Joël Adami

Datenschutz und Netzhoheit nach COVID-19

Die COVID-19-Krise hat einige negative Entwicklungen, die Datenschutz und den Zustand des freien Netzes betreffen, noch verschärft. Wenn wir nicht bald in einer Cyberpunk-Dystopie aufwachen wollen, in der Megakonzerne die Welt weitestgehend lenken, müssen rasch andere Lösungen her.

Krisen haben oft den Effekt, dass sie Entwicklungen beschleunigen. Bei COVID-19 ist das im Bereich der Digitalisierung in einem starken Maß zu sehen gewesen. Die viel besungene digitale Transformation brach mit einem Schlag in die Lebenswelt von sehr vielen ein. Videokonferenzsoftware wurde zu einem alltäglichen Tool, soziale Netzwerke wurden wichtiger denn je, um mit Freund*innen und Familie in Kontakt zu bleiben, aber auch um das kulturelle Leben verfolgen zu können. Die brachliegende lokale Wirtschaft setzte zunehmend auf Lieferplattformen. Zusätzlich wurden neue digitale Methoden in Betracht gezogen, um die Pandemie einzudämmen – allen voran das sogenannte *Contact Tracing*.

Den allermeisten dieser Dienste ist gemein, dass Datenschutzbedenken bestehen und Tendenzen in Richtung Zentralisierung und Monopolbildung zu beobachten sind. Besonders in Kombination kann das eher besorgniserregend wirken, vor allem wenn Alternativen fehlen, die dezentral funktionieren oder datensparsam sind. Das ist die Fortführung einer Entwicklung, die das Netz bereits seit geraumer Zeit mitmacht – und bisher scheint die Politik nicht willens, sie aufzuhalten.

Wie schlecht staatliche und parastaatliche Akteur*innen teilweise auf Krisen reagieren, hat sich bei den Diskussionen um eine Tracing-App herausgestellt.[1] In Europa wurde schnell eine Gruppe namens *Pan-European Privacy-Preserving Proximity Tracing* (PEPP-PT) gegründet, die aus Forschungsinstitutionen, aber auch aus Firmen besteht. Ziel war es, ein Protokoll für eine App zu entwickeln, die mittels Bluetooth Begegnungen von Menschen aufzeichnet. Im Falle einer Infektion soll es möglich sein, diese „Kontakte" zu informieren. Nach einem Richtungsstreit, der zu Austritten und Protestbriefen führte, wählte PEPP-PT einen zentralisierten Ansatz für die Frage, wer Kontakte speichern und benachrichtigten sollte: eine einzige Instanz, in den meisten Fällen vermutlich der Staat. Damit hätte dieser ein detailliertes Verzeichnis, wer sich wo mit wem getroffen hat.

Wer sich das neuste Update auf sein iPhone geladen hat, verfügt bereits über die technische Möglichkeit für *Contact Tracing*.

Datenschutzgau Contact Tracing?

Eine datensparsamere Methode hört auf den klingenden Namen *Decentralized Privacy-Preserving Proximity Tracing* (DP-3T). Der maßgebliche Unterschied liegt darin, dass ein dezentraler Ansatz gewählt wurde. Kein zentraler Server weiß, wer mit wem Kontakt hatte – allerdings wird dennoch eine Instanz benötigt, die weiß, wer infiziert ist. Diese Daten sollen dann anonymisiert an alle Apps geschickt werden, die die Liste mit den gespeicherten Kontakten vergleicht und im Infektionsfall den*die Nutzer*in benachrichtigt.

In den meisten europäischen Ländern steht eine politische Entscheidung über eine App noch aus. In Österreich ist das Rote Kreuz vorgeprescht, hat seine App jedoch kurzfristig gestoppt, weil auf das Modell von DP-3T gewechselt werden sollte. Apple und Google, die gemeinsam beinahe den gesamten Smartphone-Markt mit Betriebssystemen beliefern, haben das DP-3T-Modell übernommen und in iOS und Android eingebaut. Wer sich das neuste Update auf sein iPhone geladen hat, verfügt bereits über die technische Möglichkeit für *Contact Tracing*. Ohne eine staatlich sanktionierte App kann sie jedoch nicht aktiviert werden.

Doch auch, wenn das DP-3T-Modell besser ist als eine zentralisierte Lösung: Kritik gibt es dennoch. Datenschutz- und Netzaktivismusgruppen wie der deutsche Chaos Computer Club pochen auf die Prinzipien der Freiwilligkeit, Datensparsamkeit und Anonymität, andere IT-Forscher*innen warnen vor Missbrauchsmöglichkeiten und davor, dass die vermeintliche Anonymität sich als Trugschluss entpuppen könnte. In vielen

Joël Adami ist Journalist bei der Wochenzeitung *woxx*, Podcaster bei *Méi wéi Sex* und bloggt täglich unter soulzeppel.in.

