Die Sicherheitsversprechen digitaler Technologien

von Andreas Langenohl, Carola Westermeier

Ein Beitrag zur Reihe "Sicherheit in der Krise"

In Zeiten von SARS-CoV-2 und COVID-19 wird digitaler Infrastruktur eine enorme Sicherungsleistung zugesprochen, da man sich – in bisher unbekanntem Ausmaß – von der Digitalisierung eine Lösung existenzieller gesellschaftlicher Probleme erhofft. So findet Erwerbsarbeit nun im internetbasierten Home-Office statt, Whatsapp und Videotelefonie ermöglichen eine ansteckungsfreie Sozialität, die Veranstaltungen des Sommersemesters 2020 werden nicht in Seminarräumen, sondern auf digitalen Lernplattformen abgehalten und mit den Daten mobiler Endgeräte, so die aktuellen Planungen der Bundesregierung, können die aufgrund einer Ansteckung problematischen Sozialkontakte nachvollzogen werden. Anhand dieser Beispiele wird offensichtlich, was der digitalen Infrastruktur alles zugetraut, was aber auch von ihr erwartet wird.

Erstens soll sie negative Effekte auffangen, sofern andere Infrastrukturen lahmgelegt werden oder überlastet sind. Unterbrochene oder erschwerte ökonomische Prozessketten – von betrieblicher Kommunikation bis hin zur Wertschöpfung – sollen digital substituiert werden. Das Gesundheitssystem mit seinen medizinischen Infrastrukturen könnte eventuell vor einem Kollaps bewahrt werden, wenn mobile Endgeräte bei Verdacht auf kontaminöse Sozialkontakte Warnungen an die Betroffenen versenden. Schul- und Hochschulunterricht, hier verstanden als pädagogische Infrastrukturen, wird im virtuellen Raum nachgebildet. Mit diesem sich in mehreren Bereichen vollziehenden Bedeutungszuwachs avanciert digitale Technologie in noch stärkerem Maße zur kritischen Infrastruktur, als solche wurde sie von der Politik bereits lange vor der Corona-Pandemie adressiert. Ihre Beeinträchtigung oder gar ihr Ausfall hätten weitreichende Konsequenzen für als vital verstandene soziale Institutionen.[1] Wohin das führen kann, erlebten Mitarbeitende und Studierende der Justus-Liebig-Universität Gießen im Dezember 2019, als die Universität, lahmgelegt durch den virtuellen Virus einer Schadsoftware, für fast zwei Wochen vollständig vom Netz ging. Nur wenige Monate später, in Zeiten des biologischen Virus SARS-CoV-2, müssen sämtliche Lehr-, Forschungs- und Verwaltungsabläufe möglichst komplett auf den Online-Betrieb umgestellt werden. Neben der Vulnerabilität der Infrastruktur selbst ist der Zugang zu ihren vielfältigen Möglichkeiten entsprechend den sozialen, generationalen und regionalen Unterschieden höchst

divers. Streaming-Angebote und Online-Meetings benötigen entsprechende Datenmengen und -kapazitäten. Hier ist der schleppende Glasfaserausbau, insbesondere in ländlichen Gebieten, ein limitierender Faktor. Zwar steht die digitale „Daseinsvorsorge" schon seit längerem auf der politischen Agenda, aktuell besteht aber noch ein großer digital divide.[2] Und in Haushalten, die keine Computer oder Laptops besitzen, sondern lediglich über Smartphones online gehen, sind wiederum der Zugang zu und die Nutzung von digitalen (Lern-)Angeboten besonders schwierig. Auf das Versprechen, digitale Netzwerke sicherten andere Infrastrukturen im Ernstfall ab, ist somit nur bedingt zu vertrauen, denn auch sie sind nicht immun gegen Angriffe und Ausfälle und auch ihre Verfügbarkeit gilt nicht überall und nicht für alle in gleichem Maße. Wie Antina Schnitzler in ihrer Arbeit zu *Democracy's Infrastructures* überzeugend herausarbeitet, werden solche gesellschaftlichen Ungleichverteilungen in den Debatten um Infrastruktur nur im Ansatz mitreflektiert.[3]

