padeluun und Rena Tangens (Hrsg.)

digitalcourage

für das Jahr 2019

Verlag Art d'Ameublement

Foto: Alexander Altman, cc by-sa 4.0

padeluun und Rena Tangens (Hrsg.)

digitalcourage

für das Jahr 2019

Bibliographische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detailliertere bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar

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

Bitte geben Sie bei Namensnennung (by) immer den Namen des Autors oder der Autorin eines Textes mit dem Hinweis „aus dem Buch Digitalcourage für das Jahr 2019“ 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: dpa (Deutsche Presseagentur)
Vorne unten: cc by-sa 4.0 Tom Kohler
Hinten: cc by-sa 4.0 Lisa Krammel

Digitalcourage wird teilweise von der Stiftung bridge unterstützt

Impressum:
(cc by-sa 4.0) 2017 Verlag Art d‘Ameublement
Digitalcourage e.V., Marktstraße 18, 33602 Bielefeld
Hrsg.: padeluun und Rena Tangens
Redaktionelle Zusammenstellung: Claudia Fischer (verstandenwerden.de)
Layout und Design: Isabel Wienold (iwi-design.de)
ISBN 978-3-934636-19-4

Verlag Art d‘Ameublement

Inhalt

„Einer muss ja schließlich damit anfangen!“

Foto: Fabian Kurz, cc by-sa 4.0

Im Jahr 1986 haben wir, Rena Tangens und padeluun, einen ganz besonderen Kalender gestaltet. Anders als bei den üblichen großen Wandplanern liegen hier die Wochentage alle auf einer Linie, und das ist auch aus größerer Entfernung deutlich übersichtlicher. Schon immer gab es jedes Jahr einen Spruch auf dem Kalender. Letztes Jahr, 2018, lautete der Satz „Es wird die Zeit kommen, da ihr euch entscheiden müsst zwischen dem, was richtig ist, und dem, was bequem ist.“ Das sagte Hogwarts-Schulleiter Albus Dumbledore in „Harry Potter und der Feuerkelch“ (Band vier), denn er ahnt die kommenden Konflikte und es war ein Satz, der wie gemacht war für unsere Zeit.

Mit unserem Kalenderspruch für 2019 gehen wir einen Schritt weiter: „Einer muss ja doch mal schließlich damit anfangen!“ Das sagte Sophie Scholl von der Widerstandsgruppe „Weiße Rose“ am 22. Februar 1943 Roland Freisler direkt ins Gesicht – dem gefürchteten Präsidenten des sogenannten „Volksgerichtshofs“. Für ihre Opposition zur Politik Hitlers verurteilte dieser die Mitglieder der Weißen Rose zum Tode.

Soweit ist es in Deutschland heute noch nicht. Unsere Leben als Aktivistinnen und Aktivisten sind nicht gefährdet – aber wir benötigen dennoch Mut. Den Mut, uns nicht nur gegen Feinde, sondern auch hier und da gegen unsere Freundinnen und Freunde zu stellen. Rassismus zu begegnen, Gerüchte richtigzustellen, die sie im Netz aufgeschnappt haben und nun auf der Party erzählen. Wir dürfen nicht müde werden, ihnen immer wieder zuzurufen, dass sie kein Facebook, kein Google, kein WhatsApp, kein Instagram und wie diese NSA-Spionagetools alle heißen, nutzen sollen. Dass diese Anwendungen nur eins befördern: Rechtsruck, Hass, Streit, Neid und Lärm.

Wir brauchen Mut, wenn wir Ihnen sagen, dass Google-Docs nichts ist, wo man politische Ansichten speichern sollte, und dass in fast jeder Anwendung, die blauäugig programmiert wird, stets kostenloser Google-Code drinsteckt, der uns auf Schritt und Tritt verrät. Und wenn wir den Medien zurufen: „Steigt aus dem Bett raus, in dem Ihr mit Google, Facebook, Instagram und den Regierungen und Wirtschaftsbossen liegt!“

Wir bleiben mutig in dem Kampf zusammen mit unseren Freundinnen und Freunden (und manchmal scheinbar gegen sie), die glauben, dass es schon nicht so schlimm sei, die Werkzeuge und das Geld ‚der Teufel‘ zu nutzen, die unsere Welt zer-stören wollen. Denn irgendjemand muss ja schließlich damit anfangen und wir haben viel bessere Voraussetzungen als damals die ‚Weiße Rose‘. Denn wir haben bereits jetzt die Kraft der vielen Herzen – das sind unter anderem unsere Mitglieder, die uns unabhängig und stark machen. Sie ermöglichen uns unabhängige Recherche, unbequeme Meinungen und die Gelassenheit, Klageandrohungen zu trotzen und aufrecht zu bleiben.

Es klingt vielleicht abgedroschen – aber es ist genau das, was uns stark und unabhängig macht: Tausende von Menschen, die uns monatlich Geld zukommen lassen als Fördermitglieder von Digitalcourage. Sagen Sie DAS bitte weiter, werben Sie in Ihrem Bekanntenkreis weitere Fördermitglieder. Denn – verzeihen Sie die Zitatanleihe an dieser Stelle – jemand muss ja damit anfangen.

padeluun und Rena Tangens, Herbst 2018

Foto: Stefanie Loos, cc by-sa 4.0

Viel Aufmerksamkeit bei der Aktion gegen Gesichtserkennung am Bahnhof Südkreuz in Berlin, November 2017

Was uns bewegt

Unsere wichtigsten Aktionen und Kampagnen 2018/19

von Claudia Fischer und Kerstin Demuth

Als wir im Januar 2018 davon hörten, war uns schnell klar: Das geht gar nicht! Grundschulkinder in Wolfsburg und Ludwigsburg sollten mit GPS-Wanzen ausgestattet werden, damit sie als bewegliche kleine Punkte auf Navigationsgerät-Displays im Auto sichtbar sind. Das ist auf so vielen Ebenen falsch, da müssen wir was tun! Wir reagierten mit unserer Kampagne gegen die „Schutzranzen“ (das ist der euphemistische Marketing-Begriff der Betreiber), die uns mehrere Monate beschäftigen sollte. Aber der Reihe nach:

Eigentlich waren wir Anfang Januar nämlich noch in ausklingender Feier-Laune von unserem **30. Geburtstag** im November 2017. Vor genau 30 Jahren haben Rena Tangens, padeluun und andere Netzpionier.innen den FoeBuD e.V. gegründet – so hieß Digitalcourage bis 2012. Zum Geburtstag haben wir unser erstes Jahrbuch veröffentlicht und im Stadttheater Bielefeld mit dem Stück „1984“ nach dem Buch von George Orwell und einem „Lesen gegen Überwachung“ einen langen Abend ausgiebig gefeiert. Pünktlich zur Jubiläumsfeier ging auch unsere **neue Website** online, die unsere Web-Zauberer von „Palasthotel“ für uns gestaltet haben. Die neue Website sieht nicht nur auf dem Computerbildschirm viel schicker aus, sondern ist auch auf mobilen Geräten vollständig benutzbar.

Ein anderes großes Geschenk haben uns unsere Unterstützerinnen und Unterstützer gemacht: Ende Dezember haben wir ein wichtiges Jahresziel erreicht und unser **zweitausendstes Fördermitglied** begrüßt. Über zweitausend Menschen unterstützen uns jetzt regelmäßig mit ihrem Geld. Das ist ein Riesenlob für unsere Arbeit und hat uns eine ordentliche Motivationsspritze für den Start ins neue Jahr gegeben.

Foto: Stefanie Loos, cc by-sa 4.0

Damit Protest auch wirken kann: Während draußen Kundgebungen und Demos laufen, werden im Presse-Zelt Medienanfragen bearbeitet, und Internetseiten, Blogs, Twitter etc. versorgt.

Foto: Katarzyna Mazur, cc by-sa 4.0

Schrödingers Vorratsdatenspeicherung: Speichern oder nicht speichern – das ist seit Sommer 2017 die Frage.

Verfassungsbeschwerde gegen Vorratsdatenspeicherung

Außerdem haben wir Ende 2017 erfahren, dass 2018 unsere Verfassungsbeschwerde gegen das deutsche Gesetz zur Vorratsdatenspeicherung behandelt werden soll. Auch das war ein Grund zum Feiern!

Eingereicht hatten wir diese Verfassungsbeschwerde bereits am 28. November 2016 (Az. 1 BvR 2683/16) und in all den Monaten, die wir auf eine Verhandlung warten, haben wir der Vorratsdatenspeicherung schon zwei Spitznamen gegeben: Erst nannten wir sie „Der Zombie unter den Überwachungsgesetzen“, weil es diverse Gerichtsurteile gibt, die unsere Auffassung bestätigen, dass sie europarechtswidrig, unverhältnismäßig und verfassungswidrig ist. Nach jedem dieser Urteile haben wir geglaubt, sie wäre endlich tot, aber es findet sich weder im Bundestag eine Mehrheit, die das Gesetz wieder abschafft, noch hören die Innen- und Justizminister der europäischen Mitgliedsstaaten auf, an einer europäischen Vorratsdatenspeicherung zu basteln. Die EU-Ratspräsidentenschaft lag 2017/18 bei Estland, Bulgarien und Österreich, und die hatten eine gemeinsame Agenda dazu verabredet. Wie ein Zombie wankt die Vorratsdatenspeicherung also weiter.

Und es geht noch absurder: In Deutschland ist sie seit Sommer 2017 sogar offiziell in Kraft, es gibt aber wegen der unklaren Rechtslage eine Entscheidung der Bundesnetzagentur, dass Provider, die unsere Kommunikationsdaten nicht speichern, straffrei bleiben. Daraufhin hat sie den neuen Spitznamen von uns bekommen: „Schrödingers Vorratsdatenspeiche-

Grafik: Dennis Blomeyer, cc by-sa 4.0

Machen Sie mit!
https://digitalcourage.de/staatstrojaner-stoppen

rung – unklar, ob tot oder lebendig“ (frei nach dem Gedankenexperiment „Schrödingers Katze“. Sollten Sie dieses Tier nicht kennen, finden sie die Erklärung dazu auf der Jahrbuch 19-Webseite, siehe unten).

Rechtsunsicherheit kann nicht die Lösung sein. Wir fordern: Das Gesetz zur anlasslosen Telefon- und Internetüberwachung muss weg! Aufhebungsgesetz jetzt!

Wir sind zuversichtlich: Unsere Verfassungsbeschwerde wird erfolgreich sein. Wann die mündliche Verhandlung beim Bundesverfassungsgericht stattfindet, wissen wir bei Redaktionsschluss dieses Jahrbuches noch nicht – aktuelle Updates gibt es auf unserer Website.

Ein wichtiger Weggefährte wird das leider nicht mehr erleben: Im Frühsommer 2018 ist unser Rechtsanwalt, Mitstreiter und Freund Meinhard Starostik verstorben. Einen Nachruf finden Sie auf Seite 25. Meinhards Tod war ein schwerer Schlag, nicht nur für die Arbeit an unseren Verfassungsbeschwerden. Meinhard war für uns nicht nur ein wichtiger Mitstreiter, sondern auch ein wunderbarer Freund. Wir werden seine Arbeit weiter führen.

Verfassungsbeschwerde gegen Staatstrojaner

Mit seiner Hilfe bei der Vorbereitung haben wir im Sommer 2018 noch eine zweite Verfassungsbeschwerde eingereicht: **Gegen die Staatstrojaner** in der Strafprozessordnung. Lesen Sie dazu unseren Artikel auf Seite 26.

Als Staatstrojaner bezeichnet man Schad-Programme, mit denen Polizei oder Geheimdienste in unsere Geräte (Computer, Smartphones etc.) eindringen können, um unsere Kommunikation zu überwachen, mitzulesen, was wir schreiben, unsere Adressbücher einzusehen oder uns sogar eigene Nachrichten unterzuschieben. Dazu benutzen sie Sicherheitslücken in IT-Systemen – Sicherheitslücken, die auch von Kriminellen genutzt werden können, solange sie offen sind. Anstatt bekannte Sicherheitslücken von Herstellern schließen zu lassen, will der Staat sie künftig also selbst nutzen. Das halten wir für verfassungswidrig!

Nicht jammern – klagen!

Unterstützen Sie unsere Verfassungsbeschwerden gegen Vorratsdatenspeicherung und Staatstrojaner!

https://digitalcourage.de/spende

2008 hat nämlich das Bundesverfassungsgericht im Urteil gegen Online-Durchsuchungen in NRW ein neues Grundrecht geschaffen: Das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ (auch kurz „IT-Grundrecht“ genannt). Einfacher ausgedrückt: Wir haben ein Recht darauf, unseren Geräten vertrauen zu können. Das geht nicht, solange die Regierung Sicherheitslücken als Einfallstor aufkauft, hortet und nutzt, statt sie den Herstellern zu melden.

Foto: Jan Bornemann, cc by-sa 4.0

Beim Chaos Congress 2017 haben wir für jedes neue Fördermitglied ein Buch „Qualityland“ oder ein Jahrbuch 2018 ausgelobt – mit Erfolg!
Jetzt sind wir 2000!

Gegen Staatstrojaner protestieren wir schon seit mehreren Jahren. In den vergangenen Monaten neu dazu gekommen: Wir haben ein Erklär-Video, welche Probleme sich hinter dem Staatstrojaner verbergen, mit freundlicher Genehmigung von privacyinternational.org auf Deutsch ins Netz gestellt. Wir haben eine Chronologie und eine Liste der geplanten Polizei- und Verfassungsschutzgesetze in allen Bundesländern für unsere Website recherchiert und Briefe geschrieben und natürlich kontinuierlich an der Verfassungsbeschwerde gearbeitet – alle dazugehörigen Links finden Sie über die Jahrbuch 19-Webseite (siehe unten).

Der Skandal um den „Schutzranzen“

Zu diesen langfristig geplanten und begleiteten Themen und Aktionen kommen immer wieder aktuelle Ereignisse – im Januar 2018 also war es die „Schutzranzen“-Aktion. Unter diesem scheinbar freundlichen, Eltern ansprechenden Begriff vertreibt die Firma Coodriver GPS-Tracker. Das Start-Up-Unternehmen wurde Anfang 2018 dabei von der Volkswagen AG, dem Sicherheitshelm-Hersteller Uvex und dem Automobilclub von Deutschland (AvD) unterstützt. Der Ranzenhersteller Scout hatte sich angeblich bereits aus dem Projekt zurück gezogen, wurde von Coodriver aber noch in der Werbung für die Aktion erwähnt.

Quelle: freerangekids.com

In Wolfsburg und Ludwigsburg sollten die kleinen Überwachungsgeräte in Grundschulen kostenlos an Kinder verteilt werden. Die Überwachungswanzen im Schultornister geben die Positionen der Kinder preis. Die GPS-Daten werden über eine „Cloud“ an Autofahrer übermittelt, die die entsprechende App installiert haben. Und damit nicht genug: Unsere Analysen ergaben, dass aus den Apps auch Daten an Facebook, Google, Amazon und andere große Datenkraken weitergegeben werden. Ursprünglich konnten auch Eltern damit auf einer digitalen Karte sehen, wo sich ihr Kind befindet, das wurde aber inzwischen abgestellt.

Wir meinen: Der ganze Ansatz dieses Projektes ist grundfalsch! Kinder müssen nicht an Überwachung gewöhnt, sondern zu selbstbewussten, starken Menschen erzogen werden! Nicht von den Kindern geht Gefahr im Straßenverkehr aus, sondern von den Fahrzeugen – Lesen Sie unsere Argumente auf Seite 28.

Unsere Kampagne war recht erfolgreich: Mehr als 4.500 Menschen unterzeichneten unseren offenen Brief an die beteiligten Unternehmen: „Kinder-Tracking Stoppen!“. Mehrere Datenschutzbeauftragte, Pädagogik- und Kinderhilfe-Verbände und andere offizielle Stellen schlossen sich unserer Kritik an. Die Stadt Wolfsburg und die Volkswagen AG distanzieren sich inzwischen von dem Projekt. Technische und datenschutzrechtliche Prüfungen wurden eingeleitet. Wir haben den „Schutzranzen“-Verantwortlichen also ziemlich erfolgreich Sand ins Getriebe gestreut. Zwischenzeitlich versuchte das Unternehmen sogar, juristisch gegen uns vorzugehen – allerdings erfolglos.

Aber das Ende ist nicht in Sicht: Die Firma Coodriver, der AvD und die Stadt Ludwigsburg machen weiter. Auch andere versuchen, ein Stück vom Kuchen abzubekommen: Unter anderem beobachten wir, wie die Autoindustrie, konkret die Porsche-Tochter PTV, beginnt, die Digitalisierung des Straßenverkehrs in Bund, Ländern und Kommunen nach ihren Bedürfnissen zu gestalten (Quellenangaben dazu stehen auf unserer Jahrbuch19-Webseite). Solche Versuche werden im Rahmen der „Smart City“- Entwicklungen (siehe Seite 60) demnächst häufiger auch an Schulen auftauchen. Die Angst von Eltern um ihre Kinder wird von Sicherheitstrollen und Geschäftemachern instrumentalisiert.

Grafik: Digitalcourage, cc by-sa 4.0

Kinder-Tracking ist keine Lösung für Gefahren im Straßenverkehr!

Es ist höchste Zeit, dass sich kritische Bürger.innen einmischen und ihren Vertreter.innen klar machen, dass sie sicheren, umweltfreundlichen und überwachungsfreien Verkehr wollen!

Bleiben Sie wachsam und suchen Sie das Gespräch mit anderen Eltern, wenn Ihre Kinder mit Überwachungstechnik ausgestattet werden sollen! Auch können Sie unseren offenen Brief gegen „Schutzranzen“ noch unterzeichnen.

Der Protest gegen den Überwachungs-Schulranzen hat die ersten Monate des Jahres 2018 sehr geprägt – parallel haben wir die BigBrotherAwards vorbereitet. In diesem Jahr erstmals im Bielefelder Stadttheater – ausführliche Berichte und alle Laudationes und Reaktionen finden Sie ab Seite 51 in diesem Jahrbuch.

Foto: Digitalcourage, cc by-sa 4.0

Friedemann Ebelt und Kerstin Demuth aus unserem Büro-Team verschickten Briefe an die beteiligten Kommunen und Unternehmen. Mit Erfolg: Das Projekt wurde gebremst – wenn auch noch nicht gestoppt. Sie können unseren offenen Brief noch unterzeichnen.

Neuer EU-Datenschutz Akt 1: Die DSGVO

Ende Mai 2018 kam die von uns lang ersehnte und mit vorbereitete europäische Datenschutzgrundverordnung (DSGVO), die den Datenschutz in ganz Europa auf eine einheitliche Basis stellt. Es gibt endlich mehr Transparenz und mehr Informationsrechte. Viele Firmen, Institutionen und Privatleute haben sich endlich damit beschäftigt, wie sie mit unseren Daten umgehen. Ja, das hat Arbeit gemacht, auch bei uns. Auch wir haben nun ein Teammitglied zum offiziellen Digitalcourage-Datenschutzbeauftragten fortgebildet.

Digitalcourage wirkt, wirken Sie mit!

https://digitalcourage.de/spende

Und ja, vielen kleinen Unternehmen, Vereinen, Bloggerinnen und Bloggern schien diese Aufgabe kaum leistbar. Halbwissen, das in den Sozialen Netzwerken zirkulierte, versetzte viele unnötigerweise in Panik. Dazu kamen Fehlinformationen und Gerüchte, die von interessierter Seite gestreut wurden, um Stimmung gegen Datenschutz ganz allgemein zu machen.

Wir halten einen einheitlichen europäischen Datenschutz für den richtigen Weg.

Bei einer Aktion haben wir uns sogar nackt und in Europa-Farben bemalt vor dem Bundesinnenministerium aufgebaut (siehe Titelfoto dieses Jahrbuches). Und auch international gibt es viele Stimmen, die Europa um dieses Gesetz beneiden.

Was die Datenschutzgrundverordnung neu regelt, hätte von den zuständigen Ministerien im Vorfeld in klare Informationen für Bürgerinnen und Bürger übersetzt werden müssen. Wenn das für Deutschland ausformuliert worden wäre, hätten alle sehen können, dass sich für uns im Vergleich zum alten Bundesdatenschutzgesetz gar nicht so viel ändert. Mit klaren Informationen hätte so mancher Flurschaden verhindert werden können. So hatte die DSGVO durch viel öffentliche Desinformation, Unsicherheit und Polemik in Medien und sozialen Netzwerken einen ruckeligen Start.

Das Wichtigste ist: Die Datenschutzgrundverordnung wirkt – Unternehmen, Vereine und Private haben ihre Datenverarbeitung verbessert, die Sanktionen für Datensünder wurden massiv erhöht, Datenschutz ist damit zur Chefsache geworden und Millionen Bürger.innen in der ganzen EU haben Rechte gewonnen. Es liegt an uns, sie auch auszuüben.

Wie Sie Ihre Rechte aus der DSGVO nutzen können, lesen Sie auf Seite 111. Ein Interview mit Jan Philipp Albrecht, der als Berichterstatter des Europäischen Parlaments den komplizierten Kompromiss zur DSGVO ausgehandelt hat, finden Sie auf Seite 30.

Erhältlich im Digitalcourage-Shop!
DVD „Democracy – Im Rausch der Daten“
Ein Dokumentarfilm von David Bernet

Der lange Weg zur europäischen Datenschutzgrundverordnung – „So spannend wie ein Polit-Thriller“ (FAZ)

Preis: 12,99 Euro

https://shop.digitalcourage.de

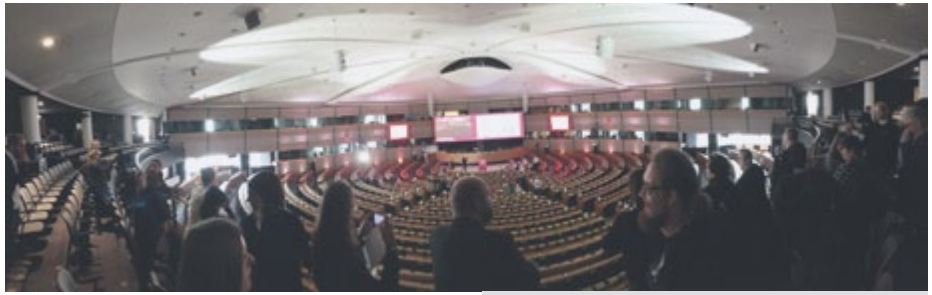


Foto: Claudia Fischer, cc by-sa 4.0

Gemeinsam mit gut 50 Aktivist.innen aus ganz Europa besuchten wir beim Arbeitstreffen „Freedom not Fear“ 2017 in Brüssel das Europäische Parlament

Neuer EU-Datenschutz Akt II: Die ePrivacy-Verordnung

Die EU-Datenschutzgrundverordnung steht also, aber die ePrivacy-Verordnung ist noch nicht verabschiedet. Und die wird über Jahrzehnte die Privatsphäre in der elektronischen Kommunikation regeln.

Wir haben zwar viel weniger Geld als die Lobby-Verbände und Unternehmen, die die Verordnung verschlechtern wollen – aber wir haben die besseren Argumente. In Deutschland setzen wir uns bei Verbändetreffen im zuständigen Ministerium dafür ein, dass die ePrivacy-Verordnung hält, was sie verspricht: Privacy.

An das Wirtschaftsministerium haben wir im Dezember 2017 einen Anti-Lobbybrief geschrieben, der die Mythen der Industrie richtig stellt (siehe Seite 35). Im März 2018 haben wir mit einer satirischen Aktion die Interessen der Tracking-Industrie entlarvt: Wir haben einen Brandbrief des Verbands der deutschen Zeitschriftenverleger (VDZ) in Klartext übersetzt und als „Verband für Datensammlung und Zweckentfremdung“ – ebenfalls VDZ – veröffentlicht.

Auf EU-Ebene haben wir uns gemeinsam mit anderen Organisationen an das Parlament gewendet, damit der Entwurf, über den die Nationalstaaten beraten, möglichst gut wird. Mit Erfolg! Der Entwurf der Kommission und die Überarbeitung des Parlaments sind vielversprechend. Aber noch ist nichts gewonnen: Einige Regierungen der Mitgliedsstaaten haben sich von der Lobby bezirzen lassen und fordern im EU-Rat, die Verordnung aufzuweichen.

Foto: Digitalcourage, cc by-sa 4.0

padeluun auf einer Demo gegen Upload-Filter in Berlin.

Wir bleiben weiter am Ball, damit Privatsphäre wichtiger bleibt als der Datenhunger einiger Unternehmen.

Überhaupt sind wir auf Europa-Ebene sehr gut vernetzt: Jedes Jahr im Herbst sind wir Mitveranstalter der Arbeitstagung europäischer Bürgerrechtsaktivisten unter dem Motto , wir setzen uns auf EU-Ebene gegen Upload-Filter ein und sind Teil der Kampagnen „Public Money, Public Code“ der Free Software Foundation Europe und der Initiative „Konzernmacht beschränken!“

▶Aktiv gegen neue Polizeigesetze

Und auch diese Bilder haben 2018 sehr geprägt: Tausende Bürgerinnen und Bürger protestierten laut und bunt gegen die neuen Verfassungsschutz- und Polizeigesetze landauf landab. Bei vielen Aktionen und Demos haben wir uns mit zahlreichen Organisationen zusammengetan und der Öffentlichkeit gezeigt: Wir lassen uns unser Rechte auf Privatsphäre, Meinungsäußerung und Freiheit nicht wegnehmen! Immer wieder tragen wir unseren Protest auf die Straße.

Allein in München waren zwischen 30.000 (Süddeutsche Zeitung) und 70.000 Menschen (Netzpolitik.org) auf der Straße

Jammern, resignieren und zynisch werden sind nicht die Lösung

Werden Sie Fördermitglied – gemeinsam können wir was bewegen!

▶ **https://digitalcourage.de/mitglied**

Foto: Fabian Kurz, cc by-sa 4.0

Der Gesetzentwurf von Grünen und CDU in Hessen ist „ein rechtsstaatswidriger Freibrief für kriminelles Handeln in staatlicher Mission“, sagt Dr. Rolf Gössner beim BigBrotherAward 2018.

gegen das bayerische Polizeiaufgabengesetz (PAG) – und unsere Digitalcourage Ortsgruppe München war natürlich mittendrin dabei. Staatstrojaner, Hausdurchsuchungen, willkürliche Ausweiskontrollen – die Liste der Maßnahmen, mit denen die Polizeigesetze unsere Freiheit einschränken, ist lang.

Unser BigBrotherAward 2018 an die Regierungskoalition in Hessen für ihre Verfassungsschutz- und Polizeigesetze-Reform hat dort zu einem internen Streit in der Grünen Fraktion und intensiven Diskussionen geführt (siehe Seite 85). Unsere Bremer Ortsgruppe hat geholfen, die dortigen Grünen zu überzeugen, den „Brementrojaner“ vorerst auf Eis zu legen, und

Foto: Aljoscha Pörtner, cc by-sa 4.0

Rund 1000 Menschen demonstrierten am 30.6.2018 gegen das NRW-Polizeigesetz in Bielefeld – landesweit waren es viele Tausend.

unser Bremer Mitglied Justus Holzberger hat für alle Aktiven in ganz Deutschland eine aktuelle Liste aller geplanten Maßnahmen, nach Bundesländern sortiert, auf unserer Website zusammen gestellt. Den Link finden Sie entweder über die Suche auf digitalcourage.de (Stichwort „Polizeigesetze“) oder direkt über die Jahrbuch19-Webseite (siehe unten). Mitte Oktober integrierten wir unsere Demonstration „Freiheit statt Angst - Stoppt die Polizeigesetze“ als großen Demoblock in die von uns mitorganisierte Grossdemonstration „#unteilbar“

Quelle: Twitter-Nutzer

Außerdem haben wir offene Briefe geschrieben, die Sie teilweise noch mitzeichnen können – schauen Sie auf unserer Webseite vorbei.

Wir haben den Protest insbesondere in Nordrhein-Westfalen intensiv begleitet und unterstützt. Wir waren bei Demos in Köln, Bielefeld, Hannover, Berlin und Düsseldorf präsent und haben andere Organisationen und spontane Bündnisse über unserem Shop mit entsprechenden Flyern, Plakaten und Infomaterial und struktureller Unterstützung versorgt.

▶Digitalcourage wächst

Von unserer Freude über unser 2.000stes Fördermitglied haben wir ja schon berichtet. Auch die Zahl der ehrenamtlich Aktiven ist stark gestiegen.

Unsere Arbeitsgruppe **„Digitale Selbstverteidigung“** hat sich im Sommer 2018 erstmals persönlich getroffen und gemeinsam ein Wochenende lang getestet, getüftelt und bewertet – bis dahin war das überwiegend eine Online-Zusammenar-

Foto: Fabian Kurz, cc by-sa 4.0

#Kids #Digital #Genial
– Das Lexikon von App bis .zip“

als Soft- und Hardcover (2,45 / 12 Euro)

▶ **https://shop.digitalcourage.de**

beit gewesen. Solche persönlichen Treffen sind enorm wertvoll für das Vertrauen unter unseren ehrenamtlichen Expert.innen. Viele Ideen wurden entwickelt, Haltungen und Organisationsfragen besprochen. Zukünftig soll so ein Treffen einmal im Jahr stattfinden. Dutzende Artikel wurden aktualisiert – einige davon finden Sie ab Seite 109, am aktuellsten natürlich immer auf unserer Website und eine Auswahl in unserem jährlichen Online-Adventskalender.

So etwas geht nur mit den vielen Menschen, die ihre Zeit spenden, um mit uns auf unser Ziel hinzuarbeiten: Eine lebenswerte Welt im digitalen Zeitalter.

Neu im Digitalcourage-Boot ist die **Arbeitsgruppe „Pädagogik“**: Sie sammelt Empfehlungen für Lehrende und Eltern, aber auch für Kinder und Jugendliche, um digitale Mündigkeit in allen Altersgruppen voranzubringen. Es gibt dafür extra zwei neue Fundstellen im Digitalcourage Blog: Die Rubrik „Kinder und Jugendliche“ und ein FAQ extra für Schulen. Jessica Wawrzyniak aus unserem Hauptamtlichen-Team hat außerdem ein gedrucktes Buch für Kinder und Jugendliche veröffentlicht und es gibt von ihr und ihrem Blog kidsdigitalgenial.de auch wieder Extra-Seiten für Kinder und ihre Eltern in diesem Jahrbuch ab Seite 130.

▶ Aus den Ortsgruppen

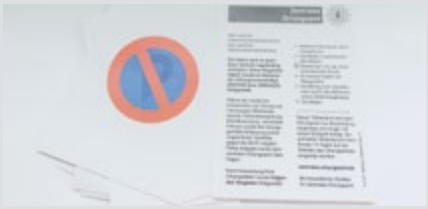
Ach ja: Eine neue Digitalcourage-Ortsgruppe haben wir auch! Im Herbst 2017 haben sich Aktivist.innen in **Köln und Umgebung** getroffen und werden mit uns im Rheinland für Freiheit kämpfen. Als Auftakt hat die Kölner Ortsgruppe direkt einen Aprilscherz „Knöllchen vom Zentralen Ortungsamt“ organisiert: Zum 1. April verteilten unsere Aktiven Fantasie-Strafzettel vom „Zentralen Ortungsamt“ wegen digitaler und vernetzter Anzeige- und Bediensysteme in Autos. (Diese „Knöllchen“ gibt‘s mit passendem Plastiktütchen in unserem Shop und sie können auch an jedem anderen Tag des Jahres verteilt werden.) Die OG Köln hat zudem die BigBrotherAwards 2018 gestreamt und die Mitglieder engagieren sich im Bündnis gegen das Polizeigesetz NRW.

Die **Ortsgruppe München** bietet Cryptocafés an, bei denen die Besucher.innen lernen, wie sie ihre Computer und Smartphones gegen Überwachung absichern. Im Sommer 2018 war bei einem Cryptocafé in München sogar der bayerische Verbraucherschutzminister dabei. Die Münchner Ortsgruppe beteiligt sich auch an Demos, sie starteten 2018 mit einer regelmäßigen Digitalcourage-Radiosendung bei Radio LORA in München und sind z.B. zu unserem 30jährigen Geburtstag mit Digitalcourage-Banner bergwandern gewesen (siehe Rückseite dieses Jahrbuchs).

Die Ortsgruppe Bremen hat es mit viel Energie und Aktion geschafft, den Brementrojaner - zumindest vorerst - zu verhindern. Wir sind stolz auf Euch!

Uli Fouquet und Petra Hagemann aus der Ortsgruppe **Braunschweig** haben sich ein eigenes Programmier-Projekt vorgenommen: Gefördert von der OpenKnowledge-Foundation und in Zusammenarbeit mit Digitalcourage-Mitglied Leena Simon, IT-Beraterin beim FRIEDA-Beratungszentrum für Frauen in Berlin, arbeiten sie an einem „StalkerBuster“. Geplant ist eine App, die den ein- und ausgehenden Datenverkehr eines Mobiltelefons analysiert und sichtbar macht, um Diagnosen und Gegenmaßnahmen zu ermöglichen.

Erhältlich im Digitalcourage-Shop!
Knöllchen vom „Zentralen Ortungsamt“:



z.B. beim Abweichen von der emissionsärmsten Route. 50 Knöllchen (DIN A 6, doppelseitig bedruckt + 50 Flachbeutel)
Preis: 3.00 Euro

▶ **https://shop.digitalcourage.de**

Foto: Justus Holzberger, cc by-sa 4.0

Freuen sich, weil der „Brementrojaner“ auf Eis gelegt wurde: Maike Schmidt-Grabia (Digitalcourage Ortsgruppe Bremen), Susanne Wendland (Mitglied der Bremischen Bürgerschaft), Aaron Frye (Forum Informatiker.innen für Frieden und gesellschaftliche Verantwortung, FIfF), Dr. Rolf Gössner (Internationale Liga für Menschenrechte und BigBrotherAward-Jury)

Von der **Ortsgruppe Berlin** gibt es zwar vorerst keine regelmäßigen Treffen mehr, aber es existiert eine Mailingliste, mit der sich schnell und spontan Aktionen organisieren lassen.

In **Bielefeld** ist unsere Digitalcourage-Hochschulgruppe im ganzen Stadtgebiet aktiv und bietet Cryptoparties, Linux-Install-Parties und Info-Veranstaltungen zur Digitalen Selbstverteidigung an.

Kommen Sie doch mal vor Ort bei uns vorbei und lernen Sie uns kennen!

Unser Team

Damit die ehrenamtliche Beteiligung leichter fällt, gibt es übrigens Unterstützung aus dem Digitalcourage-Büro: Seit Februar 2017 arbeitet Sarah Bollmann als Community-Organisatorin bei uns. Sie beantwortet Fragen, koordiniert, verschickt Einladungen für Veranstaltungen und hat immer ein offenes Ohr für alles, was Menschen brauchen, um mitzuarbeiten. Und sie ist die Stimme für die Ortsgruppen und Ehrenamtlichen im Büroteam, wenn wir im Arbeitsalltag Gefahr laufen, deren Bedürfnisse zu vergessen. Die Stiftung bridge hilft uns mit Finanzen, um die Stelle anzuschieben.

Unser Team besteht derzeit aus elf hauptamtlichen Mitarbeiter.innen in Bielefeld,

Foto: Jan Bornemann, cc by-sa 4.0

Sarah Bollmann sorgt für die Ehrenamtlichen und Ortsgruppen bei Digitalcourage.

einigen Honorarkräften, einem FSJ (freiwilliges soziales Jahr) und Praktikant.innen. Ganz maßgeblich hilft uns dabei Ihr Geld als Fördermitglied, Spenderin oder Spender.

Vielen herzlichen Dank an alle, die hinter uns stehen und uns unterstützen! Nur so können wir mit voller Kraft tagesaktuell handeln.

Auf digitalcourage.de finden Sie unsere Transparenzberichte, denen Sie Umsatz, Stellenplan etc. entnehmen können. Unser Transparenzbericht entspricht den Vorgaben der Initiative Transparente Zivilgesellschaft, der sich mehr als 500 Organisationen angeschlossen haben.

Bewerben Sie sich um ein Praktikum!

Wir suchen laufend Praktikant.innen, die Lust haben, eine freundliche politische Organisation wie Digitalcourage kennenzulernen. Wir bieten inhaltliche Arbeit, viele praktische Aufgaben, z.B. bei der Organisation von Großveranstaltungen oder bei der Websitepflege. Bitte nehmen Sie sich zwei bis drei Monate Zeit!

bewerbung@digitalcourage.de

Veranstaltungen und Infrastruktur für die Datenschutz-Bewegung

Bei all dem ist uns besonders wichtig, nicht alleine die Welt zu retten. Deshalb vernetzen wir uns und bieten selbst Vernetzungstreffen und -möglichkeiten an, arbeiten an Infrastruktur, die auch von anderen Bürgerrechtsgruppen genutzt werden kann, und setzen z.B. mit den

Foto: Jan Bornemann, cc by-sa 4.0

Auch eines unserer Infrastruktur-Projekte: Über unseren Shop stellen wir Materialien, Demo-Ausrüstung, Bücher und vieles mehr für die Bürgerrechtsbewegung zur Verfügung – teilweise sogar kostenlos.

BigBrotherAwards Themen, die die Diskussion um Datenschutz, Freiheits- und Grundrechte bis in überregionale Zeitungen, in Online-Nachrichten-Portale, in Lokalzeitungen oder in die Tagesschau bringen.

Für alle, die aktiv sind oder werden wollen und Know-How oder einen Motivationsschub brauchen, organisieren wir jährlich zum Anfang des Jahres den Aktivcongress: Datenschutz-Aktivist.innen aus unterschiedlichen Bereichen teilen dort ihr Wissen von Arbeitnehmerdatenschutz bis Zensus, planen gemeinsame Aktionen und lernen sich besser kennen. Viele Initiativen und Bündnisse (so zum Beispiel die erfolgreiche Verfassungsbeschwerde gegen ELENA, den Elektronischen Entgeltnachweis) haben auf Aktivcongressen ihren Anfang genommen.

Die Themen bringen die Teilnehmer.innen selbst zum Aktivcongress mit und stellen ihr Fachwissen oder ihre Erfahrungen den anderen zur Verfügung. Arbeitsgruppen sind länger verabredet oder bilden sich spontan. Diese Form des Austauschens nennt sich „Barcamp“ und braucht eine fachkundige Moderation. Mit uns macht das seit vielen Jahren sehr erfolgreich Wiebke Herding aus Amsterdam. Sie unterstützt uns sowohl beim Aktivcongress als auch beim europäischen Datenschutztreffen „Freedom not Fear“ in Brüssel, von dem wir oben schon berichtet haben. Besonders spannend an diesen Arbeitstagungen ist, dass wir sehr früh auf Strömungen und Entwicklungen aufmerksam werden, mit denen wir noch nichts zu tun hatten. So vom Fachwissen anderer zu profitieren, ist spannend und hilfreich für die weitere Arbeit.

Die Termine für 2019 für den Aktivcongress in Bielefeld und „Freedom not Fear“ in Brüssel finden Sie im Anhang dieses Jahrbuches, Seite 164

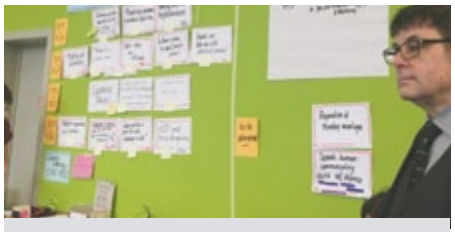


Foto: Claudia Fischer, cc by-sa 4.0

„Freedom not Fear“ in Brüssel ist ein jährliches „Barcamp“ dutzender Bürgerrechts-Aktivist.innen aus ganz Europa. Alle bringen Wissen ein, alle nehmen Wissen und gute Kontakte mit nach Hause.

Auch technische Infrastruktur stellen wir für alle, die sich für Demokratie und Grundrechte engagieren, zur Verfügung: Digitalcourage betreibt Tor-Exit-Nodes zum unbeobachteten Surfen, zensurfreie DNS-Server und offene Pads zum kooperativen Schreiben.

Foto: Digitalcourage, cc by-sa 4.0

2015 trafen wir in Brüssel den damaligen EU-Kommissar für Digitalwirtschaft, Günther Oettinger, und sprachen mit ihm über einen europäischen Suchindex. V.l.n.r.: padeluun, Rena Tangens, Günther Oettinger, Lars Tebelmann und Friedemann Ebelt (beide ebenfalls Digitalcourage)

Wir betreiben unseren eigenen Mailserver und auch die meisten anderen Dienste, die wir selber nutzen, laufen auf unseren eigenen Servern im Haus. Dafür arbeiten bei Digitalcourage zwei Admins. Das ist teurer, als die Plattformen von Datenkraken zu nutzen und unsere Daten irgendeiner Cloud anzuvertrauen. Aber wir wollen auch bei unserer eigenen Infrastruktur vorleben, wie das Netz aussehen sollte: dezentral, frei und datenschutzfreundlich.

▶Ausblick: Das wird uns 2019 bewegen

Im neuen Jahr werden wir unsere Verfassungsbeschwerden gegen Staatstrojaner und Vorratsdatenspeicherung weiter vorantreiben. Bei den Europawahlen im Mai 2019 wollen wir dafür sorgen, dass alle Kandidat.innen sich mit Freiheit und Privatsphäre auseinander setzen und dass die EU das Beste aus der ePrivacy-Verordnung herausholt. Anfang Juni verleihen wir die BigBrotherAwards – auch 2019 wieder im Stadttheater Bielefeld. Fest steht auch: Wir werden uns weiter mit Überwachungssensorik im öffentlichen Raum – Gesichtserkennung, WLAN-Tracking und anderem – auseinandersetzen. Wir werden auch weiter das Verscherbeln öffentlicher Infrastruktur und der Daten der Bürgerinnen und Bürger durch die sogenannte „Smart City“ kritisieren. Und das Konzept einer „datenschutzfreundlichen Stadt“ vorantreiben. Und weiter steht auf unserem ToDo-Zettel: Wettbewerbsrecht gegen Monopole der großen Plattformen im Netz nutzen, einen europäischen Suchindex auf den Weg bringen, um endlich wieder Wettbewerb bei Suchmaschinen zu ermöglichen, andere Geschäftsmodelle als „Nutzung pseudo-gratis gegen persönliche Daten“ fördern und coole Technik für einfachere Verschlüsselung voranbringen. Und das ist nur, was wir schon eingeplant haben ... auch unerwartete Ereignisse bekommen von uns 2019 mit Sicherheit die Aufmerksamkeit, die ihnen gebührt!

Wir trauern um Meinhard Starostik

Die Ohnmächtigen gegen die Mächtigen vertreten

Am 12. Juni 2018 verstarb Meinhard Starostik, Rechtsanwalt und Verfassungsrichter des Landes Berlin, nach schwerer Krankheit im Alter von 68 Jahren.

Unser Freund und Mitstreiter Meinhard Starostik hat sich bis zum letztem Atemzug für Grundrechte eingesetzt. Er war Verfassungsrichter des Landes Berlin und hat als Rechtsanwalt mehrere Verfassungsbeschwerden vor dem Bundesverfassungsgericht (z.B. 2010 und 2016 gegen die Vorratsdatenspeicherung, gegen die Bestandsdatenauskunft, gegen Videoüberwachung, gegen ELENA) vertreten. So hat er das erste Gesetz zur verdachtslosen Vorratsdatenspeicherung zu Fall gebracht. Er ist gegen die Protokollierung des Surfverhaltens anhand von IP-Adressen und gegen die Geheimhaltung gerichtlicher Schriftsätze bis vor den Europäischen Gerichtshof gezogen. Auch hat er sich für die Rechte von Sexarbeiterinnen eingesetzt und mit der Verwertungsgesellschaft C3S eine Alternative zur Gema aufgebaut. Jüngst gründete er die p≡p-Genossenschaft, die Werkzeuge für einfache Verschlüsselung unterstützen soll.

Foto: Tom Kohler, cc by-sa 4.0

2016 hat Meinhard Starostik unsere Verfassungsbeschwerde gegen die Vorratsdatenspeicherung eingereicht.

Meinhard Starostik sagte zu seiner Arbeit: *„Es ist eigentlich immer mein Thema gewesen, die Ohnmächtigen gegen die Mächtigen zu vertreten. Dass die technische Revolution des Internets, die ja unser aller Leben völlig umgestaltet, eben auch dazu führt, dass alte Überwachungswahnvorstellungen hochkommen und uns tatsächlich bedrohen in unserer Freiheit. Also ich sehe die größten Gefahren für die persönliche Freiheit darin, dass wir hinter unserem Rücken überwacht, ausspioniert und manipuliert werden können.“*

Meinhard Starostik hat sich um die Freiheitsrechte verdient gemacht. Durch seine freundliche, kompetente und stets hilfsbereite Art hat er sich allseits Respekt und Anerkennung erworben. Er wird der Bürgerrechtsbewegung sehr fehlen. Wir haben ihn als Freund auf seinem letzten Weg begleitet und am Totenbett versprochen, seine Arbeit weiter zu führen.

Wir haben Verfassungsbeschwerde gegen Staatstrojaner eingereicht

Am 7.8.2018 haben wir beim Bundesverfassungsgericht in Karlsruhe Verfassungsbeschwerde gegen Staatstrojaner eingereicht. Zu diesem Zeitpunkt hatten bereits über 10.000 Menschen unseren Unterstützungsaufruf unterzeichnet.

Was sind Staatstrojaner?

Die Große Koalition schlägt mit den Staatstrojanern gefährliche Sicherheitslücken in all unsere Smartphones und Computer. Der Plan: Jedes Gerät bekommt eine Hintertür, durch die staatliche Hacker und Kriminelle nach Lust und Laune einsteigen können. Kommunikation wird mitgehört, Verschlüsselung wird gebrochen, Daten werden gesammelt und Geräte, Netzwerke und ganze Clouds werden manipuliert. Das ist katastrophal für Zivilgesellschaft, Behörden und Unternehmen. Um die Schadsoftware zu installieren, werden Sicherheitslücken in Hard- und Software von Geräten ausgenutzt. Diese stehen dann weiterhin offen – auch für Geheimdienste und Kriminelle.

Wir wollen, dass das „Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens“ für verfassungswidrig und nichtig erklärt wird. Die Beschwerdeführenden sind Juristen, Grundrechtsaktivistinnen und Künstler. Alle sind potentiell durch den Einsatz von Staatstrojanern bedroht.

Der Liedermacher, Kabarettist und Autor, **Marc-Uwe Kling** (Känguru-Chroniken, Qualityland) ist einer der Beschwerdeführer und erklärt seine Betroffenheit von dem Gesetz mit seinen Publikationen: Die Känguru-Trilogie handelt ausführlich von seinem Zusammenleben in einer Wohngemeinschaft mit einem kommunistischen Känguru. Dieses hat nach eigener Aussage auf Seiten des Vietcong gekämpft, will das System umstürzen und betreibt einen Boxclub („Nazis boxen“). Auf Grund einiger absurder (realer) Erlebnisse anderer Beschwerdeführer mit der Polizei liegt die Befürchtung nahe, dass Strafverfolgungsbehörden das Känguru nicht als Romanfigur erkennen, sondern als Täter einer der in den §§ 100a Abs. 2, 100b Abs. 2 StPO genannten Anlasstaten einstufen und er Betroffener einer Online-Durchsuchung oder Quellen-Telekommunikationsüberwachung wird.

Trotz des bitteren Humors – Staatstrojaner sind eine ernste Bedrohung für die freiheitliche Demokratie.