© Patrick Galbats / Collection CNA

Fällen wäre schnell klar, wer wen infiziert hat. Frankreich hat sich trotz allen Gegenargumenten für eine zentralisierte Lösung entschieden – ob die mit Apple-Geräten harmoniert, ist fraglich, da das Tracing mit Bluetooth nur eingeschränkt funktioniert, wenn nicht auf die Apple-eigene Lösung zurückgegriffen wird.

Luxemburg will keine solche App einführen – noch nicht. Falls sich die Nachbarländer oder gar die EU doch noch auf eine App einigen werden, wird man wohl kaum daran vorbeikommen. Das würde eine Art Dammbruch bedeuten: Wir akzeptieren zwar aktuell mehr oder weniger stillschweigend, dass die Daten unserer Internetnutzung für Werbezwecke gebraucht werden – technisch versierte Nutzer*innen können sich zwar davor schützen –, aber eine staatliche Nutzung der Bewegungsdaten aller gab es bisher nicht. Wenn nun jedoch eine Überwachungs-App zur Pandemieeindämmung akzeptiert wird, was ist dann der nächste Schritt?

Ständig beobachtet im Homeoffice

Im Zuge der allgegenwärtigen Videokonferenzen haben sich manche während der COVID-19-Pandemie bereits an das Gefühl, ständig beobachtet zu werden, gewöhnt. Auch Organisationen, in denen Homeoffice bisher nur eine Eventualität war, mussten sich rasch umstellen und Lösungen finden, um weiterarbeiten zu können. Dort, wo bisher keine dauerhafte Lösung bereit war, setzte sich die Software Zoom durch. Und das trotz großer Kritik an den Methoden, mit denen die Entwickler*innen versuchten, die Installation so leicht wie möglich zu machen – in einem Fall wurde dazu sogar eine Sicherheitslücke von MacOS ausgenutzt. Auf Sicherheitsbedenken, wie etwa die Möglichkeit, fremde Zoom-Meetings „stürmen“ zu können, reagierte das Unternehmen rasch mit Updates. Über eine Ende-zu-Ende-Verschlüsselung, wie sie von Sicherheitsexpert*innen eigentlich als Goldstandard angesehen wird, verfügt die Plattform dennoch immer noch nicht.

Im Klartext heißt das: Es kann zwar niemand den Datenstrom von und zu den Servern von Zoom mitlesen, das Unternehmen jedoch schon. So fand die sexpositive Community schnell heraus, dass Zoom Bilderkennungssoftware einsetzt, um virtuelle Orgien zu unterbinden.[2] Wie sehr will man einem Unternehmen jedes Geschäftsmeeting, Uni-Seminar oder Feierabendbier anvertrauen?

Wer sich nun Sorgen macht, dass auch unsere Parlamentarier*innen und Minister*innen auf potenziell unsichere Software zurückgreifen, darf beruhigt sein: Auf einem Foto[3], das das Parlament auf Twitter veröffentlicht hat, ist deutlich zu sehen, dass die professionelle Lösung Cisco WebEx benutzt wird. Neben der teilweise zweifelhaften Inneneinrichtung der Abgeordneten ist auf dem Foto auch ersichtlich, wer mit Laptop und wer mit dem Smartphone an der Sitzung der Justizkommission teilnimmt – und welche IP-Adresse die Justizministerin dabei hatte. Dieses Beispiel zeigt dann doch,

dass es beim Datenschutz nicht nur darauf ankommt, welche Software man verwendet, sondern auch darauf, welche Daten man selbst preisgibt – von regulären Kommissionssitzungen werden eher selten Fotos veröffentlicht. Abgestimmt wurde übrigens über einen Gesetzesvorschlag gegen Voyeurismus.

Alternativen gibt es durchaus, die sind aber leider mit technischen Hürden verbunden: Die quelloffene Meetingsoftware Jitsi hat Probleme mit dem Browser Firefox, und Big Blue Button ist eigentlich für den Einsatz in der Fernlehre von Universitäten und nicht für Meetings entwickelt worden. Wer die Software sicher auf einem eigenen Server betreiben will, muss sowohl für Jitsi als auch für Big Blue Button einige Vorkenntnisse mitbringen – die Anmeldung bei Zoom ist auf jeden Fall einfacher.

Ein anderes Phänomen, das während des Lockdowns ersichtlich wurde, ist die zunehmende Konzentration auf wenige Plattformen. Amazon ist das beste Beispiel hierfür: Es gibt zwar Alternativen, aber der Gigant ist so allgegenwärtig, dass er eine Quasi-Monopolstellung einnimmt. Mit Letzshop will der luxemburgische Staat dieser Tendenz etwas entgegensetzen und sah sich gar gezwungen, eine eigene Corona-Version des Shops entwickeln zu lassen, um besonders gefährdeten Personen eine Einkaufsmöglichkeit zu bieten. Die gängigen Lieferplattformen für Supermarkt-Produkte waren nämlich alle ausgebucht. Eine neu gegründete Plattform namens nala.lu versuchte ebenfalls, kleine Unternehmen mit Lieferservice zu unterstützen. Im europäischen Ausland sind gerade bei Restaurant-Lieferdiensten immer mehr Monopolbildungen zu sehen.

