenden Lesestoff zu dieser Laudatio und einige Tipps, wie Sie Ihren eigenen Computer auf „Verwanzung“ testen können.

²⁰ Quelle Lina M. Khan bei Wikipedia

Wie es weiter ging

Von Claudia Fischer

Kommentare unseres Publikums via Twitter und Mastodon:

- ▶ „Enteignung unserer digitalen Persönlichkeiten: Das ist einen #BBA21 Wert. Sehr bewegende Rede von Rena Tangens.“
- ▶ „Berufs-non-Wunsch: Dark-Pattern-Designer.“
- ▶ „Für Rena: Empfiehl doch einfach allen [termsandconditions.game](#) ...“

▶ „Das größte Datenleck der Welt“

Natürlich hat sich Google nicht bei uns gemeldet. Auch keine Real-Time-Bidding-Plattform und kein Dark Pattern Designer. Aber etwas anderes Spannendes ist passiert:

Im Oktober 2021 hat die grüne Fraktion im EU-Parlament eine 72-seitige Studie zu Online-Werbung veröffentlicht. Rena Tangens: „Ich bin begeistert, denn diese Studie belegt mit vielen Quellen meine Recherche und Argumentation der Big-BrotherAwards-Laudatio“.

Zwei weitere spannende Punkte aus der Studie:

1. Die Auktionen um die Aufmerksamkeit von Netznutzer:innen sind „das größte Datenleck der Welt“. Denn jedes Mal, wenn wir eine Webseite aufrufen, werden jede Menge persönlicher Daten wie Alter, Geschlecht, finanzielle Situation, Interessen, mögli-

cherweise auch vertrauliche Informationen zu Sexualität und zur politischen Einstellung einfach mal rausgepusht ins Netz an alle, die Anzeigen schalten wollen. In der Theorie darf nur die Firma, die das höchste Gebot für den Anzeigenpreis macht, diese Daten behalten, die anderen müssen sie löschen. Und in der Praxis? Wird das nicht überprüft.

2. Offenbar registrieren sich auch Firmen als Bieter, die sich gar nicht für Anzeigenplatz interessieren – vielmehr interessieren sie sich für die Massen an persönlichen Daten, die da großzügig frei Haus verteilt werden. Über Tarnfirmen können so Daten auch an Kriminelle und ausländische Geheimdienste abfließen. Diese Erkenntnis beunruhigt inzwischen auch IT-Sicherheitsexperten, Politiker und Institutionen bis hin zur NATO. Nochmal zum Mitschreiben: **Personalisierte Werbung ist ein nationales Sicherheitsrisiko!**

- ▶ Die Studie „**The Future of Online Advertising**“ ist absolut lesenswert. Wir verlinken sie über die Jahrbuch-Webseite. Mehr über die notwendige Begrenzung der IT-Konzernmacht finden Sie auf Seite 40 und 142.

Unabhängige Arbeit braucht unabhängiges Geld.

Werden Sie Fördermitglied!

▶ digitalcourage.de/mitglied

Kategorie Gesundheit

Doctolib

Von Dr. Thilo Weichert

Foto: Infiac, cc by 4.0



Laudator: Dr. Thilo Weichert,
Netzwerk Datenschutzexpertise

Der BigBrotherAward in der Kategorie „Gesundheit“ geht an

die Firma Doctolib in Berlin für ihr Terminvermittlungsportal für Ärzte.

Doctolib verarbeitet mit diesem Portal unter Missachtung der ärztlichen Vertraulichkeit die Daten von zigtausenden Patient:innen.

Das Angebot für Gesundheitsfachkräfte, also vor allem für Ärzte und deren Patienten, ist genial: Die Ärzte schließen einen Vertrag mit Doctolib ab, erteilen Zugriff auf ihre Patientendaten und können dann über eine Inter-

netseite Behandlungs-, Beratungs- oder Impftermine verbindlich verabreden lassen. Und schon können die Patient:innen online Termine buchen. Kein Warten in einer Telefonwarteschleife, keine gestressten Mitarbeiter:innen, selbst das Erinnern der Patient:innen an

den Termin übernimmt Doctolib – und für das alles zahlen die Praxen nur etwas mehr als 100 € im Monat. Für die Patient:innen ist alles unentgeltlich. Und nicht nur das. Doctolib verspricht:

„Für Doctolib hat die Sicherheit und die Geheimhaltung personenbezogener Daten seiner Nutzer oberste Priorität. Daher verpflichtet sich Doctolib, alle deutschen und europäischen Vorschriften zum Schutz personenbezogener Daten einzuhalten. Doctolib hält sich an die von den jeweiligen Kammern und Verbänden erlassenen Landesregeln für Ärzte und Heilberufler.“

Na, dann ist ja alles in Butter. Auf dem Bildschirm.

Grafik: Dennis Blomeyer, cc by 4.0; Telefonhörer: Smashicons, Glocke: Pixel perfect (flaticon.com)



Keine Warteschleife,
kein gestresstes Team, Erinnerungen –
klingt doch super!

► Funktionsweise

In der Realität sollten Ärzt:innen schnell stütztig werden, denn wenn ein Arzt Doctolib für seine Praxis in Anspruch nehmen will, erscheint ein Mitarbeiter des Unternehmens und bittet zunächst einmal um Zugriff auf den gesamten im Arztinformationssystem gespeicherten Patientenstammdatensatz.

Und damit nicht genug: Nach dem Import der Patientenliste ist ein regelmäßiger Datenabgleich der Termitabelle des Arztsystems mit dem Vermittlungssystem von Doctolib nötig.

Da stellen sich unsere Stacheln auf. Trotzdem beteiligen sich Praxen an diesem Dienst. Wir vermuten: Die meisten Ärzt:innen verstehen von den technischen Vorgängen wenig und

vertrauen auf die Expertise von Doctolib sowie das Versprechen, Patientengeheimnis und Datenschutz zu beachten.

Als Zusatzangebot für die Patient:innen bietet Doctolib zur Orientierung eine bundesweite Ärzteliste sowie zur Telekonsultation einen Videodienst an. Und seit Beginn der Corona-Pandemie vermittelt Doctolib auch Impftermine, für das französische Gesundheitsministerium ebenso wie für die Gesundheitsverwaltung in Berlin.

Und tatsächlich funktioniert dann auch alles. Doctolib rühmt sich einer Kundenzufriedenheit von 97%. Nach eigenen Angaben nutzen 150.000 Ärzte und Gesundheitsfachkräfte in Deutschland und Frankreich und 50 Millionen Patient:innen den Dienst. Dass dies alles



Als erstes verlangt Doctolib Zugriff auf die gesamte Patientenkartei einer Arztpraxis.

Grafik: Dennis Blomeyer, cc by 4.0

in Ordnung geht, dafür sollen gleich drei unterschiedliche Gütesiegel bürgen.

► Intransparenz

Ein qualifizierter Blick ins Kleingedruckte aber belehrt ein geschultes Auge eines Schlechteren. Verwirrend ist zunächst die Vielzahl der Dokumente: Während es bei anderen Diensten einmal Allgemeine Geschäftsbedingungen (AGB) gibt, gibt es hiervon bei Doctolib ein Dutzend: Nutzungsbedingungen, Datenschutzhinweise, Grundsätze zum Schutz von Gesundheitsdaten (jeweils unterschieden nach Patient:innen und den sog. Gesundheitsfachkräften), zusätzlich eine Cookie-Richtlinie, eine Verarbeitungsliste, Hinweise zu Datenschutz und Sicherheit, FAQs, einen Auftragsverarbeitungsvertrag und Begriffsbestimmungen. Das ist für einen einheitlichen Dienst zu viel. Die Dokumente sind verwirrend und unklar, teilweise widersprüchlich. Die meisten sind nicht durchnummeriert, was eine Berufung darauf zusätzlich erschwert.

Der Teufel steckt im Detail: Doctolib trennt formaljuristisch zwischen einer Auftragsverarbeitung für die Gesundheitsfachkraft und einer eigenen Doc-



Foto: Inifac, cc by 4.0

Die Dokumente von Doctolib sind unklar und verwirrend, teilweise widersprüchlich.

► Für Ärzt:innen wie Patient:innen bleibt unklar, wie die Daten dann weitergenutzt werden. ◀

tolib-Verantwortung für sein eigenes Webangebot. Soweit so gut und richtig. Doch dann maß sich Doctolib an, die im Auftrag des Arztes verarbeiteten Daten in den eigenen Datenbanken zur Terminvergabe zusammenzuführen. Für Ärzt:innen wie Patient:innen und auch für uns bleibt unklar, wie die Daten dann weitergenutzt werden.

► Besonders sensible Gesundheitsdaten

Es sollte unstrittig sein, dass ärztliche Terminvereinbarungen ebenso wie die Metadaten von Videosprechstunden sensitive Gesundheitsdaten sind, die unter dem besonderen Schutz der Datenschutzgrundverordnung stehen, und die zudem der beruflichen Schweigepflicht unterliegen. Das Vertrauen des Patienten gegenüber dem Arzt verbietet es, dass Namen, Termine, Behandlungen

► **Dieses Vertrauens-
verhältnis wird in
strafbarer Weise verletzt.** ◀

gen in die Hände Dritter gelangen und für andere als Behandlungs- und Beratungszwecke in der Praxis des Vertrauens genutzt werden. Juristisch dürfen Ärzte dafür Auftragsverarbeitungsverträge abschließen, ohne dass ihre Patient.innen zustimmen müssen. Aber dieses Vertrauensverhältnis wird spätestens dann in strafbarer Weise verletzt, wenn sich Doctolib aus dem Arztsystem Daten von Patient.innen beschafft, die keine Termine vereinbaren und nicht einmal ein Konto bei Doctolib haben, und wenn die Betroffenen über diese Datenweitergabe nicht informiert werden.

► **Werbung, Tracking, Analysen – wer ist verantwortlich?**

So vollmundig sich Doctolib zum Datenschutz und zum Patientengeheimnis bekennt, so sehr müssen wir diese Versprechen nach Lektüre des Kleingedruckten in Frage stellen:

In der Cookie-Liste von Doctolib taucht z.B. Google auf mit Analytics und Adwords bzw. Ads. Als Zwecke werden das „Verfolgen“ oder „Nachverfolgen“ der Webseitennutzung angegeben. Ads dient für nichts Banaleres als Werbung. Stimmt man den Datennutzungen für Werbung und Meinungsumfragen einmal zu, dann hat dies bei allen weiteren Terminvereinbarungen offenbar zur Folge, dass die Daten z. B. auch zu Google gelangen. Das gleiche Problem stellt sich bei der Einbindung von sozi-

alen Netzwerken wie Twitter, Instagram, Facebook, LinkedIn, Medium

und YouTube schon auf der Startseite von Doctolib. Wofür das alles gut sein soll, weshalb zum Beispiel eine Terminvergabe-Seite einen YouTube-Button braucht, muss Doctolib sich ernsthaft fragen lassen. Bei den dortigen Cookieeinstellungen wird jeweils „alle akzeptieren“ angeboten. Und Doctolib erklärt dann unschuldig, dass es für die Verarbeitung von Daten bei diesen Diensten nicht verantwortlich sei.

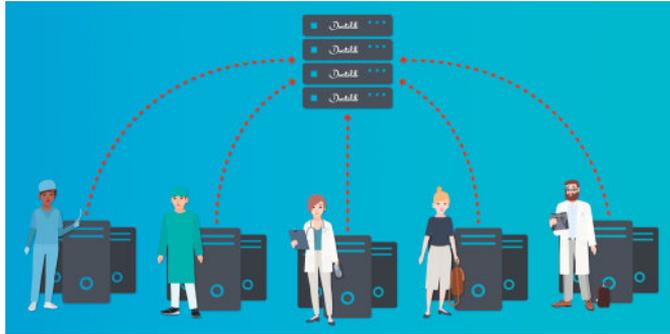
Hier irrt Doctolib: In jüngster Zeit hat der Europäische Gerichtshof gleich in drei völlig unabhängigen Verfahren festgestellt, dass bei einer solchen Datenverarbeitung eine Mitverantwortlichkeit des Seitenanbieters, also hier von Doctolib, besteht. Wir meinen: Kommerzielle Social Media-Firmen haben in der Arzt-Patientenbeziehung nichts zu



Social-Media-Anbieter haben in der Arzt-Patientenbeziehung nichts zu suchen!

Grafik: Dennis Blomeyer, cc by 4.0

suchen, schon gar nicht, wenn diese ihren Sitz in einem unsicheren Drittstaat wie den USA haben.



Grafik: Dennis Blomeyer, cc by 4.0

► Schweigepflicht

In Doctolib's „AGB Nutzer“ von 2019 kann der Patient lesen, dass er seine Ärzte mit seiner Zustimmung von der gesetzlichen Schweigepflicht entbindet. Wofür und weshalb, wird dem Patienten und wurde auch uns auf Anfrage nicht erklärt. Es sollte klar sein, dass eine solche Entbindung im Kleingedruckten unwirksam ist.

Tatsächlich beginnt die Verletzung der Schweigepflicht früher und hat eine gewaltige Dimension: Einem Arzt ist es zwar nach einer neuen gesetzlichen Regelung aus dem Jahr 2017 explizit erlaubt, technische Dienstleister wie Doctolib in Anspruch zu nehmen. Voraussetzung ist aber, dass die hierfür offenbaren Patientengeheimnisse für den Dienst erforderlich sind. Definitiv nicht erforderlich ist der gesamte Import der Patientenliste eines Arztes durch Doctolib. Dem Unternehmen würde es für seine Terminvermittlung genügen, vom Arzt die freien Termine zu erfahren, um dann diese gegenüber dem Arztsystem zu vermitteln.

► Die Verletzung der Schweigepflicht hat eine gewaltige Dimension. ◀

Doctolib hält die vorgeschriebene Mandantentrennung nicht ein.

► Mandantentrennung

Als Mitwirkender eines Arztes und als dessen Auftragsverarbeiter ist Doctolib verpflichtet, die sog. Mandantentrennung einzuhalten. Das heißt, Doctolib darf die Patientendaten von verschiedenen Ärzten bei sich nicht zusammenführen. Doch das genau scheint das Unternehmen zu tun. Auf dem Chaos Communication Congress 2020 wurde berichtet¹, dass dem Chaos Computer Club eine Doctolib-Datenbank zugespielt worden sei. Über die beschriebene Lücke sei der Zugriff auf ca. 150 Millionen Terminvereinbarungen möglich gewesen, die wohl

auf eine Synchronisierung mit den Terminkalendern der Arztpraxen zurückzuführen waren und die bis ins Jahr 1990 zurückreichten.² Wie die Daten verarbeitet wurden und werden, was Doctolib mit dieser Sammlung tut und weshalb alte Daten nicht gelöscht wurden, bleibt das

1 Videomitschnitt siehe Jahrbuch-Webseite

2 Quelle Medical Tribune 19./25.01.2021

► Ein neues Spielfeld für IT-Konzerne und Spekulanten ◀

Geschäftsgeheimnis unseres Preisträgers.

Die angeblich verliehenen Gütesiegel haben entgegen der Firmenbehauptung keine Grundlage in der DSGVO. Was hier gesiegelt wurde und weshalb, bleibt weitgehend das Geheimnis von Doctolib. In der Datenschutzerklärung nachzulesen ist u.a., dass Doctolib ein in Frankreich zertifiziertes Cloudangebot von Amazon Web Services – mit Rechnern in Europa – nutzt.³

► Was tut Doctolib wirklich?

Unsere Nachfragen beim Unternehmen wegen des millionenfachen Herunterladens von Patientendaten, zur Mandantentrennung und vieles mehr, blieben unbeantwortet.

Uns bleiben insofern nur Spekulationen, was auf den Servern von Doctolib und AWS passiert. Spekulieren tun übrigens auch Wagniskapitalgeber, die dem 2013 gegründeten Unternehmen 2016 23 Mio. €, 2017 weitere 35 Mio. € und 2019 nochmals 150 Mio. € bereitstellten. Doctolib zählt inzwischen zu den sog. Unicorns, also den Firmen, die auf dem Kapitalmarkt mit mehr als einer Milliarde € bewertet wer-

den.⁴ Der Markt der Gesundheitsdaten ist, nach-

dem der globale und auch der europäische Markt von Internetnutzungsdaten zwischen Facebook und Google aufgeteilt ist, ein neues Spielfeld für IT-Konzerne und Spekulanten. Bisher ist es halbwegs gelungen, hier in Europa US-Unternehmen draußen zu halten unter Verweis auf die ärztliche Vertraulichkeit. Doctolib arbeitet daran, sich einen großen Teil dieses Kuchens einzuverleiben mit dem vollmundigen Bekenntnis zu dieser Vertraulichkeit, ohne sich daran wirklich zu orientieren.

Die Digitalisierung unseres Gesundheitssystems ist wichtig, um die Gesundheitsversorgung der Bevölkerung zu verbessern und auf einem hohen Niveau zu halten. Dies darf aber nicht auf Kosten der Vertraulichkeit zwischen Patient, innen und Heilberufen passieren. Dafür, dass Doctolib diese Vertraulichkeit seinem Expansionsstreben unterordnet, dafür erhält das Unternehmen den BigBrotherAward 2021 in der Kategorie „Gesundheit“.

Herzlichen Glückwunsch, Doctolib.



3 Quelle Doctolib

4 Quelle: Quelle Businessinsider 20.03.2019

Wie es weiter ging

Von Claudia Fischer, Thilo Weichert und Julia Witte

Kommentare unseres Publikums via Twitter und Mastodon:

- ▶ „Mensch muss halt genau lesen: Doctolibs Kund.innen sind die Ärzt.innen, nicht die Patient.innen. Dass die Ärzt.innen zufrieden sind und deren Daten geschützt werden, ist alles, was gesagt wird.“
- ▶ „Vielen Dank für den BBA an Doctolib! In Frankreich hatte ich keine Wahl und musste über dieses Unternehmen meine Impfungen gegen das Coronavirus reservieren. Darüber hinaus wird es immer mehr unmöglich diesen Dienst zu umgehen, um einen Termin zu erhalten. Und sogar wenn man diesen Dienst nicht nutzt, werden manchmal unsere Daten an Doctolib trotzdem weitergegeben.“
- ▶ „Auch meine Hausarztpraxis hat einen Button mit „Termin online buchen“ ... der dann zu Doctolib weiterleitet. Dann werde ich wohl mal nachfragen müssen, wie die das sehen.“
- ▶ „Habe heute direkt im Anschluss an den Arzt und Doctolib zwei DSGVO-Auskünfte entsprechend Artikel 15 verschickt – beim Arzt entsprechend mit dem Verweis auf den BBA21. Wenn das mehr Leute machen, wachen dann vielleicht Arzt und Doctolib auf.“



Foto: Infiac, cc by 4.0

Und das war noch nicht alles...

Thilo Weicherts BigBrotherAward an Doctolib hat die meisten Social-Media-Kommentare ausgelöst, den Publikumspreis in unserer Online-Abstimmung gewonnen und war der Auftakt für eine Menge weiterer Recherchen.

Die Internet-Redaktion mobilssicher.de, ein Projekt von iRights e. V. und dem Institut für Technik und Journalismus ITUJ e. V., stellte bei einem Test der Doctolib-App fest, dass Daten zu Facebook und zur Werbepattform Outbrain abfließen. Andere Redaktionen griffen dieses Sicherheitsleck auf und forschten weiter, die Berliner Beauftragte für Datenschutz und Informationssicherheit kündigte eine Prüfung an. Facebook meldete sich zu Wort und gab an, Gesundheitsdaten würden von den internen Filtern geblockt und aus Datensätzen entfernt. Doctolib sagte, die Datenweitergabe durch die App sei inzwischen gestoppt worden. (Alle Quellen verlinken wir über die Jahrbuch-Webseite)

Thilo Weichert, der nach dem BigBrotherAward ein umfangreiches Gutachten für das Netzwerk Datenschutzexpertise erstellte, hat bis zum Redaktionsschluss des Jahrbuches keine Ant-

wort von Doctolib auf seine Fragen, die Laudatio oder sein Gutachten erhalten.

► **Musterbriefe für Datenauskunft und Löschungsantrag finden Sie auf**

🔗 digitalcourage.de/faq-doctolib

oder eine SMS von Doctolib erhalten. Fragen Sie in Ihrer Praxis nach – oder direkt bei Doctolib.

Bei uns im Digitalcourage-Postfach landeten viele Anfragen von Menschen, die Doctolib nutzen (mussten), weil ihre Ärzte oder Impfzentren diesen Dienst verwenden. Einige dieser Fragen haben wir in Zusammenarbeit mit Thilo Weichert auf digitalcourage.de (ausführlicher als hier im Jahrbuch) beantwortet:

Für Patient:innen:

Welche Daten genau sammelt Doctolib?

Doctolib selbst nennt in seinen Datenschutzhinweisen:

Name, Vorname, Telefonnummer, E-Mail-Adresse, Verlauf der Termine, vom Nutzer eingestellte Dokumente, Nutzungsdaten, evtl. Beruf und weitere Angaben, auch aus Freitextfeldern (z. B. zu Beschwerden).

Wie kann ich wissen, ob meine Daten bei Doctolib gelandet sind?

Wenn z. B. Ihre Zahnärztin oder Ihr Hautarzt Doctolib nutzt, dann wurden wahrscheinlich schon Ihre Stammdaten aus dem Arztinformationssystem an Doctolib übermittelt – ohne dass Sie etwas davon mitbekommen haben. Sie merken davon erst etwas, wenn Sie beispielsweise telefonisch einen Termin vereinbart haben und zur Bestätigung eine E-Mail

Kann ich von Doctolib verlangen, meine Daten zu löschen?

Ja, nach Art. 17 DSGVO hat jede betroffene Person das Recht, die eigenen Daten löschen zu lassen, wenn diese nicht mehr benötigt werden. Dies ist der Fall, wenn Sie die Dienste von Doctolib nicht (mehr) in Anspruch nehmen wollen.

Kann ich mich im Vorhinein gegen die Weitergabe von Daten wehren?

Sie können Ihren Arztpraxen auch schon im Vorhinein mitteilen, dass Sie im Fall einer Zusammenarbeit mit Doctolib der Verwendung Ihrer Daten widersprechen. Dafür können Sie unsere Widerspruchsvorlage nutzen.

Ich habe mehrere Befunde und andere Dokumente bei Doctolib hochgeladen, da ich dachte, das ginge ausschließlich an die Arztpraxis. Was passiert nun wohl damit?

Die Dokumente werden bei Doctolib zwischengespeichert und können von der behandelnden Ärztin oder dem Arzt abgerufen werden. Was Doctolib darüber hinaus mit den Dokumenten macht, ist unklar. Doctolib behauptet, diese Dokumente nicht einmal zur Kenntnis nehmen zu können und dies auch nicht zu tun. Wir halten das für wenig glaubwürdig.

Was ist mit Datensätzen aus der Vergangenheit? Muss ich jetzt bei allen Praxen, die mich jemals behandelt haben nachfragen, ob sie Doctolib benutzen?

Durch eine Sicherheitslücke, die der Chaos Computer Club aufgedeckt hat, wissen wir, dass Doctolib auch über Informationen über zurückliegende Sprechstundenbesuche – teils bis ins Jahr 1990 – verfügt hat. Vermutlich sind also auch Arzt-Patienten-Beziehungen betroffen, die schon lange beendet wurden. Sie können von Doctolib Auskunft darüber verlangen, welche Daten über Sie dort gespeichert sind und die Löschung verlangen.

Kann mein Zahnarzt oder meine Hausärztin sich weigern, mich zu behandeln, wenn ich der Verarbeitung meiner Daten durch Doctolib widerspreche?

Es besteht grundsätzlich keine Behandlungspflicht für Ärztinnen und Ärzte. Etwas anderes gilt, wenn es sich um einen Notfall handelt.

Für Gesundheitsfachkräfte

Verletze ich die ärztliche Schweigepflicht, wenn ich Doctolib nutze?

Sie verletzen Ihre Schweigepflicht dann, wenn die Offenbarung von Patientengeheimnissen zur Erbringung der ärztlichen Dienstleistung nicht erforderlich und adäquat ist.

Wenn Sie Dienstleistungen von Doctolib in Anspruch nehmen wollen, verlangt Doctolib Zugriff auf den gesamten Patientenstammdatensatz oder einen aktuellen Teil davon. Das ist aus unserer Sicht ganz klar weder erforderlich noch adäquat. Auch das Setzen von für die Dienstleistung unnötigen Cookies, so wie es Doctolib durchführt, ist eine Verletzung der Schweigepflicht.

Dieser Verstoß kann grundsätzlich strafrechtlich und datenschutzrechtlich geahndet werden. Die Datenschutzbehörde oder die Staatsanwaltschaft werden sich aber wahrscheinlich zuerst an Doctolib mit Sanktionen wenden und Ihnen zunächst nur eine Abmahnung zukommen lassen.

Ich nutze bislang Doctolib für meine Praxis. Nun sind mir Zweifel gekommen. Was kann ich machen?

Sie können z. B. Doctolib dazu auffordern, eine Stellungnahme zum Gutachten des Netzwerks Datenschutzexpertise abzugeben, damit Sie Ihren Verdacht der rechtswidrigen Datenverarbeitung überprüfen können. In jedem Fall können Sie die Inanspruchnahme der Dienste von Doctolib kurzfristig kündigen und die Löschung sämtlicher über Ihre Praxis erlangten Daten verlangen.

Jammern, resignieren und zynisch werden sind nicht die Lösung

Werden Sie Fördermitglied – gemeinsam können wir was bewegen!

▶ digitalcourage.de/mitglied

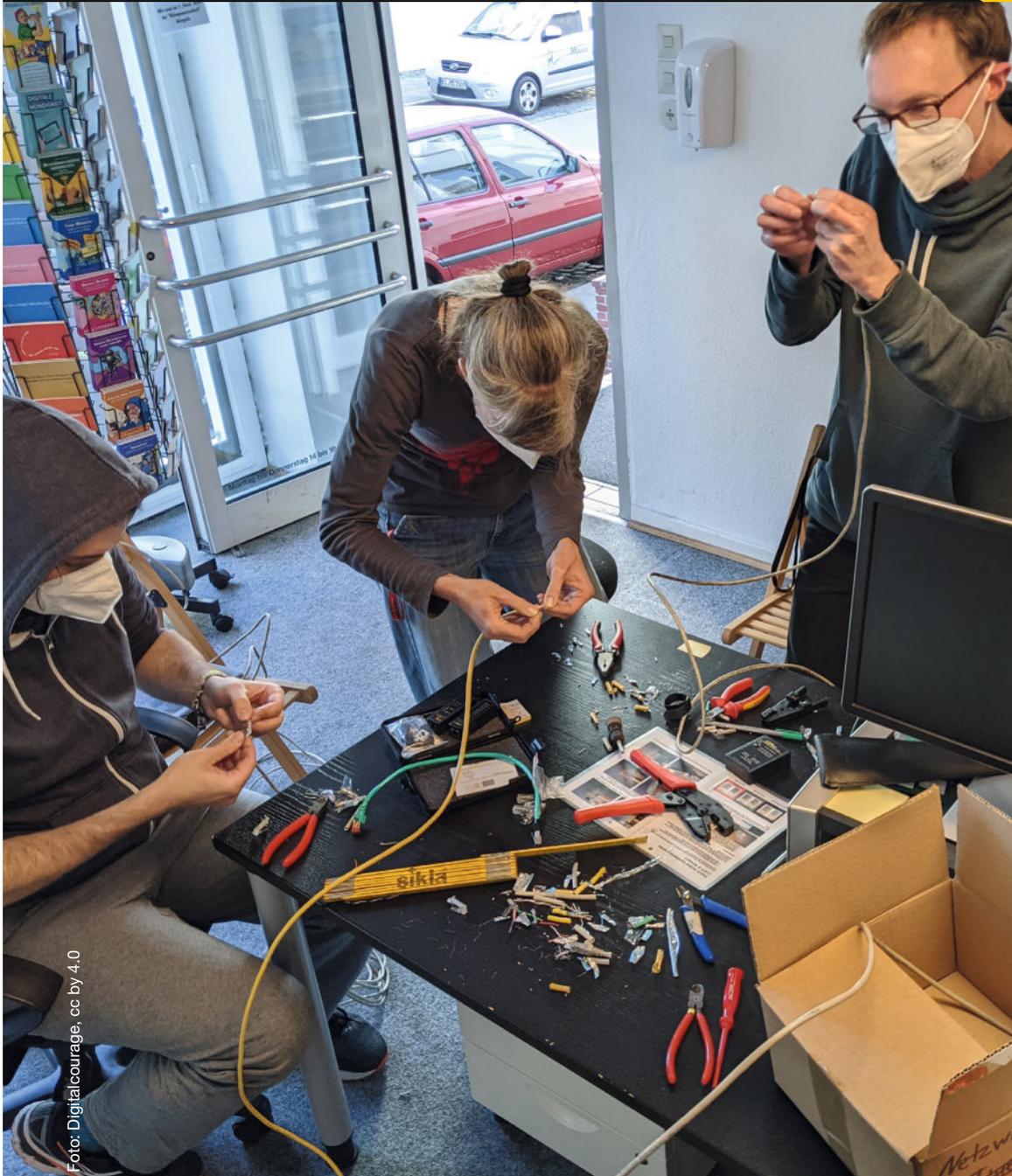


Foto: Digitalcourage, cc by 4.0

Wenn die Büro-Crew unsere Netzkabel selbst besteckt

Digitale Selbstverteidigung

Wie Sie Ihre Computer, Smartphones, E-Mails und Daten schützen können



Hinter den nächsten Seiten steht ein ganzes Team: Unsere Arbeitsgruppe „Digitale Selbstverteidigung“. Die Mitglieder dieser AG kennen sich technisch gut aus, sie haben ihre Augen und Ohren überall, wo neue Entwicklungen präsentiert werden, und bohren nach, welche Einflüsse auf Privatsphäre und Überwachungsthemen im Anmarsch sind. Sie testen, probieren, zweifeln und diskutieren im Team, welche Konsequenzen eine neue Entwicklung hat. Und

sie geben ihr Wissen und ihre Hinweise regelmäßig weiter: in Vorträgen auf Kongressen und Messen, auf unserer Internetseite, im jährlichen Digitalcourage-Online-Adventskalender, auf CryptoParties, in einem Flyer oder (mit einer sehr kleinen Auswahl) auch hier im Jahrbuch.

Möchten Sie sich selbst gegen Überwachung schützen, Ihre technischen Geräte selbst kontrollieren und besser verstehen? Krempeln Sie die Ärmel hoch: Auf den kommenden Seiten gibt es viel zu tun!

Sie möchten mit uns tüfteln? Unser Team kann kundige – insbesondere weibliche – Verstärkung gebrauchen. Melden Sie sich gern!

**Erhältlich im Digitalcourage-Shop!
Flyer mit Tipps zur
Digitalen Selbstverteidigung**



Die aktuellen Tipps zur Digitalen Selbstverteidigung können Sie auch als Flyer bei uns im Shop bestellen.

Preis: 0,12 Euro pro Stück

► shop.digitalcourage.de

► Hinweis:

Hundertprozentige Sicherheit gibt es nicht, auch nicht durch unsere Empfehlungen. Programme können unentdeckte Fehler haben und Datenschnüffeltechniken entwickeln sich weiter. Bleiben Sie wachsam! Die folgenden Texte sind auch über unsere Jahrbuch-Webseite (Siehe unten) zu erreichen. Dort sind sie mit Links versehen und unter Umständen aktualisiert.

Sollten Sie Fehler finden, Ergänzungen haben, oder sollten Empfehlungen bei Ihnen nicht funktionieren, geben Sie uns bitte Bescheid.

Online Zusammenarbeiten in Homeoffice und Büro

Wenn man nicht im gleichen Büro oder Raum sitzt, aber trotzdem zusammen arbeiten möchte, sind kollaborative Online-Tools zu einem weitverbreiteten Werkzeug geworden. Aber schnelle Lösungen sind oft nicht die besten: Viele Online-Dienste arbeiten nicht verschlüsselt oder „verpetzen“ die Nutzungsdaten an die Werbeindustrie oder Geheimdienste.

Viele nutzen die Tools der großen US-Datenkraken – häufig, weil sie nichts anderes kennen. Unsere Bitte: Tun Sie das auch im Homeoffice nicht! Sie legen nicht nur Ihre Inhalte und Kontakte, sondern u. U. auch Ihre kompletten Arbeitsstrukturen gegenüber Geheimdiensten und Firmenkonsortien offen. Das schadet nicht nur Ihnen und Ihrer Arbeit, sondern mittel- und langfristig der gesamten Gesellschaft. Der Wert der Freiheit einer Gesellschaft sollte auch in Krisenzeiten hochgehalten werden.



