Newsletter für Engagement und Partizipation in Deutschland
02/2021

Teresa Staiger

Digitale Souveränität – Ein Plädoyer für die Open-Source-Gesellschaft

Gemeinwohlorientiertes digitales Ökosystem

Daten werden nicht selten als das Öl des 21. Jahrhunderts bezeichnet. Der Besitz führt zu wirtschaftlicher und politischer Macht, es können dadurch Wahlkämpfe beeinflusst und sehr passgenaue Aussagen zu dem (Kauf-)Verhalten von Individuen getroffen werden. Und sie befinden sich in der Hand ein paar weniger Konzerne.

Wie kann das Ungleichgewicht von Big Data ausgeglichen werden und Daten und Software nicht ausschließlich in den Händen großer Konzerne oder Regierungen liegen, sondern im Dienste der Gesellschaft genutzt werden? Open Source lautet hier das Zauberwort. Die gemeinwohlorientierte Nutzung von Daten sowie freie Software und Hardware ist nicht nur für die engagierte Zivilgesellschaft interessant, sondern kann eine wirkliche gesellschaftliche digitale Souveränität herstellen, ein Motto der deutschen EU-Ratspräsidentschaft. Dieser Artikel beleuchtet einen Aspekt dieses Themenfeldes, nämlich die Vorzüge freier Software und die Gründe, die dafür sprechen, dass Open Source breitere Anwendung findet. Dabei ist Open Source eng verzahnt mit Ansätzen von Open Data und – vor allem – mit dem Datenschutz.

Forderungen nach einer Open-Source-Gesellschaft sind nicht neu, Umsetzung in die Praxis, zumindest im großen Stil und von staatlicher Seite, ließen allerdings bis jetzt noch auf sich warten. Organisationen wie die Open Knowledge Fundation (OKFN) forderten in der ersten Hälfte von 2020 im Rahmen der Initiative »Digitale Zivilgesellschaft«, dass »der Aufbau eines gemeinwohlorientierten digitalen Ökosystems endlich politische Priorität bekommen muss«[1]. Unter anderem geht es darum, dass digitale Infrastrukturprojekte der Bundesregierung oder ähnlicher Akteure vermehrt mit offener Software und mit offenen Daten arbeiten, gemäß der Losung »Öffentliches Geld? Öffentliches Gut«. Durch größere Verbreitung des Open-Source-Ansatzes ließe sich diese Forderung realisieren.

Open Source

Was bedeutet Open Source? Es ist freie Software, deren Code – also die Architektur und Statik der Software, wenn man so will – offen einsehbar ist, im Gegensatz zu der proprietären Soft-

[1] https://okfn.de/blog/2020/04/digiale-zivilgesellschaft/.

ware, bei der man den Code nicht anschauen kann und somit auch nicht weiß, wie die Software genau funktioniert. Dadurch, dass offene Software einen einsehbaren Code hat, ist die Transparenz der Software und die Kontrolle derselben höher. Sicherheitslücken und andere Hintertüren, die von Kriminellen, Regierungen oder Geheimdiensten gleichermaßen genutzt werden könnten, können so durch eine breitere Kontrollmöglichkeit aufgespürt und geschlossen werden. Ergo: Open Source gibt uns eine sicherere Infrastruktur. In Zeiten, in denen Videokonferenz-Tools zur kritischen Infrastruktur geworden sind und der Arbeitsalltag von unzähligen Menschen in die digitale Sphäre verlagert wurde, ist es besonders wichtig, dass es Alternativen zu den proprietären Anbietern mit den genannten Problemen gibt. Open Source ermöglicht deswegen auch digitale Souveränität, ein Schlagwort, das gerade in aller Munde ist.

Digitale Souveränität

Wenn man über digitale Souveränität spricht, kommt man an Themen wie Open Source nicht vorbei, da sich dadurch Abhängigkeiten reduzieren lassen und kritische Infrastruktur – das hat die Pandemie gezeigt – nicht in der Hand ein paar weniger Akteure liegen sollte und der Datenschutz hat dabei den Stellenwert hat, den er verdient. Offene Software ist dezentral, es wird Wert auf Datensicherheit und Privatsphäre gelegt, die Unabhängigkeit von großen Akteuren bleibt gewahrt und sorgt dadurch für die oft geforderte digitale Souveränität, die eines der strategischen Ziele der aktuellen EU-Kommission ist. Offene Software kann und sollte ein Baustein einer wirklichen digitalen Souveränität von Nutzer*innen sein. Dafür muss es natürlich Standards geben und die Pflege und Kontrolle der Software muss durch eine Community gewährleistet werden. Hier kommt das bürgerschaftliche Engagement ins Spiel. Bei proprietärer Software steht ein Unternehmen dahinter, welches sich um die Pflege, Kontrolle und Weiterentwicklung des Produktes kümmert. Bei offener Software hingegen steht aber oftmals kein Unternehmen, sondern eine digitale Community aus Entwickler*innen dahinter, also eine digitale Zivilgesellschaft.