Sie wollen unsere Arbeit gegen Staatstrojaner mit Ihrer Unterschrift unterstützen?

https://aktion.digitalcourage.de/kein-staatstrojaner

Foto: Mischa Burmester, cc by-sa 4.0

Von links nach rechts: Prof. Dr. Frank Josef Braun, Prof. Dr. Jan Dirk Roggenkamp, Rena Tangens, padeluun und Nils Büschke

Zitate der Beschwerdeführer.innen und Klagevertreter

„Staatstrojaner sind digitale Waffen, mit denen der Staat heimlich in Privatsphäre und Persönlichkeitsrechte, in Informationelle Selbstbestimmung und Meinungsfreiheit der Betroffenen einbrechen kann. Es handelt sich um einen der schwersten Grundrechtseingriffe, der auch die Menschenwürde verletzt sowie die IT-Sicherheit schädigt – und damit auch die Allgemeinheit. Diese Methode zur digitalen Totalüberwachung gehört deshalb dringend für null und nichtig erklärt.“

Dr. Rolf Gössner, Rechtsanwalt und Publizist

„Die Quellen-Telekommunikationsüberwachung und die Online-Durchsuchung überschreiten die äußerste Grenze (rechts)staatlicher Ausforschung der Intimsphäre zum Zweck der Strafverfolgung bei weitem. Sie gestatten nicht nur die offene Verwertung höchstvertraulicher Informationen wie sie z.B. in einem Tagebuch stehen. Sie erlauben die dauerhafte heimliche Überwachung des Verfassens der Tagebucheinträge und dessen, was der Betroffene nicht einmal seinem Tagebuch anvertrauen würde. Sie ermöglichen es, die digitalisierten Gedanken eines Menschens zu lesen.“

Prof. Dr. Jan Dirk Roggenkamp, Prozessbevollmächtigter

„Die dramatisch weitreichenden Überwachungsmaßnahmen, die quasi die Möglichkeit beinhalten ‚Gedanken auszulesen‘ stellen gerade diejenigen ins Visier der Ermittler, die in Ausübung verfassungsrechtlich geschützter Selbstschutzmöglichkeiten verschlüsselt kommunizieren. Die Verfassungswidrigkeit der Vorschriften, die in einem überstürzten und unreflektierten Gesetzgebungsverfahren ‚durch die Hintertür‘ in die Strafprozessordnung eingeführt wurden, ist evident. Es wurden grundlegende Vorgaben des Bundesverfassungsgerichts missachtet.“

Prof. Dr. Frank Braun, Prozessbevollmächtigter

„Wer Smartphones heimlich beobachtet, forscht letztlich die Gedankenwelt der Nutzer aus und kann Persönlichkeitsbilder erstellen, die umfangreicher, gläserner nicht sein können.“

Rena Tangens, Vorstandsmitglied und Gründerin von Digitalcourage

„Schutzranzen“

Kindertracking ist keine Lösung, sondern ein Problem!

von Claudia Fischer

Foto: Claudia Fischer, cc by-sa 4.0

Kinder stark machen!
Überwachung ist eine Misstrauenserklärung an das Kind.

Der Ansatz von „Schutzranzen“ ist grundfalsch: Firmen und Verbände versuchten 2018, unter diesem Markennamen GPS-Tracker und Apps an Grundschulkinder zu verteilen, die in bestimmten Navigationsgeräten die Positionen der Kinder anzeigen sollen. (siehe S. 13) Warum das technisch eher rückständig und datenschutzrechtlich bedenklich ist, können Sie auf unserer Webseite nachlesen. Im Kern aber geht es um die Frage, wie wir unsere Kinder erziehen.

Die Eltern-Kind-Beziehung darf keine Überwachungsbeziehung werden

Der Bundesvorsitzende des Verbandes Bildung und Erziehung (VBE), Udo Beckmann, unterstützte – wie mehrere andere Pädagogik-Verbände – unsere Kritik: „Sicherheit kann man nicht kaufen, aber man kann seine Kinder zu starken, selbstständigen Persönlichkeiten erziehen, die wissen, wie sie sich im Straßenverkehr bewegen.“ Die Digitalcourage-Arbeitsgruppe Pädagogik schrieb in unserem Blog:

„Aufpassen statt Überwachen“

Selbstverständlich müssen Eltern ihr Kind beschützen. Doch hundertprozentige Sicherheit kann es nicht geben. Gefahren gehören zum Großwerden, Eltern können niemals alle aus dem Weg räumen und täten ihrem Kind damit auch keinen Gefallen. Wer sich sicher glaubt, ist weniger aufmerksam und dadurch erst recht gefährdet.

Wer seinem Kind auf Schritt und Tritt über die Schulter schaut, sagt damit: „Ich misstraue dir. Ich bezweifle, dass du dich an unsere Regeln hältst. Leugnen hat keinen Zweck, auf dem Computer ist das Protokoll.“ Überwachungsgeräte sind eine teure Misstrauenserklärung an das Kind.

Aber: Wissen das die Autos?

Jetzt denken Sie vielleicht: „Das ist ja alles schön und gut, hilft im Straßenverkehr aber wenig! Mit Selbstbewusstsein kann mein Kind kein Auto stoppen!“ Genau – deshalb argumentieren wir anders herum:

In der Realität sind nicht die Kinder die Gefahren. Gefährlich sind Fahrzeuge, unachtsame Fahrer.innen, Handys am Steuer, unübersichtliche Schulwege, zu schmale Radwege, fehlende Straßenbeleuchtung und unsichere Fußgängerüberwege. „Schutzranzen“ aber fördert den Blick aufs Smartphone- oder Navigationsgeräte-Display statt auf den Verkehr.

Nicht nur für Kinder, sondern für uns alle besser wären Schülerlotsen, reduzierte Geschwindigkeit, Fahrzeuge mit gutem Rundumblick, weniger Autos durch mehr Fahrrad- und öffentlichen Nahverkehr, Geländer und beleuchtete Gehwege. Und, wie wir es im Blog von bielinski.de gelesen haben: „An der Kreuzung bei uns um die Ecke, die meine Kinder jeden Tag mehrmals queren müssen, gibt es schon eine ziemlich etablierte Warnmeldung, ganz ohne Smartphone-Push. Sie heißt Ampel.“

Grafik: Digitalcourage, cc by-sa 4.0

„Europäischer Datenschutz wird gerade zum Welt-Standard“

Ein Interview mit Jan Philipp Albrecht zur DSGVO

Foto: Claudia Fischer, cc by-sa 4.0

Jan Philipp Albrecht (Die Grünen) und Julia Reda (Piratenpartei) stellen sich den Fragen der Teilnehmer.innen des europäischen Aktiven-Treffens „Freedom not Fear“ in Brüssel (2017)

Jan Philipp Albrecht war als Abgeordneter der Grünen im EU-Parlament und hat als Berichterstatter den komplizierten Kompromiss zur europäischen Datenschutzgrundverordnung (DSGVO) ausgehandelt. Er hat mit dafür gesorgt, dass die Interessen der europäischen Bürgerrechtsbewegungen und der Zivilgesellschaft im Gesetzgebungsprozess genauso gehört wurden wie die Wünsche der IT-Wirtschafts-Lobby. Claudia Fischer hat ihn für Digitalcourage zum Einfluss der Bürgerrechtsbewegungen in Brüssel befragt.

Claudia Fischer: ***Wir hören immer wieder, speziell von Wirtschaftsvertretern, Deutschland habe im europäischen Vergleich starke Datenschutzgesetze. Und häufig ist das direkt mit der Drohung verbunden, das sei ein Standortnachteil. Ist Datenschutz ein überwiegend deutsches Thema, oder waren auch andere Länder im Gesetzgebungsverfahren zur Datenschutzgrundverordnung besonders aktiv?***

Foto: Ruprecht Stempell, cc by-sa 4.0

Jan Philipp Albrecht: Das ist eine Selbstwahrnehmung der Deutschen, dass Datenschutz in Deutschland besonders viel Aufmerksamkeit habe. Deutschland hat aber gar nicht den Ton angegeben in der Debatte. Die Zivilgesellschaft in ganz Europa hat unsere Gesetzgebung frühzeitig auf dem Schirm gehabt. Zum Beispiel aus den Niederlanden, aus Polen, aus Frankreich und aus Spanien waren die zivilgesellschaftlichen Verbände und Akteure sehr früh dabei. Auch aus Irland zum Beispiel, das ja eher als „Schmuddelkind“ in Sachen Datenschutz gilt. Da ist die Zivilgesellschaft aber sehr stark.

Deutschland spielt schon eine große Rolle, was aber einfach auch daran liegt, dass Deutschland das größte EU-Land ist und sich die Zivilgesellschaft deshalb auch ordentlich organisieren kann. Hier haben die Verbände mehr Mittel, weil sie größer sind als in anderen Ländern. Sie können es sich deshalb eher leisten, sich mit europäischen Themen auseinanderzusetzen. Zum Beispiel hat der deutsche Bundesverband der Verbraucherzentralen einen Schwerpunkt auf den Datenschutz legen können, das können kleinere Organisationen nicht. Aber das heißt noch lange nicht, dass Deutschland die Diskussion stark bestimmt hat. Im Gegenteil, gerade in kleinen Ländern war das Interesse an Datenschutz relativ schnell sehr hoch.

Das lag auch daran, dass in den Jahren 2006/2007 das Thema Überwachung von Konzerndaten durch Geheimdienste oder im Rahmen von Terrorismusbekämpfung überall diskutiert wurde. Später bestimmten die „Datenlecks“ bei Unternehmen die Debatte und der Blick richtete sich auch auf die Sicherheit von Verbraucherdaten.

CF: ***Sind die Themen in allen europäischen Staaten ähnlich? Oder gibt es regionale Unterschiede?***

JPA: In Ländern, in denen es harte Auseinandersetzungen um die Überwachung von Kritikern durch die Regierung gibt, liegt natürlich ein Schwerpunkt bei der Frage „Klassische Bürgerrechte gegenüber dem Staat“. Die dortige Diskussion wird relativ hart und rabiat geführt.

Aber man muss sagen, dass sich das in den vergangenen Jahren auch immer mehr angeglichen hat. Zum einen ist es inzwischen immer deutlicher geworden, welche Rolle Privatunternehmen auch bei Fragen nationaler Sicherheit spielen, auf der anderen Seite wurden auch in eigentlich offeneren Ländern wie Frankreich oder Deutschland die Sicherheitsmaßnahmen so verschärft, dass sie zum Teil die Praxis in repressiveren Staaten Europas übertreffen. Die Themenschwerpunkte in verschiedenen Ländern unterscheiden sich also nicht mehr so stark.

CF: ***In welcher Form hat die Zivilgesellschaft sich eingebracht? Gerade kleine Bürgerrechtsorganisationen aus weiter entfernten Teilen der EU konnten ja nicht einfach mal nach Brüssel kommen. Wie war der Kontakt für Dich, auch zu kleineren Organisationen?***

JPA: Es gab von Anfang an bei dieser Reform europäische Dachverbände, in denen sich Akteure versammelt haben. Es gab und gibt immer wieder Veranstaltungen wie zum Beispiel „Freedom not Fear“, das ja von Digitalcourage mit organisiert wird, oder andere Aktivistentreffen. Diese Treffen bringen auf sehr persönlicher Ebene Aktivisten zusammen und stellen einen Kontakt zu den Abgeordneten im EU-Parlament her. Das gibt auch kleineren Akteurinnen und Akteuren die direkt Möglichkeit, sich in einen Diskussions- und Gesetzgebungsprozess direkt einzubringen.

> „… was er oder sie zu sagen hat. Das wurde wirklich wertgeschätzt.“

Zusätzlich hat das Europäische Parlament sehr viel Wert darauf gelegt, die Akteure einzuladen – auch Einzelpersonen, die nicht in einer großen Organisation arbeiten. Das hat gut funktioniert. Ich glaube wirklich, dass es in diesem Prozess nicht auf die Größe einer Organisation ankam, sondern darauf, welche Inhalte jemand eingebracht hat, also was er oder sie zu sagen hat. Das wurde wirklich wertgeschätzt.

CF: ***Es gibt ja eine spannende Filmdokumentation über das Gesetzgebungsverfahren zur DSGVO, den Film „Democracy – im Rausch der Daten“ von David Bernet. Dort sieht man, wie Ihr intensiv in sogenannten „Schattentreffen“ um Formulierungen und Kompromisse gerungen habt. Waren Bürgerrechtler bei solchen Shadow-Meetings mit dabei?***

JPA: Die „Schatten-Treffen“ sind eine offizielle Einrichtung des Europäischen Parlaments, da sitzen nur Leute, die für die Abgeordneten arbeiten, die Abgeordneten selbst und die Sekretariate. Da kommt kein Interessenvertreter rein, und das ist ja auch richtig so, weil das Entscheidungsgremien im EU-Parlament sind.

Aber es hat ganz viele Vor- und Nachbereitungstreffen gegeben, wo sowohl gegenüber allen Stakeholdern (Interessenvertretern) als auch gegenüber Institutionen Abstimmungs- und Rückkopplungsprozesse stattgefunden haben. Auch, damit man immer wieder verabredet und deutlich macht, dass man noch „gemeinsam unterwegs“ ist. Es ist im europäischen Prozess sehr wichtig, dass man immer wieder alle Leute mitnimmt, weil man nicht am Ende etwas vorlegen sollte, was nicht mehrheitsfähig ist.

Foto: Claudia Fischer, cc by-sa 4.0

Das EU-Parlament in Brüssel – Tagungsort für „Freedom not Fear“

CF: *Nun hat es in Deutschland reichlich Kritik an der Datenschutzgrundverordnung gegeben. Auch Du persönlich bist sehr angegriffen worden. Was ist da schief gelaufen?*

JPA: Ich denke, dass in der Kommunikation in Deutschland vieles schief gelaufen ist. Diese liegt in den Händen der Bundesregierung, der Datenschutzbehörden und der bundespolitischen Akteure. Wie wir alle wissen, ist die Möglichkeit der EU-Institutionen, in Deutschland Gehör zu bekommen, begrenzt. Trotzdem haben wir uns extrem bemüht, während des Gesetzgebungsverfahrens sehr viel Öffentlichkeit dafür herzustellen. Es war auch für alle möglich, sich einzubringen. Der Prozess hat insgesamt vier Jahre gedauert vom Vorschlag bis zur Abstimmung, und schon vor dem Vorschlag war ein Konsultationsverfahren. Also seit 2010 war die Debatte eigentlich offen. Ab Anfang 2016 war die Verordnung beschlossen. Jede.r konnte darüber lesen und es wurde auch immer wieder darauf hingewiesen, was in diesem Gesetz steht.

> …dass in der Kommunikation in Deutschland vieles schief gelaufen ist.

Dass nun in Deutschland viele Menschen am 25. Mai 2018 aus allen Wolken gefallen sind, liegt aus meiner Sicht daran, dass in Deutschland offenbar immer noch nicht die Fähigkeit besteht, sich auf EU-Gesetzgebung einzulassen und sich frühzeitig damit zu befassen. Stattdessen existiert die Haltung, „Solange das hier noch nicht durch den Bundestag gegangen ist, solange das nicht bei uns vor Ort ausdiskutiert wurde, wird da schon nichts in Kraft treten.“ Und das ist mit der Datenschutzgrundverordnung eben gar nicht mehr nötig gewesen, weil wir eine Verordnung (nicht eine Richtlinie) gemacht haben. Die muss eben nicht mehr in nationales Recht umgesetzt werden, da wird auch nicht national dran gerüttelt, sondern die gilt halt einfach. Und da gab es glaube ich so einen Reflex nach dem Motto: „Das kann doch nicht sein, wir sind doch in Deutschland diejenigen, die alles zu sagen haben.“

Und ich glaube, da ist auch eine Pikiertheit dabei, dass man da einfach aus der EU irgendwas kriegt, was als nicht angemessen wahrgenommen wird, während die EU da tatsächlich endlich mal etwas macht, was den Menschen total viel bringt. Und was weltweit dafür sorgt, dass die Rechte, die es in Deutschland schon sehr lange gibt, auch weltweit respektiert werden. Viele Unternehmen machen die EU-Regelung inzwischen zu ihrem weltweiten Standard, egal, ob sie in Europa

agieren oder anderswo. Und es ist wirklich schizophren, dass das gerade in Deutschland, anders als in fast allen anderen EU-Staaten, so kritisch gesehen wird. Besonders, weil sich gerade in Deutschland durch die DSGVO so gut wie nichts verändert hat. Die Standards zwischen Bundesdatenschutzgesetz und der Datenschutzgrundverordnung haben sich nicht groß verändert. Aber plötzlich sind sie vielen offenbar bewusst geworden.

Die deutsche Bundesregierung hat in dem Gesetzgebungsprozess vor allem die Interessen der Wirtschaft vertreten.

CF: ***Kann das auch daran liegen, dass unsere Regierung 2017/18, also genau in der heißen Phase vor der Anwendungspflicht der DSGVO mit Koalitionsverhandlungen beschäftigt war?***

JPA: Ja, das kann sein. Aber es liegt auch daran, dass diese Bundesregierung (und auch die Bundesregierung davor) kein Interesse daran hatte, dass die Datenschutzgrundverordnung so kommt, wie sie ist. Und dass sie auch jetzt, im Nachhinein noch, versucht, die DSGVO zu torpedieren. Anders als viele andere Regierungen in der EU das tun, und auch anders als andere Regierungen das von Deutschland erwartet haben.

Die deutsche Bundesregierung hat in dem Gesetzgebungsprozess vor allem die Interessen der Wirtschaft vertreten. Sie haben die Verbraucherinteressen und die Grundrechtsfragen, den deutschen Datenschutz, eigentlich überhaupt nicht verteidigt. Die Bundesregierung hat kein Interesse daran gehabt, dass der deutsche Standard zum EU-Standard oder sogar zum Weltstandard wird.

Trotzdem hat aber auch die Bundesregierung am Ende diesem Gesetz zugestimmt. Alle Parteien außer der AfD haben im Europäischen Parlament zugestimmt. Man muss also sagen, hier fehlt auch einfach die Verantwortung dafür, dass man das, was man da mitbeschlossen hat, den Menschen am Ende auch ordentlich erklärt.

Lieber Jan Philipp, danke für Deinen Einsatz – und für dieses Interview!

Foto: Ruprecht Stempell, cc by-sa 4.0

Jan Philipp Albrecht hat inzwischen sein Mandat im Europäischen Parlament niedergelegt und ist ab September 2018 „Minister für Digitales und Draußen“, wie er seinen neuen Posten selbst nennt, in Schleswig-Holstein. (Die korrekte Bezeichnung ist „Minister für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung“.)

Von der DSGVO zu ePrivacy

Wir entlarven die Mythen der Industrie

Von Friedemann Ebelt

Die Europäische Datenschutzgrundverordnung (DSGVO) legt bestimmte Prinzipien des digitalen Verbraucherschutzes eher allgemein fest. Die geplante ePrivacy-Verordnung, die seit über zwei Jahren in Vorbereitung ist, soll diese Vorgaben konkretisieren: Z.B. soll künftig unsere Zustimmung nötig sein, um uns beim Besuch von Webseiten zu „verfolgen“ (zu tracken) und in unseren Internet-Browsern und Mobilgeräten sollen immer die schärfsten Privatsphäre-Einstellungen voreingestellt sein.

Kurz vor Redaktionsschluss dieses Jahrbuches ging die Meldung durch die Presse, dass Österreich die ePrivacy-Reform nicht während seines Vorsitzes im Europarat behandeln lassen will – damit könnte sich der Prozess bis 2020 verzögern. Die Lobbyisten reiben sich die Hände, und wir Verbraucher.innen haben das Nachsehen. Die Argumentation der Tracking-Industrie hat unser Mitarbeiter Friedemann Ebelt analysiert:

1. Mythos: Werbung rettet den Journalismus

Ohne Werbung gibt es im Internet keine frei zugänglichen Inhalte. Tracking und Werbung sichern die Finanzierung des Journalismus.

Dieses Verdreh-Argument ist seit längerem ein beliebter rhetorischer Kniff der Tracking-Industrie. Richtig ist allerdings, dass Werbebudgets in jedem Fall dorthin fließen, wo es die meisten Klicks, Likes und Follower gibt – das trifft eher auf Kätzchenvideos und nackte Haut zu als auf fundierte Recherchen. Von dieser Marktlogik profitieren Youtube, Facebook, Google, Influencer und Clickbaiting-Anbieter – egal, ob das Recht auf Privatsphäre gut oder schlecht geschützt ist.

Keine Redaktion in Deutschland kann ihre journalistische Arbeit über Tracking-Werbung finanzieren.

Keine Redaktion in Deutschland kann ihre journalistische Arbeit über Tracking-Werbung finanzieren. Darum sind die wertvollsten Inhalte auch dort zu finden, wo es die wenigste Werbung gibt. Die Werbefinanzierung von Inhalten ist ein überholtes Modell. Im Internet gibt es, besonders für Journalismus, nur „lousy pennies“. Für Journalismus sind andere Finanzierungsmodelle notwendig, neue Online- und Offline-Formate, Abos, Genossenschaften

oder ähnliches. Über diese Frage hat aber kein Datenschutzrecht zu entscheiden. Wenn die Werbeindustrie darüber sprechen möchte, dass der Journalismus in Gefahr ist, dann hat das nichts mit Datenschutz zu tun, sondern zum Beispiel mit Content Marketing – einer Werbestrategie, die die redaktionelle Unabhängigkeit gefährdet.

▶2. Mythos: Metadaten sind harmlos

Werbetracking ist keine Überwachung, es geht doch nur um Metadaten…

„Was ist schon dabei, die Geodaten von Millionen von Nutzer.innen in Echtzeit zu erheben und zu verarbeiten? Es geht doch nur darum, den Menschen einen Service zu bieten und dafür muss eben erfasst werden, wer sich wann und wo aufhält." So oder so ähnlich klingt es, wenn die Datenindustrie über Metadaten spricht. Im Fokus steht ihr Interesse an Daten, Kundschaft und an Diensten, die möglichst viele Menschen nutzen. Völlig aus dem Blick geraten die Folgen für die Betroffenen. Geschaut wird auf die Vorteile für die Überwacher und nicht auf die Nachteile für die Überwachten. Wenn Daten dazu genutzt werden, um Menschen zu verfolgen, zu bewerten und zu sortieren, dann um „gute" Kundinnen von „schlechten" Kunden zu trennen und den ökonomisch wertvollen Menschen bessere Angebote, Services, Bedingungen und Informationen zukommen zu lassen. Wir sagen: Die einzige Möglichkeit, digitale Wirtschaft nachhaltig, das heißt, in Einklang mit dem Grundrecht auf Privatsphäre zu gestalten, liegt in datenschutzfreundlichen Geschäftsmodellen.

▶Geschaut wird auf die Vorteile für die Überwacher und nicht auf die Nachteile für die Überwachten.◀

▶3. Mythos: Werbetracking schadet nicht der Privatsphäre

Einwilligungen sind in der Praxis nicht einzuholen. Darum sollte Tracking ohne Einwilligungen funktionieren.

Der Kern des Rechts auf Privatsphäre lautet: Wer was liest, wer sich mit wem trifft und wer wo schläft, geht Dritte nichts an. Zu dieser Grundregel gibt es Ausnahmen. Dazu gehören sachlich notwendige Datenverarbeitungen (wer eine Rechnung stellt, muss die Adresse der Kundin verarbeiten dürfen) oder zum Beispiel die Einwilligung. Wer von einer Person etwas wissen möchte, muss danach fragen. Wenn keine Einwilligung erteilt wird, dann wollen die Menschen nicht beobachtet werden. Werben ist innerhalb dieses Rahmens möglich. Der Daten- und Geldhunger der Werbeindustrie treibt sie allerdings zu invasiven Strategien der Datenerhebung an. Gewünscht sind Werbedisplays an Bushaltestellen, die die Kleidung, Gesichter und Smartphones der Passanten auslesen. Der Traum besteht in einem uneingeschränkten Datenhandel von Kundenprofilen, die auch Aufschluss darüber geben, wie viel Geld eine Person bereit ist, für Unterwäsche auszugeben. Ideal für den Datenrausch wären auch Smartphones, mit denen im Supermarkt personalisierte Preise generiert werden können, ganz nach dem Motto: „Wer jeden Freitag um 17:00 Uhr einkauft, hat sonst keine Zeit und darf sich darum über etwas höhere Preise freuen."

▶Gewünscht sind Werbedisplays an Bushaltestellen, die die Kleidung, Gesichter und Smartphones der Passanten auslesen.◀

Für Preisdiskriminierung werden wir unser Recht auf Privatsphäre nicht aufgeben! Mehr Argumente lieferte padeluun in seiner Laudatio bei den BigBrotherAwards 2017 (verlinkt über die Jahrbuch19-Webseite).

▶4. Mythos: ePrivacy schadet EU-Unternehmen

Die ePrivacy-Verordnung nützt nur den großen US-Konzernen, europäische Mitbewerber haben das Nachsehen.

Google, Facebook und Co. profitieren von einem starken Lock-in-Effekt. Wer einmal die AGB unterzeichnet, kann dann fast beliebig auf Klick und Wisch durchleuchtet werden. Mitbewerber haben den Nachteil, dass sie erst um Einwilligung bitten müssen. Allerdings können Grundrechte nicht aufgegeben werden, weil die Marktmacht großer Konzerne ein riesiges Problem ist! Google, Facebook und Co. sind mächtig, weil es die europäische Politik, Wirtschaft und Zivilgesellschaft nicht geschafft haben, bessere Plattformen aufzubauen. Warum existiert noch immer kein offener europäischer Suchindex? Warum wurden europäische Ansprüche an den Umgang mit Daten gegenüber Facebook nicht konsequent durchgesetzt? Die Antwort auf beide Fragen lautet: Weil die Werbe- und Tracking-Industrie in Google, Facebook und Co. keine Rivalen sieht, sondern Vorbilder und Geschäftspartner. Grundsätzlich wird die ePrivacy-Verordnung in gleichem Maße für alle Firmen gelten, die in der EU tätig sind.

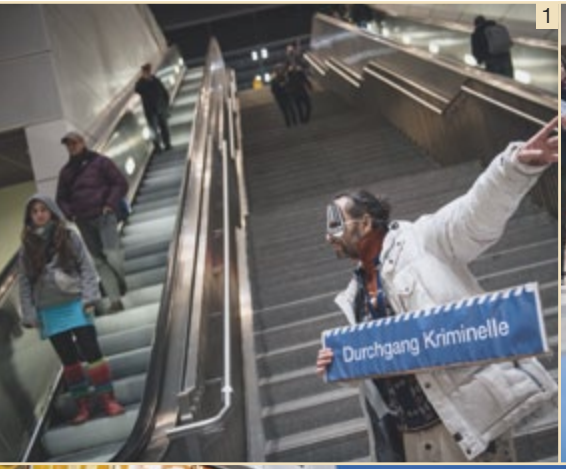
Illustration: Isabel Wienold, cc by-sa 4.0

▶Grundrechte können nicht aufgegeben werden, weil die Marktmacht großer Konzerne ein riesiges Problem ist!◀

Links und weitere Infos: digitalcourage.de/jahrbuch19

Bahnhof Südkreuz (Berlin): Proteste in Bildern

Fotos: 1= Stefanie Loos, cc by-sa 4.0 – 2= Digitale Freiheit, cc by-sa 4.0



1

1

Eigentlich machen sie weiter: Am 31.7.2018 beendete das Bundesinnenministerium zwar offiziell das Pilotprojekt zur Gesichtserkennung am Bahnhof Südkreuz in Berlin, zum gleichen Zeitpunkt kündigten sie aber an, ab Herbst 2018 weitere Videoanalyse-Systeme zu testen. So schrieb uns das Ministerium, jetzt solle es „um das automatisierte Erkennen potenzieller bahnhofstypischer Gefahren- und Belastungssituationen im Bahnhof Berlin Südkreuz gehen wie z.B. liegende Personen, abgestellte Gegenstände, Betreten gesperrter Bereiche, Überfüllung von Bahnsteigen oder auch schnelles Auseinander- bzw. Zusammenlaufen von großen Personengruppen.“ Kurz: Nun wird Videoüberwachung zur Verhaltensanalyse erprobt.

Wir haben gemeinsam mit anderen aus der „Berliner Allianz für Freiheitsrechte“ (BAfF) während des Pilotprojektes seit Sommer 2017 mehrfach demonstriert. **Und wir werden auch weiter zeigen, dass wir mit Videoanalyse-Methoden nicht einverstanden sind.** Eine Auswahl der bisherigen Aktionen sehen Sie hier.

2

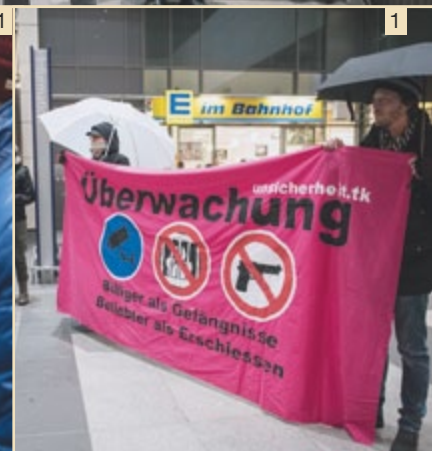
2

1

1

1

1



1

Pretty Easy. Privacy.

Von padeluun

Fotos: padeluun, cc by-sa 4.0

„Ziemlich einfach E-Mails verschlüsseln“. Davon träumen wir seit 1992, seit wir das Verschlüsselungsprogramm ‚PGP‘ in Deutschland mit unserem Buch „Der Briefumschlag für Ihre elektronische Post“ bekannt gemacht haben. PGP bedeutet ‚Pretty Good Privacy‘, was auf Deutsch ‚ziemlich gute Privatsphäre‘ bedeutet. Wir übersetzten das Programm ins Deutsche, auch das Handbuch, und halfen mit dabei, GnuPG (also PGP als Freie Software) zu konzipieren. Zusammen mit einer Journalistin schafften wir es, dass das Wirtschaftsministerium 160.000 DM für das Programmieren einer Windows-Version zur Verfügung stellte. Leider wurde aber nur an der Linux-Version gut programmiert – und die Windows-Software ist bis heute nur von Fachleuten einzusetzen.

▶Bisher ist Verschlüsseln alles andere als ‚ziemlich einfach‘.◀

In vielen Städten haben sich unter anderem deswegen Cryptoparties etabliert, wo Menschen lernen können, verschlüsselt zu mailen. Aber bis heute ist es nur ein kleiner Anteil der Nachrichten, die verschlüsselt durchs Netz gehen. Denn bisher ist Verschlüsseln alles andere als ‚ziemlich einfach‘.
Das ändert sich gerade.

Wir haben eine Stiftung in der Schweiz mitgegründet namens p≡p-Foundation. p≡p steht für ‚Pretty Easy Privacy‘. Die Stiftung hat das Recht, zu bestimmen, welche Unternehmen p≡p entwickeln und vertreiben dürfen. Nämlich nur Firmen, die sicher stellen, dass sie die Software als freie Software entwickeln. Außerdem müssen sie den Quellcode veröffentlichen (und von Fachbetrieben prüfen lassen!), so dass gewährleistet ist, dass keine Hintertüren in das Programm eingebaut sind. Stiftungsräte wachen darüber, dass alles mit rechten Dingen zugeht – Rena Tangens und padeluun von Digitalcourage sind zwei dieser Wachhunde im Stiftungsrat.

Wenn alles gut gegangen ist, dann gibt es, wenn Sie dieses Jahrbuch hier in der Hand halten, diese einfache Verschlüsselung bereits einsatzfähig, ohne dass man noch mehr tun muss als einmal zu klicken. Es gibt sie dann für die Plattformen Windows, Linux, Mac, iOS und Android. Die Mails, die ich auf dem Windowsrechner in der Firma schreibe, kann ich also auch unterwegs auf meinem iPhone lesen. (Wer’s kennt: Enigmail im Thunderbird arbeitet bereits mit p≡p.)

Und ja, das wird ‚pretty easy‘ – ziemlich einfach. Die Installation braucht nur einen Mausklick oder Fingertipp und ab dann werden alle Nachrichten verschlüsselt. Fehlt ein Schlüssel, wird’s dennoch versendet, aber eine Ampel zeigt mir an, dass diese Nachricht jetzt ‚unsicher‘ (also unverschlüsselt) ist. Gelb heißt ‚verschlüsselt“ und grün bedeutet, dass meine Nachricht auch signiert ist – dass man also ‚pretty sure‘ (ziemlich sicher) sein kann, dass die Nachricht wirklich von der Person kommt, deren Mailadresse im Absender steht. Das wird besonders Betrüger sehr ärgern.

Die Grundidee zu p≡p kommt von dem Programmierer Volker Birk, der es geschafft hat, einige ärgerliche Konzernchefs, die sich nicht mehr von der NSA ausspionieren lassen wollen, zur Finanzierung eines solchen Großprojektes zusammen zu bekommen. Jetzt arbeitet ein Haufen richtig guter Programmierer in Zürich, Luxemburg, Berlin, Bielefeld und Barcelona daran, den Geheimdiensten die Existenzgrundlage der Massenüberwachung wegzunehmen. Denn wo fast alles verschlüsselt ist, kann man nichts mehr mitlesen. Übrigens (Hinweis für die Fachleute!) ziemlich bald sind auch Metadaten unauswertbar! Das ist, finden wir: ‚Pretty Good‘!

Künstler.innen, Autor.innen, Programmierer.innen und Aktivist.innen verkündeten den Start von p≡p in einer vollen Halle auf der re:publica 2018.

p≡p-Software installieren:
https://www.pep.security/

Auf dem Laufenden bleiben:
https://pep.foundation/

Links und weitere Infos: digitalcourage.de/jahrbuch19

Das Digitalcourage-Team

Portraits

Von Claudia Fischer

In jedem Jahrbuch stellen wir drei Mitglieder, Ehrenamtliche oder Beschäftigte von Digitalcourage vor. Wir achten auf eine gute Mischung: Menschen unterschiedlichen Geschlechts und Alters. Menschen, die für Digitalcourage nach außen sichtbar werden oder nur intern dafür sorgen, dass der Laden läuft. Techniker.innen und Menschen mit ganz anderen wichtigen Talenten. Junge, alte, in Bielefeld und in den Ortsgruppen – unser Team ist bunt und darauf sind wir stolz. Und wir würden gerne noch bunter – auf unserer Homepage gibt es die Rubrik „Mitmachen“. Vielleicht ist etwas für Sie dabei?

„Ich darf nicht den Zug verpassen!“

Jessica Wawrzyniak

2018 wird als besonderes Jahr in Jessica Wawrzyniaks Lebensgeschichte eingehen: Das erste Mal hält sie ein Buch in der Hand, auf dem ihr Name steht. Ihr #kids #digital #genial-Lexikon, das im Juni erschienen ist, erklärt technische Begriffe wie „Admin“ oder „Algorithmus“ verständlich – eigentlich für Kinder, aber auch viele Erwachsene werden sich freuen, endlich zu erfahren, was sich dahinter verbirgt.

Das Buch war eine Menge Arbeit. Erstaunlicherweise, denn eigentlich war doch schon alles fertig. Die Lexikon-Beiträge waren alle schon geschrieben und in Jessicas Blog auf kidsdigitalgenial.de erschienen. Ausdrucken – fertig? „Auf keinen Fall“, rollt sie mit den Augen. „Ich habe alle Beiträge nochmal durchgesehen, die Bilder im Blog waren nicht geeignet für den Ausdruck, ich musste Texte kürzen, umschreiben, Links funktionieren in einem Buch nicht – im Grunde musste ich meinen Blog für die Print-Version völlig neu denken.“

Jetzt liegt es vor, Jessicas „Lexikon von App bis .zip“, und kann bei Digitalcourage bestellt werden. Meist wird es in Klassensätzen von Schulen und Lehrer.innen angefordert. „In den ersten 5 Wochen war schon ein Viertel der Auflage verkauft, und das kurz vor den Sommerferien. Es will sogar jemand das Buch ins Französische übersetzen“, freut sie sich. Und niemand kennt die Verkaufszahlen besser als sie, denn sie ist die Shop-Chefin von Digitalcourage. Jede Bestellung geht direkt durch ihre Hand.

Auf Digitalcourage aufmerksam wurde Jessica durch einen persönlichen Kontakt. Ein zufälliges Treffen mit Büroleiterin Sylke Kahrau im Bus. „Als ich 9 oder 10 war, habe ich neben Sylke gewohnt und auf ihre kleine Tochter aufgepasst“, erinnert sich Jessica, die heute 27 Jahre alt ist. „Und als wir uns 2016 im Bus wieder

Foto: Fabian Kurz, cc by-sa 4.0

trafen, suchte Digitalcourage jemanden, der sich um die Spendenverwaltung kümmert. Sieben Stunden in der Woche, ein Mini-Job. Dann habe ich den Shop dazu genommen und parallel privat meinen Blog für Kinder aufgebaut. 2017 kam der Punkt, an dem ich meinen Blog dem Team vorgestellt habe, und so nahm die Sache ihren Lauf. Inzwischen bin ich bei 30 Stunden in der Woche und padeluun sagt mir manchmal zwinkernd, ich hätte mich „reingezeckt“ in den Verein.“

„Ich muss da hingehen, wo die Kids sind, ich kann doch nicht warten, bis sie zu mir kommen.“

Ihre „Arbeitsgruppe Pädagogik“ bei Digitalcourage hat sie gegen einige Widerstände durchkämpfen müssen. „Es war keine leichte Entscheidung für das Team. Wie pädagogisch soll Digitalcourage werden? Medienpädagogik machen schließlich auch andere. Wird die politische Arbeit darunter leiden?“ Aber diese Zweifel sind vorbei. Heute freuen sich alle mit ihr, dass das Lexikon so viel Anklang findet und pädagogische Tipps die Website von Digitalcourage bereichern.

Jessica hat Erziehungswissenschaften und Soziologie studiert und dabei, sobald sie konnte, immer den Medienschwerpunkt gewählt. Das Masterstudium in Interdisziplinären Medienwissenschaften setzte dem Ganzen den Deckel auf. „Ich bin Anfang der 1990er geboren, das Internet war mein Zuhause. Ich habe auf ICQ gechattet, oder auf Knuddels. Wenn meine Eltern mich nicht vom PC im Gästezimmer entfernt haben, war ich den ganzen Tag online.“ Spiele haben sie nicht besonders interessiert – Kommunikation war immer ihr Ding. Das Taschengeld ging für Laptops und Handys drauf. „Nicht die neuesten Geräte, immer eher so eine Stufe hinterher.“ Das erste Smartphone hatte sie mit 14 oder 15.

Anders als viele bei Digitalcourage meidet Jessica nicht die sozialen Netzwerke der großen Datenkraken, sondern ist bei Facebook, Instagram und Co zumindest als Zuschauerin aktiv. „Das muss ich als Medienpädagogin einfach. Ich muss da

Foto: Fabian Kurz, cc by-sa 4.0

Medienpädagogin, Online- und jetzt auch Print-Autorin: Jessica Wawrzyniak und ihr frisch gedrucktes Lexikon #kids #digital #genial

hingehen, wo die Kids sind, ich kann doch nicht warten, bis sie zu mir kommen.“ Der Kontakt zu Kindern und Jugendlichen ist elementar für ihre Arbeit. Neben dem Job bei Digitalcourage bietet sie Computerkurse in den Ferienspielen an und auf ihrem Nachttisch zu Hause liegt medienpädagogische Literatur. Und wann kommt der Punkt, an dem sie selbst zu alt wird, um mit den Kids Schritt zu halten? „Eine Zwölfjährige sagte neulich zu mir: ‚Mensch, meine kleine Schwester, die ist acht, was die alles an dem Handy macht, da komme ich schon gar nicht mehr mit.‘ Da dachte ich nur, Wow, was soll ich denn sagen, und was soll ich in zehn Jahren sagen? Oder vielleicht auch schon in 5 Jahren, weil die Entwicklung so schnell ist? Ich muss am Ball bleiben und die Themen der Kinder und Jugendlichen auf dem Schirm haben. Ich darf da echt nicht müde werden und einschlafen. Wenn ich ein Mal den Zug verpasse, dann war‘s das.“

Vorerst ist das aber nicht zu befürchten. Denn ihr #kids #digital #genial-Lexikon hatte schon in der Online-Version im November 2017 einen Bürgermedienpreis gewonnen – als Anschubfinanzierung für die gedruckte Ausgabe. Aufmerksamkeit ist ihr in ihrer Rolle als Medienpädagogin, Online- und jetzt auch Print-Autorin also gewiß. Vortragsanfragen nimmt sie selbstverständlich gerne entgegen. Auch in eigener Sache, nicht nur als Digitalcourage-Teammitglied.

Erhältlich im Digitalcourage-Shop!
„#Kids #Digital #Genial
Das Lexikon von App bis .zip“

Soft- und Hardcover (2,45 / 12 Euro)
https://shop.digitalcourage.de

Informationssicherheit in München

Hartmut Goebel

„Daten sind nichts wert“, erklärt Hartmut Goebel. „Erst die Information, das Wissen, das entsteht, wenn man Daten zu einer Geschichte kombiniert, machen Daten wertvoll.“ Und deshalb nennt er sich auch „Experte für Information Security“ und nicht einfach „Datenschützer“. Der gelernte Diplom-Informatiker berät hauptberuflich als Selbständiger Firmen zu ihren IT-Sicherheitskonzepten.

„Daten alleine sind überhaupt nichts wert.“

Er ist der Mitbegründer der Digitalcourage-Ortsgruppe München. Mit seinem Technik-Wissen bereichert er außerdem die Arbeitsgruppe „Digitale Selbstverteidigung“ (ab Seite 109 in diesem Jahrbuch) und bringt sich von seinem Wohnort Landshut aus online ein. Sein Einstieg bei Digitalcourage war dann auch ein Buchbeitrag über Datenschutz beim Freihandelsabkommen TTIP, den er über Telefon- und Onlinekontakte zusammen mit Rena Tangens geschrieben hat. „Aber irgendwann muss man sich dann auch endlich mal persönlich kennen lernen“, sagte er sich, nahm seine beruflich bedingte Bahncard 100 und fuhr 2013 unangekündigt zu einer Digitalcourage-Aktion vor den Berliner Reichstag. Rena Tangens

Foto: Digitalcourage, cc by-sa 4.0

hat noch gut vor Augen, dass da „so ein großer Typ kam mit einen Schild „Unternehmer gegen Vorratsdatenspeicherung“, den kannten wir nicht. Und dann stellte sich raus: Das war Hartmut.“

„Unternehmer gegen Vorratsdatenspeicherung“

Seitdem nutzt er jede Gelegenheit für den persönlichen Kontakt zum Team in Bielefeld. Er ist bei den regelmäßigen wöchentlichen Arbeitstreffen nach Möglichkeit per Telefon dabei, nimmt an Team-Wochenenden teil und liest eifrig im Intranet nach, was in Bielefeld besprochen und beschlossen wurde. „Bielefeld ist quasi der Think Tank, auch wenn ich das Wort ganz furchtbar finde. Aber wir hier vor Ort können ehrenamtlich gar nicht die ganze politische Bühne und Entwicklungen im In- und Ausland im Blick haben, um Haltungen oder Kampagnen zu entwickeln. Das passiert in Bielefeld. Wir nehmen dann aber die Impulse auf und setzen sie in der Ortsgruppe München in Aktionen um. So wie im September 2017, als wir uns zu zweit mit einem Schild vor der ZITiS (Zentralstelle für Informationstechnik im Sicherheitsbereich, diese Behörde soll den Staatstrojaner entwickeln) postiert haben.“

“Wir sind ein kleines, aber sehr starkes Kernteam hier in München.“

Zusammen mit einer weiteren Aktivistin stand Hartmut eineinhalb Stunden lang im Regen, um der Presse und dem Innenminister zu erklären, dass die Hacking-Behörde ZITiS ein Risiko für die Sicherheit von Bevölkerung, Infrastruktur und Unternehmen ist. Da in Bayern eine Zusammenkunft schon ab zwei Personen unter das Versammlungsgesetz fällt, wurde die Mini-Demo offiziell von der Polizei aufgelöst.

„Digitalcourage bringt das auf den Punkt und in einen politischen Zusammenhang, was ich meinen Kunden jeden Tag erzähle“, freut sich Hartmut. Solche Diskussionen haben bei seinen Auftraggebern wenig Raum, dort ist er Berater, entwickelt Konzepte oder programmiert Lösungen. Aber die Digitalcourage-Aufkleber auf seinem Laptop lösen hin und wieder Rückfragen aus, die er dann gerne in der nächsten Kaffeepause beantwortet.

„Als ich nach etwas gesucht habe, wo ich mich engagieren kann, war es ein großer Pluspunkt für Digitalcourage, dass sie Hauptamtliche haben. Wenn man in Bielefeld anruft und Flyer oder anderes Material anfordert, ist das am nächsten Tag per Express in München. Das können kleinere Organisationen einfach nicht leisten“, lobt er das Team in Bielefeld. Und fügt augenzwinkernd hinzu: „Und dann wieder brauchen Mini-Entscheidungen erstaunlich lange. Wenn ich überlege, wie lange ich quengeln musste, bis für 100 Euro eine Telefon-Spinne angeschafft wurde, damit Externe bei den Teamsitzungen teilnehmen können – das hat Monate gedauert!“

Foto: Digitalcourage, cc by-sa 4.0

Mini-Demo vor der ZITiS. Diese Behörde soll den Staatstrojaner entwickeln.

Die Ortsgruppe München trifft sich alle 8-10 Wochen bei einem Italiener. Termine kann man unter ortsgruppe@muenchen.digitalcourage.de anfragen, wenn man gerne mitmachen möchte. Regelmäßige, häufigere Treffen schaffen sie alle aus beruflichen Gründen nicht. „Wir sind ein kleines, aber sehr starkes Kernteam“, freut sich Hartmut. Und neben einer erstaunlichen Anzahl von Terminen wie Cryptocafés, Lesungen und Vorträgen planen sie regelmäßig weitere Aktionen, wie z.B. die Kartierung von Videokameras in der Münchner Innenstadt. „Auslöser war, dass Lisa aus unserer Gruppe vom Bayerischen Rundfunk eingeladen war, dem bayerischen Innenminister im Fahrstuhl Fragen zu stellen. Und er sagte dort, dass es keine privaten Videokameras im öffentlichen Raum in München gäbe. Da haben wir eine Aktion draus gemacht und Leute eingeladen, mit uns die Kameras zu fotografieren und in OpenStreetMap einzutragen. Solche Aktionen brauchen wir mehr, damit wir auch Menschen ohne großes Fachwissen in die Arbeit für Bürgerrechte einbinden können. Niedrigschwellig aktiv sein können, das ist super.“

Stolz ist Hartmut darauf, dass München die erste Ortsgruppe von Digitalcourage war. „Wir haben damit sicher den Weg geebnet für andere. Die Entscheidung war für die Bielefelder nicht leicht, denn wir geben ja auch Interviews oder vertre-

ten Digitalcourage in Bayern bei Podiumsdiskussionen, das muss schon ein großes Vertrauen herrschen, dass wir hier keine Alleingänge machen."

Zum 30. Geburtstag von Digitalcourage haben die Münchner sich etwas ganz besonderes ausgedacht: Sie waren Bergwandern und haben ein Banner von Digitalcourage auf einem 2.590 Meter hohen Gipfel ausgerollt (siehe Rückseite dieses Jahrbuchs). Im Reisebericht heißt es: „Unterlegt mit feinsten Tiroler Spinat-, Speck- und Käsknödel ließen wir Digitalcourage mit vielen Bieren hochleben", und Rena Tangens wurde per Video auf der „Bielefelder Hütte" zugeschaltet. (Der Livestream von der Alm zurück nach Bielefeld hat leider nicht funktioniert.)

„Wir haben auf dich gewartet!"

Andrea Neunzig

Es ist rund 15 Jahre her, dass Andrea sich aufmachte, Rena Tangens und padeluun kennen zu lernen. „Das erste Mal sind sie mir aufgefallen in einem Zeitungsartikel in der Bielefelder „Neuen Westfälischen", da haben sie ein Interview gegeben und gesagt, sie wollen die Welt verbessern. Der Satz hat mich berührt. Dann habe ich ein Interview in der „Zeit" gelesen, da wusste ich, die beiden sind relevant. Deshalb besuchte ich 2004 eine ihrer Veranstaltungen der Reihe „Public Domain" im Bunker Ulmenwall. Sehr beeindruckend! Mir wurde damals bewusst, dass die Themen Datenschutz, Bürgerrechte sowie die Diskussionen um Sicherheit und Freiheit zukünftig wichtiger werden würden und ging einfach mal zu einem Arbeitstreffen."