Wir zeigen einige Alternativen zu etablierten Diensten – zum Lesen hier, mit Links zum Anklicken von Downloads etc. auf digitalcourage.de.

Die schnelle Antwort, die viele Wünsche auf einmal erfüllt, lautet: Nextcloud. Aber lesen Sie selbst:

Eine Lösung für ziemlich viele Fragen: Nextcloud

Seit einiger Zeit sammeln wir Erfahrungen mit der Open-Source-Software „Nextcloud“. Einmal aufgesetzt und mit ein paar Zusatz-Modulen ergänzt, bietet Nextcloud sehr vieles, was man – zumindest für kleine Teams – braucht:

- ▶ eine verschlüsselte Cloud für den Austausch von Dateien, Texten, Tabellen, Bildern usw.
- ▶ Gemeinsame Kalender und Chats
- ▶ Pads zum gemeinsamen, gleichzeitigen Arbeiten an Texten
- ▶ ein Kanban für die Arbeitsorganisation und Aufgabenverteilung
- ▶ Komplette Online-Office-Suite: Textdokumente, diese können von uns nicht empfohlene Dienste wie beispielsweise Microsoft Office 365 ersetzen.
- ▶ Umfragen und Formulare
- ▶ Nextcloud Talk für kleine Videokonferenzen bis zu vier Personen (mehr werden holprig, ist unsere Erfahrung)

Auf digitalcourage.de haben wir einige Anbieter gesammelt, bei denen Sie eine Nextcloud „mieten“ können. Sie können eine Nextcloud aber auch selbst aufsetzen, wenn Sie einen eigenen Server betreiben oder z. B. eine IT-Abteilung oder eine.n IT-Administrator.in im Team haben.

Gemeinsam an Dateien arbeiten

Schon seit über zehn Jahren arbeiten wir bei Digitalcourage erfolgreich mit Etherpads, inzwischen CryptPads (kurz: Pads). Sie ermöglichen es, Texte gemeinsam zu verfassen, auch wenn man nicht zusammen vorm Rechner sitzt und sind aus unserem Arbeitsalltag nicht mehr wegzudenken.

CryptPad

Vorteile: CryptPad verfügt nicht nur über einen Texteditor, sondern unter anderem auch über eine Tabellenkalkulation, Umfragen und ein Whiteboard. Größter Vorteil: Alle Dokumente liegen verschlüsselt auf dem Server – selbst die Admins des jeweiligen CryptPad-Servers können sie nicht einsehen. Bei Bedarf lässt sich ein Account erstellen, mit dem sich Inhalte und sogar ganze Teams verwalten lassen. (► Seite 128)

Nachteile: Es gibt es keine sprechenden Links, mit denen sich Inhalt eines Dokuments in der URL benennen lassen. Einige Funktionen sind in den Texteditoren nicht so komfortabel und umfas-

send benutzbar wie z.B. bei Etherpad; es fehlt z.B. das Speichern von Zwischenständen. Auch die bei den Etherpads beliebten Autorenfarben zum Markieren eigener Textbeiträge sind als Feature noch nicht vollständig umgesetzt.

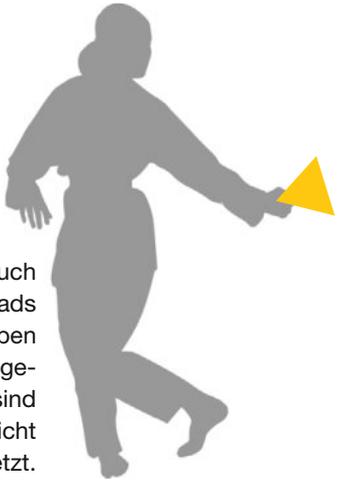
Da alle Inhalte im Browser entschlüsselt werden, belastet CryptPad den eigenen Computer beim Aufruf eines Pads stärker als vergleichbare Lösungen.

Wie Sie CryptPad nutzen können: Digitalcourage betreibt eine eigene CryptPad-Instanz unter <https://cryptpad.digitalcourage.de/>. Sie können aber z.B. auch die offizielle Instanz <https://cryptpad.fr/> oder andere öffentliche Instanzen verwenden. Technik-Kundige können auch ein eigenes CryptPad-System aufsetzen.

Etherpad (Lite)

Vorteile: Wie CryptPad erlaubt Etherpad das gemeinsame Arbeiten, beschränkt sich aber auf Texte. Hierdurch ist es oft einfacher zu nutzen. Farben zeigen, wer was geändert hat und es gibt eine Versionskontrolle.

Nachteile: Layout, Zeilenabstand, Überschriften-Gestaltung etc. sind nicht so komfortabel wie bei einem Textverarbeitungsprogramm. Zur Formatierung muss der Text, wenn er fertig ist, aus



dem Etherpad in ein anderes Programm kopiert oder exportiert und dort bearbeitet werden. Alle Texte liegen unverschlüsselt auf dem Server.

Wie Sie Etherpads nutzen können:

Auch hier gibt es offene Pads, bei denen Sie sich kostenlos eine eigene Unter-Instanz einrichten können. Beachten Sie, dass Sie damit ihre Texte, aber auch die Daten Ihrer Team-Mitglieder (vermutlich Mailadressen und IP-Adressen) diesen Anbietern überlassen – wägen Sie ab, wie groß dieses Risiko ist und wem Sie vertrauen.

Nextcloud

Vorteil: Wenn Sie eine Nextcloud haben, können Sie direkt in der Nextcloud-Weboberfläche gemeinsam an Texten arbeiten und brauchen keine weitere Instanz. Sie finden die Dateien dann auch direkt in Ihrem Dateisystem wieder.

Dafür bietet Nextcloud mehrere Varianten: „Text“ mit Formatierungsmöglichkeiten einer einfachen Textverarbeitung, ähnlich wie ein Pad. „OnlyOffice“ integriert in Ihre Nextcloud eben OnlyOffice, das auch in CryptPad enthalten ist. Und „Collabora Online“ integriert die Online-Version von LibreOffice. Auch Tabellenkalkulation oder gemeinsames Arbeiten an Präsentationen ist innerhalb von Nextcloud möglich.

Nachteil: Durch die verschiedenen Varianten können wir leider nicht sagen, welche besser und welche weniger gut funktioniert.

Wie Sie Nextcloud Text, Nextcloud OnlyOffice oder Nextcloud Collabora Office nutzen können: Nur innerhalb einer Nextcloud, in der die entsprechende App installiert ist.

Was wir nicht empfehlen:

Google-Docs: Werfen Sie Ihre sensiblen Daten – zumal im laufenden Arbeitsprozess – nicht einem der größten Datensammler der Welt in den Rachen. Zumal Google seine Server im Zweifel auch für eine Durchsuchung durch US-Behörden zur Verfügung stellen muss.

Videokonferenzen

Die folgenden Informationen zu Videokonferenzen reißen das Thema nur kurz an. Einen ausführlichen Artikel mit Erfahrungen, Tipps und Links finden Sie auf digitalcourage.de/videokonferenzen.

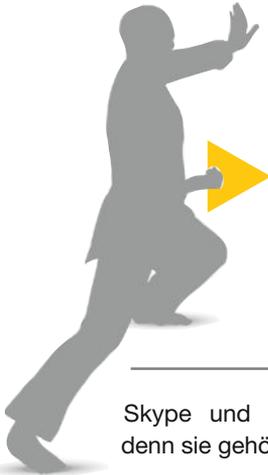
Jitsi Meet empfehlen wir für Videokonferenzen mit maximal 10 bis 15 Teilnehmenden. Jitsi Meet läuft komplett im Webbrowser oder per App auf dem Smartphone.

BigBlueButton ist ein browserbasiertes Open-Source-Tool für Videokonferenzen und speziell zugeschnitten auf Vorträge und virtuelle Klassenräume.

Nextcloud Talk eignet sich für Videokonferenzen mit bis zu vier Kontakten.

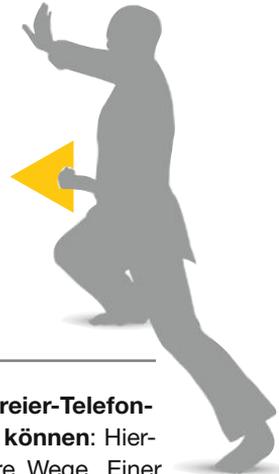
Was wir nicht empfehlen:

Zoom wegen Datenschutz-Lecks unterschiedlichster Art,



Eine kurze Überlegung:

Viele Anwendungen für Videotelefonie bieten gleichzeitig die Möglichkeit reiner Audiotelefonie. Das spart viel Datenverkehr, wenn Sie nicht unbedingt ein Bild brauchen. Dann läuft es auch problemloser und schont Netzkapazitäten – seien Sie solidarisch mit anderen Menschen in ihren Heimbüros.



Skype und Microsoft Teams, denn sie gehören zu Microsoft,

Facebook Messenger Rooms, denn es kommt ja von Facebook,

Discord, deren Datenschutzerklärung schreibt, dass alle Chats abgehört, gelesen, ausgewertet und weiterverkauft werden dürfen,

WebEx, GoToMeeting, LifeSize, denn diese Dienste sitzen in den USA, wo es mit dem Datenschutz schlecht aussieht.

Wie Sie eine Dreier-Telefonkonferenz nutzen können: Hierfür gibt es mehrere Wege. Einer davon ist dieser: Beginnen Sie ein erstes Gespräch, wählen Sie dann im Telefon „Rückfragen“, bauen das zweite Gespräch auf, und wählen abschließend im Telefon „Konferenz“. Wie diese beiden Funktionen bei Ihnen heißen, probieren Sie einfach aus, oder schauen im Handbuch Ihres Telefons nach.

Telefonkonferenzen

Dreier-Telefonkonferenz

Mal schnell jemand Drittes mit ins Gespräch zu holen, geht fast immer.

Vorteil: Es genügt ein geeignetes Telefon. Eigentlich sollten alle Handys, Smartphones und Büro-Tischtelefone Dreier-Konferenzen können.

Nachteile: Wenn Sie keine Flat-Rate haben, fallen Gebühren an. Meist können auf diesem Weg höchstens Drei teilnehmen.

Klassische Telefonkonferenz

Für die meisten Arbeitsabsprachen braucht man kein Bild, es reicht eine Telefonkonferenz.

Vorteil: Ein Telefon genügt, um an einer Telefonkonferenz teilzunehmen. Sie können also auch von unterwegs konferieren, und Gäste können problemlos dazukommen. Oft genügt auch die bestehende Telefonanlage oder Ihr vorhandener Telefonanbieter.

Nachteile: Wenn Sie keine Flat-Rate haben, fallen Gebühren an. Wenn Sie die Telefonanlage im Büro nutzen, dann belegt jede teilnehmende Person eine

Leitung – das kann schnell eng werden.

Wie Sie klassische Telefonkonferenzen nutzen können: Um eine Telefonkonferenz über Ihre Telefonanlage einzurichten, schauen Sie am besten in die Anleitung – Telefonanlagen sind zu verschieden, um hier Tipps geben zu können.

Falls Ihr Telefonanbieter keine Telefonkonferenzen anbietet: Es gibt einige Anbieter für Telefonkonferenzen, viele davon auch kostenlos. Wir können diese leider nicht prüfen und daher keinen Anbieter empfehlen. Anbieter aus Deutschland unterliegen den gleichen Gesetzen wie Anbieter von Telefonschlüssen – ein gewisses Grundvertrauen können Sie diesen also entgegenbringen.

Mumble

Wenn Sie sowieso viel am Rechner arbeiten, oder viel mit anderen Ländern telefonieren, können Sie diese Internet-Telefonie benutzen.

Vorteil: Mumble funktioniert auch mit vielen Teilnehmenden – mit Mumble können Sie sogar Großveranstaltungen digital abhalten. Es ist ein offener Standard und die Programme zur Teilnahme sind als freie Software erhältlich. Die Übertragung erfolgt mit sicherer Verschlüsselung zwischen Server und Client (damit ist das Programm des/der Nutzer:in gemeint).

Nachteile: Anders als bei den browser-

basierten Videokonferenzen müssen Sie für Mumble Software installieren. Gäste können zwar leicht teilnehmen, benötigen dafür aber auch die Software.

Wie Sie Mumble nutzen können: Wir verlinken über die Jahrbuch-Webseite die Erläuterungen der Freifunker.

Chatten, Koordinieren und Abstimmen

Chatten: Alternativen zu WhatsApp

Alternativen zu WhatsApp gibt es viele und die Liste aktuell zu halten, Änderungen zu beobachten und zu testen kostet uns viel Zeit und Nerven. Bitte schauen Sie auf digitalcourage.de/messenger nach dem aktuellsten Stand. Derzeit (Herbst 2021) sind XMPP und Signal unsere Favoriten.

XMPP: Viel Freiheit und Privatsphäre, leichte Komfort-Einschränkungen, weniger Verbreitung. Ein XMPP-Client wie z. B. Conversations/blabber.im (für Android), Monal (für iOS) und Gajim (für den PC), sofern die Ende-zu-Ende-Verschlüsselung via OMEMO aktiviert ist, sind unsere Empfehlungen für alle, die bereit sind, für die Vertraulichkeit ihrer Kommunikation minimalen Extra-Aufwand in Kauf zu nehmen.

Signal: Bequeme Einrichtung und Nutzung, weniger Privatsphäre. Die Signal-App ist kostenlos und intuitiv bedienbar. Allerdings lädt Signal Ihr Telefonbuch auf

deren Server hoch, wie WhatsApp es beispielsweise auch tut. Immerhin versucht man die ausgetauschten Daten möglichst gut zu schützen.

Termine finden

Nuudel heißt das Digitalcourage-Angebot, mit dem Sie ganz einfach und datenschutzfreundlich Termine finden und Abstimmungen organisieren können.

nuudel.digitalcourage.de

Vorteil: Betrieben von Digitalcourage und garantiert datenschutzfreundlich.

Nachteile: uns sind keine bekannt.

Wie Sie Nuudel nutzen können: Gehen Sie auf nuudel.de und wählen Sie, ob Sie eine Terminumfrage oder Ja-Nein-Vielleicht-Umfrage erstellen wollen. Der Rest sollte selbsterklärend sein.

Umfragen

Nextcloud Forms

Komplexere Umfragen mit mehreren Fragen, Einfach- oder Mehrfachauswahl, Freitext, etc. erstellen Sie in Ihrer Nextcloud. Die Antworten werden grafisch aufbereitet und Sie können sie einfach als Tabelle herunterladen. War Nextcloud Forms anfangs nur ein Aschenputtel, ist es inzwischen eine stolze Prinzessin.

Vorteil: Wenn Sie eine Nextcloud betreiben, bleiben alle Antworten auf Ihrem Server.

Nachteil: Alle Fragen erscheinen auf einer Seite, wodurch lange Umfragen

genau das werden: lang.

Wie Sie Nextcloud Forms nutzen können: Nur innerhalb einer Nextcloud, in der die App „Forms“ installiert ist.

CryptPad-Umfrage

Vorteil: Wenn Sie CryptPad benutzen, brauchen Sie kein weiteres Tool.

Nachteil: Es kann nur Ja-Nein-Enthaltung-Fragen und ist nicht sonderlich hübsch.

Wie Sie CryptPad Umfrage nutzen: Klicken Sie auf der Startseite eines CryptPads oder in Ihrem CryptDrive auf „Umfrage“.

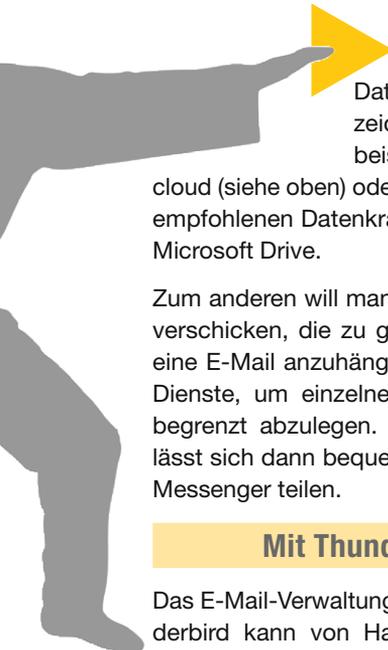
Was wir nicht empfehlen

- ▶ Doodle, denn die Website ist werbefinanziert und enthält nach unserer Untersuchung 19 Tracker.
- ▶ Google Forms, denn es kommt ja von Google.

Daten teilen und austauschen

Man kann zwischen zwei Arten unterscheiden, Dateien online zu teilen: Zum einen eine dauerhafte gemeinsame





Dateiablage mit Verzeichnisstruktur, wie beispielsweise Nextcloud

(siehe oben) oder die von uns nicht empfohlenen Datenkraken Dropbox und Microsoft Drive.

Zum anderen will man oft nur eine Datei verschicken, die zu groß ist, um sie an eine E-Mail anzuhängen. Hierfür gibt es Dienste, um einzelnen Dateien zeitlich begrenzt abzulegen. Der Downloadlink lässt sich dann bequem per E-Mail oder Messenger teilen.

Mit Thunderbird

Das E-Mail-Verwaltungsprogramm Thunderbird kann von Haus aus zu große Anhänge zu einem solchen Dienst hochladen. Standardmäßig schlägt Thunderbird hierfür den Dienst „WeTransfer“ vor. Leider ist dieser Dienst mit einem Google-Tracker verseucht, und er erscheint uns auch sonst nicht vertrauenswürdig. So richten Sie einen besseren Dienst („Plik“) zum Dateiaustausch in Thunderbird ein:

1. Im Hamburger-Menü (drei waagerechte Striche) → Einstellungen → Verfassen → nach unten scrollen bis „Anhänge“ → weitere Anbieter finden
2. bei „FileLink für Plik“ auf [+ zu Thunderbird hinzufügen] klicken und das Add-On installieren → Tab schließen
3. in den Einstellungen unter „Anhänge“ auf „Plik hinzufügen“ klicken und auf [Speichern] klicken. (Sollte der Speichern-Knopf ausgegraut ein: zweimal

auf das Kästchen „Uploads nach dem ersten Download löschen“ klicken und dann speichern.)

Falls Sie **Nextcloud** oder **Owncloud** haben, können Sie diese nutzen. Gehen Sie dazu vor wie oben beschrieben, wählen Sie aber „cloud – FileLink für Nextcloud und ownCloud“. Klicken Sie unter Anhänge natürlich auf „cloud hinzufügen“ und tragen die Zugangsdaten für Ihre Nextcloud/Owncloud ein.

Wenn das einmal eingerichtet ist, können Sie beim Schreiben von E-Mails Anhänge über Nextcloud oder Plik teilen, indem Sie neben „Anhang“ auf das √ klicken und Filelink → *cloud bzw. Plik auswählen. Oder sie stellen in den Einstellungen ein, dass das ab einer bestimmten Dateigröße automatisch passieren soll.

Anonym via Tor

OnionShare ist ein komfortables kleines Programm, das einen Onion-Dienst im Tor-Netz einrichtet, um Dateien bereitzustellen. Diese lassen sich dann per Tor Browser abrufen. Onionshare ist einfach zu installieren. Wer das spurearme Betriebssystem Tails benutzt, hat Onionshare schon dabei.

Post-It Tafeln, Bilder und Textschnipsel teilen

Es gibt noch eine Unmenge weiterer, spezialisierter Onlinedienste. Beispielsweise, um ein Brainstorming mit Post-it-



Zetteln auf einer Tafel zu machen. Oder um Bilder oder Text-Schnipsel zu teilen, die nach einiger Zeit wieder gelöscht werden.

Eine schöne Sammlung solcher Online-dienste haben die „Chatons“ zusammengestellt: entraide.chatons.org/de/

Daten und E-Mails verschlüsseln

E-Mails verschlüsseln

Am besten wäre natürlich, wenn wir alle nur noch verschlüsselte E-Mails verschicken würden. Das ist leider immer noch nicht ganz so einfach. Wir empfehlen es trotzdem, weil der Aufwand sich lohnt. Auf der Jahrbuch-Webseite finden Sie einen Link zu den Empfehlungen unserer AG Digitale Selbstverteidigung – und falls Sie noch eine Mailadresse von Anbietern wie web.de oder gmx.de haben, überlegen Sie bitte, ob Sie nicht zu einem datenschutzfreundlichen Mailanbieter wie posteo.de oder mailbox.org wechseln wollen.

Privacy Captcha

Um kurze sensible Informationen wie eine Adresse oder eine Telefonnummer, die Sie per Mail verschicken müssen, wenigstens ein bisschen zu schützen, gibt es unsere Website www.privacy-capture.net. Der Trick: Sie schreiben die Daten in ein Feld, und sie werden in eine Bild-Datei umgewandelt. Diese lässt sich dann nicht mehr so einfach wie ein Mail-Text automatisch mitlesen oder durchsuchen. Probieren Sie es einfach mal aus – es ist wirklich ganz einfach und – es wirkt.



Schütze deine privaten Daten vor automatisierter Verarbeitung. Erfahre mehr...

Digitalcourage e.V.
 Phone: +49-521-1639 1639
 Fax: +49-521-61172
 E-Mail: mail@digitalcourage.de
 PGP-Key: 0x8BCDA3492DC2A7D0

Generate 122/500



Daten verschlüsseln mit VeraCrypt

Wer Daten vom Arbeits-PC auf den Privatrechner zieht, sollte bedenken, dass diese besonders geschützt werden müssen. Noch einmal mehr, wenn es sich um personenbezogene Daten von Kund.innen oder Schüler.innen handelt.

Legen Sie solche Daten am besten in einen VeraCrypt-Container. VeraCrypt ist relativ schnell zu erlernen und sehr flexibel, da es auf allen Plattformen und Datenträgern funktioniert.

VPN verpflanzt Ihr Homeoffice ins Firmennetz



VPN steht für „Virtual Private Network“. Das ist meist eine Software, die dafür sorgt, dass sich Ihr Computer so verhält, als sei er direkt ans Netzwerk Ihrer Firma angeschlossen. Dadurch können Sie Dienste im internen Netz (Intranet) ihrer Firma nutzen, als wären Sie selbst dort. Das ist sehr praktisch. Es gibt aber

auch Fallen, in die man tappen kann:

- ▶ VPN kann alle ihre Netzwerkaktivitäten durchs Firmennetz leiten. In Hotel-WLANs kann das sinnvoll sein. Vermeiden Sie aber private Internet-Aktivitäten, während Sie VPN aktiviert haben, sonst liest Ihre Firma mit! Fortgeschrittene können alternativ die Option Split Tunneling nutzen – dann wird das VPN nur für Kontakte mit bestimmten IP-Adressbereichen genutzt.

Erhältlich im Digitalcourage-Shop! Anonym surfen mit dem PrivacyDongle



Für Mac ab OS X 10.6, Windows ab Windows 2000 und Linux, Unix, BSD (vom Rechner starten). Die Tor-Anonymisierungssoftware ist auf dem PrivacyDongle bereits konfiguriert. Einfach einstecken und anonym lossurfen.

**Marken-USB-Stick (Kingston)
Metallgehäuse und Schlüsselanhänger
USB 3.0 Hi-Speed, 32 Gigabyte**

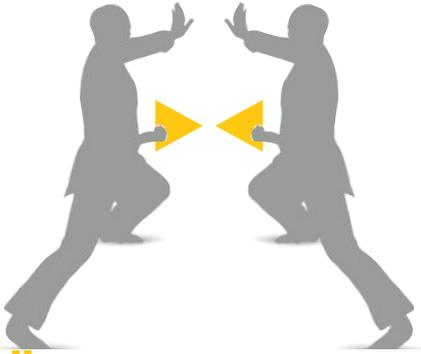
Preis: 30 Euro / Stück

▶ shop.digitalcourage.de

- ▶ Nutzen Sie keine kommerziellen VPN-Dienste! Viele kommerzielle VPN-Dienstleister werben mit falschen Versprechen wie IT-Sicherheit, Datenschutz oder Anonymität. Fallen Sie nicht darauf rein! Für anonymes Surfen empfehlen wir den Tor-Browser.
- ▶ Nutzen Sie quelloffene, Freie Software! Auch wenn Ihre Firma kommerzielle Software einsetzt, müssen Sie das zu Hause nicht unbedingt tun. Wer Linux hat, kann die Freie Software vpnc nutzen, um sich mit einem Cisco-VPN zu verbinden. Wer per SSH Direktzugriff auf einen Firmenserver hat, kann sich mit sshuttle ein eigenes kleines VPN bauen.

CryptPad

Für umfassende Teamarbeit



Über zehn Jahre lang haben wir bei Digitalcourage täglich mit Etherpads als Software zum gemeinsamen Schreiben von Texten gearbeitet. Inzwischen wurden Etherpads durch CryptPads ersetzt. Aber wer denkt, dass CryptPad nur ein etwas modernisiertes EtherPad sei, wird sich die Augen reiben.

CryptPad entstand durch die Arbeit von Privatsphäre-Aktivist:innen im Rahmen eines französischen Forschungsprojekts. Inzwischen steht das Projekt unter der Schirmherrschaft der unabhängigen Softwareschmiede XWiki SAS, die für die gleichnamige Wiki-Software bekannt sind, und wird durch Spenden, Fördermittel und Abogebühren finanziert. CryptPad ist quelloffene Software, die unter einer freien Lizenz steht.

Viele Anwendungen unter einem Dach

Wer auf der Suche nach einem sicheren Ersatz für eine ganze Reihe von Diensten

ist, könnte mit CryptPad fündig werden. Denn im Gegensatz zum alten EtherPad bietet CryptPad nicht nur einen Texteditor an, sondern eine ganze Reihe von Funktionen.

Für Texte stehen gleich zwei Anwendungen bereit. Wer lieber in Markdown oder in anderen Sprachen schreibt, wird sich mit den **Code-Pads** sehr wohl fühlen. Nur hier werden Texte in Farbe der Autor:innen markiert.

Wer lieber ähnlich wie in LibreOffice und anderen klassischen Office-Anwendungen Texte schreibt und Formatierungen sieht („What you see is what you get“), dürfte **Rich-Text-Pads** bevorzugen. Dokumente lassen sich hier auch in bekannte Office-Formate für andere Anwendungen exportieren.

Mit der **Tabelle** steht eine mächtige Tabellenkalkulation zur Verfügung, mit der auch komplexe Rechenoperationen kein Problem darstellen sollten.

Ein weiteres Highlight ist die Anwendung **Formular**. Mit ihr lassen sich umfassende Umfragen und Fragebögen erstellen, die sich nicht vor unfreien Alternativen wie Google Forms zu verstecken brauchen. Mit der neuen Vorlage „schnelle Terminumfrage“ macht CryptPad sogar unserem Nuudel Konkurrenz.

Außerdem gibt es einen Powerpoint-Ersatz („**Präsentation**“) und eine elek-

tronische Tafel („**Whiteboard**“). Für die Projektplanung ist ein Kanban dabei.

Das CryptDrive als Organisations- und Speicherzentrum

Das wichtigste Alleinstellungsmerkmal von CryptPad ist das CryptDrive. Direkt nach der Erstellung eines Accounts durch Angabe von Benutzernamen und Passwort stehen damit ein eigener Speicherbereich und eine Dateiverwaltung auf dem CryptPad-Server zur Verfügung. Dort können neben den aus den CryptPad-Apps erstellten Inhalten auch andere Dateien hochgeladen und mit anderen Nutzer:innen geteilt werden. Außerdem haben angemeldete Nutzende die Möglichkeit, Backups herunterzuladen.

Der wichtigste Unterschied zwischen CryptPad und vergleichbarer Software liegt in der Verschlüsselung: Alle Inhalte von CryptPad werden ausschließlich verschlüsselt auf dem Server abgelegt. Ohne Kenntnis des Links zu einem Dokument kann nicht darauf zugegriffen werden. Admins sehen nur verschlüsseltes Kauderwelsch auf dem Server, aber nicht nur das: Auch Accounts

können durch die Admins nicht eingesehen oder verwaltet werden.

Zur Arbeit in Gruppen können **Teams** erstellt werden, die über ihr eigenes CryptDrive verfügen. Zur Organisationen können Mitgliedsrechte frei eingestellt werden.

Mehr Sicherheit, aber auch Eigenverantwortung

Wichtig: Wer sich einen Account erstellt, sollte sicher gehen, dass die Zugangsdaten nicht verloren gehen. Eine Möglichkeit zum Zurücksetzen des Passwort gibt es nicht – auch die Admins können hier nicht helfen. Wir empfehlen ausdrücklich, die Zugangsdaten in einer Passwortverwaltung zu speichern; notfalls können die Zugangsdaten auf Papier notiert werden.

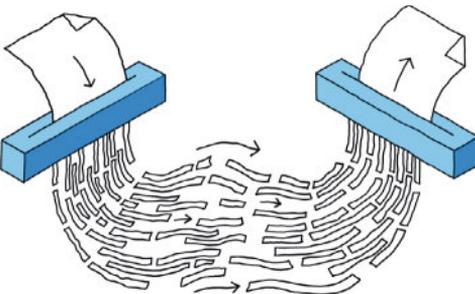
Wer CryptPad gänzlich anonym verwenden möchte, sollte zusätzlich auf den frei verfügbaren **Tor-Browser** setzen.

Neugierig geworden?

Dann können Sie CryptPads einfach ausprobieren: Neben der offiziellen Instanz cryptpad.fr stellt Digitalcourage eine eigene Instanz von CryptPad zur Verfügung, die kostenlos genutzt werden kann: cryptpad.digitalcourage.de

Hilfestellungen und Anleitungen zu den einzelnen Funktionen von CryptPad findet man in der offiziellen Dokumentation, die auch auf Deutsch verfügbar ist: docs.cryptpad.fr/de

Grafik: cryptpad.fr



Fediverse

So geht gutes Social Media

Sie haben das Gefühl, dass es falsch ist, Facebook, Instagram oder Twitter zu nutzen? Tatsächlich gibt es gute Gründe, die US-amerikanischen Netzwerke zu meiden, um Privatsphäre und Selbstbestimmung zu behalten. Deswegen müssen Sie aber nicht auf Social Media verzichten; denn es gibt eine gute Alternative – das Fediverse.

Fedi... was?

Das Fediverse ist ein dezentrales Kommunikationsnetz. Anders als bei Facebook, Instagram, TikTok und Co. spielt es technisch kaum eine Rolle, welchen Anbieter Sie nutzen: Sie können im Fediverse auch mit den Nutzer:innen kommunizieren, die auf einer anderen Fediverse-Plattform unterwegs sind. Das ist bisher einzigartig bei

sozialen Netzwerken und bedeutet: Bei bestimmten Fediverse-Angeboten (z.B. Mastodon) können Sie sogar wechseln, ohne Ihre Kontakte zu verlieren.

Das Fediverse besteht aus unabhängigen Servern (Instanzen), auf denen freie Software läuft, die das ActivityPub-Protokoll umsetzt und offene Schnittstellen bietet.

Offene Schnittstellen und Datenportabilität

„Offene Schnittstellen“ klingt technisch, ist aber einer der wichtigsten Gründe, weshalb wir im Fediverse die beste Antwort auf unsere gesamtgesellschaftlichen Probleme in Bezug auf Social Media sehen. Offene Schnittstellen ermöglichen Dezentralität.

Dadurch können wir wieder selbst über unsere Kommunikation bestimmen und nicht großen Konzernen Macht darüber einräumen. Facebook, Twitter und Co. machen sich den sogenannten Plattformeffekt zunutze (siehe auch Netzwerkeffekt und Lock-in-Effekt).



Dieser verhindert, dass Sie schon längst von Facebook oder Instagram weggegangen sind. Die meisten Leute bleiben v.a. deshalb bei den großen Anbietern, weil dort ihre Freund:innen sind, zu denen sie den Kontakt halten wollen. Dafür aber müssen sie jede Änderung der AGB schlucken, auch wenn das gegen ihre informationelle Selbstbestimmung geht.

Dank Datenportabilität ist damit Schluss. Denn damit können Sie wählen. Wenn Ihr Anbieter z.B. Menschenrechtsaktivist:innen blockiert oder Despoten ein Sprachrohr gibt, können Sie sich einen anderen Dienst suchen und dennoch alle Ihre Kontakte im Fediverse behalten. Datenportabilität ist das einzige komplett neue Betroffenenrecht der DSGVO; leider wird es außerhalb des Fediversums bisher nur zögerlich umgesetzt.

Das gibt Ihnen Kontrolle zurück und führt zwangsläufig dazu, dass die Menschen in die Entscheidungen mehr einbezogen werden.

