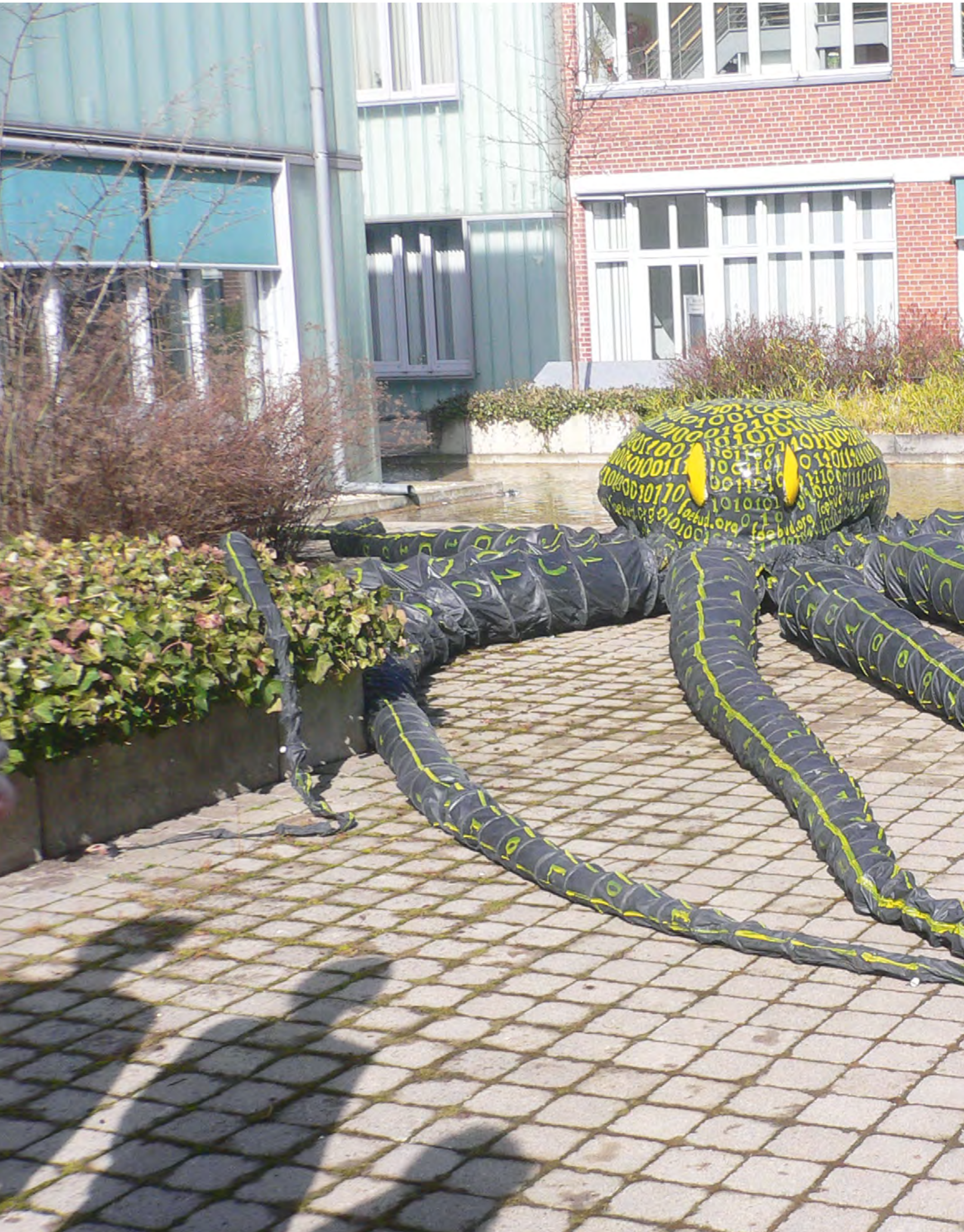
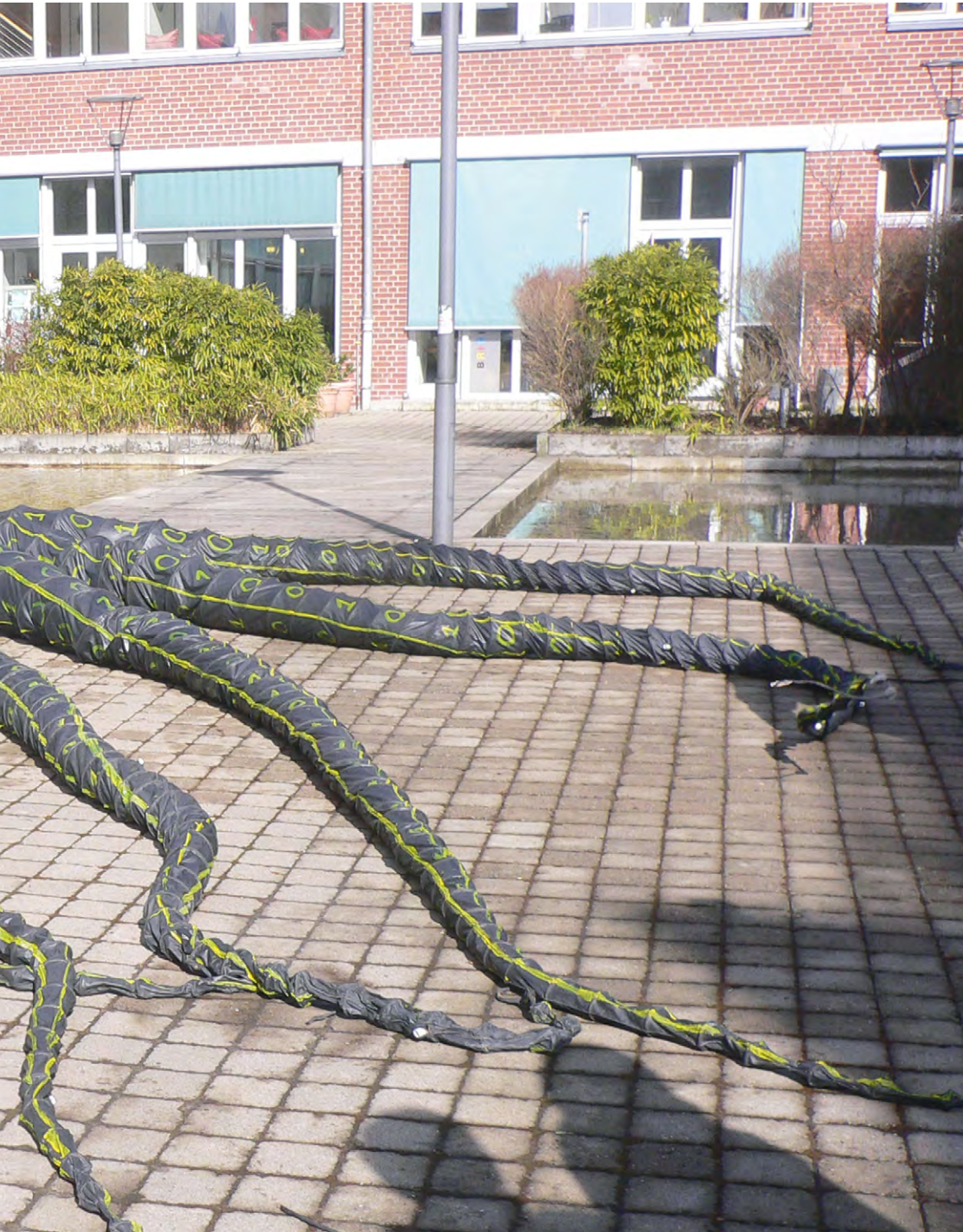
padeluun & Rena Tangens (Hrsg.)

digitalcourage

Jahrbuch 2018


foebud.org

Wir legen Datenkraken trocken.
digitalcourage.de



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

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 978-3-934636-16-3

padeluun & Rena Tangens (Hrsg.)

digitalcourage

Jahrbuch 2018

Inhalt

Aktivierendes 119

Wir sind jetzt 30!

Foto: Fabian Kurz, cc by-sa 4.0

Parallel zur Abschlussredaktion dieses Jahrbuches bereiten wir in diesen Tagen unsere 30. Geburtstagsfeier im Stadttheater Bielefeld vor. Stilecht mit einer „Lesung gegen Überwachung“ und anschließendem gemeinsamem Besuch der Bühnenfassung von „1984“ von George Orwell. Jetzt, wenn Sie dieses Buch in den Händen halten, wird die Feier vorbei sein und der Arbeitsalltag hat uns wieder.

Dieser Wechsel zwischen Genussphasen mit klugen Köpfen und kreativen Ideen und harter Arbeit prägt unseren Alltag seit es uns gibt. Auch die Idee, Ihnen und uns zu unserem Geburtstag ein Jahrbuch zu „schenken“ (Danke an alle, die es bei uns gekauft und damit beim Finanzieren geholfen haben), entstand bei einem Frühstück im Mai.

„Frühstück“ war schon immer eine wichtige Institution. In unserer Kunstgalerie Art d‘Ameublement gaben sich in den 1980er Jahren den ganzen Tag Menschen die Klinke in die Hand – und den ganzen Tag gab‘s „Frühstück“ mit großen Kannen Ostfriesentee. Weil wir dadurch irgendwann gar nicht mehr zum Arbeiten kamen, lagerten wir das aus – erst räumlich in ein Café, dann organisatorisch in einen Verein.

1987 gründeten wir den „FoeBuD e.V.“ – (Abkürzung von „Verein zur Foerderung des öffentlichen bewegten und unbewegten Datenverkehrs“). Der Name war ein Scherz auf Kosten der Deutschen Bundespost, die damals noch für die Telekommunikation zuständig war, und ihre komplizierten Abkürzungen. Das weiß heute kein Mensch mehr außer ein paar Steampunk-Hackern. *„Fö-was? Können Sie das mal buchstabieren?“* hörten wir ein Dutzend Mal täglich am Telefon. FoeBuD erklärte nichts, verweigerte sich dem Gedächtnis und war gänzlich ungeeignet für TV-Untertitel oder Schlagzeilen. Sympathisch, aber unklug, wenn man – wie wir – viele Menschen erreichen und überzeugen will. Zum 25. Jubiläum 2012 änderten wir unseren Namen in „Digitalcourage“, und unter diesem Namen legen wir Ihnen nun unser Jahrbuch vor.

Es soll eine Momentaufnahme mit bleibendem Wert sein. Es enthält **Aktuelles** – was bewegt uns gerade, welche Aktionen haben wir organisiert, an welchen Themen sind wir dran, von Videoüberwachung mit Gesichtserkennung bis zu Smart Cities. **Abgemahntes** – die BigBrotherAwards, alle Preisträger eines Jahres mit Begründung und aktuellem Update zu Reaktionen was seit der Preisverleihung geschehen ist. **Aktivierendes –** Hilfe zur digitalen Selbstverteidigung, wie organisieren Sie ein „Lesen gegen Überwachung" bei sich vor Ort oder Checklisten, z.B. wie Ihre Stadt datenschutzfreundlich werden kann. Dazu **Richtungsweisendes –** Texte aus unserer Vergangenheit, die uns heute noch etwas zu sagen haben – wir waren selbst erstaunt beim Lesen. Im **Anhang** finden Sie noch ein paar nützliche Infos wie wichtige Datenschutz-Termine für 2018. Für Aktualisierungen, Quellen und weiterführende Links haben wir eine komfortable Webseite eingerichtet: digitalcourage.de/jahrbuch18. Damit Sie die langen Internetadressen nicht umständlich abtippen müssen.

Es gab noch viele „Frühstücke" in den letzten dreißig Jahren. Einer unserer ersten Praktikanten formulierte die Kurzform seines Berichts für die Schule: „12 Uhr: Der Tag beginnt mit einem Frühstück. 16 Uhr: Welt gerettet. 17 Uhr: Logoff." Das kleine Wort „Logoff" musste damals, 1992, der Lehrerin noch erklärt werden. So wie wir heute Lehrer.innen und Schulleitungen erklären, dass Facebook kein guter Ort ist, um Hausaufgaben zu verteilen und dass auf Google Docs keine Referate oder Klassenfotos gespeichert werden sollten.

Die Welt haben wir noch nicht gerettet, aber wir sind dabei! Dass Datenschutz als Thema mitten in der Gesellschaft angekommen ist, werten wir unter anderem auch als einen Erfolg unserer Arbeit. Manchmal packt uns die Wut, wenn – wie 2017 – Überwachungsgesetze nachts durch den Bundestag geschummelt werden. Aber dann gibt es auch wieder Erfolgsmeldungen, z.B. nach den BigBrotherAwards, die uns am Laufen halten. Vieles davon können Sie auf den folgenden Seiten lesen.

padeluun und Rena Tangens, November 2017

▶ P.S.: Und auch wenn Sie nicht alle bei unseren kreativen Frühstücken dabei sein können: Wir laden Sie herzlich ein, mitzumachen bei der Rettung der Welt. Werden Sie Fördermitglied! Arbeiten Sie mit! Organisieren Sie eine Lesung gegen Überwachung! Alle sachdienlichen Hinweise finden Sie in diesem Buch und auf digitalcourage.de/jahrbuch18.

Am Girl's Day 2017 waren Alwina und Sora (beide 14) bei uns im Büro. Vormittags haben sie mit unserem Admin einen Rechner zerlegt und nachmittags ging es in unsere Redaktion. Das Ergebnis ist ein kurzer Text, vor dem die Büro-Crew nur den Hut ziehen kann. Alwina und Sora erklären klar und deutlich, warum Datenschutz – nicht nur für Jugendliche, sondern für alle – wichtig ist.

Foto: Digitalcourage, alle Rechte vorbehalten

Liebe Leute,

wie ihr wisst, ist Datenschutz ein viel diskutiertes Thema. Es geht zum Beispiel um den Schutz von persönlichen Daten wie Telefonnummern, Adressen, Fotos und persönliche Interessen. Wer nicht möchte, dass diese Daten missbraucht werden, sollte aufpassen.

- Ihr könnt z.B. eure E-Mails verschlüsseln,
- sichere Passwörter anlegen,
- aufpassen was ihr in Sozialen Netzwerken preisgebt
- und Menschen erklären wofür ihre Daten verwendet werden.

Tipp: Je weniger Daten man von sich preisgibt, desto mehr ist man geschützt. Ein paar wichtige Informationen für dich:

- Du kannst selber bestimmen wer etwas über dich erfahren soll.
- Deine Daten dürfen nur von dir genutzt werden.
- Es ist deine Persönlichkeit. Sie darf nicht durch die Nutzung von Daten, bzw. Informationen beeinträchtigt werden.
- Es ist nicht erlaubt, von anderen die Daten zu kopieren und sich selber dafür auszugeben. Du hast z.B. das Recht am eigenen Bild.

Alwina und Sora

Aktion „Ehrliche Schilder“ von Digitalcourage und FIfF gegen Videoüberwachung in Berliner U-Bahnhöfen im Februar 2017.

Was uns bewegt

Unsere wichtigsten Aktionen und Kampagnen 2016/17/18

Von Claudia Fischer und Friedemann Ebelt

Die wichtigste Aufgabe eines Jahrbuches ist, Ihnen einen Einblick zu geben, was wir alles tun, um Grundrechte und Privatsphäre zu schützen. Das kann immer nur eine Momentaufnahme sein. Der Redaktionsschluss dieses Buches lag im Sommer 2017, noch vor der Bundestagswahl. Wir sind uns aber sehr sicher: Die folgenden Themen werden uns auch 2018 auf Trab halten. Schmökern Sie sich durch – Aktualisierungen und Hintergründe finden Sie auf unserer Internetseite, ebenso unsere Jahres- und Transparenzberichte, die sich an Kalenderjahren orientieren.

„Wir sehen uns vor Gericht!“

Das sagen wir sehr ungern. Der Satz passt gar nicht zu uns, den „freundlichen Genies“, wie wir seit den 1980er Jahren immer genannt wurden. Eigentlich würden wir viel lieber argumentieren, debattieren, mit Andersdenkenden sprechen und sie überzeugen oder von ihnen lernen. Das sind für uns die besten Wege demokratischer Auseinandersetzung.

Häufig bleibt uns aber gar keine andere Wahl, als gerichtliche Entscheidungen einzufordern. Nicht nur, weil die Anhänger.innen der „Überwachung=Sicherheit“-Logik so beratungsresistent sind, sondern auch, weil häufig Gesetze paketweise durchgepeitscht, mit Finten verabschiedet oder nachts durch den Bundestag gemogelt werden. Damit werden Fakten geschaffen ohne gesellschaftliche Debatte, in die wir uns einbringen könnten. Und dann bleibt uns nur noch die Möglichkeit, juristisch dagegen vorzugehen.

Verfassungsbeschwerde gegen die Vorratsdatenspeicherung eingereicht

Die Bundesregierung will einfach nicht wahrhaben, dass das Gesetz zur Vorratsdatenspeicherung von 2015 europarechtswidrig, unverhältnismäßig und verfassungswidrig ist. Es gibt zwar schon ei-

Foto: Katarzyna Mazur, CC-BY-SA 3.0

29. Juni 2017, Demo im strömenden Regen: padeluun spricht mit der Bundestagsvizepräsidentin Petra Pau (Die Linke) über unseren Protest gegen die Vorratsdatenspeicherung

Karikatur urheberrechtlich geschützt; Rechte bei Christiane Pfohlmann, www.pfohlmann.de

nige Urteile, z.B. vom Europäischen Gerichtshof und vom Verwaltungsgericht NRW, in denen unsere Einschätzung in Teilen bestätigt wird, aber wir wollen das Gesetz insgesamt kippen. Deshalb haben wir am 19. Dezember 2016 mit unserem Anwalt Meinhard Starostik eine Verfassungsbeschwerde gegen die Vorratsdatenspeicherung eingereicht.

Als wir den Brief eingeworfen haben, war bereits klar, dass wir auf eine Entscheidung ein bis zwei Jahre warten müssen. Inzwischen hat das Bundesverfassungsgericht uns mitgeteilt, dass sie unsere Beschwerde 2017 nicht mehr bearbeiten werden.

▶Wir blicken gespannt auf 2018.

Auch, weil die Justiz- und Innenminister von Estland, Bulgarien und Österreich ihre jeweiligen EU-Ratspräsidentschaften, die von Juli 2017 bis Ende 2018 aufeinander folgen, für eine Wiederbelebung der europarechtswidrigen Vorratsdatenspeicherung nutzen wollen. Dazu entwickelten die drei Länder in einem informellen Treffen am 7. Juli 2017 ein gemeinsames 18-Monats-Programm, mit dem sie einen roten Faden für Vorratsdatenspeicherung durch ihre drei EU-Ratspräsidentschaften ziehen wollen. Auch darauf werden wir gemeinsam mit anderen europäischen Datenschützer.innen ein Auge haben.

▶Verfassungsbeschwerde gegen den Staatstrojaner vorbereitet

Staatstrojaner sind ein Angriff auf all unsere Geräte: Die Schnüffeldateien werden über Sicherheitslücken installiert, die dafür in jedem Smartphone, Computer, Tablet und in jeder Spielekonsole vorhanden sein müssen. So wurde es am 22. Juni 2017 beschlossen. Jetzt darf die Polizei z.B. bei einer Personenkontrolle am Flughafen mit Ihrem Smartphone im Hinterzimmer verschwinden und den Trojaner ins Gerät einpflanzen. Die technischen Hintertüren, mit denen das ermöglicht wird, können neben der Polizei aber auch alle möglichen Geheimdienste und Kriminelle nutzen.

„Bereits der Schadcode von WannaCry hat drastisch vor Augen geführt, dass ganze nationale Systeme in sicherheitsrelevanten Bereichen gestört werden können, so wie die IT-Systeme der Deutschen Bahn und der britischen Krankenhäuser“,

sagt unser Rechtsanwalt Meinhard Starostik. „Angesichts dieser Bedrohungen hat der Staat eine Schutzpflicht für die Sicherheit der Integrität und Vertraulichkeit informationstechnischer Systeme. Das Offenhalten von Sicherheitslücken widerspricht genau dieser Schutzpflicht."

Die Staatstrojaner werden übrigens entwickelt von dem Unternehmen „Gamma International" (BigBrotherAward 2012) und von der „Zentralen Stelle für IT im Sicherheitsbereich" (ZITiS). Einem geleakten Dokument zufolge soll die neue Generation von Staatstrojanern mit erweiterten Funktionen noch 2017 zum Einsatz kommen.

Ermöglicht wurde der Staatstrojaner durch eine juristische Hintertür: Die Regierungsparteien haben über den Rechtsausschuss in ein laufendes Gesetzgebungsverfahren auf den letzten Metern noch schnell eine „Formulierungshilfe" für eine Änderung eingebracht. Darin war die rechtliche Grundlage für den erweiterten Einsatz von Staatstrojanern verborgen. Auf diese Weise wurde die Überwachungskanone im *„Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens"* versteckt. Selbst die Bundesdatenschutzbeauftragte erfuhr davon erst im Nachhinein. Dieser Verfahrenstrick war undemokratisch und hat eine öffentliche Debatte und kritische Stellungnahmen verhindert.

Nicht jammern - klagen!

Unterstützen Sie unsere Verfassungsbeschwerden gegen Vorratsdatenspeicherung und Staatstrojaner!

- **https://digitalcourage.de/spende**

2017 haben wir eine Verfassungsbeschwerde gegen den Staatstrojaner vorbereitet und kräftig Unterschriften gesammelt. Auf unserer Webseite können Sie alle unsere Argumente gegen den Staatstrojaner nachlesen und sich über die Verfassungsbeschwerde aktuell auf dem Laufenden halten.

Verfassungsbeschwerden – im Dutzend billiger?

Leider nein – obwohl die Große Koalition in Berlin im ersten Halbjahr 2017 gleich einen ganzen Stapel von gesetzlichen Ungeheuerlichkeiten verabschiedet hat:

- Ausweis- und Passbilder dürfen nun von Geheimdiensten vollautomatisch abgerufen werden. (Bundestags-Drucksache 18/11279 und Drucksache 18/12417).
- Das „Videoüberwachungsverbesserungsgesetz" empfiehlt öffentlich zugänglichen Einrichtungen, sich im Zweifel eher für die Videoüberwachung als für Freiheitsrechte zu entscheiden. (18/78834)
- Das BKA-Gesetz (BKAG) erweitert Zuständigkeiten des Bundeskriminalamts und hebt das Trennungsgebot zwischen Nachrichtendiensten und Polizei, das sich aus dem Verfassungsprinzip des Rechtsstaats ableitet, auf.
- Das neue Bundesdatenschutzgesetz

Foto: Digitalcourage, cc by-sa 4.0

Aktion vor dem Bundesrat: Anti-Terror-Gesetze sind Placebos. Die Pillendosen mit Beipackzettel (Nebenwirkungen für Freiheit und Menschenrechte) gibt es im Digitalcourage-Shop zu kaufen.

(BDSG) weicht den Datenschutz auf. Kritisch sind vor allem Videoüberwachung, Scoring, Profiling, Betroffenenrechte und Gesundheitsdaten. (Mehr zum Bundesdatenschutzgesetz an anderer Stelle in diesem Buch.)

- Im Gesetz über die Bundespolizei (BGSG) wird die Vorratsdatenspeicherung aller Fluggastdaten beschlossen.
- Kurz bevor die Vorratsdatenspeicherung im Sommer 2017 beginnt, wird der Schutz der Daten gesetzlich ausgehebelt und der Katalog der Tatbestände, für deren Ermittlung diese Daten offiziell genutzt werden können, ausgeweitet (18/12359).
- Zur Aufklärung von Wohnungseinbrüchen sollen Handydaten aus der Umgebung in großem Umfang von Ermittlungsbehörden genutzt werden können (18/12359)
- IT-Sicherheitsgesetz: „Internet-Anbieter bekommen mehr Möglichkeiten, den Datenverkehr ihrer Kunden zu überwachen und zu filtern.“ (BSI-Gesetz)
- Die Entschlüsselungsbehörde ZITiS wird per Organisationserlass eingerichtet (18/11813)
- Start des Cyberkriegskorps der Bundeswehr (KdoCIR, BigBrotherAwards 2017, Details in der Laudatio von Rolf Gössner in diesem Buch)
- Das Prostituierten“schutz“gesetz (ProstSchG) zwingt Prostituierte, sich anzumelden, und es hebt die Unverletzlichkeit der Wohnung aller Bürgerinnen und Bürger in Deutschland auf.

Dabei haben wir nicht verfolgen können, ob sich in dem einen oder anderen Bundesland auch noch datenschutzrelevante Gesetze entwickelt haben.

Viele dieser neuen Überwachungsgesetze sind im Eiltempo durch die Ausschüsse, Bundestag und Bundesrat geprügelt worden, oft in nächtlichen Marathonsitzungen. Auffällig ist, dass das schon 2016 so war: Damals haben wir an alle Bundestagsabgeordneten und vor dem Bundesrat selbsthergestellte Placebo-Pillen-Dosen mit den Medikamenten *Terrordilin Anti* (Wirkstoff *Populismus*) und *BNDal Forte* (Wirkstoff *Terrorangst*) verteilt. Die Packungsbeilage warnte vor den Nebenwirkung der Gesetze für Demokratie und Freiheit.

Immer wird für solche Gesetze die Jokerkarte von angeblich drohenden Terror-Anschlägen gezogen und damit die Totalüberwachung der gesamten Bevölkerung legitimiert. Und „chillig“ (im Sinne von „beruhigend“) sind die Maßnahmen nicht. Eher „chilling“ wie in „Chilling Effect“ – also im Sinne von Abschreckung und Selbstzensur.

Durch die Willkür und Hektik bei der Gesetzgebung konnten wir nur wenig im Vorfeld verhindern oder zumindest abmildern – die Überwachungsgesetze sind beschlossen. Digitalcourage wird nun mit Anwält.innen prüfen, ob wir gegen einige oder alle oben genannten Gesetze Verfassungsbeschwerde einlegen werden. Glücklicherweise sind wir nicht allein, auch andere werden nach Karlsruhe ziehen. Wir werden auf jeden Fall sorgfältig abwägen und bei Erfolgsaussicht handeln. Wer uns dabei fachlich unterstützen möchte, möge sich bitte bei uns melden. Und natürlich werden wir auch zu Unterstützungs-Unterschriften aufrufen und Spenden sammeln, damit wir diese langwierigen und teuren Verfahren durchziehen können.

Jammern, resignieren und zynisch werden sind nicht die Lösung.

Werden Sie Fördermitglied – gemeinsam können wir was bewegen!

https://digitalcourage.de/mitglied

Wir werden einen langen Atem brauchen. Und wir haben einen langen Atem. Atmen Sie mit!

Strafanzeige gegen Real und Post geprüft – schneller Etappensieg gegen Gesichtserkennung

Manchmal kann es so schnell gehen: Mitte Juni 2017 erschienen die ersten Artikel darüber, dass in einigen Märkten der Supermarktkette Real und in einigen Filialen der Deutschen Post Werbemonitore aufgehängt wurden, die die Gesichter von Kundinnen und Kunden erfassen, sobald sie auf diese Bildschirme blicken. Alter, Geschlecht und andere Merkmale wurden gescannt und ausgewertet.

Wenige Tage nach Bekanntwerden dieses „Marktanalyse-Feldversuchs“ haben wir angekündigt, Strafanzeige zu erstatten und haben damit ein großes Medienecho ausgelöst. Am 27.6.2017, rund 14 Tage später, verkündete Real, mit diesen Scans aufzuhören und die Bildschirme wieder abzubauen. Das ist ein Erfolg – aber die Affäre ist noch nicht vorbei.

Erstens hat bislang nur Real reagiert – wir fordern natürlich die Deutsche Post auf, ebenfalls mit dieser Gesichtserkennung

aufzuhören! Kundinnen und Kunden müssen sich darauf verlassen können, in Ruhe Besorgungen erledigen zu können, ohne dass sie von nahezu unsichtbaren Kameras erfasst, erkannt und analysiert werden.

Zweitens suchen wir nach den Filialen, in denen Bildschirme mit diesen zugeschalteten Kameras hängen. Wir haben einen Aufruf mit Foto auf unserer Webseite veröffentlicht (siehe Bild) und wiederholen das hier im Jahrbuch: Wo hängen Bildschirme, an denen so ein Zusatzgerät angebracht ist?

Innerhalb weniger Tage nach unserem Aufruf im Digitalcourage-Blog haben uns bereits engagierte Menschen Filialen mit aufgerüsteten Bildschirmen von Real genannt. Viele haben uns für unsere Arbeit gelobt und erklärt, dass sie sich beim Kundenservice über die Nutzung von *Überwachungssensorik* beschwert haben. **Das ist einfach toll – so funktioniert Digitalcourage!**

Es ist übrigens auch nicht ausgeschlossen, dass Sie diese Technik irgendwann

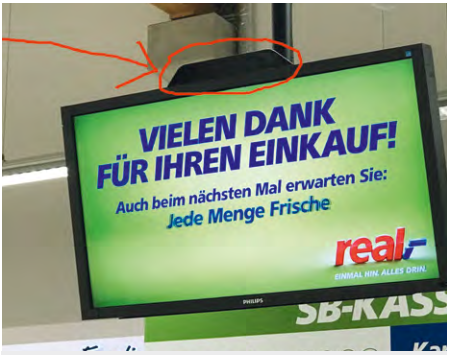


Foto: Digitalcourage cc by-sa 4.0

Gesucht: Wo hängen solche Monitore mit angebautem Gesichtsanalysegerät? Melden Sie sich bitte bei uns, wenn Sie sie entdecken.

an anderen Orten als Real- und Postfilialen entdecken – falls ja, melden Sie sich bitte bei uns (und wir freuen uns besonders über Beweisfotos)!

Und drittens hat die Staatsanwaltschaft Düsseldorf unsere Strafanzeige im Sommer 2017 zwar vorerst zurückgewiesen, aber zur Drucklegung dieses Buches prüfen wir noch, ob wir uns dagegen wehren. Wenn Sie mehr darüber lesen wollen, empfehlen wir Ihnen den Kommentar von Friedemann Ebelt zu Videoüberwachung und Gesichtserkennung weiter hinten in diesem Buch.

Und dann war da noch... unsere Strafanzeige wegen der NSA-Affäre

Seit Februar 2014 liegt unsere Strafanzeige gegen die Bundesregierung und die Geheimdienste, namentlich auch gegen den Innenminister und Kanzlerin Angela Merkel, beim Generalbundesanwalt. Die Strafanzeige haben wir zusammen mit der Internationalen Liga für Menschenrechte (ILMR), dem Chaos Computer Club (CCC) und vier Einzelpersonen eingereicht. Wir erwarten, dass der Generalbundesanwalt prüft, ob die Regierung uns vor dem, was Edward Snowden enthüllt hat, hätte schützen müssen. Im Sommer 2015 bekamen wir ein Antwortschreiben, dass der Generalbundesanwalt gedenkt, dies nicht zu verfolgen, und daraufhin haben wir ihn erneut offiziell juristisch aufgefordert.

Und was ist seitdem passiert?

„Das lässt sich schnell und genau sagen: Nichts. Null-nada-nothing!“ padeluun wird schnell wütend, wenn man ihn darauf anspricht. „Die Generalbundesanwaltschaft verharrt in Schockstarre und hat uns noch nicht einmal ein Aktenzeichen zukommen lassen. An unseren Ausführungen kann es nicht liegen, dass wir so ignoriert werden. Das können alle selbst überprüfen, denn der juristische Schriftsatz ist als Buch bei uns im Shop erhältlich.“

Mehr zum Thema „Fünf Jahre Edward Snowden“ finden Sie auch in unseren BigBrotherAward-Updates weiter hinten in diesem Buch.

Wir unterstützen die Datenschutz-Bewegung

Alleine wird das nichts: Wenn wir *Freiheit* und *Privatsphäre* gestalten und verteidigen wollen, müssen wir gemeinsam anpacken. Darum organisiert Digitalcourage Jahr für Jahr in Berlin, Brüssel, Bielefeld und vielen anderen Städten Treffen für Engagierte und solche, die es werden wollen:
Jährlich im Januar oder Februar treffen sich auf dem **AKtiVCongrEZ** im DGB-Bildungsszentrum in Hattingen viele Aktive, um sich zu vernetzen, gemeinsam Aktionen zu planen und – nicht zuletzt – ein tolles, energetisierendes Wochenende

Matthias Hornung, cc by-sa 4.0

Seit mehreren Jahren ist Digitalcourage Mitveranstalter der Freiheit-statt-Angst-Demos in Berlin.

zu verbringen. Einen gesonderten Artikel über den AKtiVCongrEZ finden Sie weiter hinten in diesem Buch.

Ebenfalls im Februar liegt der **Safer Internet Day**. Anlass für uns, bundesweit Dutzende Lesungen gegen Überwachung auf die Beine zu stellen. Menschen, die sich Überwachung einfach nicht gefallen lassen wollen, lesen in Cafés, Bibliotheken, Büros oder auch zu Hause verschiedenste Texte vor, die im Großen oder Kleinen bewusst machen, wie dringend notwendig unsere Privatsphäre für Demokratie und Rechtsstaat ist. Wie Sie selbst so eine Lesung veranstalten können, erklären wir Ihnen weiter hinten im Abschnitt „Aktivierendes“.

Im April/Mai vergeben wir jedes Jahr unsere **BigBrotherAwards**. Damit platzieren wir die jährlich neu ausgewählten und aktuell recherchierten Datenschutzthemen regelmäßig in den meisten großen deutschsprachigen Medien von Tagesschau bis Tageszeitungen. Die Laudatio-Texte für alle Preisträger aus unserer Preisverleihung 2017 und dazugehörige Updates finden Sie auch in diesem Buch.

Stefanie Loos, cc by-sa 4.0

Nicht vergessen: Wir fordern die Abschaffung der Geheimdienste! Im Oktober 2016 haben wir 1000 Männchen mit Gesichtern und Protestschild vor dem Bundestag aufgestellt. Danke an alle, die mitgemacht haben – wir bleiben dran!

Bundesweit unterstützen oder veranstalten sowohl Digitalcourage als auch andere Organisationen und Privatpersonen zahlreiche **Cryptopartys und Cryptocafés**. Dabei zeigen erfahrene Aktivist.innen, wie sich jede und jeder einfach und praktisch gegen Überwachung im Netz schützen kann. Probieren Sie es bei einer Party in Ihrer Nähe aus – und bringen Sie Ihr eigenes Gerät mit!

Im Sommer suchen Rena Tangens und padeluun eine Woche lang beim **Hattinger Mediensommer** mit Teilnehmer.innen nach Antworten auf die Frage: „Was können wir tun?“

Und im Oktober fahren wir regelmäßig mit einer Delegation nach Brüssel zu **„Freedom not Fear“** – dem europaweiten Treffen für Aktivist.innen und Organisationen aus der Datenschutz-Bewegung. Gemeinsam bilden wir das Gegengewicht zur Datenkonzern-Lobby und diskutieren mit Politiker.innen und Aktiven über unsere Zukunft in der digitalen Welt.

Wir liefern Infrastruktur

Politisches Engagement braucht Privatsphäre. Allumfassende Ausspähung bedeutet auch, dass Aktivistinnen und Aktivisten nur vertraulich kommunizieren und recherchieren können, wenn sie sich schützen. Deshalb betreiben wir einen Tor-Knotenpunkt und einen zensurfreien DNS-Server. Übrigens hat Digitalcourage schon während des Jugoslawienkriegs ein

Mailbox-Netzwerk namens ZaMir (übersetzt: „Für den Frieden“) unterstützt, das der Zivilgesellschaft trotz Blockaden und Embargo ermöglichte, weiter den Kontakt zur Außenwelt zu halten und auch zwischen den verfeindeten Ländern Ex-Jugoslawiens kommunizieren zu können. Heute erleichtern wir mit Tor-Knotenpunkt und DNS-Server vielen Aktiven die Arbeit für Grundrechte und andere politische Anliegen, die Vertraulichkeit brauchen.

Ehrenamt bei Digitalcourage

Was viele nicht wissen: Digitalcourage hat nur ein kleines Büro mit elf Teilzeit-Mitarbeiter.innen. Warum wir trotzdem so viel machen können? Weil es viele großartige Menschen gibt, die ihre Freizeit spenden und sich ehrenamtlich für unsere Grundrechte ins Zeug legen. Unsere Arbeit für Bürgerrechte könnten wir nicht ohne die vielen aktiven Menschen bewältigen: Lektorat, Grafik, Übersetzungen, und, und, und – all das tun viele liebe Leute in ihrer Freizeit, weil sie die gleiche Vision einer lebenswerten Welt im digitalen Zeitalter teilen.

Digitalcourage ist vielleicht auch in Ihrer Nähe! Unsere Zentrale ist in Bielefeld, Ortsgruppen arbeiten aber auch in Berlin, Braunschweig, Bremen und München. Sie streiten auf Demos und mit Aktionen für Grundrechte und organisieren ihre eigenen Lesungen gegen Überwachung.

Wer nicht das Glück hat, eine Digitalcourage-Ortsgruppe in der Stadt zu haben, ist herzlich in unseren Online-Arbeitsgruppen willkommen! Hier wird getextet, fotografiert, recherchiert, administriert, generdet und übersetzt.
Dafür ein ganz großes, herzliches Dankeschön an alle Aktiven!

Haben Sie Lust bekommen? Auf unserer Webseite gibt es unter der Rubrik „Mitmachen“ und „Was kann ich tun?“ ein Formular, mit dem Sie auswählen können, wo Sie sich engagieren möchten. Viele Tipps, wie Sie sich selbst schützen oder in Ihrem Umfeld, z.B. für eine datenschutzfreundliche Stadtverwaltung bei Ihnen vor Ort, engagieren können, finden Sie im Abschnitt „Aktivierendes“ auch in diesem Buch.

Praktikumsstellen bieten wir auch an: Mit technischem oder politischem Schwerpunkt. Ab 2018 ist es übrigens auch möglich, ein **Freiwilliges Soziales Jahr** bei Digitalcourage zu machen. Melden Sie sich gerne bei uns!

Digitale Selbstverteidigung: konkrete Tipps und Tricks

Die „*Digitale Selbstverteidigung*“ ist ein Kern unserer Arbeit geworden. Die Idee: Wenn die Regierung uns nicht mit guten Gesetzen vor Überwachung schützt, müssen wir das selber tun. Auch die Arbeitsgruppe dahinter lebt von der Arbeit vieler Freiwilliger: Sie testen Software, lesen Artikel, bleiben immer auf dem Laufenden. Ihre Tipps gibt‘s auf unserer Website, gedruckt in unserem Onlineshop und ein paar Auszüge auch in diesem Buch im Abschnitt „Aktivierendes“. Jeweils zu Weihnachten verstecken wir außerdem die schönsten davon hinter den 24 Türchen unseres Online-Adventskalenders.

Das neue Bundesdatenschutzgesetz und das „Videoüberwachungsverbesserungsgesetz“

Warum wir dagegen protestiert haben

Von Kerstin Demuth

Stefanie Loos, cc by-sa 4.0

Sarah Bollmann (mit Bauchladen) und Rena Tangens im Gespräch mit Kostantin von Notz (Grüne), Britta Haßelmann (Grüne) und Gerold Reichenbach (SPD), die ihre Mittagspause bei unserer Demo vor dem Bundestag verbracht haben.

Kurz vor der Sommerpause 2017 wurde das Bundesdatenschutzgesetz vom Deutschen Bundestag beschlossen. Zur ersten Lesung im März 2017 haben wir in Berlin vor dem Reichstagsgebäude demonstriert. Ein Bericht von Kerstin Demuth, in unserem Blog veröffentlicht kurz nach unserer Protestaktion.

Der Ausverkauf des Datenschutzes hat begonnen. Deshalb sind wir nach Berlin gefahren: Aktivist.innen von Digitalcourage illustrieren mit Bauchladen, Grundgesetzbüchern und Schildern, wie das Innenministerium unsere Grundrechte verramscht – „Heute 2 zum Preis von 1! Alles muss raus!“ Auch drei Abgeordnete haben ihre Mittagspause gespendet, um sich mit den Protestierenden zu treffen. Im Folgenden die Hintergründe zu den Gesetzesvorhaben, gegen die wir auf die Straße gegangen sind.

Das Videoüberwachungsverbesserungsgesetz – Mitternachtssnack für Datenkraken

„Nicht euer Ernst!“ – das war unser erster Gedanke, als wir erfahren haben, dass das sogenannte Videoüberwachungsverbesserungsgesetz mitten in der Nacht durch den Bundestag gepeitscht werden soll. Um 2:15 geht es in die zweite und dritte Lesung – und wird dann wahrscheinlich von einer Handvoll übermüdeter Abgeordneter verabschiedet. Dazu kommt auch noch der völlig misslungene Entwurf für ein neues Bundesdatenschutzgesetz! Dieser ging heute in die erste Lesung.

Das Videoüberwachungsverbesserungsgesetz soll das Bundesdatenschutzgesetz ändern. Demnach soll in öffentlich zugänglichen Einrichtungen „der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen als ein besonders wichtiges Interesse“ gelten. Bei der Entscheidung für oder gegen Videoüberwachung muss zwar weiterhin die sogenannte Abwägungsentscheidung gefällt werden, ob der daraus gewonnene Nutzen den Verlust an Freiheit rechtfertigt. Doch der oben zitierte Änderungsvorschlag ist eine recht eindeutige Empfehlung: Statt wie bisher zugunsten der Privatsphäre, soll in Zukunft für mehr Überwachung entschieden werden. Ein weiteres Problem ist, dass das Gesetz den Trend fortsetzt, öffentliche Aufgaben in private Hand auszulagern. Denn es soll private Betreiber öffentlich zugänglicher Anlagen zum Filmen motivieren: Besitzer von Einkaufszentren, Restaurants, Flughäfen … All das geschieht unter dem Pseudoargument der Sicherheit.

Datenschutzanpassungsgesetz – oder doch Datenschutzabschaffungsgesetz?

Die Große Koalition gibt sich Mühe, das neue Bundesdatenschutzgesetz noch in dieser Legislaturperiode durch die Parlamente zu jagen. Es enthält einige Regelungen, die klar erkennen lassen: Die Regierung stellt die Interessen der Wirtschaft über die der Bürgerinnen und Bürger.

Eigentlich soll das Gesetz deutsches Recht an das der EU anpassen. Denn im Mai 2018 tritt die neue Datenschutzgrundverordnung (DSGVO) in Kraft. Verordnungen sind unmittelbar gültig. Sie können aber Öffnungsklauseln enthalten, die es den Nationalstaaten gestatten, an manchen Stellen noch nachzuregulieren. Die eigentliche Idee: Ein höheres Datenschutzniveau als die DSGVO vorschreibt soll auch machbar sein. Die Umsetzung der Regierung: Möglichst viele Schlupflöcher für Big-Data-Konzerne rausholen.

So soll nach dem Entwurf des Datenschutzanpassungs- und Umsetzungsgesetzes, der am 1. Februar im Kabinett verabschiedet wurde, beispielsweise das Auskunftsrecht für Betroffene eingeschränkt werden. Die Verpflichtung, dass Personen erfragen können, welche Daten ein Unternehmen oder eine Behörde verarbeitet, gilt nur, wenn das keinen „unverhältnismäßigen Aufwand“ erfordern würde.

Man kann es sich lebhaft vorstellen:

Nutzerin so: **„Hey, Facebook, wollt ihr mir bitte sagen, welche Daten ihr von mir gespeichert habt?“** Facebook so: **„Och, nee, das ist jetzt aber unverhältnismäßig aufwendig. Sorry, geht nicht!“**

Ein weiteres Problem stellt der **Beschäftigtendatenschutz** dar, der durch § 26 des vorgeschlagenen Gesetzes geregelt wird. Die Neuregelungen gehen weit über das bislang geltende Gesetz hinaus. Sie erlauben beispielsweise die Verarbeitung von Beschäftigtendaten für die Erfüllung einer Betriebs- oder Dienstvereinbarung, ohne dass ein Mitbestimmungsrecht zum Datenschutz geschaffen wird. So können zur Beurteilung der Arbeitsunfähigkeit die Gesundheitsdaten von Beschäftigten pauschal durch „ärztliches Personal“ verarbeitet werden.

Auch in anderen Punkten bleibt der Entwurf für ein neues Bundesdatenschutzgesetz weit hinter den Standards des bisherigen zurück. Ein häufig kritisierter Punkt ist der reine Umfang: Die Öffnungsklauseln der DSGVO haben teils sehr strenge Bedingungen. Und es gibt ein Wiederholungsverbot: Was durch die DSGVO geregelt ist, darf nicht inhaltlich oder im Wortlaut in nationalen Gesetzen wiederholt werden.

Alexander Barth, cc by 3.0

Am Dienstag, 9. August 2016, haben Aktivist.innen von „Save the Internet“, Digitalcourage, StopWatchingUs Köln und dem AK Vorrat ein riesiges Paket durch Bonn getragen. Darin waren mehr als 500.000 Eingaben für Netzneutralität und ein faires Internet, die die Bundesnetzagentur entgegengenommen hat.

Die Landesdatenschutzbeauftragte Niedersachsens, Barbara Thiel, hat Zweifel, ob das gegeben ist. In einem Gastbeitrag auf netzpolitik.org schreibt sie: „Aus Sicht der DSK (Datenschützerkonferenz, Anm. d. Red.) zeichnet sich leider auch der aktuelle Entwurf durch eine fehlerhafte Anwendung und Ausfüllung von Öffnungsklauseln aus. Den Erwartungen der DSK wird er allenfalls im Ansatz gerecht. In einigen Punkten ist sogar eine Europarechtswidrigkeit zu befürchten.“ Auch Thiel erhebt den Verdacht, dass das Innenministerium auf diesem Wege versucht, Regelungen durchzudrücken, die auf der europäischen Ebene verhindert wurden.

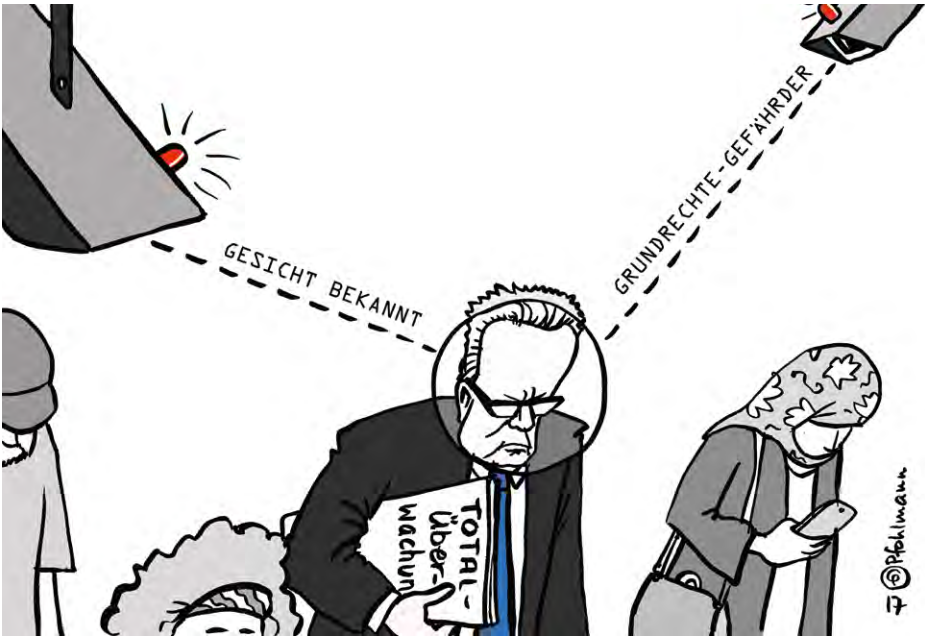
Gesichtserkennung am Berliner Bahnhof Südkreuz

von Claudia Fischer

Am 23. Juni 2017 startete die Bundespolizei am Berliner Bahnhof Südkreuz ein Pilotprojekt zur Gesichtserkennung. Freiwillige wurden mit dem Versprechen auf Warengutscheine angeworben, sich für diesen Feldversuch zu registrieren. Ihnen wurde angekündigt, sie bekämen für diesen Versuch demnächst einen kleinen Transponder in Scheckkartengröße, mit dem registriert würde, wann sie den Bahnhof Südkreuz betreten. Diesen Transponder sollten die Versuchspersonen sechs Monate lang bei sich tragen und damit der Bundespolizei ihre Gesichter zur Erfassung zur Verfügung stellen. Algorithmen würden dann die Gesichter und Bewegungen von Passantinnen und Passanten analysieren und „verdächtige Subjekte“ melden. Die Entscheidungsfähigkeit der Technik sollte getestet werden. Das Projekt sollte im August 2017 beginnen.

Direkt neben dem Infostand der Bundespolizei im Juni haben wir einen Protest-Stand aufgebaut mit der Aktion #Selfie-StattAnalyse:

„Wir rufen alle Menschen dazu auf: Bastelt euch eine Kopfbedeckung oder schminkt



euch so, dass die Überwachungskameras euer Gesicht nicht automatisch auswerten können“, sagte padeluun von Digitalcourage. „Macht ein Foto von eurem Anti-Videoanalyse-Outfit vor einem Bahnhof eurer Wahl und twittert das mit dem Hashtag #SelfieStattAnalyse.“

Wir haben – analog zum Warengutschein der Bundespolizei – ebenfalls kleine „Preise für die Privatsphäre“ aus unserem Digitalcourage-Shop angeboten und padeluun ließ sich die Gelegenheit nicht entgehen, sich offiziell als eine der Testpersonen von der Bundespolizei registrieren zu lassen. Danach behielten wir das Thema weiter im Auge, widmeten uns aber wieder anderen Aufgaben.

Bis an einem Tag im August der besagte Transponder der Polizei bei Testperson padeluun eintraf.
Erwartet hatte padeluun einen RFID-Chip – so war es ihm auch beim Unterschreiben seiner Einverständniserklärung gesagt worden. Was dann aber auf seinem Tisch landete, war ein runder Knopf von der Größe eines Anspitzers oder eines mittleren Pinnwand-Magneten. Und als wir ihn näher untersucht haben, wurde klar: Das ist kein passiv sendender RFID-Transponder, das ist ein kleines, mit Batterie ausgestattetes und aktiv sendendes Überwachungslabor. Temperatur, Neigung und

Datenschutz ist Verbraucherschutz. Machen Sie uns stark!

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

Kreative Tweets mit dem Hashtag #Südkreuz zwitscherten den ganzen Tag durch die Twitter-Welt.

Beschleunigung könnte – wenn sie Funktionen eingeschaltet worden wären – dieser Spionage-Knopf auf 50 Meter Entfernung übermitteln.

Die Testpersonen wurden darüber nicht informiert. Die Testpersonen hatten dem nicht zugestimmt. Die Testpersonen wussten nicht Bescheid. Und das ist illegal.

▶ Also wurden wir wieder aktiv:

Pressemitteilung und Blog-Artikel am Montag, 21.8.17: „Der Test am Bahnhof Südkreuz muss beendet werden!“
Dutzende Presseanfragen und Interviewwünsche erreichten uns am 22. und 23.8.

Am 24.8. hat die Bundesdatenschutzbeauftragte Andrea Voßhoff die Bundespolizei aufgefordert, von den Versuchspersonen „eine erneute datenschutzrechtliche Einwilligung einzuholen, die die Verwendung eines aktiv sendenden Bluetooth-Transponders mit einbezieht. Bis dies

> „Das wäre ein totalitäres Regime, kein Rechtsstaat.“

geschehen ist, sollte das Verfahren mangels Rechtsgrundlage ausgesetzt werden.“ Bundesinnenminister Thomas de Mazière stattete am gleichen Tag dem Bahnhof Südkreuz einen lange geplanten Besuch ab, um sich vor Ort ein Bild von dem Gesichtserkennungs-Versuch zu machen. In einer Pressekonferenz vor Ort warf er Frau Voßhoff Unkenntnis vor (laut Berliner Zeitung) und erteilte den Bedenken der obersten Datenschützerin eine Absage – stattdessen wies er die Bundespolizei an, den Versuch unverändert fortzusetzen.