Wie der Zufall es wollte, fiel dieses Arbeitstreffen aber aus. Stattdessen saßen Rena Tangens und padeluun in ihrem Büro, weil sie das Gefühl hatten, „diese Andrea, die uns im Bunker angesprochen hat, die kommt heute." Und so wurde Andrea freundlich und exklusiv begrüßt mit dem Satz „Wir haben auf Dich gewartet." Und da wußten Rena Tangens

Foto: Bernd Sieker, cc by-sa 4.0

2016 verlas Andrea den Gastbeitrag zum „Neusprech-Award" für das Wort „Datenreichtum" bei der BigBrotherAwards-Gala.

Foto: Fabain Kurz, cc by-sa 4.0

und padeluun noch nicht, was für einem Multi-Talent sie die Hand reichten.

Als Betriebswirtschaftlerin mit einem Schwerpunkt in Wirtschaftsgeschichte wollte Andrea ihr Wissen gerne einer Non-Profit-Organisation zur Verfügung stellen. So bot sie als erstes an, einen Blick auf die Finanzen zu werfen. Finanzplanung gab es bis dahin noch nicht beim FoeBuD e.V., wie Digitalcourage vor 2012 hieß. Wenn sie an diese Zeit denkt, muss sie grinsen: „padeluun hat mir irgendwann gesagt, durch mich hätte er verstanden, dass Planung nichts Statisches, Passives ist, sondern ein sehr bewegliches Instrument, mit dem man Orientierung bekommt und gegensteuern kann, wenn es Abweichungen gibt." Ein paar Jahre lang hat sie das gemacht, dann kam eine andere Fachfrau und Andrea hatte Raum für neue Aufgaben. „Das war völlig okay für mich, mit Zahlen habe ich in meinem Job bei der Stadt Bielefeld eh schon genug zu tun."

„Nach dem BBA ist vor dem BBA!"

So stürzte sich die Mutter von zwei Kindern mit all ihrem Organisationstalent auf die BigBrotherAward-Galas. „Das ist viel Vorbereitung, auch langfristig. Die Bühne muss bespielt werden, die Ehrenamtlichen

müssen rechtzeitig angesprochen werden, Keynotes (Eröffnungsvorträge) müssen häufig ein Jahr im Voraus angefragt werden, sonst haben die Expertinnen und Experten zum BBA-Termin keine Zeit.“ Deshalb hält Andrea das Motto „Nach dem BBA ist vor dem BBA“ bei Digitalcourage hoch. „Ich habe mich da mehrere Jahre sehr intensiv eingebracht und viel Energie reingesteckt. Seit wir Nils als ausgebildeten Veranstaltungskaufmann haben, kann ich mich aber mehr aufs Inhaltliche konzentrieren. Die Organisation von Auf- und Abbau, Terminplanung usw. hat Nils bestens im Griff.“

▶„Es geht ja eigentlich gar nicht „nur“ um Datenschutz, das ist viel zu kurz gedacht.“◀

Voll einsteigen in Themen, in die Verantwortung gehen, das kann Andrea wirklich gut. Und wieder aussteigen und abgeben. Das ist eine besondere Qualität, das können nicht viele.

„Ich lese sehr viel, gehe ins Theater, aus der Kultur entwickle ich meine Haltungen und Ideen, auch politisch“, beschreibt sie sich selbst. „Es geht ja eigentlich gar nicht „nur“ um Datenschutz, das ist viel zu kurz gedacht. Es geht um die Zukunft unserer Wirtschaftssysteme, um Fragen unseres Zusammenlebens. Wenn Frau Merkel sagt, die Menschen müssten für ihre Daten etwas bekommen, dann macht sie damit aus dem Persönlichkeitsrecht „Informationelle Selbstbestimmung“ ein Eigentumsrecht, das man verkaufen kann. Das hat Auswirkungen auf die Art, wie wir zusammen leben.“ Zu solchen Fragen liest sie viel, macht sich schlau und gibt dieses Wissen intern bei Digitalcourage weiter. Zum Beispiel, als padeluun 2013 auf der BigBrotherAwards-Bühne rief: „Google muss zerschlagen werden!“, da hat Andrea sich in Kartellrecht eingelesen. „Kartell- und Wettbewerbsrechtler könnten wichtige Bündnispartner für Digitalcourage sein, auch wenn sie auf den ersten Blick wenig mit Bürger- und Menschenrechten am Hut haben“, hat sie dabei festgestellt.

▶„Es geht um die Zukunft unserer Wirtschaftssysteme.“◀

„Ich bin jetzt 57, und ich habe es über all die Jahre als sehr tröstlich empfunden, zu sehen, dass so viele hochintelligente, humorvolle, engagierte junge Erwachsene ihre unterschiedlichen Fähigkeiten bei Digitalcourage einsetzen, um die Welt ein bisschen besser zu machen. Als „Elder States Woman“ kenne ich sehr viele Weggefährten von Digitalcourage und kann neue Menschen gut ansprechen. In der Rolle fühle ich mich ausgesprochen wohl“, sagt sie, und muss wieder lächeln.

Ist ein Ende ihres Engagements für Digitalcourage in Sicht? Sie reißt erschrocken die Augen auf. „Was? Nein! Die Arbeit wird doch immer wichtiger!“

Foto: Digitalcourage, cc by-sa 4.0

Der Statue auf den Code geschaut

Foto: Justus Holzberger, cc by-sa 4.0

Das erste Mal im „großen Haus“: BBAs im Stadttheater Bielefeld

Von Claudia Fischer

Die Bühne in ihrer ganzen Pracht: Nicht nur breit, sondern auch tief! Musik: Kristin Shey Quartett

Was waren wir aufgeregt im Vorfeld! Vor einem Jahr hatte die „BBA-Crew“, wie das Aufbau-Team der BigBrotherAwards intern heißt, das Fazit gezogen: „2017 war das bisher beste Jahr mit den BigBrotherAwards in der Bielefelder Hechelei. Jetzt kennen wir uns aus und alles läuft wie am Schnürchen.“ Doch es sollte das letzte Jahr dort gewesen sein. 2018 fanden die BigBrotherAwards im „Großen Haus“ des Stadttheaters – mitten in Bielefeld, direkt neben dem Rathaus – statt. Und das Team hatte großen Respekt vor dieser neuen, wirklich anspruchsvollen Aufgabe.

Entstanden war die Idee im Dezember 2017 nach der Premiere des „satirischen Jahresrückblicks“, bei dem Rena Tangens mit dem Kabarettisten Ingo Börchers auf der Bühne war. Bei der anschließenden kleinen Feier verabredete Rena Tangens mit dem Theaterintendanten Michael Heicks, mit den BigBrotherAwards in das große Haus des Stadttheaters umzuziehen. Dort gibt es nicht nur mehr als 600 Plätze, sondern auch ganz anderes Flair. Diesen Ort zu bespielen war eine ganz große Herausforderung!

Für die Aufbau-Crew von Digitalcourage gab es im Theater einerseits weniger zu tun, denn die beeindruckende Tontechnik stand bereit, Stühle mussten nicht aufgebaut werden, Beamer und Beleuchtung des Theaters waren fest installiert und wurden von den professionellen Mitarbeiter.innen des Theaters eingerichtet und bedient. Wir hatten deutlich weniger Material zu bewegen: Statt einen Sprinter zu mieten, zu be- und entladen, konnte unsere gesamte Ausrüstung, bis hin zu den T-Shirts für den reich gefüllten Shop-Tisch mit zwei Handkarren aus dem Digitalcourage-Büro in der Marktstraße 300 Meter weiter ins Theater befördert werden.

Trotzdem geriet unsere Crew ganz gut ins Schwitzen. Zum einen war es Ende April in Bielefeld 30 Grad heiß und ab Nachmittags waren die nach Westen ausgerichteten Räume für den traditionellen Sektempfang, den Videostream und die Web- und Bildredaktion enorm aufgeheizt. Zweitens lagen diese Räume auf mehreren Stockwerken verteilt, und die Treppen in dem alten Jugendstil-Theaterbau werden immer ein bisschen länger, wenn man zum zehnten Mal rauf oder runter läuft.

„Allein bis wir die Wege hinter den Kulissen gefunden haben, hatte wohl jeder mehrfach versucht, verschlossene Türen zu öffnen“, grinst unser Aufbauprofi Nils Büschke noch heute. „Aber die Theater-Leute waren einfach großartig! Alle waren unglaublich freundlich, hilfsbereit und immer gut gelaunt – es hat echt super Spaß gemacht, mit ihnen zusammen zuarbeiten!“ Das fanden die Theaterleute auch. Unsere Gäste waren begeistert, das Stadttheater war quasi ausverkauft und der neue Ort bescherte den BigBrotherAwards viel neues Publikum.

Und so gibt es auch 2019 wieder eine BigBrotherAwards-Gala „im großen Haus“. (Termin: 8.6.2019, bitte vormerken!)

Foto: Fabian Kurz, cc by-sa 4.0

Die Jury der BigBrotherAwards 2018

Von links nach rechts:

- **Dr. Rolf Gössner**, ILMR. Die Internationale Liga für Menschenrechte e.V. (ILMR) ist eine traditionsreiche unabhängige und gemeinnützige Nichtregierungsorganisation, die sich im Geiste von Carl von Ossietzky für die Verwirklichung und Erweiterung der Menschenrechte und für Frieden einsetzt.
- **Dr. Thilo Weichert**, DVD, Netzwerk Datenschutzexpertise. Die Deutsche Vereinigung für Datenschutz e.V. (DVD) ist eine unabhängige Bürger.innenrechtsvereinigung, 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.
- **Prof. Dr. Peter Wedde** ist Professor für Arbeitsrecht und Recht der Informationsgesellschaft an der Fachhochschule Frankfurt a.M., Direktor der Europäischen Akademie der Arbeit an der Universität Frankfurt a.M., sowie Herausgeber und Autor.
- **Rena Tangens**, Digitalcourage
- **padeluun**, Digitalcourage

Kategorie Arbeit

Die Firma Soma Analytics für ihre Gesundheits-App „Kelaa“

Von Prof. Dr. Peter Wedde

Der BigBrotherAward 2018 in der Kategorie Arbeit geht an die Soma Analytics UG aus Bruckmühl bei München, vertreten durch ihren Geschäftsführer Johann Huber, für ihre Bemühungen, die Gesundheits-App „Kelaa“ bei Beschäftigten und das zugehörige „Kelaa Dashboard“ in Personalabteilungen von Firmen zu platzieren. Gesundheitsdaten von Beschäftigten in die Hände von Arbeitgebern zu legen ist ein Tabubruch. Aber der Reihe nach:

Foto: Matthias Hornung , cc by-sa 4.0

Laudator: Prof. Dr. Peter Wedde, Arbeitsrechtler

Die Kelaa-App überwacht, wie viele andere Gesundheitsapps, die Vital-Daten der Nutzerinnen und Nutzer. Vor Gesundheitsapps warnen wir seit Jahren. Soma Analytics führt unsere Kritik aber in eine neue Dimension. Die von dieser Firma entwickelte Kelaa App kann zwar jeder auf sein Smartphone laden. Sie funktioniert aber nur, wenn der Arbeitgeber über die Software „Kelaa Dashboard“ verfügt. Mit dieser Software können sich die Arbeitgeber die aktuellen Stress- und Vitalwerte ihrer Beschäftigten in (Zitat) „aggregierter und anonymisierter Form“ anzeigen lassen. Die entsprechenden Auswertungen stellt Soma Analytics bereit.

Dieses Dreieck dient „natürlich“ nur der besseren Gesundheit: Beschäftigte, die die Kelaa App auf ihrem Smartphone installiert haben, bekommen z. B. Hinweise für Entspannungstechniken, wenn die App Anzeichen für Stress wahrnimmt. Und Arbeitgeber erfahren, wie gestresst ihre Mitarbeiter sind. Ob sie das nutzen, um Arbeitsbedingungen zu verbessern, oder um Mitarbeiter.innen mit „schwachen Nerven“ einfach zu entlassen, darüber kann nur spekuliert werden.

Die Funktionsweise

Erfasst werden die sensitiven personenbezogenen Daten über das Smartphone, das zentrales Arbeitsmittel und Tagesbegleitung ist. Von vielen Menschen wird dieses Gerät von morgens zum Aufwecken bis abends zum Einschlafen verwendet. Wer die dort vorhandenen Gesundheitsdaten oder „Stressinformationen“ auslesen und auswerten kann, der weiß mit hoher Wahrscheinlichkeit mehr über den psychischen und physischen Zustand des Besitzers als dieser selbst.

Wer Stressinformationen auswertet, weiß wahrscheinlich mehr über den Nutzer als dieser selbst.

Aber das reicht Soma Analytics nicht: Die Firma weitet den Sammelzeitraum für sensitive Daten durch die Aufforderung aus, das Gerät zur Erfassung von Bewegungen während des Schlafs direkt mit ins Bett zu nehmen. Damit kann das Unternehmen nicht nur Erkenntnisse zum Schlafverhalten sammeln, sondern nebenbei auch noch zum Beischlafverhalten. Ob Partner von Beschäftigten dies mögen und erlauben, mag an dieser Stelle dahingestellt sein.

Weiterhin werden Gefühlsregungen der Stimme beim Telefonieren ausgewertet. Ergänzt wird das Ganze durch Antworten auf Fragen, die Beschäftigten gestellt werden (“Self-assessment Fragebogen”).

In Veröffentlichungen zur Kelaa-App ist davon die Rede, dass die Soma-Software auch das Schreib- bzw. Tippverhalten sowie die Nutzung des Smartphones selbst auswertet. Dabei wird etwa die Häufigkeit des Griffs zum Gerät durch Beschäftigte ebenso erfasst wie die Dauer des Blicks auf den Bildschirm.

Ob darüber hinaus auch andere Datenquellen genutzt werden, wie etwa der Schrittzähler in einer anderen Gesundheits-App, oder ob Gespräche auch

Foto: Maik Meid, cc by-sa 4.0; Grafik: Dennis Blomeyer, cc by-sa 4.0

Nie ohne Smartphone!

Bild: Panthermedia, Grafik: Dennis Blomeyer, cc by-sa 4.0

Kann der Arbeitgeber wirklich keine einzelnen Mitarbeiter.innen aus dem Kelaa-Datenmaterial identifizieren?

außerhalb von Telefonaten abgehört und ausgewertet werden, ist nicht bekannt. Aufgrund der rechtlichen Hinweise auf der Website wären auch solche Datensammlungen grundsätzlich nicht ausgeschlossen. Und uns würde es eher überraschen, wenn Soma dieses Informationspotential nicht berücksichtigen würde.

▶Der Effekt für Arbeitnehmer.innen...

Dafür verspricht Soma Analytics den Beschäftigten viel: Kelaa wird wie eine „gesundheitsfördernde Wunderwaffe“ angepriesen: „Wenn ihr die Kelaa-Apps einsetzt, werdet ihr leistungsfähiger als je zuvor und macht dabei euren Arbeitgeber auch noch durch eine erhöhte Produktivität glücklich!“ Da fehlt eigentlich nur noch das Versprechen von besserem Haarwuchs.

Nicht erwähnt werden von Soma Analytics mögliche Risiken und Nebenwirkungen für die Beschäftigten, weil sie – zu Recht – das Gefühl haben, dass ihr Arbeitgeber sie permanent beobachtet, sogar zu Hause und im Schlaf. Nach dem Motto: Feierabend ist ein völlig veraltetes Konzept.

▶... und der Effekt für Arbeitgeber.innen

Soma verspricht auch den Arbeitgeberinnen und Arbeitgebern viel: Der Einsatz des Kelaa Dashboards soll ihre Entscheidungsfindung stärken. Sie sollen mit den Soma-Daten die Bereiche identifizieren, in denen Verbesserungsbedarf besteht, um mit der Gesundheit der Beschäftigten auch deren Produktivität zu verbessern.

Wir sagen: Soma Analytics versucht, Arbeitgebern die Rundumkontrolle des physischen und psychischen Befindens ihrer Beschäftigten zu ermöglichen. Dass dieses Angebot Arbeitgeber begeistert und auf neue Ideen bringt, zeigen erste Erfahrungen aus Großbritannien, wo Kelaa in einer großen Anwaltskanzlei mit über tausend Mitarbeitern eingesetzt wird. Dort hat der für die Nutzung der Kelaa-App zuständige Mitarbeiter festgestellt: „Die App zeigt uns die Potentiale auf, die wir realisieren können, wenn wir mit unseren Mitarbeitern zusammen an ihrem Schlaf arbeiten“. Derartiges möglich zu machen, ist ohne Einschränkung auszeichnungswürdig.

Soma Analytics verwendet nach eigenen Angaben Big Data und anspruchsvolle Algorithmen. Außerdem führt Soma Analytics an, dass sie durch weltweit führende Forscher aus den Bereichen Psychologie, medizinische Schlafforschung und Informatik unterstützt wird. Die Namen dieser renommierten Forscher werden allerdings diskret verschwiegen. Und natürlich wird auch der Aufbau des für die Auswertungen verwendeten Algorithmus nicht erläutert.

▶Firmengeheimnisse

Vielleicht sind das Firmengeheimnisse, genau wie die Art der Aggregierung und Anonymisierung der von den Smartphones der Beschäftigten gesammelten Daten für die Ausgabe im Dashboard. Wie anonymisiert wird und wie sicher das hierfür verwendete Verfahren ist, darüber gibt es auf der Webseite keine Informationen. Wir werden aber misstrauisch, wenn Soma Analytics gleichzeitig die Möglichkeit anpreist, besonders stressige Abteilungen in ihren Betrieben zu identifizieren. Daraus lässt sich folgern, dass Informationen sich auf kleinere Einheiten, Abteilungen oder Personengruppen einer Firma beziehen lassen. Und dann ist unter Umständen der Weg zur Identifikation eines bestimmten Mitarbeiters oder einer bestimmten Mitarbeiterin nicht mehr weit.

▶Datenschutzrechtliche Grundlagen sind nicht erkennbar.◀

Eindeutige datenschutzrechtliche Grundlagen für die Auswertungen sind nicht erkennbar. Soma Analytics räumt sich durch die Rechtshinweise auf seiner Website zwar weitgehende Verarbeitungsbefugnisse ein. Im deutschen Rechtsraum wäre aber erforderlich, dass die Beschäftigten dieser Verarbeitung auch zustimmen. Dies fordert das (gerade) noch geltende Bundesdatenschutzgesetz. Auch aus dem Disclaimer zur Kelaa-App folgt keine datenschutzrechtlich wirksame Einwilligung von Beschäftigten in die Verarbeitung sensitiver personenbezogener Daten. Aber auch mit Blick auf die ab dem 25. Mai 2018 anwendbare Europäische Datenschutzgrundverordnung (DSGVO) und die hierin enthaltenen Wirksamkeitsanforderungen einer Einwilligung ist die Situation nicht anders zu bewerten. Im Gegenteil: sowohl das alte wie auch das neue Datenschutzrecht schützen die Verarbeitung von Gesundheitsdaten ganz besonders. Und noch einmal höher ist dieser Schutz bezogen auf Beschäftigungsverhältnisse.

▶Verbreitung

Wir wissen nicht, wie erfolgreich das Geschäftsmodell von Soma Analytics ist. Berichte über die praktischen Erfahrungen beziehen sich auf Beispiele aus Großbritannien und Italien, obwohl der Hauptsitz der Firma in Bruckmühl bei München ist. Über die Verbreitung bei deutschen Arbeitgebern ist uns nichts bekannt – darum geht es uns aber auch nicht.

Unabhängig vom Standort, unabhängig von der Marktmacht, unabhängig von der Größe der Firma ist es der Gedanke hinter

Links und weitere Infos: digitalcourage.de/jahrbuch19

der Kelaa App, der den Tabubruch darstellt. Warum entwickeln Menschen solche Software? Weil sie kein Gespür für moralische Grenzen haben. Weil „Digital first, Bedenken second“ als Werbeslogan der FDP im vergangenen Herbst genutzt wurde und in gewissen Kreisen gesellschaftsfähig ist. Weil Datenschutz nicht als deutsche Tugend und als deutscher Exportschlager angesehen wird, sondern als Behinderung von Geschäftsmodellen. Und weil viele kleine Start-Ups davon träumen, von einem Weltkonzern aufgekauft zu werden, wenn sie aus Big Data so viel wie möglich herausholen können. Da werden laufend rote Linien überschritten – und das muss aufhören!

▶…weil sie kein Gespür für moralische Grenzen haben.◀

Denn die Debatte um Kelaa trifft zusammen mit der um den Einsatz von Anwendungen aus dem Bereich „Predictive Analytics“. Diese zielen ebenfalls darauf ab, aus der Stimme oder aus dem sonstigen Umgang von Beschäftigten mit technischen Anwendungen Hinweise auf sich anbahnende Probleme oder auf das Vorliegen eines arbeitsrechtlichen Fehlverhaltens abzuleiten. Werden derartige Konzepte der permanenten und verdeckten automatisierten Ausforschung von Beschäftigten Praxis, schafft dies Erkenntnis- und Handlungsmöglichkeiten für Arbeitgeber, von denen Big Brother bisher nur träumen konnte.

Wenn Sie als Beschäftigte meinen, dass es Ihrer Gesundheit förderlich ist, auf Ihrem Smartphone eine App zur Stresserkennung und Stressreduzierung zu installieren, dann steht es Ihnen natürlich frei, dies zu tun. Aber achten Sie darauf, dass es keine Software ist, die ihrem Arbeitgeber gehört. Wer diese simple Grundregel beachtet, der muss auch keinen Ausschlag des „Stress-O-Meters“ in seiner App befürchten, wenn der Arbeitgeber wieder einmal davon redet, dass er olympiareife Mannschaften braucht und dass deshalb die nicht so leistungsfähigen Beschäftigten das Boot verlassen müssen.

▶ In diesem Sinne: Herzlichen Glückwunsch zum BigBrotherAward Soma Analytics UG.

Wie es weiter ging

Von Claudia Fischer

Kommentare unseres Publikums:

▶ „Im jetzigen System ist Arbeit für viele unabdingbar, deshalb ist ein Eingreifen in die Freiheit des Menschen in diesem Raum absolut nicht in Ordnung.“

▶ „Die Informationen des „Schwächeren“ werden an den „Mächtigeren“ blanko abgetreten.“

▶Die Firma Soma Analytics hat einen Brief geschrieben:

Genauer gesagt hat Geschäftsführer Johann Huber den Brief auf der Soma-Webseite veröffentlicht (den Link finden Sie auf der Jahrbuch-Webseite, siehe unten). Er erklärt darin, dass die Idee entstand, als ein Freund an einer arbeitsbedingten Depression erkrankte. Daraufhin habe er mit einem Kollegen die App entwickelt, um „Arbeitnehmern, Konzernlenkern und Unternehmern ein validiertes Werkzeug an die Hand zu geben, um stressbedingte Erkrankungen Vergangenheit werden zu lassen. ... Sorgsam erhobene Daten sind dazu unerlässlich. Es steht außer Frage, dass dies im Einklang mit bestehenden und neuen Datenschutzrichtlinien und -gesetzen erfolgen muss.“

Deshalb seien sie von der Stimmanalyse durch die Kelaa-App inzwischen auch wieder abgerückt. Die Texte auf der Webseite, in denen davon die Rede war, seien veraltet – dies werde er unverzüglich nachbessern. Sämtliche Hinweise in den Datenschutzerklärungen sind inzwischen verschwunden, lediglich ein Blog-Eintrag „Voice Analysis Added to Kelaa Mental Resilience“ aus dem Juli 2017 ist zum Zeitpunkt der Drucklegung dieses Jahrbuches immer noch online zu finden.

Sie wären gerne persönlich gekommen, schreibt Herr Huber weiter, unsere Einladung sei – wie unsere Recherchen – aber sehr kurzfristig gewesen. Die Statue könnten wir gerne ins Büro nach London schicken. „Wir würden den Pokal in unserem Büro aufstellen als Erinnerung für unsere Mitarbeiter, dass Datenschutz weiterhin absolute Priorität ist.“

Das Smartphone ist allgegenwärtig – ausgestattet mit Stimmanalyse-Technologie wird das richtig gruselig.

Foto: cc0, Bearbeitung: Dennis Blomeyer, cc by-sa 4.0

▶„…mit ihren Angestellten an deren Schlafverhalten arbeiten…“◀

Laudator Peter Wedde: „Was Herr Huber offensichtlich nicht verstanden hat, ist, dass wir mit diesem BigBrotherAward **einen Tabubruch** ausgezeichnet haben. Den Tabubruch, dass nach den Plänen von Soma Gesundheitsdaten in personenbeziehbarer Form mit dem Arbeitgeber geteilt werden – Anonymisierung funktioniert hier nämlich nur bedingt. Dass Premium-Anwender der Kelaa-Software werbewirksam und ohne Widerspruch durch Soma überlegen dürfen, ob eine Firma „mit ihren Angestellten an deren Schlafverhalten arbeiten“ könne, geht einfach zu weit.

Wir haben die Statue nicht nach London versendet. Wir übergeben Originale nur, wenn ein Preisträger sich während oder nach der Preisverleihung einem persönlichen Gespräch mit uns stellt. Übrigens schickt mir Soma Analytics seit der Laudatio regelmäßig Newsletter mit Seminarangeboten.

▶ Ich kann mich nicht erinnern, dem zugestimmt zu haben.“

Smombie-Grafik: Dennis Blomeyer, cc by-sa 4.0

Links und weitere Infos: digitalcourage.de/jahrbuch19

Kategorie PR & Marketing

Das Konzept der „Smart City“

Von Rena Tangens

Der BigBrotherAward in der Kategorie „PR & Marketing“ geht an das Konzept der **„Smart City“**. Das „Smart City“-Konzept propagiert die „Safe City“: die mit Sensoren gepflasterte, total überwachte, ferngesteuerte und kommerzialisierte Stadt. „Smart Cities“ reduzieren Bürger auf ihre Eigenschaft als Konsumenten, machen Konsumenten zu datenliefernden Objekten und unsere Demokratie zu einer privatisierten Dienstleistung.

Eine „Smart City“ ist die perfekte Verbindung des totalitären Überwachungsstaates aus George Orwells „1984“ und den normierten, nur scheinbar freien Konsumenten in Aldous Huxleys „Schöne Neue Welt“.

Der Begriff „Smart City“ ist eine schillernd-bunte Wundertüte – er verspricht allen das, was Sie hören wollen: Innovation und modernes Stadtmarketing, effiziente Verwaltung und Bürgerbeteiligung, Nachhaltigkeit und Klimaschutz, Sicherheit und Bequemlichkeit, für Autos grüne Welle und immer einen freien Parkplatz. Angefangen hat das 2008 mit IBM und ihrem Werbeslogan vom „Smarter Planet“, mit dem sie sagen wollten, dass sie unseren Planeten „schlauer“ machen können. Im Business tummeln sich inzwischen eine Menge weiterer Firmen, die ihre Dienstleistungen an Städte verkaufen wollen, zum Beispiel Siemens, Microsoft, Cisco, Huawei, Hitachi und Osram.

Foto: Fabian Kurz, cc by-sa 4.0

Laudatorin: Rena Tangens, Digitalcourage

▶Doch wie sieht so eine „Smart City“ konkret aus?

Als große Errungenschaft für eine „Smart City“ wird zum Beispiel ein neuer Typ Straßenlaterne angepriesen. Die leuchtet nicht nur, sondern enthält auch gleich Videoüberwachung, Fußgänger-Erkennung, Kfz-Kennzeichenleser, Umweltsensoren, ein Mikrophon mit Schuss-Detektor und einen Location-Beacon zum Erfassen der GPS-Position. Stellen wir uns dies noch kombiniert mit WLAN vor, mit dem die Position von Smartphones ermittelt werden kann, Gesichtserkennung und Bewegungsanalyse, dann ist klar: Wenn diese Technik in unsere Stadt kommt, werden wir keinen Schritt mehr unbeobachtet tun.

Foto Public Domain, Grafik: 4.0 Dennis Blomeyer, cc by-sa 4.0

Smarte Straßenlaternen können mit allerlei Überwachungssensorik ausgestattet werden (WLAN-Tracking, Gesichts- und Stimmanalyse, GPS, KFZ-Kennzeichenerfassung usw.)

„Mit der heutigen Technologie (...) können vollkommen sichere Städte gestaltet werden. Die neue Gesichtserkennungstechnologie ermöglicht es Regierungen und privaten Unternehmen, alle Gesichter zu erkennen und zu archivieren, während dies zuvor auf eingetragene Straftäter beschränkt war,“ schwärmt der türkische Überwachungstechnik-Anbieter Ekin in einer Pressemeldung über die „Safe City“. Das Gesichtserkennungssystem ordnet den Merkmalen jedes Gesichts eine ID zu, mit der eine Person später wiedererkannt werden kann, auch wenn ihr Name nicht bekannt ist, und analysiert außerdem Alter, Geschlecht und Ethnie.

Grafik: Dennis Blomeyer, cc by-sa 4.0

Was die „smarte“ Straßenlaterne alles kann: • Videoüberwachung • Fußgängererkennung • KFZ-Kennzeichenleser • Mikrofon • Schuss-Detektor • WLAN • Gesichtserkennung • Bewegungsanalyse

Foto: Kolja Quakernack, cc by-sa 4.0

Im chinesischen Shenzen zeigen Monitore per Gesichtserkennung an, wer gerade bei rot über die Ampel gegangen ist.

Während in Deutschland noch mit Begriffen wie Nachhaltigkeit, Umweltschutz, Effizienz und Bequemlichkeit für die „Smart City“ geworben wird, sprechen die Technologiefirmen in China, Dubai und der Türkei offen aus, um was es geht: Lückenlose Überwachung und Kontrolle der Bevölkerung.

In China boomt die Kombination von Videoüberwachung und Künstlicher Intelligenz.

Der chinesische Marktführer für Gesichtserkennungssoftware, SenseTime, freut sich über „*die hohe Nachfrage, die von Smart Cities und Überwachung angetrieben wird*“.

In Shenzhen, der südchinesischen Sonderwirtschaftszone in unmittelbarer Nachbarschaft zu Hongkong, werden Menschen, die bei Rot über die Straße gehen, identifiziert und sogleich auf großen Monitoren mit Angabe ihrer Personalien an den Pranger gestellt. Es wird ein Bußgeld berechnet und der Arbeitgeber benachrichtigt. Außerdem gibt es Punktabzug bei ihrem „Social Score“, der darüber entscheidet, ob sie eine Wohnung, einen Job, einen Studienplatz bekommen.

Die ganze Provinz Xinjiang im Nordwesten Chinas ist inzwischen ein Echtzeit-Labor für Massenüberwachung. Dort werden von der gesamten Bevölkerung zwischen 12 und 65 Jahren DNS und Blutgruppe getestet, Iris-Scans, Fingerabdrücke und 3D-Bilder erstellt – im Rahmen einer sogenannten „kostenlosen Gesundheitsuntersuchung“ (Quellenangaben finden Sie auf unserer Jahrbuch19-Webseite, s.u.). Dazu hat die chinesische Regierung 2017 in Xinjiang ein Überwachungssystem installiert, das die Polizei automatisch informiert, wenn ein Verdächtiger sich mehr als 300 Meter von seiner Wohnung oder seinem Arbeitsplatz entfernt. Verdächtig sind nicht nur Kriminelle, sondern auch Angehörige der muslimischen Minderheit oder Personen, die sich für Menschenrechte einsetzen.

Sie meinen, China ist weit weg?

Nun, am **Bahnhof Südkreuz in Berlin** testet die Bundespolizei seit August 2017 intelligente Videoüberwachung mit Gesichtserkennung. Das ist der Anfang. Denn völlig egal, wie der „Test“ ausgeht – Ex-Innenminister Thomas de Mazière hat schon zu Beginn dieses Freilandversuchs betont, dass Gesichtserkennung bundesweit an möglichst vielen öffentlichen Orten eingeführt werden soll. Und der neue Innenminister Horst Seehofer hat längst bestätigt, dass er das auch so sieht. Mehr noch: Die neue Bundesregierung hat in ihrem Koalitionsvertrag bereits eine Weiterentwicklung zu einer „intelligenten“ Videoüberwachung vorgemerkt. Geschmackvolle Straßenlaternen mit Überwachungskameras und Sensoren können Sie übrigens auch bereits in „Arcadia“, einer **Gated Community in Potsdam**, besichtigen.

Quelle: Twitter-Nutzer

„Nicht jeder lässt sich so gern überwachen wie Thomas de Maizière“

Oder schauen wir mal in unser direktes Nachbarland, nach Holland, wo die „Smart Cities“ wie Tulpen aus dem Boden

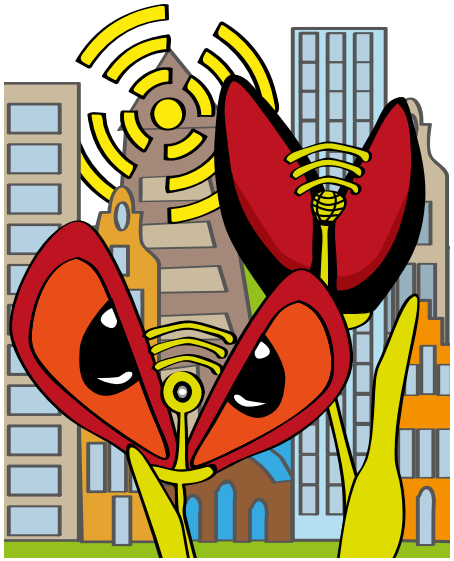
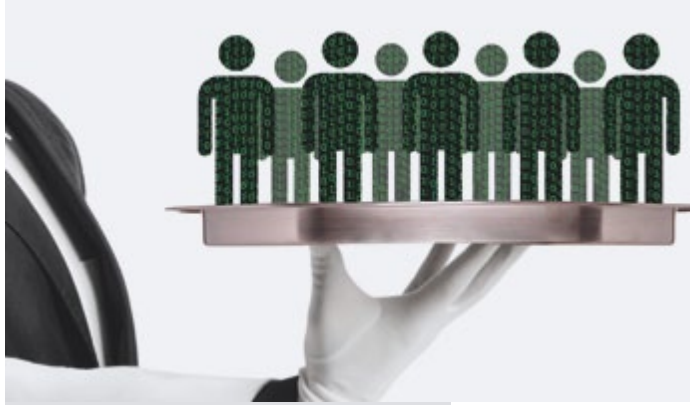


Illustration: Isabel Wienold, cc by-sa 4.0

sprießen: **Die Stadt Enschede** will wissen, wer sich wie oft wo lang bewegt und trackt dafür alle Menschen, die ein Smartphone mit aktiviertem WLAN bei sich tragen, mit Hilfe der eindeutigen MAC-Adresse. Die Traffic-App von Enschede belohnt Menschen für gutes Verhalten – zu Fuß gehen, Fahrrad fahren, öffentliche Verkehrsmittel nutzen – ironischerweise mit einem Tag freiem Parken in der Stadt. Was man erst im Kleingedruckten der App findet: Die gesammelten persönlichen Bewegungsprofile gehen an eine Firma namens Mobidot.

In **Eindhoven** ist die **Partymeile Stratumseind** zu einem Überwachungslabor geworden: Dort gibt es Straßenlaternen mit WLAN-Tracking, Kameras und Mikrophonen, mit denen aggressives Verhalten erkannt werden soll. Ab Frühjahr 2018 soll bei Bedarf Orangenduft versprüht werden, um die Menschen zu beruhigen.

Utrecht schließlich überwacht die Jugendlichen der Stadt, wenn sie sich in



Grafik: Dennis Blomeyer, cc by-sa 4.0

Mit „Smart Cities“ verscherbeln Lokalpolitiker den Unternehmen etwas, was ihnen nicht gehört: Die Privatsphäre ihrer Bürgerinnen und Bürger

den Straßen bewegen: Wie viele sind es? Welche Altersgruppe? Kennen sie sich? Wie gehen sie miteinander um? Und machen sie Ärger oder nicht? Seit 2014 hat Utrecht 80 „smarte“ Projekte in der Stadt und den Überblick verloren, was wo läuft, denn das meiste davon liegt in den Händen von Firmen.

▶Das ist weder clever noch smart, sondern kurzsichtig und gefährlich.◀

▶Firmengeheimnisse

„Smart City“-Firmen sammeln Daten und weigern sich, darüber Auskunft zu geben. Sie geben oft auch den Städten selbst keinen Zugriff auf die Daten – denn die sind Firmengeheimnis! Der Eindruck drängt sich auf, dass sich die Städte von den Firmen über den Tisch ziehen lassen. Doch das können weder Bürgerinnen und Bürger noch Presse überprüfen, denn die Verträge, die die Städte mit den „Smart City“-Dienstleistern abschließen, dürfen zumeist nicht eingesehen werden – aus Wettbewerbsgründen.

Ja, „smarte“ Technik ist teuer. Wo soll das Geld herkommen? Städte lassen sich von günstigen Einstiegsangeboten locken und von den Landes- und EU-Fördermitteln.

Städte werden wieder einmal verlockt, ihre Infrastruktur in kommerzielle Hände abzugeben – wie in den 90er-Jahren beim Cross-Border-Leasing. Das ist weder clever noch smart, sondern kurzsichtig und gefährlich.

Und es droht mehr als das billige Verscherbeln städtischer Infrastruktur: Städte verkaufen hier leichtfertig etwas, was ihnen gar nicht gehört, nämlich die Daten der Bürgerinnen und Bürger – und damit deren Privatsphäre, deren Autonomie und deren Freiheit.

Die Bürger werden nicht gefragt. Denn die Tech-Firmen wollen doch nur spielen – das kann man denen doch nicht übel nehmen! Bei innovativen Tech-Projekten müssen alle anderen Interessen schweigen: „Digital first, Bedenken second“. Das amerikanische Original heißt „Permissionless Innovation“, also „Innovation ohne Erlaubnis“. Das bedeutet: Das Vorsorgeprinzip wird außer Kraft gesetzt – wer behauptet, innovativ zu sein, muss sich nicht an lästige Regeln halten.

▶Das Schlaraffenland ist nicht das Paradies. Es macht satt, aber nicht glücklich.◀

Den Firmen ist klar: Nicht der Service, sondern die Daten der Bürgerinnen und Bürger sind die eigentliche Cash Cow. Wer wüsste das besser als Alphabet, Googles Mutterfirma. Die hat sich gerade im kanadischen **Toronto** eingekauft, um das dortige Waterfront Viertel als „Smart City“ zu entwickeln. Name des Projektes: **Sidewalk Labs**, also „Bürgersteig-Labor“. Google hat sich wohl nicht träumen lassen, wie viel Kritik und konkrete Nachfragen zu Datenschutz aus der kanadischen Bevölkerung kommen würden. Sidewalk Labs hat mittlerweile die ehemalige Datenschutzbeauftragte von Kanada, Ann Cavoukian, eingestellt. Smart Move. Ann Cavoukian hat 2009 das Konzept der „Privacy by Design“ entwickelt (also so etwas wie „eingebaute Privatsphäre“). „Smart Cities“ aber sind eher „Surveillance by Design“ (eingebaute Überwachung). Wir sind ehrlich gespannt, wie sie das Eine in das Andere bringen will, ohne das Geschäftsmodell von Google komplett umzukrempeln.

Doch wir wollen ja gar nicht so negativ sein. Denn eigentlich mögen wir Technik. Wir nehmen jetzt einfach mal an, dass die Hack-Sicherheit der vernetzten Systeme kein Problem wäre. Dass der Staat mit der Komplett-Überwachung ausschließlich unser Wohl im Auge hätte. Und dass die Tech-Firmen nur Gutes mit unseren Daten tun würden. Und jetzt stellen wir uns diese freundliche „Smart City“ vor, deren Sensoren uns ständig begleiten, die uns sagen, was wir als Nächstes tun sollen und deren Algorithmen aus unserem Profil in Echtzeit unsere Wünsche errechnen, bevor wir sie selber kennen. Immer grüne Welle, immer sofort einen Parkplatz finden und stets die aktuellen Stickoxid-Werte der Umgebung auf meinem Handy – klingt das nicht verlockend?

Im Märchen vom Schlaraffenland fliegen den Menschen die gebratenen Gänse essfertig in den Mund. Aber: Das Schlaraffenland ist nicht das Paradies. Es macht satt, aber nicht glücklich. Bequemlichkeit macht träge und dumm. Wir brauchen das Beinahe-Stolpern, um unseren Gleichge-

Bild: Screenshot

So präsentiert sich das Projekt „Sidewalk Labs“ in Toronto im Internet.

wichtssinn zu trainieren. Wir brauchen die Anstrengung, um uns über das aus eigener Kraft Erreichte zu freuen. Wir brauchen den Zufall, das Andere, das Unbekannte, die Überraschung, die Herausforderung, um zu lernen und uns weiterzuentwickeln. Wir müssen uns als Menschen frei entscheiden können und es muss uns möglich sein, Fehler zu machen. Wie anders sollten wir unseren „Moral-Muskel“ trainieren?

Auch deshalb müssen wir uns wehren gegen die Bevormundung durch Technik und Technik-Paternalismus.

Eine Stadt ist nicht „smart“ – klug sind die Menschen, die darin leben. Wir haben die Wahl: Wollen wir in einer post-demokratischen Konsumwelt leben, in der andere für uns entscheiden und die einzig mögliche Antwort „ok“ ist? Oder wählen wir die Freiheit?

Albus Dumbledore sagt in Harry Potter Band 4: „Es wird die Zeit kommen, da ihr euch entscheiden müsst zwischen dem, was richtig ist und dem, was bequem ist.“

- Die Zeit ist jetzt.
  Herzlichen Glückwunsch zum BigBrotherAward, „Smart City“!

Wie es weiter ging

Von Claudia Fischer

Kommentare unseres Publikums:

- „Dieser Preisträger hatte für mich den größten „Wow!“-Faktor – meine Kinnlade ist runtergefallen, im negativen Sinne!“
- „Meine Stadt soll gerade Smart City werden, wird als etwas ganz tolles von der Smart Factory „verkauft“ – ich wusste nicht, was kleine Annehmlichkeiten für Horrorfolgen haben können.“
- „Ich möchte mich bei Bewegung im Raum frei fühlen.“

Es geht um die Zukunft der Städte

Die Laudatio von Rena Tangens wird viel gelesen und diskutiert. So wurde zum Beispiel in einem Handlungsleitfaden „Schritte zur Einführung einer kommunalen Fußverkehrsstrategie“ im Juli 2018 vom FUSS e.V. aus der Laudatio zitiert. Rena Tangens spricht als Expertin und Rednerin auf Konferenzen zu „Smart Cities“ und digitaler Zukunft in Städten. Und sie arbeitet an einem Buch zum Thema, das 2019 erscheinen soll.

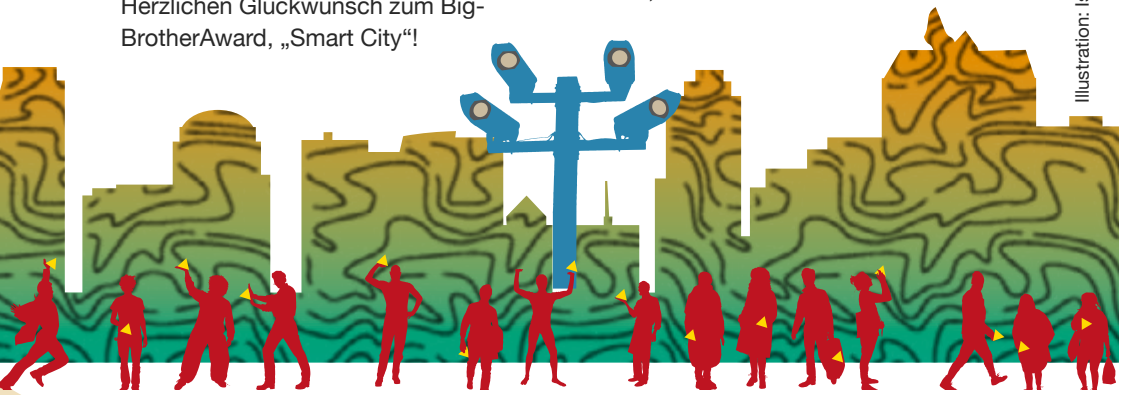


Illustration: Isabel Wienold, cc by-sa 4.0

Kategorie Behörden und Verwaltung

Die Cevisio Software und Systeme GmbH aus Torgau

Von Dr. Thilo Weichert

Der BigBrotherAward 2018 in der Kategorie Behörden und Verwaltung geht an die **Cevisio Software und Systeme GmbH aus Torgau** für ihre **Software „Cevisio QMM“** (Quartiermanagement), die in Zusammenarbeit mit dem Deutschen Roten Kreuz speziell für Flüchtlingsunterkünfte entwickelt wurde. Mit dieser Software werden Bewegungen zum und auf dem Gelände, Essenausgaben, medizinische Checks wie durchgeführte Röntgen-, Blut- und Stuhluntersuchungen, Verwandtschaftsverhältnisse, Religions- und Volkszugehörigkeiten und vieles mehr erfasst und gespeichert. Die Daten ermöglichen eine Totalkontrolle der Flüchtlinge und zeigen anschaulich, auf wie vielen Ebenen Privatsphäre verletzt werden kann.

Laudator: Dr. Thilo Weichert, Deutsche Vereinigung für Datenschutz

Foto: Fabian Kurz, cc by-sa 4.0

Die Software ist nicht nur preiswürdig wegen der mit ihr möglichen Datenschutzverstöße, sondern vor allem wegen des Menschenbildes, das dahinter steht. Flüchtlinge sind Menschen, keine Sachen. Sie liegen nicht in einem Regal zur späteren Abholung und Verwendung, sie sind keine Gefangenen und bedürfen keiner verschärften Beobachtung. Sie suchen Schutz bei uns und haben Rechte – Menschenrechte und Grundrechte, die für Cevisio keine Rede wert sind.

Als 2015 viele Flüchtlinge nach Deutschland kamen, war das Chaos bei Behörden groß. Die Erhebung von Daten sowie die Organisation von Unterbringung und Versorgung stellten die Beteiligten vor große Herausforderungen. Der Mittelständler

Cevisio erarbeitete mit dem Deutschen Roten Kreuz Landesverband Sachsen e.V. **die** Lösung. Das Unternehmen wirbt für seine Software auf seiner Homepage damit, dass sie in über 280 Aufnahmeeinrichtungen eingesetzt wird. Insgesamt würden „bereits mehr als 380.000 Flüchtlinge verwaltet."

> ▶Das ist Totalkontrolle. Tagesabläufe, Gewohnheiten, Kontakte, Verwandtschaft, Gesundheitszustand, Asylstatus – alles verknüpft und auswertbar.◀

Über all diese Menschen liegen demnach in der Cevisio Quartiersmanagement-Software erfasste Daten vor. Basis für die Erfassung ist eine Ausweiskarte mit RFID-Chip oder Barcode. Mit dieser Karte bewegen sich die Bewohner.innen in ihrer Unterkunft und – so der Plan der Software-Macher – halten sie an verschiedenen Stellen vor ein Lesegerät: Am Ein- und Ausgang, bei der Essensausgabe, bei der Wäschestelle, wenn sie Taschengeld bekommen, beim Ausleihen von Büchern oder Videofilmen, bei medizinischen Untersuchungen oder bei ehrenamtlicher Arbeit.

