padeluun und Rena Tangens (Hrsg.)

digitalcourage

für das Jahr 2022

Verlag Art d'Ameublement

Schulen datenschutzfreundlich voranbringen!

Von Jessica Wawrzyniak

Foto:Fabian Kurz, cc by-sa 4.0

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

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

Feierstimmung!

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

Was in der Zwischenzeit geschah:

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

Foto: Cord Santelmann, cc by-sa 4.0

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

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

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

März/April 2021: Im März verkündete Ministerin Eisenmann ihren Rückzug, und dann wurde es richtig spannend: Ralf Armbruster, Leiter der Stabstelle Digitale Bildungsplattformen, zeigte sich optimistisch und erklärte am 1. April bei Twitter, dass für den Start der Bildungsplattform mit Microsoft 365 alles vorbereitet sei. Leider kein April-Scherz. Die datenschutzrechtliche Auswertung des vorausgegangenen Pilotprojekts liege aber noch beim LfDI und die Frage, ob die Software tatsächlich eingebaut würde, in der Hand des zukünftigen Kultusministers bzw. der künftigen Bildungsministerin. Zu diesem Zeitpunkt war Eisenmanns Nachfolge nicht geklärt, aber es wurde bekannt, dass das Ministerium an die Grünen übergeht. Das Bündnis erfasste die Gelegenheit und mischte sich mit einem Positionspapier in die Koalitionsverhandlungen der neuen Regierung ein. Ende April die große Erleichterung: Der LfDI sprach sich gegen den schulischen Einsatz von Microsoft 365 aus und kündigte eine Duldung bis nach den Sommerferien 2021 an. Danach würde die Nutzung datenschutzrechtliche Konsequenzen mit sich ziehen.

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

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

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

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

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

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

Das Digitalcourage-Bildungspaket

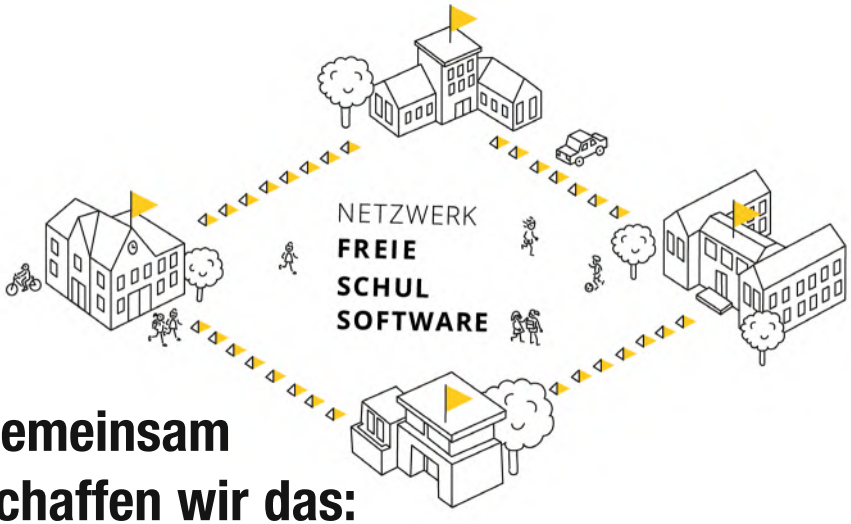
Digitalcourage verfolgt das bildungspolitische Geschehen überall im Land. Baden-Württemberg ist nur ein Beispiel, das öffentlich stark diskutiert wurde und zeigt, wie viel Stress und Ärger die Wahl der falschen Schulsoftware mit sich bringen kann. Auch andere Bundesländer und Städte haben Nachholbedarf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

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

Mit dem Digitalcourage-Bildungspaket möchten wir Aufmerksamkeit für das Thema Datenschutz an Schulen schaffen: Sowohl im Umgang mit den Daten von Schülerinnen und Schülern, als auch bei der Vermittlung von Datenschutzthemen in der Lehre.