Open Source und bürgerschaftliches Engagement

Diese digitale Community, das digitale Engagement, muss aber mit ausreichend Ressourcen ausgestattet werden, damit sie sich um die Pflege der Software angemessen kümmern können. Es wird deutlich: Open Source bedarf einer kontinuierlichen Begleitung von kompetenten User*innen und Entwickler*innen. Die Community der Entwickler*innen und Nutzer*innen freier Software ist zwar groß und sehr engagiert. Allerdings ist es unabdingbar, dass mehr Ressourcen zur Verfügung gestellt werden müssen. Das gilt neben der Entwicklung und Begleitung offener Software gleichermaßen auch für die Implementierung dieser Infrastruktur in der Praxis, etwa bei zivilgesellschaftlichen Organisationen. Oft fehlt es den Organisationen an finanziellen und personellen Ressourcen, um einen eigenen Server für Jiitsi oder Big Blue Button zu finanzieren, geschweige denn diese Infrastruktur über eine lange Zeit sicher zu betreiben.

Auch ein gutes UX Design, also die Nutzer*innenführung, das Nutzer*innenerlebnis sowie die Oberfläche einer Software kostet Geld und würde offene Software, die daran oft spart, attraktiver machen. Anbieter proprietärer Software sind in diesem Bereich sehr erfahren, was die

Benutzung für die Nutzer*innen natürlich sehr attraktiv macht. Proprietäre Software mag einfach, bequem und ansprechend im UX-Design sein. Was aber oft unter den Tisch gefallen lassen wird, ist, dass man das nicht nur monetär, sondern auch und vor allem mit den Nutzer*innen-Daten bezahlt. Offene Software geht dagegen sorgsamer mit Datenschutzbelangen um.

Sicherheit durch Open Source

Auch für Regierungen lohnt sich die Emanzipierung von proprietärer Software hin zu mehr Unabhängigkeit durch offene Software. Die technische Infrastruktur darf, besonders jetzt in einer Pandemie-Situation, nicht unterschätzt werden, vor allem ihre Implikationen für das gesellschaftliche und politische Leben. Technologien ermöglichen Teilhabe sowie die Artikulation von Bedürfnissen verschiedenster Interessengruppen. Die Corona-Krise hat für viele Umbrüche gesorgt, aber vor allem hat sie abermals verdeutlicht, dass die kritische digitale Infrastruktur, von der eine große Anzahl von Menschen abhängig ist, in der Hand einiger weniger liegt. Die altbekannten großen Technologiekonzerne haben von der Corona-Pandemie in hohem Maße profitiert: durch die Verlagerung vieler Arbeits- und Kommunikationsprozesse in die digitale Sphäre haben sie nicht nur die Nutzungszahlen vervielfachen können, sondern sie konnten vor allem viel mehr Daten sammeln.

Eine digitale Infrastruktur, die freie Software und freies Wissen auch in Krisen bereitstellt, würde sich lohnen und die Abhängigkeit von wenigen Anbietern wenn nicht stoppen, dann zumindest minimieren. Was also kann die Politik tun? Ein solches gemeinwohlorientiertes digitales Ökosystem bedarf einer umfassenden Förderung. Darüber hinaus sollten zivilgesellschaftliche Akteure ernst genommen und in Entscheidungen eingebunden werden. Das vielfältige Wissen und die Kompetenzen der Zivilgesellschaft sollte genutzt werden, es sollte mehr freie Software in Vorhaben der öffentlichen Hand eingesetzt und für die Vermeidung von Monopolstellungen einzelner Anbieter gesorgt werden.