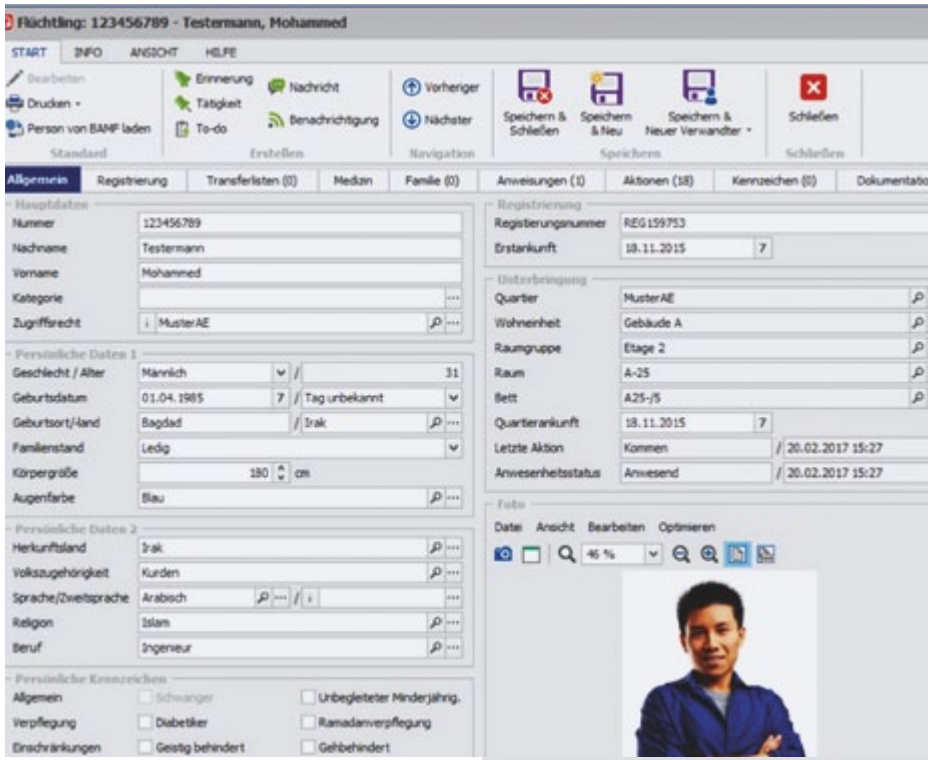
Diese in den Unterkünften erfassten sogenannten „Aktionen" führt die Software über Schnittstellen zusammen mit den Daten des Bundesamtes für Migration und Flüchtlinge – dem BAMF – und mit den Dateien der Ausländerbehörden. Erfasst werden u. a. Angaben zu bestehender Schwangerschaft, zu den verwandten Personen, medizinische Daten mit „Erst- und Folgeuntersuchungen inkl. Befund". Gewährleistet wird auch die Erfassung „sämtlicher Dokumente". Die Software ermöglicht damit nicht nur die „Verwaltung", sondern auch die (Zitat) „Abrechnung der Flüchtlinge". Sie erlaubt die „Erfassung sämtlicher Daten zum Asylverfahren, wie EASY-Optimierung und BAMF-Daten".

Das ist Totalkontrolle. Tagesabläufe, Gewohnheiten, Kontakte, Verwandtschaft, Gesundheitszustand, Asylstatus – alles an einem Ort. Verknüpft und auswertbar.

Manches ist sicher sinnvoll, z.B. Hinweise auf Allergien, oder ob spezielle Ramadan-Verpflegung gewünscht wird. Die Cevisio-Software geht aber deutlich weiter: In der Broschüre zum Funktionsumfang ist z.B. die Rede von der „Erfassung aller an eine

Foto: Digitalcourage, cc by-sa 4.0

Essensausgabe, Bewegungen auf dem Gelände, Ausleihen von Büchern oder Filmen – jede „Aktion" wird per Chipkarte von der Cevisio-Software erfasst.



Screenshot von Cevisio-Homepage

Von A wie Asylstatus bis Z wie Zweitsprache – Der feuchte Traum von Überwachungs-Fanatikern.

Person ausgegebenen Mahlzeiten" sowie „Hinweis bei Mehrfachausgabe einer Mahlzeit an eine Person". Wofür braucht man das?

Ist es nötig, jede Bewegung ins Haus oder aus dem Haus heraus minutiös zu erfassen und zu speichern? Ja, sagt die besagte Broschüre (Zitat): „Über die integrierte Anwesenheitsübersicht ist immer sekundenaktuell erkennbar, welche Flüchtlinge und Helfer/Mitarbeiter sich aktuell in einer Unterkunft befinden. Neben einer reinen Kontrollfunktion ist diese Übersicht insbesondere im Katastrophenfall (Brand etc.) unverzichtbar."

„Unverzichtbar!" Es kommt einem fast seltsam vor, dass hunderttausende von Schulen, Kaufhäusern oder Jugendherbergen noch ohne eine solche sekundenaktuelle Übersicht auskommen. Sind die alle verantwortungslos?

Nein, das ist Leben. Inklusive einem gewissen Lebensrisiko. Die Datensammlung von Cevisio hingegen ist ein feuchter Traum für Überwachungs-Fanatiker. Wir sehen hier keinerlei Empathie mit Menschen, die auch wegen eines Lebens in Freiheit nach Deutschland geflüchtet sind.

Vielleicht ist es also Pragmatismus nach dem Motto „interessiert doch kei-

nen“, wenn das Wort „Datenschutz“ in der 15-seitigen Systemdarstellung nicht ein einziges Mal vorkommt. Technische Datensicherheitsvorkehrungen verbergen sich hinter dem Begriff „Administration“. Funktionalitäten zu den Betroffenenrechten, z. B. für eine Auskunftserteilung oder Transparenz für die Flüchtlinge, konnte ich nicht finden.

Auch in der Praxis gibt es Mängel: Die Datenschutzbeauftragte in Bremen äußert in ihrem aktuellen Jahresbericht (den Link finden Sie auf unserer Jahrbuch19-Webseite, s.u.) „erhebliche datenschutzrechtliche Bedenken“. Speicherfristen waren viel zu lang. Weshalb jede Essensausgabe kontrolliert werden muss, erschloss sich ihr nicht. Die Speicherung der Gesundheitsdaten musste auf ihre Veranlassung massiv zurückgefahren werden. Bei Verwandtschaftsangaben wurde den Betroffenen keine Optionen eröffnet. Viele Fragen sind bis heute offen.

Die bremische Datenschutzkontrolle bezog sich nur auf wenige der Einrichtungen. Es besteht keine Gewähr und Kontrollmöglichkeit, dass in den anderen über 270 Einrichtungen rechtswidrige Überwachungsmöglichkeiten abgestellt werden. Die Rechtslage ist überall gleich und könnte, z. B. mit automatischen Löschfristen, in der Software voreingestellt sein. Cevisio könnte den Betreibern Hilfen und Hinweise zur Wahrung des Datenschutzes geben.

Wir fragen: Hat diese Softwaregestaltung damit zu tun, dass hier Flüchtlinge die Betroffenen sind? Sicher – Flüchtlingsunterkünfte sind logistisch komplexe Systeme und die Betreiber wie das DRK und andere können digitale Unterstützung gut gebrauchen. Doch wie sollen Flüchtlinge sich bei uns integrieren, wenn ihnen dabei die Werte unserer gern beschworenen Leitkultur vorenthalten werden, also die Werte unseres Grundgesetzes? Zu diesen Werten gehört Selbstbestimmung, das Recht auf informationelle Selbstbestimmung.

▶Was heute an Flüchtlingen praktiziert wird, wird morgen vielleicht schon auf uns angewendet.◀

Die Cevisio Software „Quartiersmanagement“ steht nur exemplarisch für einen bevormundenden, intransparenten und überwachungsgierigen Umgang mit Flüchtlingen generell. Da gibt es Schweigepflichtentbindungen der Bundesagentur für Arbeit, die alle und jeden von der Vertraulichkeit entbinden, einschließlich Sozialämter und Migrationsberatungsstellen. In einem sog. Datenaustauschverbesserungsgesetz wurde 2016 festgelegt, dass praktisch jede Stelle jede andere über Flüchtlinge unterrichten darf, wenn es erforderlich erscheint. Um die Herkunft von Flüchtlingen bestimmen zu können, ließ sich das BAMF den Zugriff auf die Smartphones der Flüchtlinge genehmigen, auf denen sämtliche Kommunikationen und viel Privates gespeichert sind. Und gleichzeitig berichten unabhängige Flüchtlingsberatungen, dass ihnen manche Behörden mit dem Verweis auf den Datenschutz hilfreiche Informationen verweigern.

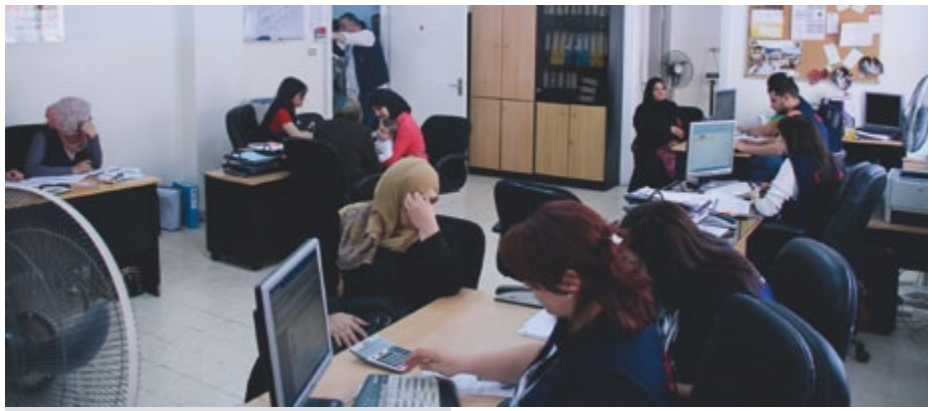


Foto: Caritas Schweiz, cc by-sa 4.0

Die Behörden wissen alles – Hilfsorganisationen bekommen aber „aus Datenschutzgründen“ keine Auskunft.

Wissen ist Macht. Datenschutz darf nicht als politisches Machtmittel missbraucht werden.

Beim Umgang mit den Daten von Flüchtlingen müssen wir besonders umsichtig sein. Sowohl die Nationalsozialisten als auch das DDR-Regime haben mit Informationen und Datenerfassung ihre Bevölkerung kontrolliert und malträtiert. Die Regierungen der Länder, aus denen Menschen zu uns flüchten, quälen ihre Bevölkerung nicht selten durch Kontrolle, Willkür und Verwendung von dem, was sie über diese Menschen wissen. Die Gefahr, dass wir bei der Datenverwaltung à la Cevisio bestehende Traumata vertiefen, und auch die Gefahr, dass unsere Datensammlungen in falsche Hände geraten, etwa von Geheimdiensten des Heimatlandes, ist groß. Auch Software-Unternehmen haben eine Verantwortung dafür, dass solche Gefahren gebannt werden. Wir sollten uns bewusst machen: **Was heute an Flüchtlingen praktiziert wird, wird morgen vielleicht schon auf uns angewendet.**

- Herzlichen Glückwunsch zum BigBrotherAward 2018 in der Kategorie Verwaltung, Cevisio.

Wie es weiter ging

Von Claudia Fischer

Kommentare unseres Publikums:

- „Die Einschränkung der Rechte von geflüchteten Menschen wird allzu oft hingenommen oder ignoriert. Der Preis ist wichtig, um diesen blinden Fleck sichtbar zu machen. Er entsteht durch in der Gesellschaft verankerten Rassismus.“
- „Wir dürfen unsere Menschlichkeit nicht aufgeben!“
- „Die schwache Stellung der Geflüchteten wird durch die zynische Technik

Foto: Campact, cc by-sa 4.0

Flüchtlinge sind Menschen.
Menschen mit Rechten.

noch mehr geschwächt und ausgenutzt für politische Zwecke."

- „Überwachungsmaßnahmen zuerst an Menschen zu „testen", die schon derartig „gebeutelt" sind, sollte uns höchst misstrauisch machen gegenüber denjenigen, die diese Mittel anwenden!"
- „Menschen, die bei uns Zuflucht suchen, sind keine lästigen, potentiell gefährlichen Wesen, die man kontrollieren, kategorisieren und abstempeln müsste. Die Menschenwürde ist unantastbar!"

Schweigen im Walde

Öffentlich blieben sowohl die Firma Cevisio Software und Systeme GmbH in Torgau als auch das Deutsche Rote Kreuz als Mitentwickler und Betreiber von Flüchtlingsunterkünften stumm. Ein Journalist auf „Stern.de" fasste das so in Worte: „Cevisio äußerte sich auf eine schriftliche Anfrage des Stern nicht. Hinterfragen müssen sich letztlich aber vor allem die Betreiber der Flüchtlingsunterkünfte, die die Software einsetzen."

Thilo Weichert: „Die Debatte, die der seit Frühjahr 2018 neue Innenminister Horst Seehofer um die Schließung der Grenzen und Bildung von Ankerzentren ausgelöst hat, nimmt extrem viel Raum ein. Solange wir darüber diskutieren (müssen), ob wir Europas Außengrenzen so gestalten, dass die Geflüchteten im Mittelmeer ertrinken, bevor sie an Land gehen, fühlt es sich fast wie ein „Luxusproblem" an, wenn die, die es bis zu uns geschafft haben, hier ausgeforscht und um ihre Grundrechte gebracht werden. Trotzdem stehen wir zu diesem Preis und finden es wichtig, das Thema auf die Agenda gehoben zu haben! Schade, dass sich die Firma Cevisio und die Betreiber von Unterkünften hinter dieser Debatte verstecken können."

Kategorie Technik

Microsoft Deutschland für Windows 10

Von Frank Rosengart

Der BigBrotherAward 2018 in der Kategorie Technik geht an **Microsoft Deutschland,** vertreten durch die Vorsitzende der Geschäftsführung, Sabine Bendiek, für die kaum deaktivierbare Telemetrie (das ist die Übermittlung von Diagnose-Daten) in **„Windows 10"**. Selbst versierten Nutzerinnen und Nutzern ist es kaum möglich, die Übermittlung dieser Daten zu stoppen.

Foto: Matthias Hornung, cc by-sa 4.0

Laudator: Frank Rosengart,
Chaos Computer Club

Mit der Einführung von Office 365 und Windows 10 ist Microsoft einem allgemeinen Trend gefolgt: Viele Daten werden jetzt in der Cloud gespeichert, die Software wird abonniert, anstatt einmalig gekauft und Microsoft als Konzern ist sehr neugierig, was die Nutzerinnen und Nutzer so treiben. Allein schon für die Lizenzaktivierung ist eine Online-Verbindung erforderlich. Möchte ich aus gutem Grund auf eine Internet-Verbindung verzichten, ist das mit Windows 10 praktisch nicht mehr möglich.

Wenig dramatisch klingt es erst mal, wenn z. B. mein Betriebssystem Windows 10 einmal täglich Informationen über die Größe des Arbeitsspeichers an Microsoft übermittelt. Leider ist es heutzutage fast normal, dass Geräte oder Programme „nach Hause telefonieren", um statistische Daten zu übermitteln. Nicht mehr so belanglos werden es die meisten Menschen finden, wenn eine Liste der auf ihrem Computer installierten Programme übermittelt wird. Was geht es Microsoft an, ob Sie Ihren Computer eher als Schreibmaschine, als Spielzeug, als Fernseher oder für Bildbearbeitung benutzen? Und was macht die Firma mit dieser Information? Wir wissen es nicht.

Laut Microsoft übermittelt Windows 10 aber auch scheinbar ganz banale Informationen: Wie oft wird z.B. die Tastenkombination Alt+Tab benutzt, um schnell zwischen Programmen umzuschalten? „Stört mich doch nicht, wenn der Hersteller das erfährt", mag die eine Hälfte der Nutzer. innen sagen. „Das geht Microsoft doch nichts an!" sagt die andere Hälfte.

Fotos: Tom Alby, cc by-sa 4.0

Wer zu zweiten Gruppe gehört, möchte die Datenübermittlung sicher gern unterbinden. Dafür gibt‘s doch bestimmt irgendwo einen Schalter?! Wer unter Einstellungen/Datenschutz nachschaut, wird mit Schaltern und Auswahllisten erschlagen. Dutzende Dinge sind hier zu aktivieren und zu deaktivieren, und bei den meisten ist nicht klar, welche Konsequenzen die eine oder andere Einstellung hat.

Spätestens mit der Einführung der Europäischen Datenschutzgrundverordnung Ende Mai 2018 sollten alle Schalter grundsätzlich auf „Keine Übermittlung“ gestellt sein und aktiv eingeschaltet werden müssen – Privatsphäre und Datensparsamkeit sind Grundidee der DSGVO. Wir alle – Sie alle – sollten ein Auge darauf haben, ob sich Microsoft daran hält.

„Übermittle bitte nichts, gar nichts“, fehlt als Option.

Es gibt in Windows 10 tatsächlich auch Einstellungen zum Datenschutz. Die befinden sich „nur“ hinter einer Barriere von fünf Klicks hinter dem üblichen Arbeitsbildschirm, also nicht an einem Ort, wo man „zufällig“ mal drüber stolpert. Und selbst wenn wir dort hingelangt sind, haben wir nur die Wahl zwischen „einfacher“ und „vollständiger“ Übermittlung. „Übermittle bitte nichts, gar nichts“, fehlt als Option.

Und diese komplizierten Einstellungen betreffen ohnehin nur die Daten, die das Windows 10 Betriebssystem von Microsoft über den Computer sammelt. Dass Daten vom Browser, von den App-Kacheln oder vom Antivirus-„Defender“ übermittelt werden, lässt sich nirgendwo abschalten. Und dann gibt‘s da noch die Spracherkennung, die Suche im Startmenü und und und ...

Wie mühsam bis unmöglich es ist, Windows zum Schweigen zu bringen, dokumentiert der Bericht des Bayerischen Datenschutzbeauftragten in seinem „Windows 10 Investigation Report“. Selbst wenn sämtliche Telemetrie-Einstellungen über knapp 50 Änderungen in der sogenannten Registry verändert werden (die ausdrücklich nur für Expert.innen gedacht ist und die das Potential hat, den Rechner durch einen unbedachten Eingriff unbrauchbar zu machen), senden Windows 10-Rechner immer noch jede Menge Anfragen an Internet-

Foto: Eigensinn e.V.

Frank Rosengart hat zur BBA-Gala einen Alt+F4-Pulli des Chaos Computer Clubs mitgebracht. Mit Alt+F4 beendet man Windows-Programme. Das Shirt gilt seit vielen Jahren als eine Art Markenzeichen des CCC.

Dienste für Kacheln, Updates oder Empfehlungsdienste. Dort wird mindestens die IP-Adresse des Nutzers registriert, bereits ohne dass man bewusst eine Webseite aufgerufen hätte. Möglich ist eine Änderung der Registry überhaupt nur in der „Enterprise“-Variante von Microsoft, also für Geschäftskunden.

Aus Nutzer.innensicht ist es einfach eine Sauerei.

Wir wollen Sie gar nicht damit langweilen, die (Un-)rechtmäßigkeit jeder einzelnen Datenübermittlung juristisch zu bewerten. Aus Nutzer.innensicht ist es einfach eine Sauerei, dass sich die Übermittlung praktisch nicht deaktivieren lässt – zumal es für viele Menschen zu Windows als Betriebssystem aus Kompatibilitätsgründen keine gangbare Alternative gibt.

Die Firma Microsoft hat im Jahre 2002 den „Lifetime“-BigBrotherAward erhalten. Damals hat der Datenschutzbeauftragte von Microsoft, Sascha Hanke, den BigBrotherAward sogar persönlich abgeholt und gesagt, die Firma würde unsere Kritik ernst nehmen. Spätestens mit der Einführung von Office 365 hat Microsoft viele Anwendungen und damit Ihre Daten, sehr geehrte Damen und Herren, in die Cloud übergeben. Allein das wäre schon einen Preis wert gewesen. Schon 2011 – zwei Jahre vor Edward Snowden – hat der damalige Datenschutzberater von Microsoft, Caspar Bowden, vor den Zugriffsmöglichkeiten durch Geheimdienste auf die Cloud-Daten gewarnt. Er hat eindringlich erklärt, dass Microsoft damit die Inhalte seiner Kunden an NSA, CIA & Co preisgibt, denn die US-Geheimdienste dürfen durch den FISA Act (Foreign Intelligence Surveillance Act) von 2008 auf alle Clouddaten zugreifen – und Nicht-US-Bürger haben keine Rechtsmittel dagegen. Caspar Bowden ist für diese deutlichen Worte von 2011 von Microsoft gefeuert worden. Es wäre besser gewesen, sie hätten auf ihn gehört!

Dadurch, dass Windows 10 nun auch noch ständig „nach Hause telefoniert“, werden Microsoft-Produkte zu einem nicht mehr tragbaren Problem!

- Herzlichen Glückwunsch, Microsoft, zum inzwischen zweiten BigBrotherAward.

Wie es weiter ging

Von Claudia Fischer

Kommentare unseres Publikums:

- „Absolute Ohnmacht und Ausgeliefertsein als Nutzer, keine Handhabe dagegen."
- „Dieser Preis betrifft mich schon jetzt."
- „Meine Firma führt es in Kürze ein und mir graut jetzt noch mehr davor!"
- „Durch den de-facto-Standard im Bereich der Wirtschaft und weil man nichts anderes kennt, bzw. da ja die meisten Programme drauf laufen, ist man oftmals gezwungener Windows-Anwender. Dieser Konzern ist eines der ersten und datenschutzverachtenden Big-Data-Monopole. Er gehört zerschlagen!"

Microsoft hat uns eine E-Mail geschrieben

Darin bedankt sich der Konzern für unsere Einladung, er könne es aber auch Termingründen nicht einrichten, jemanden zur Verleihung zu schicken. Microsoft findet auch nicht, dass der Konzern den Preis verdient habe. „Auch ohne einen BigBrotherAward haben wir verstanden, dass sich viele mit der Übertragung von Daten, die durch das Betriebssystem veranlasst sind, schwer tun – insbesondere, wenn nicht klar ist, um welche Daten es geht und zu welchem Zweck die Übertragung erfolgt." Deshalb würden die Datenschutzeinstellungen kontinuierlich überarbeitet und „verbessert", insbesondere in den Versionen für Unternehmen und Behörden. Microsoft investiere rund 1 Milliarde Dollar jährlich in Datensicherheit und Datenschutz – weltweit.

Foto: fr Rama, cc by-sa 4.0

„Microsoft hätte auf seinen ehemaligen Datenschutzberater Caspar Bowden hören sollen, als er vor dem Zugriff von Geheimdiensten warnte."

„Das ist nur ein lächerlicher Teil des jährlichen Umsatzes", kommentiert Laudator Frank Rosengart diese Zahl. Allein der Bund habe in den letzten drei Jahren eine Viertelmilliarde Euro Lizenzgebühren an Microsoft gezahlt, schrieb die Stuttgarter Zeitung in ihrem Artikel zum BigBrotherAward 2018. „Die Datenübermittlung standardmäßig abzuschalten, kostet Microsoft außerdem keinen Cent mehr – im Gegenteil", so Frank Rosengart weiter. „Der ganze Traffic müsste bei Abschaltung ja auch nicht mehr bearbeitet werden, das spart Geld. Aber natürlich kommt dann auch deutlich weniger Datenberg zusammen, den man auf andere Weise zu Geld machen könnte", bekräftigt er. Und fordert weiterhin: „Windows-Betriebssysteme und MS Office-Programme müssen auch offline nutzbar sein!"

Kategorie Politik

Die Fraktionen von CDU und Bündnis 90/Die Grünen im hessischen Landtag

Von Dr. Rolf Gössner

Der BigBrotherAward 2018 in der Kategorie Politik geht an **die Fraktionen von CDU und Bündnis90/Die Grünen im hessischen Landtag.** Die beiden Regierungsfraktionen erhalten den Negativpreis für ihr geplantes neues Verfassungsschutzgesetz und für die geplante Novellierung des hessischen Polizeigesetzes. Ihre Gesetzesinitiative enthält eine gefährliche Ansammlung gravierender Überwachungsermächtigungen, die tief in Grundrechte eingreifen und den demokratischen Rechtsstaat bedrohen. Die schlimmsten Regelungen im Überblick:

Foto: Matthias Hornung, cc by-sa 4.0

Laudator: Dr. Rolf Gössner, Internationale Liga für Menschenrechte

1. Der Inlandsgeheimdienst „Verfassungsschutz" soll auch vorbestrafte V-Leute rekrutieren und kriminell gewordene Verfassungsschutz-Mitarbeiter.innen weiter einsetzen und abschöpfen können. Das tut er zwar schon heute, wie die Praxis zeigt; neu aber ist, dass dies erstmals gesetzlich abgesichert werden soll und kriminelle V-Leute ganz legal der strafrechtlichen Verfolgung entzogen werden können – anstatt solche V-Leute unverzüglich abzuschalten. Ein rechtsstaatswidriger Freibrief für kriminelles Handeln in staatlicher Mission. Diese Regelung legalisiert praktisch die bisherigen Skandale und mit ihnen die obszönen Verflechtungen des Verfassungsschutzes in rassistische, kriminelle und gewalttätige Neonaziszenen.
2. Erlaubt werden soll auch, Berufsgeheimnisträger wie Ärzte, Anwälte oder Journalisten als V-Leute anzuheuern oder V-Leute in deren beruflichem Umfeld zu platzieren. Damit werden die Verschwiegenheitspflichten und zu schützenden Vertrauensverhältnisse zu ihren Mandanten, Patienten oder Informanten verletzt. Nur Abgeordnete und ihre Mitarbeiter.innen sollen vor dieser geheimdienstlichen Instrumentalisierung und Ausforschung ausdrücklich geschützt werden.

Foto: Detlev Sieber, cc by-sa 4.0

3. Selbst Daten über Minderjährige unter 14 Jahren, also von Kindern, sollen in Dateien und Akten des Verfassungsschutzes erfasst und gespeichert werden dürfen. Diese frühzeitige geheimdienstliche Stigmatisierung kann fatale Folgen für die weitere Entwicklung der Betroffenen haben – etwa bei der späteren Berufswahl, Lehrstellen- oder Jobsuche.
4. Der Verfassungsschutz soll ermächtigt werden, personenbezogene Überwachungsdaten an öffentliche Stellen zu übermitteln – und zwar zur *„Überprüfung der Verfassungstreue von Personen, die sich um Einstellung in den öffentlichen Dienst bewerben“.* Das erinnert fatal an die menschenrechtswidrige Berufsverbotspraxis früherer Zeiten. Auch Organisationen und künftigen Mitarbeiter.innen staatlich geförderter Demokratie- und Präventionsprojekte, etwa gegen Rechtsextremismus oder Salafismus, drohen anlasslose geheimdienstliche Überprüfungen – womit sie pauschal zu Sicherheitsrisiken erklärt und unter Generalverdacht gestellt werden. Dieses gesetzliche Misstrauensvotum untergräbt Akzeptanz und Vertrauen, die für eine erfolgreiche Arbeit solcher zivilgesellschaftlichen Projekte unerlässlich sind.
5. Spionage-Programme, also sog. Staatstrojaner, sollen künftig über gefundene oder aufgekaufte Sicherheitslücken in Computern oder Smartphones Verdächtigter eingeschleust werden, um sie präventiv per Online-Durchsuchung oder Quellen-Telekommunikationsüberwachung (TKÜ) umfassend ausforschen zu können.
6. Und die Polizei soll künftig u.a. ermächtigt werden, sogenannte „Gefährder“ vorsorglich in elektronische Fußfesseln zu legen, um ihren Aufenthalt, ihre Bewegungen und Kontakte über Wochen und Monate lückenlos kontrollieren zu können. Das sind Menschen, die keine Straftaten begangen haben, sondern denen die Polizei aufgrund bestimmter Anhaltspunkte künftige Straftaten zutraut.

Auf dem Weg in den präventiv-autoritären Sicherheitsstaat

Mit dieser Gesetzesinitiative geht die schwarz-grüne Regierungskoalition in Hessen einen großen Schritt in Richtung präventiv-autoritärer Sicherheitsstaat. Mit besonders prekären Regelungen reiht sie sich damit in die bundesweiten Reformen ein, mit denen u.a. der Staatstrojaner zur Quellen-TKÜ und Online-Durchsuchung sowie die elektronische Fußfessel für „Gefährder“ legalisiert werden. So etwa im BKA-Gesetz (2017), in der Strafprozessordnung (2017), in den Geheimdienstgesetzen Baden-Württembergs (2017) und Bayerns (2016). Interessanterweise klagt die grüne Oppositionsfraktion im bayerischen Landtag gegen das dortige Verfassungsschutzgesetz – ausgerechnet gegen ein Gesetz, das sich das hessische Regierungsbündnis unter Mitwirkung der Grünen zum Vorbild genommen hat.

Ursprünglich sollten die Verfassungsschutzgesetze in Bund und Ländern novelliert werden, um überfällige Konsequenzen zu ziehen aus den zahlreichen Missständen, Pannen und Skandalen im Zusammenhang mit der NSU-Mordserie und NSA-Massenüberwachung. Primäre Ziele müssten demnach sein, den Verfassungsschutz und seine Befugnisse wirksam rechtsstaatlich zu zähmen und die Kontrolle über ihn erheblich zu stärken. Doch stattdessen erhalten ausgerechnet diese demokratisch kaum kontrollierbaren Geheimbehörden des Bundes und der Länder – geschichtsvergessen muss man sagen – wieder unverdienten Auftrieb, werden abermals aufgerüstet und massenüberwachungstauglicher gemacht, anstatt die Bevölkerung endlich vor ihren klandestinen Machenschaften und Skandalen wirksam zu schützen. Das heißt: Der Verfassungsschutz geht gestärkt aus dem Desaster und seiner Skandalgeschichte hervor. Und auch die Polizei wird weiter hochgerüstet.

Collage: Maximilian von der Heyden, cc by-sa 4.0

„Die Erlaubnis, vorbestrafte Neonazis als V-Leute rekrutieren zu dürfen, ist ein rechtsstaatswidriger Freibrief für kriminelles Handeln in staatlicher Mission.“

Foto: Torsten Grote, cc by-sa 4.0

„Polizei- und Verfassungsschutzgesetze enthalten eine gefährliche Ansammlung gravierender Überwachungsermächtigungen und Grundrechtseingriffe.“

Was bedeutet das für unmittelbar Betroffene und für uns alle? Zwei Beispiele:

1. Heimlicher Angriff auf Computer und Smartphones mit Staatstrojanern

Der hessische Verfassungsschutz soll unter bestimmten Bedingungen erstmals mit technischen Mitteln heimlich „informationstechnische Systeme“ angreifen dürfen – bei „Gefahr im Verzug“ zunächst sogar ohne richterliche Anordnung. Das heißt im Klartext: Dieser Inlandsgeheimdienst darf zur verdeckten Informationsgewinnung Computersysteme mit Hilfe von Spionage-Programmen hacken – und zwar mit Hilfe der berüchtigten „Staatst-

Links und weitere Infos: digitalcourage.de/jahrbuch19

Collage: Dennis Blomeyer, cc by-sa 4.0

Staatstrojaner stellen uns alle unter Generalverdacht und dringen in unsere privatesten Lebensbereiche ein.

rojaner“, die im Land der Hessen auch „Hessentrojaner“ heißen. Diese Überwachungssoftware wird heimlich in Computer, Tablets oder Smartphones von Verdächtigten eingeschleust, um diese unter Ausnutzung von Sicherheitslücken zu infiltrieren. So können dann Quellen-Telekommunikationsüberwachungen oder Online-Durchsuchungen durchgeführt werden.

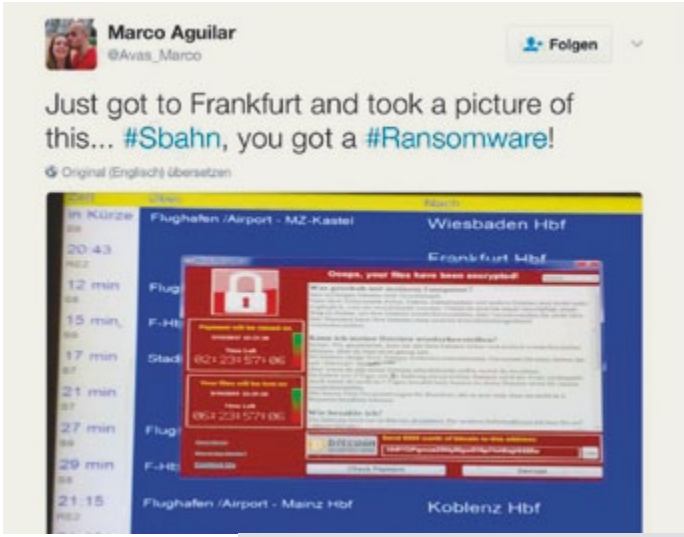
Mit diesen Methoden, die der Abwehr einer „dringenden Gefahr“ dienen sollen, bricht der Staat massiv in Privatsphäre und Persönlichkeitsrechte, in Informationelle Selbstbestimmung und Meinungsfreiheit der Betroffenen ein: Denn damit können PC-Mikrofone und Webcams eingeschaltet sowie sämtliche laufenden Kommunikationsinhalte vor ihrer Verschlüsselung überwacht werden – inklusive SMS, E-Mails, Chats und Messenger-Dienste. Mit Hilfe der Trojaner kann der Geheimdienst auf sämtliche Datenbewegungen, auf alle gespeicherten Festplatten-Inhalte, auf Textdokumente, Gesundheits- und Finanzdaten, auf intimste Informationen, Adressbücher, Fotos und Filme zugreifen – letztlich auf das gesamte digitale und vernetzte Leben der Betroffenen. Angesichts der hieraus entstehenden Persönlichkeits-, Kontakt- und Bewegungsprofile ist an den verfassungsrechtlich gebotenen Schutz des Kernbereichs persönlicher Lebensgestaltung praktisch nicht mehr zu denken – ganz abgesehen davon, dass solche Geheimmethoden weder gerichtlich noch parlamentarisch wirksam kontrollierbar sind. Es handelt sich um einen der schwersten staatlichen Grundrechtseingriffe mit totalitärem Potential – um einen Einbruch in alle Lebensbereiche bis hinein in die Gedanken- und Gefühlswelt der Betroffenen.

▶Solche Geheimmethoden sind weder gerichtlich noch parlamentarisch wirksam kontrollierbar.◀

▶Schwerer Grundrechtseingriff mit totalitärem Potential.◀

Diese digitale Waffe unterminiert darüber hinaus das *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht)*: Denn der Verfassungsschutz muss Software-Sicherheitslücken ausfindig machen, um einen Staatstrojaner auf dem Gerät installieren und aktivieren zu können. Er wird versuchen, solche Schwachstellen für eigene Zwecke künftig weiter offenzuhalten – anstatt sie sofort schließen zu lassen, um Attacken Dritter abzuwehren, das IT-System insgesamt zu schützen und damit die Allgemeinheit. Stattdessen werden also mutwillig Sicherheitslecks als Einfallstore aufrechterhalten, über die auch andere Geheimdienste, Cyber-Kriminelle, Betrüger, Erpresser und Terroristen gefährliche Angriffe auf private, betriebliche oder staatliche Computersysteme ausführen können oder auf die kritische Infrastruktur insgesamt (etwa von Strom- und Wasserversorgern, des Krankenhaus-, Gesundheits- oder Verkehrswesens).

Dieses unverantwortliche Staatsverhalten öffnet Missbrauch und gefährlichen Cyberattacken Tür und Tor. Abschreckendes Beispiel: der Erpressungs-Trojaner „WannaCry“, der im Mai 2017 neben Privat-PCs auch Automobilkonzerne, Bahnunternehmen und Krankenhäuser lahmlegte und Schäden in Milliardenhöhe verursachte. Die dabei genutzte Sicherheitslücke war dem US-Auslandsgeheimdienst NSA bereits seit Jahren bekannt. Verantwortungsvolle Sicherheitspolitik, die diese Bezeichnung verdient, sieht anders aus. Denn es gehört zum Auftrag des Staates, seine Bürger zu schützen und Sicherheitslücken zu schließen, und nicht, sie mutwillig für eigene Trojaner sperrangelweit offenzuhalten – und damit auch für andere Cyberangreifer.



Quelle. Twitter-Nutzer

Im Mai 2017 legte der Erpressungs-Trojaner Verkehrsunternehmen, Krankenhäuser und andere Infrastruktur lahm.

2. Beispiel: Elektronische Fußfesseln zur Aufenthaltskontrolle von Gefährdern

Die hessische Polizei soll künftig – wie seit 2017 das BKA auf Bundesebene – so genannte „terroristische Gefährder“ präventiv in elektronische Fußfesseln legen sowie Meldepflichten, Aufenthaltsbeschränkungen, Hausarrest und Kontaktverbote verhängen können. Nach einer gerichtlichen Anordnung sollen diese Freiheitsbeschränkungen mit einer elektronischen Fußfessel über GPS lückenlos überwacht werden, selbst innerhalb von Wohnungen. Zulässig soll dies dann sein, so heißt es im schwarz-grünen Gesetzentwurf wörtlich, *„wenn bestimmte Tatsachen die Annahme rechtfertigen“,* dass die betreffende Person *„innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise“* eine Straftat begehen wird, *„oder deren individuelles Verhalten eine konkrete Wahrscheinlichkeit dafür begründet, dass sie innerhalb eines übersehbaren Zeitraums“* eine Straftat begehen wird.

Es gehört zum Auftrag des Staates, seine Bürger zu schützen und Sicherheitslücken zu schließen.

Die elektronische Überwachungsmaßnahme, mit der u.a. terroristische Straftaten verhütet werden sollen, ist auf höchstens drei Monate zu befristen, kann aber um jeweils drei Monate verlängert werden – das heißt im Zweifel: unbeschränkt. Weigern sich Betroffene gegen die Maßnahme, können sie mit richterlicher Entscheidung bis zu zehn Tage lang in Polizeigewahrsam gesteckt werden.

Solche eingriffsintensiven Polizeimaßnahmen, die lückenlose Bewegungsprofile liefern und Rückschlüsse auf die persönliche Lebensführung zulassen, sollen gegen sogenannte Gefährder verhängt werden – also gegen Menschen, die bislang nicht straffällig geworden sind, denen dies aber in Zukunft aufgrund bloßer Indizien und Annahmen oder unterstellter Absichten und Gesinnung polizeilicherseits zugetraut wird. Solche Prognosen für künftiges Verhalten können entweder aus polizeilichen oder geheimdienstlichen Persönlichkeits- und Kontaktprofilen oder auch aus Risikobewertungen per Computeranalyse (zB. Precrime-Programm „Radar-iTE“) resultieren. Doch wie lässt sich dabei verhindern, dass institutioneller Rassismus und Islamophobie zu folgenschweren Einschätzungen führen?

Foto: Digitalcourage, cc by-sa 4.0

Einschränkungen der Freiheit kommen einem Ausverkauf des Grundgesetzes gleich.

Derart gravierende Grundrechtseingriffe auf mehr oder weniger vage Mutmaßungen zu stützen, dürfte den Verfassungsgrundsatz der Verhältnismäßigkeit verletzen. Denn rund um die Uhr und in Echtzeit überwachte Aufenthalts- und Kontaktverbote schränken die Betroffenen, die ja als unschuldig zu gelten haben, unmittelbar in ihrer Handlungs- und Bewegungsfreiheit ein und verletzen ihre Privatsphäre und Persönlichkeitsrechte – und letztlich auch ihre Menschenwürde. Solche verhaltenssteuernden und freiheitsberaubenden Präventionsmaßnahmen gleichen letztlich einer vorweggenommenen Verdachtsstrafe – also einer rechtsstaatswidrigen Strafe ohne Tat.

Gegen die hessische Gesetzesinitiative regt sich heftiger Protest und Widerstand.

Im Übrigen dürfte die elektronische Fußfessel, die ohnehin relativ leicht manipulierbar und entfernbar ist, im Ernstfall auch ungeeignet zur Verhinderung terroristischer Straftaten sein – besonders wenn es sich um potentielle Täter handelt, die zu allem entschlossen sind: So trug etwa einer der beiden Täter, die 2016 einem katholischen Pfarrer in der Normandie die Kehle durchtrennten, eine elektronische Fußfessel; und auch das Berliner Attentat auf dem Weihnachtsmarkt im Dezember 2016 hätte damit wohl kaum verhindert werden können – wohl aber mit anderen, längst gesetzlich erlaubten Polizeibefugnissen, die aber, wie sich herausgestellt hat, nicht genutzt worden sind.

Zivilgesellschaftliche Proteste und innergrüner Streit um „Hessentrojaner“

Gegen die hessische Gesetzesinitiative regt sich heftiger Protest und Widerstand: Ein breites Bündnis von Demokratieprojekten sowie Bürgerrechts- und Datenschutz-Organisationen unterstützen eine gemeinsame Erklärung, in der sie die geplanten Verschärfungen ablehnen, weil sie Demokratie und Grundrechte schädigen. Während einer Anhörung im Hessischen Landtag hat die überwiegende Mehrzahl der Sachverständigen die Gesetzespläne heftig kritisiert und erhebliche Änderungen angemahnt.

Auch die grüne Basis in Hessen votierte schon Ende 2017 gegen die schwarz-grünen Pläne, speziell gegen die Legalisierung des „Hessentrojaners“. Damit verweigerte sie der grünen Landtagsfraktion ihre Unterstützung. Vollkommen zu Recht, lehnen doch die Grünen die Staatstrojaner generell ab und hatten doch die hessischen Grünen im letzten Wahlkampf versprochen, keine Online-Durchsuchung zur Gefahrenabwehr zuzulassen. Doch die Landtagsfraktion bleibt stur und begründet ihr gebrochenes Versprechen mit „terroristischen Bedrohungen“, die es nötig machten, die digitale Kommunikation weitgehender als bisher zu überwachen. Das miese Spiel mit der Angst vor Terrorismus zur Beschränkung der Freiheits-

rechte, um angeblich mehr Sicherheit zu erlangen, das haben die Grünen bislang eher gemieden und anderen überlassen, wie etwa der CDU/CSU oder auch der Großen Koalition. Die grüne Fraktion in Hessen aber spielt nun selbst beim Überwachungspoker mit, beteiligt sich am sicherheitspolitischen Überbietungswettbewerb und behauptet noch dreist, ihr Gesetzentwurf trage eine „grüne Handschrift".

Mit solchen Geheimdienst- und Polizeigesetzen, wie im schwarz-grün regierten Hessen geplant oder im grün-schwarz regierten Baden-Württemberg teilweise schon umgesetzt, können die Grünen ihr Selbstverständnis als Bürgerrechtspartei allmählich begraben.

Ich bringe die Kritik an der hessischen Gesetzesinitiative noch einmal auf den Punkt:

- Die künftig gesetzlich abgesicherte Zusammenarbeit mit vorbestraften und kriminell gewordenen V-Leuten widerspricht rechtsstaatlichen Grundsätzen.
- Die geplante geheimdienstliche Regelüberprüfung künftiger Mitarbeiter.innen von Demokratieprojekten bedeutet Gesinnungsschnüffelei und erinnert an unselige Zeiten grundrechtswidriger Berufsverbote.
- Verhaltenssteuernde und freiheitsberaubende elektronische Fußfesseln verletzen Privatsphäre und Persönlichkeitsrechte – und letztlich auch die Menschenwürde.
- Und Staatstrojaner bedrohen den Kernbereich privater Lebensführung und gefährden Sicherheit und Vertraulichkeit des IT-Systems.

Collage: Maximilian von der Heyden, cc by-sa 4.0

„Geheimdienstliche Regelüberprüfung erinnert an unselige Zeiten grundrechtswidriger Berufsverbote."

Das ist „digitale Inquisition", so Heribert Prantl von der Süddeutschen Zeitung. Und er fragt erstaunt, weshalb die allermeisten Bürger*innen sich das gefallen lassen. Und liefert drei Antworten gleich mit: 1. wegen der Politik mit der Angst vor Terror, die die Wähler.innen selbst maßlose Freiheitsbeschränkungen schlucken lässt, wenn sie angeblich mehr Sicherheit versprechen; 2. weil die meisten Freiheitsbeschränkungen nicht zu spüren sind, da sie heimlich stattfinden, und 3. weil die Bürger.innen letztlich darauf vertrauten, dass das Bundesverfassungsgericht es wieder richten möge.

Foto: Matthias Hornung, cc by-sa 4.0

Der Journalist Heribert Prantl hielt 2014 auf der BBA-Gala die Laudatio zu unserem Positiv-Preis Julia-and-Winston-Award für Edward Snowden

Apropos Bundesverfassungsgericht: Es gibt bereits Initiativen für Verfassungsbeschwerden, so u.a. von Digitalcourage, um etwa Staatstrojaner stoppen zu lassen. Und so mündet diese Laudatio in einen öffentlichen Appell, solche Verfassungsbeschwerden kräftig und massenhaft zu unterstützen – als Akt bürgerrechtlicher Notwehr.

- Herzlichen Glückwunsch, CDU- und grüne Fraktion im hessischen Landtag, zum Big-BrotherAward 2018.

Wie es weiter ging

Von Claudia Fischer

Der BigBrotherAward von Rolf Gössner hat in diesem Jahr wieder die Publikumsabstimmung bei der Verleihungsgala gewonnen.

Kommentare auf den Abstimmungskarten:

- „Die Politik sollte uns Bürger schützen und nicht ausspionieren."
- „Staatstrojaner – kompletter Eingriff in alle Grundrechte."
- „Die Unwissenheit, mit der die Politik an dieses Gesetz herangeht, ist absolut niederschmetternd. Entgegen jeglicher Empfehlungen von Expert.innen versuchen die Fraktionen CDU und Grüne, wieder einmal ein Überwachungsgesetz durchzupeitschen."
- „Schade, dass es den Grünen so leicht fällt, die Ideale der Freiheits- und Bürgerrechtsbewegung für etwas politische Macht zu opfern."

Abgestraft, aber rausgemogelt

Unser BigBrotherAward traf zum richtigen Zeitpunkt: Am Wochenende nach der Verleihungsgala hatten die Bündnis-Grünen in Hessen ihren Landesparteitag und wählten die Kandidat.innen für die Landtagswahlen im Herbst 2018. Jürgen Frömmrich, der Grünen-Innenpolitiker und Befürworter des neuen Verfassungsschutzgesetzes, wurde deutlich abgestraft und landete auf einem hinteren Landeslistenplatz. Besser schnitt der Software-

Links und weitere Infos: digitalcourage.de/jahrbuch19

Experte Torsten Leveringhaus ab, der sich zuvor dezidiert „gegen die digitale Aufrüstung“ ausgesprochen hatte. Er wollte den Gesetzentwurf gründlich ändern, „damit wir den ‚BigBrotherAward’ so schnell wie möglich zurückgeben können“, so sagte er.

„Das wäre immerhin ein Novum: den BBA zwar weder annehmen noch abholen, ihn aber später wieder zurückgeben“, kontert unser Laudator Rolf Gössner. „Immerhin können wir festhalten: Wir haben mit dem BBA die kritische Debatte um den Gesetzentwurf entscheidend beeinflusst.“

Ende Juni 2018 ist dann die Verschärfung des hessischen Verfassungsschutz- und Polizeigesetzes vom hessischen Landtag mit der Mehrheit der Regierungsfraktionen durchgesetzt worden. Dabei hatte die grüne Landtagsfraktion nach den heftigen zivilgesellschaftlichen Protesten allerdings noch erreichen können, den so genannten „Hessentrojaner“ – also die heimliche Online-Durchsuchung und Quellen-Telekommunikationsüberwachung – aus dem Verfassungsschutzgesetzentwurf ersatzlos zu streichen. Ein toller Erfolg! Es ist aber ein Pyrrhussieg, denn dafür haben sie statt dem Verfassungsschutz nun die Polizei gesetzlich mit dem Staatstrojaner ausgestattet. „Am grundsätzlichen Problem des Staatstrojaner-Einsatzes für die IT-Sicherheit ändert dies nichts – es bleibt dabei, dass Sicherheitslücken nun offen bleiben, statt geschlossen zu werden“, ärgert sich Rolf Gössner. „Und das ist ein Skandal! Der Staat versagt dabei, seine Bürger vor digitalen Übergriffen zu schützen.“

Foto: Fabian Kurz, cc by-sa 4.0

▶ Ebenfalls ein Skandal: Der zweite Preisträger CDU hat sich gar nicht geäußert.

