Gezielte Förderung

Die digitale Zivilgesellschaft ist nur durch das ehrenamtliche Engagement und die Spenden von Bürgerinnen und Bürgern arbeitsfähig. Gerade in Krisensituationen brechen diese Stützpfeiler schnell weg und bedrohen die Existenz von Vereinen, Stiftungen und Initiativen.

In Deutschland mangelt es an niedrigschwelliger finanzieller Unterstützung für Organisationen und Sozialunternehmen aus der digitalen Zivilgesellschaft. Es braucht neue Fördermechanismen, die den Aufbau nachhaltiger Strukturen unterstützen und nicht nur Innovation im Blick haben, sondern auch die Instandhaltung und Weiterentwicklung bestehender Technologien. Möglich wäre eine solche Förderung beispielsweise durch eine vom Bund geförderte Stiftung öffentlichen Rechts, die Entwicklung, Wartung und Bereitstellung digitaler Technologien für die Gesellschaft fördert.

Öffentliches Geld, Öffentliches Gut

Es braucht rechtliche Grundlagen
dass mit öffentlichen Geldern er

lich und weiterverwendbar gemacht werden. Der Datenschutz muss dabei immer gewahrt sein.

Dazu gehören: öffentlich finanzierte Software, Datenbestände und Informationen öffentlicher Stellen, Forschungs- und Bildungsinhalte öffentlich getragener Institutionen sowie die Inhalte des öffentlich-rechtlichen Rundfunks.

Entwicklung öffentlicher digitaler Infrastruktur

Wir empfehlen kontinuierliche staatliche Investitionen in die Entwicklung und Instandhaltung digitaler Infrastruktur und den Aufbau widerstandsfähiger Netze.

Wir fordern die Förderung von Dezentralisierung und einem breiten Ökosystem von Betreibern digitaler Infrastruktur, um digitale Souveränität zu erlangen und Abhängigkeiten von einzelnen Anbietern aufzulösen, durch den Abbau von Betreibermonopolen sowie dem konsequenten Einsatz von of- Open-Source-Software-Tech-

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Unterzeichnende Organisationen:

Free Software Foundation Europe (fsfe), Digitale Gesellschaft, epicenter.works – for digital rights, Chaos Computer Club, Wikimedia Deutschland, Superrr Lab, D64 – Zentrum für digitalen Fortschritt, Stiftung neue Verantwortung, Prototype Fund, iRights.lab – Think Tank für die digitale Welt, Algorithmwatch, Nextcloud, FIfF – Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung, Open Knowledge Foundation Deutschland, Bundesverband deutscher Stiftungen, gig – Global Innovation Gathering, freifunk.net, Ashoka, Center for the Cultivation of Technology, Bits & Bäume – Digitalisierung und Nachhaltigkeit, Simply Secure, SEND – Social Entrepreneurship Netzwerk Deutschland, Stiftung Erneuerbare Freiheit, Verstehbahnhof, Goethe-Institut, OpenData.ch, Retune, Digitale Freiheit, BIB – Bundesverband Information Bibliothek, linuxmuster.net, Akademie für Ehrenamtlichkeit Deutschland, AStA TU Berlin, Bits & Bäume Berlin, #DMW – Digital Media Women, Public Beta, Privacy Week Berlin, NODE – Forum for Digital Rights, BildungsCent, Landesbibliothekszentrum Rheinland-Pfalz, Deutscher Bundesjugendring, youvo, IfZ – Initiative für Zukunftsverantwortung, Open Government Netzwerk Deutschland, Citizens for Europe, Nitrokey – secure your digital life, Seitenstark, Liquid Democracy, European Hub for Civic Engagement, BUNDjugend – Young Friends of the Earth, Selbstbestimmt.digital, FFII – Förderverein für eine freie Informations-Infrastruktur, Germanwatch, Digital Guerilla, freie.it, Education Innovation Lab, heldenrat – Beratung für soziale Bewegungen, cbm. Computer Bildung Medien, Das progressive Zentrum, Civil Liberties Union for Europe, Rosy DX, www.aufdraht.org, The Urban Tech Republic Berlin TXL, Phineo – damit Engagement wirkt, Computertruhe, FOSSGIS, Social Impact, Stiftung Ecken wecken, Wechange, Stiftung Bürgermut, Project Together, et – Evangelische Trägergruppe für gesellschaftspolitische Jugendbildung, dbv – Deutscher Bibliotheks-Verband, hackerfleet, The Isomer Community, betterplace.lab, Evangelische Schule Berlin Zentrum, ownCloud, ifa – Institut für Auslandsbeziehungen, GGC – Global Goals Curriculum 2030, In-Haus

FIfF e. V.