Corona-Warn-App

Die Corona-Warn-App (CWA) ist ein gutes Beispiel, warum offene Software, die Einhaltung des Datenschutzes und die Einbeziehung der Zivilgesellschaft der richtige Weg ist. Schon nach einigen Wochen der Corona-Pandemie wurden Rufe nach einer App laut, welche Infektionsketten nachverfolgbar machen sollte, ohne, dass die Daten bei Staat oder Polizei zentral gespeichert werden. Der Prozess wurde durch eine lebhafte Diskussion in Politik und Gesellschaft begleitet, um das Maß des Datenschutzes in der App und in der Pandemiebekämpfung auszuhandeln. Durch die bisher so nicht gekannte Einbeziehung der Zivilgesellschaft und des Engagementsektors, wie etwa Organisationen wie dem Chaos Computer Club (CCC) und anderen Expert*innen, fiel die Entscheidung zugunsten des dezentralen, datenschutzfreundlichen und damit nutzerfreundlichen Modells. Dadurch lassen sich Infektionsketten nachvollziehen und unterbrechen, es werden keine Standortdaten erfasst und der gesamte Quellcode ist Open Source und auf der Software-Entwicklungs-Seite GitHub zu finden. Auf Basis der Bluetooth-Low-Energy Technologie werden für die Kontaktnachverfolgung zwar auch personenbezogene

Daten generiert, die Begegnungen werden allerdings nur lokal auf dem jeweiligen Handy gespeichert und sind pseudonymisiert[2]. Schon vor der App-Veröffentlichung wurde der Quell-Code auf der Open-Source Plattform GitHub veröffentlicht, wo nach wie vor in unzähligen Threads Fehler, Schwachstellen und Verbesserungsvorschläge eingehen.

So konnte von Beginn an der Quellcode der App von Expert*innen, Datenschützer*innen und Bürger*innen begutachtet und kontrolliert sowie Verbesserungsvorschläge eingereicht werden. Dadurch hat sich gezeigt, dass eine nutzer*innenzentrierte Herangehensweise an Technologie durch Open Code gelingen kann und dass das Schule machen sollte. Sogar der Chaos Computer Club, der grundsätzlich keine Apps empfiehlt, hat an der CWA keine Kritik geäußert: eine kleine Sensation.

Fazit

Was zeigt uns dieser kleine Exkurs in die Entwicklung der Corona-Warn-App und in den begleitenden Diskurs?

Erstens: es lohnt sich Quellcodes, also die Architektur der App oder des Programms, offenzulegen und Meinungen sowie Expertise aus der Zivilgesellschaft einzubeziehen. Das muss von jetzt an zum Standard werden. Dadurch können Technologien entstehen, die transparent sind, einen hohen Datenschutz-Standard haben und dennoch ihre Funktion erfüllen, denn Datenschutz muss kein Hindernis darstellen.

Zweitens: digitale Projekte der öffentlichen Hand können auch unter dem Druck einer Pandemie in Zusammenarbeit mit Expert*innen und der Zivilgesellschaft zustande kommen und gleichzeitig Standards des Datenschutzes und der Datensicherheit wahren.

Drittens: Digitalisierungsprozesse sind in vielerlei Hinsicht – ob gesellschaftlich, wirtschaftlich, oder sozial - so einschneidend, dass sie besonders den Diskurs mit der Zivilgesellschaft benötigen und sich einem Dialog mit derselben öffnen müssen.

Viertens: es bedarf einer aktiven, digital souveränen Zivilgesellschaft im Digitalisierungsdiskurs, um eine gemeinwohlorientierte Software- und Datennutzung zu realisieren. So kann der Aufbau eines gemeinwohlorientierten digitalen Ökosystems, wie es u. a. die Open Knowledge Foundation fordert, gelingen.

Autorin

Teresa Staiger *ist Referentin im Projekt »Forum Digitalisierung und Engagement« des BBE. Zuvor war sie am Max-Planck-Institut für Intelligente Systeme tätig. Sie hat ihr Studium an der Johannes-Gutenberg-Universität Mainz und Cardiff University (B.A. Politikwissenschaft und*

[2] Genauere Informationen bei netzpolitik.org: https://netzpolitik.org/2020/faq-corona-apps-die-wichtigsten-fragen-und-antworten-zur-digitalen-kontaktverfolgung-contact-tracing-covid19-pepppt-dp3t/#Datenschutz%20allgemein.

Geschichte) und an der Philipps-Universität Marburg (M.A. Politikwissenschaft) absolviert. Sie interessiert sich besonders für eine gemeinwohlorientierte Digitalisierung, die durch eine digital souveräne und engagierte Zivilgesellschaft begleitet wird.

Forum Digitalisierung und Engagement:

Kontakt: info@forum-digitalisierung.de

Website: www.forum-digitalisierung.de

Twitter: @BBE_Forum

Redaktion

BBE-Newsletter für Engagement und Partizipation in Deutschland

Bundesnetzwerk Bürgerschaftliches Engagement (BBE)

Michaelkirchstr. 17/18

10179 Berlin

Tel: +49 30 62980-115

newsletter@b-b-e.de

www.b-b-e.de