Kategorie Verbraucherschutz

Amazon Alexa

Von padeluun

„Alexa, an wen geht der BigBrotherAward 2018 in der Kategorie Verbraucherschutz?“

Alexa-Stimme: „Der BigBrotherAward 2018 in der Kategorie Verbraucherschutz geht an **die Firma Amazon, für ihren Sprachassistenten Alexa.“** (Publikum applaudiert nach der Einspielung)

Ich ahne, dass es für diese Art Preisträger viel Beifall geben würde, dabei habe ich Apple Siri, Google Assistant, Microsoft Cortana, Samsung Bixby und Nuance noch gar nicht erwähnt, die wir im Großen und Ganzen mit auszeichnen könnten. Aber von allen diesen Anwendungen ist Amazon „Alexa“ das preiswürdigste unter ihnen. Das Gerät lauscht 24 Stunden am Tag in meiner Wohnung, weil es darauf lauert, dass ich das Wort „Alexa“ sage. Sobald es dieses Wort ‚hört‘, zeichnet es die nachfolgenden Sätze auf und sendet diese zur Analyse zu den Rechnern in der Amazon-Cloud. Dort wird mein Text übersetzt, analysiert und dann werden Aktionen fernausgelöst. Zum Beispiel wird ein Timer oder Wecker gestellt, Musik, meiner Stimmung entsprechend – oder was das Gerät dafür hält – abgespielt, ein Trommelwirbel gestartet oder auf Amazon ein neuer Goldhamster bestellt.

Laudator: padeluun, Digitalcourage

Foto: Matthias Hornung, cc by-sa 4.0

▶ Mit „Alexa“ will Amazon noch mehr Macht im Onlineversandhandel kriegen. ◀

Mit diesem „Alexa“ will Amazon noch mehr Macht im Onlineversandhandel kriegen. Damit wird Amazon noch weiter zu dem, was Marc-Uwe Kling in seinem Buch „Qualityland“ *„The Shop“* nennt. Zeichnen wir damit „wirtschaftliche Cleverness“ und „Erfolg“ mit unserem Negativpreis aus? Nein. Zu groß

Foto: Ttsurunda, cc by-sa 4.0

„Das „Alexa“-Gerät selbst tut gar nichts. Es gibt Tonaufnahmen weiter an die Amazon-Cloud, die dann einen Trommelwirbel startet oder einen Goldhamster bestellt.“

zu werden und Hybris anzustreben (und damit gefährlich zu sein) ist verwerflich.

Muss ich mehr sagen? Muss ich wirklich begründen, warum eine Abhörschnittstelle, die sich zum Beispiel als Wecker tarnt, aber ein allwissender Butler in fremden Diensten ist, der sich von mir höchstpersönlich ins Schlafzimmer tragen und an das weltweite Überwachungsnetz anschließen lässt, einen BigBrotherAward bekommen soll? Nein, muss ich nicht. Oder?

Herzlichen Glückwunsch an Amazon „Alexa“. Und gut. [Abtritt, Herr Liebold, übernehmen Sie.] Halt, bleiben Sie noch sitzen. Natürlich habe ich noch mehr zu sagen!

Rena Tangens hat in ihrer Laudatio zur Smart City von der „perfekten Verbindung des totalitären Überwachungsstaates aus George Orwells ‚1984‘ und den normierten, nur scheinbar freien Konsumenten in Aldous Huxleys ‚Schöne Neue Welt‘ “ gesprochen. Die sogenannten „Sprachassistenten“ sind die lästige Ergänzung zum totalen Überwachungssystem, das sich „smart“ nennt, aber „teuflisch“ ist. Skylla und Charybdis in einem, das Private (Alexa) und das Öffentliche („Smarte“ Straßenlaternen) wenden sich gegen mich. Es geht gegen meine Freiheit, gegen meine freie Entfaltung, gegen meine Würde. Bald wird es so sein, dass ich, wenn ich auf der Straße spreche, von der Straßenlaterne an der Stimme erkannt werde. Wer ich bin, hat das Gerät „Alexa“ verraten, das mein Stimmprofil aufgesaugt und der großen Big-Data-Krake zum Verdauen vorgeworfen hat. Diese imaginäre Datenkrake weiß dann nicht nur, wen ich besuche, sondern auch, welchen Weg ich nehme, um den Besuch abzustatten.

Bild: Panthermedia, Collage: Dennis Blomeyer, cc by-sa 4.0

„Warum lassen wir eine Abhörschnittstelle, die sich als Butler oder Wecker tarnt, in unser Haus?“

Heute, wo die Einführung gerade erst begonnen hat, habe ich mir angewöhnt, in einer fremden Wohnung erst einmal „Alexa, bestelle 100 große Dosen Ravioli“ zu rufen. Wenn die Wohnungsinhaber nervös reagieren, weiß ich, dass ich mich in einem verwanzten Haushalt befinde.

Und wenn es da draußen wirklich Leute gibt, die das Gerät – mit dem Gefühl, nun einen Butler zu haben – bei sich zu Hause installieren, denken Sie daran, dass derjenige, der das „Alexa“-Gerät installiert, die Möglichkeit hat, alles, was sie diesem „Alexa“ zu Gehör bringen, über seine Smartphone-App wieder abzuhören. Wer das Gerät einrichtet, kann auch noch Monate später alle Sprachfetzen, die Alexa aufgeschnappt hat, in einer langen Liste mit Datum und Uhrzeit verschriftlicht sehen und auf Klick auch neu abspielen. Das sollten z.B. auch Beratungsstellen für Stalkingopfer im Blick behalten.

Ich habe einige Tage mit diesem Gerät herumgespielt. Es ist schön, beim Nudelkochen einfach in den Raum zu rufen „Alexa, Timer 8 Minuten“. Auch beim morgendlichen Wecken, ohne sich umzudrehen, „Alexa, noch 10 Minuten“ knurren zu können, ist schön. Aber wenn das bedeutet, dass die Aufzeichnung im Internet bei Amazon gespeichert wird, und der Konzern damit weiß, wann ich aufstehe, dann sollte ich doch besser auf diesen Komfortgewinn verzichten. Denn mit „Alexa“ ist mein Wecker-Stellen keine lokale Aktion innerhalb meines Smartphones mehr, sondern wird zu einem Stück Big Data im Besitz von Amazon.

Ich werde immer wieder gefragt, ob Amazon mit „Alexa“ denn irgendetwas besonders Böses macht. Ob der Konzern nicht vielleicht doch heimlich ALLES aufzeichnet, was im Raum gesagt wird und das weiter schickt, auch wenn nicht vorher „Alexa“ gesagt wurde. Die Wochenzeitung „Die Zeit“ hat einen Techniker von Tactical Tech nachgucken lassen. Und der sagt: „Naja, könnte sein. Das Gerät verschlüsselt Daten, die es sendet, da kann man nicht herausbekommen, ob es nur „gewünschte“ Aussagen sendet oder mehr.“

Screenshot: Digitalcourage, cc by-sa 4.0

In der Alexa-App sind alle Details aufgezeichnet: Als Text, Ton, mit Datum, Stimme usw.

Wir schätzen das mal so ein: Amazon wird sich da schon möglichst sauber halten. Das, was das Gerät ohnehin tut, ist schon schlimm genug. Und noch schlimmer ist, was da in Planung ist.

Wir haben nachgeschaut, was für Patente es gibt, die sich Amazon, Google und Co. gesichert haben und die sehr schön zeigen, wohin die Reise in die „Bedenken-Second-Zukunft“ gehen soll: Die Konzerne halten nicht nur Patente dafür, zu erkennen, WER spricht, sondern auch, aus der Stimme zu erkennen, in welcher Stimmung man gerade ist. Von einer App, die das nutzt, haben wir ja eben schon von Peter Wedde gehört. Wenn Mama vormittags verzweifelt weint, wird gleich Klosterfrau Melissengeist geliefert. Der Ruf „Alexa, Musik“ spielt dann entsprechend des Psychogramms, das dem Konzern geläufig ist, Punkrock oder Gregorianische Choräle ein. Oder Amazon ruft präventiv die Polizei, die die Wohnung „swattet“, wenn die Algorithmen aus der Stimme den Eindruck gewinnen, dass jemand vielleicht gleich ein Attentat verüben will. Es gibt Patente dafür, mehrere Stimmen zu unterscheiden und Personen zuordnen zu können. Da kann dann Klein-Bubi noch so oft mit tiefer Stimme „Alexa zeig Porno“ rufen, die Kindersicherung würde das verhindern. Die Nebenwirkung: Noch mehr manipulationsrelevante Informationen über die Privatsphäre und das Familienleben gehen an den Konzern.

▶Dass das „Alexa“ nur auf sein Schlüsselwort reagiert, ist auch bald Makulatur.◀

Foto: U.S.Army Materiel Command, cc by-sa 4.0

Wenn anhand der Stimme die Stimmung erkannt wird, könnten auch sogenannte Precrime- oder Preventive Crime-Systeme Interesse daran haben, ein SWAT-Team vorbei zu schicken, wenn der Algorithmus denkt, dass eine Straftat droht.

Und dass das „Alexa“ nur auf sein Schlüsselwort reagiert, ist auch bald Makulatur: Es gibt Patente, die den kompletten Audiostream nach bestimmten Keywörtern abfragen – und dann Werbung abspielen. Auf die Frage „Schatz, wollen wir heute Essen gehen?“ empfiehlt Alexa dann vorlaut das Sonderangebot bei „Little Italy“ und reserviert gleich einen Tisch auf der Terrasse.

Wie ein junger Hund versucht das „Alexa“ alles über uns zu lernen, indem es dauerhaft auf unsere Stimme, Intonation, bestimmte Wörter wie „mögen“ oder „gekauft“ hört, um das Aufgeschnappte wie alte gammelige Knochen im großen Datengarten von Amazon zu verbuddeln. Und Amazon belohnt mit Gollum-Stimme: „Mein Schatz!“

Foto: Matthias Hornung, cc by-sa 4.0

„Jetzt sagen die Konzerne wieder, dass sie das ja nie tun würden. Das höre ich seit 30 Jahren, und alles das, was ‚niemals umgesetzt würde‘, ist heute Normalzustand.“

Auch können die Kinder im Kinderzimmer automatisch verwarnt werden, wenn sie zu laut streiten, oder die Eltern werden gewarnt, wenn die Kinder im Flüsterton gemeinsam etwas aushecken.

Jetzt sagen die Konzerne wieder, dass das ja alles nur Features sind, die sie nur „mal so“ angemeldet hätten, das würden sie doch gar nicht einbauen wollen. Aber erstens höre ich sowas seit dreißig Jahren – und sehe, dass alles, was „niemals umgesetzt würde“ heute Normalzustand ist. Und zweitens können wir niemals wissen, ob solche Features mehr oder weniger heimlich oder auch offen implemetiert und freigeschaltet werden – oder es bereits schon sind.

Es geht nicht um „Missbrauch“. Es geht um das Potential, das dieses Gerät hat. Und das Potential, das die Firma Amazon hat, um genau das erbarmungslos auszunutzen. Zumal das Alexa (wie ein Smartphone) nichts anderes als ein Computer ist, für den alle möglichen Firmen jetzt sogenannte Skills – also Apps – programmieren, die wir auf dem „Alexa“-System installieren sollen und die alle wieder für sich irgendwie Daten aus dem Haus ins Netz schaufeln werden. Da gibt es den „Furz-Skill“ (ja, der tut genau das, was Sie jetzt denken – allerdings noch ohne Duftnote), den FoxNews-TV-Skill (der steht auf Platz 1 der beliebtesten Skills), den Abfallkalender-Skill (der in Bielefeld nicht funktioniert) und hunderte oder tausende mehr. Hinterher will es wieder niemand gewesen sein – wie bei Facebook, die vorgeben, fassungslos zu sein, was Cambridge Analytica mit ihren Daten gemacht hat. Dabei ist genau das Ausforschen von Menschen und ihren Angewohnheiten, ihren geheimsten Wünschen, ihren Freundschaften, ihren politischen Überzeugungen bis hin zu ihren Gesundheitsproblemen das Geschäftsmodell dieser Konzerne. So auch bei Amazon.

Foto: Susanne Holzgraefe, cc by-sa 4.0

Sabine Leutheusser-Schnarrenberger kam als Gastrednerin zu den BigBrotherAwards 2016 (hier neben Rena Tangens in der ersten Reihe). Alle Texte und Videos von unseren Verleihungs-Galas finden Sie auf bigbrotherawards.de.

Ich möchte den schwarzen Peter aber auch an die Menschen weiter reichen, die solche Spielzeuge in ihr Leben lassen und damit skrupellose Kaufleute dazu bringen, Instrumente herzustellen und zu verkaufen, die unsere Zivilisation gefährden. Das können wir an der just (Frühjahr 2018) laufenden Debatte zu Facebook sehen. (Facebook hat übrigens von uns schon 2011 einen BigBrotherAward bekommen – dem Text von damals haben wir auch in der 2018 laufenden Debatte um Cambridge Analytica nichts hinzuzufügen.)

Liebe Menschen. Seid vernünftig. Sabine Leutheusser-Schnarrenberger ist 1996 als Justizministerin zurückgetreten, weil ihre Partei den großen Lauschangriff beschließen wollte. Heute stellen wir uns einen riesengroßen Lauschangriff freiwillig in unsere intimsten Lebensbereiche. Liefert Euch nicht aus, behaltet Eure Widerstrebsamkeit, ohne die Zivilisation und Demokratie nicht lebendig existieren können. Ja, das bedeutet, dass wir den Wecker noch ein paar Jahre von Hand stellen müssen. Aber wenn das alle tun, können wir unsere Kinder und Enkel darum beneiden, dass sie Technik komfortabel nutzen können, ohne die Angst, Opfer von Manipulation und Machtinteressen zu werden. Denn es ist unsere Aufgabe, jetzt dafür zu sorgen, dass wir datenschutz- und freiheitsfördernde Technik bekommen. Das ist möglich! Doch dafür müssen wir hartnäckig und widerständig bleiben – auch gegenüber unseren Freundinnen und Freunden und gegenüber uns selbst – und wir dürfen weder der Technikgläubigkeit, noch dem Kontroll- oder Spieltrieb, der Bequemlichkeit oder dem Überwachungswahn nachgeben.

▶Hartnäckig und widerständig bleiben!◀

- Herzlichen Glückwunsch, Amazon, zum inzwischen dritten BigBrotherAward. (2015 in der Kategorie Arbeitswelt für die Überwachung von Logistik-Angestellten und in der Kategorie Wirtschaft für „Mechanical Turk“.)

Wie es weiter ging

Von Claudia Fischer

Kommentare unseres Publikums:

- „Alexa wäre nur der Anfang – siehe Richtung China.“
- „Noch ist es Zeit, selbstgewählter Überwachung und Kontrolle zu entgehen. Action gegen Alexa!“
- „Die Verletzung des Selbstbestimmungsrechts findet – weitgehend unbemerkt – in der eigenen Wohnung statt.“
- „Es wirkt so harmlos, wie ein Spielzeug.“

▶Voodoo-Zauber von Amazon

Uns gegenüber hat Amazon sich nicht zu Wort gemeldet. Der Spiegel zitierte Amazon mit einem kleinen Statement: „Alle Daten sind während der Übertragung und in der Cloud verschlüsselt. Der Kunde behält jederzeit die volle Kontrolle über seine Sprachaufzeichnungen. Jede einzelne Aufnahme kann einfach über die Alexa App oder Amazon.de gelöscht werden.“

▶“Cloud“ = Anderer Leute Computer◀

Dieses Statement ist gleich mehrfach falsch! Erstens: Nichts, was in der Cloud steht, ist noch unter der eigenen Kontrolle. Die richtige Übersetzung für „Cloud“ ist „Anderer Leute Computer“. Die Daten schweben nicht einfach so im Raum, sondern sind auf Amazon-Servern gespeichert. (Der Begriff „Cloud“ hat von uns 2012 einen BigBrotherAward bekommen).

Zweitens: Nicht Kunde oder Kundin haben die Kontrolle über die Aufzeichnungen, sondern die Person, die ein Alexa-Gerät angemeldet und in Betrieb genommen hat. Das sind nicht selten die Kinder oder Enkelkinder der eigentlichen Kundinnen und Kunden, manchmal auch hilfreiche Nachbarn oder (Ex-)Partner.innen. Es ist inzwischen beliebt, Technik an nicht so kundige Menschen zu verschenken mit dem freundlichen Hinweis „Und ich installiere Dir das Gerät dann auch gleich.“ Das bedeutet dann aber auch: jemand anders bekommt in seiner/ihrer App meine Sprachnachrichten zu sehen und zu hören. Das wissen die wenigsten und Amazon klärt darüber auch nicht so direkt auf. Ein El Dorado für Stalker und Spitzbuben! Und drittens: Ja, die einzelnen Aufnahmen können in der App gelöscht werden. Aber löscht das auch die Speicherung auf Amazons Servern? Und mal ehrlich: Wer will jeden Tag vom Wecker über die Wetterabfragen bis zum Kochrezept sein „Alexa“ aufräumen?

- padeluun: „Der Vorschlag ist weltfremd und eine Unverschämtheit! Außerdem sind bis zur Löschung die Metadaten-Sammeltools (wer, was, wann) und Stimmanalysen von Amazon mit Sicherheit bereits über die Aufnahmen hergefallen und haben sich rausgesaugt, was immer sie verdauen wollen. Ich kann mich nur wiederholen: Liebe Leute: Seid vernünftig! Lasst diese Spionagewanzen nicht in Eure Wohnungen!“

Foto: Justus Holzberger cc by sa 4.0

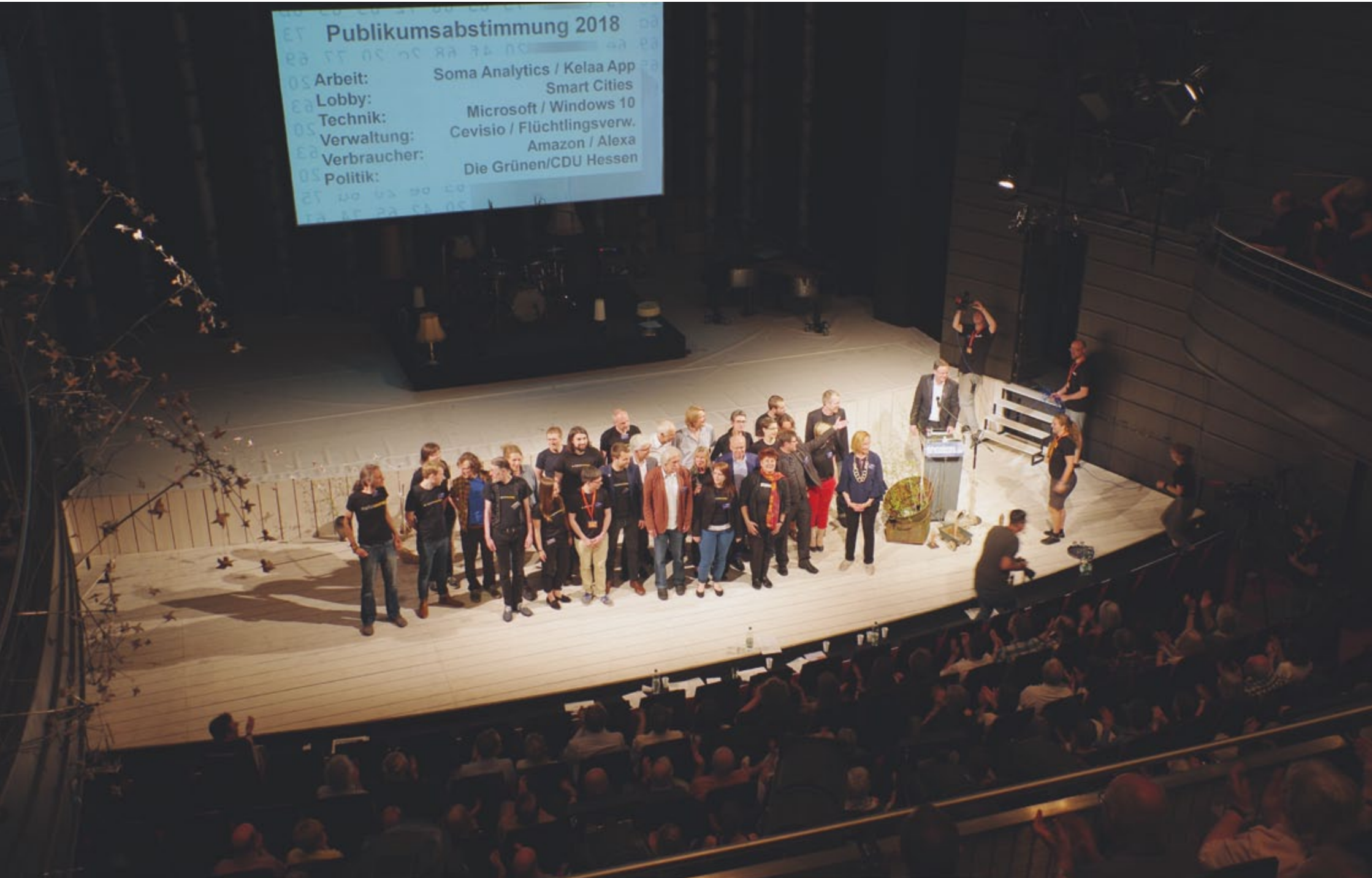


Foto: Fabian Kurz, cc by-sa 4.0

Die Big-Data-Illusion

Das Digitale und der Kampf um die Werte

Keynote bei den BigBrotherAwards 2018
von Dr. Sarah Spiekermann, Wirtschaftsuniversität Wien

Liebe Jury, liebes Publikum,

in der Moderne haben die Eliten – und ich denke da vor allem an Finanz-Eliten, Kapital-Eliten und politische Eliten – ein ganz eigenartig pointiertes Vorurteil angenommen und das lautet: Neu ist immer gleich gut. Ob nun also Menschen zu Robotern werden, Hunde zu Robotern werden, Kinder zu Robotern werden oder das Gras digital immer noch am schönsten ist: Neu scheint immer gleich gut zu sein.

Ich würde ja zustimmen wollen, dass dem Digitalen viel Gutes innewohnt, wie einem guten Glas Wein, aber wie in allen guten Dingen im Leben gibt es dann einen Punkt, da wird es schlichtweg zu viel. Und dieser Punkt ist für das Digitale erreicht. Ich würde behaupten, dass wir uns jetzt Gedanken machen müssen. Sie denken vielleicht an Ihre Smartphones, an Ihre Kinder, an die virtuellen Welten, an unsere Abhängigkeiten. Ich würde behaupten, dass wir uns ernsthaft darüber Gedanken machen müssen, wie wir Sorge dafür tragen, dass Digitalisierung auch in Zukunft zu unserem menschlichen Wohlbefinden beitragen kann und hoffentlich nicht ihre eigenen Kinder frisst.

▶Das Netz war und ist global gesehen ein gigantisches Friedensprojekt.◀

Die Digitalisierung konnte in den achtziger, neunziger Jahren ungeheure wirtschaftliche und private Vorteile durch IT schaffen. Das Netz war und ist global gesehen ein gigantisches Friedensprojekt, ein ökonomisches Integrationsprojekt, ein Demokratie-Projekt und ein Projekt, was uns auch in nie dagewesener Form Zugang zu Wissen gegeben hat. Das muss ich vor allen Dingen als Wissenschaftlerin natürlich positiv wertschätzen. Aber seitdem digitale Geräte breitbandig vernetzt sind – das ist Mitte der Zweitausender passiert – und angefangen haben, ein Eigenleben zu entwickeln, das uns permanent an diese Geräte bindet, seitdem – habe ich das Gefühl – geht es bergab. Und in meiner Forschung beschäftige ich mich mit diesem Knick nach unten, mit der Frage: Wann ist das Digitale eigentlich ins Negative abgekippt? Und ich möchte heute ein Thema vorstellen, das zu diesem Knick dazugehört: die Big-Data-Illusion.

▶Wann ist das Digitale eigentlich ins Negative abgekippt?◀

Bei der Big-Data-Illusion geht es um die Frage, welche Information eigentlich für uns als Menschen von Bedeutung ist, und dazu eine kleine Geschichte: Mein Mann und ich waren vor kurzem in Rom und wie man auf unserem Urlaubsfoto sehen kann, waren wir ziemlich enthusiastisch. Die Schönheit und der Zauber dieser Stadt hat uns wirklich voll erfasst. Im Pantheon haben wir ein ungeheures Gefühl von Zentralität empfunden. An einem tausendneunhundert Jahre alten Tempel steht man unter einer fünfzig Meter hohen Wand mit einer Öffnung, und diese Grandezza hat uns wirklich gefangen genommen. Wir haben im Vatikan gewohnt. In der Casa Marta sind wir sogar dem Papst begegnet, das hat in uns eine unglaubliche Ehrfurcht ausgelöst. Wenn man in die Kirchen von Rom kommt und in den Vatikan, dann ist dort die Schönheit und dieses ergreifende Gefühl, auch von Frömmigkeit und Vergangenheit, die einen irgendwie beschäftigt. Man fragt sich, welche Bedeutung dieses Vergangene für die Zukunft hat, und man denkt an Wünsche und Vorsätze.All das beschäftigt einen. Gleichzeitig weiß man: In statistisch 47 Prozent der Zeit denken Menschen an etwas anderes als das, was sie gerade tun. 47 Prozent. Und so haben auch wir, trotz der Schönheit Roms, an unser Haus in Österreich gedacht und haben uns überlegt, wo wir gerade renovieren, und die Planungen für die nächsten Wochen wa-

Links und weitere Infos: digitalcourage.de/jahrbuch19

ren mindestens so wichtig wie die nächste Straßenecke in Rom. Das sieht man natürlich auf unseren Urlaubsfotos nicht.Warum erzähle ich Ihnen das alles? Kurz: Unsere Wirklichkeit, was uns als Menschen ausmacht, ist, dass wir durch die Welt gehen. Vergangenheit, Zukunft, Gegenwart, Ferne, Nähe und vor allen Dingen die Werte: Zauber, Grandezza, Ehrfurcht, Frömmigkeit, das ist das, was für uns wesentlich ist und Bedeutung hat in unserem Leben. Und wissen Sie was? All das ist unsichtbar. Es ist nicht messbar. Es ist für Maschinen nicht erfassbar.

Maschinen sind sehr gut darin, Second-Hand-Daten zu erfassen. Also, Facebook kann zum Beispiel sofort auf den Fotos erkennen, dass wir lachen und dass wir somit ja offensichtlich fröhlich gewesen sein müssen. Sie wissen ja selbst, wie oft Sie fröhlich sind, wenn Sie in eine Kamera schauen. Facebook weiß auch, dass das auf dem Foto neben mir mein Mann ist. Weil es entweder die Daten zugekauft hat oder weil man es selbst eingegeben hat, und aufgrund des Geotaggings weiß die Plattform auch, dass wir bei der Aufnahme im Vatikan waren.

▶Sie wissen ja selbst, wie oft Sie fröhlich sind, wenn Sie in eine Kamera schauen.◀

Mein Mobiltelefon, mein Smartphone weiß noch viel mehr über mich, nämlich auch, an welcher Art von Ort ich war und welche Menge Menschen um uns herum war. Es weiß, ob es mir gut ging, denn die Handy-Sensoren messen meine Bewegungen. „Jetzt geht sie ein bisschen langsamer als normalerweise oder ein bisschen schneller – dann ist sie wohl offensichtlich gut drauf, oder? Sie hat Emotionen in ihren Smileys und so weiter, dann geht es ihr also offensichtlich ganz gut."

Foto: Fabian Kurz, cc by-sa 4.0

Einen First-Hand-Eindruck machte sich das Publikum bei den BigBrotherAwards.

Es gibt nur einen Haken: Ich bin nicht auf Facebook, mein Mann auch nicht. Auch keiner der Freunde, die für uns relevant sind, sind auf Facebook und wir würden so ein Foto auch nie posten. An diesem Platz hier, den Sie auf dem zweiten Foto sehen, war ich nie. Das Foto habe ich mir aus einer Bildergalerie hochgeladen. Und dieses Foto hier unten links, das stammt von meinem Mann, gar nicht von mir. Ach, und außerdem habe ich mein Telefon in Breitenbrunn tatsächlich auf dem Küchentisch vergessen. Es hat da die ganzen Tage dort herumgelegen und Apple hat wahrscheinlich gedacht: „Die bewegt sich gar nicht, die liegt bestimmt depressiv im Bett, sie schickt auch gar keine Nachrichten."

▶Er lässt ein Bild von uns entstehen, das sehr wenig mit unserer menschlichen Realität zu tun hat.◀

▶Was heißt das alles?

Der Second-Hand-Eindruck von uns ist extrem groß, aber er lässt ein Bild von uns entstehen, das eigentlich sehr wenig mit unserer menschlichen Realität zu tun hat. Während uns die Schöne-Neue-Welt-Spezialisten aus Silicon Valley erzählen, sie würden virtuelle Spiegelwelten herstellen, lassen uns klügere Leute wie Jaron Lanier wissen: Die tiefe Bedeutung des menschlichen Daseins wird reduziert auf eine Illusion von Bits.

Trotz dieses Defizits wird der digitale Abdruck, den wir hinterlassen – diese Second-Hand-Daten – als Öl auf den Personal-Data-Markets heute gehandelt und die künstlichen Intelligenzen werden auf diesen Second-Hand-Daten trainiert.

Foto: Fabian Kurz, cc by-sa 4.0

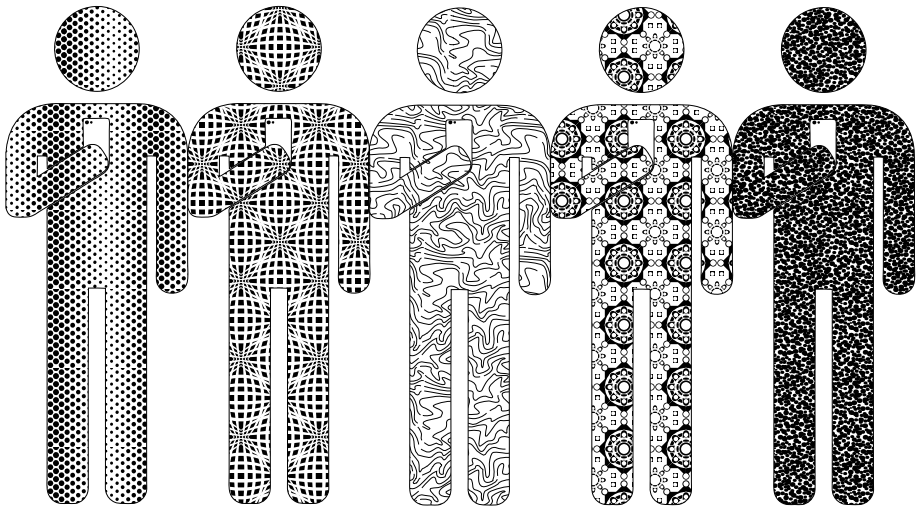
„Neu ist immer = gut" – warum eigentlich?

Und dann erzählen sie uns, dass unsere Zukunft darin bestünde, zum Cyborg zu mutieren.

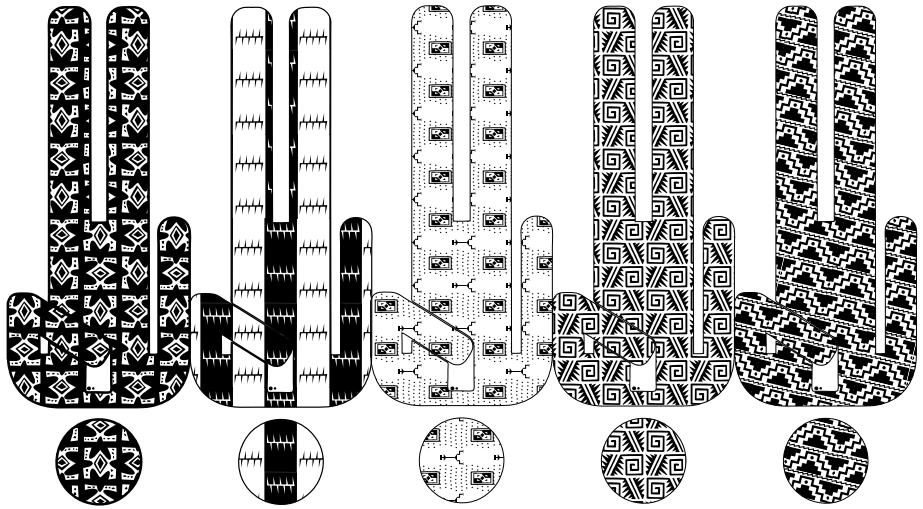
Die Leute, die heute diese Big Data sammeln, verwalten und managen, wissen sehr wohl um diese nicht zufriedenstellende Situation ihrer Second-Hand-Daten. Die wissen, dass ihre Daten nicht vollständig sind, dass sie oft falsch sind, dass sie selektiv sind, und dass sie über Kontexte hinweg, wenn sie verbunden werden, auch verfremdet werden. Und was machen sie? Was ist ihre Antwort, ihre Strategie? Sie wollen mehr Daten. Sie sind auf der Suche nach dem Unsichtbaren, nach dem, was ich gerade beschrieben habe, dem nicht Messbaren. Aber wie wollen die das eigentlich je messen?

Ihre Strategie ist, dass sie uns einfach vollständig mit Technologie eindecken und zuschmeißen, um uns zu – man sagt das im Englischen – zu „envelopen“, mit Smart Homes und Smart Klos und Smart Glasses und Smart Chips unter die Haut und wer weiß noch was, und dann erzählen sie uns, dass unsere Zukunft darin bestünde, zum Cyborg zu mutieren.

Selbst die Museen in großen Städten machen inzwischen Ausstellungen (z.B. im Museum moderner Kunst in Wien) über die Zukunft des Menschen als Cyborg. Und selbst die britische Regierung wirbt mittlerweile dafür, dass man sich Chips und Prothesen einsetzen lassen kann. Es wird ein ungeheurer Unsinn verbreitet, nur damit diese Branche mehr Daten bekommt. Denn während wir lustig mit unserem IT-Zeug spielen, entstehen parallel gigantische Second-Hand-Datenmärkte. Datenmärkte, die zwar groß sind, aber voller Fehler und Einseitigkeiten und am Rande der Legalität. Nehmen wir mal eine Firma wie Axion. Die schreiben offiziell, dass sie 700 Millionen Profile haben und für jeden Menschen, also wahrscheinlich auch für alle hier im Raum, auf ungefähr 3.000 Dateneinträge pro Person zugreifen können. Noch schlimmer, Oracle, mit der Tochterfirma Oracle Key, spricht von 700 Millionen Profilen und sie haben angeblich 30.000 Attribute in Echtzeit. Sie haben Kooperationen aufgebaut mit allen Kreditkartenunternehmen der Welt, mit Facebook usw., unglaublich.



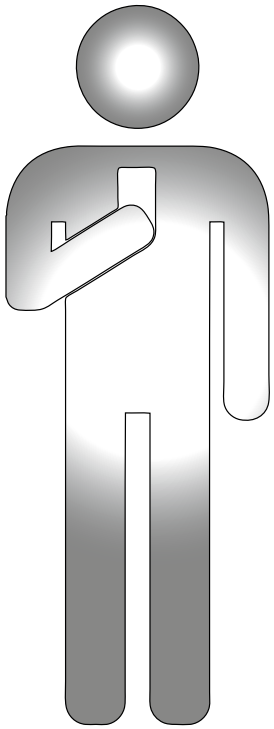
Smombie-Grafik: Dennis Blomeyer, cc by-sa 4.0; Adaption: Isabel Wienold



Die Menge an Daten sagt gar nichts über deren Qualität und Bedeutung für uns aus.

Wir dürfen nur eines nie vergessen: Die Menge an Daten sagt gar nichts über deren Qualität und, wie gesagt, deren Bedeutung für uns aus. Trotzdem hat sich eine gigantische Zahl von weit über tausend Firmen etabliert, die alle von dem Versprechen leben, dass diese Daten irgendwann mal etwas wert sein werden und dass sie alle diese ganzen Second-Hand-Daten professionell sammeln. Sie versuchen jetzt, diese Dienste, die noch mehr Daten sammeln, massiv in die Haushalte zu drücken, Stichwort Smart Home. Einsicht in das Unsichtbare.

Aber wie gut funktioniert denn all diese tolle Werbung, die uns personalisiert zugespielt wird? Die neuesten Untersuchungen zeigen, dass 95 Prozent der Werbung, die man bekommt, im falschen Moment kommt. Trotz der 30.000 Daten pro Person. Und daher gibt es ein Problem für diese tausenden von Firmen: Sie können in Zukunft nicht von Werbung leben. Das weiß auch jeder, der in der Branche arbeitet, dass das nicht gehen



Smombie-Grafik: Dennis Blomeyer, cc by-sa 4.0; Adaption: Isabel Wienold

wird. Aber wenn heute schon jeder Mensch von uns 3.000 Werbungen pro Tag bekommt und 85 Prozent davon gar nicht wahrnimmt, wovon leben diese Firmen dann?

Sie leben von einer Unzahl von Anwendungsfeldern, in denen Second-Hand-Daten heute als gut genug akzeptiert werden. Für die Werbung ist das übrigens gut genug, diese 30.000 Einträge, auch wenn eben 85 Prozent in die Hose gehen. Macht ja nichts, denn es betrifft uns ja nicht wirklich. Aber: Die Daten sind in jedem Fall gut genug, um unsere Freiheit und Demokratie zu untergraben, indem sie Facebook dazu verhelfen, arabische Frühlinge zu organisieren, amerikanische Präsidentschaftswahlen zu manipulieren und Europa in den Brexit zu jagen. Sie werden auch als gut genug angesehen, um unser Wohlbefinden zu untergraben, weil Institute unsere Kreditwürdigkeit auf dieser lückenhaften Basis bewerten und unsere Versicherungsraten in den AGBs daran anpassen und genau wie Flugpreise in Echtzeit je nach Kaufbereitschaft und Zahlungsmöglichkeiten angepasst werden.

Sie werden herangezogen, um die Güte von Job-Bewerbern zu prüfen und damit über die Zukunft von Menschen zu entscheiden. Sie werden als gut genug empfunden, um Software-Assistenten wie Alexa zu trainieren, die dann unsere Kinder erziehen, und immer mehr Länder ziehen diese Second-Hand-Daten auch heran, um Polizeieinsätze zu planen, wie in China zum Beispiel, wo jetzt individuelle Vertrauens-Scores pro Bürger ausgerechnet werden. Wie sicher darf man sich in Zukunft in Ländern fühlen, die Second-Hand-Daten benutzen, um fundamentale Eingriffe in die Freiheit von Bürgern zu legitimieren? Immer mehr Menschen, Politiker, Sicherheitsbehörden oder Journalisten fällen ihre Entscheidungen auf der Basis ihrer eigenen Filter-Bubbles und Echo-Chambers, die auf diesen Second-Hand-Daten aufgebaut sind und die ihnen eine scheinbar objektive Datenwelt in ihre Twitter- und Facebook-Nachrichten spielen. Und das Resultat ist: Das sind postfaktische Konflikte, in denen jeder nur noch seine tatsächlich eigene Wahrheit kennt und der öffentliche Raum als Grundlage jeder Demokratie zusammenbricht.

- Zusammengenommen untergräbt also eine gigantische Big-Data-Illusion unsere Werte und es ist wirklich höchste Zeit, dass diese Blase platzt und wir diese ganze Big-Data-Illusion mal kritisch hinterfragen und endlich wieder Realismus einzieht.

Herzlichen Dank!

Foto: Justus Holzberger, cc by-sa 2.0

Unsere Bühnendeko wurde auch in diesem Jahr gezaubert von Angelika Höger.

BigBrotherAwards

Was macht eigentlich ...?

Von Claudia Fischer

Meistens freut man sich ja, alte Bekannte zu treffen – bei uns lösen BBA-Preisträgerinnen und –Preisträger, die uns in Medienberichten wieder begegnen, meistens eher ein Augenrollen aus. Denn einige machen einfach weiter oder setzen in Folgejahren, nachdem sie von uns mit dem Negativpreis ausgezeichnet wurden, auch noch „eins drauf“. Wir beobachten diese Entwicklungen nicht besonders systematisch, aber immer mal wieder. Eine bunte, mal gruselige, mal amüsante Auswahl aus den letzten 12 Monaten haben wir für Sie alphabetisch zusammen gestellt. Belege, Links und Original-Artikel finden Sie über die Jahrbuch19-Webseite (siehe unten).

Bayer AG

▶BBA 2002 für Urinproben bei Auszubildenden

Nicht nur die Supermarktkette Real (BBA an die Metro-Group 2005) und die Post (BBA 2013 an die Post Adress) haben im vergangenen Jahr versucht, in ihren Filialen Gesichter von Kundinnen und Kunden zu erfassen und zu analysieren. Das wurde nach unseren Protesten gleich wieder eingestellt.

Nein, auch die Bayer AG hat das probiert, und zwar in einem besonders sensiblen Bereich: In Apotheken! Ende November 2017 wurde bekannt, dass Bayer die

Foto: Fabian Kurz, cc by-sa 4.0

Rolf Gössner geißelte mit dem BigBrotherAward 2017 Ursula von der Leyen für ihre Cyberkrieg-Initiative. Sie ist immer noch Verteidigungsministerin.

Gesichter von Kund.innen in zwei Apotheken in Österreich nach Alter, Geschlecht und Länge des Blickkontakts automatisch auswerten ließ. Nach den ersten kritischen Presseberichten wurde der Versuch beendet – vermutlich aus Angst vor negativer Presse und Kritik von Kund.innen. In Österreich kann man also jetzt wieder Schwangerschaftstests, Hämorrhoidensalbe oder Viagra kaufen gehen, ohne eine Skimaske überzuziehen. Wir haben dazu ein Interview für Spiegel-Online gegeben.

Bundeswehr

▶BBA 2017 an Ursula von der Leyen für die Cyberkrieg-Offensive

Wir haben eine neue Bundesregierung. Frau von der Leyen ist weiterhin Verteidigungsministerin.

Wir empfehlen die Aufkleber des Künstlerkollektivs !Peng. Diese machen die Website www.bundeswehr.lol bekannt. Sie sind erhältlich in unserem Shop (siehe Anzeige).

Change.org

▶BBA 2016 für den Umgang mit Adressen

Es traf nicht change.org, sondern eine ähnliche Online-Petitions-Plattform: avaaz.org bekam im Februar 2018 eine 168seitige Anklageschrift des durch Gentechnik und Umweltgifte wie Glyphosat in Verruf geratenen Saatgut-Konzerns Monsanto (übrigens inzwischen aufgekauft von der Bayer AG, siehe oben). Monsanto forderte von avaaz.org die Herausgabe von Unterlagen, Korrespondenzen und E-Mail-Adressen von Menschen, die Petitionen gegen den Einsatz von Glyphosat unterschrieben haben.

Auch wenn Monsanto die Drohung nicht wahrgemacht hat: Das war ein Dammbruch! Hier wendet sich ein Konzern nicht nur gegen eine Organisation, die Kritik übt, sondern er fordert auch die Daten der Einzelpersonen ein, die diese Kritik unterstützen. Sie haben wohl gedacht „Frechheit siegt“.

▶Wir können nur wiederholen, wie wichtig es ist, mit den Daten von Online-Unterschriftensammlungen höchst gewissenhaft umzugehen.◀

Sowohl Avaaz.org als auch change.org speichern ihre Unterschriftenlisten in den USA und wir werden nicht müde zu betonen, dass dort auch US-Behörden und Geheimdienste über den FISA Act Zugriff darauf fordern können.

Change.org haben wir aus genau diesem Grunde 2016 einen BigBrotherAward verliehen – kurz nach der Preisverleihung 2016 tauchte übrigens in Italien eine Preisliste auf, mit der Change.org seine gesammelten Adressen zum Kauf anbot (unser Blog-Artikel dazu ist über die Jahrbuch19-Webseite verlinkt).

Erhältlich im Digitalcourage-Shop!
Aufkleber: www.bundeswehr.lol

Aufkleber, 10 Stück
bedingt nass- und
UV-fest (für Außeneinsatz)
9,8 x 4,2 cm
10 Stück 0,30 Euro

▶ **https://shop.digitalcourage.de**

Foto: Raimond Spekking, cc by-sa 4.0

Die DİTİB-Zentralmoschee in Köln. DİTİB fällt immer wieder mit türkischer Regierungspropaganda auf.

DİTİB

▶BBA 2017 für Imame, die ihre Gemeinde bespitzeln

Die Türkisch-Islamische Union DİTİB hatte 2017 in ihrem Schreiben an uns noch betont, dass sie nicht mit dem türkischen Regime zusammen arbeitet, sondern lediglich „Empfängerin der religiösen Dienste seitens der DIYANET“, der türkischen Religionsbehörde, sei. Zur Erinnerung: In genau diesem Brief, der uns kurz vor der Preisvergabe 2017 erreichte, hatte uns die DİTİB eine Klage angedroht. Wir haben uns davon nicht einschüchtern lassen und den Preis trotzdem vergeben. Die weiteren Entwicklungen bestätigen uns in dieser Entscheidung:

Denn 2018 gerieten DİTİB-Gemeinden mehrfach in die Schlagzeilen, weil sie z.B. in Hessen und Nordrhein-Westfalen

Kriegspropaganda verbreitet haben. Ende August 2018 teilte das Bundesinnenministerium mit, dass vorerst keine DİTİB-Projekte mehr gefördert werden.

Facebook

▶BBA 2011

Dass Facebook 2018 in den Schlagzeilen war, führen wir hier nur der Vollständigkeit halber auf. Das wird nicht an Ihnen vorbei gegangen sein.

Aber falls Sie Facebook immer noch nutzen, ist Ihnen vielleicht folgendes entgangen: Kurz vor Einführung der DSGVO hat der Konzern Milliarden von außereuropäischen (z. B. afrikanischen oder asiatischen) Nutzerdaten aus Irland in die USA verschoben. Dort unterliegen sie nicht den neuen, verbraucherfreundlichen europäischen Datenschutzgesetzen.

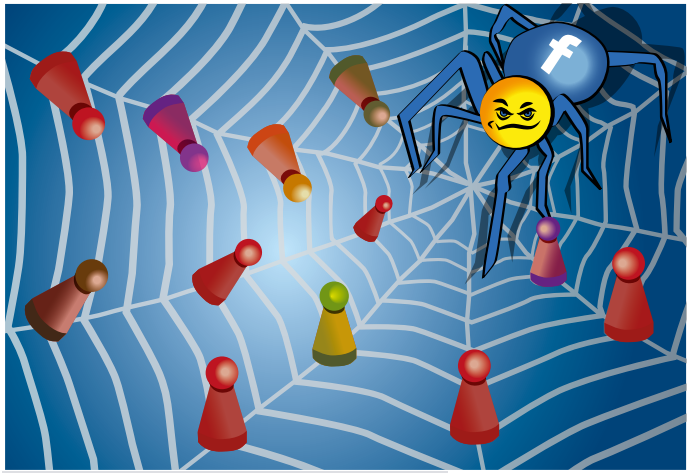


Illustration: Isabel Wienold, cc by-sa 4.0

Facebook erhielt schon 2011 von uns einen BigBrotherAward. Dem aktuellen Cambridge Analytica-Skandal 2018 hatten wir nichts hinzuzufügen.

Gamma-Group / FinFisher

▶BBA 2012

Die gute Nachricht ist, dass das „Defender"-Programm von Microsoft (BBA 2002 fürs Lebenswerk und für 2018 Windows 10) den Staatstrojaner „FinFisher" der Gamma-Group bei einem Test im März 2018 gefunden hat. Dieser Trojaner ist also gerade nicht geheim, sondern auffindbar.

Die schlechte Nachricht ist, dass diese Erfolgsmeldung nicht von Dauer sein wird. Die Programmierer von „FinFisher" werden versuchen, den Staatstrojaner besser zu verstecken. Und die Virenscanner werden versuchen, ihn weiterhin zu finden. Ein Wettlauf, der Unmengen an Geld verschlingt und die allgemeine Sicherheit gefährdet. Sicherheitslücken müssen geschlossen, und nicht von staatlichen Behörden ausgenutzt werden.