„Wir wissen nicht, was hinter den Kulissen der Regierung jetzt für ein Streit tobt, weil der Innenminister sich so über Frau Voßhoffs Aufforderung, nachzubessern, hinwegsetzt. Wir wissen aber, dass es einen bundesweiten medialen Aufschrei nach unserer Enthüllung gab und dass viele Menschen mit sehr kreativen Aktionen und Gesichts-Verhüllungsmaßnahmen bei de Mazières Besuch in Berlin protestiert haben“, freut sich Friedemann Ebelt von Digitalcourage, der an dem Tag in Berlin war. „So entwickeln sich unsere Aktionen häufig – planbar ist wenig, Überraschungen haben wir fast jeden Tag. Das Jahrbuch 2018 geht in den nächsten Tagen in Druck. Wer weiß, ob es den Gesichtsanalyse-Test am Bahnhof Südkreuz oder anderswo (noch) gibt, wenn es auf dem Tisch liegt. Wir hoffen nicht.“

„Bei all der Freude über diesen kleinen schnellen Erfolg“, fügt padeluun hinzu, „dürfen wir aber nicht vergessen: Das eigentliche Problem ist nicht die Versuchsphase im Pilotprojekt und die Fehlinformation der Bundespolizei. Das eigentliche Problem ist die Gesichtserkennung. Die Kameras scannen die Gesichter ALLER Personen im Bahnhof Südkreuz, nicht nur die Gesichter derjenigen, die dem Versuch zugestimmt haben. Würden Gesichtserkennungs-Kameras flächendeckend eingesetzt, so wie de Mazière es sich wünscht, wäre quasi so, als würde man von allen Bundesbürgerinnen und Bundesbürgern ununterbrochen Fingerabdrücke nehmen. Das dürfen wir nicht zulassen. Das wäre ein totalitäres Regime, kein Rechtsstaat.“

Erhältlich im Digitalcourage-Shop!

Nicht nur für Kinder:
T-Shirts „Keine Bilder!“

Shirts mit Aufschrift „Keine Bilder! Hiermit widerspreche ich der Aufzeichnung, Speicherung, Ausstrahlung und sonstigen Verwendung meines Bildes. Dieses T-Shirt ist maschinenbedruckt und bedarf daher keiner Unterschrift.“
Größen: S-XXL Preis: 17 Euro
▶ **https://shop.digitalcourage.de**

Sicherheit durch Gesichtserkennung?

Ein gefährliches Versprechen

Von Friedemann Ebelt

Die Flut von allgegenwärtigen Überwachungskameras beschäftigt Digitalcourage schon seit langem. 2017 kam eine neue Dimension hinzu: Die Gesichtserkennung scheint Marktreife erlangt zu haben. Ob im öffentlichen Raum am Berliner Bahnhof Südkreuz, in Real-Supermärkten oder in Postfilialen – wir werden nicht mehr nur gefilmt, sondern erkannt.

So wünscht es sich Bundesinnenminister Thomas de Maizière: Wer einen Bahnhof oder ein Schwimmbad betritt, wird von einer Videokamera erfasst. Sofort tastet ein Algorithmus das Gesicht automatisch ab. Mit einer Datenbank wird im selben Moment abgeglichen, ob das Gesicht dem einer gesuchten Person ähnelt. Wenn ja, schlägt das System Alarm und alles ist gut. Die perfekte Überwachung ist das Ende von Kriminalität? Nein, sie ist ein Albtraum.

Ein gefährliches Versprechen

Politiker erpressen Stimmen im Wahlkampf, indem sie ein verlockendes, aber falsches Versprechen machen: „Ich beschütze euch vor allen Gefahren. Dafür muss ich nur eure Grundrechte und Freiheiten nehmen.“ Die fatale Formel lautet: Überwachung bringt Sicherheit. Allerdings gibt es keine Studie, die belegt, dass Videoüberwachung eine Gesellschaft sicherer macht. Ja, in Einzelfällen kann durch intensive Polizeiarbeit ein schweres Ver-

brechen verhindert werden. Aber dann ist es die Polizeiarbeit, die Sicherheit bringt und nicht die Kamera an der Wand, die täglich zehntausende Gesichter scannt von Menschen, die gerade Zeitung lesen, in der Nase bohren, sich streiten oder küssen.

Ehrlich ist: Kriminalität wird es immer geben

Es ist wichtig, Sicherheit und Überwachung getrennt voneinander zu verstehen. Bei Überwachung geht es um Macht und Kontrolle. Denn Überwachung produziert nur: Überwacher und Überwachte. Sicherheit ist ein anderes Thema. Wenn die Kriminalität von Wenigen politisch dazu genutzt wird, die Grundrechte und Freiheit aller abzuschaffen, dann ist der Rechtsstaat in Gefahr. Ehrlich ist, zu sagen: „Kriminalität wird es immer geben, egal, ob mit oder ohne Überwachung."

London: Überwachung steigt, Verbrechen bleiben

Das belegen Studien und das zeigt auch der Blick nach London. Dort sind Millionen Überwachungskameras installiert. Als Folge verlagern sich Diebstahl und Sachbeschädigung in ärmere Viertel, also dorthin, wo keine Kameras sind. Aber die Delikte bleiben. Vor allem bleiben Gewaltverbrechen. Ein konkretes Problem ist, dass die Hemmschwelle gesunken ist, Menschen Gewalt anzutun. Hier helfen aber nur Sozialarbeit, Einbindung in das kulturelle Leben, psychologische Betreuung und Polizeiarbeit, nicht Überwachung. Kein Überwachungssystem der Welt kann Verbrechen jemals beenden, weil es selbst ein Verbrechen ist. Videoüberwachung wird noch nicht einmal Gewalttaten signifikant reduzieren, das belegen Studien. Wenn Täter.innen im Affekt handeln, ignorieren sie Kameras. Wer kaltblütig einen Mord plant, bereitet sich auch auf die Videoüberwachung vor und verkleidet sich so, dass der Algorithmus nichts erkennt.

Südkreuz: Ein Schritt weiter Richtung Überwachungsstaat

Der Innenminister will jedes Gesicht kennen, auch wenn dafür die Rechtsgrundlage fehlt. Er arbeitet an einem System der kompletten Überwachung. Das Überwachungsprojekt am Südkreuz ist ein Schritt auf diesen Abgrund zu. Monate zuvor haben SPD und CDU beschlossen, dass Behörden automatisch auf die biometrischen Fotos aller Personalausweise zugreifen dürfen. Die Büchse der Pandora wird Zentimeter für Zentimeter aufgehebelt.

Ende 2017, so wurde es auf der Sicherheitskonferenz in München in einem Nebenraum mitgeteilt, soll die Gesichtserkennung auf möglichst viele Kameras ausgeweitet worden sein. Auch wenn der Termin nicht eingehalten werden kann: Das muss verhindert werden!

Das Digitalcourage-Team

Portraits

Von Claudia Fischer

In jedem Jahrbuch stellen wir drei Mitglieder, Aktive oder Beschäftigte von Digitalcourage vor. Was sind das eigentlich für Leute, die für eine lebenswerte Welt im digitalen Zeitalter eintreten? Alles Technik-Freaks? Oder Studis mit viel Zeit, sich zu engagieren? Alle unter 20? Mitnichten! Lesen Sie selbst!

Zwischen Buchhaltung und Werkzeugkasten

Nils Büschke

2017 war ein entscheidendes Jahr für Nils Büschke. Als Veranstaltungskaufmann waren die BigBrotherAwards am 5. Mai für ihn – wie für die gesamte Crew – das zentrale Event im Jahr. Nur, dass er da noch gar kein Veranstaltungskaufmann war. Vier Tage nach der BBA-Gala, am 9. und 10. Mai, hatte er nämlich seine schriftliche Abschlussprüfung. Beides quasi gleichzeitig zu stemmen, war vielleicht die eigentliche Leistung und damit ein würdiger Abschluss seiner Ausbildung. „Es ging irgendwie. Ich habe da natürlich auch gemerkt, dass ich schon 31 bin. Die Prüfung war anspruchsvoll, aber schaffbar.“ Herzlichen Glückwunsch!

Nils war der erste Auszubildende bei Digitalcourage. Mit Büroleiterin Sylke Kahrau hat er sich auch in der heißen Phase der BigBrotherAwards regelmäßig zurück gezogen und gelernt. „Aber das kennen wir ja nicht anders – in unserem Großraumbüro ist immer viel los und alle 5 Minuten steht jemand neben einem und fragt irgendwas. Da lernt man mit umzugehen.“

Genau dieser Trubel ist es nämlich auch, den Nils besonders mag. Den Überblick behalten, Prioritäten setzen, mal politisch nachdenken, Kisten schleppen oder Demo-Plakate tackern. „Als Veranstaltungskaufmann würde ich immer nur bei politischen Initiativen arbeiten wollen. Weil ich da weiß, wofür ich’s tue. Mir den Veranstaltungsorgastress zu geben für irgendein Privatunternehmen, Messestände aufbauen oder am Wochenende mit irgendwelchen Schlagersängern durch Deutschland touren, nee, dann würde ich lieber was anderes machen.“ Erzieher vielleicht. Schlagzeugspielen soll Hobby bleiben.

Mit 30 Stunden ist er bei Digitalcourage jetzt fest angestellt, unbefristet. Nach einem Praktikum 2011 hat er seine Talente entdeckt: Er bewahrt Ruhe auch im Sturm, behält den Überblick über fast alles, was in den Vereinsräumen in Bielefeld gerade passiert, welcher Karton mit Flyern wo abgestellt wurde, wer welche Aufgabe übernommen hat, auch vor Monaten. Körperlich geht er ohne zu zögern an seine Grenzen. So wie damals, als er mit zwei anderen Vereinsmitgliedern spontan in Nürnberg einen Stand auf einer IT-Security-Messe gemacht hat. „Dafür bin

Digitalcourage, cc by-sa 4.0

Wirklich versinken kann er auch bei Lärm und Unruhe in die Buchhaltung von Digitalcourage. Auch diese Leidenschaft hat er während der Ausbildung entdeckt: „Buchhaltung ist cool. Das sind Zahlen, das ist eindeutig, und das ist irgendwann fertig. Dann ist alles kontiert, sortiert und abrufbar, so dass andere damit weiter arbeiten können. Sehr befriedigend!“ Und das meint er ernst, auch wenn er – so wie immer eigentlich – dabei lacht.

▶„Als Veranstaltungskaufmann würde ich immer nur bei politischen Initiativen arbeiten wollen.“◀

ich mit dem Transporter von Bielefeld nach Berlin, habe unsere neue Datenkrake abgeholt, bin von da nach Nürnberg gefahren, war 3-4 Tage auf der Messe und nett untergebracht bei Freunden von Digitalcourage-Mitglied Hartmut. Dann kurz nach Bielefeld und direkt wieder zurück nach Berlin zur Großdemo. Das war eine tolle Kombination.“

Fragt man ihn nach seiner schönsten Veranstaltung mit Digitalcourage, kann er sich nicht entscheiden. „Eigentlich ist es eine Kombination: ‚Die Congresse‘ (Kurzform für die Chaos-Communications-Congresse des Chaos Computer Clubs, jedes Jahr zwischen Weihnachten und Silvester) sind immer toll. Und der Kirchentag 2015, das war auch

Foto: Sylke Kahrau, cc by-sa 4.0

Nils Büschke an seinem ersten Schultag als Azubi bei Digitalcourage

super. Das hat mich echt beeindruckt, was für ein kritisches, offenes Publikum wir dort getroffen haben. Den Unterschied zu sehen, war besonders spannend: Du hast auf ‚dem Congress' lauter Leute, die tierisch tief im Thema Computer und Datenschutz stecken, aber häufig nicht so das politische Bewusstsein haben. Während Du auf dem Kirchentag jede Menge Leute hattest, die keine Ahnung von Digitalisierung haben, aber mit einem super-kritischen Bewusstsein gekommen sind. Das war echt toll, da Gespräche zu führen und spontane Aktionen – wie den Kirchentagsbeschluß gegen Vorratsdatenspeicherung – zu planen und umzusetzen!"

Und beginnt jetzt für ihn eine neue Lebensphase? Nicht mehr Azubi, sondern Mitarbeiter auf Augenhöhe sein bei Digitalcourage? „So ein Quatsch", schnaubt er bei dieser Frage. „Ich habe mich nie als Azubi gefühlt." Aber irgendwas muss doch jetzt, mit der Prüfung in der Tasche, anders werden? „Irgendwie nicht", grübelt er. „Ist alles okay so, wie es ist. Außer vielleicht, dass wir weniger Themen gebrauchen könnten. Aber das ist unsere Realität: Die Digitalisierung durchdringt nun mal alle unsere Lebensbereiche, dementsprechend hoch ist die Vielfalt an Themen und Katastrophengebieten. Da fällt es uns schwer, uns auf einzelne Dinge zu fokussieren und uns nicht in Dutzenden Projekten zu verstrampeln, die aber eben alle gleich wichtig sind. Eigentlich wissen wir das ja auch, aber wir kriegen es noch nicht wirklich umgesetzt. Das wäre definitiv was, was wir besser machen können, auf jeden Fall. Andererseits ist es aber auch genau die Breite an Themen, die die Arbeit bei Digitalcourage für mich so spannend macht."

Wenn sich der Raum bewegt

Angelika Höger

„Manchmal macht Digitalcourage inzwischen den Eindruck einer Firma, wenn man in das Büro in der Markstraße kommt. Immer wieder andere Leute, viele Praktikant.innen, alle sind konzentriert – aber irgendwie ist da eine Struktur geschaffen worden, aus der man bereichert wieder raus geht und Anregungen mitnimmt."

Justus Holzberger, cc by-sa 4.0

Die Bielefelder Künstlerin Angelika Höger gestaltet für Digitalcourage jedes Jahr die Rauminstallationen bei den BigBrotherAward-Galas.

Angelika Höger geht schon seit vielen Jahren im Digitalcourage-Büro ein und aus und hat diese Entwicklung miterlebt. „Als ich 2000 das erste Mal dort war, haben wir noch alleine mit padeluun im Büro gesessen. Damals hatten sie gerade die „Privacy Card“ entwickelt, das fand ich ein tolles Projekt.“

„Das war einfach eine geniale Idee! Gute Kunst entsteht oft so“

Die Privacy-Card funktionierte an der Supermarkt-Kasse genau wie eine Payback-Karte und die gesammelten Punkte wurden Digitalcourage, damals FoeBuD e.V., gutgeschrieben. Das war eine Form, gemeinsam Spenden zu sammeln, ohne dass die Spender.innen ihre privaten Einkaufsprofile preis geben mussten. Inzwischen funktioniert diese Karte nicht mehr.

„Payback-Karten waren etwas, über das wir uns geärgert haben – und dieses Ärgernis wurde umgedreht, indem man die Technik nutzt und für einen guten Zweck verwendet. Aus passiven Kunden, die ausgeforscht werden, wurden damit aktiv Handelnde. Das war einfach eine geniale Idee! Gute Kunst entsteht oft so“, sagt Angelika Höger. „Und außerdem hat der FoeBuD hat schon sehr früh den Wert von Privatsphäre erkannt – noch vor der allumfassenden Digitalisierung. 2000 hatten wir ja noch keine Smartphones, kein Facebook, es hatte nicht mal jeder E-Mail.“

Privatsphäre? Angelika lebt im Künstler.innenprojekt „Artists Unlimited“ in Biele-

Claudia Fischer, cc by-sa 4.0

Die neonfarbenen Gebilde von Angelika Höger bestehen aus Strohhalmen, die auf Fäden und Fiberglasstäbe aufgezogen sind. Sie reagieren auf Luftbewegungen und ergänzen die Stahl- und Betonkonstruktionsteile des Raumes. Das blaue Licht lässt sie aussehen, als würden sie von innen leuchten.

feld – einer Hausgemeinschaft mit über 30 Menschen, die alle künstlerisch tätig sind. „Das geht nur mit viel gegenseitigem Respekt. Es gibt natürlich gemeinsame Vereinbarungen und es ist sehr wichtig, sich aktiv für gemeinsame Projekte einzusetzen, aber es muss eben auch Verständnis dafür geben, dass man auch Zeit und Raum für sich und seine eigenen Ideen hat. Dafür brauche ich keine geschlossenen Türen, sondern nur den Respekt der anderen, dann geht das ganz gut."

Für Digitalcourage gestaltet sie schon seit mehreren Jahren den Veranstaltungsraum für die BigBrotherAwards. „In der Hechelei, in der wir mit den Awards ja ein paar Jahre lang waren, habe ich die Verstrebungen und Vernetzungen der Industriekultur-Säulen aufgegriffen. Meine Strohhalm-Gebilde sollten Dynamik dort hineinbringen, sich selbst bewegen und ein Eigenleben führen." Sich bewegende dreidimensionale Räume gestaltet Angelika Höger am liebsten. „Ich denke nicht gerne linear oder wie beim Texte-Schreiben, einen Satz hinter dem anderen." Auch wenn sie das Schaufenster von Digitalcourage in der Bielefelder Marktstraße gestaltet, nutzt die die Tiefe des Raumes gerne aus.

„Manchmal kann ich frei gestalten, dann fallen mir Dinge ein, die vielleicht nur mit etwas Phantasie mit Digitalcourage assoziiert werden können." Und manchmal bekommt sie einen konkreten Anruf aus dem Büro. „Kannst Du uns für diese oder jene Kampagne ein Schaufenster gestalten?"

„Dann fühle ich mich eher als Dienstleisterin, was auch mal eine spannende Aufgabe ist, das mache ich sonst nicht so oft", lacht sie. Digitalcourage ist nur eines ihrer Projekte – neben eigenen Einzel- oder Dialogausstellungen mit anderen Künstler.innen arbeitet sie auch im Kunstmuseum Marta Herford und gibt künstlerische Workshops.

Auf 2018 ist sie schon sehr gespannt: „Dann sind wir mit den BigBrotherAwards zum ersten Mal im Bielefelder Stadttheater. Da geht die Veranstaltung – auch bei der Bühnengestaltung – wieder in eine andere Dimension."

Rahmenbau in Bremen

Justus Holzberger

„Im Nachgang merke ich, dass da so viele Punkte zusammen kamen, die schon immer Interessensgebiete von mir waren, die ich aber nicht so verknüpft gesehen habe. Sich mit freier Software auseinandersetzen und das als größere politische Bewegung begreifen zum Beispiel, das war für mich ein Push bei Digitalcourage“, sagt Justus Holzberger über sein Praktikum bei uns 2015. Computer haben ihn schon seit der Schulzeit interessiert. Auf freie Software war er auch schon gestoßen und während seines Soziologie-Studiums an der Uni Bremen beschäftigte er sich mit Feminismus. In Bielefeld brachte er alles unter einen Hut.„Im Studium machen wir ein Pflichtpraktikum, und irgendwie war ich auf der Website von Digitalcourage. Da stand, dass sie gerade Praktikanten suchen. Ich bin dann nach Bielefeld gefahren und es hat gleich gepasst. Gerade auch meine künstlerische Ader wurde gebraucht.“ Justus fotografiert seit etwa zehn Jahren leidenschaftlich gerne und gehört inzwischen fest zur Foto-AG von Digitalcourage. Um die BigBrotherAwards zu dokumentieren, reist er regelmäßig wieder nach Bielefeld. Auch wenn kreative Bildideen für die Webseite gebraucht werden, bietet er gerne seine Bilder für den Pool an – selbstverständlich unter Creative Commons-Lizenzen. Davon hat auch dieses Jahrbuch profitiert – viele Fotos sind von Justus.„Auf dem AKtiVCongrEZ 2017 habe ich Maike aus Bremen kennen gelernt und wir hatten die Idee, eine Ortsgruppe von Digitalcourage zu gründen. Als wir mit Sarah aus dem Büro in Bielefeld gesprochen haben, hat sie angeboten, den 350 eingetragenen Fördermitglie-

Foto: padeluun, cc by-sa 4.0

dern oder Unterstützer.innen aus Bremen eine Mail zu schicken. Ich war echt platt. So viele Menschen aus Bremen? Damit hatte ich nicht gerechnet!“ Mehrere Rundmails später hatten sich etwa 20 Leute gefunden, die sich jetzt ein Mal monatlich jeden zweiten Dienstag im „Ausspann“, mitten im Bremer Altstadt-Viertel „Schnoor“ treffen.

▶„Digitalisierung ist kein Extra-Lebensbereich.“◀

„Wir finden gerade noch unseren gemeinsamen Schwerpunkt und Konsens als Ortsgruppe. Besonders viele haben aber schon ihr Interesse an der Digitalcourage AG Pädagogik geäußert. Bildung und Digitalisierung sind große Themen, die aber oft nicht mit dem Schwerpunkt vermittelt werden, den Digitalcourage hat. Dazu wollen wir hier Info-Abende und Fortbildungen anbieten“, sagt Justus. Damit verbindet er ein größeres Anliegen: Den Rahmenbau – das künstlerische Konzept, das Rena Tangens und padeluun schon seit den 1980er Jahren verfolgen. Es geht darum, die Umgebungen und Voraussetzungen zu schaffen, damit inhaltliche Arbeit gut gelingen kann und damit Menschen sich aktiv einbringen können.

Foto: Justus Holzberger, cc by-sa 4.0

Presseschau am Morgen nach den BigBrotherAwards. So analog kann Digitalcourage sein.

„Hier in Bremen sind viele kleine engagierte Gruppen, die für ihre Ziele einzeln vor sich hin arbeiten, aber „gefühlt“ mehr gemeinsam machen könnten. Ich finde es total wichtig, denen zu sagen: Digitalisierung ist kein Extra-Lebensbereich, den man beliebig an- und ausknipsen kann. Nein, der betrifft Menschen auf der Arbeit und zu Hause, in der Freizeit und bei politischer Aktivität. Da kann man sich einfach nicht rausnehmen. Deshalb möchte ich sagen: Ihr könnt weiter so aktiv sein wie bisher, aber es ist gut, einen Raum zu haben oder Ansprechpersonen, bei denen man weiß, die setzen sich mit dem Thema auseinander und die kann man dazu fragen. Und zu diesen Themen können wir auch zusammen etwas erarbeiten oder Aktionen machen. Das wäre gut für Bremen.“

Foto: Justus Holzberger, cc by-sa 4.0

Einen Beamer mit bunten Bildern auf zwei Alu-Mülleimer strahlen zu lassen...

Das Auge arbeitet mit

Justus Holzberger: „Auf dem AKtiVCongrEZ kam ich abends in den großen Konferenzraum und dort wurde an verschiedenen Tischen gearbeitet, geredet, musiziert. Alles war unglaublich nett beleuchtet und ich fragte mich, woher – bis mir diese Konstruktion auffiel. Aus dem schnöden Konferenzraum wurden einfach zwei verchromte Mülleimer oder Schirmständer entwendet und als Discokugeln auf irgendeine Konstruktion mit dem Garderobenständer vor den Beamer gestellt. Eine Musikvisualisierung sorgte dann über den Beamer für den Lichtzauber. Hacking, Rahmenbau, Kreatives, Fürsorge füreinander… da kommt für mich ganz viel zusammen.“

... hat einen enormen Effekt auf die Arbeitsatmosphäre.

Foto: padeluun, cc by-sa 4.0

Unsere Überwachungs-gesamtrechnung

Warum die Vorratsdatenspeicherung verfassungswidrig ist

Markus Winkler, cc by-sa 2.0

Die Vorratsdatenspeicherung ist mit Art 10 Grundgesetz (Post- und Fernmeldegeheimnis) „schlechthin nicht vereinbar“ sagt das Bundesverfassungsgericht.

Diesen Artikel haben wir für unsere Verfassungsbeschwerde gegen die Vorratsdatenspeicherung zusammengestellt. Er steht für alle nutzbar auf unserer Webseite und ist dort mit Dutzenden Links zu Studien und Originaltexten versehen. Dort addieren wir auch verabschiedete Gesetze und neue Erkenntnisse laufend hinzu. In diesem Jahrbuch lesen Sie „nur“ unsere grundsätzlichen Gedanken als Einführung ins Thema – wenn Sie ins Detail gehen wollen, schauen Sie bitte online nach.

Im Jahr 2010 urteilte das Bundesverfassungsgericht (BVerfG), eine Vorratsdatenspeicherung sei „mit Art. 10 GG nicht schlechthin unvereinbar“. Voraussetzung sei es jedoch, dass sie legitimen Zwecken diene und in ihrer Ausgestaltung „dem besonderen Gewicht des hierin liegenden Eingriffs hinreichend Rechnung trägt“ (BVerfG, NJW 2010, 833 Rdnrn. 205f., 213).

Die Notwendigkeit, alle staatlichen Überwachungsmöglichkeiten auf ein Maß zu beschränken, bei dem die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert wird, zählt sogar zur, europarechtsfesten, verfassungsrechtlichen Identität der Bundesrepublik Deutschland'. (Rossnagel, NJW 2010, Heft 18)

Was ist der „Chilling Effect"?

In seinem Grundsatzurteil von 1983 begründete das Bundesverfassungsgericht das Recht auf Informationelle Selbstbestimmung mit der Gefahr einer Selbstzensur, die ausgelöst wird durch die Verunsicherung, welche Daten erfasst würden – dem sogenannten „Chilling Effect". Die Menschen dürften sich nicht totalüberwacht fühlen, denn: „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen."

Gefahr einer Selbstzensur

Was ist eine Überwachungsgesamtrechnung?

Aus dem Urteil von 2010, das die Vorratsdatenspeicherung kippte, erwuchs der Begriff der „Überwachungsgesamtrechnung", der einer Weisung des Bundesverfassungsgerichtes einen Namen gibt: Alle staatlichen Maßnahmen zur Überwachung dürfen nicht ausschließlich einzeln für sich bewertet werden, sondern müssen unbedingt in ihrer Gesamtsumme betrachtet werden. Denn in ihrer Summe dürfen sie nicht das für eine Demokratie erträgliche Maß an Überwachung überschreiten.

Das heißt im Klartext: Für sich gesehen *könnte* (auch wenn wir das anders sehen) eine Vorratsdatenspeicherung bei richtiger Umsetzung verfassungsgemäß sein. Das gilt allerdings nur dann, wenn es nicht bereits zu viele andere Überwachungsmaßnahmen gibt, die in ihrer Gesamtheit das Gefühl der ständigen Überwachung auslösen.

Das war 2010. Nun wissen wir seit Edward Snowdens Enthüllungen vor 5 Jahren (2013), dass die tatsächliche Überwachungssituation weitaus umfangreicher ist als bis dahin angenommen. Und da seitdem weitere Überwachungsgesetze erlassen wurden, handelt es sich bei der Vorratsdatenspeicherung aus unserer Sicht – juristisch gesprochen– um einen additiven Grundrechtseingriff.

Überwachungsmaßnahmen durch den Staat

Konkret wird es schwierig, eine Überwachungsgesamtrechnung tatsächlich durchzuführen. Wir können nur die staatlichen Überwachungsmaßnahmen auflisten, die wir kennen, und auf das Schutzversagen des Staates verweisen. Wir beschränken uns für dieses Jahrbuch auf die Gesetze von 2016 und 2017 – und wir weisen darauf hin, dass wir Gesetze, die für einzelne Bundesländer beschlossen wurden, nicht vollständig im Blick haben können.

Neue staatliche Überwachungsmaßnahmen (Bund) 2016/2017:

§ Gesetz zur Verbesserung der Registrierung und des Datenaustausches zu aufenthalts- und asylrechtlichen Zwecken (2. Februar 2016)
§ Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts (17. Februar 2016)
§ Gesetz zur Änderung des Hochschulstatistikgesetzes (2. März 2016)
§ Gesetz zur Einführung beschleunigter Asylverfahren (11. März 2016)
§ Anti-Terror-Paket (24. Juni 2016)
§ Vorratsdatenspeicherung (beschlossen, noch nicht angewendet)
§ Gesetz zur Regulierung des Prostitutionsgewerbes sowie zum Schutz von in der Prostitution tätigen Personen (21. Oktober 2016)
§ Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes – „BND-Gesetz", Plenarsitzung ansehen (4. November 2016)
§ Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) (24. Februar 2017)
▶ Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) wird ins Leben gerufen (März 2017)
§ Gesetz über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz – FlugDaG) (13. März 2017)
§ Gesetz zur Änderung des Strafgesetzbuches – Ausweitung des Maßregelrechts bei extremistischen Straftätern (20. März 2017)
§ Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (30. März 2017)
▶ „Kommando Cyber- und Informationsraum" (KdoCIR) in Dienst gestellt (05. April 2017)
§ Gesetz zur Änderung des Bundesdatenschutzgesetzes – Erhöhung der Sicherheit in öffentlich zugänglichen großflächigen Anlagen und im öffentlichen Personenverkehr durch optisch-elektronische Einrichtungen (Videoüberwachungsverbesserungsgesetz) (28. April 2017)
§ Gesetz zur Verbesserung der Fahndung bei besonderen Gefahrenlagen und zum Schutz von Beamtinnen und Beamten der Bundespolizei durch den Einsatz von mobiler Videotechnik (05. Mai 2017)
§ Gesetz zur Änderung des Strafgesetzbuches – Wohnungseinbruchdiebstahl (16. Mai 2017)
§ Gesetz zur Förderung des elektronischen Identitätsnachweises (17. Mai 2017)
§ Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes (01. Juni 2017)

Online-Durchsuchung

Das Bundeskriminalamt kann mit Hilfe staatlicher Schadsoftware (einem sogenannten **„Staatstrojaner“**) Online-Durchsuchungen durchführen sowie Internettelefonie (beispielsweise über Skype oder andere Messenger-Dienste) abhören. Informationen zu unserer Verfassungsbeschwerde gegen den „Staatstrojaner“ finden Sie im Kapitel „Was uns bewegt“.

Telekommunikationsdaten

Telekommunikationsanbieter erfassen bereits vor der Einführung der Vorratsdatenspeicherung neben den Bestandsdaten eindeutige Geräteidentifikationen ihrer Kundinnen und Kunden, *Verkehrsdaten* sowie *Standortdaten*. Folglich wird erfasst, wer wo mit wem wie lange über Festnetz, Handy oder Smartphone telefoniert sowie SMS versendet und empfangen hat. Ermittlungsbehörden können diese Informationen mittels **Funkzellenabfragen** in Erfahrung bringen.

Die Anzahl der Funkzellenabfragen steigt stetig. Die Zahlen für September und Oktober 2015 zeigen, dass in Berlin die Funkzellenabfrage unverhältnismäßig und entgegen geltender Beschlüsse des Abgeordnetenhauses eingesetzt worden ist. So waren allein durch eine Maßnahme im Postleitzahlenbereich 12 über 1,4 Millionen Mobilfunkanschlüsse betroffen.“ (Christopher Lauer)

Von Funkzellenabfragen sind täglich zehntausende Menschen betroffen. Die Polizei verfügt in der Folge über alle in den Zellen angefallenen Kommunikationsdaten. Laut Gesetz müssen die Betroffenen darüber informiert werden (§101 StPO). Praktisch erfolgen solche Benachrichtigungen jedoch nur äußerst selten, denn:

Claudia Fischer, cc by-sa 4.0

Sieht harmlos aus, hat es aber in sich!

„Die Benachrichtigung einer […] Person, gegen die sich die Maßnahme nicht gerichtet hat, [kann] unterbleiben, wenn diese von der Maßnahme nur unerheblich betroffen wurde und anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung hat.“ (§101 StPO)

Demnach entscheidet der zuständige Staatsanwalt, ob es in Ihrem Interesse liegt, über eine Überwachung Ihrer Kommunikation informiert zu werden.

Das Telekommunikationsgesetz beinhaltet außerdem das staatliche Instrument der **Bestandsdatenauskunft**, die sowohl manuell als auch automatisch erfolgen kann.

Foto: Carolin Hinz, cc by-sa 2.0

Noch Fragen?

Trotz einer Entschärfung im Jahr 2013 gilt bei der Erfassung: Die Polizei sowie Geheimdienste dürfen persönliche Informationen von Mobiltelefonbesitzern und Internetnutzern abrufen, und zwar automatisiert und ohne größere rechtliche Hürden.

Überwachung von Postsendungen

Von einer **verdachtsunabhängigen Speicherung der Adressdaten** sind auch alle Sendungen der Deutschen Post betroffen. Die Zusammenarbeit mit Sicherheitsbehörden soll sich angeblich *nur* auf Sendungen in die USA beschränken. Mit Hilfe der massenhaften Datenüberwachung will man beispielsweise die Zollabfertigung vereinfachen, so heißt es. In Deutschland werde zwar jede Adresse abfotografiert, aber nur für interne Zwecke wie den korrekten Briefversand, teilte die Deutsche Post mit. Unbefriedigenderweise ist nicht bekannt, wie lange eine Speicherung der Adressen erfolgt.

Finanzdaten

Mithilfe von Metadaten, welche auch aus Finanzdaten gewonnen werden, können Beziehungsgeflechte unter Personen, Organisationen oder Ereignissen nachvollzogen werden. Durch das Gesetz zur Förderung der Steuerehrlichkeit haben Finanzbehörden und bestimmte andere Behörden die Möglichkeit, Bestandsdaten zu Konto- und Depotverbindungen bei den Kreditinstituten über das Bundeszentralamt für Steuern abzurufen. Eine übergreifende Politik für Finanzkriminalität und Finanzermittlungen wird seitens der Europäischen Kommission und Europol bereits seit mehreren Jahren forciert. Das Ausmaß der **Kontenabfragen** nimmt konstant zu. Im Jahr 2010 gab es bundesweit 105.615 Abfragen; im Jahr 2014 waren es bereits 131.753. Ursache ist insbesondere die deutlich gestiegene Zahl der Auskunftsersuchen von Polizeibehörden.

Finanzermittlungen länderübergreifend

Inzwischen sind alle „Financial Intelligence Units“ der Mitgliedsstaaten der Europäischen Union miteinander verbunden. Auf diesem Wege ermöglicht Europol eine europaweite und unverzügliche Verfolgung auffälliger Transaktionen. Um ausreichend Kapazitäten für die Speicherung zur Verfügung zu haben, sind Finanzämter, Polizei und Zollbehörden der EU-Mitgliedsstaaten dazu angehalten, ihre Daten an Europol und Eurojust weiterzureichen. Hierdurch könnten wiederum in Deutschland nicht zulässige Analyseverfahren auf die

betreffenden Daten durch Europol angewandt werden. Europol hat eine Software für das Data Mining programmiert, die in Fachkreisen auch „Al-Capone-Methode“ genannt wird. Mit dieser inzwischen computergestützten Analyse werden nicht nur Finanzströmungen abgeglichen; es handelt sich um eine europaweite Rasterfahndung in den jeweils vorhandenen Vorratsdaten. Kritisch ist vor allem, dass die Datenschutzrichtlinien einzelner Staaten über- beziehungsweise umgangen werden.

Zugriff auf die Daten aller Finanztransaktion der europäischen Bürgerinnen und Bürger erhielten auch die USA, nachdem sie ein Abkommen mit der Europäischen Union aushandelten. Das sogenannte **SWIFT**-Abkommen (BigBrother-Award 2006, seit 01. August 2010 in Kraft) ermöglicht den US-amerikanischen Behörden nun nach Genehmigung durch Europol einen ungehinderten Zugriff auf die Daten der Society for Worldwide Interbank Financial Telecommunication (SWIFT), die den europäischen Zahlungsverkehr überwacht. Darüber hinaus legitimiert das Abkommen eine anschließende Speicherung (bis zu 5 Jahren) sowie die Weitergabe der Daten.

Wohnraumüberwachung

Die akustische Wohnraumüberwachung wurde durch das Einfügen der Absätze 3 und 6 des Artikel 13 Grundgesetz im Jahr 1998 ermöglicht. Im Jahr 2004 erklärte das Bundesverfassungsgericht den **„Großen Lauschangriff“** für teilweise verfassungswidrig, woraufhin eine Gesetzesanpassung im Jahr 2005 folgte. Das Gesetz enthält jedoch kein absolutes Überwachungsverbot für Gespräche im privaten Bereich; es regelt lediglich allgemeine Eingriffsbefugnisse und nennt die Bedingungen, wann abgehört werden darf. Aber auch vergleichsweise „kleine Andwendungen“ wie **Smart Meter** gehören zum Bereich der Wohnraumüberwachung. Sie

Foto: Panthermedia

Wussten Sie, dass auch Ihr „smarter” Fernseher eine Kamera und ein Mikrofon enthalten kann? Und per Internetverbindung andere an seinem Wissen über Sie teilhaben lässt?

Dieses Foto haben wir vor 15 Jahren auf der CeBit gemacht. Schon damals wurden Gesichter erkannt und Emotionen interpretiert.

können häufiger und vor allem in kürzeren Intervallen als herkömmliche Zähler Daten zum Energieverbrauch abfragen und aufzeichnen. Die Verbrauchsdaten lassen viele Rückschlüsse auf den Tages- und sogar den Lebensablauf des Kunden zu. Bei einer sehr feinen Abfrage dieser Daten können Verbrauchsprofile und Analysen des Verhaltens von Menschen in den eigenen vier Wänden erstellt werden, die auf vielfache Weise missbraucht werden können. Ferner sind moderne Rauchmelder in der Lage, mittels Funk und Ultraschall ihr Umfeld zu überwachen, sogar Gespräche aufzuzeichnen. Eine gesetzlich verpflichtende Installation von Rauchmeldern ist aus diesem Grund äußerst kritisch.

▶Videoüberwachung

Über 500.000 Kameras überwachen in Deutschland die Umgebung – neben der Quantität steigt auch die Qualität der Überwachungsaufnahmen. Gleichzeitig ist immer weniger Kameras anzusehen, in welche Richtung sie ausgerichtet sind und mit welcher Auflösung sie filmen. Besonders erschreckend: Ein Großteil der Installationen im öffentlichen Raum verstößt gegen geltende Datenschutzbestimmungen. So wurde beispielsweise in Niedersachen im Jahr 2010 festgestellt, dass zu diesem Zeitpunkt nur 23 von 3345 Kameras korrekt angebracht und betrieben wurden. Mal fehlten Hinweisschilder auf die Videoüberwachung, mal wurde das aufgezeichnete Material über Monate nicht gelöscht, dann wieder wurde ohne Scheu in Wohnungen, Arztpraxen oder Anwaltsbüros hinein gefilmt – technisch so hochwertig,

dass die abgelichteten Personen und ihre Handlungen detailliert erkennbar waren. Am Berliner Bahnhof Südkreuz werden seit Mai 2017 sogar von der Bundespolizei – ohne Rechtsgrundlage – Kameras mit Gesichtserkennung und Verhaltenserkennung getestet. (Dazu gibt es ein Extra-Kapitel in diesem Buch.)

Reisedaten

Bereits im Anti-Terror-Gesetz war eine schärfere Überwachung des Flugverkehrs beschlossen worden – Dann verabschiedete das EU-Parlament am 14. April 2016 eine neue EU-Richtlinie zur Vorratsdatenspeicherung von Passagierdaten (passenger name records, kurz: PNR). In Zukunft sind alle Mitgliedsstaaten der EU dazu verpflichtet, Fluggastdaten und Schiffspassagierlisten von allen Reisen aus der EU und in die EU zu speichern. Pro Fahrgast fallen bis zu 60 Daten an, die jeweils fünf Jahre zentral gespeichert werden. Nachdem der Europäische Gerichtshof am 26.7.2017 das geplante Abkommen mit Kanada gekippt hat, werden die Abkommen neu verhandelt werden müssen.

Krankendaten

Gesundheitsdaten sind sehr sensibel. Darum muss das, was gespeichert werden *muss*, zwingend besonders gut geschützt werden. Auch Abwesenheits- und Fehlzeiten von Mitarbeitenden werden durch Arbeitgeber gespeichert. Jedoch dürfen Arbeitgeber insbesondere die krankheitsbedingten Fehlzeiten nur so lange speichern, wie sie für arbeitsrechtliche Maßnahmen, beispielsweise eine Abrechnung, erforderlich sind. Mit Hilfe des E-Health-Gesetzes wird der Ausbau der Nutzung der elektronischen Gesundheitskarte gefördert. Bis Ende 2018 sollen die Voraussetzungen dafür geschaffen werden, dass Daten der Patienten aus bereits vorhandenen Anwendungen und Dokumentationen (beispielsweise Notfalldaten oder Medikationspläne) in einer solchen elektronischen Patientenakte bereitgestellt werden. Durch die elektronische Gesundheitskarte wird nicht nur eine horrende Geldsumme aus dem Gesundheitssektor hin zu Herstellern technischer Systeme verschoben, auch das Gefühl der Bürger.innen, gläsern zu werden, nimmt immens zu.

Kommerzielle Überwachung

Ebenfalls relevant für das Gefühl der permanenten Überwachung sind Datensammlungen von privaten Anbietern. Hierbei handelt es sich zwar nicht um staatliche Überwachung, doch in dem Wissen, dass Geheimdienste und andere Behörden auf diese Datenbestände zugreifen, spielt diese Unterscheidung eine immer kleinere Rolle. Außerdem steht der Staat in der Verantwortung, hier klare Rahmenbedingungen zu stecken und deren Umsetzung zu kontrollieren. Die fehlende klare Positionierung an dieser Stelle mehrt das Unbehagen und Misstrauen gegenüber dem staatlichen Schutz.

Geheimdienste

Deutschland betreibt Geheimdienste und handelt mit Daten. Vorwürfe, dass dabei auch Daten von Deutschen verbreitet wurden, konnten nicht entkräftet wer-

Karikatur: Panthermedia

Auch diese Bürgerin wurde nicht vor Geheimdiensten geschützt.

den. Darüber hinaus ist die Unwilligkeit der Bundesregierung, die Menschen vor Übergriffen durch fremde Geheimdienste zu schützen, oder gar überhaupt diese Machenschaften aufzuklären, derzeit an vielen Stellen zu bewundern: Durch den Umgang mit der Selektoren-Liste, Beschwichtigungen und nicht zuletzt durch schallende Nichtaussagen im NSA-Untersuchungsausschuss wird immer klarer: Die Bundesregierung hat kein Interesse daran, unsere Daten (und damit unser Persönlichkeitsrecht) vor den Geheimdiensten zu schützen. Dafür erhielt das Kanzlerinnenamt 2014 einen BigBrother-Award. Auch die ausbleibende Verteidigung unserer Grundrechte muss in die Überwachungsgesamtrechnung einbezogen werden. Denn sie vermittelt ein klares Bild davon, wie viel Vertrauen an dieser Stelle angemessen ist: keins.

Meldedaten

Mit der Einführung des neuen *Rundfunkbeitrags* (früher: Rundfunkgebühr) 2013 wurde ein erneuter bundesweiter Abgleich von Meldedaten beschlossen, §9a:
„Zur Sicherstellung der Aktualität des Datenbestandes wird zum 1. Januar 2018 ein weiterer Abgleich entsprechend Absatz 9 durchgeführt. Die Meldebehörden übermitteln die Daten bis längstens 31. Dezember 2018."

Überwachungsgesetzespakete / staatliche Datensammlungen

Es existieren ganze Gesetzespakete, die in einer Form zusammengeschnürt wurden, dass sie – auf einen Schlag – die Überwachung diverser Lebensbereiche ermöglichen oder ausbauen. Das Anti-Terror-Gesetz (Terrorismusbekämpfungsgesetz, Sicherheitspaket II, Luftsicherheitsgesetz) beispielsweise hat Auswirkungen auf die Datenerhebung im Luftverkehr, bedingte biometrische Personalausweise, unterstützte die Einführung einer Antiterrordatei und führte zur Ausweitung der Befugnisse verschiedener Sicherheitsbehörden.

Datenabgleich bei Sozialhilfe und Asylverfahren

„Wissen ist Macht", und folgerichtig sind insbesondere Menschen, die von staatlicher Unterstützung abhängig sind, besonders ausführlich registriert und unterliegen gesonderten Gesetzen.

2004 haben wir der Bundesagentur für Arbeit einen BigBrotherAward verliehen für

Karikatur urheberrechtlich geschützt; Rechte bei Christiane Pfohlmann, www.pfohlmann.de

die Ausgabe eines 16seitigen Antragsformulars an Langzeitarbeitslose, mit dem hochsensible Daten teils unzulässig abgefragt wurden und Informationen auch unbefugten Stellen zugänglich werden konnten. Damit verstieß die Bundesagentur massiv gegen den Sozialdatenschutz, das Grundrecht auf informationelle Selbstbestimmung und den Grundsatz der Datensparsamkeit. Bis heute wird das Privatleben von Hartz IV-Empfänger.innen besonders durchleuchtet.

Menschen, die nach Deutschland geflüchtet sind und Asyl suchen, müssen ganz praktisch Einschnitte in ihre Privatsphäre hinnehmen. In Notunterkünften und Wohnheimen ist Privatsphäre ein sehr seltenes Luxusgut. Fingerabdrücke werden bei der Registrierung sowieso genommen. Und im Mai 2017 geisterte plötzlich eine „Biometrie-Superdatenbank“ durch die Schlagzeilen. Gemeint war der Plan der EU-Kommission, alle nationalen Sicherheits-Datenbanken aus den Sektoren „Sicherheit“, Grenzschutz und „Migrationsmanagement“ zu vernetzen.

(Die Materialsammlung zur Überwachungsgesamtrechnung ist ein fortlaufendes Projekt vom Digitalcourage-Team. Hinweise und Ergänzungen nehmen wir gerne entgegen.)

Karikatur urheberrechtlich geschützt; Rechte bei Christiane Pfohlmann, www.pfohlmann.de

„Auch online tut‘s richtig weh“

Mobbing und sexuelle Übergriffe im Netz

Foto: Eigensinn e.V.

Dies ist eine Rede von padeluun, gehalten am 30.6.2016 anlässlich des 25jährigen Jubiläums von „Eigensinn – Prävention von sexualisierter Gewalt gegen Mädchen und Jungen e.V.“, Bielefeld

Eine Schule. Genauer: Ein Gymnasium. Ländliche Gegend.
Hofpause. Eine junge Lehrerin hört Geschrei aus dem Jungenklo und schaut nach: Eine Gruppe von Knaben steht im Kreis um zwei Jungs herum und feuern den anscheinend Stärkeren an. Dieser etwas stämmige drückt den Kopf eines kleineren, schmächtigen Jungen, in die Kloschüssel. Niemand hilft. Niemand greift ein. Erst das Auftauchen der Lehrerin beendet das böse Spiel.

Waren Sie schon einmal oder öfter in der Situation der oder des Unterlegenen? Können Sie sich in die Gefühle des Opfers hineindenken, sie nachempfinden, mitempfinden? Dieses Ausgeliefertsein? Die Angst sich zu wehren, weil es dann wohl noch schlimmer wird? Gleichzeitig diese Wut, dass man nichts machen kann? Und diese unglaubliche Scham, das Schlimmste überhaupt, diese Scham, immer und immer wieder zu versagen, der Schwächling zu sein, das Opfer, der Verspottete, der Mülleimer, der mit dem man‘s machen kann, der Unwerte, der Gemobbte ...?

Und im Lehrerzimmer? Da stand die Ansicht im Raum, dass die Jugendlichen das unter sich aushandeln müssen, das gehöre zum Leben dazu. Erst eine heftige Intervention der jungen Lehrerin führte dazu, dass der Fall als das behandelt wurde, was er war: Ein gewalttätiger Übergriff, ich möchte es sogar Folter nennen.

Für das Opfer (und auch die Täter) ist dieser Fall (von der Traumatisierung mal abgesehen) vorerst ausgestanden. Wie anders wäre es, wenn das noch per Smart-

> „Wenn eine herzlose Software Klick um Klick hochzählt, wie oft die Tat wieder begangen wird.“

phone mitgefilmt worden wäre, wenn das auf Plattformen ins Internet gestellt worden wäre, wo es nicht (oder nur sehr schwer) löschbar wäre? Wenn die Tat immer und immer wieder angeklickt würde und eine herzlose Software Klick um Klick hochzählt, wie oft die Tat wieder begangen wird. Begangen durch Begaffen. Immer wieder und immer wieder. Die Demütigung von Handy zu Handy gesendet, via WhatsApp oder Facebook, und dem Opfer bewusst ist, dass die gesamte Schülerschaft das nun mindestens einmal gesehen hat. Das tut *richtig* weh.

Wie empathielos muss man sein, um einem anderen Menschen so etwas anzutun?

Ich habe mir gestern Nacht – einem Hinweis einer Freundin folgend – ein Video via Internet angesehen. Monica Lewinsky hielt im letzten Jahr einen sogenannten TED-Talk. Sie beschreibt dort, wie sich das anfühlte, innerhalb von Stunden von der gesamten Welt gedemütigt zu werden. Gerettet, sagt sie, hat sie die „Compassion“ ihrer Eltern und guter Freunde. Das Mitgefühl, die Loyalität, der Trost. Deswegen hat sie keinen Selbstmord begangen. Aber noch sehr lange haben ihre Eltern darauf bestanden, dass sie bei offener Badezimmertür duscht, damit sie sich nichts antut. Dieses Video, den TED-Talk, haben sich bisher nur 8,5 Millionen Menschen angeschaut.

Bundesjustizminister Heiko Maas sagte letzten Monat: „Im digitalen Zeitalter kann Gewalt Menschen überall erreichen“. Er sagte das anlässlich einer Preisverleihung des Deutschen Anwaltsvereins an Schülerinnen und Schüler, die Arbeiten zum Thema „Menschenwürde“ eingereicht hatten. Meine Kollegin Rena Tangens war dort als Jurorin und hat sich alle 84 eingesandten Arbeiten angeschaut. Es waren Filme dabei, Tonbeiträge, Texte, Bilder. Und sie war sehr schockiert. Sie war schockiert, weil sich fast alle Beiträge statt mit ‚Menschenwürde‘ mit Mobbing beschäftigen. Und wiederum viele dieser Beiträge beschrieben als Ausweg aus dem Mobbing den Freitod.

Stiller, viel stiller, noch als das Mobbing, das von Handy zu Computer und von dort wieder zum Handy weiter gereicht wird, ist eine andere Art von Übergriff. Das ist der Kerl, der im Chatprogramm lauert. Im harmlosen Onlinespiel nennt er sich „littledog“, ist vorgeblich jung und chattet junge Mädchen – manchmal auch Jünglinge – an. Erst mal geht es nur um das Onlinespiel, dann kommt schon bald die Frage, ob sein Gegenüber lieber junge Hunde oder junge Katzen mag. Ein Gespräch kommt zustande. Man verlässt gemeinsam den öffentlich einsehbaren Chatraum und wechselt in einen etwas privateren Kommunikationskanal. „littledog“ ist aufmerksam, nimmt sich Zeit, hört zu, möchte gerne mal ein Foto, damit er sieht, mit

wem er da spricht. Und natürlich ist auch die Frage „Hast Du einen Freund?“ bald da – und die Unterhaltung führt mehr und mehr in die Richtung, die „littledog“ einschlagen möchte. Bald telefoniert man auch. Oder trifft sich im Videochat.

„Cybergrooming“ wird das genannt.

Die Absichten sind klar: Der Herr möchte Bilder haben, erotische natürlich.
Und die bekommt er in der Regel auch. Schließlich war er immer so nett. Und dann hat man ihm auch schon ein Bild geschickt, wo die Bluse nur ein bisschen offen war. Man will ihn jetzt ja auch nicht verärgern. Immerhin schenkt er einem Aufmerksamkeit. Die will man nicht verlieren. Es ist so schön, wenn da einer ist, der einen ernst nimmt. Und man ist ja gerade dabei, die Welt jenseits der Kindheit zu erkunden. Da wird man schon mal ein bisschen leichtsinnig ... denn die eigenen Gefühle sind echt – und wie leicht lässt man sich betrügen. Aber mit den leicht aufreizenden Bildern gibt sich „littledog“ natürlich nicht zufrieden. Er möchte nackte Tatsachen. Er möchte nackte Tatsachen in eindeutigen Posen. Er macht eindeutige Vorgaben. Erst schmeichelt er – und wenn das nicht zum Erfolg führt, droht er mit den Bildern, die er schon hat. Dass er diese an Mitschüler schickt, oder die Eltern. ... Oft, sehr oft, führt das zum Erfolg.

Genügt „littledog“ es, wenn er Bilder hat? Vielleicht. Aber da gibt‘s auch noch „tomcat“, der nicht Ruhe geben wird, bis man in ein Treffen eingewilligt hat und nach Düsseldorf in die Wohnung seines Täters fährt.

Auf den Webseiten von Organisationen, die Präventionsarbeit leisten, steht, dass jede zweite / jeder zweite damit schon konfrontiert worden ist. Ich habe im letzten Monat mal ein bisschen rumgefragt. Und fast jede junge Frau, die ich letzten Monat fragte, hatte so etwas – zumindest solche Versuche – schon einmal erlebt.

Ich habe eine betroffene Frau gefragt, was ihr geholfen hätte. Sie sagte: „Mir hätte ein Verbot geholfen. Das hätte mich stark gemacht. Mir hätte es geholfen, wenn mir meine Mutter verboten hätte, mit Männern über 18 zu chatten oder gar aufreizende Bilder zu senden.“ Dann hätte sie sich nicht blöd gefühlt, wenn sie zu dem netten „littledog“ (so nannte er sich) „nein“ sagt und den Kontakt abbricht. Aber es gab kein Verbot, das ihr den Rücken gestärkt hätte. Auf das sie sich hätte berufen können. So kamen ihr ihre Freundlichkeit und Höflichkeit in die Quere – und glücklicherweise nach einem heftigen Chat – ohne Pornofotos – und einer schlaflosen Nacht, kam die Eigenerkenntnis, dass ‚das da‘ nicht gut ist und sie den Kontakt beenden muss.