Obwohl alle Fediverse-Instanzen grundsätzlich mit allen anderen Nachrichten austauschen können, ist es wichtig, die Heimat-Instanz, bei der Sie Ihr Konto anlegen, gut zu wählen. Zum einen, damit die lokale Zeitleiste relevante Inhalte enthält, zum anderen, weil die Instanz bestimmte Regeln festlegt und diese zu Ihnen passen sollten. Im Rahmen der gesetzlichen Vorgaben findet jede Fediverse-Instanz ihre eigenen Methoden, um das richtige Gleichgewicht zwischen Redefrei-

heit und Schutz vor Hassrede zu finden. Dafür sollte jede Instanz ein Moderationsteam haben, aber es kommt vor allem auf die User:innen selbst an. Nur so können wir uns den zunehmenden gesellschaftlichen Problemen, die sich aus Social Media ergeben, erfolgreich stellen.

Die vielen Optionen des Fediverse

Vergleichbar mit Facebook

Friendica und Hubzilla: Hier können Sie Beiträge gleichzeitig im Fediverse, auf Twitter und auf Diaspora veröffentlichen – also in fast jedem sozialen Netzwerk außer Facebook und Instagram.

Zap: ethische Alternative zu Facebook, quelloffen, aber leider nur wenige deutschsprachige Instanzen.

Mobilizon: vielversprechende freie Alternative zu Facebook-Events.

Diaspora: eine der ältesten Facebook-Alternativen mit starkem Fokus auf Privatsphäre und Kontrolle. Sie können z.B. den Kreis der Empfänger:innen frei wählen. Leider kommt es teilweise zu Kompatibilitätsproblemen mit anderen Anbietern.

Vergleichbar mit Twitter

Mastodon: Hier verschicken Sie keine Tweets, sondern Tröts. Großen Wert legt die Community auf einen freundlichen Umgangston und konstruktive Beiträge. Sie können den Empfänger:innenkreis der Nachrichten einschränken

und entscheiden, ob eine Nachricht von anderen geteilt werden darf. Gern gesehen sind Inhaltswarnungen und Bildbeschreibungen (wichtig für Barrierefreiheit). Einschränkung: Beiträge sind maximal 500 Zeichen lang.

Wer sich für Mastodon entscheidet, findet auf der offiziellen Projektwebsite joinmastodon.org eine Instanz in der passenden Sprache und inhaltlichen Ausrichtung. Die Anleitung, um einen Mastodon-Account (auch auf dem Smartphone) einzurichten, finden Sie auf der Digitalcourage-Seite.

Pleroma: ähnelt Mastodon sehr. Auf vielen Pleroma-Instanzen können Sie Beiträge mit mehr als 500 Zeichen verfassen.

GNU-Social: eine der ersten freien Twitter-Alternativen. Leider noch nicht mit allen hier genannten Fediverse-Diensten kompatibel.

Vergleichbar mit Instagram

Pixelfed: für visuelle Menschen die Antwort des Fediversums auf Instagram.

Vergleichbar mit YouTube

PeerTube: freie und dezentrale Alternative zu Videoplattformen. Mehr als 60.000 Nutzer:innen und 400.000 Videos.

Vergleichbar mit Soundcloud

Funkwhale: wie PeerTube, aber für Audio statt Video. Die App finden Sie im F-Droid-Store.

Vergleichbar mit Reddit

Lemmy: Social-News-Aggregator für Nachrichten-Junkies, die Reddit oder HackerNews nutzen. Hier können Sie Links teilen und diskutieren.

► Crossposting mit der Social-Media-Bridge

Sie wollen das Fediverse in Ruhe ausprobieren und erstmal Ihre Accounts bei Facebook, Twitter und Co. behalten, aber keine doppelten Posts schreiben? Kein Problem. Dafür können Sie den Twitter-Mastodon-Crossposter nutzen. Das ist ein quelloffener Bot, der Ihre Tweets zu Ihrer Fediverse-Instanz spiegelt oder umgekehrt.

Zitate, Retweets und Antworten bleiben normalerweise auf die jeweilige Plattform beschränkt. Auch Antworten gehen nur auf einer Plattform ein. Social Media aber lebt vom Austausch und Diskurs. Deshalb ist es wichtig, dass Sie sich regelmäßig auf Mastodon einwählen. Sonst entsteht ein unattraktiver Zombieaccount, der zwar dauernd plappert, aber nicht für Antworten, Rückfragen oder Kritik erreichbar ist.

Wir empfehlen, Mastodon als Hauptinstanz zu betrachten und die Nachrichten von dort nach Twitter zu senden.

Wenn Sie ausschließlich über Ihr Smartphone tröten bzw. twittern, können Sie die freie App Twidere nutzen (erhältlich im F-Droid-Store), die beide Kanäle gleichzeitig füttert. Damit haben Sie beide Plattformen gleichermaßen im

Blick, Twitter versucht allerdings immer wieder, Störschritte einzubauen.

Wem folgen?

Beobachten Sie, wem andere folgen und mit wem sie interessante Dialoge führen. Digitalcourage betreibt selbst Accounts und zeigt Ihnen auch Nutzer:innen aus dem DC-Umfeld.

► Das Fediverse ist kein Heilsbringer

Das Fediverse ist nicht die einfache Antwort auf unsere Probleme. Auch hier gibt es Accounts oder Instanzen, die inakzeptable Inhalte verbreiten. Doch das Fediverse ermöglicht uns, diese Probleme sinnvoll anzugehen und zu diskutieren. In vielen kleinen Diskussionen auf Augenhöhe finden die Instanzen zunächst im Kleinen eine Haltung zu unterschiedlichen Fragen. Jede:r kann die Instanz wählen, die ihr/ihm am besten entspricht. So wird ein gesellschaftlicher Diskurs ermöglicht, in dem wir gemeinsam Antworten finden können.

Warum Sie auf Facebook und Co. verzichten sollten

Facebook, Instagram, Twitter, YouTube, Soundcloud etc. haben keine offenen Schnittstellen. Sie bilden jeweils ein eigenes Universum, innerhalb dessen sie konkurrenzlose Monopolisten sind. Als Nutzer:in haben Sie also nur die Möglichkeit, alle Änderungen des Betreibers

(auch zu Ihren Ungunsten) zu akzeptieren oder die Plattform zu verlassen und damit den Kontakt zu allen verlieren, mit denen Sie dort verbunden sind. Das ist ein hoher Preis und tut Ihnen womöglich mehr weh als dem Plattformbetreiber. Denn was bringt es Ihnen, zu einem Anbieter zu wechseln, auf dem Sie keine Person erreichen, die für Sie relevant ist?

Den kommerziellen Plattformen geht es nicht darum, Ihnen ein gutes Angebot zu machen, sondern ums Geld verdienen. Es geht ihnen darum, Sie möglichst oft und effektiv mit Werbung in Kontakt zu bringen. Besonders viele Werbeeinnahmen lassen sich erzielen durch

- Nachrichten, die zu Interaktionen verleiten (intensiver Werbekontakt)
- süße und witzige Inhalte wie Katzenfotos (werden gerne geteilt und geliked)
- Falschaussagen (führen zu Beifall und Korrekturen)
- Hassnachrichten (bekommen Zustimmung oder Solidarisierung mit den Angegriffenen)

Differenzierte Inhalte, die inhaltlich in die Tiefe gehen, werden meist lesend zur Kenntnis genommen, führen aber viel seltener zu Interaktionen und werden deswegen algorithmisch diskriminiert.



Der freie App-Store

F-Droid und seine Apps

Android-Nutzer:innen, die nicht mehr vom Google-Play-Store abhängig sein wollen, sollten den alternativen App-Store „F-Droid“ nutzen, in dem ausschließlich Freie Software vertrieben wird. Die Apps sind funktional, in der Regel datenschutzfreundlich, nicht kommerzialisiert und verbraucher:innenfreundlich. Es gibt weder Kostenfallen noch Icons und Werbung. F-Droid kann parallel zum Play-Store und anderen Store-Apps genutzt werden.

Alle Links zu den folgenden Empfehlungen finden Sie auf der Jahrbuch-Webseite.

Internet und Kommunikation

- ▶ **blabber.im:** einsteigerfreundlicher Client für Chat-Protokoll XMPP (Jabber) auf Basis von Conversations.
- ▶ **Conversations:** Client für Chat-Protokoll XMPP (Jabber), der die sichere Verschlüsselung OMEMO unterstützt.
- ▶ **DAVx⁵:** hilft, die eigenen Kontakte, Aufgaben und Kalendereinträge geräteübergreifend zu synchronisieren.
- ▶ **Element:** Referenzmessenger mit Ende-zu-Ende-Verschlüsselung für das Matrix-Protokoll.
- ▶ **FairEmail:** moderner E-Mail-Client mit Oberfläche im Material-Design. Einige Funktionen müssen bezahlt werden.
- ▶ **Fedilab:** Client für zahlreiche Fediverse-Dienste. Unterstützt die gleichzeitige Benutzung mehrerer Accounts.

Auch als schlankere Lite-Version verfügbar.

- ▶ **Feeder:** hilft beim Verwalten und Lesen von Newsfeeds via RSS/Atom.
- ▶ **Fennec F-Droid:** befreite Variante des Browsers Mozilla Firefox für Android. Kann mit Add-ons erweitert werden.
- ▶ **Fritter:** Twitter ohne Account komfortabel nutzen.
- ▶ **K-9-Mail:** Klassiker unter den freien Android-Apps mit vielen Features. Im Verbund mit der App OpenKeyChain können E-Mails via OpenPGP verschlüsselt werden.
- ▶ **RedReader:** leichtgewichtiger Client für Reddit.
- ▶ **Twidere:** alternativer Client für Twitter. Bietet viele Optionen und verwaltet auch mehrere Accounts, auch bei den dezentralen Twitter-Alternativen GNU social und Mastodon.
- ▶ **Twire:** freier Client für die Streamingplattform Twitch.tv.

Multimedia

- ▶ **AntennaPod:** verwaltet und spielt Podcasts ab.
- ▶ **NewPipe:** einfacher, effizienter Zugang zur Videoplattform YouTube, PeerTube und weiteren Diensten. Sie können ohne Google-Account Kanäle abonnieren und Videos speichern.
- ▶ **OpenCamera:** umfassende Kamera-App.Tipp: Camera2-API einschalten.
- ▶ **QR Scanner (Privacy Friendly):** sicherer QR-Code-Scanner und -Generator.

- ▶ **RadioDroid**: ruft zentrale Webradio-verzeichnisse und kann sie abspielen.
- ▶ **Simple Gallery Pro**: Galerie-App, um Bilder und Videos zu verwalten und anzuzeigen.
- ▶ **Transistor**: gute Radio-App, schlanker als RadioDroid. Sie tragen ihre Radiosender selbst ein.
- ▶ **Vanilla Music**: schlanker Audioplayer.
- ▶ **VLC**: ungeschlagener Media-Player, der die meisten Audio- und Videoformate abspielen kann.
- ▶ **Voice**: spielt und verwaltet Hörbücher.
- ▶ **Zapp**: zeigt Streams deutschsprachiger öffentlich-rechtlicher TV-Sender und bietet Zugriff auf deren Mediatheken.
- ▶ **AFWall+**: Firewall auf Basis von iptables. Einige wenige Bezahlfunktionen. Benötigt Root-Rechte.
- ▶ **Exodus**: prüft installierte Apps auf vorhandene Trackingkomponenten.
- ▶ **Greentooth**: schaltet die Bluetooth-Schnittstelle automatisch ab, wenn sie nicht gebraucht wird.
- ▶ **KeePassDX**: moderner Passwortmanager auf Basis von KeePass, unterstützt das automatische Ausfüllen von Log-in-Feldern.
- ▶ **NetGuard**: Firewall, um ein- und ausgehende Verbindungen via VPN-Schnittstelle zu regeln. Einige Bezahlfunktionen.
- ▶ **OpenKeyChain**: Schlüsselverwaltung für OpenPGP-Schlüssel. Hilft bei Ver- und Entschlüsselung entsprechender Inhalte anderer Apps.

Navigation

- ▶ **Öffi**: Bekannte ÖPNV-App – andere Bedienung als bei Transportr mit ähnlichem Funktionsumfang.
- ▶ **Organic Maps**: attraktive und übersichtliche Navigationsanwendung auf Basis von OpenStreetMap, weniger Funktionen als OsmAnd+.
- ▶ **OsmAnd+**: Landkarten- und Navigationsanwendung auf Basis des Kartenmaterials von OpenStreetMap. Die Karten sind oft besser als die von Google oder Bing und können auch offline genutzt werden – das spart Datenvolumen.
- ▶ **Transportr**: bietet Zugriff auf Fahrpläne der Deutschen Bahn und vieler lokaler Verkehrsverbünde weltweit.
- ▶ **Scrambled Exif**: entfernt Metadaten bei Bildern und Fotos.
- ▶ **Shelter**: isoliert installierte oder neue Apps im Android-Arbeitsprofil. So können z.B. Apps von den Kontakten im Hauptprofil ferngehalten oder mehrere Accounts parallel genutzt werden. Wichtig: Vorher Hinweise der Entwickler:innen lesen.
- ▶ **UntrackMe**: leitet auf datenschutzfreundliche Varianten von z.B. Twitter, Google Maps und YouTube um. Kann Trackingparameter aus URL entfernen. Auch als Lite-Version verfügbar.
- ▶ **WiFi Automatic**: hilft, das WLAN unter bestimmten Umständen automatisch zu (de-)aktivieren.

Privatsphäre und Sicherheit

- ▶ **Aegis**: generiert Codes zur Zwei-Faktor-Authentifizierung via TOTP.

Produktivität

- ▶ **AnkiDroid**: Lernkartei-App mit kom-

fortabler Kartenerstellung. Bietet zu fast jedem Thema viele Inhalte aus der Community.

- ▶ **Etar:** Kalender-App mit Erinnerungsfunktion und Widgets. Kann sowohl Offline-Kalender als auch via DAVx⁵ synchronisierte Kalender anzeigen.
- ▶ **MuPDF Viewer:** PDF-Reader, der auch mit XPS-Dateien und E-Books umgehen kann.
- ▶ **Notepad:** einfache App, um Textnotizen zu erstellen und zu verwalten.
- ▶ **OpenTasks:** Aufgabenverwaltung. Im Verbund mit DAVx⁵ können Sie Ihre Aufgaben auch über mehrere Systeme synchronisieren.
- ▶ **QuickDic:** Offline-Wörterbuch, das viele Sprachen unterstützt.
- ▶ **Web Opac:** bietet Zugriff auf hunderte von Stadt- und Universitäts-Bibliotheken – direkt über die jeweilige Online-Schnittstelle.

Spiele

- ▶ **Apple Flinger:** freie Variante von Angry Birds.
- ▶ **BobBall:** taktisches Geschicklichkeitsspiel mit Suchtpotenzial.
- ▶ **Lexica:** simples Wortfindespiel. Aktuell leider nur in Englisch voll nutzbar.
- ▶ **Mindustry:** komplexe Mischung aus Aufbau- und Tower-Defense.
- ▶ **Minesweeper-Antimine:** sehr gut gemachte Adaption des Windows-Klassikers Minesweeper.
- ▶ **Minetest:** freier Minecraft-Klon mit vielen Features.
- ▶ **Puzzles:** viele kleine Rätselspiele für die kurze Wartezeit zwischendurch.
- ▶ **OpenSudoku:** wunderbare Sudoku-Ansicht.
- ▶ **Pixel Wheels:** ein Rennspiel aus der Vogelperspektive.
- ▶ **Pysolfc:** große Sammlung mehrerer Kartenspiele (wie z.B. Solitär).
- ▶ **Rabbit Escape:** bringt die Lemminge in Hasenform aufs Smartphone.
- ▶ **Shattered Pixel Dungeon:** klassischer Rogue-Like im Fantasy-Stil.
- ▶ **Simple Solitaire Collection:** klassisches kartenbasiertes Solitär in mehreren Varianten.
- ▶ **SuperTuxKart:** von Mario Kart inspiriertes Rennspiel, in dem Freie-Software-Maskottchen gegeneinander antreten.
- ▶ **Turo:** Spiel, in dem Sie möglichst viele Blöcke stapeln, ohne dass der Turm umkippt.

Sport und Gesundheit

- ▶ **Corona Contact Tracing Germany:** komplett freie und inoffizielle Variante der Corona-Warn-App. Kompatibel mit der offiziellen App, funktioniert ohne Play-Dienste, nutzbar ab Android-Version 5.
- ▶ **Drip:** Zyklus-App mit vielen Funktionen und minimalen Berechtigungen.
- ▶ **FitoTrack:** Fitness-Tracking lokal auf dem Gerät.
- ▶ **OpenFoodFacts:** Einscannen von Lebensmitteln, Infos über Inhaltsstoffe und Nährwert.
- ▶ **OpenScale:** Kontrolle von Körpermaßen und Gewicht.
- ▶ **Periodical:** simple Zyklusapp mit minimalen Berechtigungen.

Tools

- ▶ **Aurora Store:** erlaubt Zugriff auf Google-Play-Store über anonymen Google-Account und ohne Play-Dienste.
- ▶ **CPU Info:** zeigt umfassende Informationen über Hardware und Sensordaten des Smartphones.
- ▶ **GPSTest:** prüft die Daten zur Positionsbestimmung via GPS.
- ▶ **KISS launcher:** Launcher mit alternativem Bedienkonzept – nicht mehr suchen, sondern direkt finden.
- ▶ **Material Files:** umfassender Dateimanager.
- ▶ **OpenBoard:** Alternative zu Hersteller-/Android-Tastatur ohne Datenabfluss.
- ▶ **Termux:** bringt das von Linux bekannte Terminal auf das Smartphone. Stark erweiterbar.
- ▶ **WiFiAnalyzer:** hilfreiche App, mit der Sie Ihr WLAN analysieren können.

Weiteres

- ▶ **Forecastie:** einfache, übersichtliche Wetterapp, die internationale Wetterdaten von **OpenWeatherMap.org** einbezieht.
- ▶ **Gadgetbridge:** erlaubt Verbindung und Datenaustausch mit vielen Wearables/Smartwatches ohne Hersteller-Apps oder -Konten.
- ▶ **Kleine Wettervorschau Deutschland:** bietet Wetterdaten und Unwetterwarnungen auf Basis des Deutschen Wetterdienstes (DWD).
- ▶ **Phyphox:** ermöglicht, Physik-Experimente mit Hilfe der Gerätesensordaten durchzuführen.

- ▶ **ScreenStream:** erlaubt es, den Bildschirm des Android-Geräts unkompliziert über HTTP zu teilen.

Apps aus fremden Paketquellen:

- ▶ **Bromite:** Chromium-Browser mit integriertem Werbeblocker, der auf Privatsphäre und Sicherheit optimiert ist.
- ▶ **Collabora Office:** Office-Suite auf Basis von LibreOffice.
- ▶ **Orbot:** leitet den Netzwerkverkehr ausgewählter Apps oder des gesamten Geräts durch das Tor-Netzwerk.
- ▶ **Tor Browser:** Webbrowsers zum anonymen Surfen auf Basis von Firefox.

Nachteile

Leider haben kommerzielle Anbieter F-Droid oft nicht auf dem Schirm. Daher sind ihre Apps dort unterrepräsentiert. Zwar werden viele (externe) Funktionen von F-Droid-Apps übernommen, enthalten aber keine konkreten Services. Beispiel: Apps für Bahn und ÖPNV sind ohne Ticketreservierung und -buchung. Auch Taxi-Apps, Online-Banking, vernetzte Spiele usw. fehlen. Selbst die Corona-Warn-App wurde zunächst nur für den Play-Store erstellt. Inzwischen ist sie im F-Droid erhältlich, weil sie ehrenamtlich nachgebaut wurde. Altersbeschränkungen können nicht eingestellt werden. Leider werden auch Apps angeboten, die gegen die Richtlinien des Google-Play-Stores verstoßen würden. Auch Funktionen, um Schadsoftware aufzuspüren, fehlen.

- ▶ Mehr über F-Droid, Installationsanleitungen und weitere Tipps finden Sie auf digitalcourage.de/f-droid

Kriterien für vertrauenswürdige Apps

Sie haben eine App programmiert und wundern sich, warum so wenige Leute sie benutzen, obwohl sie kostenlos ist? Das könnte daran liegen, dass die Leute Ihrer App nicht vertrauen. Das können Sie ändern! Nutzen Sie dafür unsere Checkliste für Android-Apps. Die Liste gilt sinngemäß auch für iOS-Apps.

► Eine vertrauenswürdige App hat mindestens folgende Eigenschaften:

- 1. Sie ist quelloffen.** Der Quellcode wird also fortlaufend veröffentlicht. Nur so kann von unabhängiger Seite mit vertretbarem Aufwand geprüft werden, was die App tut und was nicht. Auch Abhängigkeiten von unfreien Komponenten wie z. B. den Play-Diensten von Google sollten vermieden werden. Mindestens sollte es alternativ eine Variante der App geben, die gänzlich frei ist.
- 2. Sie ist reproduzierbar.** In den meisten Fällen wird Software nicht in Form von Quellcode, sondern als Installationspaket oder ausführbare Datei verteilt. Damit von unabhängiger Seite mit vertretbarem Aufwand nachgeprüft werden kann, dass ein Installationspaket oder eine ausführbare Datei aus dem veröffentlichten Quellcode gebaut wurde, muss dieser Bauprozess reproduzierbar sein. Das



heißt: Für einen gegebenen Quellcode wird beim Bauen immer dieselbe ausführbare Datei erzeugt. Die selbstgebaute App kann dann leicht mit der App verglichen werden, die in App-Stores und auf anderen Websites zum Download angeboten wird. Das ist heute Stand der Technik.

- 3. Sie enthält keine Tracker.** Apps, die nicht quelloffen sind, enthalten oft Tracker. Das ist Schadsoftware, die Informationen aus der App an Websites ausleitet. Wir nennen sie Schadsoftware, weil sie nicht im Interesse der User:innen agiert. Ob eine Android-App Tracker enthält, kann man bei Exodus Privacy prüfen. Auch ein Tracker, der „nur“ zum Zählen von Usern Daten an Google Analytics meldet, ist eine Schadsoftware.
- 4. Sie arbeitet möglichst datensparsam.** Nicht nur Tracker sind ein Problem für die Privatsphäre. Es ist

eine weit verbreitete Unsitte, dass Apps Daten auf dem Gerät erheben, die sie für ihre eigentliche Aufgabe gar nicht benötigen. Aufmerksam sollten Sie werden, wenn Berechtigungen abgefragt werden, die nicht zur beworbenen Funktionalität der App passen. Entwickler:innen sollten daher darauf achten, dass nur absolut notwendige Daten erhoben werden. Auf Berechtigungen, die technisch nicht zwingend notwendig sind, sollte verzichtet werden. Weniger Neugier schafft Vertrauen.

5. Sie zwingt nicht zur Benutzung eines bestimmten App-Stores.

Die Nutzung des Google-Play-Stores ist an Geschäftsbedingungen gebunden, die der informationellen Selbstbestimmung widersprechen, und auch technisch hat Google damit mehr Kontrolle über Android-Telefone als nötig. Deshalb bevorzugen gut informierte User:innen andere Wege, Apps zu installieren, z.B. F-Droid. Versuchen Sie, Ihre App in F-Droid unterzubringen! Bis dahin können Sie Ihre App in einem mit F-Droid kompatiblen Repository auf Ihrer Website bereitstellen. Oder bieten Sie wenigstens die APK-Datei auf Ihrer Website zum Download an.

6. Kein Registrierungszwang.

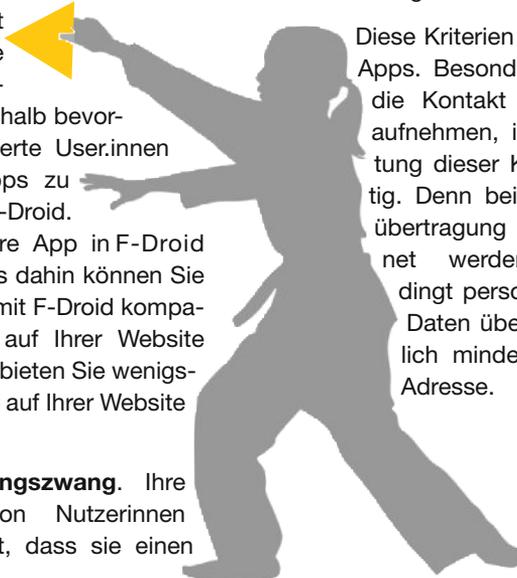
Ihre App verlangt von Nutzer:innen und Nutzern nicht, dass sie einen

Account anlegen müssen. Bei Apps, die Funktionen beinhalten, für die ein Account unerlässlich ist (zum Beispiel, wenn Daten auf unterschiedlichen Geräten genutzt werden sollen), ist nur dieser Teil von einem Log-in abhängig. Der Rest der App funktioniert ohne. Geräte haben genügend Rechenpower, so dass alle Berechnungen auf dem Gerät selbst und nicht in der Cloud ausgeführt werden können.

7. Sie hält sich an geltendes Recht.

Das sollte selbstverständlich sein, ist es aber zur Zeit nicht. Wenn eine App auch von Bürger:innen der EU genutzt wird, muss sie sich zum Beispiel an die DSGVO halten (Marktortprinzip). Wie das zu erreichen ist, beschreibt die Website gdpr4devs.com in einfachem Englisch.

Diese Kriterien gelten für alle Apps. Besonders bei Apps, die Kontakt zum Internet aufnehmen, ist die Einhaltung dieser Kriterien wichtig. Denn bei jeder Datenübertragung via Internet werden prinzipbedingt personenbezogene Daten übertragen, nämlich mindestens die IP-Adresse.



OpenStreetMap

OpenStreetMap (OSM) ist eine vollwertige und freie Alternative zu Google Maps – oft aktueller und detailreicher. Die Daten werden von mehr als 2,3 Millionen registrierten Nutzer:innen bearbeitet und weiterentwickelt. Hausnummern, Parkwege und andere spezielle Gebiete sind häufig präziser als bei Google Maps. Zunehmend werden sogar Gebäudehöhen und -formen in OSM erfasst.

Seit einigen Jahren liefern sogar offizielle Kataster- und Landesvermessungsämter Daten an OpenStreetMap und nutzen dessen Karten für eigenen Angebote.

Weil das gesammelte Material der Allgemeinheit gehört, konnten daraus viele Folgeprojekte entstehen – zum Beispiel Fahrrad-, ÖPNV- und Eisenbahnkarten.

Navigation mit OpenStreetMap

Routenplanung ist direkt in die Website von OpenStreetMap integriert. Berechnet werden die Routen von externen Diensten, die auf OpenStreetMap aufbauen. Zwischen diesen können Sie umschalten und die Ergebnisse vergleichen.

Mehr Funktionen bieten folgende Geschwister-Projekte:

- ▶ Das Web-Interface von **Graphhopper** ist schlank, schnell und kommt ohne Plug-ins aus. Sie können einstellen, ob Sie spazierengehen oder wandern, welches Fahrrad Sie nutzen oder

ob Sie einen Laster fahren. Ein nettes Gimmick ist das Höhenprofil für geplante Routen.

- ▶ Auf der Karte der **Open Source Routing Machine** (OSRM) können Sie Zwischenziele einfach hinzufügen, indem Sie einen Punkt auf der Route anklicken und wegziehen. Die Routing-Maschine dahinter wurde unter anderem vom Karlsruhe Institute of Technology (KIT) betreut.
- ▶ **OpenRouteService** wird von der Universität Heidelberg entwickelt und angeboten. Dies ist einer der wenigen Dienste, der auch Routen für Rollstuhlfahrende sucht. Zusätzlich gibt es dort interessante Auswertungen, z.B. wie weit Sie in drei Minuten zu Fuß kommen oder welche Ziele Sie nach 15 gefahrenen Kilometern erreichen.

Orientierung und Navigation für unterwegs

Auch unterwegs müssen Sie nicht auf freies Kartenmaterial verzichten; denn OpenStreetMap wird von sehr vielen Apps (z.B. für Android und für iOS) verwendet und unterstützt. Das Kartenmaterial können Sie auf dem Smartphone speichern, so dass Sie keine Internetverbindung brauchen.

Weit verbreitet ist die freie und quell-offene App OsmAnd, die On- und Offline-Navigation unterstützt und in einer abgespeckten Version kostenlos ist. Wer F-Droid verwendet, bekommt die Ver-



sion ohne Einschränkungen. Menschen, die gerne wandern, empfehlen wir, auch Höhenlinien-Relief-Schattierungen herunterzuladen und die „Touring View“ einzustellen. Leider verzichtet OsmAnd nicht ganz auf Tracking: Wenn Sie sich die Liste installierbarer Karten anzeigen lassen, werden Informationen über Ihr Gerät auf einen Server hochgeladen.

Auf 4UMaps können Sie sich Stadtpläne und andere topografische Karten in hoher Qualität selbst ausdrucken.

Karten auf der eigenen Website einbinden

Das Setzen eines Kartenmarkers und das Extrahieren von Links auf Adressen ist mit OpenStreetMap problemlos möglich. Die Lizenz erlaubt uneingeschränkte private und gewerbliche Nutzung. Sie können die Karte also problemlos auf der eigenen Website einbinden. Anfahrtsskizzen und Lagepläne können Sie mit uMap schnell und professionell realisieren.

Eigene Karten

Mit uMap können Sie auch Karten erstellen, die mehrere Marker, Flächen oder Strecken enthalten. Sie können Formen und Farben festlegen, Beschreibungen angeben und veranlassen, dass die Daten von einer externen Quelle geladen werden.

Offizielle Karten

Der Bayernatlas.de bietet thematische Ansichten, z.B. zu Freizeit, Planen und Bauen oder Naturgefahren.

Beim Topografischen Informationsmanagement des Landes Nordrhein-Westfalen gibt es ebenfalls thematische Karten, beispielsweise zu Fluglärm. Fehler können Sie direkt online melden.

Marble – die Welt auf dem Rechner

Mit Marble können Sie die Welt als Kugel betrachten und sich in einzelne Kartenausschnitte zoomen. Dafür stehen Ihnen neben OpenStreetMap-Karten Satellitenbilder, historische Karten und andere Spielereien zur Verfügung. Laden Sie sich die entsprechenden Kartenbereich und die Navigation-Engine herunter, um ohne Internetverbindung agieren zu können.

Auf dem Handy können Sie OpenStreetMap ohne teure Datenverbindung nutzen. Und Sie können das Programm in Ihre Website einbauen, ohne Kosten befürchten zu müssen.

Gibt es ein Leben ohne Google?



Nick Schilken war Anfang 2021 als Praktikant in unserem Team. Er will sich und den Rest der Welt von der Bevormundung durch Google befreien. In einem Blogtext fragte er sich: Werde ich eine nachhaltige Alternative zur Google-Suchmaschine finden? Im Rahmen seiner Bachelorarbeit mit dem Titel: „Der Spion, den ich liebte – die Macht der kommerziellen Überwachung im digitalen Alltag“ recherchierte Nick bei uns zum Thema Überwachungskapitalismus. Quellen und Hintergründe zu seinem Text finden Sie verlinkt auf der Jahrbuch-Webseite.

Ich bin Nick, studiere Soziologie und bin 23 Jahre alt. Mir ist es wichtig, im Internet so auftreten zu können, wie ich es in der realen Welt tue. Ich möchte nicht in einer vorbestimmten und berechneten Welt leben. Man kann und soll mich nicht berechnen und analysieren, ich halte mich für mündig genug, um zu wissen, was mir gefällt. Vor allem aber sollte man mir Informationen und Produkte nicht vorenthalten. Nur weil ich Hip Hop oder Techno höre, heißt das nicht, dass

ich nicht in klassische Musik hineinhorchen möchte. Nur weil ich mich für Gaming interessiere, möchte ich nicht, dass mir Nachrichten zu Politik und Wirtschaft vorenthalten werden. Wir sollten unsere Sicht auf die Welt nicht von einigen wenigen Unternehmen vorstrukturieren lassen, deren Kriterien zur Strukturierung wir gar nicht kennen, denn so werden wir abhängig und unmündig. Ein Teil der Lösung ist ein freier und offener Suchindex!

► Gefangen in der Filterblase

Die meisten Menschen – inklusive mir – befinden sich täglich in einer eigenen digitalen Filterblase. Algorithmen bestimmen, welche Informationen relevant für uns sind. Sie gestalten die Anordnung der Informationen in unseren Timelines, Feeds oder Suchmaschinenergebnissen. Spinnt man den Gedanken weiter, stellen sich mir die Fragen: Auf welcher Informationsgrundlage sollen wir uns denn dann austauschen? Wie sollen Diskurse – ohne die Demokratie nicht möglich ist, – geführt werden, wenn sich jeder auf Informationen bezieht, die auf ihn oder sie zugeschnitten wurden?

► Woher haben Suchmaschinen ihre Antworten?