▶ Staatstrojaner gehören in die Tonne!

Foto: opyh cc by-sa 4.0

Seit Jahren wird gegen die Elektronische Gesundheitskarte protestiert. Jetzt ist auch der neue Gesundheitsminister Jens Spahn nicht zufrieden damit – und hat noch schlimmere Ideen.

Gesundheitskarte

▶BBAs 2004 und 2015

Dass wir gegen die elektronische Gesundheitskarte und die Systeme drumherum sind, haben wir bereits in zwei BBAs ausführlich begründet. So horchten wir kurz auf, als es hieß, der neue Bundesgesundheitsminister Jens Spahn wolle die Karte auch nicht mehr. Aber Jens Spahn wäre nicht Jens Spahn, wenn er nicht deutlich über das Ziel hinaus geschossen hätte: Er kündigte im Mai 2018 an, die Gesundheitskarte durch eine allumgreifende Identitätsnummer ersetzen zu wollen, mit der wir zukünftig sowohl einen Pass beantragen als auch unsere Steuererklärung abgeben oder unsere Gesundheitsakte einsehen könnten.

Die Idee wurde nicht weiter diskutiert. Wir hoffen, jemand hat ihm fürsorglich, aber mit Nachdruck erklärt, dass lebenslange ID-Nummern für Personen gefährlich und zentrale Datensammlungen dieser Art keine gute Idee sind. Vermutlich hat er es noch nicht eingesehen. Denn nun spricht er davon, Gesundheitsdaten auf Smartphones auszulagern.

Datenschutz ist Verbraucherschutz. Machen Sie uns stark!

▶ https://digitalcourage.de/mitglied

Lidl

▶BBA 2004 wegen Ausschnüffelns von Angestellten

In ihrer Laudatio zur Discounter-Kette Lidl benannte Laudatorin Rena Tangens 2004 ein pikantes Detail: Der Gründer der Lidl-Unternehmensgruppe, Dieter Schwarz, taucht grundsätzlich nicht auf Fotos auf. Das ist sehr auffällig für einen deutschen Großunternehmer. Und das war auch im Februar 2018 wieder so: Da spendete die Dieter-Schwarz-Stiftung der Technischen

Foto: Claudia Fischer, cc by-sa 4.0

Lidl-Inhaber Dieter Schwarz hält sich aus Bildern raus.

Universität München (BBA 2017 für datenschutzrechtlich riskante US-Online-Kurse) gleich 20 Professorenstellen. Und Dieter Schwarz selbst war mal wieder weit und breit nicht zu sehen.

Mattel, Toytalk

▶BBA 2015 für die „Hello Barbie“ und „Track your Kid“: BBA 2004 für Handyortung bei Kindern

Das Thema begegnet uns immer wieder. Ob beim „Schutzranzen“-Projekt (siehe Seite 13), oder ob Puppen mit Abhörgeräten verkauft werden – immer wieder versuchen verantwortungslose Firmen, aus der Angst von Eltern um die Sicherheit ihrer Kinder, gepaart mit Spieltrieb, Profit zu schlagen. Nach der „Hello Barbie“ (BBA 2015), die es gar nicht erst in deutsche Spielzeugregale geschafft hat, kam die Puppe „Cayla“, die von der Bundesnetzagentur verboten wurde und aus dem Spielzeughandel genommen werden musste. Aber sie lassen nicht locker: Auf der Spielwarenmesse „Toy Fair“ in New York 2017 wurde eine Hologramm-Barbie präsentiert, die den Kindern z.B. Wetterberichte für ihren Wohnort erzählen kann. In Presseberichten wird ausdrücklich erwähnt, dass Mattel nach eigenen Angaben keine Sprachbefehle mehr speichern will und Daten verschlüsselt übermittelt werden – selbst wenn wir ihnen das glauben: Zur Befehlsanalyse müssen die Tonaufnahmen auf Mattelservern landen und das Standort-Erfassungs-Feature ist offenbar neu hinzugekommen. Sie geben nicht auf...

2018 sind dann auch noch Smartwatches, also Armbanduhren, aufgefallen, weil sie sich ganz einfach anrufen ließen und dann die Umgebung abgehört haben.

Wir wiederholen den Appell von padeluun in seiner Alexa-Laudatio: „Liebe Menschen. Seid vernünftig. Gebt dem Spieltrieb nicht nach!“ (siehe Seite 94).

▶Abhörwanzen gehören nicht ans Handgelenk und schon erst recht nicht ins Kinderzimmer!

Foto: Susanne Holzgraefe, cc by-sa 4.0

Puppen mit Mikrofon und Server-Verbindung – Überwachungsspielzeug hat im Kinderzimmer nichts zu suchen!

Foto: Internet-Meme, Quelle unbekannt

„Wie könnte nur dieser geheime Zugangscode lauten?“
Wie Sie Ihre Daten besser für sich behalten, verrät Ihnen unsere AG Digitale Selbstverteidigung.

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
▶ https://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.

Selbstverteidigungsabbildungen: Panthermedia

DSGVO: Nutzen Sie Ihre Rechte aus der EU-Datenschutzgrundverordnung

Die europäische Datenschutzgrundverordnung enthält eine ganze Reihe an Rechten für uns Verbraucher.innen. Diese galten in Deutschland durch das Bundesdatenschutzgesetz schon vorher fast genauso. Aber wer die neuen Betroffenenrechte nutzen will, muss sich auf die Artikel der Grundverordnung berufen. (Dieser Artikel ersetzt keine Rechtsberatung – die können und dürfen wir nicht geben.)

Art. 15: Auskunftsrecht

Sie haben das Recht zu erfahren, ob personenbezogene Daten von Ihnen verarbeitet werden oder nicht. In beiden Fällen haben Sie das Recht auf Auskunft – zum Beispiel darüber, welche Daten zu welchem Zweck verarbeitet werden, woher diese Daten stammen, an wen sie weitergegeben werden und ob und wie lange die Daten gespeichert werden. Falls keine Daten von Ihnen verarbeitet werden, muss Ihnen auch das mitgeteilt werden. Außerdem muss Ihnen darüber Auskunft gegeben werden, ob und wie die Daten eine Rolle in einer automatisierten Entscheidungsfindung (z.B. durch Algorithmen) spielen.

Art. 16: Recht auf Berichtigung

Das Recht auf Berichtigung besagt, dass Sie eine Korrektur falscher Daten verlangen können.

Art. 17: Recht auf Löschung

Sie haben das Recht, dass Ihre persönlichen Daten auf Ihren Wunsch hin gelöscht werden, z.B. wenn die Daten zu dem Zweck, zu dem sie erhoben wurden, nicht mehr gebraucht werden, wenn Sie die Einwilligung widerrufen oder die Daten unrechtmäßig verarbeitet wurden. Sollten Ihre Daten noch benötigt werden, können Sie sie nach Artikel 18 auch sperren lassen.

Zudem ist in der DSGVO ein „**Recht auf Vergessenwerden**“ verankert. Der Grundgedanke ist, dass personenbezogene Daten nicht dauerhaft im Netz auffindbar (z.B. durch Suchmaschinen) sein sollen, wenn die betreffende Person das nicht will. In der DSGVO ist dieser Gedanke leider nur teilweise abgebildet: Stellen Sie einen Antrag auf Löschung, müssen die Verantwortlichen dies an betreffende Stellen, z.B. Suchmaschinen, weitergeben. Eine Garantie auf die tatsächliche Löschung der Links ist das nicht.

Art. 20 Recht auf Datenübertragbarkeit

Sie wollen einen Anbieter wechseln und Ihre Daten mitnehmen? Meistens können Sie nun von Sozialen Netzwerken, Telefonanbietern, Versicherungen oder Banken eine Kopie Ihrer nicht Informationen, die aus der Verarbeitung dieser Daten gewonnen wurden. Sie können die Daten entweder für sich selbst verlangen oder an den neuen Anbieter weiterleiten lassen.

Art. 21 Widerspruchsrecht

Zum Beispiel Ämter und Behörden dürfen Ihre Daten verarbeiten auch ohne dass Sie dem zustimmen. Sie haben allerdings ein Widerspruchsrecht im Fall besonderer persönlicher Umstände. Wenn Sie dieses Recht geltend machen, dürfen die Daten nur noch verarbeitet werden, wenn gewichtige Gründe nachgewiesen werden, die Ihre Interessen, Rechte und Freiheiten überwiegen.

Art. 22: Automatisierte Entscheidungen

Artikel 22 DSGVO zufolge haben Sie das Recht, dass gravierende Entscheidungen über Ihre Person nicht ausschließlich auf automatisierten Verarbeitungen Ihrer Daten oder Profiling (z.B. durch Algorithmen) beruhen. Leider ist es leicht, dieses Recht auszuhebeln: Es reicht, wenn eine Person das Ergebnis der automatisierten Verarbeitung formell bestätigt, und schon gilt es nicht mehr als „ausschließlich automatisiert“.

Art. 77: Ihr Recht auf Beschwerde

Nach Artikel 77 haben Sie das Recht, sich bei einer Aufsichtsbehörde zu beschweren – zum Beispiel bei den Landesbeauftragten für Datenschutz an Ihrem Wohnort, am Arbeitsplatz oder auch woanders. Diese Aufsichtsbehörde kümmert sich um Ihr Anliegen und hält Sie dann auf dem Laufenden, was den Stand Ihrer Beschwerde betrifft.

Machen Sie sich bewußt, **wem gegenüber** Sie die Betroffenenrechte haben. Versuchen Sie die Datenschutzbeauftragten der jeweiligen Stelle zu ermitteln, die Ihre Daten verarbeitet. Dort können Sie Ihre Rechte **schriftlich beantragen**. Beziehen Sie sich auf den entsprechenden Artikel in der DSGVO. Es gibt Musterformulare – Links finden Sie auf der Jahrbuch19-Webseite. Mit einer Antwort können Sie **innerhalb eines Monats** (festgelegte Frist) rechnen. Auch über eine Fristverlängerung müssen Sie innerhalb eines Monats unter Angabe der Gründe informiert werden.

Wenn die Verantwortlichen Ihrem Antrag nicht nachkommen, können Sie **Beschwerde bei einer Aufsichtsbehörde** einreichen. Die Adressen der Landesdatenschutzbeauftragten aller Bundesländer und Mustervordrucke finden Sie ebenfalls auf der Jahrbuch19-Webseite. Die Behörde muss sich innerhalb von drei Monaten um Ihr Anliegen kümmern und Ihnen ein Ergebnis oder einen Zwischenstand mitteilen.

Und wenn das Unternehmen keinen Sitz in der EU hat?

In der DSGVO ist das so genannte Marktortprinzip verankert. Dieses Prinzip besagt, dass alle Unternehmen sich an die DSGVO halten müssen, die sich offensichtlich an europäische Kund.innen richten, auch wenn sie keine Niederlassung in der EU haben.

Außereuropäische Unternehmen, auf die das zutrifft, müssen einen Vertreter in der EU benennen. Bei diesem Vertreter können Sie Ihre Betroffenenrechte geltend machen, außerdem ist er Ansprechpartner für die Aufsichtsbehörden.

Wie Sie Ihre Passwörter richtig behandeln

Tipps zum Erstellen von sicheren Passwörtern gibt es zuhauf im Internet. Was bei besonders ausgeklügelten technischen Tricks häufig aus dem Blick gerät, ist das richtige Verhalten im Umgang mit Passwörtern.

- **Verwenden Sie für verschiedene Zugänge nicht das gleiche oder ähnliche Passwort.** Damit wird verhindert, dass ein.e Angreifer.in ein erbeutetes Passwort bei einem anderen Zugang wieder nutzen kann.
- **Verschieden sichere Passwörter für verschiedene Zwecke.** Manchmal reicht „passwort123“. Für wichtige Zugänge aber, z.B. zum E-Mail-Postfach, zum Online-Banking oder zum Sozialen Netzwerk, sollten die Passwörter besonders lang und schwer zu erraten sein. Bedenken Sie, dass jemand, der oder die das Passwort für Ihre Mails kennt, auch fast alle Ihre anderen Passwörter bekommen kann, wenn er oder sie jeweils die „Passwort vergessen“-Funktion benutzt.
- **Passwörter auch mal ändern.** Wie oft Sie das tun, sollten Sie je nach Sensibilität des Zugangs entscheiden und eine Erinnerung z.B. in den Kalender (oder ein Passwortverwaltungsprogramm, wir empfehlen KeePass oder KeePassX) eintragen.
- **Passwörter niemals weitergeben oder im Klartext (= unverschlüsselt) versenden!** Auch wenn es schwer fällt: Selbst unsere Liebsten sollten unsere Passwörter nicht kennen. Wenn die Weitergabe einmal unvermeidlich ist, dann ändern Sie das entsprechende Passwort sofort danach. Das Passwort für sich zu behalten bedeutet auch: Benutzen Sie keine Passwort-Generatoren im Internet!
- **Schicken Sie Ihre bestehenden Passwörter keinesfalls an Webseiten, die Ihnen versprechen, die Sicherheit Ihres Passwortes zu überprüfen.** Der von uns empfohlene Identity Leak Checker (einen Link finden Sie auf der Jahrbuch19-Webseite) fragt z.B. nach Ihrer Email-Adresse, fragt aber nicht nach Ihrem Passwort).
- **Passwörter nicht direkt neben dem Gerät lagern.** Aber: Es ist besser, ein sicheres Passwort zu verwenden und aufzuschreiben, als ein unsicheres Passwort zu benutzen. Denn letzteres kann eine Angreiferin oder ein Angreifer erraten. Um an ersteres zu kommen, braucht sie oder er den Zettel. Und der ist im Portemonnaie passabel sicher verstaut – wenn nicht dabei steht, für welchen Zugang es ist. Ein sicher verwahrtes Passwort (etwa in einem Safe oder Bankschließfach) ist sogar empfehlenswert, wenn Sie möchten, dass berechtigte Personen im Falle eines Unfalls Zugriff auf Ihre Daten bekommen können.

Selbstverteidigungsabbildung: Panthermedia

Verschlüsseltes Surfen mit HTTPS

Ein erster Schritt in Richtung sicheres Surfen ist die **Benutzung von HTTPS** beim Besuchen von Internetseiten. Achten Sie darauf, dass hinter dem „http“ in der Adresszeile möglichst immer ein „s“ (für „secure“) steht oder ein Symbol mit einem Schloss zu sehen ist. Schreiben Sie bei Bedarf selbst „https://“ davor.

Was ist HTTPS?

Damit z.B. Websites über das Internet übertragen und auf Ihrem Gerät angezeigt werden können, braucht es ein sogenanntes „Übertragungsprotokoll“. HTTPS ist die verschlüsselte Variante von HTTP, dem Internetprotokoll, über das sich Websites aufbauen und Daten im Internet übertragen werden. Mit HTTPS werden die Daten zwischen der Website und dem eigenen Computer verschlüsselt übertragen. Auch die Identität der Gegenseite wird geprüft. Dadurch kann unterwegs kein Unbefugter die Daten im Klartext mitlesen oder gar manipulieren.

Nicht nur beim Online-Banking

Vielen wird HTTPS, wenn vielleicht auch unbewusst, schon beim Online-Banking begegnet sein. Dort werden Daten aus gutem Grund nicht im Klartext, sondern verschlüsselt übertragen. Alle Web-Formulare, in die Sie z.B. Ihre Adresse oder einen Benutzernamen und ein Passwort eintragen, müssen seit der europäischen Datenschutzgrundverordnung (DSGVO, Mai 2018) mit HTTPS ausgestattet sein. Zur Sicherheit sollten Sie sich aber immer mit einem kurzen Blick vergewissern, bevor Sie Ihre Daten eingeben.

Doch HTTPS ist nicht beschränkt auf Online-Banking oder Webshops: Immer mehr Websites bieten neben dem unverschlüsselten Abrufen ihrer Inhalte auch eine verschlüsselte Version an.

Automatisch HTTPS

Ein einfaches Tool, mit dem man automatisch die HTTPS-Version von Webseiten benutzt, ist die Erweiterung HTTPS-Everywhere, die für die Webbrowser Firefox und Chrome verfügbar ist. Sie sorgt dafür, dass Webseiten automatisch mit einer HTTPS-Verbindung angesurft werden, wenn diese verfügbar ist.

Selbstverteidigungsabbildung: Panthermedia

Ist dieser Link sicher?

Oft erhalten wir E-Mails mit Links und wissen nicht, ob wir sie anklicken sollten – hier ein kleiner Tipp: Bewegen Sie den Mauszeiger auf den Link, ohne zu klicken. Unten links im Bildschirmfenster wird bei den meisten Programmen dann angezeigt, wohin dieser Link führt. Beginnt der Link mit https? Führt er z.B. zu Ihrer Bank oder ganz woanders hin?

Lightbeam – durchleutet das Internetdickicht

Wollen Sie wissen, wer alles weiß, was Sie im Internet tun? Lightbeam gibt Ihnen Antworten:

Ein Großteil der heutigen Webseiten bindet Inhalte wie Schriftarten, Werbung, Webstatistik-Tracker, Bilder, Videos und andere Ressourcen von Drittanbietern wie Google, Facebook, Twitter und einigen großen Content Distribution Networks (CDN) ein. Dieses Verhalten ist problematisch, weil Drittanbieter wie Facebook dann genau sehen, wann welche Webseiten von Benutzer.innen besucht werden, selbst wenn Sie nie einen Facebook-Account genutzt haben. Es entsteht eine Art „digitaler Verfolgungsspur“. Haben Sie einen Account und loggen sich gleichzeitig oder später namentlich ein, dann kann Facebook dieser digitalen Verfolgungsspur entsprechend Ihren Namen und Ihre Anschrift zuordnen. Gleiches gilt auch für Google, Twitter und viele Werbefirmen.

Mit dem Internet-Browser Firefox kann diese Verfolgung leicht aufgedeckt werden. Dafür ist die Browser-Erweiterung Lightbeam praktisch. Lightbeam stellt die Verbindungen zu Drittanbietern grafisch dar und erlaubt so einen Blick hinter die Kulissen. Verschaffen Sie sich einen Überblick darüber, welche Drittanbieter der Webseiten, die Sie besuchen, Ihr Surfverhalten verfolgen können.

Nach der Installation von Lightbeam erscheint das Lightbeam-Logo rechts oben in Ihrer Symbolleiste. Klicken Sie es an, und schon gelangen Sie auf die Lightbeam-Übersicht. Lightbeam ist jetzt aktiv und zeigt bei jeder weiteren aufgerufenen Webseite an, welche Verbindungen zu Drittanbietern beim Surfen aufgebaut werden. Schon nach dem Aufruf weniger Webseiten (insb. Nachrichtenseiten) wird ein dichtes Netz sichtbar. Als Kreis werden die angesurften Webseiten dargestellt, als Dreieck die Drittanbieter. Potentiell können Sie am besten von denjenigen Drittanbietern verfolgt werden, die in der Mitte des Netzes stehen, denn sie werden von mehreren Webseiten verwendet.

Lightbeam bietet eine „Tracking Protection“ an, die den Firefox-eigenen „Schutz vor Aktivitätsverfolgung“ aktiviert. Da Lightbeam relativ viel Leistung benötigt, kann es sinnvoll sein, nach den Tests Lightbeam wieder zu deaktivieren und den „Schutz vor Aktivitätsverfolgung“ in den Firefox-Einstellungen per Hand auf die Einstellung „Immer“ zu setzen.

- Auf unserer Website zur Digitalen Selbstverteidigung können Sie sich über Gegenmaßnahmen gegen das Tracken informieren. Bleiben Sie dran.

Ihr Browser ist einmalig – und hat einen Fingerabdruck

Wenn Sie eine Webseite aufrufen, kann der Betreiber der Seite Sie anhand des Browser-Fingerabdrucks eindeutig identifizieren. Und das ohne, dass Sie sich irgendwo einloggen und ohne dass ein Cookie gesetzt wird. Ihr Browser teilt nämlich jeder Website eine ganze Menge mit: Browserversion, Betriebssystem, Zeitzone, Bildschirmauflösung, installierte Schriftarten, installierte Browser-Plug-Ins und noch ca. 50 weitere Merkmale mehr. In den meisten Fällen ist die Kombination aus diesen Informationen weltweit einzigartig, wie ein Fingerabdruck.

▶Sehen Sie sich Ihren digitalen Fingerabdruck an

Wie einzigartig Ihr Browser im Netz erkennbar ist, können Sie auf der Website der Electronic Frontier Foundation (EFF) überprüfen: Panopticlick heißt das Online-Werkzeug dafür. Nach dem Test sehen Sie Ergebnisse in verschiedenen Kategorien. Mit einem Klick auf „Show full results for fingerprinting“ können Sie die detaillierten Ergebnisse zu Ihrem Browser Fingerabdruck einsehen. Merken Sie sich das Ergebnis, folgen Sie den Tipps dieses Artikels und vergleichen Sie am Ende!

▶Fingerabdruck verhindern

Als erstes empfehlen wir generell, **Java und Flash zu deaktiveren**. Damit schalten Sie zugleich häufig missbrauchte Sicherheitslücken aus. Prüfen können Sie dies z.B. im Firefox unter Extras -> Addons -> Plugins.

Mit dem Firefox-Addon **NoScript** können Sie die Ausführung von JavaScript auf Webseiten unterbinden. Dies ist für den Datenschutz- und die Sicherheit beim Surfen im Netz sehr zuträglich, aber wenn alle Skripte blockiert werden, funktionieren manche Seiten nicht mehr richtig

▶Fingerabdruck verschleiern

Über die Konfiguration des Browsers können sowohl der „User Agent“, d.h. der verwendete Browser und die Version, als auch die „Platform“, d.h. das Betriebssystem, manuell angepasst werden (Link dazu auf der Jahrbuch19-Webseite).

▶Ein Fingerabdruck für viele Nutzer

Um soweit wie möglich anonym zu Surfen, dürfen die auslesbaren Merkmale nicht eindeutig sein. Um dies zu erreichen, können Sie einen Browser mit Schwerpunkt auf Datenschutz installieren und dürfen dann die Standardeinstellungen nicht ändern, nicht mal die Größe des Browserfensters. Dafür empfehlen wir den Tor Browser (siehe Jahrbuch19-Webseite und Seite 117 in diesem Buch).

Und jetzt gehen Sie auf Panopticlick und schauen Sie, wie sich Ihr Ergebnis verbessert hat. Ausprobieren und Freunden weitersagen!

Selbstverteidigungsabbildung: Panthermedia

Das 3-Browser-Konzept

Dieses Konzept wurde von Mike Kuketz entwickelt und erstmals in seinem kuketz-blog.de als ausführliche Artikelserie veröffentlicht. Mike ist Mitglied unserer AG Digitale Selbstverteidigung und wir dürfen die Grundidee für unser Jahrbuch als Gastbeitrag übernehmen. Vielen Dank dafür!

Richtig angewendet soll das 3-Browser-Konzept das User-Tracking bei der Internet-Nutzung reduzieren. Wie gut das gelingt, hängt im Einzelfall immer davon ab, ob Sie das Konzept konsequent durchhalten und welche Internet-Dienste Sie nutzen. Das „Geheimnis“ des Konzepts besteht aus der korrekten Anwendung von drei unterschiedlichen Browsern, die jeder für sich einem Zweck dienen.

1. **Ein Tor-Browser**: Tor basiert auf einem Anonymisierungsnetzwerk mit dynamischer Routenwahl über mehrere Stationen (auch Onion Routing genannt). Spuren zum ursprünglichen Computer, der eine Anfrage gestartet hat, sind damit nicht mehr nachvollziehbar. Tor-Browser stehen vorkonfiguriert für Windows, Linux und Mac OS X bereit. **Der Zweck**: Der Tor-Browser wird von uns zum alltäglichen Surfen eingesetzt. Wann immer wir bspw. nach Informationen suchen, online shoppen oder News-Seiten besuchen, greifen wir auf den Tor-Browser zurück. Wenn wir uns allerdings mit einem Nutzerkonto anmelden müssen, sollten wir dies NICHT mit Tor durchführen, sondern zum zweiten Browser wechseln.
2. **Ein „JonDoBrowser“:** Der JonDoBrowser beinhaltet eine Sammlung von Plug-Ins und Browser-Einstellungen, die ein User-Tracking erschwert und (bei korrekter Anwendung) gleichzeitig die Sicherheit erhöht. **Der Zweck:** Den JonDoBrowser nutzen wir für Online-Dienste, die eine Anmeldung erfordern. Also immer dann, wenn wir nicht anonym surfen, sondern uns mit einer Kombination aus User und Passwort (Account) anmelden müssen: Beim Einkaufen, bei Diskussionen in Foren, beim Online-Banking. Entscheidend ist, dass die Plugins bspw. Cookies, JavaScripts oder das Nachladen von externen Inhalten reduzieren.
3. **Ein Browser Ihrer Wahl:** Entgegen Ihrer Erwartungen werden Sie diesen dritten Browser vermutlich nur sehr selten benötigen. Bei der Wahl dieses Browsers haben Sie völlig freie Hand. Der Zweck: In seltenen Fällen sind Webseiten über das Tor-Netzwerk nicht oder nur mit Einschränkungen nutzbar. Funktioniert eine Webseite also nicht korrekt, können Sie im ersten Schritt noch immer auf den JonDoBrowser ausweichen. Erst, wenn das auch nicht geht, kommt dieser dritte Browser ins Spiel.

▶Hier im Jahrbuch können wir nur das Konzept vorstellen – technische Hinweise, Links, Download-Seiten und weitere Hintergründe gibt es direkt bei Mike auf kuketz-blog.de (verlinkt auch über unsere Jahrbuch19-Webseite).

Festplatten, Sticks etc. verschlüsseln

Warum Festplatten verschlüsseln?

Ob Diebstahl, Hausdurchsuchung oder ob Sie Ihren Rechner oder Datenträger aus Versehen im Zug vergessen – Ihre Daten auf Computern, mobilen Festplatten oder Sticks sollten Sie verschlüsseln. Nicht zuletzt liegen unter Umständen auch Ihre Passwörter ungeschützt auf Ihrer Festplatte.

Auch die vermeintlich sicherste Verschlüsselung kann jedoch gebrochen werden. Seien Sie deshalb sorgfältig bei der Auswahl von Passwörtern! Insbesondere sollten Sie daran denken, dass Sie Ihre Daten entschlüsseln, wenn Sie damit arbeiten – also lassen Sie Ihr Gerät möglichst nicht unbeaufsichtigt laufen.

Was soll verschlüsselt werden?

Die Daten auf Ihrer Festplatte und in Ihrem Benutzerverzeichnis werden standardmäßig nicht verschlüsselt. Auch wenn Sie ein Login-Passwort für das Benutzerkonto gesetzt haben, wird damit lediglich der Zugang über das Betriebssystem verwaltet. Wenn Computerdiebe Ihre Festplatte als normales Speichermedium, beispielsweise als externe Festplatte benutzen, umgehen sie die Passwortabfrage und können sich leicht Zugriff zu den Daten verschaffen. Deshalb sollten Sie mindestens Ihr Benutzerverzeichnis, besser noch die gesamte Festplatte verschlüsseln. Achten Sie sorgfältig auf Ihr Passwort, denn wenn Sie die Festplatte verschlüsseln, bedeutet das: Ohne dieses Passwort kann Ihr Rechner nicht hochfahren. Wenn Sie also Ihr Passwort vergessen, können Sie selbst in der Regel Ihre Daten auch nicht mehr auslesen.

Aktuelle Betriebssysteme bringen üblicherweise von Haus aus die Fähigkeit mit, Dateien, Partitionen oder die gesamte Festplatte zu verschlüsseln. Teilweise ist eine solche Möglichkeit jedoch nur in den kostenpflichtigen Business-Versionen verfügbar. Die verschiedenen Betriebssysteme nutzen dabei unterschiedliche Lösungen. Wir sind da etwas skeptisch, weil sich dabei nicht um Freie Software handelt (Erläuterungen zum Konzept „Freie Software“ finden Sie im Linux-Artikel auf Seite 122). Deshalb ist es nämlich für Außenstehende schwierig einzuschätzen, wie effektiv die jeweilige Verschlüsselungsmethode ist oder ob sogar eine Hintertür eingebaut ist, die es Geheimdiensten erlaubt, die Verschlüsselung zu umgehen.

Als Alternative empfehlen wir die freie Software „VeraCrypt“. Sie ist für alle gängigen Betriebssysteme verfügbar. Ihr Programmcode wurde unabhängig überprüft. Mit ihr können Sie einzelne Dateien, Partitionen oder die ganze Festplatte verschlüsseln, auch auf externen Festplatten oder USB-Sticks. Nähere Informationen zu VeraCrypt und einen Link zur einer Installationsanleitung finden Sie über die Jahrbuch19-Webseite.

E-Mails verschlüsseln

E-Mail-Verschlüsselung ist nicht mehr so kompliziert wie früher. Und es gibt drei gute Gründe für das Verschlüsseln: Den Schutz der Vertraulichkeit, der Authentizität und der Integrität.

Schutz der Vertraulichkeit heißt, die Nachricht ist nur für diejenigen lesbar, für die sie bestimmt ist. Dies ist bei weitem nicht selbstverständlich, denn der Inhalt unverschlüsselter E-Mails wird im Klartext versendet und ist somit grundsätzlich für alle lesbar.

Schutz der Authentizität heißt, dass Sie sicher sein sollten, dass Sie auf elektronischen Wegen wirklich mit den Personen kommunizieren, mit denen Sie zu kommunizieren glauben.

Selbstverteidigungsabbildung: Panthermedia

Und **Schutz der Integrität** bedeutet, dass der Inhalt der Nachricht auf dem Weg von Absender zu Empfänger nicht verändert wird.

Wie verschlüsseln?

Der erste Schritt ist, dass Sie Ihre Mails nicht im Browser verwalten, sondern auf Ihrem Computer ein E-Mail-Programm wie zum Beispiel Thunderbird, The Bat!, Microsofts Outlook oder Apples Mail installieren. Dadurch schreiben Sie Ihre E-Mails zunächst einmal nur auf Ihrem eigenen Computer, ohne dass der Text Zeichen für Zeichen ins Internet übertragen wird. Erst durch das Abschicken (oder Zwischenspeichern) verlässt die Nachricht Ihren Computer und geht ins Internet. Im besten Fall ist sie dann verschlüsselt, und niemand außer dem Empfänger kann sie lesen.

Verschlüsseln Sie deshalb Ihre E-Mails, zum Beispiel mit PGP (Links gibt’s auch hier wieder auf der Jahrbuch19-Homepage, siehe unten). PGP steht für „Pretty Good Privacy“ (zu deutsch: „ziemlich gute Privatsphäre“) und wurde Anfang der 1990er Jahre von Phil Zimmermann entwickelt. Früher brauchte man ein Handbuch dafür. In den 90er Jahren haben wir deshalb ein deutsches Handbuch für PGP herausgegeben.

In der Zwischenzeit ist es mit der Thunderbird-Erweiterung Enigmail, die auf der modernen PGP-Software GnuPG aufbaut, einfacher geworden. GnuPG gibt es für verschiedene Betriebssysteme. So gibt es beispielsweise unter Mac OS X ein Apple-Mail-Plugin und für Windows gibt es Gpg-4win.

Diese Plugins und detaillierte Anleitungen finden Sie ebenfalls über die Jahrbuch19-Webseite (siehe unten). Am meisten Spaß macht das Einrichten von GnuPG bei einer Cryptoparty, und dabei können alle ihre Schlüssel gegenseitig beglaubigen, um ein „Web of Trust“ (Achtung: nicht verwechseln mit dem gleichnamigen Datenkraken-Addon WOT) zu weben.

Erhältlich im Digitalcourage-Shop!

Anonym surfen mit dem PrivacyDongle

Die Tor-Anonymisierungssoftware ist auf dem PrivacyDongle bereits konfiguriert. Einfach einstecken und anonym lossurfen. USB 2.0, erhältlich für Windows XP, Vista, 7, 8, 10, Mac OS X (10.6+), Linux, Unix, BSD (Für Linux auf den Rechner kopieren und dort starten).

16GB | Preis: 25 Euro / Stück

https://shop.digitalcourage.de

Aber bedenken Sie: Bei der Verschlüsselung von E-Mails werden nur die Inhalte verschlüsselt. Um auch Anhänge zu verschlüsseln, achten Sie darauf, das Übertragungsformat PGP/MIME und nicht PGP/inline zu verwenden! Absender und Empfänger sind trotzdem sehr leicht einsehbar. Auch der Betreff (engl.: Subject) der E-Mail wird meist nicht verschlüsselt.

Verschlüsselte Kommunikation leicht gemacht: p≡p

Aktuell ist es immer noch der Normalfall, dass E-Mails nicht Ende-zu-Ende-verschlüsselt übertragen werden, sondern allenfalls streckenweise. E-Mail-Verschlüsselung ist erlernbar, das haben wir Ihnen gerade erklärt – aber es ist eben noch eine Einarbeitung in das Thema erforderlich.

Ganz anders denkt das Volker Birk: Er hat es sich mit seinem Projekt p≡p („pretty Easy privacy“) zum Ziel gesetzt, diesen Zustand umzukehren: Wo immer möglich, sollen E-Mails und andere digitale Nachrichten verschlüsselt werden. Verschlüsselung soll ziemlich einfach („easy“) statt nur ziemlich gut („good“) werden. Digitalcourage unterstützt das Projekt, Rena Tangens und padeluun sitzen zum Beispiel im Stiftungsrat (siehe auch Seite 40.)

Ist p≡p einmal installiert, sucht es automatisch nach vorhanden PGP-Schlüsseln oder anderen Kryptostandards, um diese zu nutzen. Ist kein PGP installiert, erstellt es automatisch selbst Schlüssel zur Verwendung – nur wenn absolut keine Verschlüsselung möglich ist, etwa weil der Gesprächspartner keine Möglichkeit bietet, wird die Nachricht unverschlüsselt verschickt.

Zur Zeit ist die p≡p-Software erhältlich für Microsoft Outlook und Android-Smartphones. Außerdem ist p≡p im Thunderbird-Add-on Enigmail seit Version 2 enthalten. Für iphones ist eine p≡p-App zu Redaktionsschluss dieses Jahrbuches angekündigt – bitte halten Sie sich im Netz auf dem Laufenden.

p≡p-Software installieren:
https://www.pep.security/

Auf dem Laufenden bleiben:
https://pep.foundation/

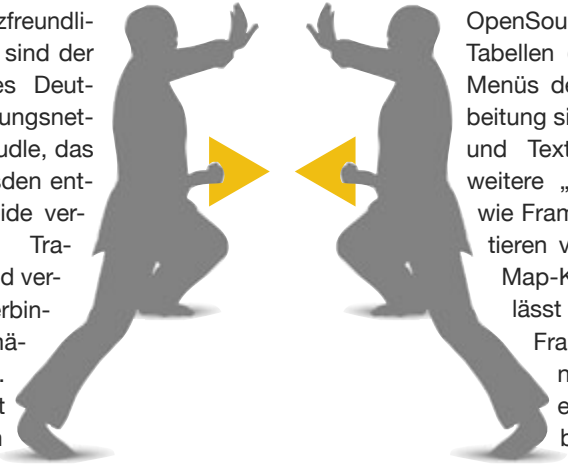
Online zusammen arbeiten ohne Google Docs

Wenn gemeinsame Texte und Tabellen entstehen sollen, muss es nicht immer GoogleDocs sein: EtherPad und EtherCalc sind Alternativen, die auf dem eigenen Server laufen. Organisationen können beispielsweise ihre Adressdaten-Verwaltung mit CiviCRM im Griff behalten. Und Termine. Sie haben doch bestimmt schon mal „gedudelt“, oder?

dudle / DFN-Terminplaner: Termine ohne Tracking und Werbung planen

Wenn es darum geht, einen gemeinsamen Termin zu finden oder eine Umfrage zu starten, verwenden viele Menschen Doodle. Das ist nicht unbedingt sicher: Wer den Link kennt, kann Umfragen abrufen – ein zusätzlicher Passwortschutz ist nicht vorgesehen. Darüber hinaus verwendet Doodle laut eigener Datenschutzerklärung nach wie vor GoogleAnalystics und weitere Tracker.

Zwei datenschutzfreundliche Alternativen sind der Terminplaner des Deutschen Forschungsnetzes (DFN) und dudle, das von der TU Dresden entwickelt wird. Beide verwenden keine Tracking-Dienste und verschlüsseln die Verbindung standardmäßig über HTTPS. Bei dudle lässt sich zudem ein Passwort zur Teilnahme einrichten und angemeldete Nutzer.innen können gegenüber anderen Teilnehmer.innen anonym an Umfragen teilnehmen, das heißt, es wird kein Name angezeigt.



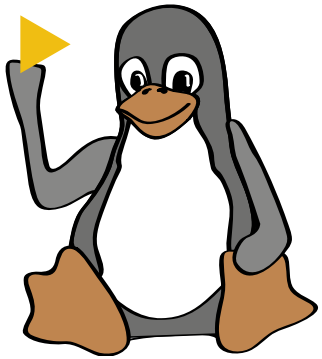
Selbstverteidigungsabbildung: Panthermedia

EtherPad & Ethercalc: Texte und Tabellen gemeinsam bearbeiten

Gemeinsame Arbeit an Texten und Tabellen lässt sich mit EtherPad und EtherCalc bewerkstelligen. Insbesondere für Firmen und Organisationen ist interessant, dass sich beide auf dem eigenen Server betreiben und mit einem Passwort absichern lassen. Damit steht dem guten Vorsatz „raus aus der Cloud“ nichts mehr im Wege. Achtung: Über den Timeslider können auch „gelöschte“ Inhalte rekonstruiert werden – bedenken Sie dies, bevor Sie Daten in einem Pad oder Calc ablegen!

Francophile finden bei Framasoft, einem der größten französisch-sprachigen Portale zur Verbreitung von OpenSource, neben Tabellen (FramaCalc, die Menüs der Tabellenbearbeitung sind auf Englisch) und Texten (FramaPad) weitere „libres services“ wie FramaMap zum Editieren von OpenStreetMap-Karten. Vieles lässt sich auch ohne Französisch-Kenntnisse benutzen, einfach ausprobieren!

Trauen Sie sich: GNU/Linux now!



Es scheint so ungemein praktisch, dass auf jedem erworbenen Computer bereits ein Betriebssystem vorinstalliert ist. Computer kaufen, einschalten und los geht's … Leider werden die meisten Computer ausschließlich mit Windows oder macOS ausgeliefert. Dass es auch benutzerfreundliche freie Alternativen gibt, ist vielen Nutzer.innen nicht bekannt. Insbesondere GNU/Linux – manche sprechen der Kürze halber auch nur von Linux – ist in vielfältig, deckt unterschiedliche Anwendungszwecke ab und hat entscheidende Vorteile. Damit ist es gerade auch für Menschen interessant, die hauptsächlich E-Mails schreiben, im Web surfen und vielleicht noch Textdokumente bearbeiten wollen. In den letzten Jahren ist GNU/Linux auf Augenhöhe mit Windows angekommen oder übertrifft dieses sogar.

Vorteile

Bei Digitalcourage schätzen wir insbesondere folgende Eigenschaften:

- Es handelt sich um Freie Software. Das heißt, Expert.innen können sehen, wie Linux programmiert ist; Fehler können behoben werden und verbesserte Kopien dürfen weitergegeben werden. Es handelt sich also um ein offenes System, welches auf Hintertüren kontrolliert werden kann und Abhängigkeiten von einem bestimmten Hersteller (wie Microsoft, Apple und Google) vermeidet.
- GNU/Linux ist hochoptimiert und zugleich sehr zuverlässig im Betrieb. Deshalb werden viele kritische Systeme im Internet und auch Supercomputer damit betrieben.
- Es benötigt wenig Festplattenplatz und läuft auch auf alten Computern zügig.
- Durch verschiedene Zusammenstellungen von freier Software ergibt sich eine große Vielfalt: GNU/Linux kann auf dem WLAN-Router wie auch auf dem Schul-Server laufen. Ebenso lässt sich GNU/Linux am normalen Arbeitsplatzrechner für fast jeden Anwendungszweck einrichten.
- Es ist meist erheblich datenschutzfreundlicher als proprietäre (sprich: unfreie) Betriebssysteme wie Windows oder Apple macOS.

Der möglicherweise größte Vorteil von Linux gegenüber Windows ist die **Paketverwaltung**. Es handelt sich dabei um ein Programm zur Softwareverwaltung, mit dem jegliche für diese GNU/Linux-Version verfügbare Software installiert werden kann (bei Debian sind dies ca. 50.000 Programme). Dadurch ist es nicht mehr notwendig, im Internet nach Programmen zu suchen mit dem Risiko, eventuell Schadsoftware zu installieren. Systemweite Updates sind dann vollautomatisch.

Politisch geht es den Verfechtern von Freier Software nicht darum, dass Software kostenlos ist („Frei wie Freibier"), sondern dass Software nicht die Anwender.innen ihrer Freiheiten und Rechte beraubt („Frei wie Freiheit"). Dennoch sind viele Linux-Distributionen kostenlos.

Wichtige Begriffe

Um den Einstig in GNU/Linux zu erleichtern, möchten wir fünf wichtige Begriffe erklären:

- **Eine GNU/Linux-Distribution** (kurz: Distro) ist eine Zusammenstellung von Programmen, Installationsmedien, Aktualisierungsdiensten und Dokumentation, die unter einem einschlägigen Namen angeboten wird. Zu den bekanntesten zählen: Linux Mint, Ubuntu, Debian, OpenSuse, ...
- Häufig gibt es **64- und 32-Bit-Versionen von GNU/Linux**. Es empfiehlt sich, immer die standardmäßig angebotene 64-Bit-Version zu nehmen. Lediglich bei manchen alten Computern (Baujahr vor 2009) ist nur eine 32-Bit-Installation möglich.
- Mittels einer **Live-CD/DVD (oder USB-Stick)** können die meisten Linux-Distributionen ohne Installation ausprobiert werden. Das bestehende System wird nicht angefasst.
- **Dual-Boot(-System):** Wer GNU/Linux nutzen möchte, muss Windows dafür nicht entfernen, sondern kann beide Betriebssysteme nebeneinander installieren. Bei jedem Start des Rechners kann fortan ausgewählt werden, ob Linux oder Windows verwendet werden soll. Sie sollten aber – wie immer bei größeren Änderungen an Ihrem Rechner – vorher eine Datensicherung machen.

Wer Programme benutzt, die nur für Windows verfügbar sind und keine Alternative unter Linux findet, kann versuchen die **Windows-Programme direkt unter Linux auszuführen**, mit Hilfe von Wine. Es gibt eine App-Datenbank (erreichbar über unsere Jahrbuch19-Webseite), die für viele Programme beschreibt, wie gut sie funktionieren.

Der sicherlich einfachste Weg, Linux auszuprobieren, ist eine Linux-Install-Party oder der Besuch einer Linux-User-Group (LUG). Dort kann nicht nur der eigene Laptop auf Linux-Verträglichkeit (ohne Installation) getestet werden, üblich sind auch Hilfestellung und das gemeinsame Lösen von Problemen vor Ort.

Selber machen

Wollen Sie Linux sofort und alleine ausprobieren, so benötigen Sie zuerst ein Boot-Medium, das immer auf der Website der entsprechenden Distribution heruntergeladen werden kann. Üblicherweise handelt es sich um eine CD/DVD oder ein Abbild („Image") für einen USB-Stick. Nachdem dieses entsprechend gebrannt oder kopiert wurde, muss der Computer vollständig heruntergefahren werden. Dann kann beim Start mit eingelegter CD, Stick oder für was Sie sich entschieden haben, mit dem Drücken einer Taste dieses Medium ausgewählt werden. Übliche Tasten für das sogenannte Boot-Menü sind: Esc, F8, F9, F11 und F12. Für Anfänger.innen, die keinerlei Erfahrung mit Linux haben, empfehlen wir zur Zeit Linux Mint 19 mit Cinnamon 64bit.

Links und weitere Infos: digitalcourage.de/jahrbuch19

Social Media-Alternativen: Komm mit uns ins Fediverse!

Sie haben das mulmige Gefühl, dass Sie etwas Falsches tun, wenn Sie Facebook oder Twitter benutzen? Dieses Gefühl täuscht Sie nicht. Es gibt gute Gründe, die Social-Media-Großmächte zu meiden. Aber Sie müssen nicht auf Social Media verzichten, um Ihre Privatsphäre und Selbstbestimmung zu behalten. „Fediverse“ heißt die von uns empfohlene Alternative. Wir zeigen Ihnen, wie Sie das Fediverse unverbindlich ausprobieren können, ohne gleich alle Brücken abzubrechen. Zugegeben: Für Facebook haben wir keine Lösung. Aber Twitter und das Fediverse können Sie gleichzeitig nutzen, ohne dass Sie Kontakte verlieren oder doppelt so viel Zeit aufwenden müssen.

▶Fedi ... was?

„Fediverse“ ist die Kurzform von „Federated Universe“. Es handelt sich um ein dezentrales Kommunikationsnetz. Wählen Sie sich zuerst einen Anbieter aus. Das sind Server, auf denen freie Software läuft – meist GNU social oder das neuere Mastodon, auf das wir uns hier konzentrieren. Diese Server nennt man auch Instanzen. Meist werden Sie von Enthusiasten betrieben, und die Benutzung ist kostenlos. Viele haben einen thematischen Schwerpunkt. Eine passende Instanz kann man zum Beispiel über die Datenbank https://instances.social/ finden. Wie beim E-Mailen spielt es technisch kaum eine Rolle, bei welcher Instanz man ist – die Nutzer einer Instanz können denen anderer Instanzen folgen, so wie Sie Mails an jede beliebige Mailadresse verschicken können.

Um Digitalcourage im Fediverse zu folgen, geben Sie am besten „digitalcourage“ in das Suchfeld ein, das auf Mastodon-Instanzen links oben zu finden ist. Oder besuchen Sie unser Fediverse-Profil direkt. Den Link finden Sie über die Jahrbuch19-Webseite.

▶Mastodon einrichten

1. Finden Sie eine „Instanz“ für Ihren Account

Das Einrichten von Mastodon ist in wenigen Minuten erledigt. Auf einem Smartphone (Android oder iOS) lässt sich eine entsprechende App installieren. Für Android sind die freien und quelloffenen Apps Tusky, Mastalab und Twidere einen Blick wert. Letztere funktioniert auch mit Twitter. Auf einem Desktop-Rechner wird Mastodon über den Internetbrowser bedient.

Während Twitter und andere Social-Media-Kanäle gewöhnlich über eine zentrale Website gesteuert werden, besteht der Witz von Mastodon gerade darin, dass das Netz über viele verschiedene und voneinander unabhängige Server gebildet wird. Diese Server (Instanzen) haben je einen eigenen Namen wie z.B. „@name“ und bilden den „Heimathafen“ ihrer jeweiligen Nutzer.innen.

2. Registrierung

Zur Registrierung auf der so ermittelten Wunsch-Instanz wird gewöhnlich die Angabe eines Usernamens, einer E-Mail-Adresse und eines selbst gewählten Passworts verlangt. Usernamen sind immer an die „Heimatinstanz“ gebunden, weswegen Sie es auch einfach auf einer anderen Instanz probieren können, wenn Ihr Lieblings-Username auf einer bestimmten Instanz bereits vergeben ist.

3. Und schon: Tröten, Folgen, Boosten ...

Englisch „tooten“ oder deutsch „tröten“ heißt das Versenden von Nachrichten bei Mastodon. Das sollte für Twitter-erfahrene Nutzer.innen ein Klacks sein.

▶Twitter und Fediverse koppeln

Niemand erledigt eine Aufgabe gern doppelt, und das gilt auch für das Schreiben von Status-Updates. Also gibt es technische Lösungen. Für den Anfang am einfachsten finden wir den Twitter-Mastodon-Crossposter. Das ist ein quelloffener Bot, der Ihre Tweets zu Ihrer Fediverse-Instanz spiegelt oder wahlweise auch umgekehrt. Um ihn einzurichten, muss man einmalig folgende Schritte durchgehen:

1. In einem Reiter auf Twitter einloggen.
2. In einem anderen Reiter auf einer Mastodon-Instanz einloggen.
3. Auf https://moa.party/ die beiden Buttons „Twitter“ und „Mastodon“ anklicken und die erbetenen Rechte gewähren.
4. In den Optionen mindestens den Schalter unter „Post my tweets on Mastodon“ umlegen. Jetzt noch unten auf „Update User“ klicken und fertig.