Es ist so schön, wenn da einer ist, der einen ernst nimmt.

Und sie sagte noch etwas: Aufklärungsplakate in der Schule, auf denen vor solchen Kerlen und Techniken gewarnt wird,

hätten ihr geholfen. „Natürlich“, sagte sie gleich dazu, „werden sich alle Schülerinnen und Schüler über die Poster lustig machen (wir kennen das von den Kondomkampagnen) – aber sie helfen dennoch. Sie helfen, eine schamhaft verborgene Unterwelt ans Licht zu zerren.“

▶Je mehr wir als Erwachsene gebührenden Abstand zu Kindern und Jugendlichen halten, desto besser.◀

In anderen kriminellen Bereichen kennen wir Aufklärungskampagnen. Ich erinne an die Sendung „Vorsicht Falle“, die ich schon als Kind gerne geschaut habe. Dort wurde vor allen möglichen Betrugsmaschen gewarnt und aufgeklärt. Einige der Betrugsmaschen funktionieren heute immer noch. Mit jeder Spammail, auf die Sie nicht hereinfallen, mit jedem Preisausschreiben, das Sie nicht ausfüllen, können Sie ihren kritischen Verstand schulen. Und dennoch wird es immer wieder jemanden geben, der reinfällt. Deswegen braucht es Organisationen, die immer wieder aufklären. Und es braucht Auffangbereiche für Menschen, die zu Opfern geworden sind, in denen den Menschen, die hintergangen und missbraucht worden sind, die Scham genommen wird.

Und – auch das möchte ich nicht unerwähnt lassen – es braucht Präventionsmaßnahmen für Menschen, die nicht zu Tätern werden wollen. Diese Präventionsmaßnahmen für Täter können wir nicht nur an die unterfinanzierte Charité in Berlin abgeben. Sie gehören in den Alltag. Je mehr wir als Erwachsene gebührenden Abstand zu Kindern und Jugendlichen halten, desto besser. Wir haben nicht mit ihnen auf Facebook oder WhatsApp befreundet zu sein. Wir haben als Lehrende nicht das neue Bauchnabelpiercing der Schülerin lobend zu erwähnen. Wie vielen Jungen fehlt ein Vater, der Lebensweisheiten mitgibt?

Noch heute ist das Vergewaltigung verherrlichende Lied „Einst ging ich am Strande der Donau entlang“ in den Umkleidekabinen der Schulen zu hören – zumindest in meiner Jugendzeit kam dann nie der Sportlehrer herein und hat uns mal erklärt, WAS wir da gerade singen. „Hey, das Lied ist doch nur Spaß, jetzt sei mal nicht so spießig.“ Nein, ich bin nicht spießig. Im Gegenteil. Ich bin aktiver Unterstützer von Frauen, die freiwillig und mit Freude ihr Einkommen in der Sexarbeit verdienen. Ich unterstütze die sexuelle (und gesellschaftliche) Selbstbestimmung von Frauen. Ich arbeite aktiv an der Verhinderung des sogenannten Prostituiertenschutzgesetzes mit, das Frauen die Fähigkeit abspricht, für sich selbst zu entscheiden und weiterhin im Stigma der ewigen Opfer verharren lässt.

Und ich sehe exakt und präzise, wie Frauen nach wie vor von Rockern versklavt werden. Ich sehe exakt und präzise, das ich nur eine emanzipatorische Bemerkung in sozialen Netzwerken veröffentlichen muss, um einen Schwall von Fäkalkom-

mentaren zu erhalten. Ich erspare Ihnen die Zitate, ich finde es nicht hilfreich, diese zu verbreiten.

Was können Sie tun?

Monica Lewinsky sagte, wir brauchen „Compassion“. Das bedeutet Mitgefühl, Mitleid – mir gefällt am besten die Übersetzung „Barmherzigkeit“. Seien Sie barmherzig – achten Sie auf Ihre Mitmenschen. Nein, Sie sollen Ihre Nase nicht in Dinge stecken, die Sie nichts angehen. Aber auch in Ihrer Nachbarschaft leben Menschen, die von ihrem Elternsein gerade in der digitalen Welt überfordert sind. Machen Sie die Augen auf. Sprechen Sie mit Ihren eigenen Kindern offen. Vertüddeln Sie sich dabei nicht. Ihre Kinder haben im Netz vielleicht schon mehr Schrecklichkeiten gesehen, als Sie – sprechen Sie darüber, was am Schrecklichen schrecklich ist, warum es bei aller Meinungsfreiheit immer noch ein „richtig“ und „falsch“ gibt. Und erklären Sie ihren Kindern, dass es auch im Umgang mit anderen Kindern einen „richtigen“ und „falschen“ Umgang geben kann. Falsch ist: Mitmobben. Richtig ist, Opfern Hilfe anzubieten und ihnen beizustehen. Ihre Kinder bekommen mehr mit und sind viel verständiger, als Sie denken. Ihre Kinder wissen, wer „verwahrlost“ und wer lautlos nach Hilfe schreit. Auch Lehrerinnen und Lehrer haben oft tiefere Einblicke in Familienstrukturen. Zum Beispiel, wenn Kinder ohne Frühstück in die Schule geschickt werden, kann das ein Alarmsignal sein. Bedenken Sie aber: Auch Lehrenden fehlt hier die Unterstützung, etwas tun zu können. Wir können unsere Barmherzigkeit nicht an Lehrende delegieren.

Beobachten Sie sich selber: Schauen Sie in der Straßenbahn auch auf Ihr Smartphone? Gucken Sie im ICE Videos, anstatt sich mit den anderen Reisenden zu unterhalten? Nutzen Sie Chatprogramme, um sich zu unterhalten, statt miteinander zu reden? Sind Sie selbst Teil einer Verwahrlosigkeitstendenz, die sich im Online-Sein immer mehr ausbreitet? Glauben Sie, dass die Medien, die Regierung, Schulen oder Organisationen Sie von der Pflicht befreien, achtsam und barmherzig zu sein? Glauben Sie, dass man Übergriffe technisch beschränken kann, statt zu lernen, nicht übergriffig zu sein? Lassen Sie zu, dass unser Alltag videoüberwacht wird, statt dass wir lernen, nicht übergriffig zu sein? Lassen Sie zu, dass der Gesetzgeber immer übergriffiger wird, weil er glaubt, dass wir das brauchen, weil wir unser eigenes Leben nicht mehr selbst geregelt bekommen wollen?

- Wir alle wünschen uns für unser Leben Sicherheit, heißt es. Ich wünsche mir für unser Leben mehr: Ich wünsche mir Frieden statt Sicherheit.

Smart Citizens und die Rattenfänger

von Rena Tangens

Dieser Text fußt auf einem frei gehaltenen Vortrag von Rena Tangens bei den Stadtentwicklungstagen zum Thema „Smart City“ im Mai 2017 in der Stadthalle Bielefeld.

„Smart City“ ist ein Buzzword – niemand weiß so ganz genau, was unter „Smart City“ zu verstehen ist. Klar, „smart“ wollen alle sein. Städte, die zeigen wollen, dass sie voll angesagt sind, sehen das Label als Chance, etwas für ihr Marketing zu tun. Der Begriff ist wolkig, jede und jeder stellt sich etwas anderes darunter vor. Und es wird das Blaue vom Himmel herunter versprochen: Bessere Verkehrsleitung, mehr Umweltschutz, Energie sparen, effizientere Verwaltung, mehr Bürgerbeteiligung und so weiter.

Auf jeden Fall wird der Eindruck erweckt, dass unbedingt neue Technologie gebraucht würde, um bestimmte Probleme zu lösen – oft handelt es sich dabei allerdings um Kleinkram, der bis dahin noch gar kein Problem war. Oder es wird der Eindruck erweckt, dass nur es mit Hilfe neuer Technologie möglich wäre, tatsächlichen Problemen wie Klimawandel, Ressourcenverknappung und so weiter zu begegnen. Dieser Eindruck wird vor allem von denen geweckt, die an dem Hype verdienen wollen, also von den großen Technologiekonzernen IBM, Cisco, Microsoft, Huawei, Siemens etc. Der Begriff „Smart City“ ist weniger ein Beitrag von Stadtplanern, Architektinnen oder Klimaschützern zur Stadtentwicklung, sondern eher ein Marketinginstrument der Firmen, die ihre Technik an Städte verkaufen wollen. Die Verantwortlichen bei den Kommunen fühlen sich im Zugzwang, weil „Smart City“ voll im Trend ist; sie glauben, dass sie das jetzt ganz schnell starten müssen, um nicht ins Hintertreffen zu geraten.

Foto: Claudia Fischer, cc by-sa 4.0

Problematisch ist die Verknüpfung von Smart Cities mit Big Business.

> „Hoppla, Ihre Daten wurden verschlüsselt“

Mit der „Smart City“-Vision einher gehen leichtfertige Technologiegläubigkeit („Wir können soziale Probleme mit Technik lösen!“) und Fortschrittsoptimismus („Alles wird immer besser!“). Dabei gerät aus dem Blick, dass viele Aufgaben auch ohne neue Technologie, dafür mit besserer Aufklärung, mehr Bürgerbeteiligung und besserer Organisation zu lösen sind. Und es bleibt unberücksichtigt, dass die Technologien selbst ganz neue Probleme mit sich bringen können.

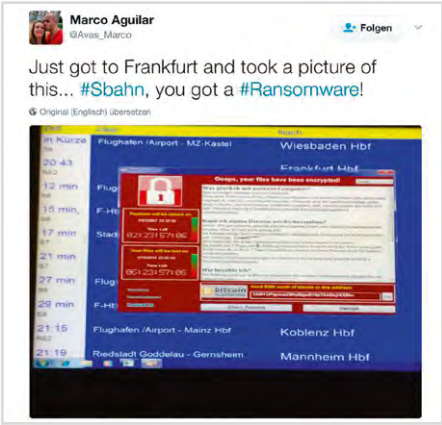
Grundsätzlich problematisch ist die Verknüpfung von Smart City mit Big Business. Denn die Vertreter des Big Business meinen, dass „Daten das neue Öl“ seien. Sie wollen ihre Claims abstecken und betrachten Bürgerinnen und Bürger als Rohstoff, den sie ausbeuten können.

Und es gibt noch mehr zu bedenken: 1. Sicherheitsprobleme und Missbrauchsmöglichkeiten, 2. Dauer-Überwachung und Manipulation, 3. Abhängigkeit durch Privatisierungs und 4. Technikpaternalismus statt freier Entfaltung.

Aber der Reihe nach:

1. Sicherheit im System? – Fragen Sie WannaCry!

Im Mai 2017 gab es eine weltweites Real-Life-„Event“, das auch Nicht-Techies nicht übersehen konnten: WannaCry, eine Schadsoftware, hatte eine Unmenge von Systemen gekapert. Die Erpressungsmeldung („Ooops, your files have been encrypted“ – „Hoppla, Ihre Daten wurden verschlüsselt“) mit einer Geldforderung in anonymen Bitcoinstauchte sogar auf den Anzeigetafeln an den Bahnhöfen der Deutschen Bahn auf und wurde sogar von internationalen Besuchern mit Grinsen zur Kenntnis genommen („Hallo, Ihr habt ein Schadsoftware-Problem“ - von @Avas_Marco)



WannaCry gab uns eine kleine Ahnung davon, was alles passieren kann, wenn z.B. übermütige jugendliche Hacker mit der smarten Stromversorgung, dem Verkehrsleitsystem oder den Wasserwerken Jojo spielen.

Je mehr wir uns von vernetzten Systemen und Steuerungen abhängig machen, desto verletzlicher werden wir. Und je komplexer die Systeme sind, desto anfälliger sind sie für Angriffe und desto folgenreicher sind die Ausfälle. Das gilt insbesondere für Städte und Kommunen, die unsere Energie-, Wasser- und Verkehrsinfrastruktur verantworten.

Sehr hübsch illustriert ist das Ausgeliefertsein in dem Cartoon „Internet of Ransomware Things“ (Internet der Erpressungsdinge) von Joy of Tech mit einem Blick in ein Smart Home: Der elektronische Rauchmelder droht, nicht mehr bei Feuer zu warnen, wenn nicht 30 Dollar in Bitcoin überwiesen werden. Der Kühlschrank will erst Geld, bevor er die Tür öffnet und der Besen fordert 25 Dollar – sonst verrät er all deinen Social-Media-Freunden, dass du so blöd warst, einen Besen mit Internetanschluss zu kaufen.

▶2. Surveillance by Design – Überwachung eingebaut

Als große Errungenschaft für eine Smart City wird zum Beispiel ein neuer Typ von Straßenlaterne angepriesen. Die leuchtet nicht nur, sondern enthält auch gleich Videoüberwachung, Fußgängererkennung, Kfz-Kennzeichenleser, Umweltsensoren, einen Schuss-Detektor und einen Location-Beacon fürs Tracking der Position. Stellen wir uns dies noch kombiniert mit WLAN vor, mit dem die Position eines Smartphones durch Triangulation ermittelt werden kann, Gesichtserkennung jeder Person und Bewegungsanalyse, dann ist klar: Wir werden keinen Schritt mehr unbeobachtet tun können, wenn diese Vision tatsächlich gebaut wird. Das ist „Surveillance by Design“. (im Unterschied zu „Privacy by Design“).

▶Je mehr wir uns von vernetzten Systemen und Steuerungen abhängig machen, desto verletzlicher werden wir.◀

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. Und: Staatliche Kontrolle und Business lässt sich ganz wunderbar miteinander vereinbaren.

Die Smart City soll zugleich eine „Safe City“ sein. Einmal mehr wird hier Sicherheit mit Überwachung und Kontrolle der Bevölkerung gleichgesetzt. So lesen wir in der Pressemeldung eines Überwachungstechnik-Anbieters:

„Mit der heutigen Technologie (...) können vollkommen sichere Städte gestaltet werden. Gesichtserkennungssysteme unter der Kontrolle der Sicherheitsbehörden von Städten mit intensiver Überwachung können das weltweite Sicherheitsverständnis (…) völlig verändern“, sagt Ekin. „Die neue Gesichtserkennungstechnologie ermöglicht es Regierungen und privaten Unternehmen, alle Gesichter zu erkennen und zu archivieren, während dies zuvor auf eingetragene Straftäter beschränkt war.“ Er beendete seinen Vortrag mit der Erwähnung mobiler Geräte, die in Autos, Fahrräder und andere Fahrzeuge eingebaut werden und die gesamte Stadt scannen können.

Es wird suggeriert, dass es eine Stadt sicher machen würde, wenn alle Bürger.innen jederzeit im Blick und unter Kontrolle seien. Schalten Sie den Rechner jetzt nicht aus – Panoptikon wird installiert – willkommen im Polizeistaat.

Am Bahnhof Südkreuz in Berlin testet die Bundespolizei seit August 2017 intelligente Videoüberwachung mit Gesichtserkennung. Völlig egal, wie der „Test" läuft – es ist sowieso klar: der Innenminister will das haben und zwar an möglichst vielen öffentlichen Orten. Judith Horchert schreibt dazu auf Spiegel online: „Der Test am Südkreuz wird auch ein Test für unsere Freiheit." und „Noch mehr zu fürchten als ein Staat, der seine Bürger überwachen will, sind Bürger, die das gleichgültig hinnehmen."

Naive Gemüter meinen, dass sich Menschen besser verhalten würden, wenn sie sich beobachtet fühlen, und dass das deshalb ok sei. Ich meine, dass Angst vor Entdeckung kein Ersatz für einen eigenen ethischen Kompass ist.

Kleine Kinder klauen oft im Supermarkt – sie wissen zwar irgendwie, dass das nicht ok ist, aber es ist das schnelle Haben-Wollen und eine Grenzüberschreitung, eine Mutprobe, ein Nervenkitzel. Egal, ob sie erwischt werden oder nicht: Die allermeisten Kinder kommen zu der Einsicht, dass Klauen nicht ok ist und lassen es sein, denn sie selbst wollen auch nicht beklaut werden. Wenn Kinder sich aber nur noch aus Angst vor Dauerüberwachung und Entdeckung korrekt verhalten, dann haben sie keine Gelegenheit, eine eigene Haltung zu entwickeln. Was werden sie tun, wenn dann mal das Überwachungssystem ausfällt? Richtiges Verhalten muss erlernt und geübt werden – auch unser „Moralmuskel" braucht Training.

Freiheit beinhaltet die Möglichkeit, Fehler zu machen. Und daraus zu lernen.

3. Privatisierung – Städte verkaufen ihre Bürger

Microsoft, Cisco, Huawei, IBM und Siemens kaufen sich ein – sie machen günstige Angebote zum Einstieg und es locken ja auch Landes- und EU-Fördermittel für Smart Cities. Doch diese Firmen sind die Rattenfänger, die spätestens dann, wenn die Stadt nicht mehr zahlen will oder kann, die Menschen, die in der Stadt leben, zum Produkt machen.

Foto: Claudia Fischer, cc by-sa 4.0

Wollen wir eine Welt, in der nur dort nicht geklaut wird, wo eine Kamera in der Nähe ist?

Grafik: Panthermedia

Wenn die Städte ihre Infrastruktur verschachern, werden die Bürger.innen zum Produkt.

Eine Smart City in Konzernhand ist ein Danaergeschenk – „Timeo Danaos et dona ferentes“ („Ich fürchte die Griechen, auch wenn sie Geschenke bringen.“). In der griechischen Sage bringt das geschenkte hölzerne Pferd das Verderben in die Stadt Troja. Sobald es in den Stadtmauern ist, ist die Stadt schutzlos.

Städte werden wieder einmal verlockt, ihre Infrastruktur in kommerzielle Hände zu geben. Das ist kurzsichtig und gefährlich. Die Erfahrungen mit Cross-Border-Leasing zeigen sehr deutlich, dass das keine gute Idee ist. Per Cross-Border-Leasing wurden kommunale Anlagen wie Elektrizitätswerke, Wasserwerke, Straßenbahnlinien, Schulen, Krankenhäuser an ausländische Konzerne verkauft, um sie dann von ihnen zurück zu mieten. Das war ein Steuersparmodell insbesondere von US-Konzernen, mit dem der öffentlichen Hand in den USA Milliardenbeträge an Steuereinnahmen verloren gingen. Gleichzeitig begaben sich deutsche Städte und Kommunen in Abhängigkeit von profitorientierten Konzernen und wurden erpressbar. Viele Städte haben mittlerweile den Irrtum bemerkt und haben ihre Stadtwerke oder ihre Wasserversorgung teuer zurückgekauft. Aus dem Debakel mit Cross-Border-Leasing sollten Städte und Kommunen gelernt haben und nicht wieder denselben Fehler mit den Smart-City-Anbietern machen.

- Wer will schon in eine Stadt ziehen, deren Infrastruktur Huawei, IBM oder Microsoft gehört?

Bei Public Private Partnerships für Smart Cities droht allerdings mehr als nur das billige Verscherbeln städtischer Infrastruktur: Städte könnten hier leichtfertig etwas verkaufen, was ihnen gar nicht gehört, nämlich die Daten der Bürgerinnen und Bürger – und damit ihre Privatsphäre, ihre Autonomie, ihre Freiheit.

4. Kulturelle Veränderungen – Bequemlichkeit macht dumm

Selbst wenn wir jetzt einmal annehmen, dass das Smart City System absolut sicher wäre, dass die Technologie-Firmen nichts Böses mit unseren Daten im Schil-

de führten und der Staat bei all der Überwachung ausschließlich unser Wohl im Blick hätte – selbst wenn alles perfekt optimiert wäre, gibt es doch fatale kulturelle und geistige Nebenwirkungen. Wenn die Smart City uns alles Mögliche abnimmt, ist das natürlich erst mal sehr bequem. Aber auf lange Sicht macht Bequemlichkeit träge und dumm. Und wir lernen nicht mehr, selbst Probleme zu lösen.

Im Märchen vom Schlaraffenland fliegen den Menschen die gebratenen Gänse essfertig in den Mund. Das moderne Pendant wäre wahrscheinlich die nach unseren errechneten Wünschen von Amazon generierte Bestellung, die uns sogleich von einer Drohne geliefert wird, wo auch immer wir gerade sind. Aber: **Das Schlaraffenland** ist nicht das **Paradies**. Es macht satt, aber nicht glücklich.

Wir brauchen das Beinahe-Stolpern, um unseren Gleichgewichtssinn zu trainieren. Wir brauchen die Anstrengung, um uns über unsere eigene Leistung zu freuen. Wir brauchen den Zufall, das Andere, das Unbekannte, die Überraschung, die Herausforderung, um zu lernen und uns weiterzuentwickeln.

▶Statt mehr Überwachung und Kontrolle brauchen wir mehr Menschen, die sich für ihr Umfeld verantwortlich fühlen.◀

Auch deshalb müssen wir uns wehren gegen die Bevormundung durch Technik und den Technik-Paternalismus. Statt mehr Überwachung, Kontrolle, Sensoren und Leitsystemen brauchen wir mehr Menschen, die sich für ihr Umfeld, ihre Nachbarn und für ihre Stadt verantwortlich fühlen. Dafür brauchen wir Freiräume, die uns ermöglichen, dieses Verantwortungsgefühl zu entwickeln.

Der große Landschaftsarchitekt Frederick Law Olmsted (1828-1903) hat den Central Park in New York, Prospect Park in Brooklyn und viele andere Parks in Kanada und USA durchgesetzt, konzipiert und gestaltet. Olmsted hat den Satz geprägt: **„Citizens need parks!“** Damit meinte er, dass Bürgerinnen und Bürger Grünflächen und damit Freiraum brauchen, um Bürgerinnen und Bürger sein zu können. Nur an Orten, die wir als angenehm empfinden,

„Citizens need parks!“

Foto: Rena Tangens cc by-sa 4.0

können wir uns entspannen, unsere Umwelt mit allen Sinnen zugleich wahrnehmen und uns als Teil der Gemeinschaft zu fühlen.

Was aber sind angenehme Orte? Dafür haben Architekturpsychologie und Kognitionsforschung verschiedene Kriterien gefunden. Tony Hiss hat sie in seinem lesenswerten Buch „Ortsbesichtigung“ dokumentiert: Angenehme Orte sind 1. anregend 2. lesbar 3. geheimnisvoll 4. sie bieten Ausblick und 5. sie bieten ein Versteck.

Anregend bedeutet: vielfältig, nicht gleichförmig. Lesbar bedeutet, dass der Ort den Eindruck erweckt, dass ich lernen kann, mich hier zu orientieren und zurecht zu finden und zu verstehen, was hier wie funktioniert. Geheimnisvoll bedeutet, dass nicht alles offen liegt, sondern dass ich aktiv werden muss und es erkunden. So wie ein Hügel dazu einlädt, ihn zu erklimmen und zu schauen, was dahinter ist. Freier Ausblick schenkt uns Weite, ein hoher Raum oder freier Himmel gibt uns Raum zum Denken. Ein Versteck kann ein Waldrand, ein Gebüsch oder auch eine Ecke in einem Cafe sein, wo ich mich geborgen fühle und wo ich nicht von Menschen beobachtet werde, die ich selber nicht sehen kann.

Das englische Wort für Erholung beschreibt sehr viel schöner, um was es geht: Re-creation – das heißt, sich immer wieder selbst neu zu erfinden.

Eine Smart City, in der mir Technik die meisten Entscheidungen abnimmt, die alles für mich bequem macht, die mich ständig mit auf mich zugeschnittenen Angeboten begleitet und mich ständig im Blick hat, gibt mir nicht mehr den Raum für persönliches Wachsen.

Fazit

Eine Stadt ist nicht smart – smart sind die Menschen, die darin leben. „Smart Citizens“ sehen sich als Bürgerinnen und Bürger – nicht nur als Konsument.innen, die es möglichst bequem haben wollen und die geleitet, beobachtet, manövriert und bevormundet werden. Aktive Bürgerinnen und Bürger wollen mitbestimmen, sich engagieren und ihre Stadt mitgestalten.

Marta Suplicy, die als Kulturministerin und als Bürgermeisterin von Sao Paulo in Brasilien für die dortige Ausgestaltung der Smart City verantwortlich war, stellte 2017

bei einem Panel auf der RightsCon-Konferenz in Brüssel klar: Eine Stadtverwaltung sollte zuerst die Menschen fragen, was ihre Stadt, ihr Dorf, ihr Viertel lebenswert macht – und was ihnen dafür noch fehlt oder was verändert werden sollte. Und: Viele der angesprochenen Punkte seien ganz ohne smarte Technik lösbar.

Wenn wir weniger Abgase und weniger Lärm haben wollen, ist ein Verkehrsleitsystem, das vernetzte Autos optimal synchronisiert durch die Stadt schleust, eben nicht die richtige Maßnahme. Denn dadurch werden es nicht weniger, sondern mehr Autos in der Stadt.

Wenn wir klug sind, sorgen wir dafür, dass in der Stadt fast keine Autos mehr gebraucht werden – durch den Ausbau eines günstigen oder kostenlosen öffentlichen Nahverkehrs im Takt, attraktive und sichere Straßen für Fahrräder und Fußgänger und eine Stadtplanung, die Infrastruktur wie Läden, Restaurants, Kitas, Schulen, Arztpraxen in der Nachbarschaft fördert. Laut Staatssekretär im Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit Gunther Adler sind die folgenden fünf Einrichtungen die, die sich die Menschen am meisten in ihrer Nähe wünschen: Einzelhandel, Kita, Schule, öffentlichen Nahverkehr per Bus oder Bahn und eine Arztpraxis. Übrigens: 20% der deutschen Kommunen erfüllen kein einziges dieser Kriterien! Ja, natürlich wollen wir auch Breitband-Internet. Aber das ist kein Ersatz für alles andere. Denn es braucht auch öffentliche Orte abseits von Wohnung und Arbeit, wo Menschen einfach hingehen, sich treffen und kennenlernen können. Parks, Cafés, öffentliche Plätze, Wochenmärkte, Freibäder und so weiter.

Wir haben die Wahl: Wollen wir in einer post-demokratischen Konsumwelt leben, wo andere für uns entscheiden und die einzig mögliche Antwort „ok“ ist? (Sehr schön beschrieben in „Qualityland“ von Marc-Uwe Kling!) Oder wollen wir frei sein?

Albus Dumbledore wusste schon 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.

Smart Health

Der verkabelte Mensch und seine Gesundheit

Von Maximilian von der Heyden

Dieser Artikel stammt aus unserer Blog-Reihe „Smart Everything – Das Internet der Dinge“ (Stand April 2016).

Das Smartphone klingelt. Es hat ein nahendes Nierenversagen erkannt. Über eine Echtzeit-Übertragung bekommt ein Facharzt die Informationen und überprüft sie. Die Smart Health-Anwendung der Krankenkasse schlägt einen OP-Termin gleich nächste Woche vor. Die Krankheit wird schnell erkannt und eine frühe Behandlung ist möglich. Doch wer hört bei der Datenübertragung mit und wer wertet die Daten aus? Ist der Tausch von Privatsphäre gegen Gesundheit ein fairer Handel?

Foto: Panthermedia

Wenn der Arzt der App mehr glaubt als dem eigenen Fachwissen.

Was ist „Smart Health“?

„Smart Health“ beschreibt die Digitalisierung des Gesundheitswesens; sowohl Vorsorge, Pflege als auch Betreuung werden durch automatisierte Prozesse erweitert und ersetzt. Es geht um die Entwicklung neuer IT-Methoden, wie zum Beispiel die Nutzung von elektronischen Patientenakten, die Möglichkeit zu Ferndiagnosen via Telemedizin oder den Einsatz von Maschinen, etwa in Form von Assistenzsystemen für ältere Menschen. Die Entwicklung vollzieht sich zunehmend von der traditionellen „Boxenstopp-Medizin“ hin zu einem kontinuierlichen Austausch von Gesundheitsdaten und Diagnosen – so soll beispielsweise zukünftig der Arztbesuch, etwa zur Besprechung eines Laborberichtes, völlig entfallen, um Ressourcen einsparen zu können.

Wo stehen wir aktuell?

Fitness-Apps kommen zunehmend zum Einsatz, um zur regelmäßigen sportlichen Tätigkeit zu motivieren und den gesundheitlichen Fortschritt aufzuzeichnen. Über 100.000 Fitness-Apps und sogenannte „Wearables“ wie Armbänder, Uhren oder aber auch Sportgeräte bieten derzeit einen Zugang zu Datenbankservern, die wiederum Rückmeldungen über den gesundheitlichen Zustand ermöglichen. Das

Foto: Panthermedia

Das Tablet als Gesundheitstrainer.
Nur Turnen müssen wir noch selbst.

eigene Smartphone wird schnell zu einem persönlichen, jederzeit verfügbaren Fitness- und Gesundheitscoach. Der Nachwuchs lässt sich ganz sorgenlos durch einen angebrachten Sensor via Smartphone überwachen, sodass Zeit für anscheinend wichtigere Dinge, wie Übungen auf der smarten Yogamatte, bleibt.

Darüber hinaus werden immer häufiger sogenannte **„altersgerechte Assistenzsysteme für ein selbstbestimmtes Leben“** beworben. Dieser Begriff umfasst Technologien, die sich auf das Leben und die Bedürfnisse der Menschen anpassen sollen und nicht umgekehrt. So richten sich, im Sinne des „Smart Home-Prinzips“, Beleuchtungs-, Raumtemperatur- oder Musiksteuerungen nach den jeweiligen, von einem Programmcode bestimmten Ansprüchen der Menschen.

Aber auch das öffentliche Gesundheitssystem greift zunehmend auf Smart Health-Möglichkeiten zurück. Ob digitaler Abgleich von Messwerten oder sogenannte Telediagnosen – die Krankendaten werden immer dichter vernetzt. Befürworter legen dies als eine Chance aus, um schneller Fachleute erreichen zu können, damit erkrankte Menschen möglichst selten das häusliche Umfeld verlassen müssen. Beispielsweise kommunizieren Patientinnen und Ärzte mittlerweile über eine Plattform namens SMAP, um so einen direkten Kontakt zwischen Patienten, Hausärztinnen und Fachärzten zu ermöglichen, sodass weite Anreisewege und doppelte Untersuchungen vermieden werden können.

In Deutschland wurde ein großer Schritt mit der Einführung der elektronischen Gesundheitskarte in diese Richtung gemacht.

Am 1. Januar 2014 löste die eGk offiziell die alte Krankenkassenkarte ab, wobei die Versicherungspflichtigen freiwillig über die zentrale Speicherung von Patientenakten in der sogenannten „elektronischen Patientenakte“ entscheiden konnten. Mit dieser sind einige Risiken verbunden (BigBrotherAwards 2004 und 2015).

In anderen Industrienationen werden bereits zunehmend Roboter innerhalb von Pflegeberufen eingesetzt, sowohl unterstützend in der Pflege (z.B. für das Umbetten von Patient.innen), als auch er-

setzend als Unterhaltungsquelle und Anti-Depressionsschutz. Beispielsweise stellte der Konzern Toyota 2007 den Roboter Robina vor, der künftig in der Krankenpflege assistieren und Patient.innen betreuen soll.

Foto: opyh, cc by 2.0

Silke Durchscheinend protestiert gegen die Elektronische Gesundheitskarte.

Welche Daten werden gesammelt?

Im Rahmen von Smart Health werden Daten über den gesundheitlichen Zustand erhoben, also das elektronische Sammeln, Auswerten und Vernetzen von medizinischen Daten, wie Röntgenbildern, Medikamentenlisten, psychologischen Gutachten, Behandlungsnotizen und so weiter.

Diese Daten können dann entweder direkt genutzt werden, um beispielsweise eine Diagnose treffen zu können. Darüber hinaus können diese Daten aber auch langfristig gesammelt und aufbewahrt werden, etwa in Form einer Gesundheitskarte oder mithilfe einer Datenbank.

Wo liegen die Gefahren?

Big Data ist im Gesundheitswesen besonders kritisch zu betrachten. Zwar versprechen die meisten Anbieter in Form von wohlklingenden Datenschutzerklärungen, dass man auf Datenschutz achte, dennoch stellt sich die Frage, was langfristig mit den gesammelten Gesundheits-Biographien geschehen wird. Ebenfalls erscheint fraglich, wie sich derzeitige Sparmaßnahmen und die Kommerzialisierung des Gesundheitswesens auf die Datenmassen auswirken werden.

„Es muss uns klar sein, dass Big Data, wie jedes andere Werkzeug, für gute und schlechte Zwecke eingesetzt werden kann.“ (Spektrum Digital-Manifest S. 34)

Die Beziehung zwischen Patient und Ärztin könnte sich durch Smart Health gravierend verändern. Der persönliche Kontakt während einer Behandlung lässt sich nicht mit Robotern und Datenbanken ersetzen, weil Gesundheit mehr ist als nur Messergebnisse und Behandlungsvorschläge.

Darüber hinaus stellt sich die Frage, ob nicht überall dort, wo Personen eindeutige Identifikations-Nummern zugewiesen werden, die Gefahr einer systematischen Diskriminierung Einzug hält. Hacker.innen, Versicherungen, Arbeitgeber.innen

und Geheimdienste besitzen ein hohes Interesse, Zugriff auf diese Daten zu erlangen. Die ärztliche Verschwiegenheitspflicht würde so langfristig faktisch ausgehöhlt werden.

Fraglich erscheint ebenfalls, welcher körperliche Zustand eigentlich als gesund gilt und ab wann die Erkrankung beginnt. Ist es eine Ausprägung von Autonomie, darüber entscheiden zu können, ein Wearable zu benutzen, um die Kontrolle über den eigenen Körper zu erlangen, oder besteht nicht sogar eine Form von Fremdbestimmtheit? Beispielsweise zeigten verschiedene Versicherungskonzerne Interesse daran, Boni und günstigere Versicherungsprämien an das kontinuierliche Sammeln und Kontrollieren von Daten zu koppeln. Da Krankenkassen bislang vorrangig auf dem Solidaritätsprinzip beruhten, könnte dieses mit der Koppelung von Leistungen an Tracking unterlaufen und schließlich ganz abgeschafft werden. Im Ergebnis könnte das eine fundamentale Entsolidarisierung bedeuten.

Foto: Panthermedia

Wer ist krank? Wer ist gesund? Wer ist fit, wer faul? Soll das ein Computer entscheiden?

Fazit

Das Konzept von Smart Health ermöglicht es, die Lebensqualität von Menschen mit Behinderung oder anderen Einschränkungen zu verbessern, beispielsweise durch die oben beschriebenen Assistenzsysteme oder Anwendungen wie zum Beispiel „Be My Eyes“, die Nutzer.innen via VoIP mit Menschen mit Sehbehinderung überall auf der Welt verbindet, um diese im Alltag zu unterstützen.

Allerdings verführt das Konzept auch dazu, sich nicht mehr der Preisgabe der intimsten aller Daten bewusst zu sein. So entsteht die Gefahr, Krankenkassen, Arbeitgeber.innen, Versicherungen oder dem Staat ausgeliefert zu sein. Die Verkabelung unserer Gesundheit komplettiert in diesem Sinne die Metapher des gläsernen Bürgers.

Technische Entwicklung muss gerade im Gesundheitssektor streng an unserem Wertesystem ausgerichtet sein, zu dem natürlich auch die Entscheidung zählt, selbst darüber entscheiden zu können, ob man krank ist.

Der AKtiVCongrEZ in Hattingen

Gemeinsam aktiv für Datenschutz und Bürgerrechte

Von Claudia Fischer

„Es wird sehr viel moderiert. Das ist einerseits natürlich ein bisschen einschränkend, andererseits aber auch sehr, sehr ergebnisorientiert." So beschreibt Digitalcourage-Mitglied Leena Simon den AKtiVCongrEZ im DGB-Tagungszentrum Hattingen in einem Internet-Video.

▶Warum AKtiVCongrEZ?

Dass dieser Tagungs-Titel so komisch geschrieben wird, liegt an der Zusammensetzung: AK steht für die Arbeitskreise, die an dem Kongress beteiligt sind. Das V steht für Vorratsdatenspeicherung. Das C für den CCC (Chaos Computer Club), das große E für den Arbeitskreis Elektronische Verwaltung und das Z für Zensur oder Zensus (=Volkszählung).

Jedes Jahr im Januar oder Februar treffen sich Aktive aus Gewerkschaften, Bürgerinitiativen und anderen Verbänden, um ihre Arbeit für Privatsphäre und Freiheitsrechte zu koordinieren, Bündnisse zu schmieden und gemeinsam Visionen zu entwickeln. „Persönliche Treffen sind sehr sinnvoll", findet padeluun von Digitalcourage, „denn es laufen viele Sachen einfach nebenbei, über die man sich in Mailinglisten monatelang den Mund fusselig redet. Hier kann man die bei einem Bier mal eben schnell beilegen." Insbesondere, so betont ein anderer Teilnehmer: „Für jemanden, der ein bisschen alleine steht in seinem Ortskreis, sind die Kontakte und Arbeitsgruppen hier sehr wichtig."

Seit 2010 richten Digitalcourage und DGB-Gewerkschaften diesen Kongress aus, und schon im ersten Jahr mündete eine der Arbeitsgruppen in einer Verfassungsklage: 22.005 Menschen beteiligten sich an einer Klage gegen ELENA, den „elektronischen Entgeltnachweis", auch bekannt als die Massen-Datenspeicherung von Arbeitnehmer.innendaten, die bereits 2008 einen BigBrotherAward erhalten hatte. Eine Arbeitsgruppe beim ersten AKtiVCongrEZ hat diese Verfassungsklage maßgeblich mit vorangebracht – Ende 2011 wurde ELENA wieder eingestampft.

Anfang des Jahres 2013 hat ein Entwurf eines Gesetzes zum Beschäftigtendatenschutz Gewerkschafter.innen, Beschäftigte und Datenschützer.innen aufgeschreckt. Im Entwurf waren viele Dinge enthalten, die Arbeitgeber gerne zur Kontrolle ihrer Beschäftigten verwirklicht gesehen hätten. Auch hier hat sich auf dem

Foto: padeluun, cc by-sa 4.0

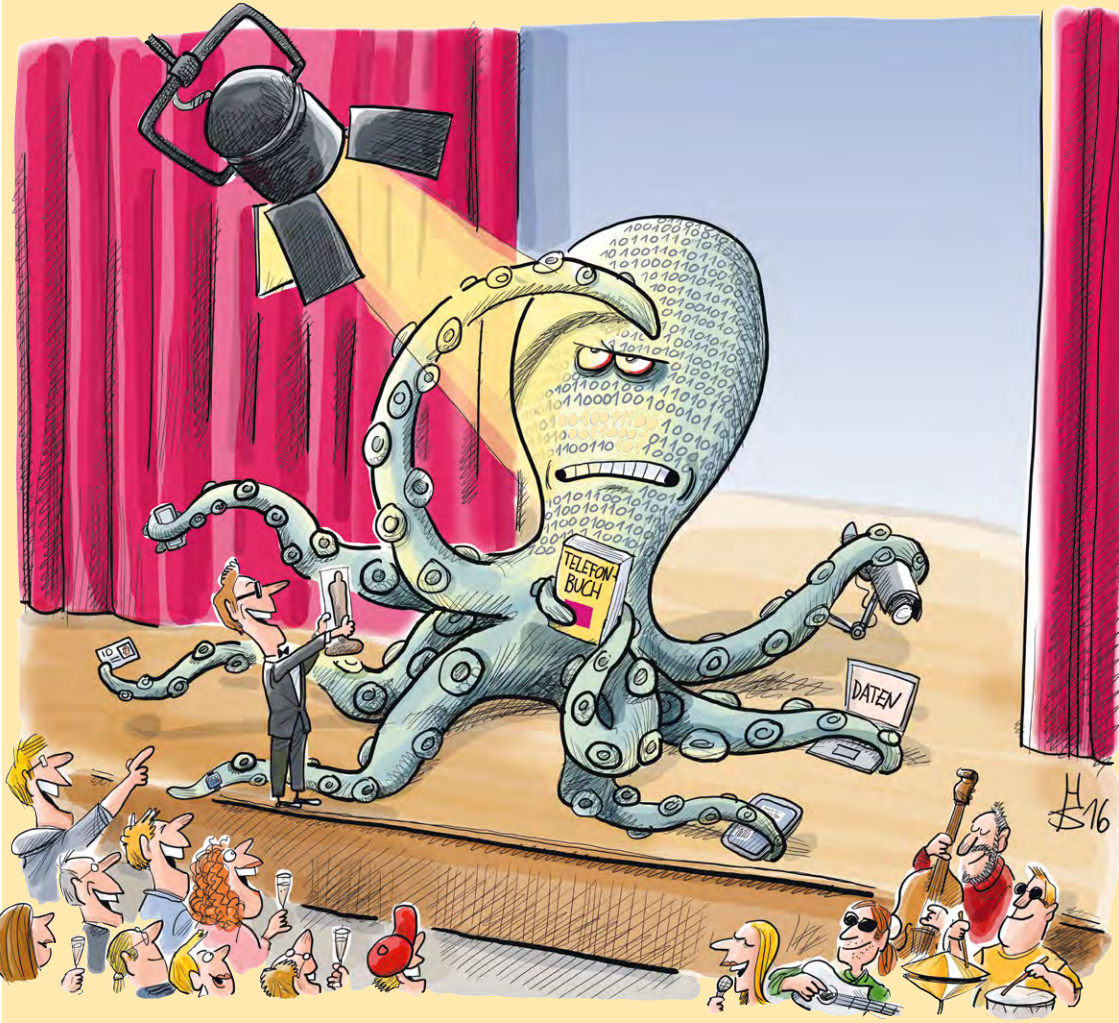
Drei Tage Zeit nehmen für Datenschutz und Bürgerrechte, Bündnisse schmieden, Aktionen planen: Der AKtiVCongrEZ stärkt alle, die sich engagieren.

AKtiVCongrEZ sehr schnell eine Arbeitsgruppe gefunden, die eine Strategie zur Verhinderung dieses Entwurfes entwickelt und durchgezogen hat. Mit Erfolg! „Wir haben einen juristischen Gegenentwurf entwickelt und um Stellungnahmen prominenter Arbeitsrechtler wie Peter Wedde und Wolfgang Däubler gebeten. Diese haben wir veröffentlicht, den DGB und die Einzelgewerkschaften aktiviert und eine riesengroße Campact-Kampagne durchgeführt. Dies alles geschah innerhalb weniger Wochen“, erinnert sich Monika Heim, die von Anfang an beim dabei war. „Die Wellen, die wir geschlagen haben, waren so hoch, dass der Entwurf noch nach der zweiten Lesung im Bundestag zurückgezogen wurde. Ohne den AKtiVCongrEZ wäre das nicht geschehen.“

Diese zwei Beispiele zeigen, wie erfolgreich Angriffe auf Beschäftigte (besser: auf Grundrechte) abgewehrt werden können, wenn sich die richtigen Leute finden. Beim AKtiVCongrEZ in Hattingen lernen sich Menschen aus den unterschiedlichsten Handlungsfeldern kennen und vernetzen sich miteinander: aus Betriebsräten und Gewerkschaften, Datenschutz und Digitalcourage, Arbeits- und Bürgerrechtsarbeit.

Die Zukunft wird mit Industrie 4.0, Beschäftigtendatenschutz nach der Neuregelung durch die Europäische Datenschutzgrundverordnung, Crowd- und Clickworking noch viele Themen bringen, die in den Betrieben und Gewerkschaften umgesetzt werden müssen. Ein Betriebsrat allein, eine Gewerkschaft allein, eine Gruppe Ehrenamtlicher allein wird da nicht so viel ausrichten können wie eine Gemeinschaft Gleichgesinnter, die ihre unterschiedlichen Fähigkeiten und Sichtweisen zusammenbringen. „Die jährlichen Treffen auf einem AKtiVCongrEZ sind Initialzündung für viele Ideen und Hilfestellung in den Betrieben. Die Kontakte, die mensch dort knüpft, sind Gold wert“, sagt Gewerkschafterin Monika Heim, und freut sich schon auf das nächste Mal in Hattingen, im Februar 2018.

Die BIG BROTHER AWARDS 2017



Karikatur: Heiko Sakurai, cc by-sa 4.0

Die BigBrotherAwards 2017

Backstage

Von Claudia Fischer

Foto: Justus Holzberger, cc by-sa 4.0

Der Technik-Raum während der BigBrotherAward-Gala. Die Crew links betreut Presse, Blog und Internetseite und schaltet live die Texte frei. Rechts arbeitet das Team „Livestream und Bebilderung“.

Hektisch wird es immer, kurz vor der Verleihungsgala. Auch wenn „die Crew“, wie das Aufbauteam genannt wird, beim Stühlerücken, Lichtaufbau und Sektflaschenverteilen inzwischen sehr eingespielt ist. „Dieses Jahr kamen die Jungs von der Parkour-Gruppe erst auf den letzten Drücker“, erinnert sich Nils Büschke. „Das waren die Artisten, die uns in den Pausen gezeigt haben, wie man Hürden nimmt.“ Parkour ist eine Sportart, bei der man Hindernisse nur mit eigener Körperkraft überwindet – als die jungen Männer aus Gütersloh dann während der Gala über die Bühne flogen, sah das fast schwerelos aus. „Aber die riesigen Kisten, die sie dabei hatten, waren ganz schön schwer! Und wir haben sie quasi in der letzten Minute noch auf die Bühne gewuppt.“

Während am Veranstaltungsort in der Bielefelder Hechelei nach und nach die Kamerateams, Übersetzer, Livestream-Betreuer.innen und Jury-Mitglieder eintrafen und die letzten Tonproben gemacht wurden, hatten Rena Tangens und padeluun in der Marktstraße schon eine erste Presseschau hinter sich. Ungewöhnlich, denn eigentlich veröffentlichen die Medien keine Preisträger vorab. 2017 allerdings gab es eine Klageandrohung von DİTİB, und einige Medien hatten dies vor Ablauf der Sperrfrist schon veröffentlicht. Mehr dazu lesen Sie im Update zur DİTİB-Laudatio von Thilo Weichert.

Inhaltlich standen die Preisträger dieses Jahr recht eindeutig fest – Dank der professionellen Vorbereitung im Digitalcourage-Büro-Team. „Wir hatten im Herbst 2016 den Recherche-Spezialisten Albrecht Ude exklusiv bei uns für ein Seminar. Danach haben wir einen Ablaufplan entwickelt, wie wir für die BigBrotherAwards vorgehen, was wir prüfen und welche Quellen wir nutzen wollen“, erklärt Rena Tangens. „Damit haben wir die Arbeit der

Jury sehr gut vorbereitet, so dass wir uns flott und fundiert einigen konnten, wer dieses Jahr preiswürdig ist. “Insgesamt, da war sich die fast ausnahmslos ehrenamtliche, stresserprobte Crew im Nachhinein einig: „2017 ist alles ziemlich perfekt gelaufen.“

2018 ziehen die BigBrotherAwards um, aus der Hechelei ins Stadttheater Bielefeld. Live-Streaming, Bühnenbild, Publikumsraum – alles muss neu gestaltet und geplant werden. Die Vorbereitungen dafür haben schon kurz nach der 2017er Gala angefangen.

Foto: Nils Büschke, cc by-sa 4.0

Die Jury der BigBrotherAwards 2017 Von links nach rechts:

- **padeluun**, Digitalcourage
- **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.
- **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.
- **Rena Tangens**, Digitalcourage
- **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.
- **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.

Kategorie Arbeitswelt:

Die PLT Planung für Logistik und Transport GmbH

Von Prof. Dr. Peter Wedde

Der BigBrotherAward 2017 in der Kategorie Arbeit geht an die **PLT – Planung für Logistik Transport GmbH,** weil sie mit dem PLT Personal Tracker ein Gerät anbietet, dass eine „*minutengenaue*“ und „*unterbrechungsfreie Spurenverfolgung*“ von Außendienstmitarbeiterinnen und -mitarbeitern ermöglicht. Dies führt zu einer lückenlosen Totalkontrolle der Beschäftigten, die dieses Gerät bei sich tragen müssen.

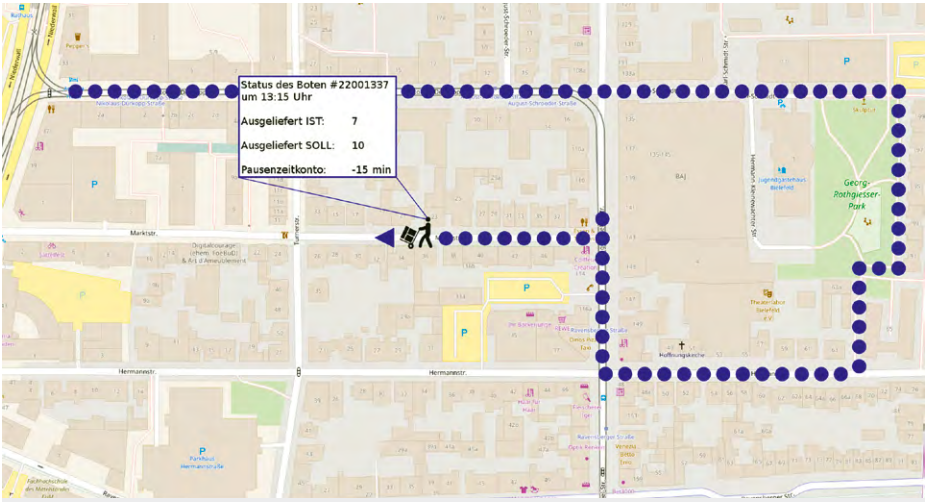
Der Tracker ist nur wenige Zentimeter groß, enthält einen GPS-Empfänger, ein GSM/GPRS-Modem, einen leistungsfähigen Akku und einen internen Datenspeicher, damit die Tourdaten von Beschäftigten auch dann abrufbar sind, wenn das Mobilfunknetz ausfällt.

Besonders komfortabel ist die Echtzeit-Ortung, wenn die von PLT ebenfalls angebotene Begleitsoftware „TrackPilot“ verwendet wird. Mit dem im „TrackPilot“ integrierten „*sehr genauen Kartenmaterial*“ können sich Arbeitgeber beispielsweise die von Beschäftigten absolvierte Strecke „*exakt*“ anzeigen lassen. Den Anwendern werden nach Aussage von PLT auf diesem Weg neben „*exakten Fahrtenbüchern und Arbeitszeitberichten zahlreiche Auswertungen und Statistiken geliefert, um Personal und Fuhrpark wirkungsvoll zu steuern.*“ Mit wenigen Klicks können hier verschiedene Berichte generiert und auf Wunsch exportiert werden. Durch das versprochene „*metergenaue* Tracking“ kann dabei beispielsweise erkannt werden, in welchem Tempo sich Zeitungsausträger oder Zusteller bewegen, wie lange sie an einer Haustür oder in einem Büro verweilen oder wann sie eine Pause machen.

Laudator: Prof. Dr. Peter Wedde

Foto: Fabian Kurz cc by-sa 4.0

Die Firma PLT erhält den BBA 2017 stellvertretend für alle Anbieter dieser Art von Überwachungstechnik, die ohne Rück-



Grafik: Stephan Porada cc by-sa 4.0, Stadtplan OpenStreetMap, Paketbote Dieter Petereit

Die metergenaue Wegverfolgung (Das Tracking) von Beschäftigten ist verboten!

sicht auf die Rechte von Beschäftigten eingesetzt wird. Unsere Preisverleihung soll diesen Trend stoppen.

PLT hat den BigBrotherAward besonders verdient, weil diese Firma in ihrer Werbung gesetzliche Vorschriften verfälscht, um den Einsatz von Personal Trackern nicht nur als gesetzeskonform, sondern quasi als gesetzlich erforderlich darzustellen. So behauptet PLT auf seiner Webseite:

„Insbesondere das neue Mindestlohngesetz (MiLoG), welches am 01.01.2015 in Kraft trat, macht es in vielen Branchen notwendig, die Arbeitszeiten der Mitarbeiter zu überwachen und minutengenau zu dokumentieren, damit später bewiesen werden kann, dass auch tatsächlich der Mindestlohn i. H. v. 8,50 Euro gezahlt wurde. Daraus erwächst in einigen Branchen ein immenser Mehraufwand, nur um die Einhaltung des Gesetzes zu dokumentieren und den Nachweispflichten nachzukommen. Besonders hart betroffen sind vom Mindestlohn Zustelldienste und Zusteller der Zeitungslogistik und Brieflogistik. Die tatsächlichen Arbeitszeiten der Zeitungszusteller müssen aufgezeichnet und für Prüfungen des Zoll mindestens 10 Jahre vorgehalten werden."