Daneben wurden Streaming-Seiten wie Netflix für viele zum Ersatzprogramm für kulturelle Events, wobei auch viele Konferenzen, Konzerte, Lesungen und Theaterstücke mittels Livestream vom Wohnzimmer ins Wohnzimmer ausgestrahlt wurden. Die Vortragenden und Künstler*innen griffen verständlicherweise vor allem auf Facebook und YouTube zurück; immerhin kennt und nutzt das Publikum diese Plattformen seit langem, und es ist relativ leicht, einen Stream einzurichten. Es gibt zwar eine gewisse Anzahl dezentraler Alternativen zu bekannteren sozialen Netzwerken, die Nutzer*innenzahlen dort sind jedoch überschaubar.

Von der Fremdbestimmung zur Eigenkontrolle

Die Internetgiganten könnten nach der kommenden Wirtschaftskrise noch mehr Macht erhalten, während die politische Sphäre sie entweder hofiert oder die Entwicklungen verschläft. Durch die Krise wurde auf jeden Fall deutlich, dass wir im digitalen Bereich nicht vorbereitet werden. Durch neue Schulfächer wie „Programmieren“ sollen Schüler*innen zu echten Digital Natives herangezogen werden – sicher ein lobenswerter Ansatz, aber wenn junge Menschen lediglich Produkte von Microsoft oder Apple kennenlernen,

Wie bereitet man sich digital auf eine Pandemie vor?

werden sie kaum die Werkzeuge haben, um sich digital emanzipieren zu können. Hier sollte konsequenter auf quelloffene Software gesetzt werden, sowohl für die eingesetzten Werkzeuge, als auch für den Stoff.

Wie bereitet man sich digital auf eine Pandemie vor? In Luxemburg wird seit über sieben Jahren an einer elektronischen Krankenakte gebastelt – wie gut Patient*innendaten geschützt sein werden, wird wohl schwierig herauszufinden sein. Es scheint, als wäre Datenschutz mit Inkrafttreten der Datenschutz-Grundverordnung von der politischen Agenda verschwunden – dabei bräuchte es hier klare Regeln, die im Fall von ansteckenden Krankheiten sowohl Privatsphäre als auch Gesundheit schützen. Zwar ist es in sozialen Netzwerken möglich, die Daten, die über eine*n gespeichert wurden, einzusehen, bei vielen Services gleicht das aber einem Spießrutenlauf. Hier müssten einheitliche Standards her, wie diese Transparenz auszusehen hat.
Schlussendlich braucht es mutige digitale Initiativen, die nicht als hippe Start-Ups daherkommen, deren Businessplan ohnehin darin besteht, von einer größeren Firma aufgekauft zu werden. So könnten sich beispielsweise die „alternativen“ Medien Luxemburgs zusammentun, um einen Server der quelloffenen Twitter-Alternative *Mastodon* auf die Beine zu stellen. Das würde eine Plattform schaffen, die lokale Relevanz hat und dennoch weltweit vernetzt ist – auf die schwammigen Moderationsregeln von Facebook und Twitter wäre man nicht mehr angewiesen.

Auch das Kulturministerium könnte – nicht nur für den Lockdown während der zweiten Welle – eine Plattform für digitale Kunst schaffen. Theaterstücke, Ausstellungen und andere Kunst, die öffentlich gefördert wird, könnten dort ausgestellt oder gestreamt werden – das würde mehr Publikum und eine größere Unabhängigkeit von den großen Anbietern bedeuten.[4]

„Die Cloud ist nur ein Computer, der jemand anderem gehört“ lautet ein Stehsatz von Internetaktivist*innen. Wer diese Computer kontrolliert, kontrolliert letzten Endes, wie wir kommunizieren, konsumieren und unsere Freizeit gestalten. Eine resilientere digitale Infrastruktur braucht mehr demokratische Kontrolle – die wird am besten durch gemeinschaftliches Eigentum gewährleistet. ◆

1 Mehr zum Contact Tracing auf https://www.woxx.lu/contact-tracing-mit-einer-app-aus-der-krise/ (alle Internetseiten, auf die in diesem Beitrag verwiesen wird, wurden zuletzt am 29. Mai 2020 aufgerufen).

2 https://www.them.us/story/zoom-cracking-down-on-virtual-sex-parties

3 Voyeuristische Einblicke in die Chamber-Justizkommission: https://twitter.com/ChambreLux/status/1255446076313780225/photo/1

4 Anm. d. Red.: Zum Plan einer digitalen Plattform für Kultur vgl. das Gespräch mit Serge Tonnar ab S. 64 in diesem Heft.