Wenn Sie ausschließlich über Ihr Smartphone tooten bzw. twittern, können Sie stattdessen auch eine App nutzen, die immer gleich beide Kanäle mit einem Schlag befüttert. Die freie Android-App „Twidere“, die im F-Droid angeboten wird, kann das zum Beispiel. Das hat den Vorteil, dass Sie beide Plattformen gleichermaßen im Blick haben. Nachteil ist allerdings, dass Twitter regelmäßig Schritte unternimmt, um es solchen Drittanbieter-Apps schwer zu machen. Es kommt dadurch hin und wieder zu Komplikationen, die sich manchmal nicht so schnell lösen lassen.

▶In gekoppelten Universen leben

Jetzt können Sie wie gewohnt eine Twitter-App nutzen, um Nachrichten abzusetzen. Früher oder später wird Ihnen die Mastodon-Instanz Ihrer Wahl eine E-Mail schreiben mit dem Hinweis, dass es Reaktionen auf einen Ihrer „Toots“ gab. So heißen die Status-Updates bei Mastodon. Lassen Sie sich auf der Mastodon-Instanz Ihrer Wahl auf ein Gespräch ein. Wir haben festgestellt, dass die User im Fediverse engagierter sind als die auf Twitter, und auch vom Umgangston sind wir begeistert.

Irgendwann halten Sie sich vielleicht die meiste Zeit im Fediverse auf und loggen sich nur noch ab und zu auf Twitter ein, um Fragen zu beantworten.

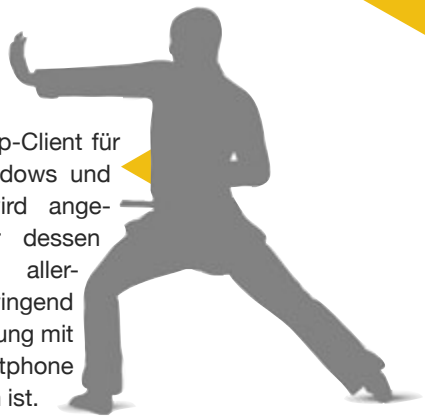
Links und weitere Infos: digitalcourage.de/jahrbuch19

„WhatsApp kommt mir nicht in die Hosentasche!“

Ob Kindergeburtstag, Arbeitsanweisungen oder Urlaubsfotos: Für viele ist WhatsApp im Alltag fest verankert. Dabei sollten Sie aufpassen: WhatsApp gehört seit 2014 zu Facebook. Der Konzern lebt von Werbung und Datenhandel und arbeitet, wenn nötig, mit Geheimdiensten zusammen. Viele Menschen wollen da nicht mehr mitmachen – aber was wäre eine Alternative zu WhatsApp als Messenger für den Alltag?

Unsere Kriterien für „gute“ Messenger:

- **Offene Schnittstellen**: Das technische Kommunikationsprotokoll sollte vollständig dokumentiert oder anderweitig verfügbar und kostenlos für Softwareentwickler verwendbar sein. Wie bei E-Mails sollte Kommunikation zwischen verschiedenen Anbietern funktionieren.
- **Freie Software**: Der Quellcode der Software soll verfügbar und unter einer freien Lizenz stehen; nicht nur für die App, sondern auch für die Serversoftware.
- **Ende-zu-Ende-Verschlüsselung**: Nachrichten sollten auf Ihrem Smartphone verschlüsselt und erst wieder auf dem anderen Smartphone entschlüsselt werden, damit „unterwegs“ niemand Zugriff auf Ihre Nachrichten hat.
- **Sicherheit (Kryptografie):** Die App sollte aktuell, sicher und nachvollziehbar verschlüsseln.
- **Unabhängiges Audit**: Unabhängige Dritte sollten die Software auf Sicherheitslücken geprüft haben und auch weiterhin regelmäßig prüfen.
- **Metadatensparsamkeit**: Unnötige Zugriffe auf Server (zum Beispiel zum Nachladen von Bildern, Schriftarten, etc.) sollten vermieden werden, damit nicht noch mehr (Meta-)Daten der Vorratsdatenspeicherung anheimfallen oder zur Profilbildung missbraucht werden. Dezentrale Dienste mit vielen Servern haben hier Vorteile.
- **Kein Adressbuch-Upload**: Die meisten Messenger-Apps arbeiten mit den Handy-Nummern der Nutzer.innen und erkennen automatisch, wenn jemand aus Ihrem Adressbuch den gleichen Messenger benutzt. Dafür werden alle Telefonnummern aus Ihrem Adressbuch an die Server des Anbieters übertragen. Das ist ein Eingriff in die Privatsphäre Ihrer Kontakte. Besser ist es, einen Messenger zu haben, der die Nutzer.innen mittels Nicknames verwaltet.
- **Betriebssysteme**: Grundsätzlich sollte ein Messaging-Dienst auf allen gängigen Betriebssystemen verfügbar sein. Da ein Großteil unserer digitalen Kommunikation mittlerweile auf dem Smartphone stattfindet, möchten wir mindestens Android und iOS (iPhone/iPad) unterstützt sehen.
- **Freie Verfügbarkeit**: Die App sollte unter Android auch außerhalb von Googles Play Store angeboten werden, so dass die App auch ohne Google-Account nutzbar ist. Besser sind direkte Downloadmöglichkeiten oder F-Droid, ein alternativer „Store“, in dem ausschließlich freie und quelloffene Software angeboten wird.
- **Kein Tracking**: Gerade Apps, die private Kommunikation versprechen, sollten ihren Nutzer.innen nicht hinterherschnüffeln und keine zusätzlichen Softwarekomponenten enthalten, die Nutzungsdaten sammeln und übertragen.



Selbstverteidigungsabbildung: Panthermedia

Welche Kriterien Ihnen wichtig sind, müssen Sie selbst entscheiden. Die folgenden Alternativen machen vieles anders und besser als WhatsApp. Trotzdem gilt: Den perfekten Messenger gibt es nicht. Probieren Sie doch einfach aus, welche Lösung für Sie am besten funktioniert.

Matrix ist ein offenes Protokoll, das Kommunikation via Textnachrichten, Sprach- und Videoanrufen ermöglicht. Als Client-App steht Riot für Android, iOS, Linux, Windows und macOS zur Verfügung. Ein Vorteil von Matrix ist, dass es mit anderen Protokollen wie z.B. XMPP und IRC zusammen arbeitet. Optional bietet Matrix Einzel- und Gruppenchats mit Ende-zu-Ende-Verschlüsselung an.

Signal ist für Android und iOS verfügbar und bietet dank Ende-zu-Ende-Verschlüsselung vertrauliche Kommunikation via Text, Audio und Video. Die Software ist frei und quelloffen. Allerdings lädt auch Signal Ihr Adressbuch auf den Server hoch und die Angabe einer Telefonnummer ist zwingend erforderlich. Das ist z.B. für Journalist.innen mit Informantenschutz-Bedarf ein Ausschlussgrund. Für einige Funktionen greift Signal unter Android auf Google-Dienste zurück, läuft mittlerweile aber auch „entgoogelten” Geräten. Auch ein Desktop-Client für Linux, Windows und macOS wird angeboten, für dessen Nutzung allerdings zwingend eine Kopplung mit dem Smartphone erforderlich ist.

Wire bietet ähnlich wie Signal auf Android und iOS Text-, Audio- und Video-Kommunikation mit Ende-zu-Ende-Verschlüsselung. Entscheidender Unterschied zu Signal ist die freiwillige Nutzung einer Telefonnummer. Auch ein Desktop-Client für Linux, Windows und macOS ist verfügbar. Leider sind in Wire Tracker enthalten, die nach Einwilligung Nutzungsdaten sammeln und an Dritte übermitteln.

XMPP (früher: **Jabber**) ist ein offenes Protokoll, das ursprünglich für das Chatten auf Desktop-PCs entwickelt wurde und ähnlich wie E-Mail funktioniert: Man erstellt ohne Telefonnummer ein Konto auf einem von vielen Server-Anbietern und kann trotzdem mit Nutzer.innen auf anderen Servern kommunizieren. Es gibt zahlreiche Clients für XMPP, z.B. Conversations für Android, ChatSecure für iOS und Gajim für Linux und Windows, die auch Ende-zu-Ende-Verschlüsselung unterstützen.

- Steigen Sie um – und natürlich ist das nur sinnvoll, wenn Sie Freund.innen und Familie auch dazu bewegen können. Aber eine.r muss ja schließlich anfangen... (siehe Vorwort)

Facebook – Eine Grundsatzentscheidung

Wir haben uns unsere Entscheidung nicht leicht gemacht. Wie viele anderen Bürgerbewegungen oder Firmen stehen wir vor dem Dilemma, dass wir Menschen erreichen wollen – können wir uns also leisten, auf Facebook zu verzichten? Zumal wir 2011 einen BigBrotherAward an Facebook vergeben haben?

Nach vielen Diskussionen haben wir uns entschieden, dort nicht aktiv zu sein. Wir können aber verstehen, wenn Sie sich dafür entscheiden, Facebook trotz der damit verbundenen Risiken zu benutzen. Immerhin können wir Ihnen ein paar Dinge vorschlagen, die Sie tun oder vermeiden sollten.

- **1. Mindestens eine alternative Kontaktmöglichkeit anbieten:** Nutzen Sie nicht nur Facebook, wenn Sie mit Menschen Kontakt aufnehmen wollen. Ihre Homepage zum Beispiel sollte alle Inhalte verbreiten, die Sie auch auf Facebook zur Verfügung stellen. Wer selbst keine Alternative anbietet, ist mitverantwortlich dafür, dass manche Menschen inzwischen Facebook für „das Internet“ halten.
- **2. Aus Facebook heraus linken, nicht hinein:** Verweisen Sie stets auf Websites außerhalb von Facebook. Auch innerhalb von Facebook sollten Sie Links immer auf externe Seiten setzen, und nicht innerhalb von Facebook verlinken, wenn es nicht unbedingt nötig ist.
- **3. Ihr Team vor AGB schützen:** Facebook sollte in Ihrer Organisation von einem gesonderten Computer betreut werden, denn es ist unklar, ob und wie auch nicht auf Facebook bezogene Online-Aktivitäten am gleichen Rechner evtl. mit ausgeforscht werden. Reduzieren Sie Facebook in Ihrem Büro am besten auf separate Geräte und verbinden Sie diese Arbeitsplätze nicht mit Ihren anderen Dienstprogrammen wie Kundenverwaltung oder dem E-Mail-Konto von Teammitgliedern, denn Facebook greift sonst evtl. auch darauf zu.
- **4. Ablehnung von Facebook kundtun:** Machen Sie Ihren Umgang mit Facebook auch auf der Facebook-Seite transparent und animieren Sie andere zur Einhaltung dieser Tipps von uns. Verweisen Sie stets auf die alternativen Plattformen, mit denen Sie lieber arbeiten.
- **5. Social-Media-Buttons allenfalls als Ein-Klick-Lösung:** Sollten Sie auf Ihrer Website Social-Media-Buttons einbinden, können Sie dies tun, ohne Ihr Publikum gesammelt an die Datenkraken auszuliefern. Mit den privatsphäretauglichen Buttons per „Shariff“ können Share-Buttons mit „Ein-Klick-Lösung“ datenschutzkonform auf der eigenen Website eingebunden werden. Nutzer.innen stehen hierdurch erst dann mit Facebook und Co. direkt in Verbindung, wenn sie aktiv werden, zuvor können die sozialen Netzwerke keine Daten über sie erfassen.
- Merke: Im Zweifel hat Facebook mehr von Ihrer Organisation als Sie von Facebook.

Navigation und Wikipedia offline nutzen

Landkarten und die Texte der Wikipedia lassen sich auch ohne Internetverbindung nutzen. Das ist praktisch, weil es unabhängig von der Datenverbindung funktioniert, ob beim Wandern auf dem Smartphone oder im Zug auf dem Laptop. Und vor allem: Bei Offline-Navigation greift niemand Ihre Standortdaten ab.

Orientierung und Navigation für unterwegs

Das Kartenmaterial des Freie Software-Projekts OpenStreetMap lässt sich herunterladen und offline nutzen. Damit ist die Navigation unabhängig von einer Datenverbindung. Das ist besonders im Ausland praktisch, wenn das Datenvolumen begrenzt und teuer ist. Oder wenn weit und breit kein WLAN bereitsteht.

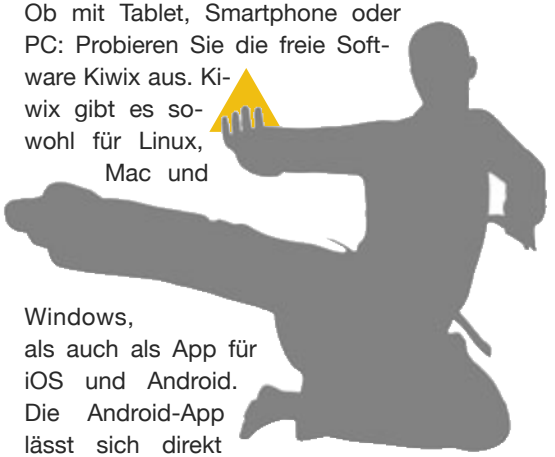
OsmAnd – App, die Navigation offline kann

Die App OsmAnd („OpenStreetMap Automated Navigation Directions“) nutzt OpenStreetMap-Daten für die Navigation – online und offline. Durch den Kauf von Karten und durch Spenden helfen Sie, das Projekt weiterzuentwickeln. Das Geld fließt in die Entwicklung.

Marble – die Welt auf dem PC

Auf dem PC können Sie mit Marble (engl.: „Murmel“) die Welt als Kugel betrachten und mit dem Zoom lassen sich Kartenausschnitte betrachten. Neben OpenStreetMap-Karten stehen Satelliten-Bilder, historische Karten und allerlei andere Spielereien zur Verfügung. Um ohne Internetverbindung navigieren zu können, müssen Sie den entsprechenden Kartenbereich herunterladen (File -> Download Region) und die Navigation-Engine herunterladen.

Wikipedia immer dabei – auch ohne Netz



Ob mit Tablet, Smartphone oder PC: Probieren Sie die freie Software Kiwix aus. Kiwix gibt es sowohl für Linux, Mac und Windows, als auch als App für iOS und Android. Die Android-App lässt sich direkt über den F-Droid-Store herunterladen. Im Kiwis-Wiki lassen sich verschiedene Versionen der Wikipedia und anderer Sammlungen herunterladen. Zum Beispiel passt die gesamte deutschsprachige Wikipedia ohne Bilder und Versionsgeschichte mit ca. 5,3 GB auf die meisten gängigen Smartphones und 25GB (mit Bildern) lassen sich zumindest auf dem PC gut speichern. Die Inhalte in den sogenannten ZIM-Dateien laden Sie am besten über Ihren PC herunter und überspielen sie später auf das Smartphone. Damit schonen Sie das Datenvolumen Ihres Handyvertrags und Ihre Nerven.

Selbstverteidigungsabbildung: Panthermedia

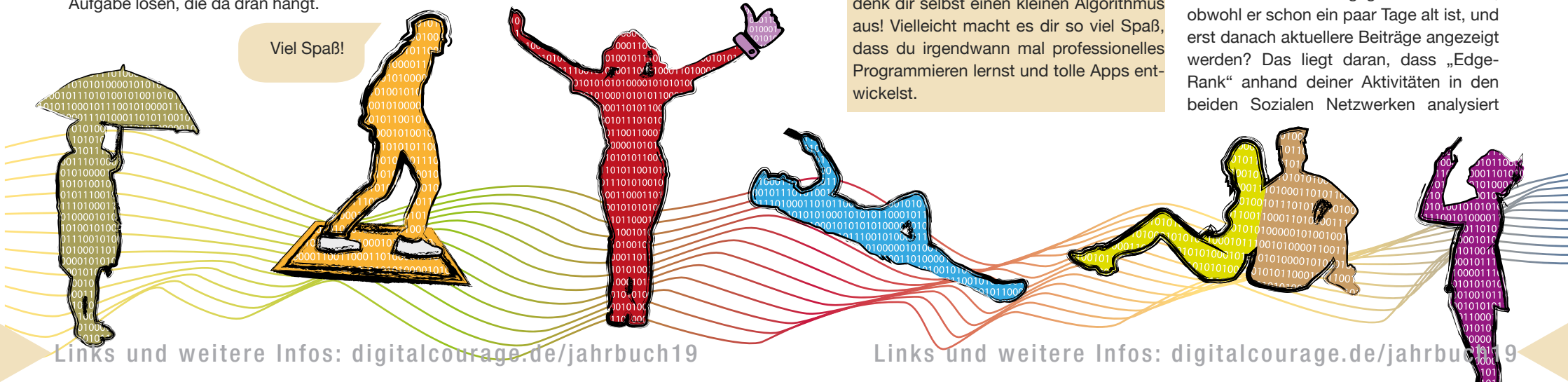
Foto: Fabian Kurz, cc by-sa 4.0

Hallo,

hier ist wieder Eure Jessi, ich arbeite bei Digitalcourage, betreibe den Blog #kids #digital #genial (www.kidsdigitalgenial.de) und habe im Sommer 2018 das Kinder- und Jugendlexikon „#kids #digital #genial von App bis .zip“ herausgebracht. Mehr über mich findest du auch auf Seite 42 in diesem Buch.

In meinem Lexikon erkläre ich Begriffe aus der Computer-/Smartphone- und Online-Welt so, dass es hoffentlich jeder verstehen kann – auch deine Eltern. :-) du kannst direkt ein Spiel draus machen: Nimm einen der folgenden Begriffe und frag deine Eltern z.B. „Was ist eigentlich ein Algorithmus?“ Mal sehen, ob sie dir das erklären können! Und dann könnt Ihr ja auch gemeinsam meine Erklärung lesen und vielleicht die kleine Aufgabe lösen, die da dran hängt.

Viel Spaß!



Illustrationen: Isabel Wienold, cc by-sa 4.0

Algorithmus

Ein Algorithmus ist ein Bauplan, der ein Problem lösen soll. Die einzelnen Schritte der Vorgehensweise müssen klar und unwidersprüchlich definiert sein, z.B. „Führe den Schritt nur durch, wenn die Bedingung A erfüllt ist. Führe den Schritt so lange durch, bis Bedingung B erfüllt ist.“

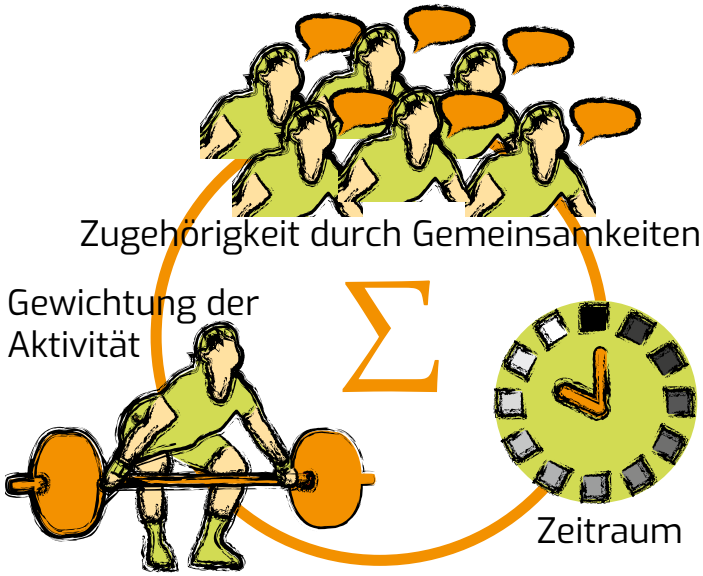
Schwer zu verstehen? Dann stell dir vor, du darfst nach dem Essen erst spielen gehen, wenn deine Hände sauber sind (siehe Grafik).

Nicht nur Menschen können eine Aufgabe oder ein Problem lösen, sondern auch Computer. Diese können viel komplexere Probleme mit ganz vielen Bedingungen lösen. Daher werden Algorithmen eingesetzt um große Datenmengen zu verarbeiten und zu analysieren Ein Algorithmus, den du ganz bestimmt kennst, ist der EdgeRank bei Facebook und Instagram.

Aufgabe: Schnapp dir Zettel und Stift und denk dir selbst einen kleinen Algorithmus aus! Vielleicht macht es dir so viel Spaß, dass du irgendwann mal professionelles Programmieren lernst und tolle Apps entwickelst.

EdgeRank

Der „EdgeRank“ ist ein Algorithmus von Facebook und Instagram. Dieser Algorithmus bestimmt, welche Nachrichten dir in deiner Chronik/Story angezeigt werden. Hast du dich schon gewundert, wieso manchmal ein Beitrag ganz oben steht, obwohl er schon ein paar Tage alt ist, und erst danach aktuellere Beiträge angezeigt werden? Das liegt daran, dass „EdgeRank“ anhand deiner Aktivitäten in den beiden Sozialen Netzwerken analysiert



und verknüpft, welche Beiträge für dich interessant sein könnten. Dabei wird auch beachtet, welche Mitteilungen andere interessant finden (z.B. durch die Anzahl der Likes und Kommentare). Daraus ergibt sich dann, welche Beiträge dir angezeigt werden. Da Instagram und Facebook seit 2012 zusammen gehören, tauschen die Netzwerke ihre Analysen untereinander aus, um noch besser abzuschätzen, was dir wohl wichtig ist.

Diese Filterung ist wirklich schlecht, denn Facebook und Instagram bestimmen damit, wen du zu sehen bekommst, indem sie dir keine anderen Möglichkeiten geben. Sie schränken Dich damit ein. Verschiedene Informationen und Beiträge von Personen, zu denen du schon länger keinen Kontakt hattest, werden dir teilweise gar nicht mehr angezeigt. Dieses Phänomen nennt sich auch „Filterblase“.

Aufgabe: Denk mal darüber nach, zu welchen Menschen du schon lange keinen Kontakt mehr hast, obwohl ihr immer gut befreundet wart. Sind diese Personen wirklich alle weniger interessant als diejenigen, die dir auf deiner Startseite angezeigt werden? Schreib ihnen doch mal wieder etwas Nettes.

„Filterblase“

▶Cybergrooming

„Cybergrooming“ bezeichnet die erste Stufe der Anmache im Internet („grooming“= anbahnen, vorbereiten) mit dem Ziel, eine Straftat zu begehen, wie z.B. sexuellen Missbrauch, oder um (kinder) pornographisches Material zu bekommen. Meist erfolgt diese Anmache durch Schmeicheleien im Chat und das langsame Aufbauen einer Vertrauensbasis

Illustrationen: Isabel Wienold, cc by-sa 4.0

Illustrationen: Isabel Wienold, cc by-sa 4.0

von Personen, die sich ein falsches Profil angelegt haben, also sich als jemand anderes ausgeben (falscher Name, falsches Alter, falsche Fotos,…). Oft handelt es sich dabei um Pädophile. Pädophilie ist eine psychische Erkrankung, bei der Erwachsene erotische Fantasien mit Kindern (und sogar mit Babys) entwickeln. In den meisten Fällen sind das Männer, aber auch Frauen können pädophil sein. Wenn sie sich Dein Vertrauen mit falschen Angaben erschlichen hat, verlangt die Person häufig Fotos, Videochats oder ein persönliches Treffen.

Aufgabe: Sprich mit deinen Freundinnen und Freunden oder deinen Geschwistern darüber, ob sie so etwas schon einmal erlebt haben. Oft muss nur einer den Anfang machen, damit man sich traut, darüber zu reden. Gemeinsam solltet Ihr euch stärken und vielleicht überlegen, ob Ihr erwachsene Personen um Hilfe bittet. Cybergrooming ist eine Straftat, kein Spaß!

So, wenn du jetzt neugierig auf weitere Tipps geworden bist, kannst du auf www.kidsdigitalgenial.de weiter lesen und stöbern oder du kannst das Lexikon bei uns bestellen.

▶Warum ich ein Kinderlexikon geschrieben habe?

Einfach, weil ich mich für die Mediennutzung von Kindern und Jugendlichen interessiere und etwas Gutes dazu beitragen möchte. Chatten, Fotos machen, Spiele zocken, Videos gucken, ... das macht alles sehr viel Spaß! Leider muss man dabei aufpassen, weil der Spaß, den wir haben, leicht ausgenutzt werden kann. Auf die Ideen, wo die Fallen sind, haben mich häufig die Mädchen und Jungen in mei-

Erhältlich im Digitalcourage-Shop!
„#Kids #Digital #Genial
Das Lexikon von App bis .zip“

Soft- und Hardcover (2,45 / 12 Euro)
▶ https://shop.digitalcourage.de

nen Projekten gebracht. Deshalb erkläre ich euch mal an ein paar Beispielen, wie ich auf meine Themen komme.

Medien-Workshop, 6. Klasse:

„Ich stell meinen Insta-Account nicht auf ‚privat', ich will doch fame!"

Ich kann das Mädchen, das das gesagt hat, total gut verstehen. In Sozialen Netzwerken geht es meistens darum, Anerkennung von anderen zu bekommen, neue Leute kennenzulernen, Freundschaften zu halten, aber auch von Fremden bewundert zu werden. Klicks und Likes zu bekommen, ist eine große Ehre und die „großen" YouTuber.innen machen es vor. Du solltest dir allerdings immer klar machen, dass nur die Wenigsten wirklich eine erfolgreiche Onlinekarriere erreichen. Nur, weil du deine Profile auf „öffentlich" stellst, heißt es leider noch lange nicht, dass du dadurch berühmt wirst. du solltest abwägen, ob es dir wirklich wert ist, deine Daten preiszugeben. Auch die Internetstars haben bestimmt mal Momente, wo sie es genießen, unerkannt über die Straße zu gehen.

6. Klasse, Thema In-App-Käufe:

„Meine Mutter ist übelst scheiße! Alle sind 3 Level über mir und ich darf keine Items kaufen!"

In-App-Käufe werden gezielt an bestimmten Stellen eingesetzt, damit du immer mehr und mehr Geld für die App ausgeben musst. Wenn dir deine Eltern also verbieten, Geld für In-App-Käufe aus-

zugeben, dann gehörst du nicht zu den benachteiligten Kindern, sondern zu denen, die bei dem Kaufzwang nicht mitmachen. Darauf kannst du stolz sein! Natürlich ist es ein wenig ärgerlich, wenn du im Spiel deshalb nicht weiterkommst, obwohl es bis dahin so viel Spaß gemacht hat, aber denk daran: Es ist doch nur ein Spiel.

6. Klasse,
Thema: gruselige Kettenbriefe.

„Ich hatte voll Angst. Ich weiß ja das ist Fake, aber was ist wenn doch nicht?"

Du kennst das… die nervigen Kettenbriefe bei WhatsApp und in anderen Sozialen Netzwerken. Manche Kettenbriefe

Illustration: Isabel Wienold, cc by-sa 4.0

sind so schön geschrieben, dass man sie gerne weiterleitet, aber manche sind wirklich grausam. Oft geht es darum, dass du die Nachricht weiterschicken sollst, weil sonst etwas Schlimmes passiert. Aber: Das stimmt nicht! Die Nachrichten denkt sich irgendjemand aus und da ist kein Stückchen Wahrheit dran. Hab also keine Angst, schick die Texte nicht weiter, lösch die Nachricht einfach und sag deinen Freunden, dass sie dir solche Nachrichten nicht mehr weiterleiten sollen!

Medien-Workshop, 8. Klasse.

„Privatsphäre? Ah! Das ist doch das, was man bei Facebook und so einstellen kann."

Das klingt ganz witzig, ist aber eigentlich schlimm: Privatsphäre ist ein Menschenrecht und nichts, was Facebook uns freundlicherweise ermöglicht. Facebook und andere Soziale Netzwerke sind genau die großen „Datenfresser", die mit Privatsphäre nicht viel zu tun haben, im Gegenteil!

Medien-Workshop, 6. Klasse
Thema Passwörter:

„Ich weiß nicht, ob meins so sicher ist, ich hab…"

„STOP!"

Dies ist ein gutes Beispiel dafür, wie leichtgläubig manchmal mit Passwörtern umgegangen wird. Auch wenn du jemanden fragen möchtest, ob dein Passwort sicher ist, darfst du es natürlich nicht verraten!

Mutter-Tochter-Workshop:

„Die daddelt 24/7."

„Man Mama, wenn ich nicht zurück schreibe sind die sauer!"

Wenn du so eine Diskussion auch zu Hause hast, dann solltest du deinen Eltern erklären, wieso die Nutzung des Smartphones für dich so wichtig ist und was du da genau tust. Du solltest aber auch darüber nachdenken, ob es wirklich notwendig ist, immer jeder Person sofort zurück zu schreiben… du kannst das Handy auch

ruhig mal eine Weile zur Seite legen und das kannst du auch ganz bewusst trainieren. Wenn du deinen Freunden z.B. sagst, dass du nicht immer direkt zurückschreiben kannst/willst, dann sind sie dir auch nicht böse, wenn sie mal länger auf eine Antwort warten müssen.

Mädchen, 15 Jahre:

„Ich mach jetzt ganz viele Gewinnspiele mit. Da muss ich nur meine E-Mail-Adresse angeben und kann voll geile Sachen gewinnen."

Ein weit verbreiteter Irrtum. Bei den wenigsten Gewinnspielen gibt es tatsächlich etwas zu gewinnen. Das wissen allerdings auch viele Erwachsene nicht. Die meisten Gewinnspiele dienen nur dazu an deine privaten Daten ranzukommen, wie Name, Adresse, E-Mail-Adresse, Kontodaten,… Außerdem stecken oft Abonnements hinter Fake-Gewinnspielen. Selbst wenn es tatsächlich mal etwas zu gewinnen gibt, dann kommst du nicht drumherum sensible Daten preiszugeben, wenn du den Gewinn entgegen nehmen möchtest.

Situation in der Straßenbahn.
Junge, ca. 15 Jare:

„Ey, mach mal Foto von dem Mann da. Musst du später posten."

Das Recht am eigenen Bild ist den meisten Kindern bekannt. Nur sie achten es oftmals nicht. Sie nehmen es nicht ernst genug. Das Verlangen danach, möglichst vieles fotografisch festzuhalten, verletzt dieses Recht sehr oft. Deshalb ist eines ganz wichtig: Du musst immer vorher fragen, ob du ein Foto von der Person machen darfst! Es gibt bei diesem Gesetz, das unter anderem im Kunsturheberrechtsgesetz festgelegt ist, kaum Spielraum. Sobald du eine Person ganz gezielt fotografierst, wie es in diesem Beispiel der Junge in der Straßenbahn tut, dann machst du dich strafbar.

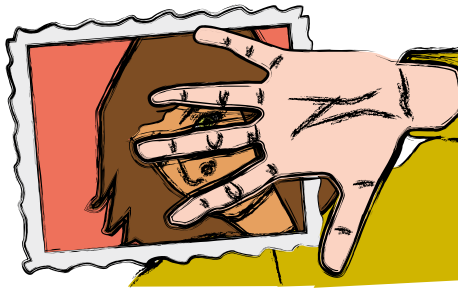


Illustration: Isabel Wienold, cc by-sa 4.0

Mädchen, 13 Jahre:

„Insta, Snapchat, WhatsApp, … hab ich alles auf privat! Mehr Daten gebe ich im Netz nicht preis!"

Dass die Profileinstellungen bei diesem Mädchen auf privat gestellt sind, ist ja bereits lobenswert. Doch du darfst nicht unterschätzen, wann und wo überall private Daten gesammelt werden. Mit dem Online-Tool „Trace my Shadow" kann man gut erkennen, welche Daten – abhängig vom Gerät und Betriebssystem – beim Surfen im Internet gesammelt werden.

Solche und noch viele andere andere Kurzgeschichten kannst du in meinem Blog www.kidsdigitalgenial.de lesen. Diese hier stammen aus meinem Adventskalender. Schau doch mal vorbei!

Liebe Grüße
deine Jessi

Foto: Stefanie Loos, cc by-sa 4.0

Beim Bürger.innenfest „Rettet die Grundrechte",
Gendarmenmarkt Berlin, 2017

Digitalcourage vor 30 Jahren

Public Domains

▶Rena Tangens erinnert sich:

„Die Public Domains (kurz „PDs“ genannt) waren unsere Veranstaltungsreihe sonntags im Bielefelder Bunker Ulmenwall. „Public Domain“ heißt öffentlicher Bereich und stand für uns für „offen für alle“ und „öffentliche Angelegenheit“. Ende 1988 waren padeluun und ich gerade aus Kanada zurück gekommen, wo wir 3 Monate als „Artists in Residence“ gelebt und ausgestellt hatten. Schon bevor wir abgereist sind, hatten sich die PDs immer mehr in Richtung Raubkopier-Party entwickelt.

▶Die Kids mussten ihre schweren Rechner und Bildschirme mitbringen.◀

Um gegenzusteuern haben wir ab 1989 immer einen Vortrag an den Anfang gestellt, und erst dann gab es Freiraum für Austausch. Es kamen viele Kids, die sich vorher bei Karstadt unten in der Computerabteilung getroffen hatten. Wir haben Tische aus einem Jugendzentrum geholt und jedes Mal einen Kopierer von unserem Copy-Shop die ganze Bunker-Treppe runtergeschleppt, damit auch was aus Handbüchern kopiert werden konnte. Laptops waren noch unerschwinglich, die Kids mussten also ihre schweren Rechner und Bildschirme mitbringen und die Eltern zum Taxidienst überreden. C64, Atari ST und Amiga waren damals angesagt.

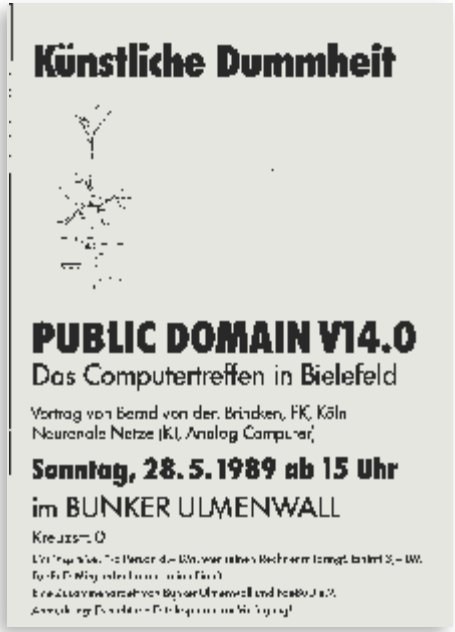
In der ersten Themen-PD (V10.0) hat padeluun GeoNet vorgestellt. Das GeoNet-System von Günther Leue war das Vorbild für unsere eigene Zerberus-MailBox, mit einfachen Befehlen auf Deutsch: Lesen, Inhalt, Suchen usw. Über GeoNet hatten 1986 nach der Reaktorkatastrophe von Tschernobyl Wissenschaftler.innen Radioaktivitätsmesswerte veröffentlicht, die offizielle Stellen nicht oder nur zögerlich herausgaben. padeluun hat sich bei der PD damals gewünscht, „So ein Medium zur Gegenöffentlichkeit in Echtzeit wollen wir hier.“

Im Sommer 1989 war es soweit: Wir haben unsere BIONIC-MailBox aufgemacht. Die haben wir in der PD V16.0 vorgestellt. 17 11 88 war unsere erste MailBox-Telefonnummer – später kam die 68000 dazu.

„Bielefelder MailBox AG“ stand für „Arbeitsgemeinschaft“, aber padeluun liebte auch den Anklang von Aktiengesellschaft im Sinne von „Alle tun ihren Anteil dazu, denn wir haben keine reichen Eltern.“ Bei unserer MailBox musste man 5 DM monatlichen Beitrag bezahlen. Und je mehr wir heute über Google & Co wissen, desto mehr denke ich: Das war ein faires Geschäftsmodell. Wir wollten nicht unsere Teilnehmer.innen ausspähen – im Gegenteil: Wir wollten ihre Privatsphäre möglichst wirkungsvoll schützen.

Die Zerberus-Software hatte datenschutzfreundliche Voreinstellungen, hat die Nachrichten in den privaten Postfächern standardmäßig verschlüsselt und auch

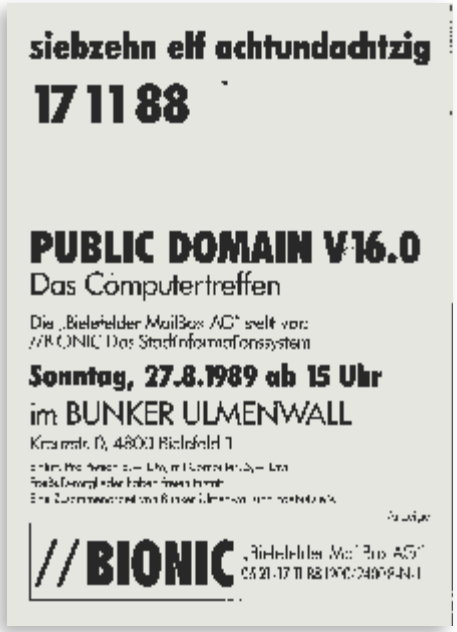
▶Ein Medium zur Gegenöffentlichkeit in Echtzeit◀

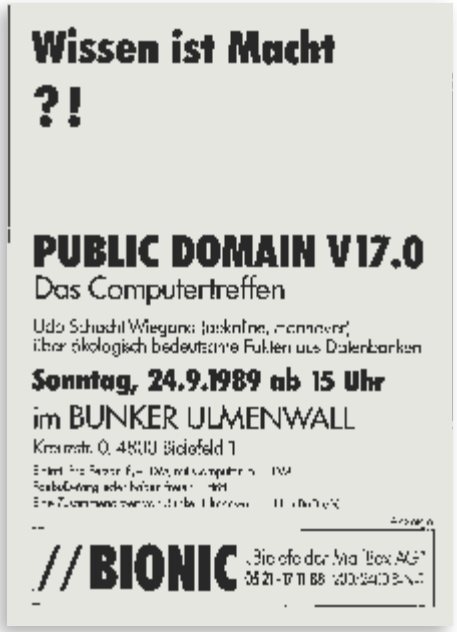


auf unserem Bildschirm auf dem Flur nur mit Sternchen angezeigt. (Nachzulesen im Jahrbuch 2018, S. 168ff.) Anfangs hatten wir eine 20 MB (ja, MegaByte!) Festplatte, dann kauften wir eine mit 80 MB für damals deutlich über 1000 Mark. Auch die lief voll – wir mussten ständig von Hand löschen. Immer die ältesten Nachrichten, aber nicht den Anfang einer Diskussion – Handarbeit mit hohem inhaltlichem Anspruch.

Auch sonst denke ich, wenn ich auf die Themen aus 1989 gucke, dass wir mit vielem sehr früh dran waren. In der PD V11.0 ging es um Verschlüsselung mit DES, in PD V12.0 um ein Anti-Viren-Programm. Horst Willenberg verwaltet übrigens ein Bielefelder Studi-Wohnheim und hat das zum ersten Bielefelder Wohnheim mit

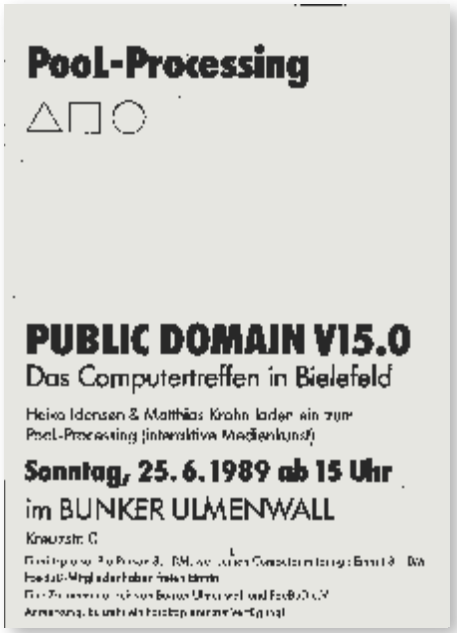
▶Anfangs hatten wir eine 20 MB (ja, MegaByte!) Festplatte.◀



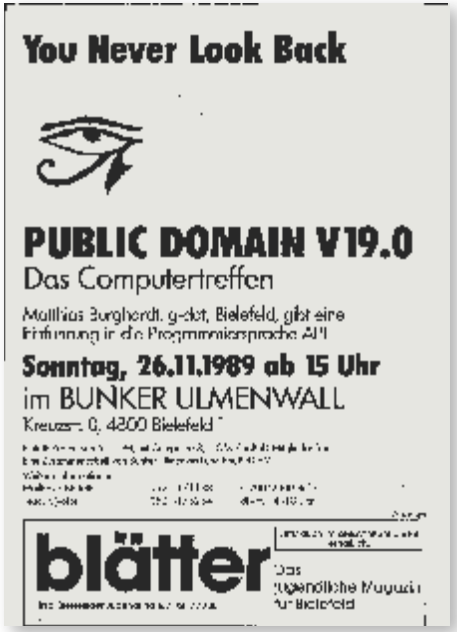


Internetanschluss gemacht. Für die PD V13.0 „73 aus Stuttgart“ (73 ist das Funker-Kürzel für „Schöne Grüße!“) hatten wir mit Saskia Fischer eine sehr fitte junge Frau, damals gerade mal 16 oder 17, als Referentin eingeladen. Ansonsten ging es um „Künstliche Dummheit“ (PD V14.0), und die Anspielung auf „Künstliche Intelligenz“ funktioniert auch heute noch, oder Pool Processing (PD V15.0). Das war ein Hyperlink-System, das Heiko Idensen für seine Datenbank zu Kunst, Computern, Literatur usw. entwickelt hat.

Auf der PD V18.0 hat Pengo, ein Hacker, der in den 1980ern an den KGB-Hacks beteiligt war, GNU vorgestellt, das freie Unix-Betriebssystem (Siehe Seite 122), heute Linux. Was für eine Aufbruchstimmung! Und wir mittendrin.“



▶Was für eine Aufbruchstimmung! Und wir mittendrin.◀



Eine Herkulesaufgabe

Mein Fazit aus meiner Arbeit in der Enquête-Kommission „Internet und digitale Gesellschaft“ des 18. Deutschen Bundestags

Von padeluun

Foto: Stefanie Loos, cc by-sa 4.0

„Es war mir eine Ehre mitzuarbeiten. Aber die Kraft von 17 Abgeordneten, 17 Sachverständigen und einem 18. Sachverständigen, der Öffentlichkeit, hat kaum ausgereicht, den Stall gründlich auszufegen.“

Digitalcourage-Gründungsvorstand padeluun arbeitete von 2010 bis 2013 als Sachverständiger in der Enquête-Kommission „Internet und digitale Gesellschaft“. Drei Jahre lang pendelte er zweimal pro Woche zwischen Bielefeld und Berlin. Die Arbeit in der Enquête-Kommission war eine große Ehre und sicher für beide Seiten sehr lehrreich. Auf die Arbeit in der Enquête folgte in der nächsten Sitzungsperiode der ständige Ausschuss „Digitale Agenda“.

2014 gab er ein Abschlussinterview, das wir heute, fünf Jahre später, in diesem Jahrbuch dokumentieren. Ursprünglich war es im Abschlussbericht der Enquête-Kommission veröffentlicht worden. Dort war es aber eine Zeit lang quasi „beerdigt“: 2015 wurden wir stutzig, weil die Inhalte der Enquête-Berichte mit Suchmaschinen nicht zu finden sind. Offensichtlich lassen sich die Inhalte des Online-Archivs des Deutschen Bundestages zu „Enquête“ nicht durchsuchen. Dabei war doch beschlossen worden, dass alle Ergebnisse der Enquête beim Bundestag auf der Website archiviert werden sollten, damit sie der Öffentlichkeit zur Verfügung stehen. Wir entdeckten, dass das Webarchiv des Bundestagsservers allen Suchmaschinen verbietet, die Inhalte zu indizieren – damit können sie in der Regel nur sehr schlecht gefunden werden. Das „Durchsuch-Verbot“ fand sich in der Datei ‚robots.txt‘ im Webarchiv des Bundestages:

*User-agent: **
Disallow: /

Daraufhin stellten wir als Service für Legislative, Exekutive, Judikative und für uns alle den gesamten Enquête-Bericht auf der digitalcourage-Website zur Verfügung. Alle Suchmaschinen dürfen ihn durchsuchen. Wir grüßten damit alle Mitarbeiterinnen und Mitarbeiter derzeitiger und zukünftiger Ausschüsse im Bundestag und Europaparlament und hofften, dass wir ihnen die tägliche Arbeit damit etwas erleichtern. Den Link finden Sie auf der Jahrbuch19-Webseite (s.u.). Mittlerweile ist die ‚robots.txt‘-Datei des Bundestags so umgeschrieben, dass Suchmaschinen diese Inhalte finden und indexieren dürfen.

Doch nun zum Interview mit padeluun – die Fragen stellte das Sekretariat der Enquête-Kommission.

▶Welche Ihrer Erwartungen an die Arbeit der Kommission haben sich erfüllt, welche nicht?

Eigentlich schreibt man an dieser Stelle: „Es war eine große Ehre für mich, bei dieser Enquête-Kommission mitwirken zu können.“ Ja, das war es auch, aber so what?! Eigentlich war es ein Augiasstall voll Arbeit. Die Kraft von 17 Abgeordneten, 17 Sachverständigen und einem 18. Sachverständigen, der Öffentlichkeit, hat kaum ausgereicht, um den Stall gründlich auszufegen. Die gute Nachricht: Ein Großteil des „Mists“ – also der zu beantwortenden Fragen – ist heraus. Und es gibt noch eine gute Nachricht: Diese Enquête hat im Bundestag bereits während ihrer Konsolidierungsphase eine Menge bewegt.

▶Die gute Nachricht: Ein Großteil des „Mists“ ist heraus.◀

Ich hätte mir allerdings noch mehr Informations- und Meinungsaustausch gewünscht. Stattdessen spielten wir oft „Text-Tetris“ und schoben Textbaustei-

Links und weitere Infos: digitalcourage.de/jahrbuch19

ne hin und zurück. Das lag daran, dass wir zwölf Berichte produzieren mussten: Wir hatten einfach viel zu viel Stoff für eine einzige Enquête – mit unseren Fragestellungen wären auch acht Kommissionen gut ausgelastet gewesen. Dabei begannen wir mit den härtesten Themen, der Netzneutralität, dem Urheberrecht und dem Datenschutz. Am Ende konnten wir fast nur den Ist-Zustand beschreiben – und selbst das war häufig ein parteipolitisches Desaster. Dabei gab es oft Überraschendes zu erleben: Einerseits stritten sich selbst in nicht-öffentlichen Sitzungen die verschiedenen Parteivertreter, andererseits gab es erstaunliche Koalitionen zwischen den Fronten und unerwartet viel Konsens.

Unser Bericht ist ein Stückwerk auf hohem Niveau. Er hat viele fortschrittliche Gedankenansätze, er bietet Stoff für viel wissenschaftliche Forschung, zum Beispiel zu Immaterialgütern und elektronischem Bargeld. Ganz sicher gilt: Es liegen recht viele Nuggets im Mist. Wer sich nicht scheut, kann reich werden beim Durchsieben der Texte.

▶Welche Erfahrungen haben Sie gemacht?

Es war mir wichtig, weite Teile der Netzbewegung mit in die Kommission zu nehmen. So freute ich mich, dass die Politiker und Referentinnen, die den Einsetzungsantrag geschrieben hatten, sich eine (informelle) 18. Sachverständige ausgedacht hatten. Diese virtuelle Person sollte die Bürgerinnen und Bürger repräsentieren und dafür Sorge tragen, dass die „Öffentlichkeit in besonderem Maße“ in die Enquêtearbeit eingebunden werden sollte.

