

Forderungen

Wir, zehn Organisationen aus der Netz-, Umwelt- und Entwicklungspolitik, haben mit der Konferenz *Bits & Bäume* eine gemeinsame Grundlage dafür geschaffen, wie die Digitalisierung so gestaltet werden kann, dass sie dem Gemeinwohl und Frieden dient, Datenschutz ernst nimmt und soziale und ökologische Ziele gleichermaßen fördert. Die fast 2.000 TeilnehmerInnen der Konferenz in Berlin, die Ergebnisse der Workshops und die zahlreichen Diskussionen auf und vor der Bühne zeigen: Die Zivilgesellschaft und eine kritische Wissenschaft haben gemeinsam die Wissensgrundlage, die Kompetenzen, die Weitsicht, den Willen und auch die Kraft, eine nachhaltige Digitalisierung mitzugestalten, wenn sie sich zusammenschließen.

Wir können die Digitalisierung nicht alleine der Wirtschaft und der Politik überlassen. Deshalb werden wir uns zukünftig noch stärker und gemeinsam in die gesellschaftliche Diskussion und die praktische Umsetzung einbringen.

Als Bündnis von Organisationen mit zehn verschiedenen Perspektiven auf die notwendigen Veränderungen stellen wir gemeinsam diese Forderungen:

Sozial-ökologische Zielsetzung bei Gestaltung der Digitalisierung

1. Die Gestaltung der Digitalisierung soll dem Gemeinwohl dienen. Sie darf nicht einseitig auf die Förderung einer wirtschafts- und wachstumspolitischen Agenda abzielen, sondern muss auf sozial-, umwelt-, entwicklungs- und friedenpolitische Ziele ausgerichtet sein. Die Digitalisierung soll zu einer nachhaltigen Energie-, Verkehrs-, Agrar- oder Ressourcenwende beitragen und konkrete Beiträge zur umfassenden Gewährleistung der Menschenrechte, der Klimaschutzziele und zur Beendigung von Hunger und Armut leisten. Eine nachhaltige Digitalisierung in unserem Sinne setzt auf sinnvolle, menschenwürdige Arbeit, soziale Gerechtigkeit und suffiziente Lebensstile.

Demokratie

2. Basis einer gerechten Gesellschaft sind demokratische Entscheidungen: Die Digitalisierung muss in sich demokratisch gestaltet werden und gleichzeitig demokratische Prozesse unterstützen, statt diesen entgegenzuwirken. Dafür muss sie konsequent darauf ausgerichtet werden, emanzipatorische Potenziale, dezentrale Teilhabe, offene Innovationen und zivilgesellschaftliches Engagement zu fördern.

Datenschutz und Kontrolle von Monopolen

3. Datenschutz, Manipulationsfreiheit und informationelle Selbstbestimmung sollen als Grundlage von freien, demokratischen, friedlichen und langfristig souveränen Gesellschaften national und global vorangetrieben werden.

4. Es müssen Rahmenbedingungen zur Kontrolle digitaler Monopole geschaffen werden, damit sich im Norden und globalen Süden eine eigene, selbstbestimmte digitale Wirtschaft entwickeln kann. Bestehende Monopole von BetreiberInnen kommerzieller Plattformen müssen gebrochen werden, indem beispielsweise eine definierte Schnittstelle zum Austausch zwischen Social-Media-Diensten verpflichtend eingeführt wird.

Bildung

5. Politische Regulierung muss darauf zielen, auch Informationen und Bildungsangebote zu Technik und Wirkungsweisen als einen Teil des öffentlichen Gemeinguts zu begreifen, sie müssen elementarer Bestandteil des öffentlichen Wissens sein. Ein kritischer und emanzipatorischer Umgang mit digitaler Technik soll Teil von digitaler Bildung sein, dazu gehört auch der kompetente Umgang mit Falschinformationen und Hassrede in digitalen Medien.

Entwicklungs- und Handelspolitische Aspekte

6. Länder des globalen Südens müssen die Möglichkeit haben, eine eigene auf die lokalen und nationalen Bedürfnisse ausgerichtete Digitalisierung zu entwickeln. Alle Gesellschaften sollen gleichen Anteil an Nutzen und Kosten der Digitalisierung haben können. Die negativen Seiten wie menschenunwürdige Arbeitsbedingungen, Umweltverschmutzung, Gesundheitsschäden und Elektroschrott dürfen nicht einseitig auf den globalen Süden abgewälzt werden.
7. Bilaterale und multilaterale Handelsabkommen dürfen keine Verbote und Einschränkungen in den Bereichen Besteuerung (Taxation), Offenlegung des Quellcodes (Open Source) und Ort der Datenverarbeitung (Localisation) enthalten.
8. Die Technologie-Branche muss verpflichtet werden, in Fragen der Ressourcenschonung und Nachhaltigkeit die Prinzipien menschenrechtlicher und ökologischer Sorgfaltspflichten in den Abbau- und Produktionsländern konsequent anzuwenden.