Zweitens sollen mittels digitaler Kommunikation die soziale Zirkulation und Mobilität, die durch das Virus stark beeinträchtigt sind, am Leben erhalten werden. Flächendeckendes Home-Schooling und weitgehendes Home-Office zielen darauf, physische Sozialkontakte in der Schule oder im Büro digital zu ersetzen. Aus demselben Grund verlagern sich Besuche bei Freunden und Verwandten in diverse Chat- und Telekommunikationsräume. Wir sehen hier eine weitere Anrufung von Sicherheit, die sich weniger auf die Aufrechterhaltung existenzieller Sektoren der Gesellschaft, sondern auf eine Dimension des Sorgens bezieht.[4] Anstatt als Abwehr einer Bedrohung erscheint Sicherheit hier vielmehr als Garant für und Unterstützung von sozialen Beziehungen. Einem mittlerweile medial verbreiteten Idealbild zufolge sind diese digitalen Beziehungsgefüge geprägt von Solidarität mit den Mitmenschen, von Aufmerksamkeit für die Nachbarn und von Interesse an den anderen: Man kümmert und sorgt sich um die Schwachen, die Alten, die Schulkinder und Studierenden, die Kranken, die Obdachlosen, bisweilen sogar um die Geflüchteten. Entsprechend werden derzeit – mithilfe sozialer Medien – vielerorts nachbarschaftliche Hilfsnetzwerke organisiert. Aber auch hier ist kritisch zu fragen, inwieweit diese communities of care sozial exkludierend wirken oder bestehende Ausschlussmechanismen zumindest reproduzieren.[5] Der nachweisliche Anstieg häuslicher Gewalt unter dem Eindruck von Selbstisolierungsmaßnahmen lässt außerdem vermuten, dass das Bild vom heimeligen Zuhause, das als Ausgangs- und zugleich als Fluchtpunkt digitalisierter Sorgepraktiken fungiert, stark überidealisiert ist.[6]

Drittens soll mittels digitaler Kommunikations- und Datenübermittlungstechnologien die Ausbreitung des Virus bekämpft werden. Eine derzeit diskutierte Corona-App wäre so konfiguriert, dass Personen, die eventuell Kontakt zu Infizierten hatten, qua Nachricht gewarnt und zum Test oder einer häuslichen Quarantäne aufgefordert würden.[7] Im Zuge der Debatten um eine Implementierung beziehen sich sowohl politische wie mediale Akteure immer wieder auf Beispiele aus digital hocherschlossenen Gesellschaften wie Südkorea, Singapur und Taiwan,[8] um die Vorteile einer digital erfassten Sozialwelt bei der

Eindämmung des Virus zu betonen: Weil sich dort praktisch jeder Schritt und jeder Sozialkontakt digital nachverfolgen und damit im Fall einer Ansteckung rekonstruieren ließe, könnten Infektionsketten schnell erfasst und durch Isolation der Risikopersonen unterbrochen werden. In einer der möglichen Versionen der Corona-App könnte die Kontakterfassung mit weiteren Kategorien wie Vorerkrankungen kombiniert werden und so zu einer zunehmend personalisierten Risikoeinschätzung führen. Zugleich sollen bestimmte Architekturen der App verhindern, dass die europäischen Datenschutzbestimmungen verletzt werden, obwohl die App sehr persönliche Daten und per Bluetooth-Technologie insbesondere Nahfeldkontakte erfassen würde.[9] Neben verstärkten Testungen und dem contact tracing mittels App, das letztendlich die telefonische Nachverfolgung von Kontakten durch die Gesundheitsämter beschleunigen soll, werden auch andere Optionen zur Datenerfassung und -analyse diskutiert. So könnte es beispielsweise durch akkumulierte Daten und Methoden der digitalen Epidemiologie demnächst möglich sein, die Verbreitung des Virus nicht nur ‚in Echtzeit' zu beobachten, sondern sogar vorhersagbar zu machen, so die Wissenschaftler und wenigen Wissenschaftlerinnen der Leopoldina.[10] Wenn die Bevölkerung weiterhin die Hygiene- und Abstandsbestimmungen einhalte und ihre pseudonymisierten Kontakte zur digitalen Nachverfolgung bereitstelle, könne das öffentliche Leben wieder einsetzen.