▶Ganz sicher gilt: Es liegen recht viele Nuggets im Mist.◀

Um mitarbeiten zu können, brauchte es auch Informationen. Deshalb schlug ich vor, dass sich die Enquête eines der Instrumente der

Quelle: Screenshot

Foto: Stefanie Loos, cc by-sa 4.0

„Liquid Democracy“ bedienen solle. Ich machte mich für das Programm „Liquid Feedback“ stark und es gab sehr breite Zustimmung. Man entschied sich für „Adhocracy“. Es gab allerdings Widerstand aus dem Präsidium des Bundestages. Nach dessen Verständnis – so interpretiere ich das – ist ein Mandat eben gerade vom Willen der Wählenden unabhängig: „Sie sind Vertreter des ganzen Volkes, an Aufträge und Weisungen nicht gebunden und nur ihrem Gewissen unterworfen“ (Artikel 38 GG).

▶Sie sind Vertreter des ganzen Volkes und nur ihrem Gewissen unterworfen.◀

Wir holten uns also den Sachverstand, der sich manchmal auch als Meinung entpuppte, und entschieden dann nach demokratisch legitimierten Prinzipien, welche Ratschläge und Texte wir mit in den Bericht nahmen. Dafür mussten wir allerdings zuvor Präsidium und Ältestenrat „hacken“. Auch dies gelang interessanterweise unter anderem mit den Stimmen der Regierungsfraktionen und der SPD – und mithilfe des Liquid Democracy e.V., der das System – außerhalb des Bundestags – auf seinen Servern installierte und betrieb. Sachverständige sind unabhängig von den Parteien. Dennoch wird von ihnen erwartet, dass sie sich bei Abstimmungen an die Fraktion gebunden fühlen. Sie sind direkt den Fraktionen zugeordnet und von ihnen abhängig. Das beginnt schon damit, dass Sachverständige im Bundestag nicht das Recht haben, sich Papiere auszudrucken. Das muss über die Fraktion geschehen. Auch viele interne Infos bekommen die Sachverständigen nur über die Fraktion.

Zu Beginn meiner Tätigkeit für die Kommission hatte ich diese starke Bindung unterschätzt. Ich hätte mir erhofft, dass die Fraktionen eine geringere Rolle spielen, wenn wir gemeinsam darüber nachdenken, wie wir uns die digitale Zukunft wünschen. Schade ist: Sachverständige können auch keine Vertretung schicken. Zudem wird es einem nicht gerade leicht gemacht, eigene Mitarbeiter für die Arbeit einzusetzen. Da sich der Fraktionszwang stärker auswirkte, als ich es mir gewünscht hätte, geriet ich in eine Rolle, die so zuvor nicht abzusehen war: Ich wurde

Foto: Stefanie Loos, cc by-sa 4.0

„Die vielen kleinen Revolutionen, die wir in den Bundestag getragen haben, waren für mich persönlich der größte Erfolg.“

bei vielen Abstimmungen zum Zünglein an der Waage. Diese Position zeichnete sich dadurch aus, dass man es niemandem recht machen konnte. Doch sie konnte auch sehr wertvoll sein, wenn man die Möglichkeit, die Mehrheit umzudrehen, nicht zu ausgiebig auskostete.

Leider bekam ich für diesen Balanceakt nur wenig Unterstützung von der Opposition. Stattdessen wurde versucht, mich öffentlich unter Druck zu setzen. Wie viel ich im Vorfeld schon aus Texten heraus verhandelt hatte, war nach außen nicht mehr erkennbar, wenn ich (im Gegenzug) meine Stimme für einen Text gab, der vielen nicht weit genug ging.

Insgesamt kann ich feststellen: Jetzt, wo der Bericht fertig ist, habe ich genügend Erfahrung gesammelt, um zu wissen, was wir alles von Anfang an hätten anders machen sollen.

▶Was sind für Sie die wichtigsten Ergebnisse der Enquête?

Die vielen kleinen Revolutionen, die wir in den Bundestag getragen haben, waren für mich persönlich der größte Erfolg. Wir haben in der Kommission viele „neue“ Instrumente ausprobiert, um die Kommunikation und Textarbeit zu erleichtern. Wir haben neue Arbeits- und Beteiligungsformen in den Bundestag gebracht und diese erstmals erprobt. Wir haben mit Hilfe der Beteiligungsplattform Adhocracy erste vorsichtige Schritte in Richtung flüssiger Demokratie gemacht. Ich hatte zudem extern Mailinglisten eingerichtet, die allerdings am Spamschutz des Bundestags scheiterten. Wir nutzten – argwöhnisch beäugt – EtherPads zum kollaborativen Schreiben, weigerten uns selbstverständlich, Facebook oder Xing als Kommunikationsplattformen zu verwenden, nutzten Doodles zur Terminfindung, zwitscherten mit unterschiedlichsten Absichten auf Microbloggingplattformen, und ich lernte nach und nach, wie so ein Bundestag funktioniert. Dabei vermisste ich nach wie vor Zeit für Dialoge statt formeller Sitzungen mit „Text-Tetris“. Soviel aber kann ich sagen: Diese Revolution der Bürgerbeteiligung im Bundestag wird im Nachgang noch weitere Auswirkungen haben.

▶Viel Wissen über die „Netzwelt“ konnte tief sickern.◀

Ich hatte den Eindruck, dass in den vielen Gesprächen in und um die Sitzungen herum viel bei den Abgeordneten ankam. Viel Wissen über die „Netzwelt“ konnte tief sickern und wird auf diesem Weg auch die einzelnen Parteien erreichen. Doch auch wir Sachverständigen haben viel gelernt und können Wissen über politische Abläufe in unsere Organisationen tragen.

▶Diese Revolution der Bürgerbeteiligung im Bundestag wird im Nachgang noch weitere Auswirkungen haben.◀

Die wichtigsten thematischen Ergebnisse dieser Enquête waren für mich die Handlungsempfehlung zur Einführung eines anonymen digitalen Bargeldes und die Empfehlung, einen ständigen Ausschuss zum Thema „Netzpolitik“ einzurichten. Ebenso freue ich mich über die Eindeutigkeit, mit der sich die Kommission für die Förderung von Freier Software ausspricht. Als persönlichen Erfolg sehe ich, dass es mir zusammen mit Leena Simon gelungen ist, in einem Konsenstext der Enquete den äußerst umstrittenen Begriff „geistiges Eigentum“ die juristisch korrekten Begriffe „Immaterialgüter“ und „Monopolrechte“ einzuführen.“

Viel Dank gebührt den Referentinnen und Referenten aller Fraktionen und den Mitarbeiterinnen und Mitarbeitern im Enquête-Sekretariat, die geradezu übermenschliches geleistet haben, um die vielen „Tetris-Steinchen“ zu einem Gesamtbericht von mehr als 2000 Seiten werden zu lassen. Und ich danke allen, die mir und uns zugearbeitet haben. Abschließend möchte ich der Koalition und den Sachverständigen danken. Sie haben mich trotz meiner oft abweichenden Positionen und meines Abstimmverhaltens – manchmal auch zähneknirschend – gestützt und bestärkt.

▶Soviel scheint klar: Der auch von mir unterstützte Vorschlag zur Bildung eines ständigen Ausschusses zur vernetzten Gesellschaft wird ein ständiger Augiasstall sein, der ausgemistet und gepflegt sein will.

Tausche Bürgerrechte gegen Linsengericht

Die Wir-Wollen-Alles-Über-Sie-Wissensgesellschaft

Von Rena Tangens

Foto: Stephan Röh, cc by-sa 4.0

Diesen Text hat Rena Tangens 2006 geschrieben und für das Jahrbuch 2019 eingekürzt. Die Version von 2006 beschäftigte sich intensiv mit unserer Stop-RFID-Kampagne, die damals aktuell war, und mit unserem Streit mit der Metro-Group. Die Teile mit damals aktuellem Bezug haben wir gekürzt, so dass eine Menge zeitloser Wahrheiten übrig bleiben. Das Original von 2006 finden Sie auf unserer Webseite mit dem Suchwort „Linsengericht“ oder auf einen Klick über die Jahrbuch19-Seite (siehe unten).

Der Titel „Linsengericht“ stammt aus der Bibel: Hintergrund ist die biblische Erzählung (1. Buch Mose 25:29-34), derzufolge Jakob, der jüngere Sohn Isaaks, seinem älteren Bruder Esau dessen Erstgeburtsrecht im Tausch gegen einen Teller Linsen abkaufte, als Esau von der Feldarbeit erschöpft heimkehrte. Als Linsengericht bezeichnet man demzufolge im übertragenen Sinne eine momentan verlockende, in Wahrheit aber geringwertige Gabe im Tausch für ein sehr viel höherwertiges Gut.

„Schöne neue Welt“, Aldous Huxleys Vision eines Staates, in dem Menschen angenehm konsumieren können, aber perfekt manipuliert in geistiger Unfreiheit leben, ist weitaus moderner als „1984“, George Orwells Schilderung eines totalitären Überwachungsstaates. Wir sollten aber nicht annehmen, dass der Überwachungsstaat sich damit überlebt hätte. In den letzten Jahren sind die bürgerlichen Freiheiten in Deutschland immer weiter eingeschränkt worden. Einige Stichworte: Vorratsdatenspeicherung sämtlicher Kommunikationsverbindungen, Großer Lauschangriff, Verschärfung der Polizeigesetze der Länder (wohlgemerkt: Hier sind die Polizeigesetze von 2006 gemeint, Anmerkung der Jahrbuch-Redaktion) mit Rasterfahndung, Videoüberwachung im öffentlichen Raum und Platzverweis, Kfz-Kennzeichenerfassung an Autobahnen, biometrische Merkmale in Reisepässen, gespeichert auf RFID-Chip, Ausweitung der DNS-Speicherung etc.

Foto: Panthermedia, Grafik: cc by-sa 4.0 Dennis Blomeyer

Die Unschuldsvermutung wird faktisch ausgehebelt.

Das deutsche Innenministerium und die Überwachungsindustrie zählen klar zu den Profiteuren des 11. September 2001. Kaum eine Überwachungsmaßnahme, die nicht mit dem angeblich drohenden „internationalen Terrorismus“ begründet würde. Fast alle Maßnahmen zielen allerdings nicht auf Kriminelle oder unmittelbar Tatverdächtige, sondern betreffen Millionen völlig unbeteiligter Bürgerinnen und Bürger. Die Unschuldsvermutung – die bedeutendste Regelung des Rechtsstaatsprinzips folgt aus Artikel 6 Abs. 2 der Europäischen Menschenrechtskonvention – wird faktisch ausgehebelt. Diese willkürliche Law-and-order-Politik ohne Rücksicht auf Verluste bedarf der Aufmerksamkeit, der Kritik und des Widerstandes.

Die Innenpolitik ist *nicht* Thema dieses Artikels, aber sie bildet den Hintergrund, vor dem das Folgende betrachtet werden sollte. Der vorliegende Text befasst sich mit dem kommerziellen Datensammeln durch die Wirtschaft und den daraus folgenden Gefahren für Privatsphäre und informationelle Selbstbestimmung. Viele halten dies für ein „Luxus-Prob-

lem“, denn die Nutzung beispielsweise von Handy, Kredit- oder Kundenkarten sei freiwillig, und „mündige Verbraucher“ könnten ihre Vertragsbedingungen selbst aushandeln. Oder mit anderen Worten: Das Thema Datenschutz in der Wirtschaft sei unwichtig, denn das regele der freie Markt schon alleine. Doch wie kommt es, dass Menschen für ein „Linsengericht“, eine einfache, schnelle Bedürfnisbefriedigung, ihre Bürgerrechte leichtfertig aufgegeben, die andere Menschen vor Jahrhunderten unter Einsatz ihres Lebens erkämpft haben? Warum geben Menschen durch Nutzung einer Kundenkarte für 0,5 Prozent Rabatt ihren kompletten Einkaufszettel preis (personalisiert mit Name, Adresse, Geburtsdatum und Telefonnummer)? Vermutlich nicht, weil sie denken, dass ein halbes Prozent viel wäre, sondern weil sie – mangels besserer Information – den Daten, die sie im Tausch dafür hergeben, keinen großen Wert beimessen. Der Gegenwert ist aber nicht nur ganz pragmatisch der Preis, den ihr Datensatz später im Adresshandel erzielt, sondern der Gegenwert ist die Privatsphäre, die Handlungsfreiheit und die informationelle Selbstbestimmung.

▶Der Gegenwert ist die Privatsphäre, die Handlungsfreiheit und die informationelle Selbstbestimmung.◀

Foto: Tom Alby, cc by-sa 4.0

Sind dem Supermarkt unsere Vorlieben und unsere Kaufkraft bekannt und unser Handy oder die Gesichtserkennung verraten, vor welchem Regal wir gerade stehen, können elektronische Preisschilder uns unseren individuellen Preis anzeigen. Nicht unbedingt den günstigsten...

Den meisten Menschen ist klar, dass ihre Privatsphäre angegriffen wird, wenn sie Objekt von Überwachung werden (z.B. durch Videoüberwachung oder Abhören des Telefons) oder wenn ihre persönlichen Geheimnisse an die Öffentlichkeit gezerrt werden. Doch dass ihre Privatsphäre auch verletzt werden kann durch die ständige Sammlung, Auswertung und Nutzung einer Vielzahl von Daten, die bei jeglichen alltäglichen Handlungen anfallen – dieses Bewusstsein ist erst langsam im Entstehen.

▶Warum ist Privacy wichtig für die Demokratie?

Ein Mensch, der ständig beobachtet, registriert, vermarktet und von speziell auf ihn abgestimmten Vorschlägen und Angeboten begleitet wird, verändert mit der Zeit sein Verhalten und richtet es nach den Erwartungen derer aus, die seine Daten auswerten. Auf Individuen abgestimmte Manipulationsmöglichkeiten durch die zunehmende Erfassung z.B. von Konsumverhalten und Bewegungsdaten sowie faktischer Anpassungsdruck führen zu einer zunehmenden Fremdbestimmung.

Dabei ist nicht nur zweckentfremdender Daten”missbrauch” möglich, vielmehr ist bereits der Daten”gebrauch” problematisch. Die Sammlung, Speicherung, Akkumulation, Kombination, Auswertung und Nutzung von vielen banalen Daten aus dem alltäglichen Leben – Informationen, die jeweils für sich gesehen keineswegs „geheim“ sind – birgt somit bereits Gefahren für die informationelle Selbstbestimmung. Werden diese Daten vernetzt, können sie zu weitreichenden Persönlichkeitsprofilen zusammengestellt werden. Anonyme Maschinerien (Algorithmen), auf die die Bürgerinnen und Bürger keinen Einfluss haben, von deren Existenz sie oftmals nicht einmal wissen, ordnen sie nach Merkmalen und Verhaltensweisen in verschiedene Typisierungen ein (Fachbegriff: Scoring) und sorgen dafür, dass sie fortan entsprechend der Typisierung behandelt werden. Von den Daten kann nicht nur abhängen, welche Werbung ihnen zugeschickt wird, sondern auch welchen Job, welche Versicherung, welche Wohnung sie bekommen – und ob überhaupt. So kann eine derartige Typisierung zu einer erheblichen Einschränkung der persönlichen Handlungsspielräume führen.

▶Der „mündige Verbraucher“ wird von der Wirtschaft immer dann herbeizitiert, wenn er über den Tisch gezogen werden soll.◀

Wer sich dieser Datenerfassung *nicht* bewusst ist, tauscht sorglos Privatsphäre gegen Bequemlichkeit ein. Das Machtgefälle zwischen Bürger/innen und Verwaltung bzw. zwischen Verbraucher/innen und Wirtschaft verstärkt sich. Merke: Der „mündige Verbraucher“ wird von der Wirtschaft immer dann herbeizitiert, wenn er über den Tisch gezogen werden soll. Da die Speicherung und Auswertung vieler Datenspuren für die Bürger/innen nicht transparent ist, und weil negative Folgen für die Individuen nicht direkt spürbar sind, sondern möglicherweise erst viele Jahre nach der Datenspeicherung auftreten und die Ursache oft nicht erkennbar ist, findet hier ein substantieller Kontrollverlust der Bürgerinnen und Bürger statt. Sie werden nicht unvoreingenommen in der Gegenwart betrachtet und auch nicht mehr gefragt, sondern sie werden auf Grundlage von Daten aus der Vergangenheit kategorisiert und gemäß einer Prognose für die

Datenschutz ist Verbraucherschutz. Machen Sie uns stark!

▶https://digitalcourage.de/mitglied

Links und weitere Infos: digitalcourage.de/jahrbuch19

Foto: Alexander Altmann, cc by-sa 4.0

„Wer sich laufend beobachtet fühlt, nimmt von der Verfassung garantierte Rechte wie freie Meinungsäußerung und Versammlungsfreiheit möglicherweise nicht mehr in Anspruch.“

Zukunft behandelt: Firmen interessiert in der Regel weder der Einzelfall noch die Wahrheit, es geht um Gewinnmaximierung im Gesamtergebnis. Jede Bürgerin und jeder Bürger ist aber ein Einzelfall – ihnen gehen Handlungsoptionen und Entscheidungsfreiheit verloren. Wer die möglichen Folgen der Datensammelwut nicht kennt, wird zur Manövriermasse derer, die Zugriff auf die Daten haben und diese für sich verwerten.

Wer sich hingegen bewusst ist, dass eben diese Art der Informationsauswertung stattfindet, wird sich bemühen, sein oder ihr Verhalten anzupassen. Das kann je nach Situation bedeuten: sich unauffällig (oder auch besonders auffällig) benehmen, die (vermutete) Erwartung des Beobachters erfüllen oder aber auch ausweichen, sich verbergen, sich nicht äußern, anonym bleiben, lügen.

Wer sich aber laufend beobachtet fühlt, wird nicht nur in der freien Entfaltung der Persönlichkeit behindert, sondern nimmt auch von der Verfassung garantierte Rechte wie freie Meinungsäußerung und Versammlungsfreiheit möglicherweise nicht mehr in Anspruch. So zerstört der Verlust der informationellen Selbstbestimmung die Fähigkeit zur Kommunikation und zur Partizipation. So gehen die Ideen, Meinungen und Talente dieser Menschen nicht mehr in die Allgemeinheit ein und damit auch das Engagement für etwas, das über die eigenen Interessen hinaus geht, für die Gesellschaft verloren. Hier geht es also keineswegs nur um private Bedürfnisspielräume, die jeder ohne Schaden für sich selbst aushandeln könnte. Zur Disposition stehen vielmehr zunehmend Grundrechte, die nicht verhandelbar sind, sondern unverzichtbar für Gemeinwohl und Demokratie.

▶Zur Disposition stehen vielmehr zunehmend Grundrechte, die nicht verhandelbar sind, sondern unverzichtbar für Gemeinwohl und Demokratie.◀

▶Warum nicht den Datenschutz dem freien Markt überlassen?

Von Seiten der Wirtschaft wird oft das Argument vorgetragen, die Menschen seien doch mündige Verbraucher und könnten selbst entscheiden, was sie wollen. Im Folgenden einige Gründe, warum das mit dem selbständigen Aushandeln der Datenschutzbedingungen zumeist nicht klappt.

- Die Verbraucher.innen haben keine oder nur sehr rudimentäre Information über mögliche langfristige Folgen.
- Die Vertragsbedingungen, denen sie zustimmen sollen, sind meist völlig unlesbar. Es ist schlicht nicht zumutbar, erst seitenlange, in Juristensprache verfasste AGBs kritisch zu lesen, um z.B. eine Bestellung aufzugeben.
- Oft wird eine Irreführung der Verbraucher.innen auch mehr als billigend in Kauf genommen. Welcher Verbraucher ahnt schon, dass „Ihre Daten werden vertraulich behandelt, sie werden grundsätzlich nicht an unberechtigte Dritte weitergegeben.“ keineswegs heißt, dass die Daten nicht weitergegeben würden. Sondern vielmehr, dass das zwar „grundsätzlich“ so ist, aber das „grundsätzlich“ keine Verstärkung der Aussage ist, sondern bedeutet, dass es Ausnahmen gibt, und zwar bei „berechtigten“ Dritten. Diese „Ausnahme“ ist übrigens die Regel – fast alle Versandhandelsunternehmen „vermieten“ oder verkaufen die Adressen ihrer Kunden. An diesem Beispiel einmal durchexerziert: Damit die Verbraucher verstehen, um was es geht, müsste der Vertragstext etwa so lauten:

  Ich bin einverstanden, dass meine Adresse, angereichert mit Alter, Wohnortgröße, Kaufkraft und Versandhandelsneigung auf dem kommerziellen Adressmarkt verkauft wird.

  [ ] *Hier ankreuzen, falls ja.*

  Wie viele da wohl „ja“ ankreuzen würden?

▶Der einzelne Verbraucher verhält sich zunächst einmal egoistisch.◀

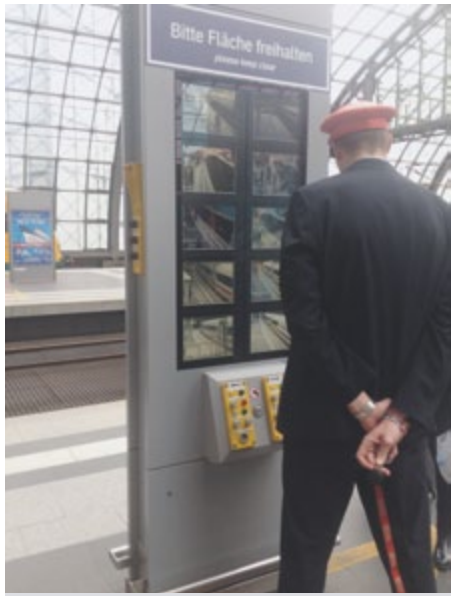
- Oder wer weiß, dass die „Informa Unternehmensberatung“, mit der viele Direktbanken laut ihrer Vertragsbedingungen Daten austauschen, keine Unternehmensberatung ist, sondern ein Scoring-Unternehmen?
- Verbraucher verlassen sich in Deutschland a) auf die Gesetze, b) darauf, dass, wenn etwas schief geht, sich schon irgendeine Institution für sie darum kümmern wird. (Also erst einmal fleißig Rabatt in Anspruch nehmen und sich dann bei den Datenschutzbeauftragten oder bei den BigBrotherAwards beschweren.)
- Und: Der einzelne Verbraucher verhält sich zunächst einmal egoistisch und keineswegs so, wie es für die Gesamtheit der Verbraucher von Vorteil wäre. Langfristig ist das ein Nachteil auch für den einzelnen.

- Divide et impera. (Teile und herrsche) Solange die negativen Folgen nur andere betreffen, ist alles egal. (Es geht ja nur um Terroristen, Sexualstraftäter, Schwarzfahrer, Arbeitslose oder auch nur um die nervigen LKWs auf der Autobahn etc., das betrifft mich also nicht oder es nützt mir vielleicht sogar.) Diese Haltung hat Martin Niemöller in seinem bekannten Zitat gut charakterisiert. („Als die Nazis die Kommunisten holten, habe ich geschwiegen; ich war ja kein Kommunist./ Als sie die Sozialdemokraten einsperrten, habe ich geschwiegen; ich war ja kein Sozialdemokrat./ Als sie die Gewerkschafter holten, habe ich nicht protestiert; ich war ja kein Gewerkschafter./ Als sie die Juden holten, habe ich nicht protestiert; ich war ja kein Jude. / Als sie mich holten, gab es keinen mehr, der protestierte.“)
- Das Sein bestimmt das Bewusstsein: Solange jemand eine Senator Card von der Lufthansa hat und als „A-Kundin“ hofiert wird, findet sie das „Miles and More“-Konzept toll. Wenn sie ihr entzogen wird, weil Lufthansa mitbekommen hat, dass sie wegen Jobwechsel nicht mehr so viel verdient, findet sie das System plötzlich nicht mehr so gut.
- Die Argumentation mit dem Eigentumsbegriff („Meine Daten gehören mir!“) hat sich als nicht hilfreich herausgestellt. Denn die Wirtschaft argumentiert, dass die einzelne Adresse nichts wert sei, kostbar werde eine Adresse erst dadurch, dass sie mit weiteren Informationen angereichert und mit anderen Adressen mit ähnlichen Merkmalen zusammengestellt wird.

> **“Als sie mich holten, gab es keinen mehr, der protestierte.“**

Was ist der Unterschied zwischen dem Bekanntsein im Tante Emma Laden und der Payback-Karte?

Das ist ähnlich wie der Unterschied zwischen einem Polizisten, der Streife geht, und einer Videoüberwachung. Zum einen ist es eine Frage der Gegenseitigkeit. Im ersten Fall ist eine *Person* das Gegenüber, im anderen eine anonyme technische Struktur, wo verborgen bleibt, was eigentlich passiert. Bei einer Videokamera ist völlig unklar, ob sie funktioniert, wer auf den Monitor guckt, ob die Kamera in meine Richtung schaut, ob jemand am Monitor gerade auf meinen Ausschnitt zoomt oder auf das Buch, das ich auf der Parkbank lese. Guckt überhaupt jemand? An wie viele Stellen gleichzeitig wird übertragen? Wird aufgezeichnet? Wie lange wird die Aufnahme aufbewahrt? Wer hat Zugriff darauf ? usw.



„Bei Videoüberwachung ist völlig unklar, ob sie funktioniert, ob jemand guckt und wer guckt.“

Foto: Claudia Fischer, cc by-sa 4.0

Im Tante-Emma-Laden bin ich bekannt und man weiß dort, was ich gerne einkaufe. Aber ich kenne meinerseits eben auch Tante Emma. Bei einer Kundenkarte liefere ich jedes Mal meinen kompletten Einkaufszettel ab, es ist unklar, wer diese Daten verarbeitet, wie lange sie aufbewahrt werden und wer welche Schlussfolgerungen aus ihnen zieht. Wer in den 90ern häufiger besonders billiges Rindfleisch im Sonderangebot gekauft hat – und wir nehmen jetzt mal an, es hätte zu dieser Zeit schon Kundenkarten à la Payback gegeben – könnte so möglicherweise heute kein Angebot mehr für eine günstige Krankenversicherung bekommen, denn die möchte das Risiko einer Creutzfeld-Jacob-Erkrankung ausschließen. Dabei war das Fleisch für den Hund bestimmt, der längst in den ewigen Jagdgründen weilt – aber danach wird nicht mehr gefragt. Tante Emmas Gedächtnis ist dagegen nicht ganz so gut und sie hat auch keinen Kontakt zu Krankenkassen, die mir ein Angebot machen wollen.

„Tante Emma kennt meine Vorlieben und ich kenne Tante Emma. Und Tante Emma verpetzt mich nicht an die Krankenkasse.“

Foto: Justus Holzberger ,cc by-sa 4.0

Der Unterschied liegt in der fehlenden Gegenseitigkeit, im Machtgefälle zwischen Mensch und anonymer Struktur, in der fehlenden Transparenz und in der Dimension.

Warum gibt es so wenig Widerstand gegen die Datensammelwut?

- Der Einzelfall der Datensammlung erscheint unwichtig
- Die Probleme tauchen erst später auf.
- Dass die Ursache der Probleme in der Auswertung der gesammelten Daten liegt, wird oft gar nicht erkannt.
- Die Zusammenhänge sind komplex und undurchschaubar.
- Es herrscht Resignation „weil wir sowieso schon überall gespeichert sind“ oder „weil die sowieso machen, was sie wollen“

Links und weitere Infos: digitalcourage.de/jahrbuch19

- Es gibt einen Trend zur Entsolidarisierung in der Gesellschaft: „ich zahle doch nicht für andere mit!“ oder „Ich zahl nur für genau das, was ich selbst verbrauche“. Das erfordert Einzelabrechnung und damit minutiöse Speicherung der persönlichen und der Verbrauchsdaten. Pauschalabgaben sind wesentlich datenschutzfreundlicher, z.B. Rundfunksteuer pro Haushalt statt GEZ, die an den Besitz eines Fernseh- oder Radiogerätes gekoppelt ist, Autobahn-Vignette statt Kfz-Kennzeichenerfassung an Mautbrücken, Kulturflatrate statt Digital Rights Management (DRM).
- Von Seiten der Innenpolitik werden solche Datensammlungen gerne toleriert nach dem Motto „Wer weiß, wozu man die auch mal brauchen kann.“

Pauschalabgaben sind wesentlich datenschutzfreundlicher.

Grundsätzliches

Daten, die wir einmal abgegeben haben, können wir nicht mehr zurückholen. Und Informationen, die wir heute als banal und unwichtig ansehen, können morgen schon eine ganz andere Bedeutung erhalten, wenn sie in einen anderen Kontext (zum Beispiel Terroristenfahndung) oder in andere Hände geraten (Arbeitgeber, Krankenkasse), wenn neue Forschungsergebnisse (zum Beispiel Zusammenhang zwischen Rindfleisch, BSE und Creutzfeld-Jakob) vorliegen oder wenn sich die politischen Verhältnisse ändern.

Auch wenn eine bestimmte Anwendung heute noch nicht gemacht wird, ist dies doch für die Zukunft keineswegs ausgeschlossen. Unternehmen können samt Datenbestand aufgekauft werden. Aktionäre können verlangen, dass die Kundendaten doch ausgewertet werden, wenn dadurch mehr Profit erzielt werden kann. Eine Ermittlungsbehörde kann die Daten beschlagnahmen. Allgemeine Geschäftsbedingungen, Datenschutzbestimmungen, sogar Gesetze können geändert werden. Vielleicht erinnern Sie sich an die Maut-Daten, die kurz nach der Einführung plötzlich ausgewertet werden sollten, um einen des Mordes verdächtigen Fernfahrer zu finden, obwohl es gesetzlich ausgeschlossen worden war? Große Datensammlungen wecken stets Begehrlichkeiten. Wenn sie erst einmal vorhanden sind, gibt es schnell Ideen, was man damit noch alles anfangen könnte. Das ist gefährlich.

Wir brauchen datenschutzfreundliche Technik („Privacy Enhancing Technologies“). Wenn eine technische Infrastruktur erst einmal in einer bestimmten Form allgemein installiert ist, kann sie kaum noch geändert werden. Wenn die Technik nicht von vornherein so designt ist, dass sie Missbrauch schwer oder unmöglich macht, wird er früher oder später passieren – legal oder illegal. Späteres Nachbessern an der Technik wird teuer und kann den Schaden kaum wieder gutmachen.

Grafik: Digitalcourage, cc by-sa 4.0

Der IT-Wirtschafts-Lobbyverband Bitkom hat 2017 einen BigBrotherAward von uns erhalten.

Wir brauchen Gesetze, die den Gefährdungen durch neue Technik wirksam begegnen. Die datensammelnde Wirtschaft, der Handel und ihre Lobbyverbände wie zum Beispiel der IT-Branchenverband Bitkom (BBA 2017) bemühen sich seit Jahren intensiv darum, gesetzliche Regulierungen abzuwehren, indem sie sogenannte „Selbstverpflichtungserklärungen“ der Wirtschaft propagieren. Diese sollten jedoch zutreffender „unverbindliche Absichtserklärungen“ genannt werden. Warum Firmen, die stets beteuern, nichts Böses mit den gewonnenen Daten machen zu wollen, Angst vor einer gesetzlichen Regulierung haben, leuchtet nicht ein. Denn eine gesetzliche Regulierung würde die „good guys“, also die Firmen, die die Privatsphäre der Bürger tatsächlich achten, schützen – sowohl vor der böswilligen Konkurrenz als auch im Zweifelsfall vor ihren eigenen Aktionären.

Es spricht einiges dafür, dass die Verwirklichung eines effektiven Datenschutzes langfristig auch im Sinne der Wirtschaft ist. Die ökonomische Argumentation sollte die bürgerrechtliche jedoch keinesfalls ersetzen. Akzeptanz-Studien können nicht das Maß der Dinge sein – denn Bürgerrechte sind keine Handelsware, auch wenn das im Tausch gebotene Linsengericht ein bisschen reichhaltiger werden sollte.

Die Zeiten ändern sich – aber nicht von selbst

Zwei Zitate:

> *“ You have zero privacy anyway – get over it.”*

(Scott McNealy,
Chef von Sun Microsystems, 1999)

> *“ Only the Beginning: The movement to respecting privacy is just getting started. We expect to see more public debate, legislative reforms, and business consequences in the years to come. Smart companies are recognizing the need to change their business practices and (...) to design and implement sound privacy policies.”*

(Sun Microsystems
Newsletter für IT-Professionals, 2004)

1999 bügelt der Geschäftsführer von Sun noch alle Datenschutzbedenken zu einem ihrer Produkte ab „Privatsphäre gibt es

sowieso nicht mehr – vergessen Sie's.". Der Sun-Newsletter fünf Jahre später hört sich ganz anders an: „IT ohne Privacy wird sich in Zukunft nicht mehr verkaufen lassen. Fragen Sie die Experten von Sun." Kompliment: Elegante 180 Grad Wende.

Derweil ist Scott McNealys saloppes „Privatsphäre gibt es sowieso nicht mehr" immer noch der Mainstream-Diskurs. Der Verlust der informationellen Selbstbestimmung wird oft als quasi naturgesetzliche Begleiterscheinung des technischen Fortschrittes – insbesondere der Digitalisierung und der Vernetzung – dargestellt, an der man nichts ändern kann.

Wer so denkt, gibt Gestaltungsmacht auf. Wer so argumentiert, will, dass andere Gestaltungsmacht aufgeben. („Widerstand ist zwecklos!") Noch ein Zitat:

> *„ Es kommt einfach darauf an, was man will, man muss sich entscheiden: Alle Menschen überall und miteinander vernetzt, global offene Kommunikationskanäle, Überwachung, usw. – und dann aber noch Privatsphäre erhalten, wie wir sie gewohnt sind – das geht nicht!"*

(Zukunftsforscher Jeremy Rifkin im aspekte-Beitrag zum Film „Minority Report", ZDF, 26.9.2002)

Sehen wir es als eine interessante Parallele zum Umweltschutz: Jahrzehntelang wurde Umweltverschmutzung als unausweichliche Nebenwirkung der Industrialisierung akzeptiert. Wer Vergiftung von Boden, Luft und Wasser durch die Industrie kritisierte, wurde geraten, doch gleich „zurück auf die Bäume zu gehen".

Der Arbeit einer Vielzahl von Umweltschutzinitiativen ist es zu verdanken, dass sich diese Einstellung geändert hat. Umweltschutz wird mittlerweile als Sicherung der Lebensgrundlagen auf diesem Planeten begriffen; er ist in vielen Ländern im Bewusstsein der Bevölkerung verankert und in vielfältiger Form in die Agenda von Politik, Verbänden und auch der Wirtschaft eingezogen.

Eine ähnliche Bewusstseinsänderung ist für informationelle Selbstbestimmung gerade im Fluss. Erste Erfolge sind da, aber es ist noch viel zu tun. Das Wichtigste jetzt: Das Bewusstsein für das Problem schärfen und möglichst vielen Menschen vermitteln, dass sie Persönlichkeitsrechte besitzen, die durch keine noch so leckere Linsensuppe aufgewogen werden können.

Erhältlich im Digitalcourage-Shop!
Terrordilin Anti + BNDal Forte

2 Pillendosen Placebos gegen Terror
Gift für Freiheit und Menschenrecht
Ein Dekoartikel, (nicht zum Verzehr geeignet). Für alle, die ihren Humor noch nicht ganz verloren haben. Hilft bei Machtdefizit und Wählermangel, aber nicht gegen Terror.
Preis pro Set 11,98 Euro.
https://shop.digitalcourage.de

Lehren aus dem Mauerfall

Nicht die Politik, die Menschen müssen die Freiheit verteidigen!

Von Leena Simon

Dieser Kommentar ist in unserem Blog im November 2014 erschienen. 2019 feiern wir den 30. Jahrestag des Mauerfalls. Wenn Sie im ersten Satz aus den 25 Jahren 30 machen, ist dieser Text heute noch genauso aktuell und aussagekräftig wie damals.

Foto: Digitalcourage, cc by 4.0

Mit einem beeindruckenden Festakt feiert Berlin den Fall der Mauer vor 25 Jahren. Ein emotionales Spektakel, das viele Menschen auf die Straße und vielen Tränen in die Augen treibt. Redner.innen sprechen von Freiheit, Politiker.innen stecken Blumen in die Überreste der Mauer und eröffnen Dauerausstellungen. Eine ergreifende Stimmung geht von der Hauptstadt aus. Was haben wir uns auf dieses Ereignis gefreut. Darauf, dass die Überwindung des Überwachungsstaats DDR gefeiert wird. Die Held.innen des Mauerfalls verdienen es, gefeiert zu werden. Große Worte werden gesprochen. Von Freiheit und der „friedlichen Revolution". Man kann sich kaum entscheiden, wen man lieber zitieren möchte. Wenn da nur nicht permanent dieser Realitätsabgleich wäre. Die Worte wollen einfach nicht so recht schmecken.

Angela Merkel bezeichnet die Mauer als „in Beton gegossenes Symbol staatlicher Willkür". Wie bitter dies klingt in den Ohren derer, die sich heute für Grundrechte einsetzen und tagtäglich gegen staatliche Willkür in Deutschland kämpfen. In einer Politik, die das Problem von Überwachung abtut und selbst immer neue Überwachungsgesetze anstößt.

Totalüberwachung kehrt das Verhältnis zwischen Bevölkerung und Regierung um. Durch Überwachung werden wir zu Beherrschten. Und darum riefen die Demonstrant.innen am 4. November 1989 auf dem Alexanderplatz auch „Wir sind das Volk". Besonders oft hört man das überaus gerechtfertigte Lob an die Bürgerrechtsbewegung der 1980er Jahre. Doch die eingeladenen Gelobten vergessen zu erwähnen, dass Überwachung in Deutschland heute zum Alltag gehört. Es schmerzt mit anzusehen, wie die gleichen Politiker.innen von Freiheit und dem Unrecht der DDR sprechen, die in Bezug auf unsere heutigen Belange auf Dauerdurchzug gestellt haben.

Gegen was traten die Menschen damals an? Die Methoden der DDR hatten System. Regimekritiker.innen wurden beschattet, bespitzelt, eingeschüchtert und aus dem Weg geräumt. Doch es ging

auch subtiler. Bei der sogenannten „Zersetzung“ wurde das „Zielobjekt“ in seiner Wahrnehmung verunsichert. Viele merkwürdige „Zufälle“ führten dazu, dass man den eigenen Sinnen nicht mehr traute. Auf diese Weise konnte man sauber und unauffällig Menschen aus der Bahn werfen. Solche Beeinflussung basierte auf den genauen Informationen, die man über das „Zielobjekt“ gesammelt hatte. Dies ist noch immer möglich. Allerdings ist der Aufwand dafür enorm gesunken, die Präzision immens gestiegen.

▶Wir wollen sagen können: „Ja, wir haben aus der Geschichte der DDR gelernt.“◀

In Gesprächen über die „friedliche Revolution“ wird betont, wie wichtig es war, dass Menschen miteinander kommuniziert haben. Dass sie zueinander gestanden und sich engagiert haben. Wie schade, dass kaum jemand den offensichtlichen Zusammenhang herstellt und darauf hinweist, dass wir die Freiheit unserer Lebensräume und Kommunikationskanäle auch heute mit Solidarität und Engagement verteidigen müssen.

Gewiss war die Repression durch die Überwachung in der DDR viel deutlicher spürbar und die Möglichkeiten wurden (nach derzeitigem Kenntnisstand) viel umfassender genutzt. Sie betrafen ganz offensichtlich alle Menschen. Aber der Schwur, die Erinnerung wach zu halten und aus der Geschichte gelernt zu haben, ist völlig leer, wenn es erst dazu kommen muss, dass die „Leidenshöhe“ so hoch ist, wie sie im Jahr 1989 war.

Besonders an diesem Datum ist, wie es uns daran erinnert, dass es nicht die Politik ist, die die Verantwortung für Freiheit und Grundrechte trägt. Es sind die Menschen, die sich gemeinsam jeden Tag neu dafür einsetzen müssen.„In dieser Nacht war es das Volk selbst, das seine eigene Geschichte schrieb“, kann man nun Martin Schulz mit schönen Worten zitieren. Er wiederum ist nicht der erste, der eindringlich den Satz „Wir sind das Volk“ zitiert. Er, als Teil eines Regierungsorgans, das uns mehr und mehr als Untertanen behandelt.

Wir wollen sagen können: „Ja, wir haben aus der Geschichte der DDR gelernt.“ Damit wir das können, hilft es uns nicht, auf das Verhalten der Anderen zu schauen und zu diskutieren, ob diese sich ausreichend distanziert haben. Ob wir das sagen können, hängt ganz allein von unserem eigenen Verhalten ab.

Das bedeutet, dass wir einen solchen „Unrechtsstaat“ schon in seinen Anfängen mit aller Vehemenz verhindern müssen. Das bedeutet, dass wir nicht warten dürfen, bis er wieder so weit fortgeschritten ist, dass man die Folgen bereits deutlich spüren kann. Wer vom Griff auf die heiße Herdplatte gelernt hat, fasst nicht erneut drauf und wartet, bis die Hand wieder schmerzt, bevor er sie weg nimmt. Daher müssen wir der Politik auf die Füße steigen, damit sie unsere Grundrechte schützt. Besonders vor sich selbst.

Foto: Jan Bornemann, cc by-sa 4.0

Zubehör und Service zum Thema Datenschutz –
gibt es auch bei uns im Shop.

Preise und Auszeichnungen für Digitalcourage

Foto: Fabian Kurz, cc by-sa 4.0

GEWÜRDIGT WIRD
DAS BESONDERE ENGAGEMENT
FÜR DAS WOHL UND DAS ANSEHEN
DER STADT BIELEFELD.

Mit Kreativität, Hartnäckigkeit und Unerschrockenheit setzen sich Rena Tangens und padeluun seit mehr als drei Jahrzehnten für die Wahrung der Grundrechte und den Datenschutz ein und senden damit aus Bielefeld wichtige Impulse für das Miteinander in unserer (digitalen) Gesellschaft.

28.Juni 2018. Pit Clausen,
Der Oberbürgermeister

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.

- **„Ehrennadel der Stadt Bielefeld“** an Rena Tangens und padeluun (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 Wawrzyniak 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. Siehe Seite 42 und 130.

- **„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 (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
- **„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)

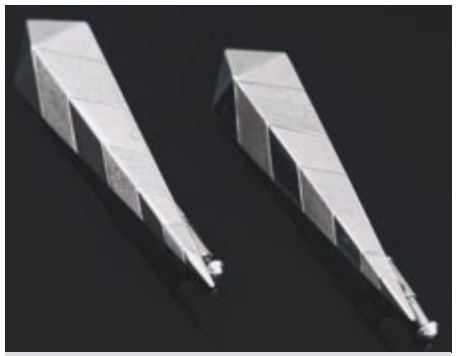


Foto: Fabian Kurz, cc by-sa 4.0

So sehen sie aus:
die Ehrennadeln der Stadt Bielefel

Und dann noch ein paar datenschutzrelevante Termine für 2019

28.1.2019	Europäischer Datenschutztag. Dieser Aktionstag erinnert an die Unterzeichnung der Europäischen Datenschutzkonvention am 28. Januar 1981.
30.1.-1.2.2019	**cpdp Internationale Datenschutzkonferenz in Brüssel.** Thema 2019: Data Protection and Democracy. Info: cpdpconferences.org/
1.-3.2.2019	**Aktivcongress** – für alle, die sich für Datenschutz, Grundrechte und Netzpolitik aktiv engagieren wollen. Im Bunten Haus von ver.di in Bielefeld Sennestadt. Anmeldung über digitalcourage.de
5.2.2019	**Safer Internet Day / Tag der Internetsicherheit.** Zur Sicherheit gehört auch, nicht überwacht zu werden! Hier gibt es aktuelle Tipps, wie Sie sich selbst schützen können: https://digitalcourage.de/digitale-selbstverteidigung
23.5.2019	**Tag des Grundgesetzes**. Am 23. Mai 1949, vor 130 Jahren, wurde das deutsche Grundgesetz verkündet. Lesetipp: Christian Bommarius: Das Grundgesetz – eine Biographie. Organisieren Sie für diesen Tag doch einfach mal selbst ein „Lesen gegen Überwachung“ – im Café oder im eigenen Wohnzimmer! https://lesen-gegen-ueberwachung.de/
25.5.2019	Die **Europäische Datenschutzgrundverordnung** ist in allen EU-Mitgliedstaaten seit einem Jahr in Kraft. Wie ist Ihr persönliches Fazit? Nutzen Sie Ihre Rechte? Wir empfehlen Seite 111.
23.-26.5.19	**Wahlen zum Europäischen Parlament**. Lesen Sie dazu auch unseren Artikel zu ePrivacy auf Seite 35
8.6.2019	**BigBrotherAwards.** Die Verleihung der „Oscars für Überwachung“ findet 2019 wieder im Bielefelder Stadttheater statt. Info: bigbrotherawards.de
8.-11.11.2019	**Freedom not Fear in Brüssel**. Datenschutz- und Netz-Aktivist.innen aus ganz Europa treffen sich für ein langes Wochenende zu einem selbstorganisierten Kongress: Sich informieren und vernetzen, voneinander lernen, Aktionen planen. Montags besuchen wir gemeinsam das Europäische Parlament. Neue Interessierte sind herzlich willkommen!
27.-30.12.2019	**36C3 – Chaos Communication Congress**. Großes internationales Treffen von Hackern und Häcksen. Ort bei Redaktionsschluss noch unbekannt.

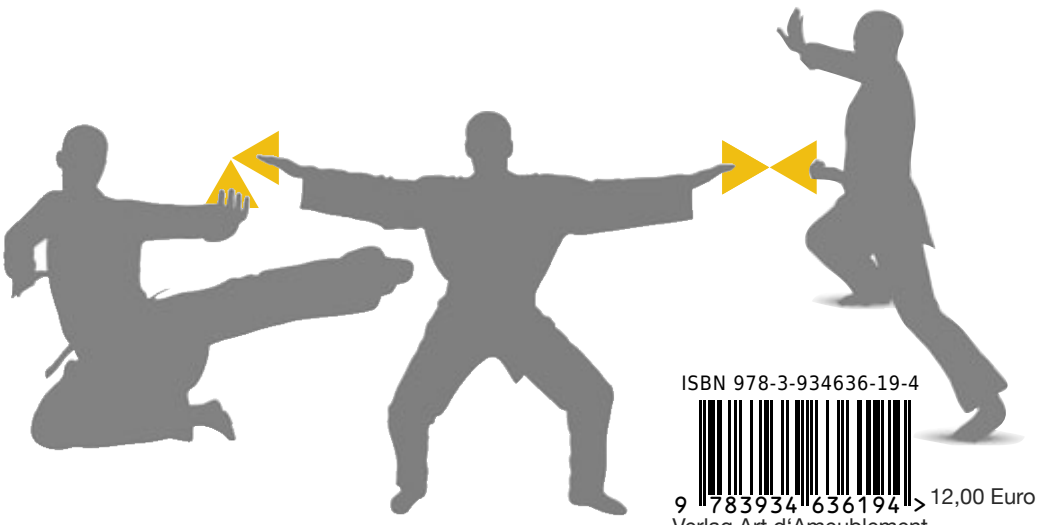
Index

Links und weitere Infos: digitalcourage.de/jahrbuch19

Foto: Matthias Hornung, cc by-sa 4.0

digitalcourage für das Jahr 2019

Themen u.a. ▶Staatstrojaner ▶Vorratsdatenspeicherung ▶Schutzranzen ▶neue Polizeigesetze ▶Gesichtserkennung und ▶Smart Cities. ▶Datenschutzgrundverordnung: Interview mit Jan Philipp Albrecht ▶Verschlüsselung leicht gemacht: „Pretty Easy Privacy“ (p≡p) ▶Alle Preisträger der BigBrotherAwards 2018 und was sich daraus entwickelt hat ▶Grundsatztext: Tausche Bürgerrechte gegen Linsengericht ▶Digitale Selbstverteidigung: Wie Sie Ihren Computer und Ihr Smartphone vor Datenkraken schützen“



ISBN 978-3-934636-19-4

9 783934 636194 > 12,00 Euro

Verlag Art d‘Ameublement