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

Sie haben selbst Kinder oder kennen Eltern schulpflichtiger Kinder? Sie kennen Lehrerinnen und Lehrer oder beteiligen sich an der Regionalpolitik Ihrer Stadt? Dann helfen Sie mit!
🔗digitalcourage.de/bildungspaket



Grafik: Ann Kathrin Damme, Digitalcourage cc by 4.0

Gemeinsam schaffen wir das:

Das Netzwerk Freie Schulsoftware

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

Es gibt viele Schulen, die bereits einen Weg gefunden haben, Freie Software an Ihrer Schule einzusetzen und damit gute Erfahrungen machen. Diese Erfahrungen sind ein wichtiger Schlüssel, denn sie können anderen schnell helfen, während Entscheidungen auf bildungspolitischer Ebene in langen Diskussionen ausgehandelt werden.

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

screenshot Projektseite

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

🔗 digitalcourage.de/netzwerk-freie-schulsoftware

Das Netzwerk soll vor allem Schulen anregen, sich untereinander zu helfen, denn sie wissen am besten „wie der Hase läuft“. Aber natürlich können auch Privatpersonen und Vereine Hilfsangebote eintragen, um Schulen zu unterstützen.

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

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

Aber neben all der Freude ist Jessica auch ein wenig verärgert:
„Wir haben trotz begrenzter Mittel und Reichweite in kurzer Zeit so ein großes Hilfsnetzwerk geschaffen. Wieso kommen von „oben“, von den Ministerien, keine ähnlichen Projekte? Und wieso müssen Bildungsprojekte immer Millionen kosten, statt erstmal das zu nutzen, was die Schulen sich schon selbst erarbeitet haben? Die Digitalisierung von Schulen könnte schon so viel weiter und besser sein.“

Foto: Fabian Kurz, cc by-sa 4.0

Verbraucherschutz:

Digitalcourage ist jetzt Mitglied beim vzbv

Von Rena Tangens und Claudia Fischer

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

Wer hätte das gedacht:

Anfang der 2000er-Jahre wurde uns noch vom Wirtschafts-/Verbraucherministerium beschieden, dass Datenschutz mit Verbraucherschutz nichts zu tun hätte. Seitdem haben wir knapp zwei Dutzend BigBrotherAwards in der Kategorie Verbraucherschutz vergeben. (bigbrotherawards.de)

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

Foto: unbekannt? xy, cc by 4.0

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

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

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

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

Datenschutz ist Verbraucherschutz. Machen Sie uns stark!

▸ digitalcourage.de/mitglied

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

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

Unsere Datenkrake im Haus der Geschichte

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

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

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

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

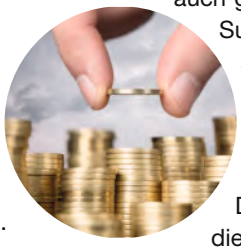
Aus hygienischen Gründen bargeldlos zahlen?

Ist Quatsch.

Von Kerstin Demuth

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

1. Kaum Schmierinfektionen nachweisbar



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

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

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

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

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

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

▶ Lassen Sie sich nicht unter Druck setzen!

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

Bild: Panthermedia

Ein Etappensieg:

Schufa zieht Pläne vorerst zurück

Von Claudia Fischer

Foto: Philip Eichler, cc by 4.0

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

Was war CheckNow? Menschen, die von der Schufa bisher eine schlechte Bewertung bekommen haben, sollten der Schufa Zugang zu ihren Kontoauszügen gewähren und so ihren Score verbessern können. Natürlich „ganz freiwillig“. Für uns aber fing der Skandal viel früher an: 2001 haben wir der Informa Unternehmensberatung GmbH (heute Bertelsmann Arvato Financial Solutions) einen BigBrotherAward für ihr Scoring übergeben.

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

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

Nicht jammern – klagen!

Unsere Verfassungsbeschwerden

Von Konstantin Macher

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

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

Seit 2016: Verfassungsbeschwerde gegen die Vorratsdatenspeicherung

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

Nein, auch 2020 und 2021 hat das Bundesverfassungsgericht – entgegen unserer Hoffnungen im letzten Jahrbuch – nicht über unsere Verfassungsbeschwerde entschieden. Aber inzwischen wird gegen den Überwachungszombie „Vorratsdatenspeicherung“ auf vielen Ebenen geklagt. Das Bundesverfassungsgericht (BVerfG) wartet anscheinend eine Entscheidung des Europäischen Gerichtshofes (EUGH) in ähnlicher Beschwerde ab. Bis dieser sein Urteil verkündet, können nach Redaktionsschluss dieses Jahrbuches noch einige Monate vergehen.