Nachdem mir all diese Gedanken durch den Kopf gegangen sind, habe ich angefangen, mein Verhalten im Netz zu über-

denken. Schließlich bieten sich uns schon viele Möglichkeiten, ein Stück Autonomie im Internet zurückzugewinnen – doch es sind noch nicht genug. Nachdem ich meinen Messenger gewechselt habe (► Seite 123) und wo immer es aktuell möglich ist, auf offene anstelle von proprietärer Software setze, sollte es der monopolartigen Suchmaschine – Sie wissen, welche ich meine – an den Kragen gehen.

Leider ist das gar nicht so einfach, wie ich es mir erhofft habe, denn es gibt eigentlich keine Alternativen, – viele denken jetzt bestimmt „Klar gibt es Alternativen, zum Beispiel Startpage oder

DuckDuckGo“. Ich kann leider nur ernüchternd feststellen, dass das gar keine „echten“ Alternativen sind. Wieso das so ist, erkläre ich im Folgenden. Bis jetzt habe ich nicht großartig darüber nachgedacht, woher Suchmaschinen ihre Informationen beziehen, doch genau hier liegt das Problem.

Ich habe mich auf die Suche nach einer Alternative zu Google begeben und bin auf einen wirksamen Weg gestoßen, der den Wettbewerb auf dem Suchmaschinenmarkt wieder beleben kann, sodass Nutzer:innen die Wahl haben, welche Suchmaschine sie nutzen möchten.

► Ein wertvoller Datenschatz

Früher waren Bibliotheken wie die in Alexandria der Wissensspeicher, auf den einige wenige Menschen zugriffen. Heutzutage schöpfen die meisten Menschen

ihr Wissen aus der Suchmaschine von Google, die auf dem europäischen Suchmaschinenmarkt einen Marktanteil von mehr als 90 Prozent hält (► Seite 101). Doch woher holt Googles Suchmaschine überhaupt ihr Wissen?

Suchmaschinen greifen in der Regel auf mindestens einen der vier großen weltweiten Suchindizes zu. Ein Suchindex bezeichnet den „Datenschatz“, also den Datenbestand, ohne den eine Suchmaschine wertlos wäre. Er kann als Abbild des Webs verstanden werden, denn er beinhaltet alle findbaren Webseiten. Neben Google (USA) und Bing (USA) zählen Yandex (Russland) und Baidu (China) zu den großen „Schatzmeistern“, die über einen eigenen Suchindex verfügen.



► **Web-Crawler indexieren das Web**

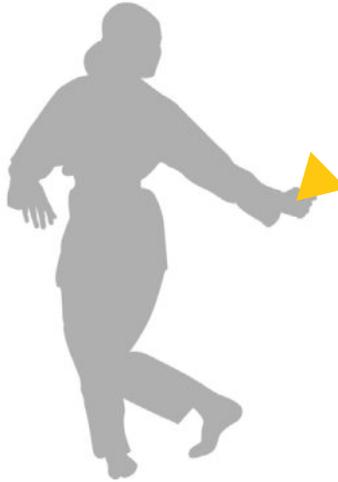
Um ihre Datensammlung ständig zu erweitern, nutzen Suchindizes sogenannte Web-Crawler. Das ist Software, mit der Webseiten katalogisiert werden, indem sich die Crawler durch Webseiten „wühlen“, den darin enthaltenen Links folgen und die gefundenen Inhalte indexieren. Ein Suchindex ist also sehr wertvoll. Ohne ihn ist es nicht möglich, eine Suchmaschine aufzubauen.

► **„World-Crawler“ indexieren die reale Welt**

Längst werden Daten für den Index von Suchmaschinen nicht nur durch das Durchpflügen des Internets geschürft: Suchindizes kaufen Daten ein, z.B. Bewegungsdaten von Mobiltelefonen, Gesundheitsdaten, Flugdaten, Reisefahrpläne, Inhalte von Medienangeboten, die hinter Paywalls stecken, aktuelles Kartenmaterial und so weiter. Auch diese Daten müssen urbar gemacht werden, damit eine Suchmaschine mit dem gewohnten Komfort funktionieren kann.

► **Suchmaschinen benötigen Suchindizes**

Man sollte meinen, dass wir uns frei aussuchen können, von welcher Suchmaschine wir unsere Informationen beziehen. Tatsächlich gibt es neben Google noch alternative Suchmaschinen wie



Startpage, MetaGer, YaCi, Ecosia oder DuckDuckGo. Doch selbst wenn wir auf eine der vermeintlichen Alternativen zugreifen, führt meist kein Weg an den großen Suchindizes von Google, Bing, Yandex oder Baidu vorbei. Die Suchmaschinen bauen nämlich in der Regel auf mindes-

tens einem der zuvor genannten vier großen Suchindizes auf. Startpage zum Beispiel darf den Index von Google mitbenutzen, Ecosia basiert auf dem Index von Bing, und auch DuckDuckGo greift unter anderem auf Yandex und Bing zu. Grund dafür ist, dass es für ein kleines Unternehmen beinahe unmöglich ist, einen eigenen Index aufzubauen, denn der Aufbau ist extrem kostspielig und erfordert ein hohes Maß an technischem Know-how. Die bestehenden Suchindizes haben also einen Vorsprung, der für einzelne kleine Start-ups nicht einzuholen ist. Das ist nicht fair und hemmt Innovation und Vielfalt in der „Suchmaschinenwelt“.

► **Suchmaschinen sind Machtinstrumente**

Google beherrscht den Suchmaschinenmarkt in Europa und verursacht Abhängigkeiten sowie wirtschaftliche Schäden. Das Unternehmen hat unter anderem seine marktbeherrschende Stellung missbraucht, indem es für Websites Dritter wettbewerbswidrige vertragliche

Beschränkungen einführte. Die Europäische Kommission hat daraufhin im März 2019 die dritte Milliardenstrafe gegen Google verhängt.

► Alle wollen oben sein

Der Google-Konzern versucht anhand der Daten, die er über uns gesammelt hat, eine unentbehrliche Position in unserem Leben einzunehmen. Die meisten Menschen schauen sich nur die erste Seite der Suchergebnisse an. Dementsprechend sind die Platzierungen auf der ersten Seite der Suchmaschine heiß begehrt. Google hat mit seinem Sortier-Algorithmus eine Geldmaschine erschaffen, bei der hauptsächlich Werbetreibende um die Erstplatzierungen in der Suchmaschine konkurrieren. Außerdem haben Politiker:innen, Unternehmer:innen und andere Personen des öffentlichen Lebens Angst, dass ihre weiße Weste durch Negativschlagzeilen auf den ersten Suchergebnisplätzen befleckt wird. Das verdeutlicht, dass allein die Art und Weise, wie Google Suchergebnisse anordnet, ein Machtinstrument von immensem Wert darstellt.

► Der Suchschlitz beobachtet uns

Auf der anderen Seite stehen die Nutzer:innen. Google hat es sich zum Ziel gemacht, die Anzeige der Suchergebnisse zu individualisieren und zu perfektionieren. Das „Perfektionieren“ spielt sich jedoch hinter unseren Rücken ab. Am liebsten würde Google uns an erster Stelle die Antwort präsentieren, die für uns persönlich perfekt erscheint. Das gelingt dem Unternehmen mittlerweile schon recht gut, da es alle Daten, die es sammelt, zusammenführt und Profile über uns erstellt. Das ist eine große Gefahr, denn Suchmaschinen sind ein Teil der digitalen Infrastruktur. Google hält eine Monopolstellung und versucht diese durch die ständige Erweiterung seiner Datensammlung zu zementieren. Es wirbt sogar damit, „die Informationen der Welt zu organisieren und allgemein nutzbar und zugänglich zu machen.“ Das ist ein bedenklicher Machtanspruch, denn um alle Informationen der Welt nutzbar zu machen, muss sich das Unternehmen erst mal alle Informationen der Welt aneignen.

Aus gutem Grund wurde Google 2013 und 2021 (► Seite 97) von uns mit dem BigBrotherAward ausgezeichnet. So

Bild: Digitalcourage, cc by 4.0



glaubt zum Beispiel Eric Schmidt, der bis 2015 Executive Chairman bei Google war, „dass die meisten Menschen nicht wollen, dass Google ihre Fragen beantwortet. Sie wollen, dass Google ihnen sagt, was sie als nächstes tun sollen.“ Larry Page, der die Google-Suchmaschine mit Sergey Brin entwickelt hat, behauptet sogar: „Die Suche wird ins Gehirn integriert werden. Schließlich werden Sie ein Implantat haben und wenn Sie über etwas nachdenken, wird es ihnen die Antwort sagen.“

Das geht zu weit! Denn es geht nicht mehr um persönliche Spielräume, die verhandelbar sind. Es geht um unverhandelbare Grundrechte. Es geht um **Gemeinwohl und Demokratie**. Unsere digitale Infrastruktur sollte nicht von marktbeherrschenden Privatunternehmen (noch dazu welchen, außerhalb der EU) abhängig sein. Sie machen sich so unverzichtbar und können über unsere Köpfe hinweg bestimmen, wie mit Informationen umgegangen werden soll. In gewisser Weise sind wir im Geschäftsmodell von Google der „Goldesel“, und unsere Daten sind das Gold. Die Studie



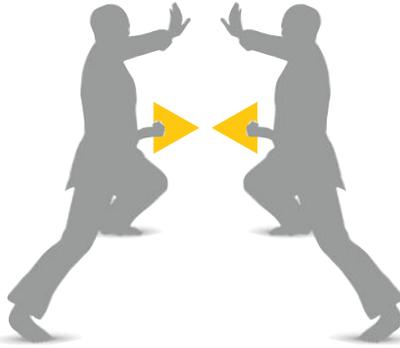
„Durchleuchtet, analysiert und einsortiert“ von Sarah Spiekermann und Wolfie Christl verdeutlicht dies sehr eindringlich (verlinkt über die Jahrbuch-Webseite).

► Filter und Zensur

Während die Gefahr bei Google und Bing etwas subtiler erscheinen mag, machen Yandex in Russland und Baidu in China deutlich, was für unheimliche Gefahren noch von Suchmaschinen ausgehen. Entsprechend politischer Vorstellungen und Wünsche können Inhalte gefiltert, zensiert und somit unzugänglich für die Bürger:innen gemacht werden. In China beispielsweise ist das Tianmen-Massaker, bei dem Studentenproteste gewaltsam niedergeschlagen wurden, nicht in der Suchmaschine Baidu aufzufinden. Aufgrund mangelnder Transparenz in Bezug auf ihre Algorithmen sind Suchmaschinen besonders anfällig für politische und wirtschaftliche Manipulation. Sie können als Instrument der „Meinungsmache“ missbraucht werden, das ist natürlich eine enorme Gefahr für Demokratie und Meinungsfreiheit.

► Ranking-Algorithmen sind manipulierbar

Die Art und Weise, wie Ranking-Algorithmen funktionieren (wie sie die Anordnung der Suchergebnisse „bestimmen“), wird von den Suchmaschinenanbietern geheim gehalten. Zum einen ist das ein nachvollziehbarer Schritt, denn wenn die Algorithmen transparent und einfach zu verstehen wären, hätte quasi jeder die Möglichkeit, die Ergebnispräsentation



tion von Suchmaschinen zu manipulieren. Andererseits ist es aufgrund der intransparenten Algorithmen schwer zu begreifen, ob Suchergebnisse frei von Manipulation sind. Das bedeutet im Prinzip, dass transparente Algorithmen Manipulation von „außerhalb“ erleichtern, während intransparente Algorithmen Manipulation von „innerhalb“, also zum Beispiel vom Suchmaschinenanbieter selbst, und von SEO-Spammern ermöglichen. Mit SEO-Spamming wird versucht, die Bewertungs-Algorithmen über Einträge in eigenen oder fremden Webseiten zu beeinflussen. Um Chancengleichheit bei der Ergebnispräsentation von Suchmaschinen zu gewährleisten und Manipulation zu vermeiden, könnte eine neutrale Institution – zum Beispiel eine europäische Stiftung – überprüfen, auf welche Art und Weise Ergebnisse angeordnet werden.

► **Abhängig von fremden Suchindizes**

Wenn wir in Europa an Informationen gelangen wollen, sind wir weitestgehend abhängig von den bestehenden Suchmaschinen und damit auch von den Suchindizes aus den USA, Russland und China. **Das ist ein Problem!** In extremen Krisen- oder Konfliktfällen könnte es sogar so weit kommen, dass wir den Zugang zu den bestehenden Suchindizes – und damit zu wichtigen

Informationen und Daten – verlieren. Denn aktuell werden die im Internet verfügbaren Informationen von den USA, Russland und

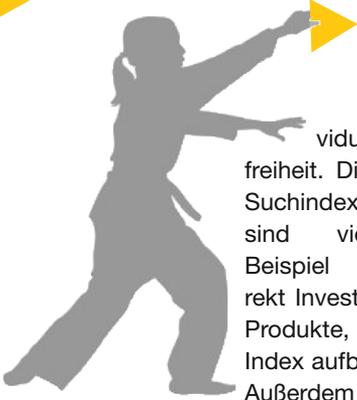
China „verwaltet“, da sie über einen oder mehrere Suchindizes verfügen. Europa hingegen verfügt über keinen eigenen Suchindex.

► **Europäische Regeln respektieren**

Für die Europäische Datenschutzgrundverordnung (DSGVO) gilt das Marktortprinzip. Das bedeutet, dass sich alle Unternehmen, die sich an EU-Bürgerinnen richten und in Europa Geschäfte machen wollen, an die DSGVO halten müssen. Viele ausländische Unternehmen unterliegen jedoch eigenen Gesetzen. Das stellt ein Problem dar, denn in den USA beispielsweise können Unternehmen auf Grundlage des Cloud Act und des FISA Act gezwungen werden, Daten an Geheimdienste herauszugeben. So können auch Daten europäischer Bürger:innen in die Hände ausländischer Geheimdienste fallen.

► **Starke Argumente für einen europäischen Suchindex**

Ein europäischer Suchindex würde die Bedingungen für frei zugängliches Wissen schaffen, auf das Unternehmen und Privatleute gleichermaßen zugreifen dürfen. Frei zugängliches Wissen bildet die Basis für Wettbewerb und Innovation, aber auch für die indi-



viduelle Meinungsfreiheit. Die Vorteile eines Suchindex für Europa sind vielseitig. Zum Beispiel werden indirekt Investitionen für neue Produkte, die auf dem Index aufbauen, gefördert.

Außerdem würde der Wettbewerb zwischen Suchmaschinenanbietern, die auf den Index zurückgreifen können, belebt werden.

Die Gründe für einen offenen europäischen Suchindex sind vielseitig:

1. Europa wäre nicht mehr darauf angewiesen, auf Indizes aus USA, Russland und China zuzugreifen – somit wird die Souveränität gestärkt.
2. Europäische Gesetze und Werte bilden den Rahmen für den Suchindex und somit auch für Suchmaschinen und andere Produkte, die auf ihm aufbauen. Eine Vielfalt an Suchmaschinen ist förderlich für die Demokratie weltweit.
3. Es gibt die Möglichkeit für neue Geschäftsmodelle von Suchmaschinen, die nicht „pseudo-gratis im Tausch gegen Nutzerdaten“ sind. Nutzer:innen könnten zum Beispiel Suchmaschinen ihrer Wahl – per Abo, als Genossenschaft oder durch Spenden – finanzieren.
4. Die EU kann sicherstellen, dass der Index zu fairen Konditionen nutzbar ist und dass ein gesunder Wettbewerb stattfindet.
5. Wir verlassen uns momentan auf

einzelne Suchmaschinen, die uns keinen Einblick in den Aufbau ihrer Suchalgorithmen und Datensammlungen erlauben. Dadurch wird Manipulation und Missbrauch ermöglicht.

6. Der Zugang zu Daten, Informationen und Wissen kann momentan gemäß wirtschaftlichen oder politischen Interessen des jeweiligen Anbieters eingeschränkt werden.

► Aufbau eines freien Suchindex beginnen

Die Idee eines europäischen Suchindex hat der Wissenschaftliche Beirat der Bundesregierung Globale Umweltveränderungen in einem EU-Politikpapier (WBGU Politikpapier S. 19, 22 und 35) und in einem Gutachten (WBGU Gutachten zur Digitalisierung, S. 234 siehe Jahrbuch-Website), die sich an die Bundesregierung richten, erwähnt und für den Aufbau eines öffentlich-rechtlichen Suchindex plädiert. In das Papier und das Gutachten sind auch Anregungen und Hinweise von Digitalcourage eingeflossen, weil wir uns schon länger mit einem europäischen Suchindex gegen Monopole befassen. Diese konkreten Forderungen sollten die Bundesregierung und die EU jetzt anpacken.

Technische Expertise und große finanzielle Investitionen stellen Prämissen für den Aufbau eines europäischen Suchindex dar. Der Index sollte möglichst alle Inhalte des Web umfassen und allen Zugriff ermöglichen. Des Weiteren sollte er am besten durch die EU finanziert,

jedoch staatsfern und unabhängig organisiert werden, um einseitige politische Einflussnahme zu vermeiden. Dementsprechend sollten auch die AGB gestaltet werden. Der Aufbau eines offenen Suchindex stellt demnach eine Infrastrukturaufgabe dar, die für die Trennung von öffentlich finanzierter Infrastruktur und privatwirtschaftlich betriebenen Diensten sorgt. Diese Infrastruktur lässt sich vergleichen mit Stromnetzen oder Straßen, die grundsätzlich zu Privatzwecken, aber auch zu unternehmerischen Zwecken genutzt werden dürfen. Die Verantwortung, einen sicheren und fairen Zugang zu schaffen, bleibt jedoch Aufgabe des Staates beziehungsweise der europäischen Staaten.

► **Nicht aufgeben, bevor wir angefangen haben!**

Auch wenn der Aufbau viel Rechenkapazität sowie hoher finanzieller und personeller Investitionen bedarf: Es lohnt sich! Wirtschaft und Wettbewerb, aber auch digitale Souveränität und Demokratie können durch einen europäischen Suchindex gestärkt werden. Außerdem hätten viele innovative Programmierer:innen und kreative Unternehmer:innen die Chance, eine Vielfalt neuer Produkte auf Basis eines europäischen Suchindex aufzubauen. Die auf Grundlage des Index erzielten Gewinne würden dann nicht mehr nur zu einem marktbeherrschenden Anbieter außerhalb der EU fließen, sondern sie könnten vielen kleineren Unternehmen in der Fläche zugutekommen.

Viele von Ihnen denken vielleicht: „Es ist doch eh zu spät, unsere Daten sind überall verteilt“ oder „Google ist bequem zu benutzen und wir kommen gegen so ein Riesenunternehmen nicht an“. Vielleicht haben Sie recht, vielleicht bin ich auch nur naiv oder idealistisch, doch selbst wenn dem so ist, sollten wir nicht tatenlos zusehen, wie uns stückchenweise unsere Autonomie genommen wird. Es ist nicht schön zu verlieren – noch schlimmer ist es jedoch, gar nicht erst anzutreten und die Niederlage von vornherein zu akzeptieren. Außerdem ist es gar nicht so aussichtslos, wie es für viele scheinen mag. Die EU-Kommissarin für Wettbewerb, Margrethe Vestager, hat auf der Technologie-Konferenz SXSW in Austin/USA viel Zuspruch erhalten, als es darum ging, wie Big Tech Unternehmen – durch Behörden – zugunsten von Demokratie, Freiheit und Autonomie gebändigt werden können. Das Thema Datenschutz gewinnt also auch in den USA an Relevanz und es werden auch dort Maßnahmen zur Einhegung der Digitalkonzerne diskutiert. Die digitale Welt befindet sich in einem ständigen Wandel – und wir können ihn mitgestalten.



► Darum bitte ich Sie:

Lassen Sie uns der Politik vermitteln, dass wir uns bei der Suche nach Wissen auf eine für alle zugängliche Infrastruktur verlassen möchten. Sie soll nicht von wenigen marktbeherrschenden Unternehmen verwaltet und zugunsten der Profitmaximierung und Machtausübung einiger weniger gestaltet werden. Wir benötigen eine Infrastruktur, die es einer Vielzahl an Produkten, unter anderem (Spezial-)Suchmaschinen, aber auch wissenschaftlichen Tools ermöglicht, auf ihr aufzubauen. Die darauf aufbauenden Suchmaschinen sollen den Schutz unserer Daten gewährleisten und uns nicht nur auf eine Konsumentenrolle reduzieren, um profitable Modelle über unser Kaufverhalten zu entwickeln.

Firmen aus Europa, die sich unseren Werten verbunden fühlen, sich an die in Europa geltenden Regeln und Gesetze halten und denen Datenschutz ein Anliegen ist, sollen Geschäftsmodelle auf dem Index aufbauen und profitabel gestalten dürfen. Wir sollten jedenfalls nicht zulassen, dass das Wissen der Menschheit von einigen wenigen oligopolartigen Privatunternehmen verwaltet wird, die Innovation und Autonomie durch intransparente Machenschaften gefährden. Außerdem sollten wir unsere Fähigkeit, selbstständig zu denken, nicht von einem Unternehmen untergraben lassen, das für uns entscheiden will, welche Informationen für uns wichtig und welche unwichtig sind.

Für die Umsetzung des Suchindex braucht es den politischen Willen, Auftrag und die finanzielle Unterstützung der EU, denn das Projekt kann und darf nicht von einzelnen Unternehmen gestemmt werden. Der WBGU (Wissenschaftlicher Beirat der Bundesregierung Globale Umweltveränderungen) hat sich wie oben erwähnt für den Aufbau eines Europäischen Suchindex ausgesprochen. Der intellektuelle Grundstein ist also bereits gelegt. Erzählen Sie Freunden, Familie und Bekannten von der Idee des europäischen Suchindex, damit das Thema an Aufmerksamkeit gewinnt und die Politik mit der Umsetzung beginnt. Europa muss ein unabhängiges digitales und freies Ökosystem entwickeln, das allen zugutekommt!

Darauf muss ich setzen, denn alleine kann ich den Weg weg von der dominierenden Suchmaschine Google nicht gehen.



Nick Schilken

Foto: Nick Schilken, cc by-sa 4.0



Foto: Ingo Jürgensmann, cc by 4.0

Immer schön wachsam bleiben!

Public Domain vor 30 Jahren

Unsere Veranstaltungsreihe zu Technik, Kunst, Wissenschaft und Gesellschaft

Public Domain heißt „öffentlicher Raum“, aber auch „öffentliche Angelegenheit“, und so haben wir unsere Veranstaltungen im Bielefelder Bunker Ulmenwall ab 1987 genannt. Es ging uns darum, dass Leute, die an etwas forschen oder arbeiten, die gute Ideen oder ungewöhnliche Perspektiven haben, uns direkt davon berichten. Und wir wollten ihnen auch unsere Sichtweise mit zurückgeben. In jedem Jahrbuch erinnern wir uns an einen Jahrgang „Public Domains“ (PDs).

► padeluum erinnert sich:

Wenn ich mir für dieses Jahrbuch die Liste der PUBLIC-DOMAIN-Veranstaltungen des Jahres 1992 durchschaue, denke ich, dass wir die Reihe dringend wieder auflegen müssten. Nicht genauso wie damals, sondern mit den Möglichkeiten und Ansprüchen von heute. 2004 haben wir mit dem FoeBuD e.V. (so hieß Digitalcourage bis 2012) eine neue Ära betreten: Mit der Stop-RFID-Kampagne haben wir uns deutlicher als vorher politisch zu Wort gemeldet. Advocacy (► Seite 19) und die damals startende regelmäßige Organisation von Großdemos und Veranstaltungen haben all unsere Kraft und Konzentration gebraucht, so dass die freundlichen, kreativen und lokal-bielefelderischen

Veranstaltungen der PUBLIC DOMAIN-Reihe leider eingeschlafen sind. Wie bedauerlich! Mal schauen, ob wir diesen Faden demnächst mit einem Konzept der 2020er-Jahre wieder aufnehmen.

Aber wir wollen hier ja zurück schauen: Anfang des Jahres 1992 hatten wir direkt volles Haus: Zur „Kommunikation unter Delphinen“ war der Bunker Ulmenwall als Veranstaltungsort knüppelvoll. Selbst für die üblichen Tische mit dicht gedrängten Computern war an diesem Tag kein Platz mehr. Letztendlich war's ein charmanter Vortrag mit bezau-

... und danke für den Fisch
(Douglas Adams, 4. Teil von „Per Anhalter durch die Galaxis“)



PUBLIC DOMAIN V37.0
Das Computertreffen

Kai von Teltenborn, Delphinist, berichtet über Kommunikation unter Delphinen (Vortrag mit Dias)

Sonntag, 2. 2. 1992 ab 15 Uhr
im **BUNKER ULMENWALL**
Kreuzstr.0, D-4800 Bielefeld 1

Eintritt: Pro Person 5,- DM, mit Computer 3,- DM
Preis-Zuschussentscheid von Bärbel Ullmann, AB, FoeBuD e.V. und Art+Anschlamm
Kontakt: 0521-173254 (di - fr, 14-18 Uhr)
7-Merz: #BIONIC 0521-68000; - Sonnet: #BENIC 05202-88888

Anzeige

// BIONIC

"Bielefelder MailBox AG"
 05 21-6 80 00/17 11 88 V.32bis

*** BITTE SPRECHEN SIE #**



Wir bitten wieder sehr herzlich
um einen Anruf bei der Adresse

CaBIT 92
HANNOVER
11. - 18. MÄRZ 1992

PUBLIC DOMAIN V38.0
Das Computertreffen

Jürgen Christ, E-Mail-Spezialist aus Köln/Hamburg,
stellt eine Voice-MailBox (=intelligenter Anrufbeant-
worter) vor

Sonntag, 1. 3. 1992 ab 15 Uhr
im **BUNKER ULMENWALL**
Kreuzstr.0, D-4800 Bielefeld 1

Eintritt: Pro Person 2,- DM, incl Computer 3,- DM
Eine Zuerstvergabe von Bunker-Ulmenwall, Ab-TreffID e.V. und Art d'Anmeldung
Kontakt: 0521-680054 di-f, 14-18 Uhr
Z.Nr.: //BIONIC 0521-68000, Subnet //BIONIC 0521-62-9888

// BIONIC "Bielefelder MailBox AG"
0521-68000/171188 V.32bis

RECHT unübersichtlich

GLOBALES DORF
Rechtsfreier Raum

PUBLIC DOMAIN V39.0
Das Computertreffen

Günter Freiherr von Gravenreuth, Starnawalt aus
München, erörtert rechtliche Aspekte von MailBoxen:
Datenschutz, Haftung, Presserecht und G10

Sonntag, 5. 4. 1992 ab 15 Uhr
im **BUNKER ULMENWALL**
Kreuzstr.0, D-4800 Bielefeld 1

Eintritt: Pro Person 2,- DM, incl Computer 3,- DM
Eine Zuerstvergabe von Bunker-Ulmenwall, Ab-TreffID e.V. und Art d'Anmeldung
Kontakt: 0521-175254 di-f, 14-18 Uhr
Z.Nr.: //BIONIC 0521-68000, Subnet //BIONIC 0521-62-9888

// BIONIC "Bielefelder MailBox AG"
0521-68000/171188 V.32bis

bernden Unter- und Überwasser-Bildern des delphinverliebten Fotografen Kai von Tettenborn, inzwischen Kameramann bei der ARD.

Im März 1992 beschäftigten wir uns mit den Möglichkeiten von Voice-Mail-Boxen, mit denen man soviel mehr machen konnte als „Bitte sprechen Sie nach dem Piep!“ Man konnte zum Beispiel virtuelle Räume aufmachen, in denen sich Leute telefonisch treffen konnten. Und für die „richtigen“ Mailboxen gab's dann auch mal rechtliche Aufklärung, wieder durch Günter Freiherr von Gravenreuth, den einzigen Rechtsanwalt zu damaliger Zeit, der zu den „jungen Computerfreaks“ Kontakt gesucht hat. Er war ja schon 1991 mit einem Rechts-Vortrag bei uns gewesen

(Siehe Jahrbuch 2021). Der Spruch, mit dem wir auf unseren Karten warben („Globales Dorf – Rechtsfreier Raum“) war als Aufkleber ein Renner und wurde auch auf den Türen von etlichen Landesdatenschutzbeauftragten gesichtet. Aber nach diesem Vortrag war auch dem

► **Rechtsfreie Räume gibt es gar nicht.** ◀

letzten Teilnehmer klar: Rechtsfreie Räume gibt es gar nicht.

Sehr zum Leidwesen unseres nächsten Referenten, einem Magier, der in der PD 40.0 solche Räume mittels Magie für sich erschaffen wollte. Die Abrakadabra-PD war ein bisschen spooky, denn so ganz nach weißer Magie klang das nicht, was er uns erzählte. Aber es war sehr spannend zu erleben, wie auch die Magier mit den elektronischen Zauberkästen – Computern – für ihre Zwecke experimentieren.

ABRAKADABRA
Magie im Computerzeitalter



PUBLIC DOMAIN V40.0
Das Computertreffen

Friedrich Delgado Friedrichs, Magier aus der Altmark, über Philosophie und seine Ausbildung in der Weißen Magie

Sonntag, 3. 5. 1992 ab 15 Uhr
im **BUNKER ULMENWALL**
Kreuzstr.0, D-4800 Bielefeld 1

Eintritt: Pro Person 5,- DM, mit Computer mitbringt 3,- DM
Faxe: 7100000000 von Bunker Ulmenwall, 1h, FoebüD o.V. und Art d'Annoebleren
Kontakte: 0521-175254 * d - f, 14 - 18 Uhr
Z-NETZ: BIONIC 0521-68000 • Unerbet. BI LINK 05202-88888
Jeden Dienstag Treffen im Café Spinnerhof, Hoepferstr.64, ab 19:30 Uhr

// BIONIC "Bielefelder MailBox AG"
0521-68000/171188 V.32bis

MEDIEN VON UNTEN
Geschichte, Perspektiven, Utopien



PUBLIC DOMAIN V41.0
Treffpunkt Zukunft, Technik & Kultur

Vortrag von Dr. Gabriele Hooffacker, München, über Neue Medien für neue gesellschaftliche Bewegungen

Sonntag, 7. 6. 1992 ab 15 Uhr
im **BUNKER ULMENWALL**
Kreuzstraße 0, D-4800 Bielefeld 1

Eintritt: Pro Person 5,- DM, wer Computer mitbringt 3,- DM
Eine Zusammenkunft von Bunker Ulmenwall, 1h, FoebüD o.V. und Art d'Annoebleren
Kontakte: 0521-175254 * d - f, 14 - 18 Uhr
Z-NETZ: BIONIC 0521-68000 • Unerbet. BI LINK 05202-88888
Jeden Dienstag Treffen im Café Spinnerhof, Hoepferstr.64, ab 19:30 Uhr

// BIONIC "Bielefelder MailBox AG"
0521-68000/171188 V.32bis

Im Juni wurde es realistischer. Wie werden die „Neuen Medien“ (die damals ja wirklich noch fast neu waren) von neuen gesellschaftlichen Bewegungen genutzt werden? Zu diesem Zeitpunkt waren wir schon dabei, das Zamir Transnational Network, die Vernetzung der Friedensgruppen in den kriegführenden Ländern Ex-Jugoslawiens, aufzubauen und standen damit erstmals weltweit in den Zeitungen.

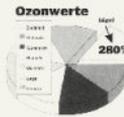
Wenn Sie sich die Karten auf diesen Seiten anschauen, fällt Ihnen etwas auf? Richtig, die PD V42.0 fehlt. Für die Nummer 42 wollten wir Douglas Adams, den Autor von „Per Anhalter durch die Galaxis“, einladen. (Logisch: „42“ ist bekanntlich die Antwort auf die Frage nach dem Leben, dem Universum und dem ganzen Rest.) Und

tatsächlich waren wir ganz nah dran. Rena hatte sich mit Beharrlichkeit an die Recherche seiner Kontaktdaten gemacht und schließlich die Telefonnummer seiner persönlichen Assistentin Oona herausgefunden. Das Telefonat lief so: Eine Männerstimme sagt „Hello?“ Rena: „Hello! My name is Rena Tangens and I am calling from Germany. I'd like to talk to Oona Phelan. Is she in?“ Männerstimme: „In what matter?“ Rena: „It's about Douglas Adams.“ Männerstimme mit einem hörbaren Lächeln: „I am Douglas Adams!“. Nach kurzer Schrecksekunde erklärt Rena, was die Public-Domain-Reihe ist, und Douglas Adams sagt, dass er das spannend fände und sehr gerne kommen würde, doch dass er für den Termin schon andere Verpflichtungen habe. Wir sollten uns gerne später wieder

► „I am Douglas Adams!“ ◄

EIN BILD LÜGT MEHR ALS 1000 ZAHLEN

Statistiken fälschen - leichtgemacht!