Grundrechtseinschränkungen in Zeiten von Corona

über Verhältnismäßigkeit, Technikeinsatz und überzogene Erwartungen

12. April 2020 – *Aktuell wird viel über die Einschränkung von Grundrechten zum Schutze der Bevölkerung diskutiert, dabei geht es um Themen wie Ausgangsbeschränkungen oder das Auswerten von Bewegungs- oder Kontaktdaten, beides zum scheinbar übergeordneten Zweck der Pandemieeindämmung. Gerade bei zweiterem fallen dann Sätze wie „Datenschutz kostet Leben", was beängstigend an das ebenso falsche „Datenschutz ist Täterschutz" erinnert. Dabei müsste in diesen Diskursen eigentlich klar sein, dass es hier keine eindeutig gebotenen Handlungen gibt. Es stehen sich unvereinbare Grundrechte gegenüber, so dass die Stärkung einer Seite immer zulasten der anderen geht. So mag eine Ausgangsbeschränkung das Recht auf Leben und körperliche Unversehrtheit schützen, sie schränkt jedoch im gleichen Atemzug die Bewegungsfreiheit, Freizügigkeit und sogar Demonstrationsfreiheit ein. Gleiches gilt für die Nutzung von Bewegungsdaten aus dem Mobilfunknetz oder anderer Ortsdaten zur Verfolgung von Infektionsketten. Diese greift ganz wesentlich in das Grundrecht auf Datenschutz und sogar die Menschenwürde ein.*

Tatsächlich müssen in diesen und anderen Fällen also verschiedene gegenläufige Grundrechte gegeneinander abgewogen werden. Das muss immer in Bezug auf ganz konkrete Maßnahmen und ihre konkrete Ausgestaltung passieren. Bevor eine letzliche politische Entscheidung getroffen werden kann, braucht es während der Abwägungsphase natürlich auch verschiedene fachliche Kompetenzen, um die Implikationen und Handlungsspielräume zu erörtern. Darum äußert sich das FIfF zu den aktuellen technischen Fragestellungen, denn hier kommt es auf das technische Detail und die konkrete Ausgestaltung an.

Das Verhältnismäßigkeitsprinzip

Zunächst jedoch ein paar Worte zum üblichen methodischen Vorgehen dieses Abwägungsvorgangs. Die verfassungstheoretische Grundlage ist dabei das sogenannte Verhältnismäßigkeitsprinzip. Dabei wird eine grundrechteeinschränkende Maßnahme in vier grundsätzlichen Schritten analysiert. Diese fragen konkret danach, ob die Maßnahme

- einem legitimen Zweck dient,
- geeignet ist, diesen Zweck zu erreichen,
- erforderlich ist, diesen Zweck zu erreichen (es also kein milderes, gleich geeignetes Mittel gibt) und
- ob die Maßnahme angemessen ist.

Eine Maßnahme ist dann legitim, wenn ihr Zweck grundsätzlich im Bereich der dem Staate übertragenen Aufgaben liegt. Geeignet ist sie, wenn sie diesem Zweck grundsätzlich kausal dienen kann. Erforderlich ist sie, wenn kein schwächeres Mittel geeignet ist, diesem Zweck zu dienen. Angemessen – oder verhältnismäßig im engeren Sinne – ist eine Maßnahme, wenn die Schwere der Grundrechtseingriffe bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe steht. Im letzten Schritt findet also eine sogenannte Rechtsgüterabwägung statt. Diese ist niemals nur rechtlich abhandelbar, sondern hat immer auch eine politische Dimension.

Beispiel: Corona-App

Wenden wir dieses Schema nun beispielhaft auf ein aktuelles Anwendungsszenario mit Technikbezug an, eine *Corona-App*.

Legitimer Zweck

Der übergeordnete Zweck der Corona-App ist in der Regel jedenfalls mittelbar angesiedelt beim Schutz des Lebens und der körperlichen Unversehrtheit von Personen während einer Pandemie; sie dient also insgesamt gesehen der Pandemieeindämmung und -steuerung, konkret derzeit der Verzögerung von Neuansteckungen, um das Gesundheitswesen nicht über seine Leistungsfähigkeit zu belasten. Dieses Ziel können Individuen nicht allein verfolgen, daher ist es ein legitimer Zweck für staatliche Stellen. Konkrete Maßnahmen brauchen jedoch einen konkreten Zweck, erst dann kann auch über eventuellen Technikeinsatz nachgedacht werden. Beispielhaft betrachten wir an dieser Stelle zwei Szenarien:

Zweck A sei die Informierung potenziell Infizierter, also die Warnung an Menschen, die mit Infizierten Kontakt hatten, sodass diese sich in Quarantäne begeben können.