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

Unterstützen Sie uns mit Ihrer Unterschrift:
aktion.digitalcourage.de/weg-mit-vds

Mehr zur Vorratsdatenspeicherung finden Sie auf Seite 34.

Seit August 2018: Verfassungsbeschwerde gegen Staatstrojaner

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

Der Einsatz von Staatstrojanern ist ein unverhältnismäßiger Eingriff in unsere

Foto: Mischa Burmester, cc by 4.0

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

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

Staatliche Behörden sollten sich nicht länger am kommerziellen Markt für Sicherheitslücken beteiligen, z. B. durch den Erwerb der Pegasus-Staatstrojaner für BKA und BND, und damit Bürger. innen und Unternehmen gefährden. Stattdessen kämen die Behörden ihrer staatlichen Schutzpflicht nach, wenn sie ihnen bekannte Sicherheitslücken an die Hersteller melden müssten, damit diese geschlossen werden.

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

Unterstützen Sie uns
mit Ihrer Unterschrift:
aktion.digitalcourage.de/
kein-staatstrojaner

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

Aktenzeichen: 1 BvR 2466/19
Wir warten auf eine Entscheidung. In der Zwischenzeit unterstützen wir Proteste gegen Bemühungen der NRW-Landesregierung (CDU/FDP), auch noch das Versammlungsgesetz in NRW bis zur Verfassungswidrigkeit hin zu verschärfen und der Polizei z. B. umfassende Rechte auf Videoüberwachung von Demonstrationen einzuräumen. (▸ Seite 60)

Unterstützen Sie uns
mit Ihrer Unterschrift:
aktion.digitalcourage.de/polg-nrw

Warum der Kinderschutz nichts mit Vorratsdatenspeicherung zu tun hat

Von Friedemann Ebelt

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

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

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

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

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

Illustration: Isabel Wienold, cc by 4.0

Die Polizei muss für ihre Arbeit gut ausgestattet werden.

- **Hoch problematisch sind Bearbeitungsrückstände** von Fällen: „Zum Stichtag 31.03.2019 … in den Kreispolizeibehörden … 557 nicht vollstreckte Durchsuchungsbeschlüsse, davon 85 älter als drei Monate“ (Anmerkung von Digitalcourage: Der 31.3.2019 war zu Beginn der Ermittlungen in Lügde. Der Missbrauchsskandal in Bergisch Gladbach wurde erst im November 2019 aufgedeckt, der in Münster erst 2020. Die Zahlen dürften heute also deutlich höher sein.)
- Der Bericht bemängelt eine **„grundsätzlich defizitäre Personalsituation“** und erläutert, in welchem Rahmen bereits Personal aufgestockt wurde.
- Mangelhaft ist ebenso: „in Teilen **zu wenig Betreuungs- und Begleitungsangebote** (z. B. Supervision)“, die „**defizitären Raumsituationen** sowie **unzureichende Technik**.“
- **Die polizeilichen Kapazitäten bewertet der Bericht als unzureichend**: Die Folge von Personal- und Sachmittelknappheit ist, „dass die seit Jahren zunehmende Anzahl an Verfahren und insbesondere exponentiell zunehmenden Datenmengen zu deutlich verlängerten Verfahrenslaufzeiten führen und damit das möglichst frühzeitige Erkennen von ggf. anhaltenden Missbrauchstaten und deren Beendigung erschweren. Das ist aus Opfersicht und unter fachlichen Gesichtspunkten nicht hinnehmbar.“
- **Hinweistelefon:** „Das LKA NRW ist beauftragt, ein Konzept für eine ergänzende zentrale Anzeigenaufnahme in Fällen von sexuellem Missbrauch/Kinderpornografie über eine zentrale Rufnummer („Hinweistelefon“) vorzulegen.“
- „In Verfahren wegen Kinderpornografie treten **zunehmend Kinder und im besonderen Maße Jugendliche als Täterinnen und Täter** in Erscheinung.