**PUBLIC DOMAIN V43.0**
Treffpunkt Zukunft, Technik & Kultur

Vortrag von Martin Husemann, itb Bielefeld, über die einfache Wahrheitskorrektur mit Tabellenkalkulationen

Sonntag, 6.9.1992 ab 15 Uhr
im **BUNKER ULMENWALL**
Kreuzstraße 0, D-4800 Bielefeld 1Eintritt: Pro Person 5,- DM; wer Computer mitbringt 3,- DM
Einig. Zusammensetzung von Bunker Ulmenwall, itb, FoeBuD e.V. und Ari d'Annoislement
Kontakt: 0521-175254 • di - fr, 14 - 18 Uhr
Z-NETZ: BIONIC 0521-69000 • UweNet: B-LINK 05202-88888
Jeden Dienstag Treffen im Cafe Spinners, Hoopstr.64, ab 19:30 Uhr

Anzeige

FoeBuD e.V. Der Club der freundlichen Genies
Werde Mitglied!**ANTI-NAZI-BALLERSPIEL**

"Wolfenstein" verbieten!

**PUBLIC DOMAIN V44.0**
Treffpunkt Zukunft, Technik & Kultur

Frank Möller, Politikwissenschaftler aus Hamburg, im Streitgespräch mit Gerald Jörns, ComPäd e.V., Hannover

Sonntag, 4.10.1992 ab 15 Uhr
im **BUNKER ULMENWALL**
Kreuzstraße 0, D-4800 Bielefeld 1Eintritt: Pro Person 5,- DM; wer Computer mitbringt 3,- DM
Zusammensetzung Bunker Ulmenwall, itb, FoeBuD e.V., ComPäd e.V., Ari d'Annoislement
Kontakt: 0521-175254 • di - fr, 14 - 18 Uhr
Z-NETZ: BIONIC 0521-69000 • UweNet: B-LINK 05202-88888
Jeden Dienstag Treffen im Cafe Spinners, Hoopstr.64, ab 19:30 Uhr

Anzeige

FoeBuD e.V. Der Club der freundlichen Genies
Werde Mitglied!

melden, dann könnten wir die 42 nachholen. Wow! Leider hat es mit dem Nachholen nicht so schnell geklappt. 1999 ist er nach Kalifornien gezogen, wodurch die Reisekosten deutlich teurer wurden. Und wir waren arm wie die Kirchenmäuse. 2001 starb Douglas Adams überraschend an einem Herzinfarkt. Und so wird es niemals eine PD 42 geben. (Anmerkung: Die Zählweise der Public Domains stimmt übrigens ab PD 43 trotzdem wieder, weil wir eine Nummer 8,5 hatten. :-)

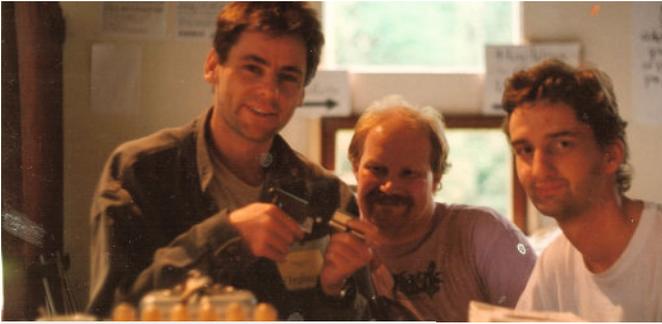
Nach der Sommerpause 1992 lernten wir, wie man mit Statistik lügt. Oder, wie man, wie es auf der Einladungskarte stand, „Wahrheitskorrektur mit Tabellenkalkulationen“ vornehmen kann. Seitdem passe ich viel besser auf, wenn man mir ein erklärendes Schaubild zeigt. Ich lasse mich damit nicht mehr ganz so leicht an der Nase herumführen.

Zur Oktober-PD hetzten wir einen Politikwissenschaftler und einen Pädagogen aufeinander. Sie sollten sich bei uns über das „Ballerspiel“ Wolfenstein streiten, in dem die Spieler:innen „Nazis abballern“ können. „Wolfenstein 3D“ war im Mai 1992 erschienen und ein Verbot wurde diskutiert. Wie die Diskussion bei uns im Bunker Ulmenwall, an der sich wie immer das Publikum rege beteiligte, damals ausging? Ich weiß es nicht mehr.

Deutlicher erinnere ich mich an den Workshop zu Desktop Publishing im November, den unser Freund Radi einen Monat später gab. Er war schon damals ein Computervirtuose und hat bei uns später sowohl Netze als auch Drucksachen gebaut. Er ist sogar bei uns ins Haus in der Marktstraße eingezogen.

Und im Dezember hatten wir wieder eine saisonal angepasste Veranstaltung: Professor Dr. Klaus Brunnstein

Foto: Digitalcourage, cc by 4.0



padeluum mit Lockpicking-Tool mit Volker Mundus und Michael „Radi“ Rademacher beim „Hacking at the End of the Universe“ Camp in Holland 1993

Hamburger Studierenden sammelten und werteten Viren aus. Und Brunnstein wurde hier und da der „Virenpapst“ genannt.

Oder „Großrechnermufti“, wie uns einer seiner Kollegen anvertraute. Die wissenschaftliche Digital-Boheme war schon damals nicht immer freundlich zueinander.

erzählte uns in bester Grippevirenzeit alles, was er damals über Computerviren wusste. Er schimpfte bitterlich über „dieses unsichere Unix“, wo (Zitat) „alle Schutzmechanismen ausgebaut“ seien. So sei es kein Wunder, dass sich diese Viren überall verbreiten würden. Seine

Aber um das zu verändern, waren wir ja aufgebrochen und haben immer wieder Menschen zusammen gebracht. Das wollen wir (fester Vorsatz für 2022 und auf Holz geklopft) endlich auch in Bielefeld vor unserer Haustür wieder mal machen.

ZEITUNG ELEKTRONISCH
DTP vs Schnippeltechnik.

PUBLIC DOMAIN V45.0
Treffpunkt Zukunft, Technik & Kultur

Workshop mit Michael Rademacher, Nord-Report / VNJ, Hannover. Eine Einführung in Desktop-Publishing.

Sonntag, 1.11.1992 ab 15 Uhr
im **BUNKER ULMENWALL**
Kreuzstraße 0, D-4800 Bielefeld 1

Eintritt: Pro Person 5,- DM; wer Computer mitbringt 3,- DM
Eine Zusammenarbeit von Bunker Ulmenwall, Bb, FoeBuD e.V. und Art of Anemulation
Kontakt: 0521-375294 • dt.-fr. 14.-18 Uhr
7 NETZ: BIONIC 0521-69000 • Usenet: BILINK 05202-89868
Jeden Dienstag treffen im Café Spirent, Haspenstr. 64, ab 19:30 Uhr

nrp die Presseagentur des Nordens Anzeige

**Weihnachtszeit
Viruszeit**

PUBLIC DOMAIN V46.0
Treffpunkt Zukunft, Technik & Kultur

Prof. Dr. Klaus Brunnstein, VTC Hamburg, über Risiken der Informationstechnik, insbesondere Computerviren.

Sonntag, 6.12.1992 ab 15 Uhr
im **BUNKER ULMENWALL**
Kreuzstraße 0, D-4800 Bielefeld 1

Eintritt: Pro Person 5,- DM; wer Computer mitbringt 3,- DM
Eine Zusammenarbeit von Bunker Ulmenwall, Bb, FoeBuD e.V. und Art of Anemulation
Kontakt: 0521-375294 • dt.-fr. 14.-18 Uhr
2-NETZ/DOMI BK/APC: BIONIC 0521-69000 • Usenet: BILINK 05202-89868

FoeBuD e.V. Der Club der freundlichen Genies
Werde Mitglied! Anzeige

40 Jahre Datenschutz- bewegung in Deutschland

Geschichte und Geschichten



Foto: StefanieLoos, cc by 4.0

Rena Tangens, Gründerin von Digitalcourage

Diesen Text hat Rena Tangens im Herbst 2020 im Auftrag der Böll-Stiftung für den German Israel Tech Policy Dialogue geschrieben. Er wurde ins Englische übersetzt und auf der Website des Israel Public Policy Institute veröffentlicht (verlinkt über die Jahrbuch-Webseite).

„**W**arum ist das Bewusstsein für Datenschutz in Deutschland so groß? Wo kommt das her?“ fragen uns des öfteren Journalist:innen aus dem Ausland. „Wie habt ihr es geschafft, die Öffentlichkeit dafür zu interessieren? Wie schafft ihr, den Frust auszuhalten, wo Politiker:innen doch immer wieder – und wider jede Vernunft – neue Überwachungsgesetze beschließen? Wie schafft ihr weiterzumachen, wo die Bürger:innen sich vielfach so unkritisch dem Kommerz im Überwachungskapitalismus hin-

geben?“ fragen uns Aktivist:innen aus anderen Ländern, z.B. bei „Freedom not Fear“, unserem jährlichen europäischen Barcamp in Brüssel. Und schließlich fragen wir uns auch selber „Warum tun wir das eigentlich?“

Über diese Fragen müssen wir auch selbst immer wieder neu nachdenken und sie neu beantworten. Einige Antworten haben eine historische Dimension, andere haben immer wieder einen anderen aktuellen Anlass. Die Dinge sind im Fluss – und wir selbst beeinflussen sie.



Foto: Joris Felix, cc-by-sa 4.0

Rena Tangens und padeluun bei der unteilbar-Demo #KeinFussbreit in Berlin 2019 gegen Antisemitismus und Rassismus

Schließlich spielt auch der Kontext der Gesprächspartner.innen eine Rolle. Und den finde ich in einem Deutsch-Israelischen Dialog besonders spannend.

Dieser Text folgt einer Chronologie, hat aber nicht den Anspruch, eine lückenlose Auflistung aller Ereignisse zum Thema Datenschutz in Deutschland zu liefern. Er erzählt einige Erlebnisse der Datenschutzbewegung aus erster Hand. Unter anderem deshalb, weil ich überzeugt bin, dass es eine gute Art ist, Geschichte aus Geschichten¹ zu lernen. Der Beitrag ist aus einer persönlichen Sicht geschrieben.

► **Meine persönliche Motivation**

Und deshalb möchte ich als erstes etwas über meine persönliche Motivation sagen, warum ich mich für Datenschutz und Bürgerrechte einsetze. Schon in der Schule habe ich dank engagierter Lehrer einiges über Geschichte und Poli-

tik gelernt, über Regeln und Streitkultur und über Rechtsstaat und Demokratie. Und über Totalitarismus, Willkür und Verbrechen. Ich habe mich gefragt, wie die Nationalsozialisten in Deutschland an die Macht kommen konnten und was ihnen ermöglicht hat, Menschen zu unterdrücken, zu verfolgen und massenhaft zu ermorden. Mein Entschluss: Ich will, dass das nie wieder passieren kann – und dazu will ich meinen Teil beitragen.

Überwachung, Erfassung und Kontrolle der Bevölkerung waren eine maßgebliche Voraussetzung für Aussonderung, Deportation und Vernichtung. Deshalb ist die logische Konsequenz: Wir müssen uns dafür engagieren, dass eine solche Überwachung, massenhafte Erfassung und Kontrolle nicht mehr passieren kann. Auch nicht in einer Demokratie.

¹ Buch Baacke/Schultze: „Aus Geschichten lernen“, Weinheim, 1993

► Volkszählungen 1933 und 1939

Doch schauen wir einmal genauer, was da in den 1930er-Jahren passierte. Als die Nazis im März 1933 in Deutschland an die Macht kamen, war es eines ihrer ersten Projekte, so schnell wie möglich eine Volkszählung durchzuführen. Das Ermächtigungsgesetz entmachtete das Parlament und gab den Nazis unbeschränkte Gesetzgebungsbefugnis. So wurde ein Reichsgesetz für die Durchführung einer Inventur des deutschen Volkes schon am 12. April 1933 beschlossen. Ab Juni 1933 wurde bereits gezählt. Es war ihnen offenbar wirklich wichtig.

Da wir wissen, wie die Geschichte weiterging, liegen die Gründe für die Volkszählung auf der Hand: Es ging um eine Bestandsaufnahme der wehrtüchtigen Männer, um den Krieg vorzubereiten, es ging um aktive Bevölkerungspolitik, um den „arischen“ Nachwuchs zu fördern und es ging um die Erfassung verschiedener Bevölkerungsgruppen, u.a. der jüdischen, um ihre Vernichtung vorzubereiten.

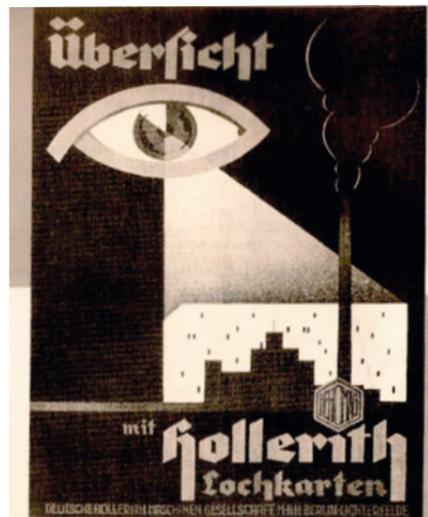
Die deutschen Statistik-Experten frohlockten und wussten, dass ihre Stunde gekommen war. Der Präsident der Deutschen Statistischen Gesellschaft, Friedrich Zahn, stellte damals fest:

„*Schon ihrem Wesen nach steht die Sta-*

► **“Schon ihrem Wesen nach steht die Statistik der nationalsozialistischen Bewegung nahe.”** ◀ (F. Zahn)

*tistik der nationalsozialistischen Bewegung nahe.“*²

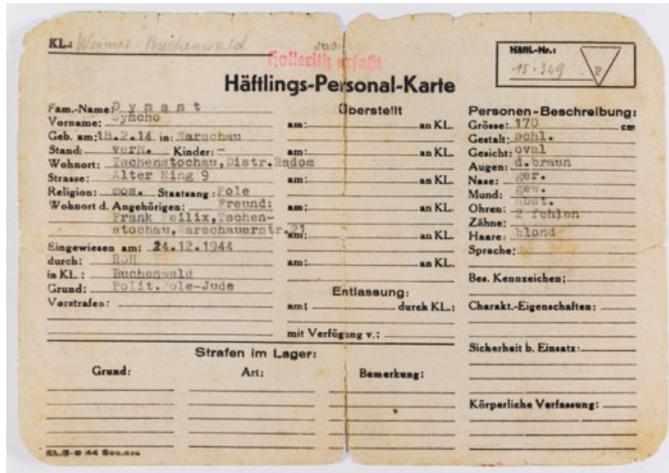
Bei der zweiten Volkszählung der Nazis 1939 gab es zusätzlich eine Ergänzungskarte, die neben der Haushaltsliste ausgefüllt werden musste. Darin fragten die Behörden nach der Abstammung („War oder ist einer der vier Großeltern Jude?“). Die Ergänzungskarte sollte in einem separaten Umschlag an die Zähler gegeben werden, um den Anschein von Anonymität hervorzurufen. Tatsächlich blieben die Angaben natürlich *nicht* anonym.



Dehomag-Werbung für Hollerith-Lochkarten für Volkszählung 1933

² Zitiert nach Buch Aly/Roth: „Die restlose Erfassung“, Frankfurt am Main 2000

Auf Falschangaben standen drakonische Strafen. Die beiden Volkszählungen blieben nicht die einzigen Maßnahmen zur Erfassung der Bevölkerung: 1935 kam das Arbeitsbuch, 1936 das Gesundheitsstammbuch, 1938 folgte die Meldepflicht am Wohnort und 1944 die Personenkennziffer.



„Hollerith erfaßt“ – Häftlingskarte eines Gefangenen im KZ Buchenwald

Bild: Buchenwald Arolsen Archives, cc by-sa 4.0

► **Hollerithmaschinen:
IBM und der Holocaust**

Und nun kommen wir zur Technik. Um Volkszählungsdaten schneller erfassen und verarbeiten zu können, hatte der US-amerikanische Ingenieur Hermann

Hollerith Ende der 1880er-Jahre ein Lochkartensystem erdacht. Inspiriert dazu hatten ihn die Schaffner in der Bahn, die damals bei der Kontrolle die Fahrkarten aus Karton gelocht haben und tatsächlich in der Platzierung der Lochung auf der Karte Information über die Fahrgäste codiert haben (männlich/weiblich, alt/jung), um die Weitergabe der Karten an andere zu erschweren. Die von Hollerith 1896 gegründete Firma für Lochkartensysteme hieß erst CTR, dann ab 1924 IBM. 1911 wurde die Deutsche Hollerith Maschinen Gesellschaft, kurz Dehomag, gegründet, die auf der Grundlage von Hollerith-Lizenzen arbeitete. Die Dehomag machte offenbar hervorragende Lobbyarbeit, um ihre Technik für die Volkszählung anzubieten. Der Firmenchef der US-Firma IBM Thomas J. Watson war sich nicht zu schade, sich mit Hitler persönlich zu treffen. Es gibt ein Foto von diesem Besuch bei Hitler vom Juni 1937. Am



Lesetipp: „Die restlose Erfassung“ von Götz Aly und Karl Heinz Roth – Ein wichtiges Buch, das anlässlich der Volkzählung in den 1980er Jahren erschienen ist.

„IBM und der Holocaust“ von Edwin Black über die Verstrickungen des Technikkonzerns IBM in die Verbrechen der Nazis.

selben Tag erhielt er den „Deutschen Adlerorden mit Stern“³ von Adolf Hitler für seine Verdienste um die Datenverarbeitung in Deutschland (und weil er als Präsident der Internationalen Handelskammer Nazideutschland verharmloste). Den Orden gab Watson erst am 6. Juni 1940 auf starken Druck der Öffentlichkeit hin zurück. IBM profitierte die ganze Zeit, auch während des Krieges, von Lizenzgebühren, die von der Dehomag bezahlt wurden. Die Dehomag war nicht nur bei der Volkszählung federführend, sondern war auch an der KZ-Verwaltung beteiligt. Die ganze Geschichte ist von Edwin Black in dem Buch „IBM und der Holocaust“⁴ umfassend aufgearbeitet worden. Er hatte im Holocaust-Museum in Washington eine Hollerith-Maschine entdeckt – das regte ihn zu dieser Recherche an. Klar ist: Ohne die Technik von Hollerith / IBM wäre eine so schnelle und effiziente Komplett-erfassung der Bevölkerung nicht möglich gewesen.

Wie es erst gewesen wäre, wenn Charles Babbage den Computer schon 40 Jahre früher erfunden hätte und die Nazis schon richtige Computer, Datenbanken

und Big Data Verarbeitung gehabt hätten, dazu gibt es eine spannende „Was-wäre-wenn“-Geschichte: Der Science Fiction Autor Andreas Eschbach schildert es in seinem Roman „NSA“ (das in diesem Fall für „Nationales Sicherheitsamt“ steht) sehr anschaulich.

► Das Böse: Menschen zur Zahl machen

Wenn wir diese Zusammenhänge auf einer abstrakteren Ebene betrachten, sollten wir erkennen, dass nicht nur der Missbrauch, sondern auch der legale Gebrauch solcher Daten problematisch ist.

Götz Aly und Karl Heinz Roth schreiben in ihrem Buch „Die restlose Erfassung“: „Liegt nicht schon in der Abstraktion des Menschen zur Ziffer ein fundamentaler Angriff auf seine Würde? Ist die Versuchung nicht gegeben, den einmal zum Merkmalsprofil geronnenen Menschen



Ein Überlebender der Shoa zeigt seine Häftlingsnummer, die im KZ eintätowiert wurde.

3 Hintergründe verlinkt über die Jahrbuch-Webseite

4 Edwin Black: IBM und der Holocaust. 2002

zu begründen, zu bereinigen, wie die Statistiker es nennen? Zählungen fördern die Macht des Objektiven, die Rationalität der Willkür. Auch ohne Mißbrauch.“

Wer Zugriff auf die Daten hat, hat Macht über die Menschen. Und die Reduzierung von Menschen auf Zahlen lässt bei denen, die die Macht haben, die Skrupel schwinden, Menschen zu kategorisieren, zu manipulieren, ihnen etwas anzutun.

► **Exkurs: Volkszählungen in der Bibel**

Es ist übrigens kein Phänomen der Neuzeit, Menschen zu Zahlen zu machen. Die Volkszählung in der Weihnachtsgeschichte⁵ ist hinlänglich bekannt. Und möglicherweise kennen einige auch die bösen Folgen, die diese Erfassung hatte: Nämlich die Geschichte aus dem Matthäus-Evangelium, wie König Herodes Angst vor dem neugeborenen Jesus als kommendem König der Juden bekam und befahl, in Bethlehem vorsichtshalber alle Kinder bis zum Alter von zwei Jahren zu ermorden⁶. Auch hier: Die Volkszählung machte es möglich.

Was aber eher unbekannt ist: Schon 1000 Jahre früher gab es eine Volkszählung unter König David – meines Wissens der älteste Bericht über ein solches Vorhaben überhaupt. Der biblische Text lässt keinen Zweifel daran, was eine Volkszählung in Gottes Augen dar-

stellt und David erkennt es im Verlauf der Geschichte selbst: Eine schwere Sünde, eine Anmaßung und eine Torheit. Zur Strafe für diese Hybris ließ Gott die Pest über Israel kommen, der viele tausend Menschen zum Opfer fielen, bis König David Gott darum bat, dass er persönlich gestraft werde, da er es ja war, der durch die Zählung gesündigt hatte und nicht das Volk Israels.⁷

► **Die geplante Volkszählung Anfang der 1980er-Jahre**

Mit dem historischen Wissen ist es wenig erstaunlich, dass die geplante Volkszählung 1981 in der Bundesrepublik Deutschland bei der Bevölkerung auf Widerstand stieß. In den 1980er-Jahren war die Aufarbeitung des Nationalsozialismus in Deutschland sehr präsent, ebenso wie das Bewusstsein für die Überwachung im totalitären Staat von Stalins Sowjetunion und auch die Überwachung durch die Stasi im Osten Deutschlands, in der DDR. George Orwells Dystopie „1984“ war populäre Lektüre, auch weil das Jahr 1984 näher rückte. Der Widerstand kam nicht nur von aktiven linken Gruppen, die dem Staat misstrauten, sondern bekam eine breite Basis auch bei einer selbstbewussten bürgerlichen Bevölkerung. Das Gefühl war: „Was geht das den Staat an, wo ich wohne, wie groß meine Wohnung ist? Am Ende wollen die noch wissen, was ich verdiene oder so!“ und „Was wollen die damit machen?“ und

5 Lukas 2, 1-20

6 Matthäus 2,1-16.

7 1. Buch der Chronik, 21. Kapitel.

„Was könnten die später damit noch alles machen?“. Menschen befürchteten den „gläsernen Bürger“ und den Einstieg in einen Überwachungsstaat. Und so wurde zum „Volkszählungsboykott“ aufgerufen – ein Akt zivilen Ungehorsames. Einige Bürger:innen entschlossen sich, Verfassungsbeschwerde vor dem Bundesverfassungsgericht einzu legen. In Deutschland dürfen Bürger:innen und Bürger innerhalb eines Jahres nach Inkrafttreten eines Gesetzes Verfassungsbeschwerde dagegen einlegen. Der höchste Gerichtshof dafür ist das Bundesverfassungsgericht in Karlsruhe.

Neben der Vielfalt der Aktionen und der zahlreichen Presseberichte trugen vor allem drei Faktoren zum großen Wachsen der Datenschutzbewegung bei: 1. Jede und jeder Einzelne war von der Volkszählung betroffen. 2. Es passierte etwas Wahrnehmbares: Zähler:innen kamen zur Wohnungstür, ein Fragebogen sollte ausgefüllt werden. 3. Die Daten sollten maschinell verarbeitet werden. Das machte Menschen Angst. Denn der Computer war zum Anfang der 1980er-Jahre in der Vorstellung der Menschen nicht der eigene PC, sondern ein Großrechner – der „Computer der Anderen“⁸.

► Ein Meilenstein: Das Volkszählungsurteil

Am 15. Dezember 1983 verkündete das Bundesverfassungsgericht sein Urteil zur Volkszählung. Es war ein Grundsatz-

⁸ Freie Assoziation auf den Kino-Film „Das Leben der Anderen“, 2006



„Das Volk zählt nicht, es wird gezählt.“
(Protestspruch zur Volkszählung)

surteil, dessen Bedeutung über die Entscheidung zur Volkszählung weit hinausging. Es etablierte das „Grundrecht auf informationelle Selbstbestimmung“. Dieses Grundrecht leitete das Gericht aus den allgemeinen Persönlichkeitsrechten und der Menschenwürde ab – also aus Artikel 1 des Grundgesetzes „Die

Foto: Ingo Jürgensmann, cc-by-sa 4.0



Erster Senat des Bundesverfassungsgerichtes, Herbst 2020

Würde des Menschen ist unantastbar.“ und Artikel 2 „Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit.“ Die Richter haben den Text des Urteils absichtlich weitgehend in allgemein verständlicher Sprache formuliert, damit es nicht nur von Jurist.innen, sondern von allen Bürger.innen verstanden werden kann.

Die wichtigste Stelle im Volkszählungsurteil erklärt, warum der Zugriff auf unsere Daten unsere Freiheit einschränken kann:

„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. [...]

Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.

Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“⁹

⁹ Link zum Volltext des Volkszählungsurteils auf der Jahrbuch-Webseite



Credit: Pressestelle Bundesverfassungsgericht.

Das Gericht macht klar, dass diese Einschränkung unserer Persönlichkeitsrechte nicht nur eine Privatangelegenheit ist, sondern unsere Demokratie insgesamt berührt.

„Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten.“

Wenn jemand aus Angst, dass es irgendwann später negative Folgen für sie oder ihn haben könnte, seine Freiheitsrechte wie z.B. Versammlungsfreiheit nicht mehr ausübt, dann schadet das eben nicht nur der einen Person, die sich einschränkt, sondern es schadet der Gesellschaft insgesamt.

Denn Meinungen, Ideen, Kritik und Verbesserungsvorschläge dieses Menschen gehen dann nicht mehr in den allgemeinen Pool ein. Damit unterbleibt

nicht nur Auseinandersetzung und konstruktiver Wettstreit der Ideen, sondern es verhindert langfristig auch die Innovation in einer Gesellschaft.

Deshalb ist Datenschutz – oder besser gesagt: der Schutz der Persönlichkeitsrechte – keine Privatangelegenheit, die jede und jeder für sich aushandeln kann, sondern er ist im Interesse der Allgemeinheit und schützt unsere Demokratie.

Die Wirkung des Volkszählungsurteils ging über den konkreten Fall weit hinaus. Es legte die Latte hoch für den weiteren Umgang mit Daten und beeinflusste die nachfolgende Gesetzgebung.

Es gab zwar schon 1970 ein Landesdatenschutzgesetz im Bundesland Hessen – verfasst von Prof. Dr. Spiros Simitis, der damit als „Vater des Datenschutzes“ gilt. Und ab 1977 gab es dann auch ein Bundesdatenschutzgesetz. Aber durch das Volkszählungsurteil 1983 wurde klar, dass die bisher darin enthaltenen Regelungen nicht den verfassungsrechtlichen Anforderungen genügten.

► **Datenschutz ist Top-Thema – die Zivilgesellschaft ist aktiv**

Dieses Urteil war ein großer Erfolg der Volkszählungsgegner:innen. Die für 1983 geplante Volkszählung wurde durch das Urteil untersagt. 1987 wurde die Zählung nachgeholt – nun unter datenschutzgerechteren Rahmenbedingungen. So wurden die personenbezogenen Angaben von den anderen Fragen getrennt und der Fragebogen überarbeitet. Damit sollte die Anonymität besser gewährleistet werden. Denn 1983 gab es die Befürchtung, dass durch die Kombination von bestimmten Eigenschaften vorgeblich anonyme Daten doch wieder bestimmten Personen zugeordnet werden könnten.

Doch die Bedenken der Kritiker:innen waren keineswegs ausgeräumt: Sie befürchteten auch 1987 eine schleichende Einschränkung von Bürgerrechten.

Damals sollten die Zähler:innen von Haus zu Haus gehen und gemeinsam mit den Bewohner:innen die Zählbögen ausfüllen. Der Widerstand wuchs. Und es gab eine große Vielfalt an Aktionsformen: Es zirkulierten Tipps, wie man die Zählbögen un-

serlich für die maschinelle Auswertung machen konnte. Leute weigerten sich, den Zähler:innen die Tür zu öffnen, klebten „Erika Mustermann“ als Namen an die Klingel und nahmen ein Bußgeld in Kauf. Es wurden Broschüren erstellt mit Argumenten gegen die Volkszählung. Es gab zahlreiche Demonstrationen in verschiedenen Orten und viele lokale Aktionsgruppen für den Volkszählungsboykott. In einigen Städten resignierte die Verwaltung und ergänzte die feh-

lenden Zahlen schließlich einfach aus dem Einwohnermelderegister. Was nicht unbedingt im Sinne einer Inventur ist...

Die öffentliche Auseinandersetzung um die Volkszählung spiegelt sich in den Umfragen aus jener Zeit wider: So ermit-

telte das Emnid-Institut im Dezember 1987 die Bedrohung durch Datenmissbrauch an vierter Stelle der Befürchtungen von Bundesbürgern – hinter Kriegsgefahr, Arbeitslosigkeit und Umwelterstörung.

Die Zivilgesellschaft war enorm aktiv in den 1980er-Jahren. Eine Vielzahl von Datenschutz-, Bürgerrechts- und Netzorganisationen gründete sich in Deutschland: Der Chaos Computer Club, Digi-

► **Leute klebten „Erika Mustermann“ als Namen an die Klingel und nahmen ein Bußgeld in Kauf. ◀**



talcourage (damals noch FoeBuD e.V.), Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FlFF), die Deutsche Vereinigung für Datenschutz (DVD), das Komitee für Grundrechte und

Demokratie. Und das zusätzlich zu den bereits bestehenden Vereinen Humanistische Union (1961) und die Internationale Liga für Menschenrechte (1914 / neu gegründet 1959). Jede Organisation hatte ihren eigenen Stil und setzte eigene Akzente, gleichzeitig gab es viel Vernetzung.

► Computer, Hacker und Haecksen

Was noch wichtig war: Im Laufe der 1980er-Jahre wurden Personal Computer bezahlbar. Viele – vor allem junge – Leute lernten damit umzugehen, probierten viel aus und wurden echte Cracks beim Programmieren. Die Szene war lebendig, mobil und extrem kreativ. 1984 hackte der Chaos Computer Club den Account der Hamburger Sparkasse im Bildschirmtext-System der Deutschen Bundespost (Btx), 1986 die NASA (ja, genau die). Die Hacks zeigten, wie



Rena Tangens und Wau Holland,
Mitbegründer des Chaos
Computer Clubs, 1985 bei
Art d'Ameublement

Foto: padaluun, cc by-sa 4.0

► Der eigene Computer wurde zu einem Werkzeug zur Befreiung, der Selbstermächtigung und des Austausches mit anderen. ◀

unsicher Daten auf Servern waren. Mit einem einfachen Atari-Rechner konnte ein Jugendlicher einen Server unter seine Kontrolle und Zugriff auf geheime Daten bekommen. Der Großrechner war früher als Unterdrückungsinstrument gesehen worden – der eigene Computer wurde zu einem Werkzeug zur Befrei-

ung, der Selbstermächtigung und des Austausches mit anderen.

Im Folgenden möchte ich exemplarisch die Anfänge von Digi-

talcourage beschreiben, denn sie zeigen, was die Szene in Deutschland auszeichnete und wie wichtig der Austausch von unterschiedlichsten Akteuren war. Insbesondere von politisch Interessierten und Techies.

1985 war der Chaos Computer Club zu Gast in der Galerie Art d'Ameublement von mir (Rena Tangens) und pade-luun in Bielefeld. Auf einem Rechner wurde ein Apfelmännchen (die sogenannte Mandelbrotmenge, eine fraktale Grafik mit Bezug zur Chaostheorie) ausgerechnet, was damals noch eineinhalb Tage dauerte. Ansonsten schraubten die Jungs als erstes die Telefondose auseinander und verbanden einen Rechner mit einem selbstgebauten Modem mit der Telefonleitung. Via Datenleitung Datex-P ging es fröhlich durchs Netz auf fremde Server. Unter anderem in den Rechner der Washington Post, wo wir schon mal die Nachrichten des nächsten Tages anschauen konnten. Das war – anders als heute – so nicht gedacht. Aber es war auch nicht illegal, denn es gab noch kein Gesetz dagegen, weil der Gesetzgeber schlicht nicht wusste, dass so etwas überhaupt möglich ist. Wir waren fasziniert! Zum einen von den unendlichen Möglichkeiten, die das Netz versprach, zum anderen von den blitzenden Augen der Menschen, die bei der Veranstaltung dabei waren. Hier passierte gerade etwas sehr Spannendes. Die neue Welt, die sich hier auftat, wollten wir nicht nur erkunden, sondern wir wollten sie mitgestalten. Und sie zu einer besseren Welt machen.