Zweck B sei an dieser Stelle die allgemeine Überprüfung der Einhaltung von Ausgangsbeschränkungen, um politisches Handeln zu evaluieren.

Die Beispielzwecke können dabei durch den Einsatz jeweils verschiedener Technik verfolgt werden oder aber ganz ohne. Die Zweckfrage an sich ist allerdings keine technische Frage.

Geeignetheit

Dieser Aspekt hat jedoch eine technische Dimension, denn wenn eine bestimmte Technologie dem Zweck gar nicht dienen kann, so darf sie auch nicht eingesetzt werden.

Zweck A: Da eine technische Evaluation von GPS- oder Mobilfunk-Metadaten ergibt, dass diese Daten für die Feststellung epidemiologisch relevanter Kontaktereignisse nicht genau genug sind, scheiden diese Technologien aus. Nahbereichstechnologien wie etwa Bluetooth hingegen sind geeignet, weil sie u. a. sogar für Entfernungsmessungen im Meterbereich gedacht sind.

Zweck B: Zur Erstellung allgemeiner Bewegungsstatistiken einer Bevölkerung, so wie sie für Beispiel B benötigt werden, wären GPS- oder Mobilfunk-Metadaten technisch geeignet. Die Nahbereichstechnologien wiederum sind nur bedingt geeignet, weil sie nicht ohne weiteres einen Ortsbezug aufweisen. Ebenfalls geeignet wären aggregierte Daten, also zusammengefasste und rein statistische Daten, die aus GPS-, Mobilfunkmeta- oder Nahbereichsdaten errechnet werden können.

Erforderlichkeit

Dieser Aspekt hat ebenfalls eine technische Dimension, denn wenn ein Zweck auch mit „milderen" technischen Mitteln erreicht werden kann, also technisch bedingt weniger Eingriffe in Grundrechte nötig sind, so ist das mildere Mittel zu wählen und das aktuell betrachtete Mittel nicht einzusetzen. Um zu evaluieren, ob es ein milderes Mittel gibt bzw. was ein milderes Mittel sein kann, ist unter Umständen technische Expertise vonnöten. An dieser Stelle sei auch auf Artikel 25 DSGVO (Datenschutz durch Technikgestaltung) verwiesen, der grundsätzlich alle Datenverarbeitungen verpflichtet, Technologien dem Stand der Technik entsprechend zu Erreichung eines Zwecks nur datensparsam und grundrechtsschonend einzusetzen.

Zweck A: Der Einsatz von Nahbereichstechnologien wie etwa Bluetooth könnte erforderlich sein, wenn etwa die Gesundheitsämter die Infektionsketten nicht mit anderen Mitteln schnell und effizient aufdecken können und eine App hinreichend erfolgversprechend scheint.

Zweck B: Für die allgemeine Überprüfung der Einhaltung von Ausgangsbeschränkungen sind keinerlei Einzeldaten mit Personenbezug notwendig, wodurch nur aggregiert-statistische Daten als milderes Mittel in Frage kommen. Detailliertere Daten,

wie beispielsweise konkrete Kontaktereignisdaten, individuelle GPS-Messungen oder andere Ortsdaten scheiden an dieser Stelle aus, da sie allein schon mit Blick auf Datenschutz eingriffsintensiver aber nicht hilfreicher sind.

Angemessenheit

An dieser Stelle müssen diverse Implikationen abgewogen werden, in diesem Beispiel sogar gesamtgesellschaftliche Auswirkungen. Das können medizinische Fragestellungen sein, aber auch soziale, wirtschaftliche oder psychologische, wobei auch diese jeweils miteinander verbunden sind. Es steht jedenfalls fest, dass **Zweck A** technisch gesehen – wenn überhaupt – mit Nahbereichstechnologien begegnet werden kann. Dabei steckt auch hier der Teufel im technischen Implementationsdetail. **Zweck B** hingegen darf technisch gesehen allein mit aggregierten Daten umgesetzt werden. Es ist jedenfalls nicht möglich, darüber hinaus Pauschalaussagen zu machen, denn es hängt ganz wesentlich von der konkreten technischen Implementierung ab, wie tief der jeweilige Eingriff in die Grundrechte ist, wie die aktuelle Diskussion um das PEPP-PT-Framework[1] und die dezentralisierte DP-3T-Implementation[2] zeigt.