Welche Rolle spielt die Vorratsdatenspeicherung?

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

Foto: Felix Kindermann, cc by 4.0

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

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

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

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

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

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

Stattdessen heißt es im Bericht:
„Das Innenministerium NRW sieht die derzeit nicht umgesetzte gesetzliche Pflicht zur Vorratsdatenspeicherung vorrangig in Fällen von Kinderpornografie und Rechtsextremismus als höchst problematisch an."

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

Was wirksam wäre

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

- Maßnahmen zur „Prävention, zum Schutz vor und Hilfe bei sexualisierter Gewalt gegen Kinder und Jugendliche“
- Mehr Personal
- Verbesserung der Arbeitsbedingungen für Ermittler.innen: psychologische Betreuung, Supervision, Erschwerniszulagen
- Optimierung der technischen Auswertung von Audio/Videomaterial
- Optimierung von Prozessabläufen
- Weiterbildung und Unterstützung von damit befassten Personen (u.a. technische Ermittlungsberatung, IT-fachliche Beratung, Förderung von Kompetenzen zur Sicherung und Aufbereitung von IT-Daten, zur Auswertung von IT-Daten, zur Anhörung von Kindern, zu Supervision, zur Auswertung von IT-Massendaten etc.)
- Fortbildungskapazitäten massiv ausbauen
- „Konzentration von spezialisierten Ermittlungskräften über die Behördengrenzen hinaus“
- Abbau offener Durchsuchungsbeschlüsse (Stand in NRW im März 2020: 540 offene Durchsuchungsbeschlüsse)
- Standards/Handlungsleitlinien (Kinderanhörungszimmer)
- verbesserte Anzeigenaufnahme (Not-Telefon-Nummer)
- verbesserte Zusammenarbeit mit Jugendämtern, Schulen, Kindergärten etc. („Förderung des Informationsaustausches und Stärkung eines gemeinsamen Verständnisses und Vorgehens zum Schutz von Kindern und Jugendlichen vor (sexueller) Gewalt“; „Mechanismen zum frühzeitigen Erkennen der Taten und die Weitergabe der Informationen“)

Unser Fazit

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

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

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

Digital Markets Act

Europas historische Chance gegen Internetgiganten

Von Rena Tangens und Andrea Neunzig

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

Die Erkenntnis ist offenbar auch in anderen Kreisen angekommen. So auch bei Andreas Schwab (CDU), dem Berichterstatter im Europäischen Parlament für den Digital Markets Act. Er sagt: „Die Vermachtung von Wirtschaft führt am Ende politisch zu sehr negativen Auswirkungen.“ Und begründet damit, warum es harter regulativer Interventionen bedarf. Nun haben wir in Europa endlich die Chance dazu, denn die EU-Kommission hat im Dezember 2020 einen ambitionierten Gesetzentwurf auf den Weg gebracht: den „Digital Markets Act”, kurz DMA.

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

Die Regulierungen des DMA zielen auf die sogenannten „Gatekeeper“. Das sind diejenigen Plattformen, die als „Torwächter“ den Zugang zu digitalen Märkten beherrschen und die Regeln auf diesen Märkten diktieren. Wird eine Internetplattform als Gatekeeper eingestuft, gelten für sie die im DMA genannten verbindlichen Regeln (Ge- und Verbote).

Der Entwurf der EU-Kommission muss noch mit dem EU-Parlament und dem Rat der Europäischen Union abgestimmt werden. In den sogenannten Trilog-Verhandlungen bringen Parlament und Rat Änderungen über sogenannte Berichterstatter ein. Die Verhandlungen dazu sind im vollen Gange. Auf Hochtouren läuft auch die Lobbyarbeit der betroffenen großen Konzerne, die mit allen Mitteln versuchen, die Gesetzgebung zu verhindern oder abzuschwächen und damit wirkungslos zu machen.