▶Diese Werbeaussage ist eine echte „Fake News".◀

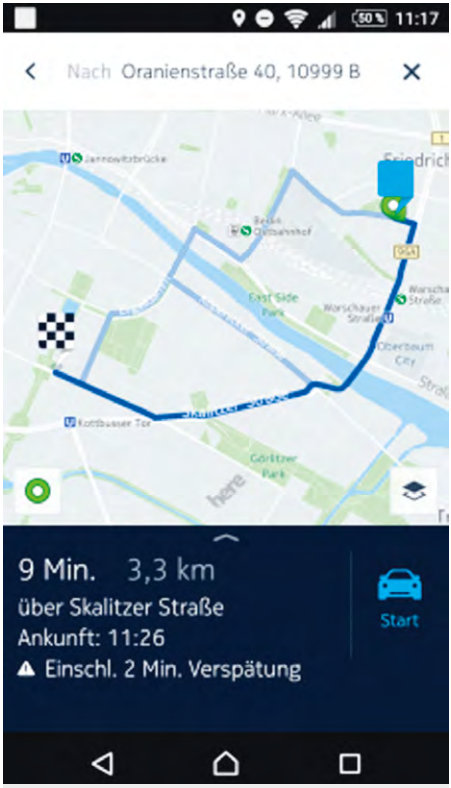
Diese Werbeaussage ist eine echte „Fake News": Richtig ist hieran eigentlich nur die Information, dass das Mindestlohngesetz (MiLoG) Arbeitgebern mit Wirkung vom 1. Januar 2015 bestimmte Nachweispflichten auferlegt. Nach § 17 Abs. 1 dieses Gesetzes sind sie verpflichtet,

„Beginn, Ende und Dauer der täglichen Arbeitszeit dieser Arbeitnehmerinnen und Arbeitnehmer spätestens bis zum

Ablauf des siebten auf den Tag der Arbeitsleistung folgenden Kalendertages aufzuzeichnen und diese Aufzeichnungen mindestens zwei Jahre beginnend ab dem für die Aufzeichnung maßgeblichen Zeitpunkt aufzubewahren".

Dazu reicht es, wenn die Beschäftigten einen Stundenzettel ausfüllen, wie sie es seit Jahrzehnten tun. Von einer Verpflichtung zur „*minutengenauen*" Überwachung der Arbeitszeit ist hingegen im MiLoG ebenso wenig die Rede wie von einem Recht der Arbeitgeber, den genauen Standort von Beschäftigten permanent zu erfassen. Auch eine angebliche „zehnjährige Aufbewahrungspflicht" gibt es schlicht nicht, auch nicht „für den Zoll". Was die Firma PLT da auf ihrer WEB-Seite schreibt, ist damit eine plumpe Verfälschung der gesetzlichen Situation.

Die vollmundigen Werbeaussagen auf der PLT-Website ändern aber nichts an der eindeutigen arbeits- und datenschutzrechtlichen Situation, nach der eine permanente und metergenaue elektronische Totalüberwachung des Standorts und der Bewegungen von Beschäftigten in den allermeisten Fällen verboten ist. Datenschutzrechtlich zulässig ist eine exakte Online-Ortung von Menschen nur in wenigen Ausnahmen, etwa für Besatzungen von vollgepackten Geldtransportern oder für Berufsfeuerwehrleute während des Einsatzes in einem brennenden Haus. Für „normale" Beschäftigte wie etwa für Auslieferungsfahrer ist es völlig ausreichend, wenn ihr ungefährer Standort oder ihre ungefähre Ankunftszeit bei Kunden an die Zentrale übermittelt wird.



Quelle: Webseite PLT April 2017

Ein Screenshot aus der PLT-Software "Trackpilot Go!"

Das minuten- und metergenaue Tracking, dass der PLT Personal Tracker verspricht, trifft damit auf leicht erkennbare und eindeutige rechtliche Grenzen. Für die Branchen, die PLT auf seiner Webseite nennt:

„Winterdienst (Handtouren), Wachdienst, Objektschutz, Gebietsbestreifung, Agrar- und Forstbetrieb, Sportveranstaltungen oder Zustelldienst, Zusteller der Zeitungslogistik und Brieflogistik."

gibt es keine gesetzliche Erlaubnis. Deshalb ist der Einsatz von Personaltrackern in derartigen Fällen arbeitsrechtlich und datenschutzrechtlich unzulässig.

▶Der Einsatz von Personal Trackern zur Totalkontrolle von Beschäftigten ist menschenunwürdig, rechtswidrig und sinnlos.◀

Umso erstaunlicher ist es, dass der Personal Tracker laut der Web-Seite von PLT bereits vielfach „legal" eingesetzt werden soll:

„Bereits etliche Zustelldienste haben Ihre Zusteller mit dem PLT Personal Tracker ausgestattet und eine entsprechende interne Betriebsvereinbarung getroffen. Danach werden die zurückgelegten Zustelltouren der Zeitungsausträger metergenau getrackt und im TrackPilot Ortungssystem zu übersichtlichen Arbeitszeitberichten verarbeitet. Die Berichte können in Dateiform gespeichert und dauerhaft archiviert werden."

Der Hinweis auf Betriebsvereinbarungen, durch die ein metergenaues persönliches Tracking von Zustellern erlaubt wird, hat uns verblüfft. Das würde ja bedeuten, dass Betriebsräte einer Form der Totalüberwachung zugestimmt hätten, die nach der Rechtsprechung des Bundesverfassungsgerichts und des Bundesarbeitsgerichts in Arbeitsverhältnissen unzulässig ist.

Deshalb haben wir uns den auf der PLT-Website hinterlegten Link „*Betriebsvereinbarungen*" genauer angesehen. Erwartet hätten wir hier eine Referenzliste mit Formulierungsbeispielen aus bereits abgeschlossenen Betriebsvereinbarungen. Stattdessen finden sich hier aber nur allgemeine Hinweise auf deren mögliche Regelungsinhalte sowie auf rechtliche Probleme. Auch dieser Teil der PLT-Präsentation ist wiederum eine geschickte Marketingaussage, die vorgaukelt, dass rechtlich alles in Ordnung ist.

Seltsam mutet auch die folgende Formulierung an:

„Durch die extrem kleinen Abmaße lässt sich das Gerät sehr leicht am Körper tragen oder versteckt positionieren und passt in jede Hosentasche."

Wieso weist die Firma PLT darauf hin, dass es möglich ist, den Personal Tracker etwa auch versteckt in einem Auslieferungswagen oder in einer Tragetasche unterzubringen? Die Ortung könnte dann ohne Wissen der Beschäftigten erfolgen. Dies aber wäre nach geltender Rechtslage definitiv unzulässig.

Der Einsatz von Personal Trackern zur Totalkontrolle von Beschäftigten – sei es das Gerät von PLT oder auch von ei-

Foto: Justus Holzberger, cc by-sa 4.0

Dr. Peter Wedde kritisiert Kontrollwahn und übertriebenes Misstrauen von Arbeitgebern.

ner anderen Firma – ist menschenunwürdig, rechtswidrig und sinnlos. Diese Geräte sind genau wie durch Videokameras „totalüberwachte“ Arbeitsplätze Ausdruck des überbordenden Kontrollwahns und des übertriebenen Misstrauens von Arbeitgebern, die meinen, jeden Meter und jede Minute der Arbeit ihrer Beschäftigten überwachen und erfassen zu müssen.

Hinzu kommt: Es gibt weder die von PLT behauptete gesetzliche Erfordernis, noch beinhaltet etwa die meter- und minutengenaue Erfassung eines Briefträgers ein nennenswertes Einsparpotenzial für die Unternehmen. Ganz im Gegenteil: Derartige Kontrollen kosten zunächst einmal Geld. Firmen wie PLT verdienen am Kontrollwahn von Arbeitgebern und an der absurden, aber weit verbreiten Logik „Überwachung gleich Sicherheit“. Die angebotene Überwachungstechnologie wird auf Kosten der Persönlichkeitsrechte der Arbeitnehmerinnen und Arbeitnehmer vermarktet.

Hoffentlich können wir mit diesem BigBrotherAward einige Firmenchefs und -chefinnen davor bewahren, auf diese Propaganda herein zu fallen. Probieren Sie es doch einmal anders: Vermitteln Sie Ihren Beschäftigten Vertrauen und Wertschätzung. Optimieren Sie mit ihnen zusammen Routenführungen und entwickeln sie mögliche Effizienz-Steigerungen gemeinsam. Nehmen Sie ernst, dass diese Menschen ihre Touren und Arbeitsabläufe am besten kennen. Das wirkt sich mit Sicherheit positiv auf die Arbeitsmotivation aus – und steigert das Arbeitstempo vielleicht ganz ohne Zusatzkosten.

- Herzlichen Glückwunsch zum BigBrotherAward 2017, Firma PLT – Planung für Logistik und Transport GmbH.

Wie es weiter ging:

Von Claudia Fischer

Kommentare unseres Publikums:

- „Hier war die Wirkung der Datenerfassung am deutlichsten und eindrücklichsten sichtbar. Ganz unübersehbar – auch für Menschen, die sich ansonsten wenig damit befassen."
- „Dem Kontrollwahn der Arbeitgeber muss etwas entgegengesetzt werden. Schon jetzt zeichnet sich eine Zweiteilung der Arbeitswelt ab – in ein Dienstleistungsprekariat und dessen Management."
- „Ich bin für Vertrauen und Respekt. Ausbeutung ist demotivierend. Ich freue mich, Mitarbeiterin bei einem Unternehmen zu sein, dem respektvoller Umgang wichtig ist."

„Ich bin für Vertrauen und Respekt. Ausbeutung ist demotivierend."

Die Firma PLT hat uns einen Brief geschrieben

Darin bedauert sie unsere kurzfristige Einladung zur Preisverleihung und erklärt, dass der Personal Tracker unter Beachtung von Datenschutzgesetzen und für Transparenz von Zeitbedarf für die Zusteller.innen eingesetzt würde. Wir zitieren: „Es geht nicht darum, Mitarbeiter auf Schritt und Tritt zu verfolgen, sondern um sicherzustellen, dass die geplante Zeit auch wirklich ausreichend ist. Insofern möchten wir doch den in der Begründung verwendeten Begriff ‚menschenunwürdig' zurückweisen." Die Firma bekräftigt ihre Aussage, dass das Mindestlohngesetz eine exaktere Dokumentation nötig macht. Und weiter heißt es: „Wir nehmen den Preis mit einem gewissen Augenzwinkern an und sehen uns an unsere Verantwortung als Marktführer ermahnt, wirtschaftlichen Erfolg nie über den Schutz und die Würde des Einzelnen zu stellen."

Peter Wedde dazu: „Ein gewisses Augenzwinkern zum Thema Beschäftigtendatenschutz geht allein auf Kosten der Betroffenen. Mitarbeiter.innen, die mit Geräten von PLT permanent oder heimlich kontrolliert werden, finden das sicher überhaupt nicht komisch." „Dass die Firma PLT in ihrem Schreiben immer noch auf das Mindestlohngesetz verweist, macht deutlich, dass der Preis gerechtfertigt ist. An anderer Stelle in dieser Antwort begrüßen sie, dass § 32g Bundesdatenschutzgesetz (BDSG) (Ortungssysteme) den Einsatz von GPS-Empfängern regelt.

- Diesen Paragrafen gibt es im BDSG aber gar nicht. PLT beruft sich da auf einen Gesetzentwurf der vorletzten Bundesregierung aus CDU/CSU und FDP. Er stammt also aus der Zeit vor 2013 und ist nicht geltende Rechtslage. Im Gegenteil: Dieser Entwurf wurde nie vom Bundestag verabschiedet und ist längst in irgendeiner Schublade verschwunden. Und damit argumentiert PLT heute noch? Das spricht nicht für ihre Kompetenz in Sachen Datenschutz!

Kategorie Wirtschaft:

Der IT-Branchenverband Bitkom

Von Rena Tangens

Foto: Fabian Kurz cc by-sa 4.0

Laudatorin: Rena Tangens

Der BigBrotherAward 2017 in der Kategorie Wirtschaft geht an den deutschen **IT-Branchenverband Bitkom,** vertreten durch seinen Präsidenten Thorsten Dirks.

Der IT-Branchenverband erhält diesen BigBrotherAward für sein unkritisches Promoten von Big Data, seine penetrante Lobbyarbeit gegen Datenschutz und weil er de facto eine Tarnorganisation großer US-Konzerne ist, die bei Bitkom das Sagen haben.

Bitkom – wer ist das überhaupt, was machen die? Hier im Stakkato: Bitkom ist der IT-Branchenverband in Deutschland, wurde 1999 gegründet, hat rund 1.600 Mitglieder, veranstaltet den jährlichen „IT-Gipfel“ mit der Bundesregierung, macht Studien, wird von der Bundesregierung immer gefragt, wenn „irgendwas mit Computern“ zur Debatte steht und hat beste Beziehungen zur Politik.

Und was meint Bitkom zum Datenschutz?

Datenschutz – findet Bitkom – „passt nicht in die heutige Zeit“, ist „veraltet“, „analog“, „letztes Jahrhundert“, überreguliert und nicht mehr zeitgemäß. *(Anmerkung: Quellennachweise finden Sie auf unserer Webseite)*

Hier bestimmt offenbar das Sein das Bewusstsein. Einbrecher finden auch, dass das Prinzip des Eigentums veraltet sei.

Aber lassen wir die Bitkom-Vertreter.innen doch selber zu Wort kommen:
Zitat Bitkom-Hauptgeschäftsführer Dr. *Bernhard Rohleder*:

> *„Selbstverständlich kann es nicht darum gehen, den Datenschutz abzuschaffen. Im Gegenteil: Je stärker Daten eingesetzt werden, umso stärker müssen sie gegen Missbrauch geschützt werden – rechtlich, technisch, organisatorisch. Genau diese Unterscheidung aber wird kaum gemacht: Sinnvoller Gebrauch gegen unerwünschten Missbrauch.“*

Doch halt – wer entscheidet eigentlich, was „Missbrauch“ und was „sinnvoller Gebrauch“ ist? Im Klartext heißt das vermutlich: „Um Ihre Daten zu schützen, müssen wir sie erstmal haben! Also her mit Ihren Daten, denn wir machen was Sinnvolles damit, nämlich Geld! Wenn jemand anderes an unseren Datenschatz heranwill, dann ist das Missbrauch.“

▶„Um Ihre Daten zu schützen, müssen wir sie erstmal haben!“◀

Nächstes Zitat: *Dieter Kempf*, Ex-Bitkom-Präsident, beim *Safer Internet Day* 2015:

> *„Ob das Konzept der Datensparsamkeit heute noch in dieser Absolutheit sinnvoll und geeignet ist, moderne Datenverarbeitung zu regulieren, muss man auch einmal fragen dürfen.“*

Bitkom propagiert „*Datenreichtum*“ statt Datensparsamkeit. So im Bitkom-Positionspapier zur „Digitalen Souveränität“. Zitat:

> *„Zwei Grundprinzipien des Datenschutzes – Datensparsamkeit und Zweckbindung – sind zu überprüfen und durch die Prinzipien der Datenvielfalt und des Datenreichtums zu ergänzen bzw. zu ersetzen.“*

Auch *Susanne Dehmel*, Mitglied der Geschäftsleitung und bei Bitkom zuständig für Datenschutz, wirbt:

> *„Lassen wir Datenreichtum zu.“*

Euphemismus-Warnung: Wer von „Datenreichtum“ spricht, verschweigt, wer eigentlich reich werden will und wer in Zukunft der Rohstoff sein soll, der ausgebeutet wird. Deshalb gab es für dieses Wort im letzten Jahr auch schon den Neusprech-Award!

Bitkom propagiert „Datensouveränität“ statt Datenschutz. So plädiert zum Beispiel Geschäftsführer Bernhard Rohleder dafür, dass „der mündige Verbraucher durch datensouveränes Verhalten entscheiden können muss“, was er nutzen und mit wem er Informationen teilen wolle.

Euphemismus-Warnung: „Datensouveränität“ ist eine schöne Idee, aber wer das sagt, tut so, als ob die Verbraucher.innen tatsächlich die Macht hätten, zu entscheiden, wer was von ihnen erfährt. Aber so ist es nicht. Mit dem Wort „souverän“ soll den Menschen suggeriert werden, dass Gesetze zu ihrem Schutz überflüssig seien und dass Verbraucherschutz Bevormundung sei.

Wer fordert, dass „Datensouveränität“ nun den Datenschutz ersetzen soll, will nicht die Persönlichkeitsrechte der Bürger schützen, sondern Datenkraken-Firmen vor wirksamen Gesetzen. Denn „souverän“ klingt nett, ist aber wolkig statt rechtsverbindlich.

Wer von „individueller Datensouveränität“ spricht, meint damit die Digitalversion des „mündigen Bürgers“ – der normalerweise nicht gefragt wird, aber der immer dann herbeizitiert wird, wenn er über den Tisch gezogen werden soll.

… magischer Feenstaub: Bitkom stäubt ihn wie Puderzucker über unsere kritische Wahrnehmung.

„Souverän" klingt erst mal gut. „Souverän" ist magischer Feenstaub und Bitkom stäubt ihn wie Puderzucker über unsere kritische Wahrnehmung. Wusch – weg sind die Persönlichkeitsrechte. Plopp – da sind die Daten als Wirtschaftsware, die die Verbraucher.innen einfach weitergeben können. Magischerweise entsteht so der Rohstoff des 21. Jahrhunderts, der aber – simsalabim – erst dann wirklichen Wert hat, wenn er in die Hände der datensammelnden Firma gerät.

Und Bitkom-Präsident *Thorsten Dirks* legt noch einen drauf:

> *„Wir wollen kein Supergrundrecht auf Datenschutz."*

Da erscheint vor meinem geistigen Auge doch gleich ein total unfaires Supergrundrecht, das die Wirtschaft drangsaliert. Jetzt mal im Ernst: Das ist doch absurd!

All dies wird immer und immer wieder wiederholt. Wir können es auch „Quengeln" nennen.

Das Schlimme ist: Das Quengeln zeigt Wirkung

Bundeskanzlerin Angela Merkel ist mittlerweile weich geworden und erfüllt dem IT-Kindergarten Bitkom jeden Wunsch. Denn diese Kinder behaupten ja, unsere Zukunft zu sein.

An dem einen Rockzipfel zerren die Firmen, die Überwachungstechnik verkaufen, an dem anderen Rockzipfel die Firmen, die freie Bahn für ihr Big Business mit Big Data wollen. Als gemeinsamer Feind ist ausgemacht: Der Datenschutz, der die Bürgerinnen und Bürger vor den schlimmsten Auswüchsen schützen soll.

Und das Quengeln wirkt nicht nur bei der Kanzlerin, sondern auch bei ihren drei Ministern, die gemeinsam fürs Digitale zuständig sind: Innenminister Thomas de Maizière, Verkehrsminister Alexander Dobrindt und (bis vor kurzem) Wirtschaftsminister Sigmar Gabriel.

Denn wenn man den Mitgliedern der Bundesregierung zuhört, dann hat man fast das Gefühl, eigentlich die Bitkom-Sprecher zu hören, die wir eben zitiert haben:

Sigmar Gabriel auf IT-Gipfel in Saarbrücken 2016:

> *„Ich glaube, dass wir uns endgültig verabschieden müssen von dem klassischen Begriff des Datenschutzes, weil der natürlich nichts anderes ist als ein Minimierungsgebot von Daten. Das ist ungefähr das Gegenteil des Geschäftsmodells von Big Data. Aber das heißt nicht Aufgabe jeder Form, sondern, statt Datenschutz ‚Datensouveränität' zum Gegenstand von Politik und Umgang mit Daten zu machen."*

Bundesverkehrsminister *Alexander Dobrindt* auf einem Empfang von Bitkom:

> *„Der bisher gültige Grundsatz, dass Datensparsamkeit das Übermaß der Dinge ist, der hat sich überholt, der muss weg. Datenreichtum muss der Maßstab sein,*

nach dem wir unsere Politik ausrichten.“ Dafür wolle sich die Regierung zusammen mit Bitkom einsetzen.

„Wenn wir es nicht machen, machen es andere,“ sagt Thomas de Maizière in seiner Bundestagsrede zum BDSG-Anpassungsgesetz. Das ist allerdings ein Argument, das man auch als Entschuldigung für Waffenhandel, Zuhälterei und Drogen-Dealen anführen könnte – und das wir nichtsdestotrotz moralisch verwerflich finden.

Bitkom genießt seinen Einfluss auf die Regierung. Manchmal ein bisschen zu sehr. So sagte ein Bitkom-Vertreter bei einer Anhörung zum E-Government-Gesetz triumphierend: „Was soll ich denn gegen ein Gesetz sagen, das ich selbst geschrieben habe?!“ Niemand bei der Anhörung schien Anstoß daran zu nehmen – soweit geht die Selbstverständlichkeit der Lobby-Einflussnahme.

Und nun raten Sie mal, was als nächstes kommt in unserer Liste der Kritik-Punkte:

▶Die altbekannte Strategie der „freiwilligen Selbstverpflichtung der Wirtschaft“.

Für die Einflussnahme in Brüssel hat Bitkom den gemeinnützigen Verein „Selbstregulierung Informationswirtschaft e.V.“, kurz SRIW, gegründet, der sich für „Selbst- und Ko-Regulierung“ einsetzt, unter anderem in einem Ausschuss der EU-Kommission. Neben Bitkom gehören zum Verein SRIW: die Deutsche Telekom, DHL, Map & Route, zwei Unternehmen für Panoramabilder, Vermessung und Georeferenzierung à la Streetview – und, ja genau: Google.

▶Freie Bahn für Big Data

Und damit wird offensichtlich, worum geht es bei der Bitkom-Lobbyarbeit eigentlich geht: Um freie Bahn für Big Data Geschäftsmodelle. Big Data bedeutet: Jede Menge Daten werden über uns en passant gesammelt. Auf diese gemischten Daten wollen Firmen ihre Algorithmen loslassen und schauen, ob sie interessante Muster erkennen können.

Aus den gesammelten Daten werden Schlussfolgerungen über unser Verhalten und unsere Motive sowie Prognosen über unser zukünftiges Verhalten angestellt. Und diese Prognosen werden von denen verwendet, die sie zu ihrem Vorteil nutzen können. Wir werden nicht mehr gefragt. Big Data **nimmt** uns unsere Souveränität.

Rührend, wie immer wieder nach guten Zwecken gesucht wird, für die Big Data angeblich die Lösung sein soll: Gesundheit, bessere Verkehrsleitung, medizinischen Erkenntnisse, betrügerische Gebrauchtwagenhändler identifizieren, … ach ja, Arbeitsplätze natürlich auch.

Big Data ist ein Euphemismus. Denn eigentlich geht es um die Enteignung von Menschen – um die Enteignung von ihren Daten, von ihren Motiven, von ihren Wünschen, Plänen und Träumen und um die Enteignung von ihren eigenen Entscheidungen. Es geht um Manipulation und Kontrolle. Es geht darum, Claims abzustecken.

Grafik: Stephan Porada cc by-sa 4.0, Figuren www.noupe.com, Dieter Petereit

Fünf von 16 Menschen im Präsidium des Deutschen IT-Branchenverbandes Bitkom vertreten eigentlich US-Firmen.

Aber Lobbyarbeit ist doch Bitkoms Aufgabe?

Klar – sie machen ihren Job. Aber sie machen ihn schlecht! Denn sie arbeiten nicht nur gegen Grundrechte und soziale Gerechtigkeit, sondern sie schaden letzten Endes auch der deutschen und europäischen IT-Wirtschaft. Denn der Wildwuchs an Datenaneignung zerrüttet das Vertrauen der Nutzer.innen – Misstrauen und mangelnde Akzeptanz werden die langfristige Folge sein.

Die Lobbyisten von Bitkom tun so, als ob **wir** Angst vor Neuerungen hätten. Dabei sind **sie** es, die nicht den Mut haben, eigene Lösungen zu erdenken und Dinge anders zu machen als die großen Brüder in den USA. Warum nutzen sie nicht die Vorteile, die deutsche und europäische Unternehmen haben, weil sie seit langem mit Datenschutz, Verbraucherschutz, Arbeitnehmerrechten, Umweltschutz und anderen Werten vertraut sind? Mit der Europäischen Datenschutzgrundverordnung gilt ab 2018 das Marktortprinzip. Das heißt, alle, die in Europa Geschäfte machen wollen, müssen sich an die hier geltenden Datenschutzregeln halten – egal, wo ihre Firma angesiedelt ist. Auch deshalb ist „Wenn wir‘s nicht machen, machen es andere!“ ein schlechtes Argument.

Warum also sind die Bitkom-Verantwortlichen nicht selbstbewusst und bringen die deutsche Wirtschaft voran? Warum nutzen sie nicht die Qualität und die Kompetenz, die deutsche Unternehmen in diesem Bereich haben? Spannende Frage – wir haben eine mögliche Antwort:

Bei Bitkom bestimmen US-Konzerne den Kurs

8 Prozent der rund 1.600 Bitkom-Mitglieder kommen aus den USA. Das klingt erst einmal gar nicht sooo viel. Aber wenn wir nicht auf die reine Mitgliederzahl schauen, sondern **wer** diese 8 Prozent sind, die sich neben den deutschen Mittelständlern tummeln, dann sollte der Groschen fallen: Amazon, Apple, Cisco, Ebay, Facebook, Google, Hewlett Packard, IBM, Intel, Paypal, Xerox und Microsoft – die Hechte im Karpfenteich in Sachen Umsatz, Macht und Marktbeherrschung. Daneben hat‘s auch noch Marktforschungsunternehmen (Forrester), Unternehmensberatungen (Accenture), Wirtschaftsprüfer (PriceWaterhouseCoopers), Cloud- und

CRM-Anbieter (Salesforce), GPS-Navigation (Garmin), Scoringunternehmen (Fair Isaac), Trackinganbieter (Zebra Technologies) und echte Sympathieträger wie Taxi-Konkurrenz Uber.

Die Machtverhältnisse bilden sich auch im Bitkom-Präsidium ab: Von den 16 Menschen im Bitkom-Präsidium sind 5, also fast jede.r Dritte, von einer US-Tochterfirma.

Und in der Tat: Seit Jahren bestimmen US-Internetkonzerne den Kurs von Bitkom. Von dort kommen die Ressourcen. Sie sagen, wo es langgeht. Bitkom ist kein deutscher IT-Verband mehr – sondern Bitkom ist inzwischen eine Lobbyorganisation von US-Konzernen, die unter falscher Flagge segeln.

Liebe Bitkoms: Wir wünschen Ihnen mehr Mut zu einem eigenen deutschen und europäischen Weg, mehr Eigenständigkeit, eigene Visionen, echte Innovation! Besinnen Sie sich auf die eigenen Qualitäten, entmachten Sie die US-Konzerne in Ihrem Verband und hören Sie auf, gegen den Datenschutz zu quengeln.

Liebe Bundesregierung: Hören Sie auf, dem Bitkom-Kindergarten jeden Wunsch zu erfüllen, solange sich dieser nicht von dem Einfluss der US-Konzerne befreit hat. Wer quengelnden Kindern dauernd nachgibt, tut auf lange Sicht weder der Gesellschaft noch den Kindern selbst einen Gefallen.

- Möge der BigBrotherAward daran erinnern – herzlichen Glückwunsch, Bitkom!

Wie es weiter ging:

Von Claudia Fischer

Kommentare unseres Publikums:

- „Es ist unglaublich, dass die deutsche Wirtschaft so stark korrumpiert wird!“
- „Bestätigt mal wieder die Macht der Lobby und die Ohnmacht der Bürger gegenüber den gewählten Volksvertretern.“

Die Bitkom hat uns ein Videostatement geschickt

Darin erklärt Bitkom-Hauptgeschäftsführer Dr. Bernhard Rohleder: „Endlich haben wir ihn also bekommen, den BigBrotherAward. Seit 15 Jahren arbeiten wir daran und setzen uns gegen Vorratsdatenspeicherung, gegen Netzsperren und gegen Zensur im Internet ein, setzen uns aber natürlich auch dafür ein, dass es eine sinnvolle Datennutzung gibt.“ Er führt an, dass jedes Jahr in Deutschland 19.000 Menschen sterben, weil aus Datenschutzgründen auf die Einführung von elektronischen Medikationsplänen verzichtet würde. Diese Zahl haben wir nicht überprüft.

padeluun:

- „Ich hatte auch persönlich Kontakt mit Herrn Rohleder. Die Bitkom möchte den BigBrotherAward gerne entgegennehmen und gut sichtbar in ihren Räumen ausstellen. Über das Wie und Wann müssen wir uns noch unterhalten.“

Kategorie Politik

Der Islamverband DİTİB

Von Dr. Thilo Weichert

Foto: Fabian Kurz, cc by-sa 4.0

Laudator: Dr. Thilo Weichert

Der BigBrotherAward 2017 in der Kategorie Politik geht an **die Türkisch-Islamische Union der Anstalt für Religion e.V., kurz DİTİB,** vertreten durch den DİTİB-Generalsekretär Dr. Bekir Alboğa, weil bei der DİTİB tätige Imame für türkische Behörden und den Geheimdienst MİT ihre Mitglieder und Besucher ausgehorcht und sie so der Verfolgung durch türkisch-staatliche Stellen ausgeliefert haben sollen.

Dieser BigBrotherAward ist etwas Besonderes. Denn er richtet sich diesmal nicht – wie Sie es von uns gewohnt sind – gegen eine Datenkrake, die erst durch die digitale Welt möglich wurde und technischer Voraussetzungen bedarf. Nein, hier geht es um handfestes Bespitzeln, um das Ausnutzen menschlicher Kontakte von Angesicht zu Angesicht, und das im Rahmen einer religiösen Gemeinschaft.

Religionsausübung, freie Meinungsäußerung und soziales Leben, „Real Life“, wie es heute heißt – mit der Spionage durch DİTİB-Imame sind elementare Grund- und Menschenrechte in Deutschland missbraucht worden, um dem Wunsch einer Regierungsbehörde in der Türkei nachzukommen.

Was ist passiert?

Im Dezember 2016 veröffentlichte die regierungskritische türkische Zeitung „Cumhuriyet“ Dokumente, die belegen, dass Imame des in Deutschland eingetragenen Vereins DİTİB Informationen über ihre Mitglieder und Besucher gesammelt und an türkische Behörden weitergegeben haben. Im Mittelpunkt des Interesses standen dabei vermutete Anhänger des Predigers Fethullah Gülen. Die türkische Regierung wirft der Gülen-Bewegung vor, für den militärischen Putschversuch im Juli 2016 in der Türkei verantwortlich zu sein. Nachweise hierfür wurden bisher nicht vorgelegt.

In den Spitzelberichten der Imame werden detaillierte Informationen über vermeintli-

Foto: Raimond Spekking, cc by-sa 4.0

Sitz der DİTİB:
Die Zentralmoschee in Köln

che Gülen-Anhänger gegeben, z.B. mit Details über deren Moscheebesuche sowie auch zu deren Verbindung in der Türkei. Eine Nachhilfeeinrichtung für Kinder wurde in den Spitzelberichten als „Hort des Bösen“ beschrieben. Gemäß einem Bericht des Landesamtes für Verfassungsschutz Nordrhein-Westfalen sind von den Denunziationen mindestens auch fünf Lehrkräfte mit deutscher Staatsangehörigkeit betroffen. Die ausspionierten Menschen, die über diese Erkenntnisse von deutschen Stellen informiert wurden, dementierten, mit Gülen zu sympathisieren.

Die für DİTİB tätigen Imame sind türkische Staatsbeamte und der türkischen Religionsbehörde Diyanet unterstellt. Ihre Spitzelberichte gehen auf eine Aufforderung der Diyanet an die Botschaften und Generalkonsulate vom September 2016 zurück. Aus den Berichten kann aber geschlossen werden, dass die Spitzelei durch DİTİB für türkische Behörden schon seit längerer Zeit stattfindet.

Nach der Veröffentlichung durch „Cumhuriyet“ im Dezember 2016 erhob der grüne Bundestagsabgeordnete Volker Beck umgehend Anzeige bei der Generalbundesanwaltschaft wegen Spionageverdachts gemäß § 99 StGB (Geheimdienstliche Agententätigkeit). Erst Wochen später wurden Ermittlungen eingeleitet. Eine polizeiliche Durchsuchung in den Wohnungen von vier Imamen erfolgte erst am 15. Februar 2017, nachdem Bundeskanzlerin Angela Merkel von ihrem Türkeibesuch zurückgekehrt war. Inzwischen hatten sich sechs stark Verdächtige der damals insgesamt 16 von der Bundesanwaltschaft Beschuldigten auf Direktive von Diyanet zurück in die Türkei begeben.

DİTİB sprach nach Bekanntwerden der Spitzelberichte zunächst empört von Unterstellungen. Wenig später erklärte der DİTİB-Generalsekretär Bekir Alboğa, die „schwerwiegenden Vorwürfe“ würden „sauber und transparent“ untersucht. Er räumte ein, es habe zwar Berichte gegeben, was aber eine auf einem „Missverständnis“ beruhende „Panne“ gewesen sei. Wiederum wenig später dementierte Alboğa, die Spitzeleien bestätigt zu haben.

In ihren spärlichen Pressemitteilungen zum Thema betont die DİTİB immer wieder, dass es sich um Privat-Aktivitäten von Imamen der Diyanet gehandelt habe und es keinerlei organisatorische Mitwirkung der DİTİB gegeben habe. Verantwortung für das, was in ihren Räumlichkeiten, unter ihrem Dach passiert ist, übernimmt

Collage: Stephan Porada, cc by-sa 4.0, Karte: OpenStreetMap, Männchen: Dieter Petereit

Sechs von 16 Beschuldigten waren bereits zurück in die Türkei beordert worden, als die Ermittlungen offiziell begannen.

sie nicht. Ein Bedauern oder ein Verurteilen von Spionage-Aktivitäten in DİTİB-Moscheen liegt uns ebenfalls nicht vor.

Der Präsident der Religionsbehörde Diyanet, Mehmet Görmez, erklärte: „Es gibt keine Spionagetätigkeit“. Die zurückbeorderten Imame hätten zwar ihre Kompetenzen überschritten, sich aber nicht strafbar gemacht. Er sei „sehr traurig“ darüber, dass die Bemühungen, die Moscheegemeinde in Deutschland zu schützen, als Spionagetätigkeit bezeichnet werden. DİTİB arbeite seit Jahrzehnten auf der „Grundlage des Rechts“. Für ihn sei nicht vorstellbar, dass der Moscheeverein Recht ignoriere. Die DİTİB erklärte die Affäre für intern aufgeklärt.

Der türkische Justizminister Bekir Bozdağ verurteilte derweil die polizeilichen Durchsuchungen bei den Imamen als „klaren Verstoß gegen internationale Abkommen und die deutsche Verfassung“, in der die Religions- und Glaubensfreiheit festgeschrieben sei.

Die Spitzelberichte der Imame sind Bestandteil einer umfassenderen geheimdienstlichen Ausforschung durch die Türkei und insbesondere des dortigen Geheimdienstes MİT, der in Deutschland, so ein namentlich nicht genannter „einflussreicher Sicherheitspolitiker“ in der „Welt am Sonntag“, ca. 6.000 Informanten beschäftigt. Die deutschen Sicherheitsbehörden gehen demgemäß davon aus, dass in Deutschland rund 150 MİT-Mitarbeiter an der türkischen Botschaft und an den Konsulaten arbeiten. Gemäß der Gewerkschaft Erziehung und Wissenschaft sollen in Nordrhein-Westfalen türkische Schülerinnen und Schüler gar aufgefordert worden sein, regierungskritische Äußerungen ihrer Lehrer heimlich zu filmen und an die Generalkonsulate weiterzumelden.

Ziel der MİT-Aktivitäten ist die Überwachung der Türkinnen und Türken in Deutschland, deren Beeinflussung pro Erdoğan, die Einschüchterung und Isolierung von Regierungsgegnern sowie die Einflussnahme auf die deutschen Behörden und auf die hier bestehende öffentliche Meinung. In Deutschland ausspionierte vermeintliche Regimegegner haben im Fall einer Reise in die Türkei eine Verhaftung, Strafverfahren und entwürdigende Behandlung, evtl. gar Folter zu befürchten. Angehörigen in der Türkei drohen Repressalien. Und auch bundesdeutsche Politikerinnen und Politiker wie Cem Özdemir von den Grünen, Michelle Müntefering von der SPD oder Emine Demirbüken-Wegner von der CDU stehen unter Beobachtung des MİT wegen angeblicher Sympathie für die Gülen-Bewegung.

Die deutschen Behörden nehmen Rücksicht auf die Befindlichkeiten der türkischen Regierung, nicht zuletzt, um das ausgehandelte Flüchtlingsabkommen, mit dem die sogenannte „Balkanroute“ blockiert werden soll, nicht zu gefährden. Auch die DİTİB wird geschont, um den Gesprächsfaden mit den Islamverbänden in Deutschland aufrecht zu halten. Dessen ungeachtet haben die Generalbundesanwaltschaft und die Polizei Ermittlungen aufgenommen und erste Schritte zur Verfolgung der Verletzungen der Rechte der ausspionierten Menschen und zu deren Schutz ergriffen.

Von den deutschen Behörden werden hier aber – das ist offensichtlich – vorrangig diplomatische Interessen verfolgt. Diese hochpolitischen Interessen dürfen nicht dazu führen, dass die schutzwürdigen Persönlichkeits- und Menschenrechte der einzelnen, ausspionierten Moscheebesucherinnen und -besucher geopfert werden.

Es ist fatal, wenn Menschen durch ein Ausspionieren an der Ausübung ihrer Religion gehindert werden. DİTİB darf ihre Spitzel-Affäre nicht für beendet erklären, muss die internen Vorgänge transparent machen und sich der öffentlichen Kritik stellen. Wir machen es uns aber zu einfach, wenn wir nur Forderungen an DİTİB stellen. Auch der deutsche Staat und die deutsche Gesellschaft müssen sich bewegen und den Weg für eine freie islamische Religionsausübung ebnen – z.B. durch die Förderung politisch unabhängiger islamischer Religionsgemeinschaften.

Grafik: Panthermedia

Deutsche Sicherheitsbehörden gehen davon aus, dass rund 150 MİT-Mitarbeiter an der türkischen Botschaft und an den Konsulaten arbeiten.

Eine Umkehr und Aufarbeitung bei DİTİB ist nur möglich, wenn sich die türkisch-islamische Union von der Abhängigkeit und der Einflussnahme durch türkische Behörden wie der Diyanet befreit. Hiervon müssen auch die deutschen Stellen abhängig machen, ob sie die DİTİB weiterhin als Ansprechpartnerin akzeptieren. Zugleich müssen alle Spionageaktivitäten, auch wenn sie unter dem Dach von religiösen Organisationen erfolgen, vollständig aufgeklärt und vor allem auch strafrechtlich, nicht nur organisationsintern verfolgt und ohne diplomatische Rücksicht angeklagt werden. Inzwischen gibt es zwanzig konkrete strafrechtliche Ermittlungsverfahren. Spionage verstößt gegen deutsches Strafrecht und ist keine „interne Angelegenheit“.

Informationelle Grundrechte gelten nicht nur für Deutsche, sondern für alle. Diese müssen sich in Deutschland angstfrei friedlich religiös und politisch betätigen können.

- Dass sie dies nicht können, dafür gebührt der DİTİB der BigBrotherAward des Jahres 2017 in der Kategorie Politik. Herzlichen Glückwunsch!

Wie es weiter ging:

Von Claudia Fischer

Kommentare unseres Publikums:

- „Besonders am Beispiel DİTİB wird deutlich, wie sehr man persönliche Daten missbrauchen kann."
- „Wirklich mutig! Hier geht es um Menschenleben! Gegen Bespitzelung und Diktatoren! Weiter so!"
- „Meinungsfreiheit ist eins der wichtigsten Grundrechte."

Die DİTİB hat uns einen Brief geschrieben

Einige Tage vor der Preisverleihung haben wir die DİTİB – wie alle andere Preisträger auch – über den BigBrotherAward informiert und ihnen unsere Begründung zugeschickt. Daraufhin schrieb uns die DİTİB: „Die vordergründigen Vorwürfe in dem Schreiben und die daraus resultierende Nominierung fußen auf Tatsachenverdrehung, Falschbehauptung und unzulässigen Verallgemeinerungen, die wir gerne richtstellen wollen. Diesbezüglich möchten wir auch gerne auf die Bundesstaatsanwaltschaft verweisen, die nicht gegen die DİTİB oder den DİTİB-Verband, sondern gegen einige wenige Personen diesbezüglich ermitteln. Ganz zu Recht wollen und müssen wir daher Ihre Nominierung ablehnen und wünschen Ihnen viel Erfolg auf der Suche nach echten BBA-Nominierungen."

> … nur die „Empfängerin der religiösen Dienste der Imame seitens der DIYANET"

Auf den folgenden zwei Seiten schrieb uns die DİTİB, sie sei nur die „Empfängerin der religiösen Dienste der Imame seitens der DIYANET", dass sie mit der DIYANET über den Vertrauensverlust gesprochen habe und die auffällig gewordenen Imame daraufhin abberufen worden seien. Am Ende weisen sie uns darauf hin, dass wir mit unserem Preis und der Begründung gegen die pressemäßige Prüfungs- und Sorgfaltsverpflichtung verstoßen hätten und eine Strafbarkeit nach § 186 StGB in Betracht kommen würde.

Diese Klageandrohung schien einigen Zeitungen wichtig genug, sie vor unserer Preisverleihung öffentlich zu machen. Eigentlich haben wir bei den BigBrotherAwards eine Sperrfrist vereinbart. Das bedeutet, dass die Medien zwar kurz nach unserer Information an die Preisträger selbst über unsere Preisvergabe informiert werden, dass aber bis zur Verlesung auf der Verleihungsgala keine Preisträger veröffentlicht werden. Sperrfristen sind eine absolut übliche Methode der Pressearbeit und sie werden normalerweise von den Medien auch eingehalten.

- Dass die Sperrfrist in diesem Fall unterlaufen wurde, hat unserer DİTİB-Nominierung viel öffentliche Aufmerksamkeit beschert. Weitere Kontakte mit der DİTİB direkt hat es nicht gegeben.

Kategorie Bildung:

Die Technische Universität München und die Universität München

Von Frank Rosengart

Foto: Fabian Kurz, cc by-sa 4.0

Laudator: Frank Rosengart, CCC

Der BigBrotherAward 2017 in der Kategorie Bildung geht an die **TU München und die Ludwig-Maximilians-Universität München**, vertreten durch Prof. Dr. Dr. h.c. mult. Wolfgang A. Herrmann und Prof. Dr. rer. pol. Bernd Huber für die Kooperation mit dem Online-Kurs-Anbieter Coursera.

Die Idee klingt grundsätzlich verlockend: Eine Professorin oder ein Dozent hält eine Vorlesung an der Uni. Diese Vorlesung zeichnet man „nebenbei" auf Video auf und bietet das Ergebnis interessierten Studierenden weltweit an. Diese können damit Vorlesungen hören und sehen, die an ihrem Studienort oder in ihrem Land nicht angeboten werden. „Massive Open Online Course", kurz MOOC, heißt diese Form von Bildungsglobalisierung. Die Firma Coursera aus den USA ist unbestrittener Weltmarktführer unter den Anbietern von Online-Kursen.

Eine Firma? Ja, genau, es geht dabei ums Geldverdienen. Der Abruf der meisten Vorlesungsmaterialien ist kostenlos, wenn man sich erst mal mit seinen persönlichen Daten eingeloggt hat. Bezahlen muss ein Student üblicherweise, wenn er sich die Teilnahme offiziell bestätigen lassen möchte, um sich bei seiner Uni den Besuch des Kurses für sein Studium anrechnen zu lassen. Doch lässt sich damit das große Geld verdienen?

Dazu werfen wir einen Blick in den Vertrag zwischen Coursera und – zum Beispiel – der Universität Michigan: Unter dem Kapitel „Ausblick – Monetarisierung" findet sich ein Absatz, der vorsieht, dass Coursera Firmen anbieten darf, Studierende nach bestimmten Kursen und Lernerfolgen zu filtern und diese gezielt anzusprechen. Für Firmen oder Personalagenturen eine bequeme Möglichkeit, mit potenzielle Kandidatinnen und Kandidaten für Top-Jobs zu finden und mit ihnen in Kontakt zu treten. Selbstverständlich nicht kostenlos.

Nun lässt sich bereits erahnen, welchen Datenschatz sich Coursera mit Hilfe der

Foto: Martin Kraft, cc by-sa 3.0

Die Ludwig-Maximilans-Universität in München

Hochschulen hier aufbauen kann: Die Tatsache, an welchem Kurs jemand teilnimmt und wie gut und schnell er oder sie die Prüfung dazu ablegt, sind äußerst interessante Informationen.

Aber nicht nur für Firmen ist Coursera ein Datenschatz: Die Daten der Studierenden werden in den USA gespeichert und verarbeitet. Damit dürften sie auch dem Zugriff durch US-Behörden ausgesetzt sein und können zum Beispiel Auswirkungen auf Einreisegenehmigungen usw. haben. Wie offen und transparent Coursera im Umgang mit den Daten und entsprechenden kritischen Nachfragen dazu ist, durfte ein Schweizer Professor erfahren, der versucht hat, bei Coursera eine Information über die von ihm und seinen Teilnehmern gespeicherten Daten zu bekommen: Er und sein Kurs wurde von der Online-Uni rigoros gesperrt.

Die Münchener Universitäten, die heute den BigBrotherAward bekommen, haben eine Kooperationsvereinbarung mit Coursera geschlossen. Ausgesuchte Vorlesungen werden von den Unis für die Online-Präsentation produziert und bei Coursera eingestellt. Studierende können Online-Kurse besuchen und damit Leistungspunkte für ihr Studium erwerben.

Wir bewerten die Kooperation der Münchner Hochschulen mit Coursera vor allem als eine Marketingmaßnahme. Die Hochschulen können sich dort weltweit präsentieren und stehen damit in einer Reihe internationaler Elite-Unis. Allerdings schmückt sich Coursera auch mit deren Namen.

Die Datenschutz-Problematik scheint dabei ausgeblendet zu sein. Ebenso wie eine kritische Auseinandersetzung mit der Frage, wem die produzierten Inhalte gehören und wem mögliche Einnahmen zugutekommen.

Noch ist das Kursangebot über Coursera übrigens freiwillig für die Studierenden – dieser BigBrotherAward soll eine Warnung an die Hochschulen sein, Online-Kurse bei datenschutztechnisch zweifelhaften Anbietern nicht zum Pflichtangebot für den Scheinerwerb zu machen.

Es ist eigentlich schlimm genug, wenn Bildung zum Wirtschaftsgut verkommt, indem öffentlich finanzierte Hochschulen ihr Angebot über kommerzielle Anbieter verbreiten. Falls es keine geeignete europäische Plattform für das Angebot von MOOC gibt, wäre es eine Sache der Unis, eine solche Plattform aufzubauen.

Mit der Verleihung des BigBrotherAwards an die TUM und die LMU möchten wir die beiden Universitäten und auch alle anderen Bildungseinrichtungen daran erinnern, dass das langfristige Geschäftsmodell von

solchen „Bildungsanbietern“ daraus besteht, dass die Studierenden durch die Verträge von Coursera nicht die „Kunden“ des Online-Bildungsangebotes sind, sondern das Produkt, das verkauft wird.

- Herzlichen Glückwunsch an die Technische Universität und die Ludwig-Maximilians-Universität München zum BigBrotherAward 2017.

Wie es weiter ging:

Von Claudia Fischer

Aus den Kommentaren unseres Publikums:

- „Bildung ist wichtig für die Gesellschaft. Sie ist keine Ware und steht jedem gleichermaßen und kostenfrei zu. Das Bildungssystem muss frei sein und darf nicht monetarisiert werden.“

Keine Reaktion aus München

München blieb stumm. Wir haben keinerlei Reaktion aus der Technischen Universität oder der Ludwig-Maximilians-Universität erhalten. Beide Hochschulen sind weiterhin auf der Webseite von Coursera zu finden und haben auch Kurse für das Wintersemester 2017/18 angekündigt – immerhin scheinen sich aber keine weiteren deutschen Hochschulen angeschlossen zu haben.

Journalisten gegenüber sagten die Hochschulen, MOOCs seien ja nicht vorrangig für ihre eigenen Studierenden konzipiert, sondern für internationale Interessent.innen. Für die eigene Studierendenschaft

Foto: Mattes, cc by-sa 2.0

Die Technische Universität München

habe man längst interne, selbstgestaltete Angebote. Außerdem sei die Teilnahme an Coursera-Vorlesungen total freiwillig. Wir finden: Ein bisschen mehr Verantwortungsgefühl für die eigene Bildungsarbeit fänden wir bei den deutschen Hochschulen wünschenswert.

Die Speicherung der Daten in den USA sehen wir nach wie vor kritisch – und nicht nur wir. Das alte Safe Harbor-Abkommen zum Datenschutz zwischen der EU und den USA ist bereits im Oktober 2015 vom Europäischen Gerichtshof für ungültig erklärt werden. Das Nachfolgemodell „Privacy Shield“ steht sehr in der Kritik (nicht zuletzt finden Sie auf unserer Webseite mehr dazu) und ist immer noch nicht verabschiedet worden. Die Wahl Donald Trumps zum amerikanischen Präsidenten hat die Verhandlungen nicht leichter und die USA nicht vertrauenswürdiger gemacht. Der Bayerische Rundfunk brachte es in seiner Berichterstattung über unsere BigBrotherAward-Vergabe an die Münchner Unis so auf den Punkt:

- „In einer Zeit, in der US-Behörden nach Passwörtern für Social-Media-Accounts fragen, um über die Einreise zu entscheiden, ist Misstrauen gegenüber US-Datenschutzstandards durchaus nachvollziehbar.“

Foto: Fabian Kurz cc by sa 4.0

Die BigBrotherAward-Crew 2017 – Sie machen es möglich

Kategorie Behörden:

Die Bundeswehr und Ursula von der Leyen

Von Dr. Rolf Gössner

Foto: Fabian Kurz, cc by-sa 4.0

Laudator: Dr. Rolf Gössner

Der BigBrotherAward 2017 in der Kategorie Behörden geht an **die Bundeswehr und die Bundesministerin für Verteidigung, Dr. Ursula von der Leyen (CDU), als deren Oberbefehlshaberin.**

Mit dieser Auszeichnung wagen wir uns erstmals in der 17jährigen Geschichte des BigBrotherAwards auf militärisches Terrain beziehungsweise Sperrgebiet. Wohingegen Frau von der Leyen schon einschlägig aufgefallen ist – schließlich haben wir sie bereits 2009 in ihrer damaligen Funktion als Familienministerin mit dem Negativpreis bedacht; wir erinnern uns: als „Zensursula" wegen ihrer Vorstöße zur Inhaltskontrolle und Sperrung von Webseiten. Doch was haben die Verteidigungsministerin und das Militär mit Überwachung, Zensur, überhaupt mit Datensünden zu tun? Weshalb soll ausgerechnet die Bundeswehr mit ihren Panzern, Bomben und Granaten eine auszeichnungswürdige Datenkrake sein – die in jüngerer Zeit eher durch Neonazi-Umtriebe, Gewaltexzesse, Misshandlungen, sexuelle Übergriffe, Mobbing und einen ausgeprägten Korpsgeist aufgefallen ist?

Nun, die heutige Verleihung erfolgt für die massive digitale Aufrüstung der Bundeswehr mit dem neuen „Kommando Cyber- und Informationsraum" (KdoCIR) – das heißt im Klartext: für die Aufstellung einer kompletten digitalen Kampftruppe mit (geplant) fast 14.000 Dienstkräften, mit eigenem Wappen, Verbandsabzeichen und Fahne – selbst ein Cyber-Marsch wurde eigens für diese Truppe komponiert, die Frau von der Leyen just vor einem Monat (am 5.04.2017) in Bonn in Dienst gestellt hat.

Schon bislang existierte eine kleine, geheim agierende IT-Einheit in Rheinbach bei Bonn (*„Computer Netzwerk Operationen"*) mit etwa 70 bis 80 Soldaten, die für operative Maßnahmen zuständig ist. Diese Einheit wird nun mit weiteren IT-Einheiten der Bundeswehr, etwa dem *Kommando Stra-*

▶Was müssen wir befürchten? Wo sind die Betroffenen?◀

tegische Aufklärung, in der neuen Cyber-Kampftruppe verschmolzen und zentralisiert. Weitere dringend benötigte IT-Fachleute versucht die Bundeswehr mithilfe großer Werbekampagnen anzuheuern.