IT-Sicherheit

9. Mangelhafte Software hat negative Folgen für deren NutzerInnen, die Sicherheit ihrer Daten und die digitale Infrastruktur insgesamt. Es bedarf einer Softwarehaftung, damit Software-Hersteller die Verantwortung für die entstehenden Risiken (z. B. Sicherheitslücken) tragen, statt die Qualität ihrer Software dem Profit zu unterwerfen. IT-Sicherheit ist die Grundlage einer nachhaltigen digitalen Gesellschaft.

Langlebigkeit von Software und Hardware

10. Software muss selbstbestimmt nutzbar sein, reparierbar sein und langfristig instand gehalten werden können, so wie es Open-Source-Software bereits verwirklicht. Hersteller müssen daher beispielsweise Sicherheitsupdates für die Hardware-Lebensdauer von Geräten bereitstellen und nach Ende des Supports den Quellcode als Open-Source-Variante freigeben, statt *Software Locks* einzubauen.
11. Elektronische Geräte müssen reparierbar und recyclebar sein – geplante Obsoleszenz darf es nicht geben. Dafür müssen Garantiefrieten massiv ausgeweitet werden; Hersteller müssen Ersatzteile, Reparaturwerkzeug und Know-How für alle anbieten und langfristig vorhalten. Dies soll unterstützt

werden durch eine stärkere finanzielle Förderung offener Werkstätten bzw. Repair-Cafés und gemeinwohlorientierter Forschung und Produktentwicklung. Öffentliches Forschungsgeld darf es nur für Open-Source-Produkte geben.

Trägerkreis Bits & Bäume

Brot für die Welt, BUND – Friends of the Earth Germany, CCC – Chaos Computer Club, DNR – Deutscher Naturschutzring, FIFF – Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung, Germanwatch, IÖW – Institut für ökologische Wirtschaftsforschung, Konzeptwerk Neue Ökonomie, OKF – Open Knowledge Foundation Deutschland, Technische Universität Berlin



Dagmar Boedicker

Leerstelle in der legislativen Praxis Plädoyer für eine Überwachungsgesamtrechnung

Über den Daumen gepeilt sind es 50 bis 80 Gesetze, die es den unterschiedlichsten Sicherheitsbehörden auf mehreren Ebenen gestatten, mich zu überwachen. Nicht nur mich, Sie natürlich auch. Schätzen Sie mal, was alles über Sie gespeichert wird, wenn Sie mit der Bahn von Bremen nach Frankfurt fahren, um dort in ein Flugzeug zu steigen, das Sie nach Rom bringt. Falls Sie aus der EU ausreisen und wieder heimkommen möchten, werden es noch ein paar Dateien und Sicherheitsbehörden mehr. Wie lange wird das eigentlich alles gespeichert? Wer bekommt da was von wem? Kontrolliert jemand, wann es gelöscht wird?

Vielleicht erwarten Leserinnen und Leser gar keine Antwort auf diese Frage, das ist ein Fehler! Es ist das eine, realistische hinzunehmen, dass unsere Rechte laufend verletzt werden. Menschenwürde setzt nämlich voraus, dass die staatliche Ordnung sich aus unserem Leben weitgehend heraushält, dass es Bereiche gibt, wo Sicherheitsinteressen weniger wichtig sind als unsere Würde.

*erschieden in der FIFF-Kommunikation,
herausgegeben von FIFF e.V. - ISSN 0938-3476
www.fiff.de*

lassen sich genaue Schlüsse auf das insbesondere deren Kontakt- und

Spuren einer Reise

Ich will versuchen, eine Geschäftsreise nach Rom zu beschreiben, die Sie jederzeit unternehmen könnten. Bei dieser Reise verhalten Sie sich ausnahmslos legal. Sie geben keinerlei Anlass für staatliche Eingriffe zur Gefahrenabwehr oder Strafverfolgung:

Die Bremer Straßenbahnen errechnen den für Sie günstigsten Tarif anhand der Route und stellen ihn auf Ihrer Monatskarte in Rechnung. Am Bahnhof übt die Bahn ihr Hausrecht aus und filmt Sie auf Ihrem Weg. Die Bahnfahrkarte haben Sie online gekauft, sie wird von Ihrem Konto abgebucht. Im Zug sitzen Sie an einem Vierertisch und in einer Funkzelle¹ mit einem dunkelhäutigen Herrn. Einem mutmaßlichen Gefährder, wovon Sie natürlich keine Ahnung haben. Während der Fahrt nutzen Sie WiFiICE für Ihr Pad und einen anderen Telekommunikations-Anbieter für Ihr Smartphone, beide Anbieter speichern mindestens MAC- und IP-Adresse, wahrscheinlicher sind es 29 Verbindungsinformationen pro Verbindung. In Deutschland speichern Telekommunikations-Dienstleister u. a. sämtliche Verkehrsdaten für zehn



Lek, Lawrence (2017): Geomancer. Ausstellung Open Codes. The World as a Field of Data. 2018 im ZKM Karlsruhe