Aber auch Digitalcourage hat sich frühzeitig in die Verhandlungen eingebracht:

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

Foto: Jan Schöttelreier, cc by 4.0

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

rungen. Dieser Brief wurde sehr gut aufgenommen.

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

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

1. Verbot von personalisierter Werbung insgesamt.

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

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

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

2. Verbot von Dark Patterns im DMA

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

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

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

Foto: Ingo Jürgensmann, cc by 4.0

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

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

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

Warum Werbetracking schädlich und gefährlich ist

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

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

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

Informationen über unsere Verhaltensweisen, Vorlieben und Eigenarten, als ob sie herrenloses Gut wären, das sie sich einfach aneignen können. Die Ausforschung und Verfolgung, sprich: Überwachung der Netznutzer.innen zur Profitmaximierung wird immer lückenloser und detaillierter. Shoshana Zuboff nennt dieses Wirtschaftsmodell „Überwachungskapitalismus“.

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

Inhalte im Netz sollen durch Werbung finanziert werden. Doch vom Werbekuchen bleibt immer weniger zur Finanzierung übrig. Während die Werbeausgaben von Firmen im Internet erheblich steigen, sinken die Einnahmen bei Medien und Kreativen. (Grafik ▸ Seite 101) Wo bleibt dieses Geld? Inzwischen kommen die Werbe-Einnahmen überwiegend nicht mehr bei den Inhaltelieferanten (Verleger, Journalistinnen, Rechercheure, Fotografinnen etc.) an, sondern bleiben zu 50-70% bei den Werbeplattformen, Targeting-Profildatenbanken etc. hängen.

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

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

Der Werbekuchen –
Die Plattformen haben ihn unter sich aufgeteilt…

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

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

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

Kampf um Zeit und Aufmerksamkeit: Um attraktiv für Werbekunden zu sein, versuchen Plattformen, Nutzer.innen dazu zu bringen, dass sie möglichst viel Zeit auf ihrer Plattform verbringen. Dazu spielen die Plattform-Algorithmen gezielt emotionale, kontroverse und immer radikalere Inhalte zu. Dieses Ausnutzen von Emotionen wie Empörung, Schadenfreude und Hass, um Menschen zu fesseln, führt zu einer Verzerrung der Weltwahrnehmung und zu einer gefährlichen Polarisierung der Gesellschaft.

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

Es gibt eine Lösung: Eine bessere Alternative wäre **kontextabhängige Werbung**, also Werbung passend zum redaktionellen Umfeld. Denn diese braucht die Nutzer.innen nicht auszuforschen und zu tracken. Und sie nützt auch den Medien, die den Werbeplatz anbieten, weil sie nicht mehr für die Tracking- und Profilingdienste bezahlen müssen. So bleibt mehr vom Werbekuchen bei ihnen hängen.

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

Kuchenfotos: Helmut Krauthauser, cc by 4.0

Lobbyismus live:

Mit Facebook gegen Überwachung?!

Von Claudia Fischer

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

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

Spaß beiseite: Eigentlich ist diese Mail eine ernste Sache.

Klar setzt sich Digitalcourage gegen staatliche Überwachung von Messengern und für Verschlüsselung ein. Hey – wir haben schon für Verschlüsselung gekämpft, da gab es weder Google noch Facebook. Wir haben 1990 in der Zerberus-MailBox-Software verschlüsselte Postfächer eingeführt, so dass auch wir Systembetreiber die Post nicht mitlesen konnten. Wir haben 1993 das erste deutsche Handbuch für das Verschlüsselungsprogramm PGP herausgegeben und 12.000 Exemplare unter die Leute gebracht.

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

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

NGOs aufgepasst – lasst euch nicht für Facebooks Greenwashing einspannen!