Mit dieser digitalen Aufrüstung wird – neben Land, Luft, Wasser und Weltraum – ein fünftes Schlachtfeld, das sogenannte „Schlachtfeld der Zukunft" eröffnet und der Cyberraum – man kann auch sagen: das Internet – zum potentiellen Kriegsgebiet erklärt. Mit der Befähigung der Bundeswehr zum Cyberkrieg beteiligt sich die Bundesrepublik am globalen Wettrüsten im Cyberspace – und zwar weitgehend ohne Parlamentsbeteiligung, ohne demokratische Kontrolle, ohne rechtliche Grundlage.

Das klingt zwar ziemlich beunruhigend, bleibt aber eher abstrakt. Was hat all das mit uns zu tun? Was müssen wir befürchten? Wo sind die Betroffenen? Berechtigte Fragen, aber sie greifen zu kurz. Denn nicht alles, was wir hierzulande nicht unmittelbar spüren und erleiden, ist problem- oder harmlos. Schließlich gelten Grund- und Menschenrechte auch für Menschen in anderen Ländern, die sehr wohl betroffen sein können – ganz abgesehen vom Eskalationspotential dieser digitalen Aufrüstung, das auf uns zurückschlagen kann; und ganz abgesehen auch von ungelösten völkerrechtlichen Problemen.

Selbstverständlich ist es legitim, wenn die Bundeswehr geeignete Schutzmaßnahmen ergreift, um sich gegen Cyberattacken von außen zu wehren, die gegen ihre eigene Militär-IT gerichtet sind – angeblich sind das Zigtausende pro Tag (2016: über 47 Mio. IT-Angriffe auf die Bundeswehr). Doch das Bundesverteidigungsministerium gibt sich damit nicht zufrieden. Im Gegenteil: Es erhebt den – unseres Erachtens nach rechtsstaatswidrigen – Anspruch auf kooperative Zuständigkeit der Bundeswehr für die – so wörtlich – *„gesamtstaatliche Sicherheitsvorsorge"* und Abwehr von Cyber-Angriffen. Also auch zum Schutz anderer staatlicher, kommunaler und ziviler

Grafik: Werbekampagne der Bundeswehr

So sieht sie aus, die Werbekampagne, mit der die Bundeswehr IT-Spezialist.innen anheuern will.

Fotorechte: Bundeswehr

Bundesverteidigungsministerin Ursula von der Leyen beim Abschreiten der Front am 5.4.2017

Netzwerke im Innern des Landes, für den in Friedenszeiten jedoch ausschließlich Polizei, Geheimdienste und Justiz zuständig sind sowie speziell das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Nationale Cyber-Abwehrzentrum, in dem alle Sicherheitsorgane zusammenwirken. Bundeswehreinsätze im Innern zum Schutz nichtmilitärischer IT-Systeme vor Cyber-Attacken sind insoweit weder verfassungsgemäß noch erforderlich.

Doch es kommt noch härter: Denn die Bundeswehr soll mit ihrer verharmlosend „Cyber- und Informationsraum" genannten Cyber-Kampftruppe nicht nur abwehren können – Ihre dort beschäftigten Cyberkämpfer sollen darüber hinaus bereits im Vorfeld in fremde IT-Systeme eindringen und diese ausforschen können sowie zu eigenen Cyberangriffen auf andere Staaten und deren Infrastruktur befähigt werden. Im Klartext: also zum Führen von Cyberkriegen – im Übrigen auch als Begleitmaßnahmen zu konventionellen Kriegseinsätzen der Bundeswehr im Ausland, etwa in Afghanistan oder Mali. So sieht es die geheime *Strategische Leitlinie Cyber-Verteidigung* des Verteidigungsministeriums (2015) vor und auch das *„Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr 2016"*. Das bedeutet: Die Bundeswehr soll eigene Cyberwaffen entwickeln, um getarnt in fremde IT-Systeme einbrechen, diese über Sicherheitslücken, Trojaner, Viren etc. ausspähen, manipulieren, fehlsteuern, lahmlegen, schädigen oder zerstören zu können.

Doch selbst wenn es sich dabei nicht um eigene völkerrechtswidrige kriegerische Angriffe handelt, sondern um Cybergewalt zur Selbstverteidigung gegen Militärattacken von außen, dann wäre das zwar völkerrechtlich prinzipiell zulässig, doch höchst riskant. Warum? Weil davon nicht allein militärische Ziele betroffen wären, sondern – zumindest als „Kollateralschäden" – auch zivile Infrastrukturen. Denn auch Cyberangriffe, die nur auf militärische Ziele gerichtet sind, können rasch zum Flächenbrand führen, sobald sie sich auf kritische zivile Infrastrukturen ausbreiten, diese lahmlegen oder gar zerstören. Digitale Waffen sind in einer vernetzten Welt keineswegs Präzisionswaffen und die

Streuwirkung kann immens sein. Und das mit gravierenden, ja lebensbedrohlichen Folgen für die Zivilbevölkerung, wenn die Gegenattacken etwa zu lang andauernden Ausfällen der Strom- und Wasserversorgung oder des Krankenhaus-, Gesundheits- oder Verkehrswesen führen. Dies wäre ein Verstoß gegen das Humanitäre Völkerrecht.

▶Dabei lassen sich Datenspuren leicht manipulieren, verdecken oder anderen in die Schuhe schieben.◀

Zusätzlich zu solchen Auswirkungen von Cyberangriffen kommen noch weitere, kaum zu lösende Probleme und Gefahren einer Militarisierung des Internets hinzu:

Erstens besteht die große Gefahr, dass es aufgrund von Fehlinterpretationen bei der Frage, ob es sich bei einem Cyberangriff um eine kriegerische oder um eine nichtmilitärische, etwa kriminelle Attacke handelt, zu vorschnellen militärischen Selbstverteidigungsschlägen kommt – und damit zu einer gefährlichen und folgenschweren Eskalation. Derzeit ist im Völkerrecht nicht klar und verbindlich definiert, wann ein Cyberangriff als kriegerische Angriffshandlung zu gelten hat. Nach derzeit noch vorherrschender Auffassung unter Völkerrechtlern liegt ein solcher Angriff jedoch nur dann vor, wenn die zerstörerischen Auswirkungen mit denen konventioneller Waffengewalt vergleichbar sind – also wenn eine solche Online-Attacke etwa Züge entgleisen, Flugzeuge abstürzen, Kraftwerke explodieren lässt und Menschen verletzt werden oder umkommen. Doch NATO wie Bundeswehr behalten sich ausdrücklich vor, im Einzelfall zu entscheiden, ab wann es sich um einen solchen kriegerischen Angriff handelt und wie darauf reagiert wird – warum das so ist, verrät ein Oberstleutnant im Verteidigungsministerium: *„weil wir hier auch ein Stück weit unberechenbar bleiben wollen und müssen“.* Diese Unberechenbarkeit hinsichtlich Anlass und Art eines Gegenschlags diene letztlich auch der Abschreckung, so die NATO-Philosophie.

Zweitens: Im Cyberkrieg gibt es keine Armeen, die sich gegenüberstehen und keine Soldaten in Uniform. Stattdessen kommen etwa Viren, Würmer oder Trojaner verdeckt und häufig auf Umwegen zum Einsatz – also Software, die keine Uniform oder Staatsabzeichen trägt. Dabei lassen sich Datenspuren leicht manipulieren, verdecken oder anderen in die Schuhe schieben – um etwa unter falscher Flagge Kon-

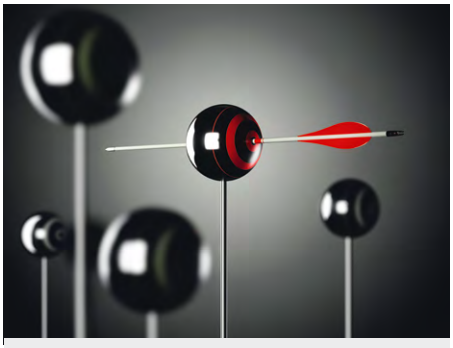


Bild: Panthermedia

Rolf Gösssner: „Cyberangriffe und Computersabotage sind keine Präzisionswaffen!“

Das Interne Verbandsabzeichen des „Kommando Cyber- und Informationsraum“ (CIR)

flikte zu schüren oder Kriegsgründe zu fingieren. So ist nicht nur schwer herauszufinden, ob es sich bei IT-Angriffen um zivil-kriminelle und wirtschaftliche oder um geheimdienstliche und militärische Operationen handelt. Der angegriffene Staat hat außerdem das Problem, die wahren Urheber zweifelsfrei zu identifizieren, um überhaupt rechtmäßig, angemessen und zielgenau reagieren zu können. Die Beweisführung ist in aller Regel äußerst schwierig. Der Internationale Gerichtshof verlangt jedoch eine klare Beweislage, denn es gibt kein Recht auf militärische Selbstverteidigung ins Blaue hinein oder aufgrund bloßer Indizien; ein Gegenschlag ohne klar identifizierbaren Aggressor ist jedenfalls völkerrechtswidrig.

Und drittens: Diese Probleme werden noch verschärft durch eine gefährliche Rechtsauslegung im *„Tallinn Manual“* – einem NATO-Handbuch zur Anwendung des Völkerrechts auf die Cyberkriegsführung (2013). Zwanzig zumeist militärnahe Rechtsexperten aus NATO-Staaten, auch aus Deutschland, haben diesen Leitfaden erarbeitet. An den darin aufgelisteten 95 Regeln sollen sich alle NATO-Staaten im Fall eines Cyberkriegs orientieren – auch die Bundeswehr. Was aber ist daran so gefährlich? Drei Beispiele:

- Danach gelten selbst solche Operationen als Cyberwar-Angriffe, die bloße wirtschaftlich-finanzielle Schäden eines betroffenen Staates verursachen, wenn diese gewisse Ausmaße annehmen, etwa einen Börsencrash. Dagegen wäre dann eine militärische, auch konventionelle Selbstverteidigung mit Kriegswaffen rechtens, so der Leitfaden, was zu einer unkontrollierbaren Eskalation der Auseinandersetzungen führen könnte.
- Laut Handbuch gelten zivile Hacker („Hacktivists“) als aktive Kriegsteilnehmer, wenn sie Cyber-Aktionen im Verlauf kriegerischer Konflikte ausführen. Solche Zivilisten können daher militärisch angegriffen und auch getötet werden. Selbst das Suchen und Offenlegen von Schwachstellen in Computersystemen des Gegners gilt demnach als kriegerische Handlung. Auf diese Weise wird die Kampfzone praktisch auf Privatpersonen und deren Laptops ausgeweitet.
- Das NATO-Tallinn-Manual sieht zudem vor, dass ein Staat sein Recht auf Selbstverteidigung auch präventiv ausüben darf – bevor überhaupt ein digitaler Angriff stattgefunden hat. Auch hier, wie bei konventionellen Militär-Erstschlägen, besteht hohe Missbrauchs- oder Missinterpretationsgefahr.

Mit der Rechtsauslegung in diesem NATO-Dokument werden die hohen völkerrechtlichen Eingriffsschwellen für bewaffnete Gewaltanwendungen zwischen Staaten unverantwortlich weit herabgesenkt sowie die restriktiven Kriterien des Selbstverteidigungsrechts aufgeweicht. Das gefährdet die Zivilbevölkerungen und die internationale Sicherheit in erheblichem Maße. Was einflussreiche, zumeist militärnahe Völkerrechtler da an Regeln für die NATO zusammengestellt haben, ist geeignet, die Grenzen zwischen innerer und äußerer Sicherheit, zwischen Zivilem und Militärischem, zwischen Krieg und Frieden, zwischen Angriff und Defensive zu verwischen – und eine schwere Datenattacke blitzartig in einen echten Krieg mit Raketen, Bomben und Granaten eskalieren zu lassen.

All dies bedeutet: Mit der Aufrüstung der Bundeswehr zum Cyberkrieg steigen Eskalationspotentiale, Kriegsbereitschaft und Kriegsgefahr – und davor schützt auch die obligatorische Zustimmung des Bundestags zu Militäreinsätzen im Einzelfall nur bedingt. Denn das Cyber-Konzept der Verteidigungsministerin für die Bundeswehr ist letztlich demokratisch kaum zu kontrollieren. Wobei die längst zur Interventionsarmee umgebaute Truppe ohnehin schwer kontrollierbar und skandalträchtig ist.

Wir vergeben unsere Negativpreise zwar für böse Pläne und Taten, aber wir geben unsere Preisträger.innen nicht verloren und verleihen den Preis gerne auch auf Bewährung. Voraussetzung dafür wäre, dass Sie, Frau Verteidigungsministerin, von der digitalen Aufrüstung abrücken, auf offensive Cyberwaffen für die Bundeswehr verzichten und eine ausschließlich defensive Cybersicherheitsstrategie verfolgen, um die Zivilbevölkerung effektiv zu schützen – flankiert von vertrauensbildenden Maßnahmen im Rahmen einer friedensorientierten Außenpolitik und Diplomatie (Stichwort: „Cyberpeace“). Wir fordern darüber hinaus eine weltweite Cyberabrüstung sowie eine völkerrechtliche Ächtung von Cyberspionage und Cyberwaffen. Und wir fordern die Schaffung einer unabhängigen Instanz der UN zur Untersu-

Wir fordern darüber hinaus eine weltweite Cyberabrüstung.

Sticker: Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF)

Der Cyberpeace-Sticker des FifF mit der „verdrahteten“ Friedenstaube löste bei unserer Gala spontanen Applaus aus.

Fabian Kurz, cc by-sa 4.0, Hintergrundbild: Bundeswehr

Laudator Rolf Gössner, im Hintergrund: Ursula von der Leyen befestigt das Fahnenband an der Flagge des CIR.

chung zwischenstaatlicher Cyberattacken und deren angemessener Abwehr.

Doch Sie, Frau von der Leyen, haben offenbar anderes zu tun. Sie suchen stattdessen, so wörtlich, „händeringend Nerds“: „Hacker, IT-Programmierer, IT-Sicherheitsfachleute, Penetrationstester, Systemadministratoren oder IT-Entwickler“. Der Bedarf der Bundeswehr liege bei rund 800 IT-Administratoren und 700 IT-Soldaten, also Cyberkämpferinnen und -kämpfern pro Jahr. Flächendeckend und großflächig wirbt die Bundeswehr auf Bahnhöfen, in Unis und Medien um Fachpersonal und Quereinsteiger für den Waffendienst am PC; auch zivile Experten aus Wirtschaft, Verbänden und NGOs werden für eine schlagkräftige „Cyber-Reserve“ geworben. In Anlehnung an den Kriegsslogan Ihres Vorvorgängers Peter Struck – *„Die Sicherheit der Bundesrepublik Deutschland wird auch am Hindukusch verteidigt“* – werben Sie nun mit dem Sinnspruch: *„Deutschlands Freiheit wird auch im Cyberraum verteidigt. Mach, was wirklich zählt…“*. Das klingt spannend und womöglich auch verlockend.

Ob Sie, Frau Ministerin und ihre Werberkolonnen schon mal beim Chaos Computer Club oder bei Digitalcourage vorbeigeschaut haben? Auch heute hier im Saal sitzen wohl reihenweise technikaffine und -kundige Menschen, die genau in Ihr Beuteschema passen. Darum hoffen wir sehr, dass diese Laudatio und unsere Preisvergabe solche Menschen dazu ermutigen, ihre Fähigkeiten für Frieden und Verständigung im Internet einzusetzen, statt für digitale Angriffe und Cyberkrieg auf dem „Schlachtfeld der Zukunft“!

- Herzlichen Glückwunsch zum Negativpreis BigBrotherAward 2017, Frau Bundesverteidigungsministerin und Oberbefehlshaberin der Bundeswehr.

Foto: Justus Holzberger, cc by-sa 4.0

Unser BigBrotherAwards-Publikum – Ob sich hier Nerds für die Bundeswehr finden lassen?

Wie es weiter ging:

Von Claudia Fischer

Der BigBrotherAward für Bundeswehr und Bundesverteidigungsministerin hat den Publikumspreis bei unserer Verleihungsgala gewonnen.

Folgende Kommentare fanden wir auf den Abstimmungskarten:

- „Die Demokratie wird ausgehöhlt und der Frieden leichtfertig gefährdet."
- „Das aggressive Potential von KdoCIR und die mangelnde demokratische Kontrolle machen die Bundeswehr besonders preiswürdig."
- „Weil es die Kriegsgefahr für uns alle auf dem Planeten erhöht."
- „Legaler Cyberwar, ein 3. Weltkrieg. Entmündigung der Bürger."
- „Menschenrechte und Datenschutz gehören zusammen (in allen Kategorien). Die Laudatio hat das sehr gut begründet."
- „Weil daraus innerhalb kürzester Zeit tödlicher Ernst werden könnte."

Keine Reaktion aus Bonn oder Berlin

Das Bundesverteidigungsministerium hat unsere Preisvergabe nicht kommentiert – weder uns gegenüber, noch haben wir in Presseberichten eine Reaktion lesen können. „Es ist die übliche, unsouveräne und Kritik missachtende Nichtreaktion, wie wir sie von staatlichen Sicherheitsorganen in Bund und Ländern sowie von ihrer politischen Führung bei BigBrotherAward-Verleihungen in den vergangenen 18 Jahren leider gewohnt sind", sagt Rolf Gössner, der seit Beginn der deutschen BigBrotherAwards dabei ist und die meisten der Politik- und Behörden-Preise laudatiert hat. Die gute Nachricht:

- Rolf Gössners Laudatio wurde mehrfach in verschiedenen Zeitschriften und Online-Medien veröffentlicht und wird innerhalb der Antikriegs- und Friedensbewegung diskutiert.

Kategorie Verbraucherschutz:

Die Prudsys AG

Von padeluun

Der BigBrotherAward in der Kategorie Verbraucherschutz geht an **Jens Scholz, Vorstand der Prudsys AG, Chemnitz**, für die Software zur Preisdiskriminierung, also für Beihilfe zur Preistreiberei und Verbreitung sozialen Unfriedens

Wissenschaft – und das gilt auch für die Disziplinen Mathematik und Informatik – ist etwas Feines. Man forscht, gewinnt Erkenntnisse und setzt diese dann – zum Beispiel mittels Ausgründung aus der Universität – zum Besten für die Menschheit um.

Unser Preisträger, die Prudsys AG, ist eine Ausgründung der TU Chemnitz. Sie beschäftigt sich mit Data Mining. Sie veranstaltet schon so lange, wie wir die BigBrotherAwards veranstalten – seit dem Jahr 2000 – den „Data Mining Cup“, wo sich die Besten der Besten einen Wettbewerb liefern, um aus riesigen Kübeln voll mit Big Data das eine oder andere Daten-Nugget herauszufischen. Mit solchen Fähigkeiten könne man – so wird erzählt – unbekannte Krankheiten heilen und das Hungerproblem der Welt lösen.

Die Prudsys AG, so scheint es, hat an diesen guten Zielen wenig Interesse. Ihr Businessmodell bietet etwas anderes an: „Preisdiskriminierung“. Und das ist uns bei den BigBrotherAwards schon im Jahr

Laudator: padeluun

Foto: Fabian Kurz, cc by-sa 4.0

2000 begegnet, als wir die Firma Payback für ihre Kundenkarten mit einem unserer hübschen, aber unbegehrten Awards beehrten.

Die Prudsys AG entwickelt Algorithmen und Strategien, die es Händlern ermöglichen, für ein- und dasselbe Produkt, sei es Apfel, Milch oder Digitalkamera, online und offline den höchstmöglichen Preis zu verlangen, der eben noch möglich ist, ohne dass Sie als Kundin oder Kunde abspringen. Also ist nicht mehr der Wert einer Ware ausschlaggebend für die Preisgestaltung, sondern Sie sind es. Sie und

Foto: Tom Alby, cc by-sa 4.0

Das Elektronische Preisschild sorgt für Unsicherheit: Bekommen Sie den gleichen Preis angezeigt wie Ihre Nachbarin?

ich. Die Händlerin oder der Händler müssen genug über uns wissen, um herauszufinden, welchen größtmöglichen Preis wir zu zahlen bereit sind. Im Marketing-Jargon heißt das: „Preisakzeptanzschwellen explorativ dynamisch austesten“. Das klingt vielleicht absurd – ist aber so.

Nehmen wir an, Sie sind alleinerziehender Vater, müssen nach der Arbeit schnell in die Kita hasten, um Ihre Tochter abzuholen und husch husch, bevor Sie das Abendessen bereiten, noch einkaufen. Dann, denke ich, werden Sie nicht drei Läden besuchen, Preise vergleichen und günstiger einkaufen. Sie werden in das Geschäft laufen, das auf dem Weg oder kleinsten Umweg liegt und in den Korb werfen, was so auf dem Einkaufzettel steht. Wenn dieser Laden nicht „Dauertiefpreise statt Sonderangebote“ garantiert, dann werden Sie sicher mehr bezahlt haben, als jemand, der mehr Zeit hat.

„Ha!“, werden Sie jetzt vielleicht antworten. „Ich habe meine Kundenkarte. Da bekomme ich als treuer Kunde alles etwas günstiger.“ Doppel-HA! Antworte ich. Jetzt haben Sie erst recht verloren! Denn jetzt weiß der Händler, was Sie so einkaufen – und wann – und wie viel Sie im Durchschnitt pro Einkauf ausgeben – und ob Sie bar zahlen oder mit Karte. Er kann abschätzen, wie groß Ihr Haushalt ist, und kann Sie ganz gezielt mit Rabattcoupons dahin steuern, wohin er sie haben möchte. Weg von den Artikeln, an denen der Händler wenig verdient, hin zu den lukrativeren Artikeln. Er kann abschätzen, wie viele Kunden zukünftig wegbleiben, und ob es sich trotzdem lohnt, wenn er die 2-Kilo-Packung Spaghetti aus dem Angebot nimmt und statt dessen ausschließlich die 250-Gramm-Packungen – die leider etwas teurer sind – ins Regal legt.

▶„Preisakzeptanzschwellen explorativ dynamisch austesten“◀

Und das entscheidet nicht der freundliche Marktleiter, sondern die Zentrale. Die kann das nämlich viel besser entscheiden, als der Mensch vor Ort – denn die Zentrale bündelt die Daten, wertet sie aus, rechnet das Wetter, Saisonzeiten, Wochen- oder Tageszeiten dazu, oder ob die Konkurrenz gerade eine Promotionaktion fährt (kein Witz!) und schon ändert sich das elektronische Preisschild am Regal.

Denn die Zentrale hat guten Rat: Die Entscheidungssysteme sind mit der Software „Realtime Decision Engine“, kurz RDE, der

Foto: Claudia Fischer, cc by-sa 4.0

„Check-Out-Couponing“ – das ist Marketingsprech für Rabattgutscheine auf Kassenzetteln.

Firma Prudsys verbunden. Die Selbstbeschreibung:

„Die Prudsys RDE ist als erstes Dynamic-Pricing-Tool in der Lage, die bestmögliche Preisfindung in Echtzeit vorzunehmen. Durch den Einsatz der Prudsys RDE werden tausende Produktpreise vollautomatisiert an das Kundenverhalten sowie sich ständig ändernde Markt- und Unternehmenssituationen angepasst.

Durch die Kombination von personalisierten Produktempfehlungen und individuellen Preisvorteilen werden Kunden durch Rabatte auf für sie relevante Produkte belohnt. Als Umsetzungsmedium für personalisiertes Pricing eignen sich besonders vollautomatisch erzeugte und personalisierte Coupons in Kunden-Newslettern, in Mailings und in mobilen Apps. Individuelle Rabatte können zudem im Zuge des Check-out-Couponings [Anmerkung des Laudators: das sind diese Zusätze, die Ihren Kassenzettel neuerdings immer so lang machen], via Kundenkarten oder auf Instore-Kiosksysteme ausgespielt werden.“

Was die Prudsys AG hier schreibt, ist schon eine Nummer härter, als dass die selben DVDs beim Marktkauf in Rahden (ein eher ärmerer Ort) grundsätzlich 30% teurer sind als beim Marktkauf in Lübbecke, wo eher reichere Leute wohnen.

Und wenn das schon im Einzelhandel an der Straße funktioniert, wie gut funktioniert das erst in Online-Shops? Hier – meint einer der Prudsys-Chefs im Interview – kommen die Händler an der Preisdiskriminierung (die natürlich nicht Preisdiskriminierung heißt, sondern „Dynamic Pricing“ genannt wird) im Zeitalter von Amazon & Co gar nicht vorbei: Online-Shops würden ohne Dynamic Pricing bald schlicht nichts mehr verkaufen.

Was können wir tun?

Hier sind ein paar praktische Tipps: Wenn Sie eine Reise buchen wollen, nehmen Sie lieber einen Windows-Rechner, statt eines Macs. Sonst wird‘s gleich teurer. Sie wollen vom Handy buchen? Ganz schlech-

Foto: Claudia Fischer, cc by-sa 4.0

Preisdiskriminierung: Wenn eine DVD nicht mehr kostet, was sie wert ist, sondern das, was wir maximal zu zahlen bereit sind.

te Idee – das wird meist richtig teuer, aber wenn, dann besser nicht vom iPhone aus, sondern lieber mit einem Smartphone mit dem Betriebssystem Android.

Foto: Justus Holzberger, cc by-sa 4.0

Mit der freundlichen Markthändlerin auf Augenhöhe? Vorbei. Bei Prudsys weiß der Computer alles über uns, wir aber nichts über den Algorithmus.

Das ist noch eine recht grobe Art der Differenzierung. Die Prudsys AG hat bessere Algorithmen, die viel feinziselierter Daten zusammenraffen, die von den meisten Menschen als „sind doch eh nicht wichtig“ fahrlässig abgegeben wurden. Jeder Kaffee, den Sie kaufen, kann gegen Sie verwendet werden!

Wenn Sie im Web einkaufen, sehen Sie die Oberfläche, die ein Designer im Auftrag des Händlers programmiert hat. Ihr Nachbar sieht eine andere. Ihre Kollegin ebenfalls. Und das Wort „Oberfläche“ trifft es genau. Sie sehen nur eine winzig kleine Spitze Ihres Wahl- und Einkaufvorgangs. Unter der Oberfläche aber werden Daten geschaufelt, Berechnungen angestellt, geschachert und alles mit dem einen Ziel: Sie abzuzocken. Bei jedem Kauf im Netz müssen Sie sich vorstellen, dass unter der Oberfläche ein leises Kichern und ein zufriedenes Händereiben zu hören ist.

▶Jeder Kaffee, den Sie kaufen, kann gegen Sie verwendet werden!◀

Das ist eine giergetriebene Welt. In dieser Welt existieren keine Menschen, keine Einzelprodukte, keine Zufriedenheit, kein Service – hier gibt es nur eins: Zahlen. Einsen und Nullen und am Ende manifestieren sich diese zu einem dicken fetten Plus an Euro und Dollar. Die Prudsys AG sagt, dass jeden Tag eine Milliarde Entscheidungen mit ihren Algorithmen getroffen werden – 8 Milliarden Dollar Handelsvolumen jährlich werden mit diesen Algorithmen erwirtschaftet. Selbst wenn Sie schon gelernt haben, dass man Begriffe wie „Premiumkunde“, „Rabatt“ und allein schon die Floskel „Sparen Sie ...“ meiden sollte, wie der Teufel das Weihwasser: Es gibt quasi kein Entkommen. Selbst wenn Sie, wie die junge Frau, die ein Hotelzimmer in Brüssel buchen wollte, dieses 17mal stornieren, um am Ende 1,38 Euro weniger zu bezahlen. Die Welt wird nicht zu einem lustigen gigantischen orientalischen Basar. Sie als Kundin haben es

Bild: Panthermedia

padeluun: „Ihr habt Euch leider für die dunkle Seite der Macht entschieden: Die Gier.“

nicht mehr mit einer Wochenmarkthändlerin zu tun, mit der Sie auf Augenhöhe um den Preis feilschen können. Hier feilscht nur einer, denn der Händler weiß alles über seine Kunden, die Kunden nichts über die Händler. Es besteht keine Augenhöhe, kein Frieden, sondern ein immerwährender Quell für das böse Gefühl, stets zu kurz zu kommen. Und das zu Recht.

Mit Data Mining, liebe Prudsys AG, mit Euren Fähigkeiten könnte man vielleicht unbekannte Krankheiten heilen und das Hungerproblem der Welt lösen. Ihr habt Euch leider für die dunkle Seite der Macht entschieden: Die Gier.

- Ihr habt schon ein paar Awards bekommen: Den „Top 100“, den „Innovationspreis-IT“, den „Top Produkt Handel“, den „Chemnitzer Meilenstein“ ... und jetzt auch noch den „Top BigBrotherAward 2017“. Herzlichen Glückwunsch, Jens Scholz von der Prudsys AG.

Datenschutz ist Verbraucherschutz.

Machen Sie uns stark!

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

Wie es weiter ging:

Von Claudia Fischer

Aus den Kommentaren unseres Publikums:

- „padeluun hat sehr überzeugend vorgetragen und das Thema war super interessant.“

Telefonat mit Prudsys

Kurz vor der Preisverleihung hat padeluun mit einem Vertreter der Firma Prudsys telefoniert. Sein Fazit: „Herr Scholz meinte, die ethische Bewertung von Preisdiskriminierungssoftware müsse erst noch gesellschaftlich diskutiert werden. Das Thema würden wir so schnell nicht los. Kurz danach hat Prudsys eine eigene Veranstaltung ausgerichtet – zu der sie uns allerdings nicht einmal eingeladen haben.

- Da hat Prudsys schon die zweite Chance verpasst, zu zeigen, dass sie diesen Dialog aktiv angehen wollen. Schade...“

Grußwort

des Bielefelder Oberbürgermeisters Pit Clausen

Foto: Fabian Kurz, cc by-sa 4.0

Der Bielefelder Bürgermeister Pit Clausen (SPD) gelobt, niemals Preisträger werden zu wollen.

Sehr geehrte Damen und Herren,

als Rena Tangens mich das erste Mal angesprochen hat, am Rande der Bundesversammlung, wo der Bundespräsident gewählt wurde, fragte sie:

„Möchten Sie nicht zur Verleihung der BigBrotherAwards in Bielefeld zu uns kommen?“
Da hatte ich so eine kleine Schrecksekunde. Kennen Sie das? So ein: „Uups… Uups was ist schief gegangen?“ (Publikum lacht und applaudiert)

Sie hat das aber ganz lieb, ganz nett, ganz schnell aufgeklärt, dass ich nicht als Preisträger eingeladen bin, sondern nur für ein Grußwort. Das hat es mir dann leicht gemacht, auch zuzusagen. Jetzt bin ich wirklich gerne gekommen, aber ich sage ganz ehrlich: das erste „Uups“ hat schon eine gewisse Berechtigung.

Ich bin nicht nur Chefrepräsentant hier in der Stadt, sondern leite eine Organisation mit mehr als 5000 Beschäftigten. Natürlich sind wir digital unterwegs und gehen mit unglaublich vielen, vor allem unglaublich sensiblen Daten um. Und natürlich kann in so einem riesigen Laden auch mal ungewollt etwas schief gehen. Wir haben natürlich ein Datenschutzsystem und wir betrieben unglaublich viel Aufwand, aber es kann immer auch was danebengehen.

▶Wir tun alles, damit wir nie Preisträger bei Ihnen werden!

Ja, jetzt ist das natürlich schon bemerkenswert, dass wir es hier mit einem Preis zu tun haben, der in der ganzen Republik Schlagzeilen macht, aber den eigentlich gar keiner will. Das ist auch eine ungewöhnliche Kombination. Die Schlagzeilen, die mit den BigBrother Awards verbunden sind, sind, soweit ich das wahrnehme, bundesweit durchweg positive. Egal in welche Medien ich hineingucke. FAZ, Spiegel, Zeit, in der Süddeutschen, überall wird das Thema positiv aufgenommen und reflektiert. Da bin ich dann auch wieder so

ein bisschen Teufelchen und denke: „Ja wenn die Medien das, egal von der oder der Seite, alle gut finden, ist das vielleicht so eine Art vorbeugender Selbstschutz, so nach dem Motto *‚Ich tu dir nichts, tu du mir auch nichts‘.*“

▶das Beste daran ist, … dass dann auch etwas in Bewegung kommt.◀

Nein, da musste mein Teufelchen im Kopf wahrscheinlich irren, das stellt man fest, wenn man auf die Liste der Preisträger schaut. Diese Liste macht deutlich, dass Sie bisher in der Jury der BigBrotherAwards nun wirklich gar keine Angst vor großen Namen haben: Google, Apple, der Verfassungsschutz, die Kanzlerin, Bitkom, TTIP, alle kriegen ihr Fett weg, wenn sie es mal verdient haben. Und das Beste daran ist glaube ich nicht nur der Moment, wo man etwas aufruft und skandalisiert, sondern das Beste daran ist, das beobachte ich, dass dann auch etwas in Bewegung kommt. Vielleicht nicht immer, aber immer öfter.

Sie vergeben die Preise jetzt, wenn ich richtig informiert bin, seit dem Jahr 2000. Und ich beobachte, dass damit eine Öffentlichkeit geschaffen wird, die durch normale Medienarbeit, durch das, was wir klassisch mit Pressearbeit erreichen können, so nie erreicht werden konnte. Sie wollen nicht nur die Finger in eine Wunde legen, sondern Sie wollen dadurch zur Diskussion anregen. Sie wollen Veränderungen forcieren. Und wie wichtig, wie unbedingt notwendig das ist, werden Manche wahrscheinlich in unserem Land erst in einigen Jahren merken.

Der Verein heißt Digitalcourage Ich verstehe unter Courage insbesondere, dass man nicht nur GEGEN etwas ist, sondern sich FÜR etwas einsetzt. Und Sie, liebe Rena Tangens, haben das einmal so formuliert: Dass sich Digitalcourage für Freiheit, für Bürgerrechte und für eine lebenswerte Welt im digitalen Zeitalter einsetzt. Und genau dieser Einsatz dafür ist unendlich wichtig und der erfolgreiche Einsatz, den Sie jetzt seit vielen Jahren, seit 30 Jahren insgesamt, leisten, dem gilt unser aller herzlicher Dank. (Applaus)

Rena Tangens, padeluun, Sie sind die Speerspitze, aber in den vergangenen Jahren haben viele Menschen daran mitgewirkt, dass die BigBrotherAwards in unserem Land diesen Stellenwert erfahren haben. Natürlich gilt Ihnen allen mein Dank, unser Dank, aktuell natürlich der Jury 2017, den hauptamtlichen, den zahlreichen ehrenamtlichen Akteuren, ich darf erwähnen auch den über 1400 Fördermitgliedern, so hat man mir aufgeschrieben, den vielen Partnern und Spendern und trotzdem der Speerspitze Rena Tangens und padeluun. Ich ziehe symbolisch meinen Hut, den ich jetzt gerade nicht auf habe. Ziehe ihn also symbolisch für Ihre Entschlossenheit, für Ihre Unerschrockenheit und Tatkraft, wünsche mir, dass Sie noch lange durchhalten, dass Sie lange dieses Thema, dieses dicke Brett, was mit diesem Thema verbunden ist, weiter bohren und Ihnen. liebes Publikum, danke ich, dass Sie mir zugehört haben.

BigBrotherAwards wirken

Entwicklungen von 2000 bis 2009

Von Rena Tangens

Den folgenden Text hat Rena Tangens im Jahr 2009 geschrieben. Damals hieß Digitalcourage noch FoeBuD e.V. Weitere Updates zu den Preisträgern vergangener Jahre finden Sie im Anschluss.

Foto: Digitalcourage, cc by-sa 4.0

Den Preis, den keiner haben will, hat der Bielefelder Künstler Peter Sommer für uns gestaltet.

In den 90er Jahren war Datenschutz kein Thema, mit dem jemand hinter dem Ofen hervorzulocken war. Wenn heute dagegen Datenschutzskandale in der Wirtschaft hohe Wellen schlagen und Großdemonstrationen gegen Überwachungsgesetze stattfinden, dann ist das unter anderem ein Verdienst dieser Preisverleihung, die zur Institution geworden ist: Die BigBrotherAwards.

Seit dem Jahr 2000 vergeben wir diesen Negativ-Preis und nennen Ross und Reiter, die für Datenschutzvergehen, für Überwachungstechnologien und -gesetze und uferlose Datensammlungen verantwortlich sind. Die BigBrotherAwards machten zum Beispiel Rabattkarten, Scoring, Mautkameras, Farbkopierer und Handyüberwachung als Gefahr für Bürgerrechte und Privatsphäre bekannt. Sie warnten schon früh vor der Gesundheitskarte, der Steuer-ID und der Vorratsdatenspeicherung. Und sie sprachen deutliche Worte zu Ausländerzentralregister, Lauschangriff und Anti-Terror-Gesetzen.

▶ Ignorieren, Abstreiten, Abwiegeln ◀

Und wie reagieren die Preisträger? Mit dem klassischen Trio: Ignorieren, Abstreiten, Abwiegeln. Politiker sind geübt darin – die Public Relations Abteilungen von Firmen auch.

Screenshot: Sat1 Fernseh-Mitschnitt

Und noch ein BigBrotherAward wurde persönlich überreicht: Rolf Gössner traf 2011 im Frühstücksfernsehen bei Sat1 auf Uwe Schünemann, der als Innenminister von Niedersachsen 2011 bereits seinen zweiten BBA erhalten hatte.

Die Aufregung hinter den Kulissen ist derweil oft groß, besonders bei Behörden und Firmen beginnt die fieberhafte Suche nach der „undichten Stelle“. Damit ist leider nicht das Datenleck gemeint, sondern der/die Informant.in, der/die sich an uns gewandt hat. Die BigBrotherAwards bekommen jedes Jahr mehrere Hundert Meldungen: von geprellten Verbrauchern, von bespitzelten Arbeitnehmerinnen, von Administratoren, Software-Entwicklerinnen und Behördenmitarbeitern. Manchmal ist es eine kurze E-Mail, die den Anstoß gibt, manchmal kommt ein ganzes Dossier. Wir gehen allen Hinweisen nach, beobachten die technische und politische Entwicklung und recherchieren.

Egal, ob Firma oder Politiker: Die Preisträger sind durch die Bank wenig erfreut über ihre Auszeichnung. Sie kommen auch eher selten zur Preisverleihung. Erstaunliche Ausnahme: **Microsoft** flog 2002 ihren Datenschutzbeauftragten ein, der den Preis fürs Lebenswerk entgegennahm. Auch die **Deutsche Telekom** hatte 2008 den Mut den Preis abzuholen. Tatsächlich erkundigte sich die Telekom sogar schon Monate vorher diskret bei uns, ob sie etwa einen BigBrotherAward bekommen würde – „sie könnten sich vorstellen, dass sie ihn verdient hätten...“

> ▶Die Preisträger sind durch die Bank wenig erfreut über ihre Auszeichnung.◀

Andere meinten, sie könnten den BBA einfach ignorieren. Zum Beispiel die **Bayer AG** – nominiert für den Drogentest per Urinprobe bei ihren Auszubildenden – gab sich nicht die Mühe einer Antwort. Doch einige Monate später bekamen wir eine Einladung der Kritischen Aktionäre und ein paar Bayer-Aktien übertragen. Damit hatten wir Rederecht auf der Bayer Aktionärsversammlung. So kam es, dass die Übergabe dieses BigBrotherAwards nicht

vor 500 Zuschauern bei der Gala in Bielefeld stattfand, sondern vor 5.000 Zuschauern bei der Bayer-Hauptversammlung in Köln.

Die Politik ist weitgehend beratungsresistent.

Manche drohen offen oder verklausuliert mit Klage, wie die Deutsche Post oder Lidl. **Lidl** – schon 2004 mit einem BigBrotherAward für die Bespitzelung von Arbeitnehmerinnen beehrt – schickte am Tag der Preisverleihung ein Einschreiben Rückschein, um uns von der Verlesung der Laudatio abzuhalten. Natürlich haben wir den Preis wie geplant verliehen. Wir wussten, unsere Recherche ist wasserdicht – und Lidl wusste, dass sie mit einer Klage gegen die BigBrotherAwards noch mehr unerwünschte Öffentlichkeit bekommen würden. Lidl – die bis dato sagten, ihre Beziehung zur Presse bestünde darin, dass sie keine hätten – zog die Konsequenz. Nein, Lidl hörte nicht auf mit der Arbeitnehmerüberwachung, sondern schaffte sich eine Public Relations Abteilung an.

Die Politik ist weitgehend beratungsresistent. Weder Otto Schily noch Ulla Schmidt noch Volker Bouffier sind nach ihrem BigBrotherAward zurückgetreten. Doch immerhin war der Datenskandal bei der **Deutschen Bahn** das Ende von Bahnchef Hartmut Mehdorn. Und hier und da gibt es späte Erfolge:

2002 hatten wir das **BKA** für seine Präventiv-Dateien ausgezeichnet. 2008 hat das Niedersächsische Oberverwaltungsgericht festgestellt, dass es im Fall der „Gewalttäterdatei Sport“ keine zureichende Rechtsgrundlage gibt – sie muss also gelöscht werden. Das gilt auch für die anderen Präventiv-Dateien.

Im Jahr 2000 hatten wir dem **Ausländerzentralregister** (AZR) einen BigBrotherAward verliehen wegen institutionalisierter Diskriminierung von hier lebenden nichtdeutschen Bürgern. Inzwischen hat der Europäische Gerichtshof mit Urteil vom 16.12.2008 festgestellt, dass das AZR gegen das Diskriminierungsverbot verstößt.

An anderer Stelle, wo wir auf illegale Praktiken hingewiesen haben, wurden die zwar zunächst abgestellt. So gab es 2003 einen BigBrotherAward für **T-Online** für die Speicherung von Verbindungsdaten, obwohl die bei einer Flatrate nicht zur Abrechnung gebraucht werden. Ein Nutzer klagte gegen T-Online und gewann. Doch

Foto: Claudia Fischer, cc by-sa 4.0

Lidl reagierte heftig auf den BigBrotherAward: Nach der Preisverleihung gründete das Unternehmen erstmals eine PR-Abteilung.

Digitalcourage, cc by-sa 4.0

Dieses Bild ging um die Welt: Wir demonstrierten 2004 vor dem Metro Future Store in Rheinberg gegen Schnüffelchips auf Frischkäse und Shampoo.

nun ist dies wieder hinfällig, denn zum Januar 2008 wurde die Vorratsdatenspeicherung sämtlicher Kommunikationsverbindungen von Telefon und Internet eingeführt.

Die **Metro AG** war 2003 nominiert für ihren „Freilandversuch“ mit RFID-Funkchips auf den Waren in einem Supermarkt in Rheinberg bei Duisburg. RFID sind winzige Chips mit Antenne, die Informationen über das Produkt und eine eindeutige Seriennummer enthalten, die per Funk ausgelesen werden können. Eine Gefahr für die Privatsphäre, denn das Auslesen funktioniert ohne Sichtkontakt, kann also unbemerkt geschehen. Wie berechtigt der BigBrotherAward für die Metro AG war, stellten wir erst einige Monate später fest. Der FoeBuD deckte auf, dass der Konzern RFID-Schnüffelchips auch in den Payback-Kundenkarten des Supermarktes versteckt hatte – ohne Wissen der Kunden. Der FoeBuD brachte den Fall in die Presse und organisierte eine Demonstration – dies war die erste Demonstration gegen die RFID-Technologie, die Bilder gingen um die Welt.

Schließlich zog Metro die verwanzte Karte zurück. Ein Erfolg, der viele beflügelt hat – und gezeigt hat, dass Widerstand nicht zwecklos ist. Der Spiegel schrieb damals:

Digitalcourage wirkt, wirken Sie mit!

https://digitalcourage.de/spende

„Es ist ein ungleicher Kampf – eine Handvoll ehrenamtlicher Enthusiasten vom FoeBuD gegen milliardenschwere Konzerne – doch er zeigt Wirkung.“

▶Der eigentliche Erfolg aber ist in den Köpfen der Menschen passiert.◀

▶Vom kleinen Club zur Bürgerrechtsbewegung

Der eigentliche Erfolg aber ist in den Köpfen der Menschen passiert. Datenschutz ist als Thema in der Mitte der Gesellschaft angekommen. Dass in den letzten eineinhalb Jahren so viele Datenschutzvergehen aufgeflogen sind – hat auch mit dem gestiegenen Bewusstsein zu tun, dass da Unrecht geschieht – und dass wir dagegen vorgehen müssen.

Aus der „Handvoll“ Enthusiasten (Zitat Spiegel) ist mittlerweile eine große Bürgerrechtsbewegung geworden. Die Verfassungsbeschwerde gegen die Vorratsdatenspeicherung hat über 34.000 Beschwerdeführer gefunden – das ist die größte Verfassungsbeschwerde in der Geschichte der Bundesrepublik. Anlässlich unserer Demonstrationen gegen Überwachung unter dem Motto „Freiheit statt Angst“ gehen immer wieder viele Zehntausend Menschen auf die Straße. Zur Großdemonstration diesen September in Berlin haben über 160 Organisationen mit uns gemeinsam aufgerufen.

Neben uns Bürgerrechtlern waren das Berufsverbände von Journalisten, Ärzten und Anwälten, Beratungsorganisationen, Gewerkschaften und Parteien verschiedenster Couleur. Sie alle haben über unterschiedliche Standpunkte hinweg an dieser Stelle für Datenschutz und Bürgerrechte eingesetzt.

- Wir mischen uns ein – zum Beispiel bei den Koalitionsverhandlungen, die gerade laufen... Und wir werden auch weiter dranbleiben. Eins ist klar – unser Einsatz für eine lebenswerte Welt im digitalen Zeitalter hat gerade erst angefangen. Helfen Sie mit.

Foto: Digitalcourage, cc by-sa 4.0

BigBrotherAwards wirken

Entwicklungen von 2010 bis 2017

Von Claudia Fischer

Foto: Fabian Kurz, cc by-sa

BBA-Moderator Andreas Liebold spricht mit Digitalcourage-Campaignerin Kerstin Demuth bei der Preisverleihung 2017 über Tadel und Erfolge

Keine Sorge, wir überwachen unsere inzwischen über 120 Preisträger.innen seit 2000 nicht lückenlos. Wir sind ja kein Geheimdienst! Aber an einigen sind wir drangeblieben. Nicht selten bleiben „unsere“ Datenkraken auch durch selbstproduzierte Pannen und Skandale in den Schlagzeilen.

Allen voran natürlich die **Vorratsdatenspeicherung**. 2009, im vorherigen Kapitel, schrieb Rena Tangens noch, dass sie im Januar 2008 eingeführt worden sei. Wir sammelten mit dem „Arbeitskreis Vorratsdatenspeicherung“ mehr als 35.000 Unterstützer.innen für unsere Verfassungsbeschwerde in Karlsruhe. Im März 2010 kassierte dann das Bundesverfassungsgericht das Gesetz zur Vorratsdatenspeicherung als verfassungswidrig und nichtig. Alle bis dahin gesammelten Daten mussten gelöscht werden. Dann kippte zu unserer Freude im April 2014 auch noch der Europäische Gerichtshof die europäische Richtlinie zur Vorratsdatenspeicherung, weil sie gegen die EU-Grundrechte-Charta verstößt.

In der Anhörung beim EuGH in Luxemburg wurde deutlich, dass kein Land nachweisen konnte, dass Vorratsdatenspeicherung überhaupt positiv auf die Verbrechensaufklärung wirkt. Nach diesem Urteil gab es keinen Vorwand mehr zur Einführung der Speicherung in Deutschland.

Foto: Digitalcourage, cc by-sa 4.0

Übrigens haben wir für RFID-Technologie 2011 nochmal einen BigBrotherAward vergeben: Die Firma Peuterey hatte RFID-Chips in ihre Kleidung eingenäht. Ein Tabubruch, denn damit sind Peuterey-Träger.innen berührungslos identifizierbar, wenn Sie an einer Antenne vorbei gehen.

Doch die Überwachungsfanatiker in der Bundesregierung wollten nicht aufgeben und haben Ende 2015 dank Großer Koalition ein neues Gesetz zur Vorratsdatenspeicherung auf den Weg gebracht (es heißt jetzt „Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten“ – Orwells „Neusprech“ lässt grüßen).

Im Dezember 2016 haben wir in Karlsruhe eine neue Verfassungsbeschwerde gegen das Gesetz eingereicht (siehe Teil 1 „Aktuelles und Begleitendes“ in diesem Jahrbuch). Zum 1. Juli 2017 sollte die Speicherung der Telefon- und Internetdaten eigentlich beginnen. Aber diverse Gerichtsentscheidungen haben das kurz vor knapp verhindert – als dieses Buch in Druck geht, herrscht Verwirrung, ob nun seit 1. Juli 2017 gespeichert werden muss oder nicht. Viele große Telekommunikationsanbieter haben öffentlich gesagt, dass sie nicht speichern werden, bis ein endgültiges Urteil da ist. Allerdings ist nicht ausgeschlossen, dass einige Firmen es doch tun. Fragen Sie also in jedem Fall bei Ihrem Anbieter nach!

▶Eine weitere alte Bekannte haben wir 2017 auch wieder in den Schlagzeilen getroffen: Die Metro AG.◀

Eine weitere alte Bekannte haben wir 2017 auch wieder in den Schlagzeilen getroffen: Die **Metro AG.** 2003 hatten wir sie für den RFID-Chip in der Payback-Kundenkarte ihres „Future-Stores“ in Rheinberg mit einem BigBrotherAward bedacht und dort vor der Tür demonstriert. Das war ein Supermarkt aus der „Extra“-Kette. Nach unseren Protesten hat die Metro AG den RFID-Feldversuch zurückgezogen. Dieses Jahr das gleiche Spiel: Mitte Mai wird bekannt, dass diesmal in 40 „**Real**“-Märkten, die auch zur Metro AG gehören, Videomonitore hängen, in denen Überwachungssensorik zur Gesichtsanalyse verbaut ist – und kurz nachdem der Skandal bekannt wurde und wir Strafanzeige erstattet haben, kam der Rückzug. Aber wir sind sicher: Die Metro AG versucht es immer wieder...

Dass unsere BigBrotherAwards leider noch nicht allen bekannt sind, hatte im Juni 2017 fatale Folgen für eine amerikani-

Überall in Deutschland hängen unsere „Asyl für Snowden“-Aufkleber

Foto: Jochen Wegner, cc by-sa 4.0

sche Whistleblowerin. Sie hatte ein geheimes NSA-Dokument an die Presse weiter gegeben („geleakt“), und die Journalist.innen der Redaktion „The Intercept“ schickten es unbearbeitet an die NSA zur Verifizierung. Hätten die zwei unsere Laudatio von 2004 für **Canon Kopierer** gekannt und etwas weiter recherchiert, hätten sie wissen können, dass inzwischen die Farb-Kopierer und Drucker vieler großer Hersteller Kennungen auf dem Papier hinterlassen. Diese Markierungen sind für das Auge fast unsichtbar (hellgelb auf weiß). Damit können Geräte, Zeitpunkte des Druckes und anderes identifiziert werden. Die amerikanische Whistleblowerin ist nun aufgeflogen und hat unter diesem Versäumnis der Journalisten zu leiden. Immerhin: Die Presse hat dadurch weltweit über diese Panne berichtet, so dass so etwas hoffentlich nicht noch einmal passiert.

Wichtige Lehre aus diesem Fall:

Journalistinnen und Journalisten sollten sich dringend mit Überwachungstechnik und geeigneten Gegenmaßnahmen befassen, um ihre Informant.innen zu schützen!

Das Stichwort „Whistleblowing“ bringt uns natürlich zu **Edward Snowden**, dessen Enthüllungen 2018 bereits 5 Jahre in der Welt sind. Wir hatten ihm 2014 den bislang einzigen Positiv-BigBrother-Award (Julia-und-Winston-Award) verliehen und versprochen, eine Million Aufkleber „Asyl für Edward Snowden“ kostenlos zu verteilen. Gleich in der ersten Woche haben Hunderte Menschen die Aufkleber in unserem Shop bestellt, die wir nur Dank der Hilfe von vielen lieben Freiwilligen, Praktikanten und Mitarbeiterinnen von Flensburg bis Freiburg ins ganze Land verschickt haben. Im September 2014 haben wir den einmillionsten Aufkleber kostenlos rausgeschickt – aber die Nachfrage reißt nicht ab. Die Aufkleber sind weiterhin bei uns im Shop, inzwischen für 10 Cent das Stück, erhältlich (siehe Anzeige).

Im September 2014 haben wir den einmillionsten Aufkleber kostenlos rausgeschickt.

▶… nicht vergessen: Edward Snowden ist auch fünf Jahre nach seinem mutigen Schritt immer noch nicht in Deutschland.◀

Bei aller Freude über so viel Solidarität dürfen wir nicht vergessen: Edward Snowden ist auch fünf Jahre nach seinem mutigen Schritt immer noch nicht in Deutschland, hat hier kein Asyl bekommen und auch nicht vor dem inzwischen beendeten NSA-Untersuchungsausschuss aussagen können, obwohl der Ausschuss 2014 schon beschlossen hatte, ihn anzuhören. Der ehemalige US-Präsident Barack Obama hätte ihn begnadigen können, als er zum Jahreswechsel 2016/17 seinen Posten als Präsident abgab – er hat es aber nicht getan.