Foto: pade-luun, cc by 4.0

Die Besucher unserer ersten PUBLIC DOMAIN 1987 im Bunker Ulmenwall in Bielefeld

Die Jugendlichen, die damals in unserer Kunstgalerie dabei waren, waren die Keimzelle für die Veranstaltungsreihe „Public Domain“ (► Seite 152) und die Gründung von Digitalcourage (damals noch FoeBuD) in Bielefeld. „Public Domain“ stand für „öffentlicher Bereich“, also: alle willkommen, auch ohne Computerkenntnisse. Und andererseits stand „Public Domain“ auch für „öffentliche Angelegenheit“, also: Themen, um die wir uns kümmern sollten. Und in diesem Spannungsbereich von Technik und Politik, Wissenschaft und Spaß entstand eine sehr kommunikative und experimentierfreudige Szene.

► Eigene Kommunikationsnetze

Eines der wichtigsten Projekte, die gemeinsam verwirklicht wurden, war ein eigenes Netzwerksystem – eine Mail-Box (englisch: Bulletin Board) mit Namen BIONIC, die 1989 in Betrieb genommen wurde. Über eine MailBox konnte nicht nur private E-Mail ausgetauscht werden, sondern auch News – öffentliche Nach-

richten in sogenannten Brettern, die thematisch organisiert waren. Damit gab es zum ersten Mal eine Möglichkeit für alle, eigene Texte zu veröffentlichen, aktuelle Nachrichten zu schreiben und Mitstreiter zu finden. Ohne eine Redaktion, ohne große Kosten und ohne Zensur.

Auf unserem Netzknoten lief die Zerberus-MailBox-Software. Schon bald waren die Bielefelder Aktiven in regem Kontakt zu den Zerberus-Programmierern. Und die waren sehr offen für Anregungen. Zerberus verwirklichte „Privacy by Design“¹⁰, noch bevor Ann Cavoukian das Konzept dazu veröffentlichte, also Datenschutz, der direkt in



► **Es gab keine Werbung. Und es gab keine Ausforschung von Teilnehmer:innen.** ◀

die Technik eingebaut ist. Die privaten Postfächer der Teilnehmer:innen wurden mit ihrem Passwort verschlüsselt. So konnten auch die Systembetreiber nicht die Nachrichten der Nutzer:

innen in ihren persönlichen Postfächern lesen. Und Zerberus hatte auch „Privacy by Default“, also datenschutzfreundliche Voreinstellungen. Andere Teilnehmer:innen konnten z.B. nicht sehen, wer gleichzeitig online war, es sei denn, man hatte diese Information bewusst freigeschaltet. Die Teilnehmer:innen bezahlten einen monatlichen Betrag für die Nutzung und finanzierten so gemeinsam die Kosten für den MailBox-Server. Es gab keine Werbung. Und es gab keine Aus-

forschung von Teilnehmer:innen. Die MailBox-Netze waren dezentral organisiert. Die Teilnehmer:innen bestimmten die Inhalte, es gab keine Zensur, aber es gab Regeln. Zweimal

im Jahr fanden bundesweite Treffen der MailBox-Betreiber:innen statt, bei denen über die Regeln im Netz – die Netikette –, Inhalte und neue Bretter und über politische Themen debattiert wurde. Daten-

Foto: Digitalcourage, cc by 4.0



„Auch wir wollten nicht wissen, was Leute per Mailbox miteinander besprechen. Wir wollten unsere Nutzer:innen schützen – auch vor uns selbst.“

10 Mehr zu „Privacy by design“ auf Wikipedia

► Der Kapitalismus fühlte sich als Sieger und ließ jegliche Rücksicht fallen. ◀

schutz war ein wichtiges Thema in den Diskussionen, denn die MailBox-Betreiber:innen kannten es aus eigener Anschauung. Es war aufregend, wir waren am Puls der Zeit und wir konnten viel bewirken. Denn die Technik, die wir gestalteten, setzte den Rahmen, in dem andere aktiv wurden und kommunizierten. Wir wollten mit dieser Macht verantwortlich umgehen. Wir wollten die Teilnehmer:innen zu mündigen Techniknutzer:innen machen und wollten sie schützen, auch vor uns selbst.

► Die 1990er-Jahre

1989: Demonstrationen erst in Leipzig, dann vielerorts in der DDR. Und dann, im November 1989, fiel tatsächlich die Mauer – das hatten nicht einmal die Geheimdienste erwartet. Eine friedliche Revolution in Deutschland! Die Begeisterung war groß (nicht bei allen, das ist klar), es gab die Hoffnung, das Beste aus beiden Systemen zusammenbringen zu können. Aber dann ging alles ziemlich schnell mit der Wiedervereinigung von Ost- und Westdeutschland. Die Sowjetunion zerfiel. Historiker:innen redeten vom Ende der Geschichte. Es wurde der Eindruck erweckt, nun sei alles gut. Kein kalter Krieg mehr. Demokratie überall.

Das ist jetzt die Kurzfassung. Klar, dass es dazu viel mehr und viel Kontroverses zu sagen gibt. Worauf ich in diesem Zusammenhang hinweisen will: Nun entfiel die Konkurrenz der politischen

Systeme. Der Kapitalismus, der vorher noch durch allerhand Regeln

und Sozialsysteme gebändigt war, fühlte sich als Sieger und ließ jegliche Rücksicht fallen. Ich komme darauf zurück.

Zunächst kam eine Blütezeit der freien Bürgernetze. Sie hatten auch in diesen frühen Zeiten schon an die 100.000 Teilnehmer:innen im deutschsprachigen Raum. Z-Netz und CL-Netz bekamen 1992 bis 1996 ein Pendant im ehemaligen Jugoslawien während des Krieges dort: Zamir Transnational Network¹¹. Zamir bedeutet auf deutsch: für den Frieden. Da die Telefonleitungen zwischen Serbien und Kroatien aus politischen Gründen blockiert waren, stellte das Zamir-Netz nun per Auslandstelefonat über Deutschland die Verbindung zwischen Friedensgruppen in verschie-



Foto: Rena Tangens, cc by 4.0

Die zwei höchsten Bürohochhäuser in Sarajevo – ausgebrannt, aber standhaft.

¹¹ Das Zamir-Netz haben wir ausführlich im Jahrbuch für 2021 vorgestellt.

Foto: Digitalcourage, cc by 4.0



Eric Bachman, Begründer des Zamir Transnational Network im ehemaligen Jugoslawien

denen Landesteilen Jugoslawiens wieder her. Zamir-MailBoxen in Zagreb in Kroatien, Belgrad in Serbien, Ljubljana in Slovenien, Pristina im Kosovo und sogar im knapp drei Jahre belagerten Sarajevo in Bosnien erlaubten Menschen dort untereinander und mit der Welt zu kommunizieren, vermisste Verwandte und Freunde wiederzufinden. Alle Zamir-MailBoxen liefen mit Zerberus. Der Netzknoten, der die Verbindung herstellte, war die BIONIC-Mailbox in Bielefeld in unserem Keller. Das war eine große Verantwortung und ein weiterer Grund, Datenschutz in der Software und im Betrieb des Netzes ernstzunehmen.

Zeitgleich entwickelte sich das World Wide Web. Mit dem Start 1993 und den grafischen Möglichkeiten wurde das Netz plötzlich auch interessant für Konzerne. AOL (America online) entwickelte sich ab Mitte der 1990er-Jahre bis in

die erste Hälfte der 2000er zum größten Provider weltweit und brachte eine völlig veränderte Netzkultur mit sich. Jahrelang lagen nun Gratis-Disketten und CDs mit der AOL-Zugangssoftware vielen Ausgaben von Computerzeitschriften bei zum Anfixen. Die Millionen neuen Nutzer:innen hatten keine Ahnung, wie das Netz funktionierte. Sie hatten keine Ahnung, wie einfach E-Mails mitzulesen waren oder ihr Verhalten online mitgespeichert werden konnte. Keine Aufklärung, keine Mitgestaltung, keine Eigenverantwortung, keine eigenen Verhaltensregeln. Hauptsache drin. Klick und bunt. Datenschutz? Ach – egal.

Mitte der 1990er-Jahre entwickelte sich die Internet- bzw. Dotcom-Blase. Der Aktienmarkt überhitzte sich, Tech-Startups überboten sich im Verbrennen von Cash. Was sie tatsächlich machten, war nebensächlich – Risiko-Kapitalfirmen kauften alles. Geld ist Macht ohne Verantwortung.

Zum Ende der 1990er-Jahre gab es schlicht keinen Markt mehr für eine Zugangssoftware – der Markt war platt. Damit gab es auch keine Möglichkeit mehr, Datenschutz direkt durch Softwaregestaltung als Rahmenbau durchzusetzen. Wir mussten uns nach anderen Einflussmöglichkeiten für unsere Idee von einer lebenswerten Welt im digitalen Zeitalter umschaun. Und die kam durch den Anruf einer Journalistin in unser Haus.

► Geld ist Macht ohne Verantwortung. ◀

BIG BROTHER AWARDS

► Die ersten BigBrotherAwards

Christiane Schulzki-Haddouti schrieb 1999 für heise.de¹² einen Artikel über die Verleihung der BigBrotherAwards in Großbritannien – ein Negativpreis, der die größten Datenschutzsünder auszeichnen sollte. Im Zuge der Recherche für ihren Artikel rief sie bei Digitalcourage (damals noch FoeBuD) an und fragte, warum es eigentlich keinen BigBrotherAward in Deutschland gäbe – und ob wir den nicht organisieren wollten? Wir sagten spontan: Ja – wir machen das! „Wir machen das“ wurde dann die Überschrift über ihrem Artikel – dann mussten wir das natürlich auch machen :). Im Jahr 2000 war es soweit.

Foto: Digitalcourage, cc by 4.0



Rena Tangens bei den ersten BigBrotherAwards im Jahr 2000, damals noch im Bielefelder Bunker Ulmenwall

¹² Der Heise-Verlag gibt die Computerzeitschrift „c’t“ heraus, die „iX“ und „Technology Review“. Unter heise.de gibt es Online-News und das Magazin Telepolis.

Wir hatten sofort beschlossen, diese Veranstaltung nicht alleine zu machen, sondern kompetente Persönlichkeiten aus anderen Datenschutz-, Bürgerrechts- und Netzorganisationen mit in die Jury zu holen. Der Chaos Computer Club, FifF, DVD und die Internationale Liga für Menschenrechte war beteiligt – Hacker, Programmierer, ein renommierter Rechtsanwalt und ein stellvertretender Landesdatenschutzbeauftragter. Mit einer Mischung aus Charme, Chuzpe und Wahnsinn (denn wir wussten zu dieser Zeit nie vorher, ob und wie wir die Veranstaltung finanziert bekommen würden und arbeiteten alle noch ehrenamtlich) stellten wir die erste Verleihung der deutschen BigBrotherAwards in Bielefeld auf die Beine. Und sie schlug ein, als ob

die Öffentlichkeit nur darauf gewartet hätte: Fernsehen war vor Ort, viel Presse und sogar ein Redakteur der Tageszeitung „Le Monde“ aus Frankreich war extra angereist. Aus seinem Artikel stammt der Untertitel für die BigBrotherAwards:

„Die Oscars für Überwachung“.

Seit 2000 verleihen wir jährlich die BigBrotherAwards in Deutschland. Wir verleihen die BigBrotherAwards in verschiedenen Kategorien: Politik, Behörden und



Foto: Markus Bentler, cc by-sa 4.0

Verwaltung, Technik, Verbraucherschutz, Arbeitswelt – weitere Kategorien entstehen nach Bedarf. Außerdem gibt es den „Preis fürs Lebenswerk“

2018 und 2019 fanden die BigBrotherAwards im Bielefelder Stadttheater statt. Und sobald die Pandemie es zulässt, möchten wir dort auch wieder die Reihen füllen.

► **Datenschutz durch Öffentlichkeit: Die BigBrotherAwards wirken**

Die BigBrotherAwards machen die abstrakten Themen Datenschutz, Überwachung und Manipulation anschaulich. Sie nennen Ross und Reiter, also Politiker:innen, Institutionen und Konzerne, die für Datenschutzvergehen, für Überwachungstechnologien und -gesetze und uferlose Datensammlungen verantwortlich sind. Sie bringen bis dahin unbekannte Informationen ins Licht der Öffentlichkeit und klären auf. So machten die BigBrotherAwards zum Beispiel Rabattkarten, Scoring, Mautkameras, Farbkopierer und Handyüberwachung

als Gefahr für Bürgerrechte und Privatsphäre bekannt. Sie warnten schon früh vor der Gesundheitskarte, der Steuer-ID und der Vorratsdatenspeicherung. Und sie sprachen deutliche Worte zu Ausländerzentralregister, Lauschangriff und Anti-Terror-Gesetzen. Die BigBrotherAwards-Gala gibt der Presse immer wieder einen Anlass für ausführliche Berichterstattung. Der öffentlich-rechtliche TV-Sender WDR ist jedes Jahr mit einer Live-Schaltung vor Ort.

Digitalcourage wirkt, wirken Sie mit!

► digitalcourage.de/spende

Wie kommen wir zu den Themen? Die BigBrotherAwards bekommen jedes Jahr mehrere Hundert Meldungen und Vorschläge für geeignete Preisträger – von geprellten Verbrauchern, von bespitzelten Arbeitnehmerinnen, von Administratoren, Software-Entwicklerinnen und Behördenmitarbeitern. Manchmal ist die Nominierung

eine kurze E-Mail, die den Anstoß gibt, manchmal kommt ein ganzes Dossier. Wir gehen allen Hinweisen nach, beobachten die technische und politische Entwicklung und recherchieren in die Tiefe.

Egal, ob Firma oder Politiker:innen: Die Preisträger sind durch die Bank wenig erfreut über ihre Auszeichnung. Wir laden sie eine Woche vorher zu der Veranstaltung ein, doch sie kommen eher selten zur Preisverleihung. Erstaunliche Ausnahme: Microsoft flog 2002 seinen Datenschutzbeauftragten ein, der für Microsoft den Preis fürs Lebenswerk entgegennahm. Der Chef



Jochen Wegner, der Chefredakteur von Zeit Online, gehörte zu den wenigen Preisträgern, die den BigBrotherAward selbst abholten.

von Zeit Online kam 2019 zur BigBrotherAward-Verleihung, um sich zu äußern. Auch die Deutsche Telekom hatte 2008 den Mut, den Preis abzuholen. Tatsächlich erkundigte sich die Telekom sogar schon Monate vorher diskret bei uns, ob sie etwa einen BigBrotherAward bekommen würde – „sie könnten sich vorstellen, dass sie ihn verdient hätten...“ (Die Telekom hatte ihren eigenen Aufsichtsrat bespitzelt und das war aufgefliegen.)

► Die Preisträger sind durch die Bank wenig erfreut über ihre Auszeichnung. ◀

Andere meinten, sie könnten den BBA einfach ignorieren. Zum Beispiel die Bayer AG – nominiert für den Drogentest per Urinprobe bei ihren Auszubildenden – gab sich nicht die Mühe einer Antwort. Doch einige Monate später bekamen wir eine Einladung der Kritischen Aktionäre. Sie übertrugen uns ein paar Bayer-Aktien. Damit waren wir plötzlich Aktionäre und hatten Rederecht auf der Bayer-Aktionärsversammlung. So kam es, dass die Über-

Foto: Mischa Burmester, cc-by-sa 4.0

**Unabhängige Arbeit braucht unabhängiges Geld.
Werden Sie Fördermitglied!**

► digitalcourage.de/mitglied

gabe dieses BigBrotherAwards nicht vor 500 Zuschauern bei der Gala in Bielefeld stattfand, sondern vor 5.000 Zuschauern bei der Bayer-Hauptversammlung in Köln.

Andere BigBrotherAwards-Preisträger drohen offen oder verklausuliert mit Klage, wie z.B. die Post AG, Lidl und der türkische Religionsverband Ditib, der wegen der Bespitzelung von Gemeindegliedern durch nach Deutschland entsandte Imame ausgezeichnet wurde. Solche Drohungen haben uns aber noch von keiner Preisverleihung abgehalten. Wir lassen uns nicht einschüchtern. Uns schützt die Öffentlichkeit – und unsere finanzielle Unabhängigkeit: Digitalcourage erhält kein staatliches Geld und

akzeptiert kein Sponsoring von Konzernen, sondern finanziert sich ganz überwiegend durch private Spenden und Fördermitgliedschaften. So kann uns niemand mal eben den Geldhahn zudrehen. Die mittlerweile (2020) fast 3.000 Mitglieder sind nicht nur wichtig für die unabhängige Finanzierung – sie zeigen auch, wie vielen Menschen in Deutschland diese Themen wichtig sind und geben Digitalcourage auch politisches Gewicht.

Die BigBrotherAwards sind ein wichtiges Instrument zur Aufklärung der Öffentlichkeit. Sie haben des häufigeren auch direkte Folgen bei den Preisträgern. So wurde Payback nach dem

Foto: Digitalcourage, cc by 4.0



padeluum und Rena Tangens mit den Kritischen Aktionären
vorm Eingang zur Bayer-Hauptversammlung 2003

BBA fürs Datensammeln via Kundenkarte vom Verbraucherschutzverein verklagt und musste sämtliche Anmeldeformulare vom Markt nehmen und seine Datenschutzbestimmungen überarbeiten. Versandhandel Tchibo widersprach zunächst dem BBA; einige Jahre später beendeten sie stillschweigend den gerügten Verkauf (sie nannten es „Vermietung“) von Nutzeradressen. Nach dem Big-BrotherAward für die Computer Science Corporation (CSC) wurden die Vergaberichtlinien für die Aufträge von öffentlichen Stellen geändert, so dass Firmen mit dieser Art von Geheimdienstkontakten dabei nicht mehr berücksichtigt werden. Etliche Bundesländer haben daraufhin ihre Verträge mit CSC gekündigt.

Schließlich wirken die BigBrotherAwards auch präventiv. Wir wissen: In Führungsetagen von Unterneh-

men wird über uns gesprochen. Die Big-BrotherAwards liefern ein gewichtiges Argument für Konzerndatenschutzbeauftragte, wenn sie Einspruch gegen ein geplantes Ausforschen von Kund.innen oder Bespitzelung von Mitarbeiter.innen erheben.

Die BigBrotherAwards wirken auch präventiv. ◀



Das Datenschutzbewusstsein in Deutschland, das in den 1990er-Jahren gelitten hatte, erhält auch durch die BigBrotherAwards neuen Auftrieb. Das ist deutlich zu sehen in einer Studie der EU, die das Datenschutzbewusstsein in den verschiedenen europäischen Ländern vergleicht¹³.

Doch kurz weiter in der Chronologie: Mitte des Jahres 2000 platzte die Dotcom-Blase, viel Risiko-Kapital war verbrannt. Google war gerade nochmal davon gekommen und sann auf andere Möglichkeiten, Geld zu

¹³ Verlinkt über die Jahrbuch-Webseite

Foto: Digitalcourage, cc by 4.0



Laudator Rolf Gössner hält bei den BigBrotherAwards 2005 die Laudatio für Bundesinnenminister Otto Schily fürs „Lebenswerk“.

► Meilenstein: Der Sieg über die Metro AG inspiriert die Bewegung

machen. Das Konzept des Überwachungskapitalismus begann sich zu materialisieren.

Dann passierten die Attentate vom 11. September 2001. Danach war nichts wie zuvor. Die Terroristen lieferten Scharfmachern unter den Politikern den willkommenen Anlass, um eine Fülle von Überwachungsgesetzen aus der Schublade zu holen und durch die Parlamente zu prügeln. In Deutschland tat sich insbesondere Innenminister Otto Schily hervor, dessen schnell gestricktes Paket an Überwachungsgesetzen als „Otto-Katalog“ verulkt wurde. Ab da wurde der Kampf gegen staatliche Überwachung wieder zum drängenden Thema. Doch viele sahen keine Handlungsmöglichkeiten: „Was kann ich als Einzelne schon dagegen machen?“ Aber das änderte sich auch wieder.

Die Metro AG erhielt 2003 einen BigBrotherAward für ihren „Freilandversuch“ mit RFID-Funkchips auf den Waren in einem Supermarkt in Rheingebirg bei Duisburg. RFID (Radio Frequency Identification) sind winzige Chips mit Antenne, die Informationen über das Produkt und eine eindeutige Seriennummer enthalten und per Funk ausgelesen werden können. Eine Gefahr für die Privatsphäre, denn das Auslesen funktioniert ohne Sichtkontakt, kann also unbemerkt geschehen. Wie berechtigt der BigBrotherAward für die Metro AG war, stellten wir erst einige Monate später fest. Wir deckten Anfang 2004 auf, dass der Konzern RFID-Schnüffelchips auch in den Payback-Kundenkarten des Supermarktes versteckt hatte – ohne Wissen der Kund.innen. Wir brachten den Fall in die Presse – er stand in der Financial Times und landete schließ-



Foto: Digitalcourage, cc by 4.0

Dieses Foto ging um die Welt. Es wurde auch in Australien und den USA gedruckt: Unsere StopRFID-Demo 2004 vor dem Future Store der Metro AG in Rheinberg

talcourage (damals noch FoeBuD) hatte zu dieser Zeit mal gerade etwas mehr als 60 Mitglieder. Trotzdem hatten wir es geschafft.

lich sogar in den Börsennachrichten zur Metro. Und wir organisierten eine Demonstration vor dem Supermarkt. Dies war die erste Demonstration gegen die RFID-Technologie – die Bilder gingen um die Welt. Daraufhin zog Metro die verwandte Karte zurück.

Das war ein Erfolg, der viele beflügelt hat! Denn er hat gezeigt, dass Widerstand nicht zwecklos ist. Das Nachrichtenmagazin Spiegel schrieb damals:

“Es ist ein ungleicher Kampf – eine Handvoll ehrenamtlicher Enthusiasten gegen milliardenschwere Konzerne – doch er zeigt Wirkung.“

In der Tat: Die Metro AG war der weltweit drittgrößte Handelskonzern. Digi-

► Der Kampf gegen die Vorratsdatenspeicherung

Dieser Erfolg war enorm wichtig für die Datenschutzbewegung. Er weckte Hoffnung und brachte Menschen dazu, aktiv zu werden. Das nächste Thema war schon ausgemacht: Die von der EU geplante Vorratsdatenspeicherung sämtlicher Telefonverbindungsdaten. Ende 2005 beim Chaos Communication Congress gründete sich der Arbeitskreis Vorratsdatenspeicherung, kurz: AK Vorrat.

Nicht jammern – klagen!

Unterstützen Sie unsere Verfassungsbeschwerden gegen Vorratsdatenspeicherung und Staatstrojaner!

► digitalcourage.de/spende

Im Arbeitskreis waren verschiedenste Organisationen und Einzelpersonen vertreten und alle setzten ihre Kompetenz ein, um gegen diese massenhafte und anlasslose Überwachung vorzugehen. Es gab Aufklärung, Studien, juristische Gutachten, Schreiben an Politiker:innen, Infostände und Demonstrationen. Der Jurist Patrick Breyer verfasste gemeinsam mit dem Rechtsanwalt Meinhard Starostik eine Verfassungsbeschwerde gegen die Vorratsdatenspeicherung (► Seite 32). Und für die Verfassungsbeschwerde sammelten wir gemeinsam Unterstützer:innen – online und auf Papier. Das Wunder: Mehr als 34.000 Menschen unterschrieben eine Vollmacht für unseren Anwalt Meinhard Starostik und wur-

► 34.000 Unterschriften gegen die massenhafte und anlasslose Überwachung ◀

den damit zu Mit-Beschwerdeführer:innen. Am 31. Dezember 2007 reichten wir die

Beschwerde in Karlsruhe ein. Das war die größte Verfassungsbeschwerde in der Geschichte der Bundesrepublik.

► Meilenstein: Demo „Freiheit statt Angst“

Der Widerstand ging weiter. Wir organisierten Demonstrationen unter dem Motto „Freiheit statt Angst“¹⁴. Zur Demo riefen mehr als 160 Organisationen mit auf. Nicht nur klassische Bürgerrechtsorganisationen, sondern so unterschiedliche wie Gewerkschaften, Ärzteverbände, Jugendorganisationen, Parteien von FDP, Grünen, Piraten bis zur Linken, Journalisten-Verbände, Amnesty

International, der antikapitalistische Block, die AIDS-Hilfe und die evangelische Telefonseelsorge. 2008 brachte „Freiheit statt Angst“ 50.000 Menschen in Berlin auf die Straße. Das war mehr als in den 1980er Jahren



Foto: Matthias Hornung, cc-by-sa 4.0

„Freiheit statt Angst“ –
Großdemonstration gegen die
Vorratsdatenspeicherung.
padeluum vor dem Fronttransparent

beim Widerstand gegen die Volkszählung.

¹⁴ Englisch: „Freedom not Fear“. Die englische Übersetzung wurde später auch zum Namen für das jährliche Barcamp in Brüssel, wo sich Aktivist:innen aus ganz Europa treffen.

► Die 2010er-Jahre

Ein großer Erfolg: Am 2. März 2010 entschied das Bundesverfassungsgericht, dass das vom Bundestag 2007 beschlossene Gesetz zur Vorratsdatenspeicherung verfassungswidrig und nichtig ist. Das Gesetz war damit gekippt, bereits gesammelte Daten mussten unverzüglich gelöscht werden. Leider war die Vorratsdatenspeicherung an sich damit nicht vollständig verboten, sondern immer noch unter bestimmten Voraussetzungen erlaubt.

Als das Urteil zur Vorratsdatenspeicherung gesprochen war, wussten wir: Wir haben eine Chance, auch ELENA¹⁵ zu kippen. ELENA (der Elektronische Ent-

geltnachweis) war eine detaillierte Vorratsdatenspeicherung von Arbeitnehmer.innen-Daten. Eine Verfassungsbeschwerde war allerdings nur noch bis zum 1. April 2010 möglich. Doch wir hatten beim Aktivcongress alles schon vorbereitet: Unser Rechtsanwalt Meinhard Starostik hatte die Klageschrift vorbereitet, die Website zum Unterstützer.innen sammeln war eingerichtet, Presseartikel waren schon geschrieben – alles wartete nur auf das „Go!“.

So schafften wir, innerhalb von nur 14 Tagen mehr als 22.000 Mitbeschwerdeführer.innen zusammenzubringen. Dafür mussten die Menschen mehr als einen Klick im Internet machen: Sie mussten

► Innerhalb von nur
14 Tagen mehr als
22.000 Mitbeschwerde-
führer.innen ◀



Digitalcourage auf dem Weg zum Bundesverfassungsgericht mit Anwalt Meinhard Starostik (oranger Schal), um die Verfassungsbeschwerde gegen die Vorratsdatenspeicherung abzugeben.

Foto: Tom Kohler, cc-by-sa 4.0

¹⁵ Zum ELENA-Verfahren gibt es Hintergründe auf Wikipedia



Foto: Ronald Wittke, cc-by-sa 4.0

das Formular ausfüllen, das daraus generierte pdf-Dokument ausdrucken, unterschreiben und per Brief an Digitalcourage schicken. Die Vollmachten füllten viele Ordner. Am 31. März fuhr ein ganzer Kleinlaster voller „Nein!“ zum Bundesverfassungsgericht nach Karlsruhe. Dieses Engagement hatte Wirkung auf Politiker:innen. Tatsächlich wurde ELENA aus Datenschutzgründen gekippt, ohne dass die Verfassungsbeschwerde verhandelt werden musste.

2011 verleihen wir Facebook einen BigBrotherAward und beschreiben es als eine kommerzielle „Gated Community“ zum Zweck der Ausforschung und Manipulation. 2013 erhält Google einen BigBrotherAward. Wir fordern: „Google muss zerschlagen werden.“ Das verärgert einige aus der Szene, weil sie Google doch so einfach

Ein Kleinlaster voll „Nein!“ – gelbe Ordner mit 22.000 Vollmachten bei der Pressekonferenz zur ELENA-Verfassungsbeschwerde

► Google hat de facto ein Monopol. Der Wettbewerb ist ausgehebelt. ◀

und nützlich finden. Aber wir sind überzeugt: Google hat inzwischen extrem viel – zuviel – Macht. Google hat in verschiedenen Bereichen ein de facto Monopol. Hier gibt es keinen funktionierenden Wettbewerb mehr. Google sammelt nicht nur aus unterschiedlichen Quellen detaillierteste Information über alle Menschen, sondern Google bestimmt auch durch seine Suchergebnisse, was Menschen als relevant ansehen, Google hat den Zeitungen die Finanzierung durch Anzeigen weggenommen, womit die Medien in Finanzierungsnot kommen. Google ist nicht demokratisch legitimiert, hat mehr Macht als viele Staaten. Google ist eine Gefahr für die Demokratie. (► Seite 40 und 97 und 142)

► **Meilenstein: Edward Snowden enthüllt Überwachung durch US-Geheimdienste**

Im Juni 2013 wird der ehemalige CIA- und NSA-Mitarbeiter Edward Snowden zum Whistleblower: Er gibt in Hongkong vertrauliche Informationen zu Überwachungseinrichtungen der US-Geheimdienste an die Presse, u.a. an Glenn Greenwald, der für den britischen „Guardian“ schreibt. Und er gibt der Filmmacherin Laura Poitras Interviews. Er legt seine Identität offen und beschreibt seine Motivation, warum er sich zu diesem Schritt entschlossen hat, der für ihn persönlich sehr weitreichende Folgen hat – er musste flüchten und lebt seitdem im Exil:

„Ich möchte nicht in einer Welt leben, in der alles, was ich tue und sage, aufgezeichnet wird. Solche Bedingungen bin ich weder bereit zu unterstützen, noch will ich unter solchen leben.“

Die Enthüllungen schlugen ein wie eine Bombe. Nach und nach wurden immer mehr Details über die massenhafte Überwachung veröffentlicht. Die Empörung in Deutschland war groß. Vielen wurde erst jetzt klar, dass sie tatsächlich auf Schritt und Tritt überwacht wurden, dass jede Bewegung, jede Kommuni-



Foto: Digitalcourage, cc by 4.0

2014 haben wir den bislang einzigen Positiv-Award („Julia- und Winston-Award“) an Edward Snowden vergeben. Deshalb haben wir 1 Million Aufkleber „Asyl für Edward Snowden“ kostenlos verteilt.

kation und jede Meinungsäußerung von den US-Diensten (und anderen der Five Eyes¹⁶) mitgeschnitten werden konnte. Wir hatten seit vielen Jahren immer wieder gewarnt, dass diese Möglichkeit bestand. Aber nun war es keine theoretische Annahme mehr – durch Edward Snowden gab es plötzlich die Beweise, dass diese Überwachung Fakt ist, dass sie tatsächlich passiert. Wir konnten sagen: „Das haben wir euch doch schon immer gesagt.“ Aber das war eine Sache, bei der es keinen Spaß machte, Recht zu haben.

¹⁶ Eine Geheimdienstkooperation von Australien, Kanada, Neuseeland, USA und Großbritannien

Dann wurde öffentlich: Auch das Mobiltelefon der deutschen Kanzlerin wurde abgehört. Angela Merkel sagte: „Abhören unter Freunden – das geht gar nicht!“ Die Bundesregierung versprach vollständige Aufklärung und vermittelte den Eindruck, dass sie etwas gegen die massenhafte Überwachung der deutschen Bevölkerung tun wollte. Tatsächlich passierte ... nichts.

► „Abhören unter Freunden – das geht gar nicht!“ ◄

► Der paradoxe Snowden-Effekt

Zunächst bekam die Bewegung für Bürgerrechte und Datenschutz neuen Zulauf. Denn viele waren empört und wollten nun selber aktiv werden. Doch dann verging Zeit und die Bundesregierung machte keine Anstalten, ernsthaft die Überwachung durch ausländische Geheimdienste unterbinden zu wollen, sie versuchte, die schwierige Sache einfach auszusitzen. Nach der Bundestagswahl im Herbst 2013 regierte eine Große Koalition von CDU/CSU und SPD. Die drei Parteien, die sich klar gegen Überwachung aussprachen, waren geschwächt (Grüne und Linke) bzw. aus dem Bundestag geflogen (FDP). Die Opposi-

tion hatte quasi keine Chance. Resignation machte sich breit. Ein Grund war ein psychologischer: Zu erkennen, dass die Massenüberwachung keine abstrakte Gefahr war, sondern man selber seit Jahren überwacht worden war, ist traumatisch.