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

Unterschreiben gegen Gesichtserkennung

Von Konstantin Macher

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

#ReclaimYourFace unterschreiben:
ReclaimYourFace.eu/de

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

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

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

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

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

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

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

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

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

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

▸ *Wir stellen uns dem entschieden entgegen!*

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

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

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

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

Wenn unsere EBI Erfolg hat,

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

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

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

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

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

Wir wollen ihn immer noch verhindern:

Den Fingerabdruck im Perso

Von Konstantin Macher

Grafik: Digitalcourage, cc by 4.0

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

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

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

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

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

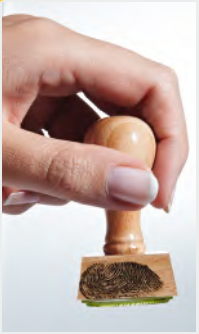
Die verpflichtende Abgabe von Fingerabdrücken ist **nicht zielführend**, da sie auf Dauer die Fälschung von Ausweisdokumenten nicht verhindern wird. In einem stetigen Katz- und Mausspiel zwischen Dokumentenfälscher.innen und (Un-)Sicherheitsbehörden werden ständig neue (und zunehmend teurere) Merkmale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

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

Hier können Sie unterschreiben (und gerne auch spenden):
aktion.digitalcourage.de/perso-ohne-finger

Erhältlich im Digitalcourage-Shop!

Stempel: Schäubles Fingerabdruck



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

Stück: 7,50 Euro zzgl. Versand

▶ **shop.digitalcourage.de**

Foto: Panthermedia

Der Digitalzwangmelder

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

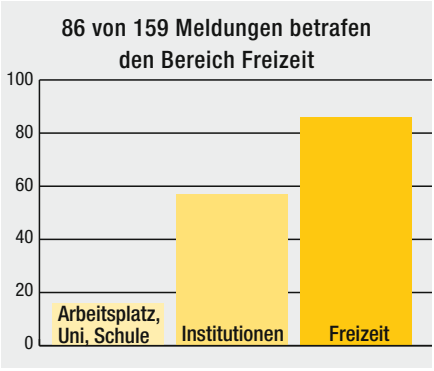
Wir lieben Technik. Und gleichzeitig finden wir es nicht in Ordnung, zur Technik-Nutzung gezwungen und davon abhängig gemacht zu werden. Denn meist werden – so ganz nebenbei und unerwähnt – dabei sehr viele Daten erhoben. Um sein Leben zu organisieren, sollte es auch immer möglich sein, auf digitale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

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

Der Rücklauf war überwältigend. Uns erreichten die unterschiedlichsten Eingaben – manche auf digitalem Weg, andere als analoger Brief. Die große Mehrheit davon kam von Menschen, die keineswegs Digitalmuffel sind. Sie kamen von Menschen, die sich in ihrem Alltag bedrängt fühlen und ein Unrechtsbewusstsein dafür haben.

Die Ergebnisse:

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



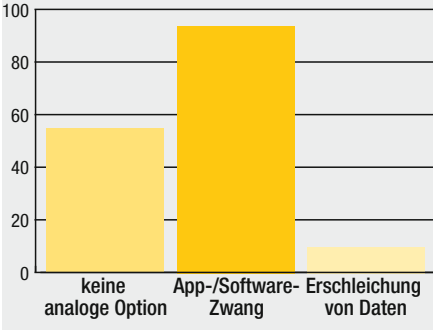
Wie erwartbar war im Sommer 2021, bezog sich mehr als ein Drittel aller Meldungen auf den Einsatz der umstrittenen und aus Datenschutzsicht nicht empfehlenswerten Luca-App. Außerdem

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

Drei verschiedene Formen von Digitalzwang konnten wir ausmachen:

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

In 94 von 159 Fällen wurden Menschen dazu genötigt, eine bestimmte Software bzw. App zu nutzen



Viele Menschen meldeten Situationen, in denen sie durch den Digitalzwang von wichtiger gesellschaftlicher Teilhabe ausgeschlossen wurden. Kitas, die Infos an die Eltern nur noch per Smartphone-App verteilen. Behörden, die nicht mehr telefonisch, sondern nur noch per Mail erreichbar sind. Museen, Zoos oder Freibäder, die man nur noch mit Online-Terminbuchung besuchen kann.

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

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

- Wir geben Ihnen eine Stimme!

Digitalcourage wirkt, wirken Sie mit!
▸digitalcourage.de/spende