Immerhin sorgen solche Diskussionen und diverse Preisverleihungen weltweit aber dafür, dass Edward Snowden im öffentlichen Bewusstsein bleibt, was ihm wahrscheinlich das Leben rettet.

Im selben Jahr 2014 verschafften wir einem anderen Preisträger unerwünschte Öffentlichkeit: **CSC (Computer Sciences Corporation)**. Diese Firma kannte bis dahin fast niemand. Dabei ist die CSC-Mutterfirma in den USA quasi die EDV-Abteilung von CIA, NSA & Co. Sie war auch in andere illegale Geheimdienstaktivitäten verwickelt, u.a. in die Organisation von Entführungsflügen in Foltergefängnisse. Dennoch haben die Bundesregierung und einige Bundesländer dieser Firma IT-Aufträge für wichtige und vertrauliche Infrastruktur gegeben. Das finden wir unerträglich und haben in der BBA-Laudatio für CSC gefordert, dass die Vergaberichtlinien für öffentliche Aufträge geändert werden. „Völlig unmöglich – das wird nicht geschehen“, sagten uns Kontaktpersonen aus dem Innenministerium. Ist es aber doch! Am 16. Mai 2014 berichtete die Süddeutsche Zeitung: „Regierung verschärft Vergaberegeln für sensible IT-Aufträge“ und am 4. März 2015 „Umstrittener NSA-Dienstleister verliert Ausschreibung“.

Lesen Sie weiter auf Seite 118


#snowden
ASYL


ASYL


Facebook
#snowden
ASYL


Welcome to Germany,
Mr. Snowden
Whistle-
blower
gesetzlich
schützen
EDWARD
SNOWDEN
HUSSAGEN
BEWEISE


ASYL


ASYL

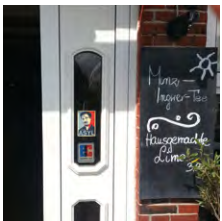

COL D'AUBISQUE
ALTITUDE 1709 m
AGGELES - GAZOST
30 km
EAUX - BONNES
12 km


ASYL


ASYL


ASYL

Eine Million Aufkleber „Asyl für Edward Snowden“



Fortsetzung von Seite 115

> „…das Betriebsklima habe sich seit dem BigBrotherAward deutlich verbessert.“

Ein weiterer Erfolg, der erst mit Verzögerung sichtbar wurde, war der BigBrotherAward 2012 für **Bofrost** wegen der Bespitzelung ihres Betriebsrates. Nachdem die Firma zunächst sehr ungehalten auf den BBA reagiert hatte, wurden wir einige Jahre später vom Bofrost-Betriebsrat kontaktiert: Sie hätten gerne nachträglich die BigBrotherAward-Statue, die bei der Verleihung nicht abgeholt worden war. Denn das Betriebsklima habe sich seit dem BigBrotherAward deutlich verbessert, so dass sie jetzt die BBA-Statue gerne als Erinnerung bei sich in eine Vitrine stellen wollten. :-)

Foto: Digitalcourage, cc by-sa 4.0

Viel Aufsehen erregte 2016 der BigBrotherAward für die Kampagnenplattform **Change.org**. Unsere Begründung: Sie geben sich den Anstrich einer gemeinnützigen Organisation – doch in Wirklichkeit ist Change.org ein US-Unternehmen, das mit den Daten derer handelt, die Petitionen unterzeichnen. Fairerweise, so empfahlen unsere Laudatoren Sönke Hilbrans und Peter Wedde, sollten sie sich in change.COM umbenennen. Neben ihrer bekannten Kampagnen-Homepage change.org gibt es jetzt eine neue Website www.changeverein.org. Dort heißt es: „Wir sind ein unabhängiger Verein – Change.org e.V. – mit einer Lizenzvereinbarung mit Change.org und unterstützen die Kampagnen von Nutzer/innen in Deutschland mit unserer Expertise.“

Change hat zwar nach dem BigBrotherAward gelobt, keine gesponserten Petitionen mehr zu machen. Dennoch landen die Daten aller Unterzeichnenden weiterhin auf unsicheren Servern in den USA, wo Geheimdienste sich jederzeit bedienen und sich damit Einsicht in die politischen Ansichten von Menschen in Europa verschaffen können. Immerhin sind seit der Preisverleihung die Aktivistinnen und Aktivisten hierzulande gewarnt – und können in Zukunft sicherere Plattformen für ihre Appelle benutzen.

“Der gläserne Kunde”,
Skulptur von Peter Ehrentraut und Angelika Höger, 2004

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 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!

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. Oder Sie geben unsere Stichworte in Ihre Lieblings-Suchmaschine ein, wenn Sie Links oder Details zu unseren Tipps brauchen.

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

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

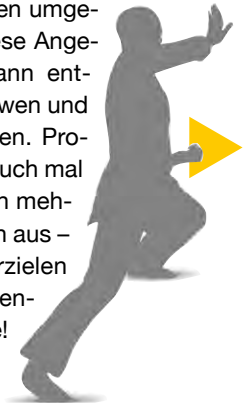
Selbstverteidigungsabbildungen: Panthermedia

Suchmaschinen: Sie brauchen mehr als eine!

Google hat aus vielen Gründen den BigBrotherAward 2013 erhalten: Google ist ein Konzern, der aus Wissen und Daten ein Geschäft macht und dafür auch noch ein Monopol anstrebt. Google arbeitet intransparent – es ist unbekannt, wie die Treffer auf Suchanfragen zustande kommen und wie sie angeordnet werden.

Außerdem sammelt Google ungeheuer viele Daten über seine Benutzer.innen und muss durch den Patriot Act mit Geheimdiensten kooperieren. Ähnliche Probleme gibt es auch bei Bing, Yahoo, Ask und Co. Gleichzeitig ist Google sehr zurückhaltend mit dem eigenen Wissen: Nur die ersten 1000 Treffer einer Suche werden angezeigt. Das klingt viel, ist aber nur ein kleiner Bruchteil aller Ergebnisse. Ähnliche Probleme gibt es auch bei Bing, Yahoo, Ask und Co. Das Geheimnis liegt im Index.

Auf der nächsten Seite werden wir Ihnen nicht bestimmte Suchmaschinen empfehlen, sondern zeigen, wie unterschiedlich Suchdienste mit Daten umgehen und wie sich diese Angebote finanzieren. Dann entscheiden Sie selbst, wen und was Sie nutzen wollen. Probieren Sie übrigens auch mal die gleiche Anfrage in mehreren Suchmaschinen aus – unter Umständen erzielen Sie damit überraschende neue Erkenntnisse!



Vorab aber ein paar Hintergründe:

Beim Suchen kommt es auf den Index an

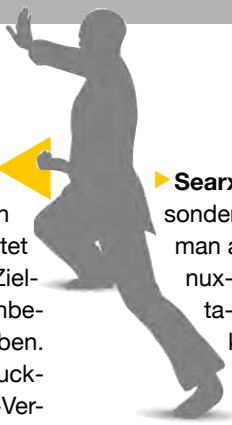
Suchmaschinen sind so gut wie ihr Index. Das ist die Sammlung der Schlagwörter, die schnell durchsucht werden kann, um die Seiten mit den gewünschten Inhalten im unübersichtlichen Internet zu finden. Der Aufbau eines guten Indexes ist kostenintensiv. Kleine Suchmaschinen, die keine oder wenig Werbung einblenden, haben oft zu wenig Geld zum Durchsuchen des gesamten Internets zur Verfügung. Ihre Suchergebnisse liefern oft nicht die gewünschten Treffer. Andere Seiten wie startpage und ixquick nutzen den Index der Großen wie Google, Bing, Yahoo oder Yandex.

Für einen offenen Webindex

SUMA e.V. – Verein für freien Wissenszugang – hat einen Aufruf für einen offenen Webindex gestartet. Ziel ist es, einen frei zugänglichen Webindex zu schaffen, der von unterschiedlichen Suchmaschinen und anderen Diensten genutzt werden kann.

Folgende Suchmaschinen können eine Alternative zu Google sein:

- **DeuSu** arbeitet werbefrei und wird ausschließlich durch Spenden finanziert. DeuSu betreibt einen eigenen Suchindex, während Meta-Suchmaschinen die Suchergebnisse anderer (z.B. Google oder Bing) nutzen. Das Thema Suchindex erklären wir weiter unten.



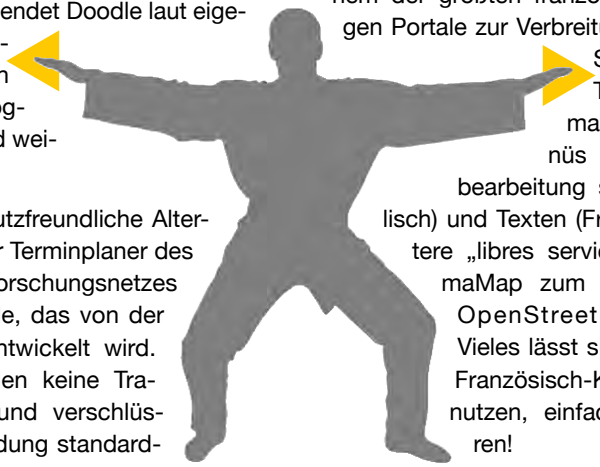
- **duckduckgo.com** unterhält einen Suchindex, speichert nach eigenen Angaben keine IP-Adressen und leitet Suchanfragen so weiter, dass die Zielseite keine Informationen über Suchbegriffe erhält, die Sie eingegeben haben. Wenn es möglich ist, leitet DuckDuckGo immer auf Seiten mit „HTTPS“-Verschlüsselung um. DuckDuckGo arbeitet mit Online-Shops zusammen und erhält Geld, wenn Suchanfragen zum Kauf führen. DuckDuckGo sitzt in den USA und unterliegt dem Patriot Act.
- **eTools.ch** ist wie metager.de eine Meta-Suchmaschine, die verspricht, keine persönlichen Daten zu speichern. Wir empfehlen, in den Präferenzen „HTTPS“ und die Methode „POST“ zu aktivieren, damit der Suchausdruck nicht in der URL erscheint (wie ixquick.eu und startpage.com es vormachen).
- **ixquick.eu** ist eine Meta-Suchmaschine über Gigablast, Yandex und Yahoo, die 2008 vom Europäischen Datenschutzbeauftragten Peter Hustinx das erste Europäische Datenschutzgütesiegel „EuroPriSe“ erhielt. Die Seite finanziert sich über gesponserte Treffer auf den Ergebnisseiten.
- **metager.de** wird vom SUMA-EV – Verein für freien Wissenszugang – mit Sitz in Hannover entwickelt. Metager speichert nach eigenen Angaben weder Ihre IP-Adresse noch den „Fingerabdruck“ Ihres Browsers, verzichtet auf Tracking und bietet einen Zugang über das anonyme Tor-Netzwerk. Metager wird finanziert über Spenden, Fördermitgliedschaften und Text-Werbe-Links.
- **Searx** ist eigentlich kein Dienst, sondern freie Software, mit der man auf dem eigenen kleinen Linux-Server eine schlanke Meta-Suchmaschine aufsetzen kann. Sie verspricht, die Privatsphäre zu respektieren.
- **startpage.com** ist die Schwesterseite von ixquick, bezieht aber ihre Suchergebnisse von Google. Sie gehört ebenfalls dem niederländischen Unternehmen Surfboard Holding B.V. und verdient nach eigenen Angaben mit „eindeutig gekennzeichneten, gesponserten Links“ Geld. Die Datenschutzrichtlinien sind dieselben wie bei ixquick. Teilweise stehen Server von startpage in den USA und unterliegen damit dem Patriot Act. In den Sucheinstellungen kann man den Serverstandort (EU oder USA) mittlerweile selbst wählen.
- **YaCy.net** ist ein dezentrales Suchkollektiv auf Basis einer freien Suchmaschinensoftware. „YaCy läuft nicht auf einem Server im Internet, sondern auf Ihrem eigenen Rechner“ und strebt Informationsfreiheit an, indem alle Nutzer.innen zu einem verteilten Suchindex beitragen. Laut eigenen Angaben werden keine Nutzerdaten gesammelt, und Zensur ist dadurch erschwert, dass der Index verteilt und der Quellcode öffentlich ist. Nach dem Download und dem Starten der Java-Software kann man den eigenen YaCy-Knoten so komfortabel wie andere Suchmaschinen per Webbrowser benutzen.

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. Außerdem wird nicht standardmäßig HTTPS verwendet, sodass die Daten unter Umständen nicht verschlüsselt übertragen werden. 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.

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 Open Source, 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!

Alternativen zu Dropbox und Cloud

Illustrationen: Isabel Wienold

Prinzipiell gilt: „Es gibt keine Cloud, nur die Computer anderer Leute.“ Aus diesem Grund hat „die Cloud“ 2012 auch einen BigBrother-Award gewonnen. Es gibt jedoch viele gute Alternativen zu den „Computern anderer Leute“.

Viele Argumente gegen Dropbox

Dropbox ist beliebt und bequem, aber problematisch in Bezug auf Datenschutz und Datensicherheit. Das Unternehmen setzt auf die Amazon-S3-Cloud und speichert in den USA. Damit haben US-Behörden Zugriff auf die Daten. Nur Daten von Firmenkunden speichert das Unternehmen auf Wunsch in Europa, aber auch hier in der Struktur von Amazon. Große Mengen von Daten sind für Hacker attraktive Ziele. Liegen Ihre Daten bei großen Unternehmen, gehen Sie immer das Risiko ein, Opfer eines Massenhacks zu werden. Hacker haben 2012 eine Datenbank von Dropbox kopiert. Im Oktober 2016 wurden 68 Millionen E-Mail-Adressen und Passwörter online veröffentlicht. Und bereits ein Blick auf die Dropbox-„Datenschutzrichtlinien“ genügt, um zu erkennen, dass Ihre Daten bei diesem Dienst nichts verloren haben.

Wir haben die folgenden „Dropbox-Alternativen“ nicht technisch geprüft und die Liste ist auch nicht vollständig. Wie schon bei den Suchmaschinen sprechen wir keine Empfehlungen aus, sondern erläutern nur ein paar Hintergründe.

Synchthing speichert die Daten gar nicht in die Cloud, sondern synchronisiert sie zwischen Geräten. Einfach auf den Geräten installieren und sie miteinander bekanntmachen. Der Quelltext ist frei und damit einsehbar.

SpiderOak ist ein US-amerikanischer Anbieter, der von Edward Snowden empfohlen wurde. Das Datenschutzprinzip „Zero-Knowledge“ ist einen gründlichen Blick wert.

Teamdrive wird in Hamburg entwickelt und wurde mit dem Datenschutzgütesiegel des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein ausgezeichnet. Teamdrive kann die Daten auch mit einem eigenen Server synchronisieren, siehe unten.

Tresorit wird in Ungarn entwickelt, von der Europäischen Union unterstützt, erklärt sich als Zero-knowledge-Dienst und informiert ausführlich über Datenschutzbestimmungen.

Ein Tipp: Studierende und Forschende bekommen häufig über die Rechenzentren ihrer Hochschule Speicherplatz zur Verfügung gestellt. Fragen lohnt immer, aber auch dort gilt, auf Sicherheit zu achten.

Cloud selber machen: allein oder mit Freund.innen!

Wer Dienste nutzt, um Daten abzulegen oder zu transportieren, muss sowohl die Angaben in den Datenschutzrichtlinien als auch die technische Funktionsweise kennen und ihnen vertrauen. Darum ist es eine gute Idee, IT selbst in die Hand zu nehmen. Alleine ist es mühsam, aber wer sich organisiert, lernt viel und gewinnt Unabhängigkeit. Das FreedomBox-Projekt hat hier schon viel Vorarbeit geleistet und stellt vorkonfigurierte Systeme bereit, die auch auf stromsparenden Kleinstcomputern laufen. Wenn Sie selbst ein System zusammenstellen möchten, könnten Sie folgende Komponenten in Erwägung ziehen:

OwnCloud bzw. die Abspaltung **Nextcloud** bietet nicht nur Datenablage und -synchronisation, sondern auch Kalender und Adressbücher. Es lässt sich mit wenig Aufwand auf einem eigenen Server installieren, denn die Voraussetzungen sind einfach zu erfüllen: Ein Webserver mit PHP genügt. Aktuelle Versionen bringen die Fähigkeit zur Dateiverschlüsselung mit – am besten aktiviert man sie gleich beim Installieren. Für Firmen und andere Organisationen bieten beide kostenpflichtige professionelle Unterstützung („Enterprise Support“) an. Wer nur eine zentrale Datenablage mit Synchronisierung braucht, ist mit Seafile vielleicht besser bedient.

Seafile ist eine freie, quelloffene Software, die stark an Dropbox erinnert. Freie Clients gibt es für Windows, Mac und Linux (einschließlich Android). Die Serversoftware kann man auf dem eigenen Raspberry Pi, einem anderen Linux-Computer oder unter Windows installieren, und Dateiverschlüsselung ist möglich. Ein Online-Kalender mit CalDAV-Unterstützung wie bei ownCloud/Nextcloud ist nicht enthalten. Dafür wird oft Baïkal separat installiert.

Synchthing ist eine gute Möglichkeit, die IT im eigenen Viertel oder in der eigenen Stadt selbst in die Hand zu nehmen. Der Server speichert keine Daten, daher benötigen die Server-Komponenten nicht viel Plattenspeicher und Sie können dafür einen günstigen virtuellen Server benutzen.

Auch bei **Teamdrive** kann man den Server-Teil der Software auf einem eigenen Server installieren und damit die Kontrolle über die Daten behalten. Die Daten werden sogar per Voreinstellung verschlüsselt gespeichert. Wer bereits einen WebDAV-Server installiert hat, kann auch den verwenden. Leider ist Teamdrive nicht quelloffen.

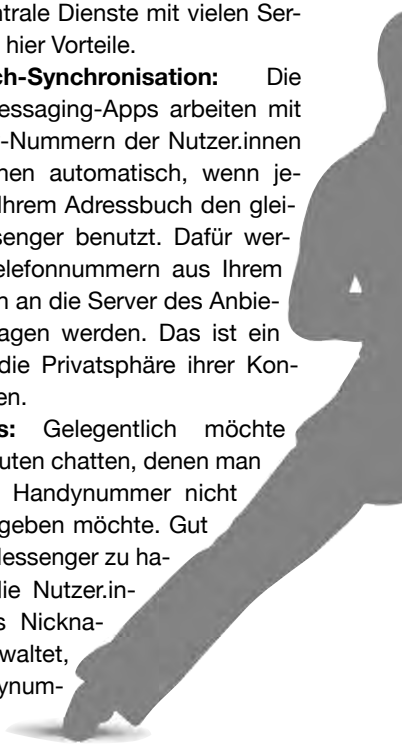
Auch **Pydio** kann man auf einem eigenen Server betreiben.

„WhatsApp kommt mir nicht in die Hosentasche!“

Ob Kindergeburtstag, Arbeitsanweisungen oder Urlaubsfotos: Bei vielen Aktivitäten geht kaum noch etwas ohne WhatsApp. Dabei sollten Sie aufpassen: WhatsApp gehört zu Facebook. Unternehmen wie Facebook leben von Werbung und Datenhandel und arbeiten, wenn nötig, mit Geheimdiensten zusammen. Die verwendete Software ist nicht frei. Die versprochene Ende-zu-Ende-Verschlüsselung bei WhatsApp hat Lücken: z.B.wandern die Telefonnummern der Kommunikationspartner.innen nach wie vor im Klartext durchs Internet.

Aus unserer Sicht sollten „gute“ *Messenger* folgende Kriterien erfüllen:

- **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. Dies ist uns besonders wichtig, damit eine Alternative langfristig nicht zu einem „zweiten WhatsApp“ wird.
- **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.
- **Adressbuch-Synchronisation:** Die meisten Messaging-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 werden. Das ist ein Eingriff in die Privatsphäre ihrer Kontaktpersonen.
- **Nicknames:** Gelegentlich möchte man mit Leuten chatten, denen man die eigene Handynummer nicht unbedingt geben möchte. Gut ist, einen Messenger zu haben, der die Nutzer.innen mittels Nicknames verwaltet, ohne Handynummern.



Selbstverteidigungsabbildung: Panthermedia

- **Betriebssysteme:** Wir möchten mindestens Android und das iOS (iPhone/iPad) unterstützt sehen, da diese mehr als 90% des Marktes ausmachen. Der Anbieter sollte jedoch auch andere Betriebssysteme ermöglichen.
- **Ohne Playstore:** Die App sollte in allen gängigen App-Stores angeboten werden – nicht nur im Google Play Store, sodass 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.
- Manche dieser Kriterien wiegen schwerer als andere – welche Ihnen wichtig ist, müssen Sie selbst entscheiden. Auch hier gilt wieder: Die folgenden Alternativen zu WhatsApp sind keine Empfehlungen, sondern wir möchten Sie über Hintergründe informieren:
  - **Signal (ehemals Textsecure)** bietet vertrauliche Kommunikation dank Ende-zu-Ende Verschlüsselung. Bei einer unabhängigen Prüfung hat sie gut abgeschnitten. Signal ist eine quelloffene, freie Software, übersichtlich und intuitiv bedienbar. Allerdings lädt auch Signal Ihr Adressbuch auf den Server hoch. Für einige Funktionen in App und Web-Browser greift Signal auf Google-Dienste zurück.
  - **Threema** ist nicht quelloffen. Deshalb lassen sich Threemas Aussagen über die verwendete Verschlüsselung nicht nachprüfen. Somit ist der einzige Vorteil von Threema gegenüber WhatsApp/Facebook, dass der Dienst weniger Marktmacht hat. Da sich das schnell ändern kann und weil es quelloffene Alternativen gibt, empfehlen wir Threema nicht mehr.
  - **Surespot** ist ein eigenständiger Messenger und bietet Ende-zu-Ende-Verschlüsselung. Aus Datenschutzgründen synchronisiert die App nicht Ihr Adressbuch. Leider ist diese App vergleichsweise schlecht bedienbar und auch schlecht ins Deutsche übersetzt. Surespot ist eine quelloffene, freie Software, die aber nur 1000 Nachrichten speichert. Außerdem ist die App unter Android ohne Play Store nicht nutzbar.
  - **Telegram** ist ein eigenständiger Messenger mit Ende-zu-Ende-Verschlüsselung – jedoch nur als optionale Funktion, die man jeweils selbst anwählen muss. Die Kryptografie („Verschlüsselung") wird als anfällig bewertet und wurde bereits einmal gebrochen. Telegram lädt Ihre Kontakte auf den eigenen Server.
  - **XMPP** (auch als „**Jabber**" bekannt) ist ein offenes Protokoll, das ursprünglich für das Chatten auf Desktop-PCs entwickelt wurde. Es gibt zahlreiche Desktop Clients für XMPP, z.B. **Pidgin** für Windows, Linux, BSD und Solaris. Man kann mit Kontakten (ohne Adressbuch-Upload) chatten, ohne die eigene Telefonnummer herauszugeben.

Für E-Mails einen sicheren Anbieter finden

Zu E-Mail- Diensten, die Ihre Nachrichten verschlüsselt durchs Netz schicken, hat unsere AG Digitale Selbstverteidigung eine E-Mail vorbereitet, die Sie an Freunde verschicken könnten:

Liebe.r ...,

nerven Dich die andauernde Werbung und die blinkenden Anzeigen in Deinem E-Mail Postfach? Mich stören diese Zeitfresser ja ziemlich. Mich stört auch, dass meine Post bei web.de, GMX, Yahoo und Gmail (Google) nicht vor automatischer Auswertung sicher ist. Und meine Daten geben sie auch noch weiter. Ich fände es gut, wenn wir uns über Anbieter schreiben, die sich mehr Gedanken um Privatsphäre und Datenschutz machen.

Gmail durchsucht beispielsweise automatisiert sämtliche E-Mails, benutzt die Daten für individualisiertes Marketing (inhaltlich passende Werbung) und gibt die Daten im Zweifelsfall auch weiter. Brisant ist, dass Gmail auch Inhalte von Mails durchstöbert, die von anderen Postfachdiensten abgeschickt wurden. Damit bin nicht nur ich als Gmail-Nutzerin betroffen, sondern auch Du mit Deiner Adresse bei einem anderen Anbieter. Und GMX gewann schon im Jahr 2000 einen BigBrotherAward.

Welche Postfächer haben‘s drauf?

Anbieter wie Posteo und mailbox.org bieten werbefreie und datenschutzfreundliche Postfächer. Sie können anonym eingerichtet werden und die Server werden mit Öko-Strom betrieben. In jedem Fall solltest Du die Nutzungsbedingungen genau lesen und bei Unklarheit nachfragen. Wie kompetent und freundlich die Anbieter sind, kannst Du mit einem Anruf rausfinden. Die Daten werden beim Transport durchs Internet verschlüsselt. Eine Ende-zu-Ende-Verschlüsselung (nächstes Kapitel) sollte man zusätzlich vornehmen. Ein weiteres Qualitätsmerkmal sind die Transparenzberichte, die einige Anbieter veröffentlichen. Auch hier sind posteo.de und mailbox.org vorbildlich. Sind diese detailliert genug? Wurde jeder behördlichen Anfrage stattgegeben oder die Berechtigung genau geprüft?

Liebe Grüße,

Dein.e ...

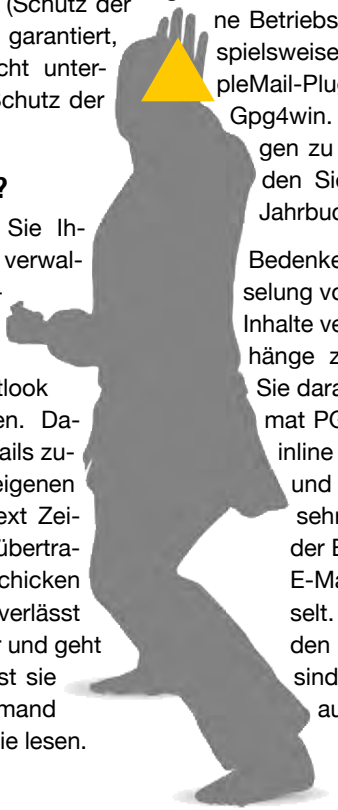
PS: Nein, das ist keine Werbe-Mail, Digitalcourage bekommt dafür kein Geld von den oben genannten Anbietern.

E-Mails verschlüsseln

Vertrauenswürdige E-Mail-Anbieter, wie wir sie eben beschrieben haben, verschlüsseln die Mails zwar auf dem Weg durchs Netz, auf dem Rechner Ihres Gegenübers können sie aber ohne weiteres geöffnet und gelesen werden. Nur wenn Sie eine E-Mail aktiv Ende-zu-Ende-verschlüsseln, kann nur die adressierte Person diese Nachricht mit elektronischen Schlüsseln und einem Passwort öffnen. Elektronische Schlüssel müssen Sie vorher angelegt und mit der Person ausgetauscht haben. So können Sie sich auch sicher sein, dass Sie wirklich mit der richtigen Person kommunizieren (Schutz der Authentizität). Und es wird garantiert, dass der Inhalt der Nachricht unterwegs nicht verändert wird (Schutz der Integrität).

▶Wie geht verschlüsseln?

Der erste Schritt ist, dass Sie Ihre Mails nicht im Browser verwalten, sondern auf Ihrem Rechner 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. PGP steht für „Pretty Good Privacy“ (zu deutsch: „ziemlich gute Privatsphäre“), und wurde Anfang der 1990er Jahre von Phil Zimmermann entwickelt. Früher brauchte man für die Nutzung ein ganzes Handbuch, das wir schon in den 1990er Jahren herausgebracht haben.

In der Zwischenzeit ist es mit der Thunderbird-Erweiterung (Add-On) Enigmail, die auf der modernen PGP-Reimplementierung GnuPG aufbaut, richtig einfach geworden. GnuPG gibt es für verschiedene Betriebssysteme. So gibt es beispielsweise unter Mac OS X ein AppleMail-Plugin. Für Windows gibt es Gpg4win. Die Links und Anleitungen zu beiden Programmen finden Sie ganz einfach über die Jahrbuch-Webseite (siehe unten).

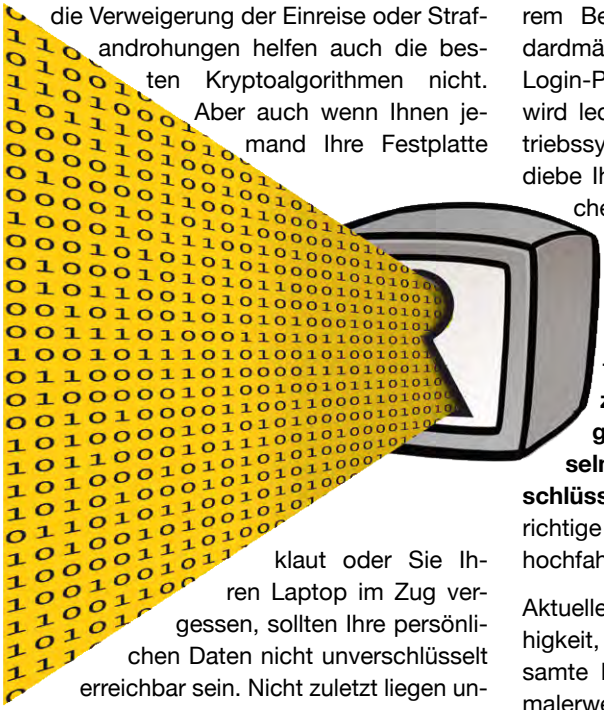
Bedenken Sie: Bei der Verschlüsselung von E-Mails werden nur die Inhalte verschlüsselt. Um auch Anhänge zu verschlüsseln, achten Sie darauf, das Übertragungsformat PGP/MIME und nicht PGP/inline zu verwenden! Absender und Empfänger sind trotzdem sehr leicht einsehbar. Auch der Betreff (engl.: Subject)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

Selbstverteidigungsabbildungen: Panthermedia

Festplatten verschlüsseln

Warum Festplatten verschlüsseln?

Die Daten, die Sie auf Ihrem eigenen Computer oder auf einer transportablen Festplatte speichern, sollten Sie ebenfalls verschlüsseln. 2017 wurde viel darüber diskutiert, dass z.B. die USA unter Präsident Donald Trump Menschen bei der Einreise auffordern, ihre Festplatten durchsuchen zu lassen. Gegen das Erpressen Ihres Passwortes durch physische Gewalt, die Verweigerung der Einreise oder Strafandrohungen helfen auch die besten Kryptoalgorithmen nicht. Aber auch wenn Ihnen jemand Ihre Festplatte



klaut oder Sie Ihren Laptop im Zug vergessen, sollten Ihre persönlichen Daten nicht unverschlüsselt erreichbar sein. Nicht zuletzt liegen unter Umständen auch Ihre Passwörter ungeschützt auf Ihrer Festplatte.

Auch die vermeintlich sicherste Datenverschlüsselung kann jedoch gebrochen werden. Seien Sie deshalb sorgfältig bei der Auswahl von Passwörtern, im Umgang mit unseren Tipps und informieren Sie sich genau über die verwendete Software! **Außerdem ist eine Festplattenverschlüsselung nur wirksam, während das Gerät ausgeschaltet ist.** Lassen Sie Ihr Gerät also möglichst nicht lange unbeaufsichtigt laufen.

Was soll verschlüsselt werden?

Die Daten auf Ihrer Festplatte und in Ihrem Benutzerverzeichnis werden standardmäßig nicht verschlüsselt. Durch das Login-Passwort für das Benutzerkonto wird 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. Wenn Sie die Festplatte verschlüsseln,** bedeutet das: Ohne das richtige Passwort kann Ihr Rechner nicht hochfahren.

Aktuelle Betriebssysteme bringen die Fähigkeit, Dateien, Partitionen oder die gesamte Festplatte zu verschlüsseln, normalerweise mit. Die verschiedenen Betriebssysteme nutzen dabei unterschiedliche Lösungen. Informieren Sie sich auf unserer Webseite über die Möglichkeiten, die Ihr Betriebssystem Ihnen bietet und über speziell zu installierende Programme.

Illustration: Isabel Wienold

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. Außerdem ist die Offline-Nutzung absolut datensparsam.

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.

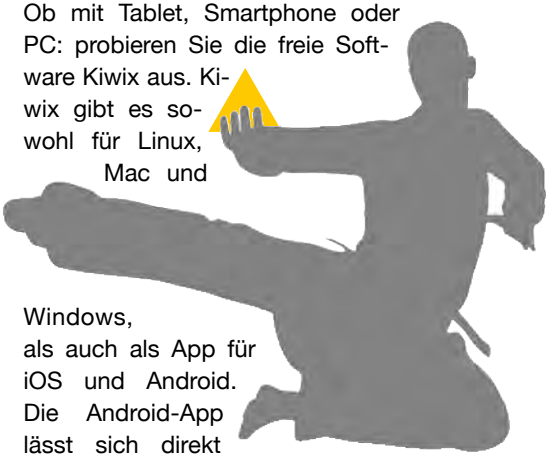
OsmAnd – App, die Navigation offline kann

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.

Vorratsdatenspeicherung – und wenn Sie kommt, was dann?

Die Vorratsdatenspeicherungskrake lauert – ob wir sie gerichtlich aufhalten können oder ob es politisch noch ein Einsehen gibt („Herr, wirf Hirn vom Himmel!"), ist völlig offen. Und wenn sie kommt, was dann? Einige Hinweise haben Sie bereits auf den vorhergehenden Seiten erhalten. Andere Möglichkeiten, auf die Vorratsdatenspeicherung zu reagieren, sind sehr technisch, wie zum Beispiel zum Tor-Netzwerk oder VPN-Verbindungen – dafür sollten Sie lieber im Internet vorbei schauen (unsere Tipps sind ganz einfach zu erreichen über die Jahrbuch18-Seite, siehe unten). Außerdem sind hier noch ein paar Tipps in Kurzform:

Internet-Telefonie (VoIP)

Die Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation der Bundesnetzagentur (Stand TR TKÜV 7.0) ist detailreich, aber unklar. Wir haben der Bundesnetzagentur 12 Fragen geschickt und um Klärung gebeten. Noch haben wir keine Antwort erhalten – wenn wir eine Antwort bekommen, werden wir sie auf unserer Webseite veröffentlichen. Wer sich für Internet-Telefonie interessiert, kann sich beispielsweise die Projekte **Open Secure Telephony Network (OSTN)** oder **Linphone** ansehen.

Freifunk nutzen und unterstützen!

„Erbringer öffentlich zugänglicher Telekommunikationsdienste" müssen Verbindungs- und Ortsdaten speichern. Gehört die „Freifunk"-Initiative dazu? Muss sie die Vorratsdatenspeicherung umsetzen? Freifunk ist eine nichtkommerzielle Initiative, die ein freies Funknetz aufbaut, das aus selbstverwalteten lokalen Computernetzwerken besteht. Es ist noch offen, ob „Freifunk" sich dem Überwachungszwang widersetzen kann – und Sie können das unterstützen! Freifunk Rheinland schrieb: „Wir wehren uns, ein paar Chancen gibt es noch." Nach Meinung von Digitalcourage ist Freifunk durch die Vorratsdatenspeicherung nicht zur Überwachung verpflichtet.

Anonyme SIM-Karten nutzen (soweit möglich)

Seit 1. Juli 2017 sind Prepaid-Anbieter verpflichtet, beim Verkauf von Prepaid-Karten die Identität der Käufer.innen festzustellen. Anonyme Prepaid-Karten gibt es damit nicht mehr. Dennoch: Teilweise sind in anderen EU-Ländern und bei einigen Prepaid-Anbietern noch SIM-Karten zu erhalten, ohne dass ein Personalausweis vorgelegt werden muss. Ein anderer Weg zu einer SIM-Karte führt über eine Tauschbörse für Prepaid-Handykarten. Hier gibt es einiges zu beachten: Zum Beispiel ist das nur sinnvoll, wenn Handy *und* SIM-Karte austauscht werden, weil mittels (häufig auch umprogramierbarer) IMEI und anderen Kennungen (z.B. IMSI) das Telefon identifiziert werden kann. Schließlich sind es die Verbindungen zu Kontakten, die auf eine Person schließen lassen. Beim Kauf eines Smartphones sollte darauf geachtet werden, dass sich der Ak-

Karikatur: Jascha Buder, cc by-sa 4.0

ku herausnehmen lässt, um es zeitweise ganz ausschalten zu können. Empfohlen sei auch noch eine „Funkschutzhülle“ für das Telefon, die Funkverbindungen verhindert, wenn es ausgeschaltet oder im Flugmodus ist, sonst verliert der Akku Energie durch die Suche nach einem Netz.

Das Smartphone zu Hause lassen

Journalist.innen tun es schon länger, wenn sie sich mit Informant.innen treffen: Leider muss in Zeiten von Vorratsdatenspeicherung überlegt werden, das Smartphone auch mal zu Hause zu lassen. Besonders bei Demonstrationen und anderen Veranstaltungen, die zusätzlich mittels Funkzellenabfrage überwacht werden können, kann es sinnvoll sein, das Telefon nicht mitzunehmen. Nur dann können Sie sicher sein, dass weder Ortungsdaten gespeichert werden, dass Sie nicht abgehört werden können und auch die Funkzellen nicht verraten, wo Sie sich aufhalten. Aber Sie sind natürlich auch nicht erreichbar und können bei brenzligen Terminen auch nicht um Hilfe rufen.

Von Vorratsdatenspeicherung ausschließen lassen

Wer kann, sollte vom Ausschluss von der Verkehrsdatenspeicherung nach § 113b Abs. 6 in Verbindung mit § 99 Abs. 2 Telekommunikationsgesetz (TKG) Gebrauch machen. Demnach dürfen die Einzelverbindungsdaten von Personen, die in der telefonischen Gesundheits- und Seelsorgeberatung arbeiten, nicht gespeichert werden. Voraussetzung dafür ist, dass Sie sich bei der Bundesnetzagentur melden – lesen Sie die entsprechenden Stellen im TKG am besten selbst nach.

Zu guter Letzt (natürlich): Finden Sie sich mit der Vorratsdatenspeicherung nicht ab!

Wir dürfen uns nicht daran gewöhnen, dass jede Telefon- und Internetverbindung per Gesetz überwacht wird. Vorratsdatenspeicherung ist eine Säule des Überwachungsstaats. Technische Gegenwehr kann nicht die Lösung sein – das Gesetz muss weg! Unterstützen Sie uns bei unserer Klage, halten Sie sich auf unserer Webseite oder mit unserem Newsletter auf dem Laufenden. Beteiligen Sie sich an Protesten, sprechen Sie mit Abgeordneten und unterstützen Sie Projekte, die für vertrauliche Kommunikation sorgen!

„Wachsam bleiben!“

Wie Sie eine „Lesung gegen Überwachung“ organisieren

Möchten Sie das Bewusstsein für Freiheit und Bürgerrechte wach halten? Mit Freunden, Nachbarinnen, Arbeitskollegen und Familie darüber sprechen, dass es nicht darum geht, ob jemand „etwas zu verbergen“ hat oder nicht? Organisieren Sie eine „Lesung gegen Überwachung“ – in Ihrem Wohnzimmer, im Cafe um die Ecke, in der Schulaula oder an einer Bushaltestelle. Wir unterstützen Sie gerne dabei.

Das Prinzip: Es wird Belletristik und Fachliteratur, z.B. aus der Philosophie, aus Kinderbüchern oder Science Fiction vorgelesen. Da kommt die Diskussion ganz von alleine.

Wie das geht?
Nichts leichter als das:

- Sie besorgen einen Raum für eine Lesung: Kneipe, Wohnzimmer, Bücherei, Bushaltestelle. Auch kleinste Aktionen zählen.
- Sie besorgen einen oder mehrere Vorleser.innen. Das können Sie selbst sein, oder jemand, den Sie für geeigneter halten (Künstler, Moderatorinnen, Schauspieler, Autorinnen, Musiker etc.).
- Sie melden eine Lesung bei uns an, damit wir sie zusammen mit anderen Lesungen bewerben können.
- Sie werben für Ihre Lesung im direkten Umfeld.
- Sie informieren die lokale Presse und das lokale Radio über Ihre Lesung (wir helfen Ihnen dabei).

Foto: digitalcourage, cc by-sa 4.0

padeluun und Rena Tangens lesen gegen Überwachung im Literaturcafe der Stadtbibliothek Bielefeld

- Bei Bedarf: Twitter-Hashtag #LesenGegenÜberwachung
- Sie suchen Texte aus. Entweder kennen Sie selbst Bücher oder Buchstellen zum Thema, oder Sie lassen sich von uns ein paar Tipps geben. Dabei beachten Sie bitte das Urheberrecht: Texte sind erst „gemeinfrei“, wenn die Autor.innen länger als 70 Jahre tot sind oder wenn sie unter einer Creative Commons Lizenz veröffentlicht wurden. Andere Texte dürfen Sie auch vorlesen, diese müssen dann aber bei der VG Wort gemeldet werden (Das machen wir für Sie, siehe unten).
- Sie machen idealerweise ein Foto von der Veranstaltung und schicken es uns per E-Mail, damit wir es auf der Webseite veröffentlichen können. Sollten Gesichter zu sehen sein, fragen Sie diese Menschen bitte um Erlaubnis.
- Bitte bevorzugen Sie Texte unter freien Lizenzen. Auf unserer Webseite „Lesen-gegen-Ueberwachung.de“ gibt es einen Reader (PDF) mit freien Texten.
- Damit wir die Lesung bei der VG-Wort anmelden können, schicken Sie uns bitte direkt nach der Veranstaltung eine Liste: Autor.innen, Titel, Verlag(e) und gelesene Minuten. Die Kosten für die VG-Wort trägt Digitalcourage.

Viele Lesungen finden am „Safer Internet Day“ (2018 am 6. Februar) statt, zum Tag des Grundgesetzes (23.5.) oder regelmäßig an einem bestimmten Tag im Monat. Trauen Sie sich – Lesen Sie mit!

Ist Ihre Stadt datenschutzfreundlich?

Worauf Sie achten und einwirken können

Von Claudia Fischer und Christian Pietsch

Städte und Kommunen verwalten unsere sensibelsten Daten: Ob Standes- oder Steueramt, ob Grundsicherung oder Schwerbehinderung: die Kommunen wissen viel Privates über ihre Bürgerinnen und Bürger und sollten diese Informationen vertraulich behandeln. Niemanden geht an, wer auf der Website die Informationen zum Wohngeld sucht oder sich die Wegbeschreibung zur Aidsberatung beim Gesundheitsamt anzeigen lässt.

Gleichzeitig stellen Städte und Kommunen die wichtigste Infrastruktur für die Bevölkerung vor Ort dar: Kindergärten und Veranstaltungsorte für Information und Freizeitaktivitäten, öffentlicher Nahverkehr, Strom-, Wasser-, Gasversorgung – fast alles, was wir täglich brauchen, hat mit der Stadt oder Gemeinde zu tun, in der wir leben.

Deshalb haben wir angefangen, Ideen zu sammeln, wie diese direkte Umgebung unseres täglichen Lebens so datenschutzfreundlich wie möglich gestaltet werden kann. Diese Liste ist ausbaufähig. Und sie sollte diskutiert werden.

Wenn Sie mitmachen wollen: Recherchieren Sie in Ihrer Kommune, wie der Stand der Dinge ist. Versuchen Sie, darauf Einfluss zu nehmen, wie bei Ihnen im Ort die Infrastruktur gestaltet wird. Schreiben Sie Briefe oder sprechen Sie die Mitarbeiter.innen im Rathaus so oft wie möglich darauf an, dass Sie Datenschutz wichtig finden und wie Sie sich Ihre Kommunalverwaltung wünschen.

Die Internetseiten Ihrer Verwaltung

Die Webseiten Ihrer Stadt oder Kommune sollten datenschutzfreundlich gestaltet sein. Das gilt ebenso für die Webseiten der stadt-eigenen Betriebe (meist z.B. die Energieversorger oder Nahverkehrsunternehmen, Bädergesellschaften usw.). Dazu sollten alle Webseiten auf HTTPS umge-

Illustration: Isabel Wienold

stellt werden (z.B. https://www.bielefeld.de) – nicht nur bei der Eingabe von Daten in Formulare, sondern jede einzelne Seite. Das Kürzel HTTPS bedeutet, dass ein verschlüsseltes Übertragungsprotokoll verwendet wird, für das die Städte ein Zertifikat brauchen. Das ist technischer Standard, kostet nicht viel oder gar nichts und ist für Techniker unkompliziert umsetzbar.

Niemanden geht an, wer auf der Website Informationen zum Wohngeld sucht.

HTTPS verschlüsselt nicht nur Ihre Daten, wenn Sie z.B. ein Formular online ausfüllen, sondern diese Technik bietet Ihnen auch die Sicherheit, dass Sie es wirklich mit Ihrer Kommune zu tun haben. Wird HTTPS verwendet, kann kein Dritter sehen, welche Seiten Sie aufgerufen haben, und Sie bekommen keine manipulierten Informationen von jemandem, der nur von sich behauptet, zu Ihrer Kommune zu gehören. Ohne HTTPS ist es möglich, dass jemand sich auf dem Kommunikationsweg dazwischen schaltet, ohne dass Sie es auf den ersten Blick bemerken.

HTTPS schützt Daten nur auf dem Transportweg. Die Speicherung von Daten ist davon nicht betroffen. Webserver-Betreiber müssen darauf achten, die gesetzlichen Fristen für die Speicherdauer von Webserver-Logdateien nicht zu überschreiten. Das wird oft vergessen. Am besten ist es, die Webserver so zu konfigurieren, dass die Logdateien keine personenbeziehbaren Daten enthalten. Darum sollten IP-Adressen nur gekürzt oder pseudonymisiert gespeichert werden.

Ein dritter, leicht umzusetzender Aspekt für die IT-Abteilung Ihrer Stadtverwaltung ist der Verzicht auf Inhalte, die von anderen Webseiten nachgeladen werden. So verwenden z.B. viele Internetseiten Facebook-Like-Buttons (BigBrotherAward 2011), Javascript-Bibliotheken oder die Schriften, wie sie z.B. Google (BigBrotherAward 2015) kostenlos anbietet.

Als Beispiel nehmen wir mal solche Schriften, die sogenannten „Web-Fonts“ (Grund für eine Tadelnde Erwähnung für WordPress beim BigBrotherAward 2017): Wenn Sie eine Webseite Ihrer Stadt aufrufen, kontaktiert Ihr Webbrowser automatisch z.B. den Server von Google Fonts, um Ihnen den Inhalt in dieser Schriftart anzuzeigen. Dabei wird unter anderem Ihre IP-Adresse übermittelt, und damit weiß Google, dass Sie diese Seite aufgerufen

Selbstverteidigungsabbildung: Panthermedia

haben. Gleiches gilt für Like-Buttons – Facebook erfährt damit, dass Sie es waren, der oder die auf dieser Seite den Button gedrückt hat – aber auch hierfür gibt es Lösungen, die Ihre Grundrechte respektieren.

▶Was hilft es ihrer Kommune, wenn sie viele Facebook-Likes hat? Stellen Sie diese Aufmerksamkeits-Hascherei in Frage!◀

Diese Abhängigkeiten sind unnötig und können leicht abgestellt werden: Wer Web-Fonts oder Javascript-Bibliotheken benutzen möchte, kann sie einfach auf dem eigenen Webserver ablegen. Websites, die keine nachzuladenden Inhalte verwenden, nennt man „self-contained“ (in etwa übersetzbar mit „eigenständig“). Auf sogenannte Content-Delivery-Networks (CDN) sollte grundsätzlich verzichtet werden. Das Einbinden von Drittanbietern ist oft Gedankenlosigkeit oder Bequemlichkeit – mit Folgen für Sie und Ihre Privatsphäre. Und was hilft es ihrer Kommune, wenn sie viele Facebook-Likes hat? Stellen Sie diese Aufmerksamkeits-Hascherei in Frage!

Und wo wir gerade schon einmal bei Google waren: Wegbeschreibungen und Ortsangaben auf Ihrer städtischen Webseite sollten nicht mit Google-Karten arbeiten, sondern OpenStreetMap verwenden.

Technische Kenntnisse braucht man, um die gängigen Privatsphäre-Checks im Internet zu verstehen, z.B. WebbKoll oder PrivacyScore. Sie finden Links dazu auf unserer Jahrbuch-Webseite (siehe unten). Geben Sie bei diesen Anbietern den Namen Ihrer kommunalen Webseite ein und schicken Sie die Ergebnisse an Ihr Rathaus. Die IT-Abteilung dort sollte sich mit den Rückmeldungen auseinandersetzen.

Viele Webseiten arbeiten mit „Cookies“, das sind kleine Dateien, mit denen Sie identifiziert werden können, wenn Sie die Seite später wieder aufrufen. Städten und Gemeinden empfehlen wir, vorrangig auf Cookies zu verzichten oder, sollten Cookies wirklich benötigt werden, nur Session-Cookies zu verwenden, also solche, die beim Beenden des Webbrowsers automatisch gelöscht werden. Selbstverständlich ist es ein toller Service, wenn Sie sich online entscheiden können, ob Sie längerfristige Cookies akzeptieren wollen, um bestimmte Seiten Ihrer Stadt schnell ansurfen zu können (z.B. den Abfallkalender oder das Veranstaltungsverzeichnis). Aber es sollte Ihre ausdrückliche Entscheidung erfragt werden (Fachbegriff: Opt-in). Ein Nein muss akzeptiert werden,

Illustration: Isabel Wienold

und Ihre Entscheidung sollte widerrufbar sein.

Hard- und Software der Verwaltung

Weitere Kriterien für eine datenschutzfreundliche Kommune betreffen die Computer und Programme, die im Rathaus und den Ämtern verwendet werden. Grundsätzlich sollten keine Plattformen im außereuropäischen Ausland verwendet werden, wo europäische Datenschutzrichtlinien nicht gelten.

Zum Beispiel ist Google Docs kein guter Rat für die Zusammenarbeit an öffentlichen Papieren. Google Docs sollten auch nicht Schülerinnen und Schülern oder der Elternpflegschaft in Schulen empfohlen werden für Zusammenarbeit bei Referaten oder zur Planung des Sommerfestes. Im Gegenteil: Aufklärung über die Risiken solcher Plattformen (Urheberrechte, Überwachung/Spionage, usw.) gehört als Thema in den Schulunterricht. Hier könnte Ihre Stadt Zeichen setzen. Das gleiche gilt für Microsoft Office Online (früher bekannt als Office 365).

Kommunen sollten bevorzugt freie und quelloffene Software (FOSS) einsetzen. Dadurch können sie sich von der Abhängigkeit von einzelnen Herstellern wie Microsoft befreien und die Überprüfbarkeit (Auditing: was die Software macht und ob sie sicher ist) durch beliebige fachkundige Bürger.innen ermöglichen.

Wie kommunizieren die städtischen Mitarbeiter.innen eigentlich untereinander und mit Ihnen? Ist verschlüsselter E-Mail-Kontakt möglich bzw. sind verschlüsselte E-Mails innerhalb der Verwaltung Standard?

Sind verschlüsselte E-Mails innerhalb der Verwaltung Standard?

Gut geschultes Personal

Alle Mitarbeiter.innen Ihrer Kommune – nicht nur der oder die Datenschutzbeauftragte! – sollten regelmäßig zu Datenschutz und Verschlüsselung geschult werden. Alle sollten die Anweisung bekommen, die Bürger.innen auf die Datenschutzoptionen aufmerksam zu machen, z.B. beim Einwohnermeldeamt „keine Adressweitergabe an Adressverlage“ festzulegen. Ankreuzen kann man diese Option fast immer – meistens erfahren die Bürger.innen aber nichts davon.

Wie viele Mitarbeiter.innen in Ihrem kommunalen Rechenzentrum arbeiten zum Thema IT-Sicherheit? Machen Sie sich

schlau und regen Sie im Zweifel eine Aufstockung an, falls man Ihre Datenschutz-Anliegen mit „dafür haben wir keine Leute“ abwimmeln will.

Chipkarten bergen die Gefahr, dass Bewegungsprofile erstellt werden können.