Um aus diesem unangenehmen Gefühl wieder herauszukommen, sagt man sich dann: „Aber der CIA interessiert sich ja gar nicht für mich. Und es ist ja auch gar nichts passiert. Dann wird das schon alles nicht so schlimm sein.“ oder auch „Jetzt ist eh schon alles zu spät.“ Das unangenehme Gefühl wird abgespalten und irgendwohin weggeschoben. Man will nicht darüber nachdenken. Die Untätigkeit der Bundesregierung, das Aussitzen kontroverser Themen bewirkte eine asymmetrische Demobilisierung¹⁷.



Foto: Stefanie Loos, cc by-sa 4.0

Aktion gegen das BND-Gesetz – mit Placebo-Pillen BNDal und Terrordilin

¹⁷ Begriffserklärung auf Wikipedia, verlinkt über die Jahrbuch-Webseite

► Einfluss von Datenschutzbewusstsein auf die Techniknutzung

Bei anderen wurde das Interesse an datenschutzfreundlichen Tools in Deutschland größer. Digitalcourage (damals noch FoeBuD) hatte schon in den 1990er-Jahren das E-Mail-Verschlüsselungsprogramm PGP (Pretty Good Privacy) unterstützt und ein deutsches Handbuch dazu herausgegeben. Dies führte dazu, dass laut Aussage des PGP-Erfinders Phil Zimmermann Deutschland die zweitmeisten Nutzer:innen hatte – weltweit.

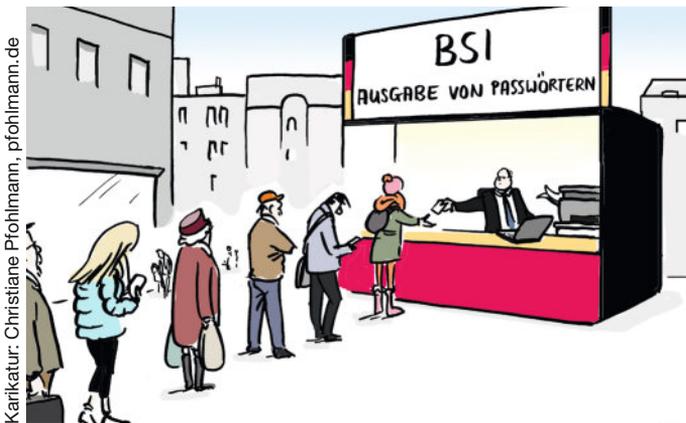
Nach Snowdens Enthüllungen 2013 hoben wir die „Digitale Selbstverteidigung“ aus der Taufe. Wir wollten Wissen

► Auch bei Suchmaschinen wird dringend eine Alternative gebraucht. ◀

über datenschutzfreundliche Tools und alternative Plattformen unter die Leute bringen. Die CryptoParty-Bewegung entstand: Treffen, wo Menschen ihre Rechner und Smartphones mitbringen können und Freiwillige ihnen helfen, die Geräte privatsphärefreundlicher einzurichten.

Aber: An vielen Stellen fehlen bisher einfache und nutzerfreundliche Alternativen – zum Beispiel gibt es keinen sicheren Messenger, den wir uneingeschränkt empfehlen können. Die Entwicklung solcher Alternativen muss bewusst gefördert werden. Auch bei Suchmaschinen wird dringend eine Alternative gebraucht, denn Google hat in Deutschland ein de facto Monopol. Wir haben einen konkreten Vorschlag zur Wiederherstellung des Wettbewerbs,

nämlich die Einrichtung eines Europäischen Suchindex (► Seite 142). Dieses Konzept ist mittlerweile auch in den Politikempfehlungen des WBGU¹⁸ für die Bundesregierung und die EU-Ratspräsidentschaft enthalten.



Karikatur: Christiane Pfohlmann, pfohlmann.de

Nicht die Art von Computersicherheit, die wir meinen...

¹⁸ WBGU – Wissenschaftlicher Beirat der Bundesregierung Globale Umweltveränderungen. Texte verlinkt über die Jahrbuch-Webseite

► Meilenstein: Die europäische Datenschutzgrundverordnung

Auf einer ganz anderen Ebene gab es Bewegung im europäischen Kontext. Schon 2012 hatte EU-Kommissarin Viviane Reding, zuständig für Justiz, Grundrechte und Bürgerschaft, eine grundlegende Neufassung des europäischen Datenschutzrechts angegangen. Es sollte keine EU-Richtlinie werden, sondern eine EU-Verordnung. Eine EU-Richtlinie muss immer erst noch in nationales Recht der einzelnen Mitgliedsstaaten umgesetzt werden – eine Verordnung dagegen gilt unmittelbar in allen EU-Ländern. Für Viviane Reding war der Hintergrund klar: Die bis dahin geltenden Datenschutzgesetze waren der technischen und wirtschaftlichen Entwicklung gegenüber nicht mehr angemessen. Gebraucht wurde so etwas wie eine „Lex Google“ und „Lex Facebook“, um der neuen Bedrohungen der Persönlichkeitsrechte durch große Digitalkonzerne besser gerecht zu werden.

Dass eben diese dabei nicht tatenlos zuschauen würden, war klar. Aber das Ausmaß der Lobby Schlacht, die daraufhin jahrelang in Brüssel tobte, hat sich wahrscheinlich niemand so vorgestellt. Die US-Handelskammer schickte Lobbyisten nach Brüssel. Die Digitalkonzerne gaben Unmengen an Geld für Lobbying, Pressearbeit und „Landschaftspflege“

aus. Sie bemühten sich, Datenschutz als Bürokratie, Hindernis für die Wirtschaft und als unzeitgemäß darzustellen. Und sie brachten über ihnen gewogene EU-Abgeordnete massenhafte Änderungsvorschläge zu dem Entwurf der Datenschutzgrundverordnung (kurz: DSGVO) ein. Es waren tatsächlich über 3.000 Änderungsvorschläge. Das war eine Art „Denial-of-Service Attacke“, wo man ein System durch Überlastung zum Zusammenbrechen bringen will, denn diese Menge kann kein EU-Abgeordneter in sinnvoller Zeit vor der Abstimmung lesen.

Dem engagierten grünen EU-Abgeordneten Jan Philipp Albrecht, der Berichterstatter für dieses Thema im LIBE-Ausschuss war, und seinem Team ist zu verdanken, dass die DSGVO (engl. GDPR) doch

► Eine Meisterleistung an Diplomatie und zähem Verhandlungsgeschick ◀

noch in der laufenden Legislaturperiode beschlossen wurde. Sie haben in einem Wahnsinns-Kraftakt die 3.000 Vorschläge auf 100 thematische Punkte zusammengedampft und haben mit einer Meisterleistung an Diplomatie und zähem Verhandlungsgeschick tatsächlich das Wunder vollbracht.

Wer einen kleinen Einblick bekommen will, wie Demokratie in der EU im besten Fall funktionieren kann, dem sei der Film „Democracy – Im Rausch der Daten“¹⁹

¹⁹ Film „Democracy“ verlinkt über die Jahrbuch-Webseite



Foto: Claudia Fischer, cc by 4.0

empfohlen, der diese Geschichte dokumentiert. Seit Mai 2018 ist die DSGVO nun in Kraft.

Natürlich ist die DSGVO ein Kompromiss, und die Datenschutzbewegung hat einiges daran auszusetzen. Aber ein wichtiger gelungener Punkt darin ist das sogenannte Marktortprinzip. Das heißt, es ist egal, wo das Unternehmen seinen Sitz hat – maßgeblich ist, wo es sein Business machen will. Wer mit EU-Bürger:innen Geschäfte machen will, muss sich an die hier geltenden Datenschutzregeln halten. Der zweite wichtige Punkt ist, dass die Bußgelder für Verstöße endlich so hoch angesetzt worden sind, dass sie einem Unternehmen im Ernstfall richtig weh tun können. Dadurch ist Datenschutz nun zur Chefsache geworden.

Vorher wurde von Lobbyist:innen die Angst geschürt, dass Europa zurückbleiben könnte, wenn es hier strenge

Unser jährliches Barcamp Freedom not Fear in Brüssel – 2017 trafen wir im Europaparlament MEP Julia Reda und MEP Jan Philipp Albrecht

► **Andere Länder nehmen seitdem die DSGVO als Vorbild.** ◀

Datenschutzregeln gäbe und dass sich weltweit niemand sonst darum scheren würde. Doch das Gegenteil ist der Fall. So nehmen sich andere Länder seitdem die DSGVO als Vorbild und gestalten danach ähnliche Datenschutzgesetze für ihr Land – so zum Beispiel Kalifornien. Die Datenschutzbeauftragte eines Kreditkartenkonzerns sagte mir bei einem Kongress, dass sie ja ursprünglich gegen die DSGVO waren. Aber nun, wo sie geltendes Recht ist, würden sie sie natürlich auch umsetzen – und zwar nicht nur für Europa, sondern weltweit. Denn sie wollten keine unterschiedliche Regelungen für verschiedene Länder. Es ist noch längst nicht alles gut mit dem Datenschutz in Europa, es müssen

Verbesserungen durchgesetzt werden und es wird noch viele Gerichtsverfahren geben müssen, um das Recht durchzusetzen.

Nun rücken die Monopole der Internetkonzerne verstärkt in den Blick. In Deutschland soll das Wettbewerbsrecht modernisiert werden, um den neuen Anforderungen durch die Digitalisierung gerecht zu werden. Eine erste Änderung war bereits, dass nicht nur der Umsatz, sondern auch der Zugriff auf Daten für die Ermittlung einer marktbeherrschenden Stellung herangezogen werden soll. Wir sehen das Wettbewerbsrecht als ein mögliches Werkzeug an, um die Macht der datensammelnden Konzerne einzuschränken und haben gemeinsam mit Oxfam, Kartellrechtlern und grünen Unternehmern den Gesetzentwurf kritisch kommentiert²⁰.

Hoffnung ruht auch auf der EU-Wettbewerbskommissarin Margrethe Vestager, die schon in der Vergangenheit Mut und Durchsetzungskraft gezeigt hat.

► Überwachungskapitalismus

Shoshana Zuboff hat 2018 mit ihrem Buch „Das Zeitalter des Überwachungskapitalismus“ ein Grundlagenwerk veröffentlicht. Sie kritisiert die massenhafte Aneignung von Daten durch die Konzerne, die Information über jegliche Lebensäußerungen von Menschen abgreifen, als ob das herrenloses Gut wäre. Die Konzerne schlachten diese

Informationen aus und erzielen damit gigantische Gewinne. Dabei werden Gesetze gezielt missachtet und Fakten geschaffen.

Derweil wurden Medien, insbesondere Zeitungen, geschwächt, deren Anzeigenmarkt sich Facebook und Google angeeignet haben (► Seite 101). Medien, Journalistenhochschulen und NGOs erhalten Geld von Facebook und Google. Sie weisen es natürlich von sich, aber es wäre naiv, anzunehmen, dass sie sich *nicht* davon beeinflussen lassen würden.

Wenn es an die Grundlagen ihres Geschäftsmodells geht, verstehen die Plattformkonzerne absolut keinen Spaß. Google hat seinen Wahlspruch „Don't be evil“ 2015 aufgegeben. Inzwischen wird von Google auch nicht mehr versucht, den Anschein zu erwecken, freundlich zu

Erhältlich bei uns im Shop

Das Zeitalter des Überwachungskapitalismus

von Shoshana Zuboff.

Aus dem Englischen von Bernhard Schmid



Gebundene Ausgabe:

727 Seiten mit
Lesebändchen

Verlag: Campus

ISBN-13:

978-3593509303

Preis: 29,95 EUR

inkl. MwSt. und Versand

► shop.digitalcourage.de

²⁰ Verlinkt über die Jahrbuch-Webseite



Margrethe Vestager,
EU-Wettbewerbskommissarin

sein – weder gegenüber kritischen Angestellten noch gegenüber Kritiker:innen der Google-Geschäftspolitik. Es wird mit harten Bandagen gekämpft. Ein Beispiel: In dem einflussreichen Washingtoner Thinktank „New America Foundation“ gab es eine Arbeitsgruppe zu „Open Markets“. Der Vorsitzende dieser Arbeitsgruppe, Barry Lynn, hat in einem Blogpost die Entscheidung der EU-Wettbewerbskommissarin Margrethe Vestager begrüßt, Google eine Strafzahlung²¹ von 2,4 Milliarden Dollar zu aufzuerlegen. Kurz darauf wurde er entlassen²². Dazu sollte man wissen, dass Google einer der Geldgeber des New America Thinktanks ist. Daraufhin hat die gesamte Arbeitsgruppe Free Markets den Thinktank verlassen und sich außerhalb neu gegründet.

Ein anderer Fall. Im Mai 2019 wurde öffentlich: Facebook-Lobbyist Richard Allen – ehemaliger Tory-Abgeordneter –

21 Quelle verlinkt über die Jahrbuch-Webseite

22 Quelle verlinkt über die Jahrbuch-Webseite

hat Mitglieder einer hochrangigen EU-Expertengruppe erpresst²³. Die Arbeitsgruppe befasste sich mit dem Thema Desinformation und wollte zur Ermittlung von marktbeherrschenden Stellungen sogenannte Sektorenuntersuchungen fordern – ein anerkanntes Mittel der Kartellbehörden. Um zu verhindern, dass diese Forderung in dem gemeinsamen Papier der Expertengruppe steht, schnappte sich Allen in den Kaffeepausen Vertreter:innen von verschiedenen Nichtregierungsorganisationen und drohte ihnen damit, dass er ihnen den Geldhahn abdrehen würde, wenn sie für Sektorenuntersuchungen stimmen.

► **Es wird mit harten Bandagen gekämpft.** ◀

Die Drohung funktionierte – es gab keine Sektorenuntersuchungen.

Was zeigt, wie gefährlich es für NGOs ist, Projekte mit Konzernen zusammen zu machen, denn damit geraten sie in finanzielle Abhängigkeit.

► **Suchterzeugung und Manipulation**

Was mit dem Überwachungskapitalismus einhergeht, ist das Bemühen der Plattform-Konzerne, insbesondere Google, Facebook, Youtube, Instagram, Tiktok, Netflix, die Menschen möglichst lange Zeit auf ihrer Plattform zu beschäftigen. Deshalb werden die Nutzeroberfläche, die Angebote und die Voreinstellungen psychologisch so gestaltet, dass sie suchterzeugend wirken. Das Smart-

23 Recherchen von Investigate Europe, Quellen verlinkt über die Jahrbuch-Webseite

► **All diese Tricks, um Verhalten zu beeinflussen, haben eine fatale Wirkung, die über Überwachung hinausgehen.** ◀

phone wirkt wie ein Glücksspielautomat – schnell nochmal nachschauen, ob eine neue Nachricht, ein neues Foto da ist. Immer lockt die Verheißung, dass jetzt etwas Nettes dabei ist. Die Aufmerksamkeitsspanne sinkt, viele sind nicht mehr in der Lage, längere Texte zu lesen oder etwas selber im Gedächtnis zu behalten anstatt „mal schnell zu googlen“. Wer sich ständig von Maps herumführen lässt, verlernt, Karten zu lesen. Menschen sehnen sich nach Bestätigung durch andere – das macht „Likes“ so wichtig und deshalb ist es eine Katastrophe, wenn sie ausbleiben. Fotos von anderen müssen innerhalb von 24 Stunden ge-like-t werden, sonst droht Abwertung. Das erzeugt sozialen Druck, ständig erreichbar zu sein. Der „unendliche Scroll“ lässt Menschen immer weiter wischen, weil sie versuchen, das Ende der Seite zu erreichen, was aber nie kommt. Autoplay als Voreinstellung spielt immer automatisch das nächste Video an – so bleiben Menschen länger daran hängen. Schließlich werden

auch die Algorithmen so gestaltet, dass sie möglichst viel Aktivität auf der eigenen Plattform erzeugen. So schlägt

Youtube nach einer Suche thematisch ähnliche Videos vor, allerdings tendenziell immer welche, die vom Inhalt radikaler sind. Denn egal, ob Menschen dem radikaleren Video zustimmen oder sich aufregen, weil sie anderer Meinung sind – es wird sie auf jeden Fall dazu bringen, noch mehr Zeit auf Youtube zu verbringen. All diese Tricks, um Verhalten zu beeinflussen, haben eine fatale Wirkung, die über Überwachung hinausgehen. Sie halten Menschen von anderen, sinnvolleren Tätigkeiten ab, sie beeinflussen ihre Meinung und sehr oft führen sie zur



Die Verführer – Pseudo-Gratis für unsere Daten

Karikatur: Christiane Pfohlmann, pfohlmann.de

Foto: Alexander Altmann, cc-by-sa 4.0



Rena Tangens,
Netzpionierin seit den 1980er-Jahren

Radikalisierung. Je wirrer und radikaler eine Geschichte ist, desto mehr geraten Menschen, die vom Algorithmus mit immer mehr davon gefüttert werden, in eine Filter Bubble, und zwar nicht nur mit einer Meinung, sondern mit ihrer eigenen Wahrheit.

All diese Effekte beeinflussen unsere Gesellschaft äußerst negativ. Es ist an der Zeit, dass wir uns dagegen wehren. Die betreffenden Konzerne werden ihr Verhalten keineswegs freiwillig ändern, denn sie berühren ihr Geschäftsmodell. Es ist notwendig, dass sie per Gesetz dazu gezwungen werden. Darum müssen wir uns kümmern, solange es noch nicht zu spät ist.

Um die Frage vom Anfang noch einmal aufzunehmen: Das Bewusstsein für Datenschutz in Deutschland hat

mit Sicherheit Wurzeln in der Erfahrung mit zwei Diktaturen auf deutschem Boden. Seit den 1980er-Jahren gab es eine wechselvolle Geschichte mit etlichen Erfolgen für die Datenschutzbewegung, die auch andere in Europa inspiriert haben. Auf der anderen Seite stellen der Überwachungskapitalismus und die ungezügelte Macht der Internet-Konzerne unseren Einsatz für Freiheit und Demokratie vor immer neue Aufgaben. Bürgerrechte müssen immer wieder neu erkämpft werden. Wenn wir sie nicht nutzen, werden wir enteignet. Und wir sollten uns hüten, sie für ein Linsengericht²⁴ einzutauschen.

**„Die Zeit wird kommen,
da ihr euch entscheiden
müsst zwischen dem, was
richtig und dem, was
bequem ist.“**

(Albus Dumbledore,
Schulleiter von Harry Potter)

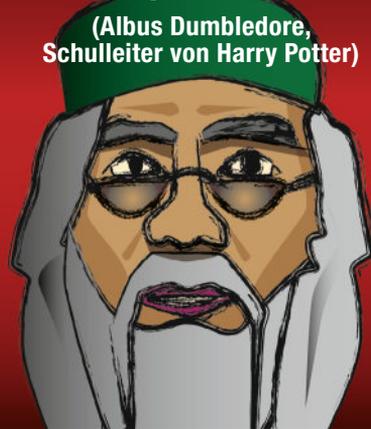


Illustration: Isabel Wienold, cc by 4.0

²⁴ Rena Tangens: Tausche Bürgerrechte gegen Linsengericht, 2004 (verlinkt über die Jahrbuch-Webseite)

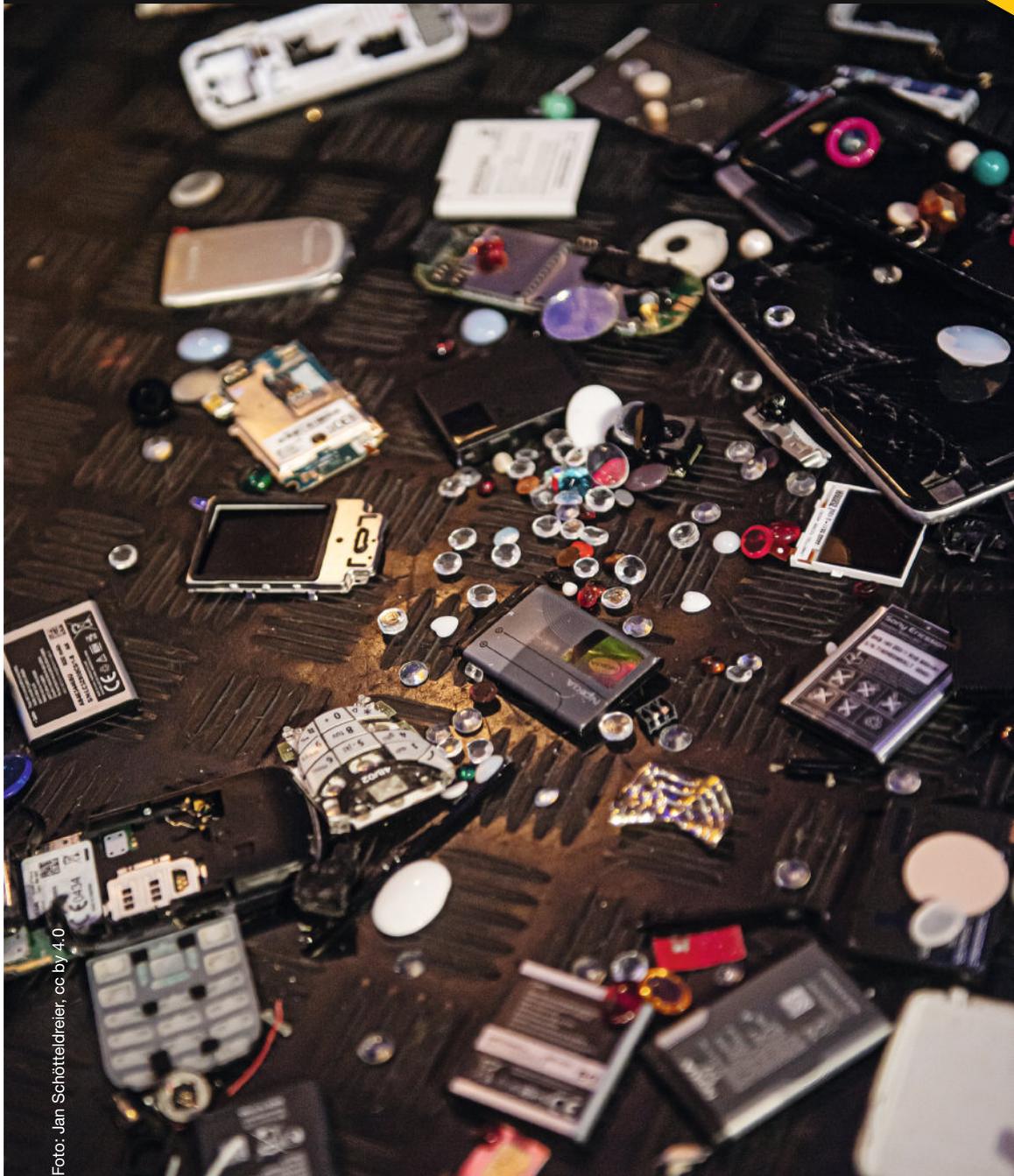


Foto: Jan Schötteldreier, cc by 4.0

Zubehör zu unseren Themen gibt es auch auf digitalcourage.de/shop
Links und weitere Infos: digitalcourage.de/jahrbuch21

Preise und Auszeichnungen für Digitalcourage

Digitalcourage hat in den vergangenen Jahren einige Preise und Auszeichnungen gewonnen. Hier ein kleiner Überblick aller Ehrungen, die der Verein – auch schon zu FoeBuD-Zeiten – bekommen hat.

- ▶ **„Spendenaktion 30 Jahre Linux“**, 8. Platz im Publikumsvoting für Digitalcourage. Die Firma B1 Systems hat anlässlich des Linux-Jubiläums 30.000 Euro Spenden per Online-Voting auf Projekte verteilt, die Open Source Software in besonderer Weise fördern. linux30.b1-systems.de
- ▶ **„Corona-Helden 2020“**, Konzerteinladung vom NDR an Rena Tangens und padeluum (2021). Sie wurden ausgezeichnet, weil sie trotz der Corona-Beschränkungen viel Aufwand betrieben haben, um die BigBrotherAwards auch während der Pandemie durchzuführen.
- ▶ **„Ehrendadel der Stadt Bielefeld“** an Rena Tangens und padeluum (2018). Beide durften sich bei der Preisverleihung in das Goldene Buch der Stadt Bielefeld eintragen.
- ▶ Nominierung für den **„Grimme-Online-Award“** in der Kategorie SPEZIAL für Digitalcourage. (2018)
- ▶ **„Bürgerprojekt“-Preis der PSD-Bank** an unsere Mitarbeiterin Jessica Wawrzyński und ihren Blog kidsdigitalgenial.de (2017). Das Preisgeld war Anschubfinanzierung für eine gedruckte Version von Jessicas Online-Kinder- und Jugendlexikon „#kids #digital #genial von App bis Zip“. Jetzt als Broschüre und Buch im Digitalcourage-Shop erhältlich.
- ▶ **„Bielefelder Frauenpreis“ für Rena Tangens** für ihre zukunftsweisenden Gedanken und ihr Durchhaltevermögen. (2016)
- ▶ **„Der Heinrich“ der Heinrich-Böll-Stiftung NRW** (2015), weil wir mit unserer Arbeit „Müde und Zweifelnde zum Nachmachen“ ermuntern.
- ▶ **„Open Source-Preis“ für „Software für Engagierte“** für Arbeit an [civiCRM](https://civiCRM.org) (2015)
- ▶ **„Bundespreis Verbraucherschutz – Persönlichkeit des Verbraucherschutzes 2015“ der Deutschen Stiftung Verbraucherschutz** an Rena Tangens für ihr jahrzehntelanges Engagement für die Wahrung der digitalen Privatsphäre der Bürgerinnen und Bürger.

Foto: Fabian Kuriz, cc by 4.0



- ▶ **„taz Panter Preis für die Held.innen des Alltags – Preis der Jury“** an Digitalcourage für Weitblick und Engagement für Grundrechte (2014)
- ▶ **„For..Net-Award“** an Digitalcourage für den PrivacyDongle als benutzerfreundliche Möglichkeit zur anonymen Internetnutzung (2013)
- ▶ **„Goldener Löwe“ in Cannes** für die „fingerprints“-Kampagne von „Nordpol Hamburg“ (2008) für den AK Vorrat – ein Webtool, das digitale Spuren sichtbar machte.
- ▶ **„Theodor Heuss Medaille“** (2008) für außerordentlichen Einsatz für die Bürgerrechte, u.a. durch die Organisation der BigBrotherAwards.
- ▶ **Kunstpreis „Evolutionäre Zellen“ vom Karl-Ernst-Osthaus-Museum Hagen und der Neuen Gesellschaft für Bildende Kunst (NGBK) Berlin** an Rena Tangens und padeluun (2004)
- ▶ **Ideenwettbewerb zur Gründung der Stiftung bridge** für die Idee zum RFID-Privatizer. (2003)
- ▶ **„Sinnformation“ Preis der Grünen Bundestagsfraktion an FoeBuD** für den Aufbau des ZaMir MailBox-Netzes in Ex-Jugoslawien (1998)
- ▶ **„Videokunstpreis Marl“ an RenaTangens & padeluun** für „TV d’Ameublement“ (1984)

Und dann noch ein paar datenschutzrelevante Termine für 2022

28.1.2022 **Europäischer Datenschutztag.** Dieser Aktionstag erinnert an die Unterzeichnung der Europäischen Datenschutzkonvention am 28.1.1981.

26.-28.1.2022 **cpdp Conference** (Computer Privacy and Data Protection) in Brüssel cpdpconferences.org

8.2.2022 **Safer-Internet-Day / Tag der Internetsicherheit.**
Zur Sicherheit gehört auch, nicht überwacht zu werden!
digitalcourage.de/digitale-selbstverteidigung

26.-29.6.2022 Die **Gulaschprogrammierenacht** (kurz: GPN) ist eine viertägige Konferenz für Hacker und Haecksen, Technikbegeisterte und interessierte Laien vom Entropia e.V. in Karlsruhe. entropia.de/GPN

15.-18.4.2022 **Easterhegg 2022** in Hamburg. Familiäres Event des Chaos Computer Clubs für Hacker und Haecksen easterhegg.eu

29.4.2022 **BigBrotherAwards.** Die Verleihung der „Oscars für Überwachung“ 2022 in der Bielefelder Hechelei und im Livestream
bigbrotherawards.de

8.-10.6.2022 **re:publica** – Bloggerkonferenz in Berlin
re-publica.com/de

17.-18.9.2022 **Datenspuren,** Konferenz des Chaos Computer Clubs Dresden
datenspuren.de

Herbst 2022 **Freedom not Fear in Brüssel.** (► Seite 16) Wenn wir uns in Präsenz treffen, besuchen wir gemeinsam das Europäische Parlament. 2020 und 2021 fanden Videokonferenz statt. Neue Interessierte sind herzlich willkommen! freedomnotfear.org

27.-30.12.2022 **Chaos Communication Congress.** Großes internationales Treffen von Hackern und Haecksen, ggf. online als rC3 (remote Chaos Communication Congress) events.ccc.de (► Seite 52)

Außerdem:

- Der **Digital Markets Act** und der **Digital Services Act** sollen 2022 in der EU beschlossen werden.
- In Deutschland gibt es 2022 eine neue **Volkszählung** zensus2022.de (► Seite 162)
- Ein übersichtlicher Ort für alle Ihre Termine: **Der Digitalcourage-Wandkalender 2022**, erhältlich in unserem Shop. shop.digitalcourage.de

Index

11. September 2001 177
 42 154
 4UMaps 141
 Abstammung 159
 Account 139
 ActivityPub 130
 Adams, Douglas 103, 154f.
 Adventskalender 118
 Advocacy 19, 152
 Aegis 135
 Afghanistan 50
 AFWall+ 135
 AGB 110, 112, 131, 149
 AK Vorrat 178
 Aktivcongress 14
 Albrecht, Jan Philipp 185f.
 Algorithmen 31, 44, 59,
 83, 86, 142, 145ff., 189f.
 Allen, Richard 188
 Aly, Götz 160f.
 Amazon 40, 43, 103, 113
 Analog 54, 55
 Android 123, 134ff.
 AnkiDroid 135
 Anonymes Bargeld 12
 Anonymität 127, 159, 166
 AntennaPod 134
 AOL 171
 Apfelmännchen 168
 APK-Datei 139
 App-Stores 138f.
 App 24, 54f., 57, 59, 62,
 88f., 96, 114, 121, 123f.,
 129, 132, 134ff., 192
 Apple Flinger 136
 Arbeit 54
 Arbeitsgruppe Digitale
 Selbstverteidigung 118
 Arbeitslosigkeit 166
 Arbeitswelt 173
 Arisch 159
 Armbruster, Ralf 23
 Art d'Ameublement 167,
 168
 Arzt 114
 Ärzteverbände 179
 Asymmetrische Demobili-
 sierung 183
 Audio 132
 Auftragsverarbeitungsver-
 trag 110f.
 Augenbewegungen 81, 86
 Aurora Store 137
 Auskunften 31
 Ausländerzentralregis-
 ter 173
 Australien 178, 182
 Ausweisdokumente 51
 Autohersteller 75ff.
 Autonomie 143, 149f.
 Babbage, Charles 161
 Backup 129
 Baden-Württemberg 22ff.,
 87
 Baidu 143f. 146
 Ballerspiel 155
 Baltik, Luisa 49
 Banken 18, 54
 Barcamp 14, 16, 157,
 179, 186
 Bargeld 12, 30
 Baseball 104
 Bayer AG 174
 Bayern 64, 74, 95
 Bayernatlas 141
 Beckedahl, Markus 89
 Bedrohung 50, 166
 Behörden 12f., 21, 33, 51,
 54f., 59, 72ff., 121, 149,
 159, 172
 Belgard 171
 Belletristik 19
 BelWü 23f.
 Benzinverbrauch 75
 Berechtigtes Interesse 97
 Berechtigungen 55, 136,
 139
 Berlin 109, 114, 194
 Bertelsmann Arvato 31
 Bethlehem 162
 Betriebssystem 100, 125
 Beuth, Peter 74
 Bewegungsdaten 77, 144
 Bewegungsstiftung 2
 Bibliotheken 136, 143
 Biden, Joe 106
 Bielefeld 192
 Big Data 15, 161
 Big Tech 103, 105f., 149
 Big-Tech-Konzern 103
 BigBlueButton 63, 121
 BigBrotherAwards 8, 14f.,
 22, 28, 65f., 68, 70ff., 74,
 88f., 99f., 107, 172ff.,
 192ff.
 Bildung 10ff., 20f., 24f.,
 56f., 79, 86
 Bildungspaket 7, 12, 19,
 25, 27
 Bildungsplattform 22ff.
 Bildungssystem 24
 Bing 135, 143f., 146
 Biometrisch 12, 28, 46, 50
 BIONIC 168, 171
 BKA 33, 36, 72
 blabber.im 123, 134
 Black, Edwin 160f.
 Blockchain 10, 12
 BND 13, 33, 72, 74
 BobBall 136
 Bosnien 171
 Bot 132
 Breyer, Patrick 73, 179
 Brin, Sergey 146
 Brink, Stefan 22, 87
 Bromite 137
 Browser-Fingerab-
 druck 100, 102
 Browser 20, 80, 100ff., 120,
 125, 127, 137
 Brunnstein, Klaus 155
 Brüssel 16, 157, 179, 185f.,
 194
 Bundesanstalt für Ar-
 beit 74
 Bundeskanzleramt 74
 Bundeskriminalamt 36, 74
 Bundesnachrichten-
 dienst 74
 Bundespolizei 74
 Bundesregierung 8, 10ff.,
 33f., 74, 77, 148, 183f.
 Bundesrepublik Deutsch-
 land 162
 Bundestagswahl 183
 Bundesverfassungsge-
 richt 17, 29, 32f., 61, 90,
 163, 165, 180f.
 Bundesversammlungsgesetz
 61
 Bundeswehr 74
 Bündnis „Unsere digitale
 Schule“ 23
 Bündnis 90/Die Grünen.
 -> Die Grünen
 Bürgernetze 170
 Bürgerrechte 158, 166,
 173, 183, 190, 193
 Campact 31, 36
 Campaigning 8
 Cavoukian, Ann 169
 CDs 171
 CDU 22, 33, 40, 74, 94,
 183
 Chaos Communication
 Congress 7, 52, 112, 178,
 194, 201
 Chaos Computer Club
 (CCC) 23, 45, 51f., 71,
 75, 112, 116, 166ff., 168,
 172, 194
 Chaostheorie 168
 Chat 20, 80, 123, 134
 Chatkontrolle 13
 CheckNow 31
 China 59, 68, 143, 146ff.
 Christl, Wolfie 146
 Chrome 80, 101f.
 CIA 182f.
 CiviCRM 18
 CL-Netz 170
 Click and Collect 55
 Cloud Act 147
 Cloud 23, 113, 119, 139
 CO2 75
 Collabora 121, 137
 Computer 21, 23, 45, 51f.,
 63, 66, 71, 75, 96, 106,
 118, 120, 127, 161, 163,
 167f., 172, 176
 Computerspiel 52
 Conversations 123, 134
 Cookie-Banner 11, 42,
 97ff.
 Cookie 11, 42, 80, 86, 97ff.,
 110f., 116
 Corona Contact Tracing
 Germany 136
 Corona-Leugner-Demo 94
 Corona 7f., 19, 30f., 57, 63,
 67, 70, 79f., 83, 88f., 92,
 94ff., 109, 136f., 192
 Coronavirus 114
 cpdp-Conference 194
 CPU-Info 137
 Crossposting 132
 CryptDrive 124, 129
 CryptoCafés 7
 CryptoParty 7, 17, 118,
 184
 CryptPad 20, 120, 124,
 128f.
 CSU 74, 183
 Cyber-Abwehrzentren 74
 Cyber-Krieg 74
 Dark Pattern 11, 41f., 98,
 103, 107
 Datenbanken 74, 110, 161
 Datenkraken 15
 Datenportabilität 130f.
 Datenraum-Mobilität 77
 Datenschutz an Schulen 19
 Datenschutzbeauftragte
 12, 87, 186
 Datenschutzbewe-
 gung 158, 163, 178,
 186, 190
 Datenschutzgesetz 165,
 185f.
 Datenschutzgrundverord-
 nung -> DSGVO
 Datensparsamkeit 55, 138
 Datenspuren 30, 194
 Datenübertragung 139
 Datenverarbeitung 41, 76,
 111, 116, 161, 164
 Datex-P 168
 DAVx5 134, 136
 DDR 162, 170
 Dehomag 159ff.