Nicht zuletzt ist es dann relevant, ob das konkrete Ergebnis des App-Einsatzes überhaupt im Verhältnis zu den eingeschränkten Rechten steht. Bei experimentellen Apps wie den Corona-Tracing-App-Entwürfen ist dies besonders heikel, ist deren Nutzen doch nach wie vor überhaupt nicht abschätzbar. Der aktuelle Fokus auf Apps als Heilsbringer scheint überhaupt sehr problematisch, ist doch ein – bislang nur theoretisch modellierter – Effekt erst bei Nutzung durch mindestens 60 %[3] der Bevölkerung zu erwarten. Erkenntnisse aus Singapur mögen dafür instruktiv sein, wo sich nur 13 % der Menschen die individualisierte TraceTogether-App installiert[4] hatten. Eine datenschutzfreundliche Ausgestaltung kann zwar wesentlich zur Erhöhung der Akzeptanz einer deutschen oder europäischen Lösung beitragen, doch ebenso motivieren auch die Notwendigkeit einer hohen Verbreitung zusammen mit der Drohung eines ansonsten länger andauernden Lockdowns. Genügt dies jedoch nicht, kommt dennoch keine „Corona-App-Pflicht“ in Frage, denn der unklare Nutzen einer solchen App kann – wie oben hergeleitet – doch nur minimale Grundrechtseinschränkungen rechtfertigen. Wie sehr die jeweiligen App-Entwürfe wiederum in Grundrechte eingreifen, ist ebenso unklar, fehlt es doch bislang an detaillierten Analysen. Unklarer Nutzen trifft also auf unklaren Schaden, kein guter Stand.

Abschluss und Fazit

Nach diesem Schema müssen alle aktuellen und zukünftigen Technikanwendungen analysiert werden, nur so können Schnellschüsse und eine weitere Aushöhlung der Grundrechte verhindert werden. Dies gilt insbesondere in Notfällen wie der aktuellen Pandemie. Grundrechte gelten auch in Notsituationen oder besser gesagt: gerade in Notsituationen müssen die Grundrechte gelten.

Der gesellschaftliche Fetisch hin zu informationstechnischen Lösungen für komplexe Probleme scheint nach wie vor ungebrochen und allzu oft werden dadurch alternative Herangehensweisen in den Hintergrund gedrängt oder unnötig Hoffnung geschürt. Und schon wird die App zum „entscheidenden Schlüssel“[5]. Aus diesem Grund müssen wir gerade in Notlagen besonders wachsam sein und den schnellen Verlockungen einfacher technischer Lösungen für extrem komplexe soziale Probleme widerstehen. So könnte es etwa zur Pandemieeindämmung unter Betrachtung aller Umstände weit sinnvoller zu sein, die staatliche Bestrebung und Kommunikation auf Maskennutzung und Erhöhung der Testkapazität auszurichten und nicht zu viel Hoffnung auf brauchbare Hilfe durch eine Corona-Tracing-App zu schüren.

Anmerkungen

1 *https://www.pepp-pt.org/*
2 *https://github.com/DP-3T/documents*
3 *https://www.heise.de/tp/features/Koennen-wir-der-Corona-App-vertrauen-4700302.html*
4 *https://www.golem.de/news/corona-app-per-bluetooth-kontaktpersonen-von-infizierten-ermitteln-2003-147461.html*
5 *https://www.merkur.de/politik/coronavirus-app-handy-pflicht-ueberwachung-daten-infizierte-symptome-deutschland-tracing-zr-13635397.html*

Göde Both

Informatiklehre durch fachspezifische *Gender Open Educational Resources* bereichern

Die Angebote des Portals *Gendering MINT digital*

Die meisten Gleichstellungsstrategien an den Hochschulen im Bereich Informatik zielen darauf, die Anzahl der Frauen zu erhöhen und strukturelle Barrieren für Studentinnen und Wissenschaftlerinnen aufzubrechen. Für die dritte Ebene von Gleichstellung – die des Gender-Wissens und der Gender-Kompetenzen – gibt es bislang kaum zielgruppenspezifische, freie Lehr-/Lernmaterialien. An diesem Bedarf hat unser Projekt angesetzt. Auf dem Portal Gendering MINT digital[1] *gibt es ab sofort eine Reihe von Lerneinheiten als* Open Educational Resources (OER) *für die Verwendung in der Lehre oder zum Selbststudium.*[2]

Nur wenige zielgruppenspezifische Lehr-/Lernmaterialien vermitteln wissenschaftliches Gender-Wissen[3] und Gender-Kompetenzen an Informatikstudierende: *Brigitte Ratzer* und *Bente Knoll* haben ein allgemeines Lehrbuch[4] für den Bereich Ingeni-