Schon 2011 haben wir einen BigBrotherAward an einen Verlag vergeben, der Schulen mit Büchergutscheinen dazu gebracht hat, die Daten ihrer Schülerinnen und Schüler an diese Firma weiter zu geben. Geblendet von diesem Lockangebot haben viele Schulen übersehen, dass sie die Bücher mit diesem Datenschatz bezahlt haben – und das auch noch ohne Zustimmung der Eltern. Das war für unseren Preisträger, den Verlag für Wissen und Information in Starnberg, sehr lukrativ, denn er kooperierte mit Anlageberatern und einem Versandhandel für Vitaminpillen. Fazit: Insbesondere Lehrer.innen und Schulleitungen sollten regelmäßig informiert und sensibilisiert werden, damit sie die neuesten Tricks der Datenkraken erkennen.

Bargeld-Verwendung, insbesondere im Öffentlichen Nahverkehr

Die Möglichkeit, städtische Dienstleistungen mit Bargeld zu bezahlen, muss beibehalten werden. Und das darf auch nicht teurer als die Bezahlung per Karte gemacht werden.

Es muss auch möglich sein, anonym mit Regionalzügen, Bussen und Bahnen zu fahren. Papierfahrkarten müssen erhalten bleiben und sie dürfen nicht teurer als die elektronischen Karten gemacht werden. Kartenzahlung oder individualisierte Chipkarten bergen die Gefahr, dass Bewegungsprofile erstellt werden können. Einen besonders dreisten Fall haben wir 2016 mit einem BigBrotherAward ausgezeichnet: Die Berliner Verkehrsbetriebe (BVG) haben auf ihrer kontaktlos verwendbaren „VBB Fahrcard“ gespeichert, welcher Bus an welcher Haltestelle betreten oder verlassen wurde. Wir empfehlen Ihnen, die Laudatio von Rena Tangens zu diesem Preis aufmerksam zu lesen und ihren Verkehrsbetrieben dazu auf den Zahn zu fühlen. Den Link finden Sie auf der unten angegebenen Jahrbuch18-Seite.

Öffentlicher Raum

Wir wünschen uns Städte, in denen wir uns ohne Angst, überwacht zu werden, bewegen können. Überwachungssensorik wie Videokameras, Gesichts- und Stimmerkennung sollten abgebaut werden, auf Straßen und Plätzen, in Parks und Bussen. Das sind kommunale Entscheidungen. Nehmen Sie Einfluss auf die Kommunalpolitik. Schreiben Sie Leserbriefe,

Illustration: Isabel Wienold

wenn wieder einmal die Notwendigkeit von Videoüberwachung zur Verbrechensbekämpfung gepriesen wird: Kameras schrecken nicht ab, und die Bilder sind schon aus technischen Gründen selten verwertbar, um Verbrechen aufzuklären. Jeder erfolgreiche Fall wird aber in den Medien gefeiert – das verfälscht das Bild. Lesen Sie die Argumente im Blog auf unserer Webseite, Suchwort „Überwachung im Alltag“.

Setzen Sie sich für freie, nichtkommerzielle Netzwerke im öffentlichen Raum ein. Sogenannte „Freifunk“-Initiativen stellen inzwischen in vielen Städten kostenlose WLAN-Hotspots zur Verfügung. Auch hier können Sie auf unserer Webseite mehr nachlesen, wenn Sie dort nach „Freifunk“ suchen.

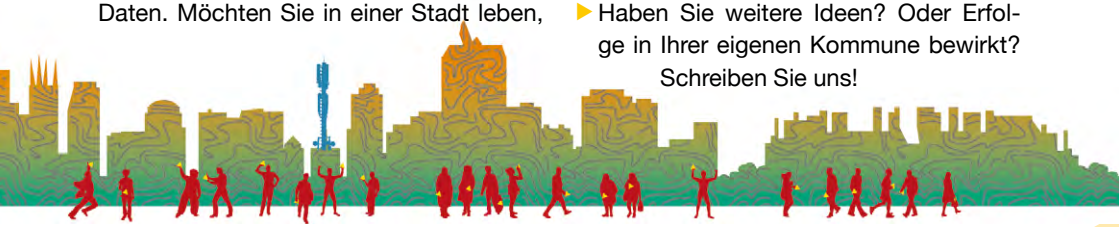
Ein recht neues Stichwort für die Gestaltung von sogenannten „Städten der Zukunft“ ist „Smart City“: (Einen Vortrag von Rena Tangens darüber finden Sie weiter vorne in diesem Jahrbuch.) Häufig ist damit verbunden, dass die öffentliche Infrastruktur an Firmen abgegeben wird, zum Beispiel als „Public Private Partnership“. Damit verscherbeln die Kommunen ihr Tafelsilber und geben die eigene Kontrolle über die Infrastruktur auf. Nicht selten bezahlen die Bürger.innen diese Firmen unfreiwillig ein zweites Mal – mit ihren Daten. Möchten Sie in einer Stadt leben, in der die digitale Infrastruktur Microsoft, Siemens oder Huawei gehört? Wenn es in Ihrer Stadt solche Überlegungen gibt, fragen Sie ruhig einmal nach: Woher kommen diese Ideen? Sind es Wünsche, die die Bürger.innen haben, oder sind Vertreter.innen Ihrer Stadt auf einer Werbeveranstaltung solcher Konzerne gewesen?

Zu guter Letzt: Nutzen die Städte ihre Einflussmöglichkeiten?

Bei Gesetzgebung auf Landes-, Bundes- und Europa-Ebene sollten sich Ihre Vertreter.innen dafür einsetzen, dass Privatsphäre und Datenschutz von Kommunen respektiert und aktiv umgesetzt wird. Sie sollten datenschutzfreundliche Innovation in und für Europa fördern: So gibt es zum Beispiel die Initiative für einen offenen europäischen Suchindex (Open Web Index), auf den dann auch kleine neue Suchmaschinen und andere datenintensive Startups zugreifen können. Das würde den Wettbewerb wieder herstellen und Googles de-facto-Monopol durch positive Maßnahmen abbauen.

Vielleicht geben Sie auch den Bundestags- oder Europaabgeordneten Ihres Wahlkreises mal einen freundlichen Stups, wie Sie als Teil der Wähler.innen-Basis sich Ihre lebenswerte Welt im digitalen Zeitalter wünschen.

- Haben Sie weitere Ideen? Oder Erfolge in Ihrer eigenen Kommune bewirkt? Schreiben Sie uns!



Digitale Selbstverteidigung

für Unternehmen und Organisationen

Von der AG Digitale Selbstverteidigung

Foto: Panthermedia

Alle haben Daten, die sie nicht in der Öffentlichkeit sehen wollen, Unternehmen und politische Organisationen ganz besonders. Beide stehen zudem gegenüber ihren Kund.innen, Mitgliedern oder Angestellten in besonderer Verantwortung. Datenverluste können nicht nur peinlich sein, sondern ganz reale Profit- oder Imageeinbußen bedeuten. Und dann heißt es: „Ach, hätten wir doch...“

Politische Organisationen haben insbesondere ein großes Interesse daran, dass ihre Pläne nicht vom „Feind“ mitgelesen werden können. Und wer will schon unfreiwillig eine Liste von potentiellen Querulant.innen veröffentlichen?

Grundsätzliches

- **Verzichten Sie auf Google-Dienste und benutzen Sie Alternativen**. Google verdient Geld mit den Daten, die Sie Google liefern und es gab wirklich viele Gründe für den BigBrotherAward, den wir 2013 verliehen haben. Bedenken Sie auch: Wenn Sie etwas über Google machen, setzen Sie Ihre Angestellten unter Druck, sich von Google ausspähen zu lassen. Besonders NGOs sollten sich bei ihrer politischen Arbeit nicht so genau auf die Finger schauen lassen. Statt GoogleDocs können Sie z.B. EtherPad und EtherCalc nutzen.
- **Verwalten Sie Ihre Kunden- oder Unterstützerinnen-Daten eigenständig.** Personenbezogene Daten haben in Clouds oder bei Dienstleistern nichts zu suchen!
- **Es gibt nichts umsonst. Sie bezahlen immer – mit Ihren Daten**. Bevor Sie ein kostenloses Tool auf Ihren Rechnern installieren, überlegen Sie sich gut, was der Anbieter sonst noch damit bezweckt. So wenig wie Sie es sich leisten können, Ihren Kunden kostenlos zu beliefern, so wenig kostenlos sind auch Dienste von Google, Skype oder Facebook. Sie bezahlen mit Ihren Daten. Erst wenn es weh tut und ihre Daten missbraucht werden (z.B. Industriespionage), wird Unternehmen klar, wo und wie sie besser auf Datenschutz Rücksicht genommen hätten. Leider.
- **Gefährlicher als Datenklau und Systemeinbrüche sind Gedankenlosigkeit, Ahnungslosigkeit und Bequemlichkeit**. Nicht alle Tools, die so praktisch und bequem scheinen, nützen auch Ihrer Organisation. Darum gilt die Devise: Prüfen Sie, ob Sie


Foto: Panthermedia

messbaren Nutzen daraus ziehen und sie nicht nur verwenden, weil alle anderen das auch tun.

- **Verschlüsseln – die Mühe lohnt**. Machen Sie sich die Mühe, Ihre Daten zu verschlüsseln. Der kleine Aufwand bringt ein großes Mehr an Sicherheit. Es gibt inzwischen einfache, sichere Lösungen für wenig Geld. Bitte achten Sie darauf, dass das Unternehmen die privaten Schlüssel aller Mitarbeiter braucht, um Geschäftskorrespondenz gesetzeskonform vorhalten zu können.
- **Sichere Passwörter**: Trainieren Sie Ihr Team darin, Passwörter sicher zu wählen und sie dann nicht mit einem Zettel an den Monitor zu kleben, sondern eine Passwortverwaltung zu nutzen.
- Trainieren Sie Ihr Team regelmäßig in Digitaler Mündigkeit. Rundmails und kurze Info-Runden frischen die Themen regelmäßig auf.
- Nutzen Sie Freie Software Oft spart das nicht nur Geld, sondern gibt Ihnen zudem Freiheit (von Herstellern) und Sicherheit (weil Sie den Quellcode prüfen lassen können).
- Für NGOs: Freie Software ermöglicht es allen, mitzumachen – nicht nur denen, die Geld für teure Software wie Photoshop ausgeben können.


Grafik: Panthermedia

Facebook und Social Media

Prüfen Sie, ob Sie auf Facebook ganz verzichten können. Falls Sie Facebook verwenden wollen, gibt es einiges, was Sie beachten sollten. Lesen Sie dazu auch das nächste Kapitel in diesem Jahrbuch.

- Viele Internetdienste haben sehr „böse“ AGBs, die Ihr Surfverhalten auf anderen Seiten verfolgen, allen voran Facebook. Dabei ist noch nicht einmal abzusehen, wie weit Facebook es damit wirklich treibt. Stellen Sie gesonderte Rechner für Facebook zur Verfügung, wenn sie nicht darauf verzichten können.
- Übrigens: Facebook ist gar nicht so nützlich, wie viele denken. Um wirklich Wirkung damit zu erzeugen, müssen Sie 1. primär Witze und Katzenbilder posten (Inhalte werden bei Facebook diskriminiert) und 2. sehr viel Zeit dort investieren. Wir bei Digitalcourage haben nach einer internen Untersuchung entschieden, dass es sich für uns nicht lohnen würde, selbst wenn wir es wollten.
- Wenn Sie wirklich nicht ohne Facebook auskommen, beachten Sie unsere Grundregeln zur Nutzung von Facebook
  - Alternative Kommunikationsplattformen anbieten
  - Aus Facebook stets nur heraus linken, nicht hinein
  - Mitarbeiter.innen vor AGB schützen
  - Ablehnung von Facebook kundtun
  - Social-Media-Buttons allenfalls als Zwei-Klick-Lösung


Foto: Panthermedia

Cloud

Eigene Infrastruktur aufbauen statt Cloud-Dienste nutzen: Ja, wir wissen, dass „Clouds“ sehr bequem scheinen. Die gute Nachricht ist: Sie können auch einfach Ihre eigene Cloud aufsetzen. Behalten sie Ihre Daten bei sich oder einem vertrauenswürdigen lokalen Provider. Für den Datenaustausch gibt es z.B. ownCloud, für gemeinsames Arbeiten EtherPad (Lite) oder Open-Xchange.

- **Auch bei der Cloud: Verzichten Sie auf Google-Dienste und benutzen Sie Alternativen**. (siehe oben)
- **Verwalten Sie Ihre Kunden- oder Unterstützerinnen-Daten eigenständig.**
- **Auch zu Dropbox gibt es Alternativen**.

E-Mail

- **Benutzen Sie einen sicheren E-Mail-Provider**. Nutzen Sie kleine, europäische Anbieter wie etwa posteo.de, oder mailbox.org oder gehen Sie zu einem lokalen Provider. Wenn Sie eine eigene Domain haben, verwenden Sie diese auch als E-Mail-Adresse. @t-online oder gar@googlemail sind Zeichen von Unprofessionalität.
- **Mails nicht im Browser verwalten**. Nutzen Sie für sich und die Rechner Ihrer Angestellten einen E-Mail-Client wie Thunderbird oder Outlook.
- **Verschlüsseln Sie Ihre E-Mails**. Mit „Enigmail“ geht es z.B. für den E-Mail-Client „Thunderbird“ ganz leicht. Von der PGP-Verschlüsselung im Browser, die web.de und GMX jetzt anbieten, halten wir nicht viel – das ist ja wieder im Browser. Es gibt inzwischen auch Anbieter, die z.B. für einen Euro im Monat Ende-zu-Ende-verschlüsselte Mailadressen anbieten (Posteo.de oder mailbox.org). Dort können Sie sogar anonym bezahlen.
- **Bieten Sie eine Möglichkeit an, Ihnen verschlüsselt zu mailen**. Stellen Sie ihren public key online zur Verfügung, drucken Sie dessen „Fingerprint“ mit auf ihre Visitenkarten, etc.
- Wenn Ihre Mitarbeiterinnen oder Mitarbeiter E-Mails nach außen weiterleiten, richten Sie besser Outlook-Web-Access o.ä. ein. Oder geben Sie ihnen ein Smartphone mit Verbindung zur Firma – am besten über einen sogenannten VPN-Tunnel.

Chat und Messenger

- **Chatten Sie nicht über Facebook oder WhatsApp oder Threema**, sondern benutzen Sie freie dezentrale Dienste, wie Jabber, Xabber, ChatSecure – auf Ihrem PC und auch auf Ihrem Mobilgerät. Dienste wie Threema und TextSecure wollen wir nicht empfehlen, können aber eine erste Alternative sein.

Browser

- **Hindern Sie andere Websites daran, Ihren Mitarbeiter.innen hinterherzuschnüffeln.** Installieren Sie auf allen Rechnern uBlock Origin, Privacy Badger oder einen anderen Werbeblocker in Ihrem Browser. Ohne Werbung gibt's mehr Konzentration und weniger Ablenkung. Da sich Viren häufig über Werbung in Webseiten verbreiten, schließen Sie zudem noch dieses Einfallstor. (Kosten: keine; Aufwand: 10 Minuten; Schulung: 10 Minuten)
- Achten Sie beim Surfen darauf, dass **hinter dem „http" in der Adresszeile immer ein „s"** steht.
- Deaktivieren Sie **Cookies.**
- **Probieren Sie andere Suchmaschinen**: z.B. Startpage.com, Metager.de, DuckDuckGo.com, ixquick.com. Oder wechseln Sie die voreingestellte Suchmaschine in regelmäßigen Abständen. Sie können auch Ihre eigene Suchmaschine betreiben, um Suchen geheim zu halten, z.B. mit YaCr. (Kosten: nix; Aufwand: 1 Minute)
- **Konfigurieren Sie die Arbeitsrechner so vor**, dass alternative Suchmaschinen und Werbeblocker bereits installiert sind. Das ist besonders wichtig unter Windows, da hier Browsererweiterungen als .exe installiert werden müssen. (Kosten: keine; Aufwand: 1–2 Stunden; Schulung: 30 Minuten)

Smartphone befreien

- Schalten Sie **Synchronisation** aus und löschen Sie **unbenutzte Konten**.
- Deinstallieren Sie **unnötige Apps**.
- Play-Store raus, **F-Droid** rein.
- **Kein WhatsApp und Facebook auf dem Smartphone**: Beide sammeln im Minutentakt Ihre Aufenthaltsorte und Ihre Kontakte. Die Konkurrenz würde sich freuen! Verwenden Sie stattdessen dezentrale Dienste wie Jabber (XMPP). (Kosten: keine; Aufwand: 5-20 Minuten; Schulung: 30 Minuten)

Ihre Website, ihr Service

Foto: Panthermedia

Verschenken Sie keine Daten. Grundsätzlich sollten Sie nur Daten erheben, die Sie auch wirklich brauchen. Nur ein fähiges Marketing- und Vertriebsteam kann die Menge an Daten, die beispielsweise Google Analytics liefert, auch auswerten und in Kampagnen umsetzen, die messbar Umsatzzuwächse bringen. Haben Sie keins, liefern Sie Google gratis wertvolles Datenmaterial, das Ihnen am Ende noch zum Verhängnis werden kann. Und die Zeit Ihrer Mitarbeitenden wird auch verschwendet. Auch Daten, die Sie wirklich brauchen, sollten Sie nicht ohne Notwendigkeit an andere Unternehmen weitergeben.


Foto: Panthermedia

- **Kein Facebook-Buttons** o.ä. auf Ihrer Website. Sonst verfolgen die Datenkraken alle Ihre Besucher. Nutzen Sie stattdessen „2-click"-Lösungen oder einen datenschutzkonformen „Sharrif".
- **Piwik statt Google Analytics**: Google Analytics brauchen Sie nur, wenn Sie auch Google-Adwords-Kampagnen fahren. Alles andere kann Piwik auch und das sammelt die Daten auf Ihrem eigenen Server. Aber auch Piwik sollte mit Bedacht konfiguriert sein. Am besten lassen Sie es gleich ganz sein, da Ihre Marketingabteilung ohnehin aus den gesammelten Daten nur bunte Folien macht. (Kosten: keine; Aufwand: ½ – 1 Stunde)
- **Alle Websites mit SSL verschlüsseln**: Es geht niemanden etwas an, was die Besucher Ihrer Website bei Ihnen ansehen – auch nicht Ihre oder deren Provider. Außerdem vereinfacht es das Setup. Einfachste und preiswerteste Lösung: Let's encrypt (Kosten: ab 0 €; Aufwand: ½ – 1 Stunde)
- **Keine externen Inhalte**: Holen Sie alles, was Ihre Website braucht, auf Ihren Server: Schriften, Scripte, CSS, etc. Sonst sammeln Google & Co. bei Ihren Besucherinnen fleißig weiter. Einfach die Dateien auf den eigenen Webserver kopieren.
- Mit Privacy Badger können Sie selbst ausprobieren, ob ihre Seite Tracker hat oder externe Inhalte enthält, die Ihnen gar nicht bewußt sind. (Kosten: keine; Aufwand: 1–2 Stunden)
- **Verwenden Sie Karten von OpenStreetMap** statt Google Maps. Diese Karten können Sie frei veröffentlichen, ohne gegen Urheberrechte zu verstoßen oder eine Abmahnung durch Google befürchten zu müssen. OpenStreetmap kann auch Routenplanung. Eigene Karten mit Punkten, Strecken, Flächen erstellen Sie unter http://umap.openstreetmap.fr/de/ -- auch diese Software können Sie auf Ihrem eigenen Server installieren.
- **Zwingen bzw. animieren Sie Menschen nicht, schnüffelnde Dienste zu nutzen**. z.B. indem Sie ihre App nur über Google Play Store zur Verfügung stellen (es gibt ja auch den F-Droid), oder Dienste nutzen, die man nur mit einem bestimmten Betriebssystem nutzen kann (selbstverständlich gibt es Ausnahmefälle, in denen es einfach nicht anders geht).

Softwareempfehlungen

- statt Internet Explorer, Edge oder Chrome: Firefox – auch mobil
- statt Windows oder Mac OS: GNU/Linux (z.B. Ubuntu, Mageia)
- statt SmallBusiness Server: Univention Corporate Server oder Zentyal
- statt MicrosoftOffice, Office 365 oder ähnlichem: LibreOffice
- Ein sehr gutes Contact Management System ist z.B. die freie Software „CiviCRM". Der Verein „Software für Engagierte" kümmert sich darum, dass diese gut gepflegt und auf Ihre Bedürfnisse angepasst wird.

Wichtige Punkte, die ein Datenschutzkonzept beachten sollte

- Gesetzliche Bestimmungen einhalten. Da steckt schon viel Wichtiges drin.
  - Opt-in: Das bedeutet, dass die Kund.innen explizit einen Haken setzen müssen, oder ihren Willen z.B. per Mail bekunden müssen, wenn sie den Datenschutzbestimmungen zustimmen oder einem zusätzlichen Service (z.B. Newsletter) erhalten möchten.
  - Nur Daten erheben, die man auch zum Erbringen der Dienstleistung (und zur Abrechnung) braucht. (Datensparsamkeit) Und diese Daten danach auch wieder löschen.
  - Verfahrensverzeichnis erstellen: Eine Art Bestandsaufnahme über „die laufenden Verarbeitungen von personenbezogenen Daten“ mehr dazu z.B. bei den Datenschutzbeauftragten.
  - Wir können hier keine Rechtsberatung leisten. Fragen Sie daher Ihre.n Datenschutzbeauftragte.n oder informieren Sie sich z.B. bei Ihrer IHK.
- Datenschutzfreundliche Voreinstellungen – die Verbraucherzentralen (vzbv.de) haben unter diesem Stichwort eine Liste veröffentlicht.
- Anonyme Bezahlmöglichkeiten mit Bargeld anbieten. Nicht nur Kreditkarte, Bankeinzug oder Paypal. Der alte Grundsatz „Erst die Ware, dann das Geld“ sollte auch heute noch gelten.
- Vertrauliche Kommunikation darf Geld kosten. Es muss ja nicht gleich ein eigener Server sein. Vertrauenswürdige E-Mail-Dienstanbieter sind nicht teuer.
- Achtung mit kostenlosen Diensten: z.B. Keine Kund.innendaten oder Angestellteninformationen in einer Google-Tabelle oder Ähnliches online speichern.
- Mitarbeiter.innen respektieren

Foto: Panthermedia

  - z.B. nicht verlangen, dass sie Lizenzbestimmungen akzeptieren (aka. sich einen Account anlegen) z.B. spioniert Facebook unseren Browser vollständig aus. Somit könnte es auch nach Feierabend den Angestellten hinterherschnüffeln. Auch wenn diese „nur“ den Firmenaccount nutzen.
  - keine Videoüberwachung von Angestellten
  - Schulungen zum sensiblen Umgang mit Daten und Passwörtern
  - Kund.innen respektieren
  - Keine Daten weitergeben, auch nicht versehentlich z.B. durch den Mailprovider oder Websitehoster
  - kurze, verständliche Datenschutzerklärung. Was genau darin stehen muss erfahren Sie z.B. bei den Datenschutzbeauftragten. Als Positivbeispiel für vorbildliche Datenschutzbestimmungen schauen Sie sich doch mal bei Posteo.de deren Datenschutzerklärung an ....

Facebook nutzen ja oder nein?

Eine Grundsatzentscheidung

Von David Bergmann

Wir haben es uns nicht leicht gemacht. Wir möchten mit unserer Arbeit möglichst viele Menschen erreichen – also gilt es, Menschen dort zu erreichen, wo sie sich tummeln. Und da ist Facebook ganz oben auf der Liste. Gleichzeitig haben wir Facebook 2011 aus sehr guten Gründen einen BigBrotherAward verliehen. Also standen wir vor einer Gewissensfrage: Können wir es uns **leisten**, auf Facebook zu verzichten? Aber wenn wir uns anschließen, müssen wir den zweifelhaften Allgemeinen Geschäftsbedingungen (AGB zustimmen). Das war für viele in unserem Verein eine Unmöglichkeit. Kommerzielle Überwachung ist eines unserer Kernthemen. In zahlreichen Interviews kritisieren wir das maßlose Sammeln von Daten durch Facebook. Nichtsdestotrotz sind die Chancen für die Vereinsarbeit mithilfe eines Facebook-Zugangs nicht von der Hand zu weisen. Wie also sollen wir damit umgehen?

▶Unsere Entscheidung lautet: Kein Facebook!

Nach langen Diskussionen haben wir den allgemeinen Konsens erreicht, dass wir uns deutlich gegen Facebook positionieren. Wir können aber gut nachvollziehen, wenn Sie privat, als Unternehmen oder Verein sich dafür entscheiden, Facebook trotz der damit verbundenen Risiken zu benutzen. Wir möchten Ihnen aber einige Tipps geben, wie Sie das möglichst „schonend“ tun können.

▶Grundregeln zur Nutzung von Facebook

Gegen die grundsätzlichen Probleme bezüglich Facebook, beispielsweise Monopolisierung, Kommerzialisierung und die Umgehung des deutschen und europäischen Datenschutzes, helfen die folgenden Regeln natürlich nicht. Aber es ist möglich, den gesellschaftlichen Schaden, der durch die Nutzung von Facebook entsteht, ein bisschen zu begrenzen.

▶Können wir es uns leisten, auf Facebook zu verzichten?◀

▶1. Alternative Kommunikationsplattformen anbieten:

Wer Facebook & Co. nutzt, sollte zusätzlich mindestens einen weiteren Kommunikationskanal anbieten. Dieser sollte frei sein und ebenfalls alle Inhalte verbreiten, die Sie auf Facebook zur Verfügung stellen. Die Auswahl der Anbieter ist groß ge-

Foto: Panthermedia

Facebook will alles! Laut AGB darf Facebook alles überwachen, was Sie ansurfen, auch wenn Sie gerade gar nicht angemeldet sind.

nug: Friendica, Quitter oder GNUnet, Sie haben die Wahl. Denn wer selbst keine Alternative anbietet, ist mitverantwortlich dafür, dass manche Menschen inzwischen Facebook für „das Internet“ halten. Durch das Befüttern alternativer Plattformen steigt auch deren Attraktivität. Wenn sich alle Organisationen, die Facebook & Co. nutzen, allein an diese Regel hielten, wäre schon viel gewonnen.

Mit Accountverwaltungsprogrammen wie Hootsuite sparen Sie Zeit bei der Pflege verschiedener Social-Media-Plattformen. Je höher die Nachfrage nach alternativen Plattformen wird, desto verlässlicher werden auch die Verwaltungsprogramme, welche diese einbinden. Dann wäre es attraktiver, auf andere Kommunikationskanäle umzusteigen, sodass langfristig die Marktmacht von Facebook aufgebrochen werden kann.

▶2. Aus Facebook raus linken, nicht hinein:

Es sollte stets auf Websites außerhalb von Facebook verwiesen werden. Die Internetnutzer.innen, welche Sie außerhalb von Facebook erreichen, sollten Sie wiederum nicht zu Facebook weiterleiten. Keine Links zu Facebook zu verwenden, ist im Interesse jeder Organisation: Denn Sie verbreiten damit Ihr eigenes Angebot, ohne parallel kostenlos Werbung für Facebook zu machen.

▶3. Ihr Team vor AGB schützen:

Das Facebook-Konto Ihres Unternehmens oder Ihrer Organisation sollte von einem gesonderten Rechner verwaltet werden. Denn es ist unklar, was es im Detail bedeutet, dass – so heißt es in den Allgemeinen Geschäftsbedingungen – das Onlineverhalten außerhalb Facebooks ebenfalls erforscht wird. Der Verbraucherzentrale Bundesverband (vzbv) mahnte Facebook bereits ab, da 19 Klauseln der Geschäftsbedingungen aus Sicht des vzbv rechtswidrig seien. Es ist demnach verantwor-

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).

Jetzt mit 16GB!
Preis: 25 Euro pro Stück

https://shop.digitalcourage.de

tungslos, Facebook von einem für diverse Zwecke genutzten Arbeitsrechner zu bedienen. Abhilfe kann ein sogenannter „virtueller Rechner“ schaffen.

4. Ablehnung von Facebook kundtun:

Eine kritische und reflektierte Haltung gegenüber Facebook sollte auf Ihrer Facebook-Seite sehr deutlich kommuniziert werden. Machen Sie ihren Umgang mit dieser Seite transparent und animieren Sie andere zur Einhaltung der hiesigen Regeln. Verweisen Sie stets auf die alternativen Plattformen, auf denen Sie ebenfalls kommunizieren.

5. Social-Media-Buttons allenfalls als Ein-Klick-Lösung:

Sollten Sie auf Ihrer Website Social-Media-Buttons einbinden, gibt es auch hierfür eine Möglichkeit, dies zu tun, ohne die Besucher.innen ihrer Site 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. Vorher können die sozialen Netzwerke keine Daten über sie erfassen.

Facebook lohnt sich nicht mehr

Auch wenn die Verlockung groß ist, auch wirtschaftlich betrachtet gibt es gute Gründe, gegen eine Facebook-Nutzung:

Grund 1: Reichweite ist begrenzt

Eine große Reichweite in den sozialen Medien macht viel Arbeit. Aufmerksamkeit kann nur durch eine hohe Interaktivität hergestellt werden. Sie müssen kommunizieren mit den Nutzer.innen, Inhalte bereitstellen, Umfragen oder Spiele durchführen und Vieles mehr. Dies kostet viel Arbeitszeit und bedeutet viel Aufwand für eine vergleichsweise kurze Aufmerksamkeitsspanne der Konsumierenden. Und vor allem: Menschen, die politisch denken und kritisch mit ihrer Mediennutzung umgehen, erreichen Sie dort unter Umständen gar nicht.

Grund 2: Inhalte haben es schwer

Die Inhalte, welche Nutzer.innen auf Fa-

cebook angezeigt werden, werden ähnlich wie bei Google anhand von Algorithmen und Rankings errechnet. Facebook filtert, was die Nutzer.innen sehen (sollen). Wenn eine Facebook-Seite beispielsweise 200 „Gefällt-mir“-Angaben hat, wird ein Posting der betreffenden Seite möglicher Weise zwischen 15 und 30 Leuten angezeigt. Die Reichweite ihrer Informationen ist somit häufiger geringer, als angenommen.

Grund 3: Katzenvideos sind interessanter

Es ist kein Geheimnis: Die Beiträge mit der höchsten Resonanz auf Facebook sind emotionale Inhalte wie Musik- und Katzenvideos. Da die meisten Inhalte von Organisationen aber eher informativer Natur sind, werden diese nur ein vergleichsweise kleines Zielpublikum erreichen. Denn laut Facebook-Algorithmus sind Sachinformationen weniger relevant und werden entsprechend eingestuft. Darum raten wir: Stellen Sie Ihre Inhalte auf Ihrer eigenen Seite zur Verfügung und investieren Sie dort Ihre Energie.

Im Zweifel hat Facebook mehr von Ihrer Organisation als Sie von Facebook.

Grund 4: Ohne Moos, nix los

Wer mehr Reichweite will, muss der Datenkrake Geld in den Schlund werfen. Bei einem bezahlten Account sind Ihre Möglichkeiten – Überraschung! – völlig andere. Facebook stellt Ihre Inhalte, in diesem Fall, allen Nutzer.innen vor. Der Slogan, „Facebook ist und bleibt kostenlos“, ist somit Augenwischerei.

Unterm Strich: Facebook ist vergebene Liebesmüh

Sie und Ihre Organisation verpassen nichts, wenn Sie nicht auf Facebook vertreten sind. Ganz im Gegenteil; in Relation überwiegt der Aufwand gegenüber dem Nutzen. Überlegen Sie es sich daher gut, ob Sie Facebook auch wirklich nutzen möchten. Im Zweifel hat Facebook mehr von Ihrer Organisation als Sie von Facebook.

Illustration: Isabel Wienold

Apps und Grundwissen für Kinder und Eltern

Von Jessi Wawrzyniak

Hallo,

ich bin Jessi, arbeite bei Digitalcourage und betreibe außerdem den Blog #kids #digital #genial (www.kidsdigitalgenial.de). In diesem Blog findest du viele Themen und Beiträge, die dir dabei helfen, sicher im Internet zu surfen und über das Thema Datenschutz nachzudenken. Die Texte sind ganz leicht formuliert, damit du sie gut verstehen kannst und die Tipps, z.B. Einstellungen an deinem Smartphone, sofort umsetzen kannst. So wie diese hier zum Beispiel:

„Askbongo“ Eine Kostenfalle bei Instagram

„Askbongo“ (übersetzt: „Frag Bongo“) oder auch „BONGO“ ist ein SMS-Dienst, der im Internet angeboten wird (www.askbongo.com). Du kannst einem kleinen Äffchen namens Bongo eine kostenpflichtige SMS schicken (1,99€), eine Frage stellen und Bongo beantwortet diese erschreckend genau, als würde er dich kennen.

Dieser Dienst hat auch eine eigene Seite bei Instagram und verbreitet sich dort bei Jugendlichen rasend schnell, denn der Slogan „Bongo weiß alles“ macht neugierig. Du wirst dazu aufgerufen, Bongo deinen vollständigen Namen, Wohnort und eine Themenkategorie mitzuteilen. Daraufhin erzählt dir das Äffchen etwas über dich, was es eigentlich gar nicht wissen kann.

Ein ausgedachtes Beispiel:

Lisa:
„*LIEBE Lisa Müller Berlin*“ (Kategorie „Liebe“, Vorname, Nachname, Wohnort – das alles hast du selbst Bongo vorher mitgeteilt)

Bongo:
„*Bongo weiß, dass Lisa ihre große Liebe bald finden wird. Wenn sie nicht zu der Party ihres Klassenkameraden Max am Samstag geht, könnte sie ihre Chance verpassen. Und ihr Traummann könnte stattdessen mit ihrer Freundin Laura zusammenkommen.*“

Wie kann Bongo von Max‘ Party am Samstag und von Lisas Freundin Laura wissen? Für viele ist das der Beweis, dass Bongo wirklich überirdische Kräfte hat. Aber das ist alles FALSCH!

Bongo weiß nicht mehr als jede Suchmaschine**!** Und bei Instagram weiß Bongo nicht mehr, als dein Instagram-Profil über dich verrät. Die Vorhersagen sind alle ausgedacht!

- **Gefährliche Kostenfalle!** Wer von Bongos Vorhersagen fasziniert ist und unbedingt noch mehr erfahren will, lässt

sich schnell über einen Link zu der offiziellen Webseite leiten, wo die Nummer für kostenpflichtige SMS sofort ins Auge sticht.

- **Bongo sammelt nur deine Daten!** Es geht darum, möglichst viele Informationen über dich zu sammeln und zu Geld zu machen. Außerdem schließt du automatisch ein SMS-Abo ab. Aus all diesen Gründen raten wir Dir sehr davon ab, auf Bongo hereinzufallen. Sprich auch mit deinen Freunden darüber, dass Bongo nur der Versuch ist, an Dein Geld und Deine Daten zu kommen.

Frühjahrsputz: Entferne Deine privaten Daten aus dem Netz

Weißt du eigentlich, welche Daten du im Internet von dir preisgegeben hast? Viele Einträge sind schnell geschrieben und geraten auch schnell wieder in Vergessenheit. Deshalb solltest du dir regelmäßig Zeit nehmen, alle deine Profile in Sozialen Netzwerken zu durchstöbern und aufzuräumen.

- **Recherchiere deinen Namen**
  Such in verschiedenen Suchmaschinen und vor allem bei Google nach deinem eigenen Namen, Wohnort, Nicknames, etc. So erfährst du, welche Fotos und Beiträge von dir öffentlich in Suchmaschinen zu finden sind. Wenn du beispielsweise Fotos entdeckst, die nicht öffentlich sein sollen, dann kannst du die verantwortlichen Stellen anschreiben und sie bitten, das Bild zu löschen, denn du hast das Recht am eigenen Bild.

- **Soziale Netzwerke und Messenger**
  Facebook, Instagram, musical.ly, Snapchat, MovieStarPlanet, live.ly,... Du hinterlässt überall Posts, Profileinträge, Fotos und Videos. Schau dir genau an, welche davon du wirklich weiterhin veröffentlichen willst. Du solltest vor allem alte Beiträge und Fotos immer löschen! Schau auch in die Datenschutz- oder Privatsphäre-Einstellungen, wer diese Inhalte sehen kann und stelle deine Profile, z.B. bei Instagram, auf „privat“.
- **Abonnements, Follower, Freunde**
  Möchtest du wirklich über alles und jeden informiert werden? Und auch jedem die Möglichkeit geben, in deinen Profilen zu stöbern oder sogar zu stalken? Geh‘ deine Freundeslisten durch und lösche Personen, zu denen du gar keinen Kontakt mehr hast. Überleg auch ganz genau, welchen Personen und Seiten du folgst und ob diese dich wirklich noch interessieren. Wenn du eine E-Mail-Adresse hast, dann kannst du auch im Posteingang nachschauen, ob du unerwünschte Newsletter bekommst und diese meistens am Ende des Newsletters über einen Link abbestellen.
- **Nachrichten und Beiträge**
  Du bekommst bestimmt jeden Tag viele Nachrichten von Freunden und Bekannten, die du gar nicht alle lesen kannst oder willst. Bitte deine Freunde, dir kei-

ne Kettenbriefe zu schicken und versuche an so wenigen Gruppengesprächen wie möglich teilzunehmen. Oft kannst du Gruppen auch stumm schalten.

- **Accounts**
  Weißt du überhaupt noch, wo du überall angemeldet bist? In welchen Sozialen Netzwerken? In welchen Foren? Bei welchen Spielen? In welchen Online-Shops? Bei welchen anderen Internet-Diensten? Accounts, die du nicht mehr nutzt, solltest du alle löschen.
- **Datenmüll auf dem Smartphone**
  Lösche Bilder, Videos und Chatverläufe, die du nicht mehr brauchst. Und vor allem Apps, die du nicht mehr nutzt. Du kannst auch zwischendurch mal in den Einstellungen kontrollieren, welche App-Berechtigungen von dir verlangt werden und entscheiden, ob du die App weiterhin behalten möchtest. Gerade „Ortungsdienste“ werden oft verlangt, obwohl sie gar nicht nötig sind. Warum muss eine Foto-App wissen, wo Du ein bestimmtes Foto gemacht hast? Das kannst Du abschalten.

App-Checks

Beispiel: WhatsApp
Im App-Check auf meinem Blog nehme ich die beliebtesten Apps genauer unter die Lupe und prüfe sie auf ihre Datenschutztauglichkeit und ob sie für Kinder und Jugendliche geeignet sind. Dort bekommst du Tipps für die richtigen Einstellungen und einen Überblick darüber, wie die Apps mit deinen Daten umgehen. Diese Informationen verstecken sich meist in den Allgemeinen Geschäftsbedingungen (AGB) und sind nur schwer zu verstehen. Nach einem Blick in den App-Check kannst du für dich selbst entscheiden, ob die Nutzungsbedingungen für dich in Ordnung sind oder nicht.

Diese Apps wurden 2017 für dich gecheckt:

- ✓ Instagram
- ✓ Live.ly
- ✓ Musical.ly
- ✓ Snapchat
- ✓ WhatsApp

Lexikon

Im Lexikon auf www.kidsdigitalgenial.de findest du viele Erklärungen zu Begriffen rund um die Nutzung von Medien, praktische Tipps zur Mediennutzung und verschiedene Anleitungen. Es ist bestimmt auch der ein oder andere Begriff dabei, den du schon oft gehört hast, aber gar nicht so genau beschreiben kannst. Könntest du erklären, was „Medien“ sind? Was bedeutet „digital“? Und was ist diese Vorratsdatenspeicherung von der alle sprechen? Schau es nach!

So, wenn du jetzt neugierig auf weitere Tipps geworden bist, kannst du auf www.kidsdigitalgenial.de weiter lesen und stöbern.

Liebe Grüße
Deine Jessi

Buchstabensalat

Findest Du die folgenden Worte? Kleiner Tipp: Du musst waagerecht, senkrecht, vorwärts und rückwärts suchen.

ADMINISTRATOR | ALGORITHMUS | APPLIKATION | BACKUP | BETRIEBSSYSTEM | BROWSER | BOT | CACHE | CLOUD | COOKIE | DATENBANK | FIREWALL | INTERNET | LINK | QUELLCODE | SERVER | SETUP | SOFTWARE | THREAD | VIDEOKAMERA | VIRUS | WLAN |

R	O	K	B	R	O	W	S	E	R	F	E	I	S	L
J	A	L	E	X	D	L	H	S	M	C	L	O	U	D
M	B	O	T	I	U	A	S	U	H	O	Z	C	M	B
S	N	I	R	S	J	N	G	R	F	O	N	Y	H	Q
O	B	G	I	H	A	M	L	I	N	K	T	A	T	U
F	I	R	E	W	A	L	L	V	B	I	D	P	I	E
T	A	F	B	O	P	U	T	E	S	E	J	P	R	L
W	E	Q	S	E	R	V	E	R	C	A	Y	L	O	L
A	H	N	S	A	T	E	N	R	E	T	N	I	G	C
R	C	L	Y	S	P	A	M	E	H	H	E	K	L	O
E	A	G	S	T	G	C	H	V	R	A	J	A	A	D
G	C	O	T	H	R	E	A	D	A	F	T	T	S	E
B	A	R	E	M	A	K	O	E	D	I	V	I	L	G
J	A	D	M	I	N	I	S	T	R	A	T	O	R	F
S	H	I	Y	F	D	A	T	E	N	B	A	N	K	A

Aus dem „Kids digital genial“-Lexikon

Betriebssystem
Ein „Betriebssystem“ sorgt dafür, dass dein Gerät überhaupt funktioniert, denn es arbeitet wie ein Übersetzer zwischen der Grafikkarte im Gerät (damit Bilder und Texte angezeigt werden können), der Sound-Karte im Gerät (damit Töne abgespielt werden können), der Festplatte (auf der Daten gespeichert werden) und jeder anderen Hardware, die in deinem Smartphone oder Tablet verbaut ist.

Browser
Einen „Browser“ (oder auch „Webbrowser“) benötigst du, um Internetseiten des World Wide Web (WWW) aufrufen zu können. Dort sind Funktionen enthalten wie z.B. „vor“, „zurück“, „Lesezeichen anlegen“, „Suche“ und viele weitere Funktionen, die du benötigst, um auf einer Webseite surfen zu können. Doch Browser speichern oft viele Daten über dein Surfverhalten. Du solltest in deinem Browser unbedingt einige Einstellungen zum Schutz deiner Daten und Privatsphäre vornehmen. Anleitung dazu findest du auf www.kidsdigitalgenial.de.

Firewall
Eine „Firewall“ (Deutsch: „Brandmauer“) ist eine Software, welche die Datenverbindungen zwischen Computern und Netzwerken überwacht. In dem Programm wird festgelegt, unter welchen Bedingungen und nach welchen Regeln Daten übertragen werden. Wenn die Daten nicht den Vorstellungen entsprechen, wird die Übertragung blockiert. So kann verhindert werden, dass Hacker oder Viren in das Computersystem eindringen.

Quellcode
Jede Software und auch jede Internetseite hat einen Quelltext/Quellcode, der sozusagen als Bauplan dient. Dort sind alle Befehle festgehalten, wie das Programm oder die Seite funktionieren und aussehen soll. Bei vielen Programmen ist der Quelltext geheim, damit nicht einfach jemand den Bauplan kopieren, klauen oder bearbeiten kann. Dadurch weiß man allerdings nie genau, was sich in dem Programm versteckt (z.B. ein Programm zum Ausspionieren). Einige Programme fallen jedoch in den Bereich „Open Source“ und stellen ihren Quelltext öffentlich zur Verfügung, damit andere diesen Bauplan auch verwenden und weiterentwickeln können.

Thread
„Thread“ ist das englische Wort für „Strang“ und wird im Internet genutzt, um eine Hierarchie, also eine Ordnung von über- und untergeordneten Elementen darzustellen. Meistens begegnet dir das Wort wahrscheinlich in Blogs und Foren, wo ein „Thread“ einen Knotenpunkt, also ein Thema abbildet, auf das dann geantwortet werden kann. Man kann einen Thread als Erzählstrang oder Gesprächsfaden bezeichnen.

Foto: Freiheit statt Angst 2008, cc by-sa 2.0

Unternehmen oder Staat - Wir treten ein gegen den Überwachungswahn

Digitalcourage vor 30 Jahren – Public Domains

padeluun erinnert sich:

„Im Februar 1987 haben wir unsere erste PUBLIC DOMAIN-Veranstaltung, kurz PD, in Bielefeld gemacht. Die Idee hatten wir beim Congress des Chaos Computer Clubs. Dort haben Menschen, die sich gut auskennen, anderen erklärt, was sie wissen. Dieses Format wollten Rena Tangens und ich regional anbieten. Corinna Luttmann und Rainer Schürmann hatten damals den „Bunker Ulmenwall“ übernommen, einen urigen Veranstaltungsort unter der Erde nahe der Bielefelder Altstadt. Dort fanden Konzerte und Lesungen statt und seit 1987 dann auch unsere PUBLIC DOMAINS. Der Name bedeutet „öffentlicher Bereich“ oder „öffentliche Angelegenheit“.

Das war eine handfeste „Raubkopier-Party“.

Eingeladen haben wir – außer bei der ersten Veranstaltung – immer mit weißen Postkarten. Die überzähligen Drucke nutzen wir heute noch im Digitalcourage-Büro als Notizzettel. Die Einladungen zu den ersten PUBLIC DOMAINS sind leider verloren gegangen. Die älteste Einladung, die wir noch als schwarz-weiß-Kopie haben, war für die dritte PD. Sorgfältig mit dem Atari und der Layoutsoftware Signum hergestellt, dreispaltig in rot und blau auf eine halbe DIN-A-4-Seite kopiert, lud „Häcker und Häcksen“ ein, zu kommen, Ideen mitzubringen und gemeinsam Spaß mit Computern zu haben.


this is your personal Invitation to the

BIT-NAPPING Party V1.0

Sunday 22nd of November 1987 (til monday)
Arrival: 9.00 to 11.00 a.m. and 2.00 to 3.00 p.m.
please be on time!

We provide:
– warm meals and drinks available at low charge
– photocopy
we want you to use it!
– videos
for your recreation
– telephone for reversed charge calls

You bring:
– sleeping bags etc.
(if you don' t prefer a hotel)
– your computer
all makes welcome
– manuals
– this postcard
no admission without this invitation
– cost sharing

666542

Art d'Ameublement, Marktstr. 18
D-4800 Bielefeld 1, ☎ ..49-521-61193

Aus 1987 ist außerdem noch die Einladung zur Bit-Napping-Veranstaltung V1.0 erhalten. Das war eigentlich gar keine Public Domain, das war eine handfeste „Raubkopier-Party“, die wir in Zusammenarbeit mit dem Jugendamt veranstaltet haben. Deshalb sind die Karten auch laufend durchnummeriert gewesen. Die Bit-Napping-Karten waren laminiert und unter der Laminierung war mit UV-fluoreszierender Farbe „Arte Absolutamente Moderne“ aufgestempelt, so dass wir die Echtheit am Eingang kontrollieren konnten.

Hamburg (DPA) ... ARIANE - so ein Sprecher der NASA - sei wohl nur deshalb so hervorragend gestartet, weil Hacker im Bootsektor der Rakete Verbesserungen vorgenommen hätten. ...

Chaos Computer Club, Schwenckestr.85, D-2000 Hamburg 20, Telefon: 040 - 490 37 57, BTX *CHAOS+
Mailboxsystem CLINCH 040 - 651 64 75, via Datex-P 44400090314, GEONET:GEO1:Chaos-TEAM

c 1988 by Art d'Ameublement

Ohne Einladung kam niemand rein, und durch die Nummer hat sich niemand getraut, die Karte bei der Polizei abzugeben. Wir hätten ja wissen können, wer das war. Tatsächlich haben wir uns aber gar nicht notiert, wer welche Kartennummer hat. Angezeigt hat uns dann trotzdem jemand und die Bit-Napping V1.0 hat uns unsere erste Hausdurchsuchung eingebracht.

Die PD 8,5 haben übrigens die FoeBuD-Mitglieder (so hieß Digitalcourage damals) ohne Rena und mich gemacht, denn wir waren damals drei Monate als „Artists in Residence“ in Kanada. Und die Zeit zwischen zwei „PDs“ dauerte unseren Mitgliedern zu lange, also haben sie gehandelt. Da die Nummer neun aber bereits fertig geplant war, wurde die eingeschobene PD 8,5 genannt. Die weitere Zählung stimmte dann ab PD 43 wieder, weil wir die 42 ausgelassen und für Douglas Adams, den Autor der Buchreihe „Per Anhalter durch die Galaxis“ reserviert haben. Der ist aber leider verstorben, bevor er nach Bielefeld kommen konnte.

1987 gab es vier reguläre PUBLIC DOMAINS und die Bit-Napping-Party. Mottos oder Themen hatten die PDs anfangs nicht. Die 8,5 hieß – daran erinnere ich mich – „in between“. Ab PD 06 sind alle Daten, Themen und gestalteten Einladungskarten erhalten.“

Hallo Häcker und Häcksen und alle anderen sorlösen User,

READ.ME

am Samstag, den 30.Mai 1987 gibt es im BUNKERULMENWALL ab 15 Uhr einen Häckertreff. Er heißt
PUBLIC DOMAIN ■■■
und soll dem Erfahrungsaustausch zwischen uns, den geplagten Usern, dienen. Drüber hinaus interessiert uns alles, was mit und oder gegen für etcetera Computern zu tun hat pp.

HEISSE ANGEBOTE:

FOTOKOPIERSERVICE
Hier können Informationen über Tips und Tricks (zum Beispiel über die Arbeit mit 'SIGNUM' etc.) weitergegeben werden.

HÄCKERRAUM
Dieser Raum gilt als 'elektrisches Labor'. Hier haben aus Sicherheitsgründen nur besonders unterwiesene Häcker Zutritt.

WORKSHOPS
Mailbox in Bielefeld. Wie groß ist der Arbeitsaufwand; was kostet eine Mailbox. Wenn's klappt und eine NUI zur Verfügung stehen sollte können wir OnLine mal in ein

-MEHR-

paar Boxen hineinschauen. Evtl. werden die Leute von der C.L.I.N.C.H.-Box aus Hamburg (CCC) wieder da sein.

DIGITALISIERUNGSSERVICE
Diesmal mit dem **Atari ST**. Ein jeder bringe seine eigene Diskette mit. Und eine Vorlage - oder sein Lieblingsvideoband. Wir können nämlich per Standbild Howard Beal (Network) vom Band holen. (Aber nur in schwarz/weiß!)

MATERIALSCHLACHT
McIntosh's sind da. IBM's sind da. C64's sind da. Ataris sind da. Amigas sind da. und hoffentlich viele Amigos!

PUBLICDOMAIN-
Softwaretausch ist natürlich voll OK! Raubkopien sind selbstverständlich verpönt.

FÜR'S LEIBLICHE WOHL
ist gesorgt. Der 'Erfrischungsstand in einem Jugendzentrum' steht mit allerlei kulinarischen Köstlichkeiten (wir empfehlen KAROKAFFEE a l'Art d'Ameublement - ehrlich!) zu echten Jubelpreisen zur Verfügung.

GEGNERN
der elektronischen Revolution sei hiermit versichert, daß dies nicht nur ein Fachidiotentreffen sein soll. Nein, wir freuen uns

-MEHR-

über jeden Besucher ('He, Nicht drängeln!'), der sich in irgendeiner konstruktiven Form mit diesem Thema auseinandersetzen möchte. Schließlich sind Computer und ihre Folgeerscheinungen nicht nur 'irgendsoeine neuere Mode' sondern tatsächlich ein riesiger Schritt auf dem Weg ins geordnete Chaos.

COMPUTER'FLOH'MARKT
Alles klar? Hier kann alles verscherbelt werden, das in irgendeiner Form mit elektronik zu tun hat. (Es gibt böse Zungen, die uns immer wieder weismachen wollen, daß Bielefeld seinen 'Verkehrsleitrechner' auf einem solchen Computerflohmarkt erstanden hat.)

NOCH FRAGEN?
ODER ANREGUNGEN?
☎ (05 21) 6 11 93 Art d'Ameublement
Marktstraße 18 * D-4800 Bielefeld 1
oder
☎ (05 21) 51 25 76 Bunker Ulmenwall
Kreuzstraße 0 * D-4800 Bielefeld 1

PUBLIC DOMAIN ■■■
Samstag 30.Mai 1987
Im Bunker Ulmenwall

-ENDE DER DATEI-

PUBLIC DOMAIN V 4.0

das Treffen der heimischen Computerscene

Freitag 6. 11. 1987
Bunker Ulmenwall
Kreuzstraße, Bielefeld
(0521) 51 2576
Zusammenarbeit mit FoeBuD e.V.