- Democracy Im Rausch der Daten (Film) 185
- Demokratie 11, 14, 19, 40, 42, 58f., 61, 73, 142, 146, 148f., 158, 165, 170, 181, 185, 190
- Demonstrationen 14, 33, 46, 58, 60, 166, 170, 178f.
- Demuth, Kerstin 30, 33
- Denial-of-Service-Attacke 185
- Deportation 158
- Design 42, 97ff., 134
- Desinformation 44, 188
- Desktop Publishing 155
- Deutsche Presseagentur 90
- Deutsche Statistische Gesellschaft 159
- Deutsche Telekom 174
- Deutsche Vereinigung für Datenschutz (DVD) 167
- Deutschland 85
- Dezentralität 130
- Diaspora 131
- Die Grünen 22f., 41, 74, 107, 179, 183, 185, 187, 193
- Die Linke 179, 183
- Diesel-Skandal 75
- Digital Markets Act 10f., 40ff., 106, 194
- Digital Services Act 10, 106
- Digitalcourage 14, 166, 168, 172, 175, 178, 184
- Digitale Angriffe 58
- Digitale Gesellschaft 45
- Digitale Infrastruktur 146
- Digitale Mündigkeit 15, 21, 57
- Digitale Selbstverteidigung 14, 17, 20, 29, 56, 63, 118, 126, 184
- Digitalkonzerne 29, 106, 149, 185
- Digitalzwang 13, 54f.
- Digitalzwangsmelder 54
- Discord 122
- Diskurs 92, 132f.
- Distributionen. -> Linux
- Ditib 175
- DNS-Server 18
- Doctolib 8, 55, 108ff.
- Doodle 124
- Dotcom-Blase 171, 176
- Drip 136
- Drittanbieter-Cookies 80
- Dropbox 125
- DSGVO 10, 78, 80, 90, 106, 110, 113ff., 131, 139, 147, 185f.
- Duck, Daisy 49
- DuckDuckGo 143f.
- e-Call 76
- E-Mail-Verschlüsselung 184
- E-Mail 70f., 115, 118, 125, 134, 168, 171, 174
- Easterhegg 194
- Ebelt, Friedemann 159
- EBI 48
- EC-Karten -> Kreditkarten
- Ecosia 144
- Ehrennadel 192
- Einwohnermelderegister 166
- Eisenmann, Susanne 22
- Element 66, 134
- ELENA 21, 180f.
- Eltern 19, 23ff., 55, 57, 65
- Emnid-Institut 166
- Entropia e.V. 194
- Entwickler:innen 135, 139
- ePrivacy 13
- Ermächtigungsgesetz 159
- Erwachsenenbildung 58
- Eschbach, Andreas 161
- Etar 136
- Etherpad 120f., 128
- EU-Kommission 40, 47f., 75ff., 145
- EU-Parlament 16, 40, 78, 107, 194
- EU-Verordnung 77
- EU 9, 11, 13, 16, 40f., 46f., 71, 74ff., 113f., 99, 105ff., 139, 144, 146ff., 176, 178, 184ff., 190, 194
- Europäische Bürger:innen-initiative (EBI) 47
- Europäische Datenschutzgrundverordnung 147
- Europäischer Gerichtshof (EUGH) 32, 111
- Europäischer Suchindex 11, 150, 184
- Europäisches Datenschutzrecht 105
- Evangelische Telefonseelsorge 179
- Ex-Jugoslawien 154, 170f., 193
- Exodus 135, 138
- F-Droid-Store 132, 139
- Facebook 8, 40, 43, 45, 62, 99, 100ff., 105, 111, 113f., 122, 130ff., 181, 185, 187f.
- Fahrzeugidentifikationsnummer 76
- FairEmail 134
- Falschussagen 133
- Farbkopierer 173
- FDP 33, 77, 179, 183
- Federal Trade Commission (FTC) 106
- Federated Learning of Cohorts 102
- Fedilab 134
- Fediverse 14, 130ff.
- Feeder 134
- Fennec-F-Droid 134
- Fernuni Hagen 87
- Filterblase 142
- Financial Times 177
- Fingerabdruck 49ff.
- FISA Act 147
- Fischer, Claudia 28, 31, 45, 54, 62, 72, 78, 87, 95, 107, 114
- FitoTrack 136
- Five Eyes 182
- FLoC 102
- Flugdaten 144
- FoeBuD 18, 64, 68, 152, 167f., 172, 178, 184, 192f.
- Fördermitglieder 68, 116, 175
- Forecastie 137
- Formulare 119
- Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FiFF) 167
- Fragebögen 38, 74, 128
- Frankreich 105, 109, 113f., 172
- Frauenhäuser 58
- Free Software. -> Freie Software
- Freedom not Fear 16, 157, 179, 186, 194
- Freibäder 54f.
- Freie Lizenz 128
- Freie Meinungsäußerung 45
- Freie Software 12f., 18, 26f., 57, 123, 127, 130, 134, 136
- Freier Markt 103
- Freiheit 14, 32, 62, 119, 123, 149, 164, 179, 190
- Friedrich, Hans-Peter 74
- Friendica 131
- Fritter 134
- Funkchips 30, 177
- Funktionalität 139
- Funkwhale 132
- Fusionskontrolle 41
- G8-Gipfel 74
- Gadgetbridge 137
- Gajim 123
- Gaming 67, 142
- Gastronomie 54
- Geflüchtete 47
- Geheimdienst 13, 44, 74, 103, 107, 119, 147, 170, 176, 182f.
- Gehirn 146
- Geld 30, 43, 51, 62, 101, 107, 133, 171, 175f., 185, 187
- Geldwäsche 12
- Geltendes Recht 139
- Gemeinwohl 146, 164
- Generalverdacht 46, 50
- Genossenschaft 148
- Geschäftsbedingungen 110, 139
- Geschäftsmodell 45
- Gesellschaft für Freiheitsrechte 87
- Gesichtserkennung 9, 12, 46, 48, 61, 81
- Gesundheit 79, 108, 160
- Gesundheitsämter 93, 96
- Gesundheitsdaten 110, 113f., 144
- Gesundheitsfachkräfte 108f., 116
- Gesundheitskarte 64, 173
- Gesundheitsministerium 109
- Gewerkschaften 179
- Girokonto 31
- Gläserner Bürger 163
- Globale Umweltveränderungen 148
- Globales Dorf 153
- GNU-Social 132
- Google Chrome 80
- Google Forms 124, 128
- Google Maps 140
- Google 5f., 8, 10, 18f., 40, 43, 45, 101ff., 111, 113, 121, 124f., 134f., 137ff., 142ff., 149f., 176, 181, 184f., 187f.
- Gössner, Rolf 71ff., 177
- GoToMeeting 122
- GPSTest 137
- Graphhopper 140
- Gratis 29, 100, 171, 189
- Gravenreuth, Günter Freiherr von 153
- Greentooth 135
- Greenwald, Glenn 182
- Greenwashing 45
- Großbritannien 172, 182
- Große Koalition -> Bundesregierung
- Großkonzern 24
- Grundrechte 11, 13f., 24, 28, 33, 46f., 51, 56, 58, 73, 80, 146, 163ff., 185, 193
- Grüne (Partei). -> Die Grünen
- Gulaschprogrammierung 194
- Gutachten 87, 114ff., 148, 179
- Hacker 167, 172, 194

- HackerNews 132
 Haecksen 53, 167, 194
 Hamburg 61
 Handyüberwachung 173
 Harms, Monika 74
 Hass 29, 44
 Hassnachrichten 133
 Hassrede 131
 Hatespeech 58
 Header Bidding 105
 Hechelei 194
 heise.de 172
 Hessen 61, 74, 165
 Hitler, Adolf 160f.
 Hochschulen 81, 83ff.
 Hokuspokus 87
 Hollerith, Hermann 160
 Holocaust 160f.
 Homeoffice 6f., 57, 119, 127
 Hosting 24
 Hubzilla 131
 IBM 66, 160f.
 Impftermine 108f.
 Impfbzentren 115
 Implantat 146
 Index
 Informationelle Selbstbestimmung 131, 139, 163f.
 Infrastruktur 145, 149f.
 Innovation 11, 144, 147, 150, 165
 Insiderhandel 104
 Instagram 111, 130ff., 188
 Instanz 16, 20, 120f., 129, 131ff.
 Institut für Technik und Journalismus (ITU) e. V. 114
 Integrität der privaten Geräte 80, 85
 Internetbrowser -> Browser
 Internetkonzerne 11, 187
 Internetmonopole 11, 40
 Inventur 159, 166
 Investitionen 148f.
 iOS 123, 138, 140
 IP-Adresse 36, 92, 121, 139
 iRights e. V. 114
 Israel 157, 162
 IT-Konzerne 113
 Jesus 162
 Jitsi Meet 121
 Journalist.innen 101
 Jude 159
 Jugendämter 37
 Jugendliche 35, 37
 Jugoslawien -> Ex-Jugoslawien
 K-9-Mail 134
 Kalender 119, 136
 Kalifornien 105, 155, 186
 Kalter Krieg 170
 Kameras 46, 55, 60, 70, 82, 84, 134
 Kanada 182
 Kanban 119, 129
 Kanzlerkandidatsmachtkampf 94
 Kapitalismus 170
 Karlsruhe Institute of Technology 140
 Karlsruhe 29, 32f., 140, 163, 179, 181, 194
 Kartell 104
 Kartenzahlung 30
 Katastrophen 93
 KeePassDX 135
 Khan, Lina 106
 KI 79, 81f., 86, 103
 Kids digital genial 24, 192
 Kinder 12
 Kindergärten 37
 Kinderschutz 34, 37
 KISS launcher 137
 Kitas 55
 Kleine Wettervorschau Deutschland 137
 Klimawandel 12, 76
 Koalitionsverhandlungen 10, 23, 34
 Koalitionsvertrag 11
 Komitee für Grundrechte und Demokratie 167
 Kommunikation 18, 45, 48, 90, 123, 130, 134, 152, 182
 Konsum 19
 Kontextabhängige Werbung 44
 Kontrolle 33, 50, 80f., 86, 89, 131, 136, 139, 158, 160, 167
 Konzernmacht 107
 Korruption 94
 Kosovo 171
 Kraftfahrzeug-Bundesamt 77
 Kreditinstitut 30
 Kreditkarten 30
 Krieg 74, 159, 166, 170
 Kryptowährungen 12
 Kuketz, Mike 87
 Kundenkarte 176
 Künstliche Intelligenz -> KI
 kurz&smündig 7, 21, 56ff.
 KZ 160, 161
 Landesdatenschutzbeauftragte 153
 Lauschangriff 173
 Lebenswerk 74, 173f., 177
 Lehrkräfte 12, 23f., 26, 57
 Leipzig 63, 170
 Lemmy 132
 Lesen gegen Überwachung 19
 Lexica 136
 Leyen, Ursula von der 74
 LibreOffice 121, 128, 137
 Lidl 175
 LifeSize 122
 LinkedIn 111
 Linsengericht 190
 Linux 17, 127, 137, 192
 Ljubljana 171
 Lobbyarbeit 19, 40, 160
 Lobbycontrol 40, 106
 Lobbyismus 29, 44, 103, 106, 185
 Lobbyregister 49
 Lock-in-Effekt 131
 Lockdown 79, 89, 92, 96
 Luca-App 38, 54, 92
 Lynn, Barry 188
 Machado, Antonio 52
 Macher, Konstantin 9f., 32, 46f., 50
 Macht 8, 10, 29, 40, 106, 130, 142, 145, 158f., 162, 170f., 181, 187, 190
 Magie 153
 Mailadressen 121
 Mailboxen 45, 68, 168ff., 153, 193
 Mandantentrennung 112f.
 Mandelbrotmenge 168
 Manipulation 11, 43f., 98, 100, 106, 146ff., 173, 181, 188
 Marble 141
 Markdown 128
 Marktortprinzip 139, 147, 186
 Mastodon 16, 78, 87, 95, 107, 114, 130ff., 134
 Material Files 137
 Matthäus-Evangelium 162
 Maus 84
 Mautkameras 173
 Medien 101, 103
 Medienpädagogik 12, 56
 Medium 111
 Meinungsfreiheit 146, 148
 Meinungsumfragen 111
 Meldepflicht 160
 Menschenrechte. -> Bürgerrechte
 Menschenwürde 96, 163
 Merkel, Angela 183
 Messenger 45, 143, 184
 MetaGer 144
 Metro AG 177f.
 Microsoft 22f., 76, 119, 122, 125, 174
 Microtargeting 44
 Mindustry 136
 Minesweeper-Antimine 136
 Minetest 136
 MLEx 104
 Mobilfunkmodul 76
 Mobilizon 131
 mobilischer.de 114
 Mobiltelefon 144, 183
 Modem 168
 Monal 123
 Monopol 43, 103, 143, 145, 148, 181, 184, 187
 Moodle 24
 Motherboard 52
 Motordaten 75f.
 Mumble 123
 München 20f., 79, 85
 Mundschutz 94
 MuPDF-Viewer 136
 Museen 55
 Musterbriefe 115
 Mustermann, Erika 166
 Nationales Sicherheitsamt 161
 Nationalsozialismus 158, 162
 NATO 50, 107
 Nazis 155, 159ff.
 NetGuard 135
 Netikette 169
 Netzphilosophie 56
 Netzwerk Datenschutzexpertise 71, 108, 114, 116
 Netzwerk Freie Schulsoftware 7, 19, 26
 Netzwerk Recherche 45
 Netzwerkeffekt 130
 Neue Medien 154
 Neumann, Linus 89
 Neunzig, Andrea 40, 54
 Neuseeland 182
 New York Times 106
 NewPipe 134
 Nextcloud 119ff., 124f.
 NFC-Funkchip 30
 Nichts zu verbergen? 58
 Nida-Rümelin, Julian 88, 90, 92, 95f.
 Niedersachsen 74
 Nordrhein-Westfalen -> NRW
 Notepad 136
 NRW 33f., 61, 192
 NSA 74, 161, 182
 nuudel 7, 19, 49, 124, 128
 Offene Schnittstelle 130
 Offene Software 143
 Öffi 135
 On-Board Fuel Consumption Meter (OBF-CM) 75ff.
 Onion Router 15
 OnionShare 125

- Online-Banking 87, 137
 Online-Werbung 107
 OnlyOffice 121
 Open Source Routing Machine (OSRM) 140
 Open Source 13, 23, 119, 121
 OpenBoard 137
 OpenCamera 134
 OpenFoodFacts 136
 OpenKeyChain 134f.
 OpenRouteService 140
 OpenScale 136
 OpenSchufa 31
 OpenStreetMap 53, 135, 140f.
 OpenSudoku 136
 OpenTasks 136
 OpenWeatherMap.org 137
 Opt-Out 78
 Orbot 137
 Ordnungswidrigkeiten 59, 61
 Organic Maps 135
 Ortsgruppen 16, 17, 20
 Orwell, George 162
 OsmAnd 135, 140, 141
 Owncloud 125
 Oxfam 187
 P-Adressbereich 127
 padeluan 2f., 5, 8, 33, 68, 71f., 78, 88, 90, 93ff., 156, 158, 167f., 175, 192f.
 Pads 119ff., 128
 Page, Larry 146
 Pandemie 63, 67, 79f., 83ff., 88, 93, 95f., 109, 173, 192
 Passwort 50, 87, 129, 169
 Patient:innen 108ff., 113ff.
 Paxton, Ken 104
 Payback 175, 177
 Paywall 106, 144
 PeerTube 7, 20, 132, 134
 Pegasus 33
 Per Anhalter durch die Galaxis 103, 154
 Periodical 136
 Personalausweis 21, 49ff.
 Personalisierte Werbung 11, 41f., 44, 48, 99, 101, 106f.
 Personenkennziffer 160
 Personenziehbare Daten 92
 Persönlichkeitsrechte 165, 185
 PGP (Pretty Good Privacy) 45, 184
 Pharmakonzerne 28
 Phelan, Oona 154
 Phyphox 137
 PIN 30
 Piraten 179
 Pixel Wheels 136
 Pixelfeld 132
 Plattformeffekt 130
 Plattformfreie Videos 20
 Pleroma 132
 Plik 125
 Plug-ins 100
 Podcast 8, 21, 65f., 89, 134
 Poitras, Laura 182
 Politik 8, 11f., 14, 21f., 47, 68, 72ff., 103, 107, 142, 150, 158, 168, 172
 Politiker:innen 16, 72, 145, 157, 173f., 179, 181
 Polizei 33ff., 37, 46, 59, 61
 Polizeiaufgabengesetz (PAG) Bayern. -> Polizeigesetze
 Polizeideaten 74
 Polizeigesetze 15, 33, 74
 Populismus 95
 Post AG 175
 Post-It 125
 Powerpoint 128
 PR-Agenturen 29, 103
 Praktikant:innen 8, 142
 Präsentationen 20, 121
 Presseausweis 94
 Pristina 171
 Privacy by Default 169
 Privacy by Design 169
 Privacy Captcha 126
 PrivacyDongle 193
 Privatsphäre 11, 13ff., 19, 24, 45, 58, 62, 86, 118, 123, 128, 130f., 135, 137f., 173, 177, 192
 Proctorio GmbH 79, 85f.
 Profile 44, 145
 Profilerstellung 42
 Project Bernanke 105
 Projektplanung 129
 proprietäre Software 143
 Provider 18, 171
 Prüfungssoftware 79
 Pseudo-gratis 42, 148
 Psychologie 98, 103
 Psychotherapeuten 31
 Public Domains 6f., 18, 68, 152, 155, 168
 Public Intellectual 88
 Putin, Wladimir 92
 Puzzles 136
 Pysolfc 136
 Quarantäne 89
 Quellcode 138
 Quelloffene Software 20, 127f., 138
 Querdenker:innen 95
 Quick-Freeze 36
 QuickDic 136
 Rabattkarten 173
 Rabbit Escape 136
 Racial Profiling 74
 Radi 155f.
 RadioDroid 135
 Rahmenbau 171
 Ramstein 74
 Ranking 146
 Rassismus 46, 158
 Rat der Europäischen Union 40
 rC3 -> Chaos Computer Congress
 re:publica 194
 Real-Time-Bidding 100, 103, 107
 Recherche und Pressearbeit 14
 Rechtsextremismus 36
 Rechtskritik 56
 Rechtsstaat 158
 ReclaimYourFace 46ff.
 Reddit 132, 134
 Redefreiheit 131
 Reding, Viviane 185
 RedReader 134
 Registrierungszwang 139
 Reimerdes, Jens 52f., 200
 Reisefahrpläne 144
 Reisen 13, 67
 Reisepass 51
 Reporter ohne Grenzen 45
 Repository 139
 Reproduzierbare Software 138
 Reul, Herbert 34
 RFID 152, 177f., 193
 Rheinberg 177f.
 Rheinland-Pfalz 74
 RKI (Robert-Koch-Institut) 93
 Rosengart, Frank 71, 75, 77f.
 Rosengart, Frank 75
 Roth, Karl Heinz 160f.
 Russland 143, 146ff.
 Sachbücher 19
 Sachsen-Anhalt 61
 Safer-Internet-Day 194
 Sarajevo 170f.
 Schadsoftware 137f.
 Schäuble, Wolfgang 51, 72, 74
 Scheuer, Andreas 78
 Schilken, Nick 142
 Schily, Otto 72, 74, 177
 Schmidt, Eric 146
 Schopper, Theresa 22f.
 Schrems, Max 99
 Schufa 31, 64
 Schule 12, 19, 22ff., 37, 54, 57, 92, 158
 Schulzki-Haddouti, Christiane 172
 Schünemann, Uwe 73f.
 Schwab, Andreas 40
 Schwahlen, Katrin 56
 Schweigepflicht 110, 112, 116
 Science Fiction 19, 161
 Scoring 31, 103, 173
 Scrambled Exif 135
 ScreenStream 137
 Selbstbestimmung 49, 90, 130, 164
 Selbstverteidigung 14f., 17, 20, 29, 63, 118, 126, 194
 SEO-Spam 147
 Serverplatz 24
 Seuchenschutzgesetz 93
 Sexualisierte Gewalt 34
 Shattered Pixel Dungeon 136
 Shelter 135
 Shop 8, 12, 17, 24f., 51, 59, 66, 73, 118, 127, 187, 192, 194
 Sicherheit 13, 17, 47, 50f., 57f., 70, 94, 108, 110, 118, 127, 129, 135, 137, 190, 194
 Sicherheitslücken 13, 33
 Signal 123
 Silicon Valley 96, 105
 Simitis, Spiros 165
 Simon, Leena 25, 54, 78
 Simple Gallery Pro 135
 Simple Solitaire Collection 136
 Skype 122
 Slovenien 171
 Smart City 15
 Smartphones 17, 28, 55, 61, 118, 121f., 132, 136f., 140, 184, 188
 SMS 115
 Snowden, Edward 16, 182
 Social Media 49, 58, 74, 111, 130ff.
 Social Score in China. -> Scoring
 Social-News-Aggregator 132
 Software-Alternativen 26
 Software 12f., 18ff., 23, 24, 26f., 42, 45, 55, 57f., 79, 80ff., 84ff., 96, 119, 123, 127ff., 134, 136, 138, 143f., 169, 171, 174, 192
 Soundcloud 132f.
 Souveränität 148f.
 Sowjetunion 162, 170
 Soziale Netzwerke 95
 Soziale Medien 48, 85
 Soziologie 142
 Spahn, Jens 92
 SPD 11, 183

- Spenden 148, 175
 Spiegel Online 31, 100
 Spiekermann, Sarah 146
 Sponsoring 8, 175
 Sportfans 47
 Staatliche Überwachung 45, 49, 177
 Staatliches Hacking.
 -> Staatstrojaner
 Staatsanwaltschaft 34, 116
 Staatstrojaner 12, 20,
 32f., 178
 Staatsversagen 94
 Stalins Sowjetunion 162
 Stalking 58
 Standortdaten 30
 Starostik, Meinhard 179f.
 Startpage 143f.
 Stasi 162
 Statistik 93, 155, 159
 Steuer-ID 173
 Stiftung bridge 193
 Stop-RFID 152
 Straftaten 61
 Streitkultur 158
 Stromnetze 149
 Stromverbrauch 12
 Studierende 47, 79ff.
 Suchindex 11, 142ff., 147ff.
 Suchmaschinen 142f.,
 150, 184
 Süddeutsche Zeitung 97
 Südkorea 88f.
 Südkreuz 46
 Supermarkt 30, 177f.
 SuperTuxKart 136
 SWR (Südwestrundfunk) 89
 Tabellenkalkulation 120f.,
 128, 155
 Tacklingfreie Instanz 20
 Taliban 50
 Talkshow-Mythos 89
 Tangens, Rena 8, 28, 40,
 45, 67, 71f., 78, 97f.,
 102, 105, 107, 154, 157f.,
 167f., 170, 172, 175, 190,
 192f.
 Targeting 43
 Tastaturen 30
 taz 193
 Tchibo 176
 Teibmann, Lars 21
 Telefonkonferenzen 122f.
 Telefonverbindungsdaten 178
 Telefonwarteschleife 108
 Telekonsultation 109
 Telematik 77
 Telemetrie 76
 Terminbuchung 55
 Terminumfrage 124, 128
 Termux 137
 Terroristen.innen 177
 Texas 103, 104
 Texteditor 120, 128
 The Guardian 106, 182
 Think Tanks 103
 Third-Party-Cookies 101f.
 Thunderbird 125
 Thüringen 74
 Tianmen-Massaker 146
 TikTok 130
 Timelines 142
 Toilettenpause 84
 Tor (Netzwerk) 7, 15, 49,
 125, 127, 129, 137
 Totalitarismus 158
 Tracking 8, 11, 42, 44,
 97ff., 101f., 106, 111,
 124f., 136, 138, 141
 trackingfreedads.eu 99, 101
 Transistor 135
 Transporter 135
 Trolle 95
 Tröts 131
 Turo 136
 TÜV 76
 Twidere 132, 134
 Twire 134
 Twitter 14, 16, 23, 78, 87,
 95, 107, 111, 114, 130ff.
 Übersichtsaufnahmen 61
 Überwachung 12, 14, 16,
 19, 33, 34, 42f., 45f., 49,
 83, 118, 142, 158, 162,
 172f., 177, 179, 182f.,
 189, 194
 Überwachungsgesamtrech-
 nung 17
 Überwachungsgesetze 72,
 74, 157, 177
 Überwachungskapitalis-
 mus 10, 29, 43, 103, 142,
 157, 177, 187f., 190
 Überwachungsstaat 163
 uMap 141
 Umfragen 6f., 19f., 119f.,
 124, 128, 166
 Umweltzerstörung 166
 Uni 54, 63
 Unicorns 113
 Universität Heidelberg 140
 Universum 90, 133, 154
 Unix 127, 156
 unteilbar 14, 46f., 158
 UntrackMe 135
 USA 84f., 103, 105f., 112,
 122, 143, 147f., 178, 182
 Vanilla Music 135
 VeraCrypt 126f.
 Verbindungsdaten 13
 Verbraucherschutz 28f.,
 41, 173, 192
 Verbraucherschutzver-
 ein 176
 Verbrechen 158
 Verbrechenbekämp-
 fung 34
 Verdeckte Ermittlerin-
 nen 61
 Verfassungsbeschwer-
 den 21, 32f., 73, 163,
 178ff.
 Verfassungsschutz 13,
 45, 72ff.
 Verhaltensprognosen 44
 Versammlungsfreiheit 21,
 58, 60, 165
 Versammlungsgesetz 33
 Verschlüsselung 13, 18, 20,
 45, 119f., 123, 126, 129,
 134, 169
 Verschwörungsheni 91
 Versicherungen 28, 54,
 77, 103
 Vertraulichkeit 108, 113,
 123
 Vestager, Margrethe 149,
 187f.
 Videoanalyse. -> Gesichts-
 erkennung
 Videokamera 81
 Videokonferenzen 7, 57,
 63, 119, 121, 123, 194
 Videoplattform 7, 134
 Videosparchstunden 110
 Videoüberwachung 16, 33,
 59f., 85
 VLC 135
 Voice 135, 153
 Volkszählung 38, 49,
 159ff., 166, 179, 194
 Volkszählungsboykott 163,
 166
 Volkszählungsurteil 163,ff.
 Vorratsdatenspeiche-
 rung 13, 16, 21, 29, 32,
 34ff., 73, 173, 178ff.
 VPN (Virtual Private Net-
 work) 49, 127, 135
 vzbv (Verbraucherzentrale
 Bundesverband) 28
 Waffensysteme 13
 Wahrheitskorrektur 155
 Währungsspekulationen 12
 Washington Post 84, 168
 Watson, Thomas J. 160
 Wawrzyniak, Jessica 22,
 25, 27, 192
 WBGU (Wissenschaftlicher
 Beirat der Bundes-
 regierung Globale Um-
 weltveränderungen) 148,
 150, 184
 WDR (Westdeutscher
 Rundfunk) 173
 Web Opac 136
 Web-Crawler 144
 Webdesign 98
 WebEx 122
 Wedde, Peter 71, 79, 83, 87
 Weichert, Thilo 71, 108,
 114f.
 Weihnachtsgeschichte 162
 Werbeeinnahmen 8, 11,
 133
 Werbeplattform Out-
 brain 114
 Werbetacking 42
 Werbewirtschaft 42, 100,
 103, 119
 Werbung 11, 41, 42ff., 48,
 99ff., 111, 133f., 169
 WeTransfer 125
 Wettbewerb 147, 149
 Wettbewerbsmanipulati-
 on 105
 Wettbewerbsrecht 11, 187
 WhatsApp 62, 123f.
 Whistleblower 103, 182
 Whiteboard 120, 129
 Wiedervereinigung 170
 WiFi Automatic 135
 Wifi 55
 WiFiAnalyzer 137
 Will, Anne 89
 Willkür 158, 162
 Windows 10 76
 Wirtschaft 10, 12f., 40ff.,
 64, 142, 149, 185
 Witte, Julia 10, 54, 64, 114
 Wohnung 162
 Wolfenstein 155
 World Wide Web 171
 XMPP 123, 134
 XWiki 128
 YaCi 144
 Yandex 143f., 146
 YouTube 20, 111, 132,ff.
 Z-Netz 170
 Zagreb 171
 Zahlen
 Zamir Transnational Net-
 work 154, 170f.
 ZaMir 193
 Zap 131
 Zapp 135
 Zeit Online 100, 174
 zensus 38, 194
 Zerberus-MailBox 45,
 169, 171
 Zimmermann, Phil 184
 Ziviler Ungehorsam 163
 Zivilgesellschaft 45, 58,
 166
 Zoom 121
 Zoos 55
 Zuboff, Shoshana 43,
 103, 187