ART D'AMEUBLEMENT, RENA TANGENS & PADELUUN, MARKTSTR. 18, 4800 BIELEFELD 1

Das Treffen für Computerbe- und entgeisterte

PUBLIC DOMAIN ■■■

mit Chaos-Gästen vom Chaos Computer Club Hamburg

Ist Verständigung im Kommunikationszeitalter überhaupt noch möglich? PUBLIC DOMAIN (öffentlicher Bereich) soll ein Treffpunkt für alle sein, die entweder nichts, ein bißchen, viel oder sehr viel von Computern verstehen. Hier kann man seinen gebrauchten Computer verkaufen oder einen kaufen, Software (nur Originalprogramme natürlich) tauschen oder veräußern; oder gemeinsam Überlegungen anstellen, wie man Bielefeld computertechnische Entwicklungshilfe geben kann. Als Star- und Chaosgäste werden ein oder zwei Mitglieder des Chaos Computer Clubs aus Hamburg anwesend sein und als besondere Attraktion gibt es einen C 64 Digitalisierungsservice (Your Face on Disk) und einen C 64 E-PROM-Brenn-Service. Computer bitte mitbringen (dann aber unter 0521 / 611 93 bitte anmelden) und weitere Infos anfordern, ebenfalls unter obiger Nummer.

BUNKER ULMENWALL

Mittwoch
25.2.
ab 15 Uhr

Kreuzstrasse, 4800 Bielefeld 1
☎ (0521) 51 2576

Rechner mitbringen!

KNACK & BUG

PUBLIC DOMAIN V6.0

Das Computertreffen in Bielefeld
Sonntag 24. April 1988 ab 15 Uhr
im **BUNKER ULMENWALL** Kreuzstr. 0
Rechner und viel Zeit mitbringen.

Wer keinen Rechner mitbringt: Eintritt 3,–
In Zusammenarbeit mit FoeBuD e.V.

Infos: 0521 / 51 2576

GLATTEIS IN SINUSKURVEN

PUBLIC DOMAIN V7.0

Das Computertreffen in Bielefeld
Samstag 25. Juni 1988 ab 15 Uhr
im **BUNKER ULMENWALL** Kreuzstr. 0
Rechner und viel Zeit mitbringen.

Wer keinen Rechner mitbringt: Eintritt 5,–
In Zusammenarbeit mit FoeBuD e.V.

Infos: 0521 / 51 2576

Ägypten?!

IN BETWEEN

PUBLIC DOMAIN V8.0
Das Computertreffen in Bielefeld
Samstag, 24. Sept. 1988 ab 15 Uhr
diesmal bei ○□◁ **INTERCOM**
Bielefeld, August-Bebel-Str. 57 (ehem. Schäfferhaus)
Rechner und viel Zeit mitbringen.

Wer keinen Computer mitbringt: Eintritt 5,– DM
Eine Zusammenarbeit von FoeBuD e.V., Bunker Ulmenwall
und ○□◁ INTERCOM
Infos diesmal: 05 21 / 17 77 57

PUBLIC DOMAIN V8.5
Das Computertreffen
Samstag, 5. Nov. 1988 ab 14 Uhr
Gaststätte 'SEDAN'
Borgholzhausener Str. 98, Werther-Theenhausen
Rechner und viel Zeit mitbringen.

Wer keinen Computer mitbringt: Eintritt 5,– DM
Eine Zusammenarbeit des FoeBuD e.V.
Telecom: 05 21 / 6 11 93

W – EIN – 8 – S – VIRUS

bit bit – hurra!

Halbrok'sche Villa
Bielitzer Str. 43
4800 Bielefeld 18
Tel. 05 21 / 51 26 67

PUBLIC DOMAIN V9.0
Das Computertreffen in Bielefeld
Sonntag, 18. Dez. 1988 ab 15 Uhr
[redacted]
Rechner und viel Zeit mitbringen.

Wer keinen Computer mitbringt: Eintritt 5,–
In Zusammenarbeit von FoeBuD e.V.

Infos: 05 21 / 51 25 76

PUBLIC DOMAIN V10.0
Das Computertreffen in Bielefeld
Vortrag von padeluun: Weltweite Kommunikation mit Message Handle Systemen am Beispiel GeoNet
Sonntag, 29.1.1989 ab 15 Uhr
im BUNKER ULMENWALL
Kreuzstr. 0

Neue Eintrittspreise: Pro Person 8,– DM
Wer seinen Rechner mitbringt: Eintritt 3,– DM
FoeBuD-Mitglieder haben freien Eintritt.
Eine Zusammenarbeit von Bunker Ulmenwall und FoeBuD e.V.

„Gott sieht alles, aber er petzt nicht!“

Eine Datenschutzpredigt

Von padeluun und Pastor Florian Schwarz, 2009

Das Thema „Datenschutz“ im Gottesdienst*? Auf diese Idee kam Pastor Florian Schwarz im Jahr 2009 und erarbeitete eine Liturgie, die sich dem Datenschutz widmete. Er suchte Bibelstellen heraus, die zum Thema passten und lud padeluun ein, bei seinem „Kulturgottesdienst“ in der Cuxhavener Martinskirche eine Predigt zum Thema Datenschutz zu halten. Wir fanden dieses Experiment, unser Thema auch in den Kulturraum Kirche zu tragen, so spannend, das wir zusagten.*

Und tatsächlich beschäftigten sich alle Textstellen (von den lithurgischen Formalien mal abgesehen) mit den Themen, „zählen“, „Wissen“ und der „Hybris“ (griechisch ὕβρις hýbris ‚Übermut, Anmaßung‘). Denn – so die Interpretation – nur Gott darf alles wissen. Wenn die Menschen sich aufschwingen, alles wissen zu wollen, dann wird (Gottes) Strafe folgen.

Man mag nun zu Religion und Kirche, grundgesetzlich garantiert, eingestellt sein, wie man will. Wir fanden diese Arbeit so spannend, dass wir diesen Text auch hier im Jahrbuch noch 2018 einmal dokumentieren wollen. Vielleicht motiviert es ja auch andere Kirchengemeinden, sich dem Thema zu nähern? Über Zusendungen von Glaubensgemeinschaften seien es katholische oder pastafarische Messen, muslimische Gebete, buddhistische Gespräche, jüdische Gottesdienste etc., würden wir uns freuen.

Begrüßung durch Herrn Pastor Florian Schwarz

701 987 453 22

Mit dieser Zahl begrüße ich Sie ganz herzlich zum Kulturgottesdienst am Samstagabend. 701 987 453 22 – Diese Zahl war der Grund, warum wir diesen Kulturgottesdienst zum Thema Datenschutz und Menschenwürde veranstalten. In der Januarausgabe der Kulturgottesdienste wollten wir einen Gastprediger zu Wort kommen lassen, der kompetent über ein Thema des vergangenen Jahres predigen kann. Dass wir das Thema Datenschutz gewählt haben, liegt an einen Brief, der vor einigen Wochen in meinem Briefkasten lag und in dem die Zahl 701 987 453 22 stand. 701 987 453 22, das ist meine Tochter Julia. Zweieinhalb Jahre alt und von ihren Eltern heiß geliebt. In dem Brief wurde uns mitgeteilt, dass Julia Maria Schwarz, geboren am 12. Mai 2006 die Steuernummer 701 987 453 22 zugeteilt wurde. *(Anmerkung der Jahrbuch-Redaktion: Die Steuernummer, Namen und Daten haben wir natürlich verändert)*

Ein Kind Gottes, reduziert auf eine Zahl

Der Versuch, jedem Menschen in diesem Land eine Personenkennziffer zu verpassen, scheiterte vor einigen Jahren am Bundesverfassungsgericht, weil dies nicht mit der Würde des Menschen zu vereinen wäre. Dann eben eine Steuernummer für jeden Menschen, egal ob er Steuern zahlt oder nicht – das erfüllt den gleichen Zweck. Für den Staat ist meine Tochter jetzt nur noch eine Nummer. Was für ein Menschenbild. In der Bibel heißt es über den Menschen: „Und Gott schuf den Menschen zu seinem Bilde, zum Bilde Gottes schuf er ihn." Das Ebenbild Gottes reduziert auf eine Zahl. Für mich als Christen ein unmöglicher Zustand. Ein Zustand, bei dem wir als Kirche nicht umhin kommen, Stellung zu beziehen. Ich war selber überrascht, in welch großem Ausmaß die Bibel auf diesen Punkt eingeht. Es ist nicht nötig, Parallelen zu ziehen oder biblische Texte in Analogien heranzuziehen. Nein, die biblischen Texte sprechen Datensammelei und Volkszählung und die Reduzierung von Menschen auf Zahlen deutlich an. Wir sind als Christen nicht alleine auf dieser Welt. Abscheu vor der Reduzierung des Menschen auf Zahlen haben auch andere Menschen. Ich freue mich, dass wir padeluun gewinnen konnten, in diesem Gottesdienst über seine Motivation gegen die Datensammelei zu kämpfen zu sprechen. Padeluun war im vergangenem Jahr die treibende Kraft hinter der Verfassungsbeschwerde gegen Vorratsdatenspeicherung und Organisator der Demonstration „Freiheit statt Angst". Mit seinem Verein FoeBuD deckte er in den vergangenen Jahren immer wieder heimliche Datenspeicherung von Konzernen und staatlichen Stellen auf und machte sie mit der Verleihung des BigBrother-Awards öffentlich. Den Titel für diesen Gottesdienst „Der liebe Gott sieht alles – aber er petzt nicht" ist auch das diesjährige Motto seines Vereins.

Für den Staat ist meine Tochter jetzt nur noch eine Nummer. Was für ein Menschenbild.

Ich wünsche ihnen einen spannenden Gottesdienst, den wir feiern im Namen des Vaters, der uns Menschen zu seinem Ebenbild geschaffen hat, im Namen des Sohnes, der auch die Ausgestoßenen und Abgestempelten als Kind Gottes angenommen hat, und im Namen des Heiligen Geistes, der uns die Kraft gibt, unsere Mitmenschen nicht als Zahl, sondern als einzigartige Wesen wahrzunehmen. Amen

Lesung aus dem 1. Buch der Chronik im 21. Kapitel

Es ist kein Phänomen der Neuzeit, Menschen zu Zahlen zu machen. Die Volkszählung in der Weihnachtsgeschichte ist ihnen sicherlich bekannt. Aber bereits 1000 Jah-

re früher gab es bereits eine Volkszählung unter König David. Meines Wissens der älteste Bericht über ein solches Vorhaben überhaupt. Der biblische Text lässt keinen Zweifel daran, was eine Volkszählung in Gottes Augen darstellt und David erkennt es im Verlauf der Geschichte selbst: Eine schwere Sünde und eine Torheit. Ich lese aus dem 1. Buch der Chronik im 21. Kapitel. (Wir kürzen den Bibeltext an den mit eckigen Klammern gekennzeichneten Stellen [...] ein. Bitte nehmen Sie eine Bibel zur Hand oder lesen Sie die „Datenschutzpredigt“ auf unserer Webseite in voller Länge, wenn Sie mehr darüber wissen möchten.)

▶Eine schwere Sünde und eine Torheit.◀

Und der Satan stellte sich gegen Israel und reizte David, dass er Israel zählen ließe. 2 Und David sprach zu Joab und zu den Obersten des Volks: Geht hin, zählt Israel von Beerscheba bis Dan und bringt mir Kunde, damit ich weiß, wie viel ihrer sind. 3 Joab sprach: Der HERR tue zu seinem Volk, wie es jetzt ist, hundertmal soviel hinzu! Aber, mein Herr und König, sind sie nicht alle meinem Herrn untertan? Warum fragt denn mein Herr danach? Warum soll eine Schuld auf Israel kommen? [...] 17 Und David sprach zu Gott: Bin ich‘s nicht, der das Volk zählen ließ? Ich bin‘s doch, der gesündigt und das Übel getan hat; diese Schafe aber, was haben sie getan? HERR, mein Gott, laß deine Hand gegen mich und meines Vaters Haus sein und nicht gegen dein Volk, es zu plagen. Und der HERR wurde dem Land wieder gnädig, und die Plage wich von dem Volk Israel.

▶Lesung aus dem Buch Hiob im 28. Kapitel

In der Geschichte von der Vertreibung aus dem Paradies verführt die Schlange die Menschen mit den Worten: An dem Tage, da ihr vom Baum der Erkenntnis esset, werden eure Augen aufgetan, und ihr werdet sein wie Gott und wissen, was gut und böse ist. Die Geschichte sagt nicht, ob die Schlange gelogen hat oder ob Adam und Eva einfach nur nicht genug von der Frucht gegessen haben. Die Geschichte vom Sündenfall will in der Sprache des Mythos davon erzählen, dass der Mensch über sich selbst hinauswachsen will, mehr wissen will als er kann und nicht akzeptieren kann, dass Gott allein alles weiß und der Mensch sich mit einem beschränktem Wissen abfinden muss.

In der Geschichte von Hiob, das vom Leiden eines Gerechten erzählt und die Frage nach der Gerechtigkeit Gottes stellt, gibt es eine Szene, in der Hiob Gott anklagt. Ganz formal nach den juristischen Gepflogenheiten seiner Zeit klagt er Gott vor Zeugen an, ungerecht zu sein. Gott reagiert auf diese Anklage. Es ist eine harte Antwort angesichts Hiobs Leiden. Gott weist ihn auf seinen Platz. Bei allem menschlichem Streben ist das, was der Mensch wissen kann begrenzt. Ich lese aus dem Buch Hiob im 28. Kapitel. [...]

Predigt von padeluun

Fühlen Sie sich wohl? Ich meine jetzt nicht die täglichen kleinen Misslichkeiten: ein Zwicken hier, ein wenig Liebeskummer da. Wenn ich Sie frage, ob Sie sich wohlfühlen, meine ich was ganz Anderes.

Ich persönlich kenne eine ganze Menge Menschen, die haben da so ein komisches Gefühl in der Magengrube. Ein Gefühl, das sie gar nicht so richtig artikulieren können. „Ach egal“, sagen wir uns oft, „Was soll mir schon passieren? Ich habe doch gar keine wichtigen Geheimnisse, nichts zu verbergen.“ Und doch ist da dieses seltsame Gefühl. Zum Beispiel am Telefon. Soll ich meiner Enkelin am Telefon sagen: „Ich hab dich lieb.“? Das ist ja eigentlich gar nicht geheim, das ist nicht besonders wichtig für andere. Aber es geht auch niemand anderen etwas an. Sie brüllen ja auch nicht im Bus lauthals ins Handy: „Hallo Enkelin, ich hab dich lieb!“ Denn das ist etwas was nur Sie beide angeht, Sie und Ihre Enkelin. Sie möchten doch sicherlich nicht, dass heimliche Lauscher das mitbekommen.

Foto: Daniel Kuri cc-by

Im Namen der Sicherheit

Ich möchte keine heimlichen Lauscher in meinem Telefon. Und doch werden seit Anfang Januar letzten Jahres alle Verbindungsdaten von Telefon- und Internetverbindungen aufgezeichnet. Also, wenn Sie telefonieren, nimmt es ein Rechner auf – nicht das Gespräch, sondern dass Sie telefonieren, mit wem Sie telefonieren, wie lange und von wo aus Sie telefonieren. Ein Rechner speichert das für mindestens ein halbes Jahr. Das heißt „Vorratsdatenspeicherung“.

Aber ich will nicht überwacht werden. Ich bin nämlich ein ganz unbescholtener Mensch und ich habe nichts Illegales im Sinn. Und deswegen will ich auch nicht überwacht werden.

Kürzlich war ein freundlicher Herr am Telefon, der hat mich Nachmittags, kurz nachdem ich aus dem Büro kam, angerufen. Er kannte sich ziemlich gut aus mit meiner Familie und meinte es nur gut. Er sagte, dass wir da so Probleme hätten, mit unserem Versicherungsvertrag. Wir sind unterversichert. Und da ist eine Versicherungslücke über Hausrat und Haftpflicht. Mit einem ein wenig teureren Vertrag könnten wir das dann ausgleichen. Aber war-

Bild: Panthermedia

Wer weiß wie viel über uns?

um wusste er so viel über mich und meine Familie? Firmen und auch die Politik wandeln auf ganz gefährlichen Wegen.

Um Wartungsverträge zu verkaufen, die monatlich Geld einbringen, ohne, dass sie dafür etwas leisten müssen, und um Gebühren für Datenleitungen zu kassieren, jubeln sie unsägliche Technik hoch und verkaufen zum Beispiel Videoüberwachung und Einbruchmeldeanlagen an Kommunen und an Privatbesitzer von Häusern. Obwohl die Kriminalistik und jeder Kriminalbeamte uns sagen wird: „Eine Einbruchmeldeanlage nutzt gar nichts“. Was man sicherstellen muss, ist, dass ein Täter gar nicht erst ins Haus kommt. In den Medien werden trotz sinkender Kriminalitätszahlen einzelne schlimme Fälle so aufgebauscht, dass wir gerade zu freiwillig bereit zu sein scheinen, die Errungenschaften von Demokratie und die Errungenschaften eines Rechtsstaates komplett über Bord zu werfen. Wir neigen dazu dem – ich nenne das immer „populistischen Geschwätz“ – von mehr Sicherheit zu glauben. Also wir neigen dazu dem populistischen Geschwätz, (wenn uns jemand sagt wir brauchen mehr Sicherheit) von mehr Sicherheit zu glauben. Statt den Wissenschaftlern, die sich wirklich mit dem Thema auskennen, zuzuhören. Klingt kompliziert, ist scheinbar nicht so einfach.

▶„Eine Einbruchmeldeanlage nutzt gar nichts“.◀

Aber wir könnten uns auch selbst fragen, einmal in uns hinein hören: Leben wir nicht in einem der sichersten Länder der Erde? – Ja. Muss ich dann ganz persönlich Angst vor einem terroristischen Anschlag haben? (padeluun adressiert gezielt Personen in der Zuhörerschaft) Sie? Sie? Nein? – Nein. Was soll also diese ganze Überwachungsfrage, mit der wir uns immer mehr auseinandersetzen müssen? Diese Überwachungspakete, die geschnürt werden, statt Sozialpakete für Arbeitslose? Warum lassen wir so etwas wie Vorratsdatenspeicherung zu? Warum schreien wir nicht auf, wenn das Trennungsgebot von Geheimdienst und Polizei aufgelöst wird? Wenn so etwas auf uns zu kommt, wie das BKA-Gesetz, in dem eine

unglaubliche Macht einer zentralen Stellen übergeben wird? Warum lassen wir das zu? Warum stehen wir nicht auf und protestieren laut gegen diese Hybris der Poltitik, die anscheinend allwissend werden möchte? Warum lassen wir es zu, wenn unsere Rechte ausgehebelt werden, damit der ehemalige Innenminister Otto Schily bei gleich zwei RFID-herstellenden Firmen im Aufsichtsrat sitzen kann? Dass wir in unseren Reisepässen und demnächst in unseren Personalausweisen einen RFID-Chip haben müssen? Das hat keinen Sinn, außer, dass die Bundesdruckerei Geld verdient. Es gibt keinen sicherheitsrelevanten Grund für diesen Chip, im Gegenteil; diese Chips machen die Ausweise unsicher, weil sie ortbar sind.

Wissen Sie, wann ich zum ersten Mal zu dem Thema Datenschutz gekommen bin? Wann ich das erste Mal richtig das Gefühl hatte, dass wir uns mit diesem Thema in einer digitalen vernetzten Welt beschäftigen müssen; und zwar intensiv beschäftigen müssen? Das war so etwa 1989 oder 1990 – ich weiß es nicht mehr so genau – Ich arbeitete damals mit einem Vorläufer dessen, was man heute Internet nennt. Es hieß „Mailbox“. Das war ein ganz normaler Computer, und diesen konnten Menschen mit ihren Computern anrufen und Nachrichten für andere Menschen hinterlassen. Eine „E-Mail“ – nennt man das heute. Diese Mailbox zeigte übrigens alles, was jemand schrieb, direkt auf dem Monitor an. Der Computer stand in meinem Hausflur

Warum lassen wir Überwachung zu? Wehren Sie sich!

Bild: Digitalcourage, cc by-sa 4.0

– ich musste immer nachsehen, ob er noch lief, denn er stürzte damals immer ab – und wenn ich dann darauf guckte, sah ich eben, was passierte. Bei so einem Kontrollblick sah ich eines Tages, dass sich gerade Peter – ein sehr guter Freund von mir, Programmierer von Beruf – eingeloggt hatte und begann eine Nachricht zu schreiben; an Monika. Da durchfuhr es mich: „Na, zwischen den beiden läuft doch ‚was."

▶Mir war sofort klar, dass mich das überhaupt nichts angeht.◀

Und wenige Sekunden später meldete sich mein Gewissen und sagte: „Das geht dich aber gar nichts an. Wenn sich zwischen den beiden etwas anbahnt, hast du das entweder von ihr oder von ihm zu erfahren. Aber nicht dadurch, dass du auf dem Rechner siehst, dass er ihr eine Mail schreibt." Mir war sofort klar, dass mich das überhaupt nichts angeht. Und überall im Land gab es solche Systeme, wo Leute zuschauen konnten, was andere schrieben.

Doch die meisten Leute, die es genutzt haben, wussten nicht, dass dort jemand zuschauen kann. In einer digitalen vernetzten Welt sind Sachen anders geworden. Heute gibt es nicht mehr ausschließlich den Briefumschlag, in den man ein Blatt Papier hinein legt, ihn zuklebt und der dann – von Gesetzen geschützt – transportiert wird. Mir wurde schlagartig klar, dass wir Menschen vor der Technik sowie den Technikern, den Systemhausmeistern und unseren Vorgesetzten schützen müssen.

Im Fall von Peter und Monika war es nun sehr einfach. Mein Freund Peter ist, wie ich schon sagte, Programmierer. Und so zwang ich ihn quasi, Datenschutz in die Software einzubauen. Ich erzählte ihm von dem Vorfall, dass ich das Gespräch von ihm und Monika mitbekommen hatte, und schnell war er sehr, sehr, sehr engagiert, dafür zu sorgen, dass ich nicht mehr mitlesen kann. Im Feld, in dem man tippte, wurden fortan nur noch Sternchen ausgegeben. Das war ganz einfach: vier Zeilen Programmcode.

Ich kann Ihnen dazu kurz sagen, wir haben später eine Firma gegründet und diese datenschutzfreundliche Software angeboten, mit noch weiteren Möglichkeiten. Dort war dann eine richtige Verschlüsselung eingebaut. Doch das war kein gutes Verkaufskonzept. Die meisten Leute haben lieber die Software gekauft, wo die Datenübermittlung nicht so sicher war.

Unsere Software hat sich nicht durchgesetzt. Heute haben wir das Internet. In dem können sehr viele Leute, an sehr vielen Stellen einfach mitlesen. Im Grunde genommen ist in all unseren Datenleitungen eine Art Stasi eingebaut. Politik und Industrie machen sich die Unwissenheit der Öffentlichkeit zu Nutze. Und bauen momentan an einem Datensammelprojekt nach dem anderen. Wenn ich einmal aufzähle: Das Mautsystem, diese komischen Teile über den Autobahnen, die jedes Autokennzeichen erst einmal aufnehmen können. Die Gesundheitskarte: Die

Bild: Ralph Steffen für Stadtmagazin Ultimo

...als der Mailbox-Rechner noch im Flur stand...

Daten der Gesundheitskarten werden erst einmal zentral erfasst. Und klar, wird gesagt, kommen an diese Daten nur die berechtigten Leute heran. Doch überall dort, wo Daten zentral erfasst sind, gibt es auch Übergriffe. Denken Sie an den Fall der Telekom. Viele Daten waren zentral in den Händen der Telekom, und die obersten Leute der Telekom haben darin herum gewühlt und darin herumgeschnüffelt, um ihre eigenen Interessen, z.B. gegen Gewerkschaften, durchzusetzen.

▶…wo Daten zentral erfasst sind, gibt es auch Übergriffe.◀

Und ich glaube, das ist der Punkt, an dem wir Bürgerinnen und Bürger aufstehen müssen, uns versammeln müssen, um laut unsere Grundrechte einzufordern. Sonst ändert sich nichts in diesem Jahr 2009, in dem Europawahl, Bundestags- und Kommunalwahlen sind. Allwissend soll die Politik niemals über Menschen sein, unser Grundgesetz ist dafür errichtet worden – damals unter dem Eindruck dieses schrecklichen Krieges, mit dem Menschenvernichtung einher ging – dass Bürgerinnen und Bürger den Staat immer abwehren können. Das gesamte Strafgesetzbuch ist dafür da, um zu regeln, was der Staat darf, wie viel Zugriff er auf die Menschen haben darf - und wie viel auch nicht.

Manchmal ist es so, dass wir uns bei einigen Sachen wünschen, härter durchgreifen zu können. So etwas kommt immer gut an beim Volk. Tatsächlich ist das in einer rechtsstaatlichen Gesellschaft bewusst nicht gewünscht, denn härter durchzugreifen bedeutet auch, Fehler zu machen. Fehlerhaft über Menschen zu urteilen, die, öfter als man denkt, unschuldig sind. Allwissend, das erlaube ich mir hier in der Martinskirche zu sagen, ist eben nur Gott. Und Gott petzt nicht, darauf können wir setzen.

▶Pastor Schwarz:

Und der Friede Gottes, welcher höher ist als alle unsere Vernunft, er bewahre unsere Herzen und Sinne in Jesus Christus unserem Herrn. Amen.

Alice im Cyberspace

Ein feministischer Blick auf das Netz

Rena Tangens erinnert sich:

„Dieser Text ist uralt – er stammt aus der Frühzeit der Vernetzung! Grundlage war ein wissenschaftlicher Beitrag von mir zum Thema Androzentrismus aus dem Jahr 1995. Da Menschen aus Geschichten besser lernen als aus wissenschaftlichen Texten, habe ich den Inhalt 1999 zur Geschichte von „Alice im Cyberspace“ umgeschrieben. Die ist 2000 bei Telepolis veröffentlicht worden. Gewiss – seitdem hat sich einiges verändert, doch anderes ist erstaunlich aktuell. Achja: Die meisten Stories von Alice habe ich in der Tat selbst erlebt. Viel Spaß bei der Zeitreise!“ (Die Links zu den Original-Quellen für diesen Text finden Sie auf der Jahrbuch-Webseite, siehe unten)

Alice ist online. Und das nicht erst seit gestern. Datenreisen waren schon ihre Leidenschaft, als Laptop, Modem, Telefonkabel und Schraubenzieher nicht als normales Gepäck einer Frau angesehen wurden und das Hilton-Hotel München ihre Bitte um eine Dreiersteckdose noch mit der Frage „Wozu brauchen Sie die denn – wollen Sie etwa auf dem Zimmer kochen?!“ quittierte.

Das Wunderland wollte nicht nur erforscht, sondern auch kultiviert werden. Unendliche Weiten, Visionen von globaler Gemeinschaft, allgemein verfügbarem Wissen und gleichberechtigter Kommunikation, Utopien wie Marianne Brüns „Socially beneficial information processor“ anstelle einer Weltregierung – Welten unendlicher Möglichkeiten taten sich auf.

Journalisten fragen Alice immer wieder, ob sie sich nicht als Exotin vorkäme, ob es sie nicht nerve, dauernd von Männern angemacht zu werden und überhaupt die viele Pornographie im Netz. Alice ist genervt: als ob es keine wichtigeren Fragen gäbe. Wo wir doch gerade dabei sind, die Welt zu retten.

Aber Alice wundert sich auch. Warum trifft sie so wenige Frauen in dieser neuen Welt? Wollen die wirklich mit Technik nichts zu tun haben, interessiert es sie nicht oder was hält sie davon ab? Da könnte glatt der Eindruck entstehen, mit Frauen gäbe es per definitionem immer Probleme. Sie beginnt, der Frage nachzugehen.

Und Alice wird fündig. Ein Lob auf die Wissenschaft – genauer gesagt, die Wissenschaftskritik. „Androzentris-

mus“ heißt das Schlüsselwort. Wissenschaftssprech ist meist grauslich, aber bringt es in diesem Fall auf den Punkt. „Zentrismus“ bedeutet, den eigenen Bauchnabel als Zentrum der Welt anzusehen; das Wort, das davorsteht, gibt an, in welcher Eigenschaft das passiert – z.B. als Europäer (Euro-), als Mensch (Anthropo-) oder eben als Mann: Andro-Zentrismus.

Auch die dümmsten Chauvis wissen, was sie tun, wenn sie Sprüche loslassen wie „Frauen können nicht logisch denken.“ oder „Frauen gehören nach Hause an den Herd.“ Das ist Sexismus. Klar gibt’s den im Netz, aber davon lassen wir uns im wirklichen Leben doch auch nicht beeindrucken. Androzentrismus dagegen kommt ganz unauffällig daher und setzt stillschweigend Mensch = Mann; Frau sein ist Zusatzeigenschaft, Sonderfall, Ausnahme. Man nimmt einfach an, dass die männliche Sicht der Welt die allgemeine und für alle gültige sei.

Die Auswirkungen solcher Voreingenommenheit sind vielfältig: In der Wissenschaft sind weit weniger Frauen als Männer tätig, es werden nur wenige Themen erforscht, die mit dem Leben von Frauen zu tun haben, und sogar die Methoden sind oft einseitig. Die radikale Wissenschaftskritik ortet eine solche Voreingenommenheit schließlich sogar in den Grundprinzipien der Wissenschaft selbst, Rationalität und Objektivität, die z.B. die strikte Abgrenzung zwischen Forscher und Forschungsgegenstand (der Wissenschaftler und die Natur) fordert.

Zeichnung John Tenniel, cc 0, bearbeitet von Isabel Wienold, cc by-sa 4.0

„Androzentrismus“
heißt das Schlüsselwort

Alice findet die Parallelen zwischen Wissenschaft und Netz, die sich hier auftun, faszinierend.

Auch in den Netzen sind Frauen und Themen, die das Leben von Frauen betreffen, unterrepräsentiert. Das Handwerkszeug, die Software, gibt sich gleich den Methoden wertfrei, ist aber doch häufig nur für Männer maßgeschneidert. Das gesamte System schließlich beruht auf der Unterscheidung von 0 und 1.

Inzwischen wird allgemein Entwarnung gegeben: Die Frauen holen auf. Im Gegensatz zu anderen benachteiligten Gruppen steigt ihr Anteil unter den Internetnutzern. Die E-Mail- und Web-Adresse auf der Visitenkarte gehört mittlerweile zum guten Ton. Wortschöpfungen wie „Webgrrrls“ und „Cyberweiber“ liegen voll im Trend. Multimedia- und Webdesign wird gerade zu einem neuen Modeberuf für Frauen. Die Medien sind voll entsprechender Geschichten.

Also alles bestens? Alice freut sich: mittlerweile sind auch etliche ihrer Freundinnen online, es gibt mehr interessante Net-

zangebote von Frauen und einige echte Erfolgsstories (z.B. amazon.de). Dennoch, ein Gefühl der Skepsis bleibt. Der Anteil der Studentinnen an den Universitäten ist in einigen Studiengängen nun auch über 50%, aber C4 Professorinnen suchen wir immer noch mit der Lupe. Der Anteil der Internet-Nutzerinnen steigt, doch wie sieht es aus bei den Netzknotenbetreiberinnen und Programmiererinnen? Und wer von ihnen arbeitet nicht nur innerhalb des vorgegebenen Systems, sondern an den Netz-Strukturen selbst? Wem gehört das Netz? Nach welchen Kriterien arbeiten Suchmaschinen? Welche Regeln werden durchgesetzt? In welcher Richtung wird die Technik weiterentwickelt? Hier entscheiden sich die Machtverhältnisse. Wer glaubt, mit einer hübsch gestalteten Homepage sei sie schon aktiv im Netz, lässt sich einlullen. Gerade der große Zuspruch, den Netz-Frauen zur Zeit von den Medien bekommen, sollte sie misstrauisch machen – Lob dient zum Ruhigstellen.

Internet-Propagandist John Perry Barlow (derselbe, der meinte, der Hunger in der Dritten Welt sei nur ein Informationsproblem) verkündete auf einer Konferenz in Amsterdam: „Das Internet ist der weiblichste Ort der Welt – es ist nämlich horizontal organisiert." (unterstrichen durch nivellierende Handbewegung). Wir lassen netterweise mal die Psychoanalyse beiseite und überlegen, was er uns damit sagen wollte: Internet = hierarchiefrei = weiblich = gut? Vorsicht – die vorgebliche Hierarchiefreiheit des Internet ist Legende.

Auch von der Industrie werden Frauen allerorten als Konsumentinnen in Sachen Telekommunikation entdeckt.

Der schwedische Hersteller Nokia brachte ein besonders einfach zu bedienendes Funktelefon auf den Markt. Empörung wurde laut, als sie die angepeilte Zielgruppe bekanntgaben: Frauen und Rentner. Ein Sprecher von Nokia entschuldigte sich umgehend: Nein, sie hätten nicht vorgehabt, irgendjemand zu diskriminieren – das sei ja kein „Bimbophone"… Die Computerzeitung kommentierte: Merke – hinter jedem Fettnäpfchen lauert ein weiteres…

Alice lacht laut und hemmungslos. Obwohl das mit der Technikgestaltung ja eher ein ernstes Thema ist. Technik ist keineswegs neutral. Auch Computerprogramme schaffen eine Sicht der Welt, schon allein dadurch, dass sie einen bestimmten Sachverhalt als das Problem darstellen und die Lösung dafür anbieten. Eine Software, mit der wir das Internet nutzen, kanalisiert ganz erheblich, ob, wie und mit wem wir kommunizieren. Ein Programm kann viele Möglichkeiten beinhalten – es reicht aus, eine wichtige Funktion als Unterpunkt in der dritten Ebene eines Menüs unterzubringen, und die überwiegende Mehrzahl der Nutzerinnen und Nutzer wird diese Funktion niemals verwenden, weil sie für sie unsichtbar geblieben ist. So transportiert unser digitales Werkzeug unmerklich Welt-Anschauungen.

Alice fällt das User-Eintragsmenü einer Netzwerksoftware wieder ein; da gibt es

unter dem Namensfeld ein Kästchen zum Ankreuzen, wo „weiblich“ dransteht. Was zunächst möglicherweise praktisch erscheint (von wegen richtige Anrede etc.), hat es auf den zweiten Blick in sich. Dieses Menü vermittelt uns nämlich ganz im Nebenbei: Der Normalfall ist männlich – weiblich ist eine Zusatzeigenschaft zum Ankreuzen. Das ist keine böse Absicht – es wurde ganz im Gegenteil überhaupt nicht darüber nachgedacht – es transportiert einfach die Vorstellungen des Programmierers von den Tatsachen des Lebens. Und die bekommen wir ungefragt mitgeliefert, wann immer wir Software verwenden. Programmiertechnisch wäre es übrigens kein Problem, das Menü anders zu gestalten: ein sogenannter Radiobutton, bei dem die Möglichkeiten, zwischen denen ausgewählt wird – „weiblich“ und „männlich“ gleichberechtigt nebeneinander stehen. So wird deutlich, dass männlich auch nur eine Option ist.

Der überwiegende Teil der Programme, die wir benutzen, wird nach wie vor von 20- bis 35-jährigen männlichen weißen US-Amerikanern geschrieben. Üblicherweise wird in solchen Jobs 12 bis 16 Stunden pro Tag gearbeitet — da bleibt wenig Raum für Freundschaften, Kinder, Reisen, Kontakt mit anderen Menschen außerhalb der Arbeit, politisches Engagement oder Beschäftigung mit Kultur. Angeblich finden 16% der erwachsenen US-Amerikaner die USA nicht auf einer unbeschrifteten Weltkarte. Schade eigentlich.

„Wer nur etwas von Musik versteht, versteht auch davon nichts.“ Was ein Komponist über die Musik sagte, gilt auch für das Programmieren.

Zeichnung John Tenniel, cc 0, bearbeitet von Isabel Wienold, cc by-sa 4.0

Das Internet ist eine Mogelpackung

Wahrscheinlich sähen Computer insgesamt ganz anders aus, wenn sie von einem Team von lebenslustigen, aktiven Menschen aus unterschiedlichen Kulturen, und z.B. Frauen, die auch noch jede Menge anderes im Leben zu tun haben, völlig neu entworfen würden.

Alice sieht das Netz vor lauter Webseiten nicht…

Sie denkt an die Visionen, die viele in den Netzpioniertagen bewegt haben: allgemein verfügbares Wissen, mehr Beteiligung und mehr direkte Demokratie, globale Verständigung, Interaktion von vielen mit vielen… „Wir wollten alles – und was haben wir nun…?“ („Wir wollten alles – was haben wir nun?“ ist übrigens der Titel eines empfehlenswerten Buches von Ursula Nuber (Hsg.) – eine Bestandsaufnahme der Frauenbewegung.)

Das Internet ist eine Mogelpackung – die

Anpreisung ist noch die gleiche, aber das Produkt hat sich fundamental geändert. Wie schaut die hauptsächliche Netznutzung aus: „Surfen“ im WWW unterscheidet sich nur graduell vom „Zappen“ quer durch die TV-Programme mit der Fernbedienung. Hier wie dort kann etwas ausgewählt werden, aber es handelt sich um Alternativen, die von anderen vorgegeben wurden. Solch ein Angebot schafft nur eine scheinbare Individualität. Interaktion ist etwas anderes.

Die Möglichkeit, zwischen vorgegebenen Alternativen auszuwählen, schafft keine mündigen Bürgerinnen, sondern bestenfalls zufriedene Konsumentinnen. Eine lebendige demokratische Gesellschaft braucht Menschen, die bereit sind, selbst und gemeinschaftlich mit anderen zu handeln. Abstimmungsrituale sind keine Garantie für Teilhabe. So mutiert Demokratie zu Demoskopie – das Volk soll den Mund nur noch aufmachen, wenn es gefragt wird.

Eine virtuelle Demokratie ist eine nichtexistierende Demokratie. Direkte Demokratie dagegen wurde immer als eine Demokratie des Dialogs gedacht. Entscheidungen werden getroffen, indem man miteinander spricht, indem man die Ideen der anderen anhört und seine eigenen erläutert. Wenn diese Vorgehensweise zu einem Druck auf die Fernbedienung verkümmert, erreichen wir keine Demokratie, sondern nur eine Willensbekundung. Die unmittelbare Interaktivität verliert ihren Inhalt und wandelt sich zu einem gefährlichen Multiplikator von Dummheit.

Partizipation ist anstrengend. Für alle Beteiligten.

Wo sind denn nun die Frauen, die uns etwas zu sagen haben? Die intelligenten, kämpferischen, musischen, scharfzüngigen, lustigen, politisch aktiven…? Warum meinen sie eigentlich, dass eigene Werke, die unterhalb einer Doktorarbeit sind, nicht veröffentlichungswürdig seien? Ist das Faulheit, Harmoniesucht oder Selbstmitleid („Keiner versteht mich…“)?

Leider neigen viele Frauen dazu, nach den ersten Auseinandersetzungen im Netz nur noch mit Menschen zu kommunizieren und zusammenzuarbeiten, mit denen sie gleicher Meinung sind und nur noch private Nachrichten zu schreiben. Das führt zum einen dazu, dass sie im Netz unsichtbar bleiben, zum anderen berauben sie sich damit selbst der Möglichkeit, durch Auseinandersetzung und Kritik etwas zu lernen, und sei es auch nur, ihren Standpunkt allgemein verständlich zu formulieren.

Natürlich ist es frustrierend, wenn auf einen eigenen Text in einer Newsgroup oder Mailingliste nur Antworten kommen wie „Stell deine Umlaute gefaelligst richtig ein!“, „Das Thema hatten wir doch vor ein paar Monaten schon mal.“ oder „Ist doch Unsinn!“. Widerspruch, Genervtsein und persönliche Ablehnung führen im Netz oft zu einer schnellen Antwort, während Zustimmung viel seltener aktiv als Nachricht formuliert wird. Das zustimmende Kopfnicken und das gemurmelte „Genauso ist es!“ von vielen anderen beim Lesen des-

selben Artikels bleibt in diesem Medium unsichtbar. Das müssen wir uns mitdenken. Folglich: Mehr Gelassenheit im Umgang mit Kritik!

Und weitergedacht: Selbst häufiger einmal anderen (insbesondere anderen Frauen!) eine positive Rückmeldung auf etwas Gelesenes geben, wenn es uns gefallen hat, wenn wir etwas gelernt haben! Danke-Sagen ist wichtig – dem Netz etwas von den eigenen Erkenntnissen zurückzugeben ist gelebte Solidarität in einer Ökonomie des Schenkens.

Es ist gut, dass Frauen sich in den Datennetzen ihre eigenen Zusammenhänge und Freiräume schaffen (das geschieht zur Zeit vor allem in verschiedenen Frauen-Mailinglisten). Ebenso wichtig ist es, öffentlich sichtbar zu werden – nicht nur mit der eigenen Homepage, sondern in der allgemeinen Diskussion mitzumischen, eigene Themen und Anliegen aufzubringen und sich damit bewusst auch der Auseinandersetzung zu stellen.

Unabhängigkeit gibt es nicht geschenkt

Obacht: Wer dauerhaft mit Technikferne und Pragmatismus kokettiert und sich nur ins gemachte Netz setzen will („Ich will das alles gar nicht so genau wissen, wie das funktioniert – ich will nur Briefe an meine Freundin schreiben."), demonstriert eigentlich nur die eigene geistige Bequemlichkeit. Wer nicht wissen will, welchen Weg eine elektronische Nachricht nimmt, an welchen Stellen sie unter Umständen mitgelesen, kopiert oder manipuliert werden kann, kann auch keine wirksamen Gegenmaßnahmen ergreifen (z.B. Nachrichten mit PGP verschlüsseln und signieren, Empfangsbestätigung anfordern).

Zeichnung John Tenniel, cc 0, bearbeitet von Isabel Wienold, cc by-sa 4.0

Der Blick über den Monitorrand ist gefragt

Das gilt im weiteren Sinne auch für die Wahl der verwendeten Software oder des Netzzugangs: Wer anstatt zu der örtlichen unabhängigen Betreibergemeinschaft zu einem zentralen kommerziellen US-basierten Internet-Provider geht (weil es da zwei DM pro Monat weniger kostet und die Software geschenkt gibt), nervt...

1. ... anschließend garantiert Freundinnen und Bekannte, ihr beim Anschließen des Rechners zu helfen (kein Support vor Ort!) und ärgert sich.
2. ... sich selbst über die zielgerichtete Werbeflut an ihre Adresse (die Weitergabe persönlicher Nutzungsdaten ist ein zunehmend wichtiger Zweig des Business – wen kümmern da deutsche Datenschutzgesetze?) und wundert sich.
3. ... als sie den Provider wechseln will (z.B. weil ihre Rettet-den-Regenwald-Gruppe in den USA unerwünscht ist), dass es mittlerweile keinen Netz-Anbieter vor Ort mehr gibt.

Kurz: Die Neigung, sich mit Dingen erst auseinanderzusetzen, wenn sie ein spürbares Problem geworden sind, ist fatal.

Zap-Netz oder Surf-TV?

Kürzlich sagte der Multimediachef von Bertelsmann im Rahmen eines Vortrags: „Das Internet wird erst dann breitenwirksam sein, wenn es mit der TV-Fernbedienung bedient werden kann." In der anschließenden Diskussion meldete sich eine Frau aus dem Publikum: „Jetzt bin ich aber erleichtert. Ich hatte bisher etwas Angst, dass wir eine 2-Klassengesellschaft bekommen, also von Leuten, die am Netz sind und denen, die es nicht sind. Doch wenn das in Zukunft so einfach mit der Fernbedienung geht – dann bin ich ja beruhigt."

Alice rauft sich die Haare. Genauso sieht er aus, der Weg in die 2-Klassengesellschaft, und die, die es betrifft, merken es nicht einmal. Es geht in unseren Breitengraden nicht mehr um „online" oder „offline", sondern um die Qualität dessen, was wir online tun. Gestatten: Info-Elite und Unterhaltungsproletariat. Die einen werden das Geschehen im Netz aktiv mitgestalten, die anderen rufen fertige Angebote ab – dafür reichen die Tasten „order" und „pay".

Alice sagt es nochmal zum Mitschreiben: Um Himmels willen nicht die Tastatur aus der Hand geben!

Es gibt viel zu tun!

Gerade auch für Frauen. Jetzt mal im Stakkato: Präsenz im Netz, Demokratie im Dialog, Netzstrukturen und Machtverhältnisse, Ökonomie und Bürgerrechte, Technikgestaltung. Das ist Netzpolitik im weitesten Sinne. Und dabei geht es eben nicht nur um Frauen.

Der Blick über den Monitorrand ist gefragt: Zum Beispiel die Netzressourcen sinnvoll einzusetzen. Webdesignern und Programmierern, die bei ihrer Arbeit über Standleitung mit dem Netz verbunden sind, fehlt oft jegliches Bewusstsein dafür, dass andere 1. ihren Netzanschluss über Modem und eine normale Telefonleitung haben und 2. ihre Telefonkosten selber bezahlen müssen. Der verschwenderische Umgang mit Plugins, Grafik, Animation, Sounds und so weiter schließt de facto viele Menschen (insbesondere sozial Benachteiligte und solche aus Ländern der Dritten Welt) von der Kommunikation aus. Weiterhin muss der Schutz der Privatsphäre ernstgenommen werden. Die Netze der Zukunft brauchen eigene Regeln, die sie auch als sozialen Raum überleben lassen.

Es gibt nichts geschenkt, aber wir haben die Chance vieles besser zu machen. Die Welt ist voll faszinierender Probleme, die gelöst werden wollen.

Schließlich und überhaupt geht es nicht um die Vernetzung von Computern, sondern um die von Menschen — und nicht um den virtuellen Raum, sondern um das wirkliche Leben. Apropos, kennen Sie eigentlich Ihre Nachbarinnen? Maybe you are living next door to Alice…

Leitfaden

für gendergerechte Sprache

Von Leena Simon

Digitalcourage ist schon seit der Gründung als FoeBuD in den 1980er Jahren feministisch ausgerichtet. Es ist wissenschaftlich belegt, dass beim generischen Maskulinum im Gehirn auch ein männlicher Prototyp entsteht. So etwas gibt es auch in anderen Zusammenhängen. So ist z.B. in unserer Gegend der Prototyp für das Wort „Baum“ meist ein Laubbaum, während er auf Hawaii eher eine Palme ist. So ändern sich Antworten auf die Frage, wer sich als Bundeskanzler.in eignen würde, wesentlich, wenn die weibliche Form in der Frage mit verwendet wird. Wenn man immer nur von Männern spricht, dann denkt man sie auch – und somit kommen z.B. weniger Frauen auf ein Podium, wenn es in der Vorbereitung heißt „Welchen Redner wollen wir denn?“. Deshalb ist es wichtig, dem Gehirn einen kleinen Stolperstein zu legen, so dass klar wird: Es sind nicht nur Männer gemeint.

Stolpern, aber nicht stürzen

Wir sind der Ansicht, dass dieser Stolperstein das Gehirn nur aufwecken, es aber nicht durcheinanderbringen soll. Daher ist für uns die beste Art von gendergerechter Sprache eine, die beide Geschlechter gleichermaßen nennt, aber möglichst wenig im Lesefluss stört.

Unsere Strategie

Kann eine geschlechtsmarkierte Form vermieden werden? (z.B. „Grundrechte“ statt „Bürgerrechte“, „Studierende“ statt „Studenten“ oder „alle“ statt „jeder“)

1. Falls nein, ist Beidnennung elegant möglich?
2. Falls nein, lässt sich ggf. abwechseln? („Ärztinnen und Patienten“)
3. Falls nein, Beidnennung durch den Punkt („Redner.in“). Der Punkt ist das kleinste Satzzeichen und quasi die verkleinerte Form des „Gender-Gap“ (z.B. „Redner_in“) und beinhaltet auch das Wissen, dass es Menschen gibt, die sich weder männlich noch weiblich zuordnen wollen/können. Wer den Punkt häufiger nutzt, bemerkt noch einen entscheidenden Vorteil: Als häufigstes Satzzeichen liegt der Punkt so gut erreichbar, wie kaum ein anderes Satz- oder Sonderzeichen. Die Finger kennen den Weg deutlich besser als zum Stern oder Unterstrich und werden daher weniger im Schreibfluss gestört.

Zitate lassen wir (im Normalfall) so, wie sie sind, und wir versuchen, damit nicht allzu dogmatisch aufzutreten (etwa bei „der Anbieter“ oder „der Gesetzgeber“). An anderen Stellen experimentieren wir gerne auch etwas. Wir bemühen uns um Konsistenz, aber da wir hier eben selbst noch experimentieren, bitte nicht wundern, wenn diese Strategie nicht überall zu 100% eingehalten wurde.

Geballtes Zubehör zum Datenschutz – auf den folgenden Seiten, aber auch bei uns im Shop (ehemals im Shop-Team: David Höger)

Preise und Auszeichnungen für Digitalcourage

Digitalcourage hat in den vergangenen Jahren einige Preise und Auszeichnungen gewonnen. Hier ein kleiner Überblick aller Ehrungen, die der Verein – auch schon zu FoeBuD-Zeiten – bekommen hat.

- **„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 Rena Tangens & padeluun** für „TV d’Ameublement“ (1984)

So sieht er aus: Der „Bielefelder Frauenpreis“ auf der Hand von Rena Tangens.

Foto: Digitalcourage CC BY 4.0

Wichtige Datenschutz-termine für 2018

24.-26.1.2018	**cpdp** Internationale Datenschutzkonferenz in Brüssel. Info: cpdpconferences.org/
28.1.2018	**Europäischer Datenschutztag**. Dieser Aktionstag erinnert an die Unterzeichnung der Europäischen Datenschutzkonvention am 28. Januar 1981.
16.-18.2.2018	**AKtivCongrEZ** – für alle, die sich für Datenschutz, Grundrechte und Netzpolitik aktiv engagieren wollen. Dieses Jahr nicht in Hattingen, sondern im Bunten Haus von ver.di in Bielefeld Sennestadt. Anmeldung: https://digitalcourage.de/aktivcongrez
8.2.2018	**Safer Internet Day** / Tag der Internetsicherheit. Wir finden: Zur Sicherheit gehört auch, nicht überwacht zu werden! Besuchen Sie oder organisieren Sie für diesen Tag doch einfach mal selbst ein „Lesen gegen Überwachung“ (Seite 134) – im Cafe oder im eigenen Wohnzimmer. Info: lesen-gegen-ueberwachung.de
20.4.2018	**BigBrotherAwards.** Die Verleihung der „Oscars für Überwachung“ findet dieses Jahr im Bielefelder Stadttheater statt. Info: bigbrotherawards.de
23.5.2018	**Tag des Grundgesetzes.** Am 23. Mai 1949 wurde das deutsche Grundgesetz verkündet. Lesetipp: Christian Bommarius: Das Grundgesetz – eine Biographie. Auch ein geeigneter Termin für ein „Lesen gegen Überwachung“!
25.5.2018	Ab heute gilt die **Europäische Datenschutz-Grundverordnung** in allen EU-Mitgliedstaaten unmittelbar. Damit sollte der Datenschutz europaweit einheitlich geregelt werden. Allerdings gibt es Öffnungsklauseln, durch die einzelne Länder doch wieder abweichende Regelungen einführen können. Es lohnt sich also, weiter für starken Datenschutz zu kämpfen!
6.6.2018	Heute vor 5 Jahren wurden **Edward Snowdens geheime Dokumente** vom Guardian und der Washington Post veröffentlicht
September oder Oktober 2018	**Freedom not Fear in Brüssel**. Hier treffen sich Datenschutz- und Netz-Aktivist.innen aus ganz Europa für ein langes Wochenende zu einem selbstorganisierten Kongress: Sich informieren und vernetzen, voneinander lernen, Aktionen planen. Montags besuchen wir gemeinsam das Europäische Parlament.
27.-30.12.2018	**Chaos Communication Congress.** Großes internationales Treffen von Hackern und Häcksen. Ort noch unbekannt.

Index

Foto: Justus Holzberger

Bis zum nächsten Jahr ;-)

digitalcourage Jahrbuch 2018

Aktuelles, Aktivierendes, Richtungsweisendes ▶Die Themen und Aktionen, die uns 2017/2018 auf Trab halten: Vorratsdatenspeicherung, Gesichtserkennung am Bahnhof Südkreuz, bei Real und Post usw. ▶Wo die Datenkraken lauern – Unsere Überwachungsgesamtrechnung ▶Die kompletten Texte der BigBrotherAwards 2017 und alles, was sich daraus entwickelt hat ▶Digitale Selbstverteidigung: Wie Sie Ihr Smartphone und ihren Computer aktiv vor Datenkraken schützen können ▶Hinter den Kulissen von Digitalcourage: Das Team, die Aktionen, die Themen 1987/1988 ▶„Alice im Cyberspace“ – Frauen im Netz ▶Es geht auch ohne Facebook! Wetten? ▶Und was sind eigentlich „Smart Cities“?

ISBN 987-3-93463-616-3