Bei allen drei Punkten – Absicherung, Sorge und Bekämpfung – wird immer wieder darauf hingewiesen, dass digitale Infrastrukturen nur dann wirksam und hilfreichen seien, wenn der Grad an digitaler Konnektivität in der Bevölkerung, also der Zugang zu und die Nutzung von digitaler Kommunikationsinfrastruktur, möglichst hoch sei. Eine solche, wenn man so will, demografische Konnektivität – gemeint sind hiermit die digitale Anbindung wie auch die digitale Erschließung der Bevölkerung – wird somit zur Voraussetzung und Gelingensbedingung digitaler Sicherheitstechnologien. Weiterhin gilt: Wenn die Wiederaufnahme des öffentlichen Lebens diskursiv an die Ausweitung digitaler Überwachung gekoppelt ist – nur damit sei eine sichere Rückkehr zu üblichen öffentlichen Verkehrsformen überhaupt denkbar –, dann gilt digitale Konnektivität als Vorbedingung zur Gewährleistung des öffentlichen Lebens. Anders als beispielsweise die ebenfalls umstrittenen Überwachungskameras auf öffentlichen Plätzen sollen die derzeit diskutierten digitalen Technologien nicht das bestehende öffentliche Leben vor Kriminalität schützen, sondern das künftige öffentliche Leben erst ermöglichen.

Im dritten Fall der individualisierten Risikoerfassung und -bekämpfung ist es außerdem unerlässlich, dass sich die Menschen mit den zentralen wie dezentralen Servern der Contact-Tracing-App nicht nur verbinden können, sondern auch verbinden wollen. Während etwa in China die individualisierte Risikokalkulation die vorherige Nutzung von zwei Payment- und Messenger-Apps voraussetzt,[11] soll in Europa ebendiese Verknüpfung von kommerziell erfassten mit gesundheitsrelevanten Daten vermieden werden. Die anhaltenden Diskussionen über die Möglichkeiten digitaler Vernetzungstechnologien zur Bekämpfung der Pandemie offenbaren indes schon jetzt verschiedene sicherheitspolitische

Dilemmata. Bezüglich der Einführung einer flächendeckenden Corona-App werden Bedenken geäußert, dass geltende Datenschutznormen ausgesetzt oder unterlaufen werden. Weiterhin wird die mögliche ökonomische Verwendung der digitalen Daten kritisch beäugt. Digitale, auf die gesamte Bevölkerung zielende Konnektivität forciert Geschäftsmodelle, die auf eine Maximierung der Online-Zeit von Nutzerinnen und Nutzer setzen. Europäische Initiativen betonen zwar, dass eine Corona-App nur dann auf breite Akzeptanz stoße und entsprechend hohe Verbreitung finde, wenn ihre Nutzung der Daten auf epidemiologische Zwecke beschränkt sei, es also zu keiner Verknüpfung mit kommerziellen Analysen kommen dürfe.[12] Jedoch zeigt der politische Nachdruck, mit dem die Sicherheit der Daten beteuert und die Bevölkerung von ihrer Effektivität überzeugt werden soll, zunächst einmal nur an, dass von einer generischen Korrumpierbarkeit solcher digitalen Anwendungen auch in Expertenkreisen ausgegangen wird.

Am Ende zeigt sich ein zutiefst ambivalentes Bild der Sicherheitsversprechen digitaler Technologien und Infrastrukturen. Sie substituieren nichtdigitale Zirkulationsprozesse, die für die und in der Gesellschaft als entscheidend angesehen werden. Dadurch erzeugen sie aber eine Vulnerabilität höherer Ordnung und verstärken außerdem ohnehin vorhandene Ungleichheiten in den Zugängen zu Infrastrukturen. Sie ermöglichen einerseits die Aufrechterhaltung einiger Praktiken des Sorgens auch ohne direkte physische Kopräsenz, andererseits reproduzieren sie häusliche Stereotype von Sicherheit und Geborgenheit, obwohl gerade dieses Zuhause für viele ein höchst unsicherer, bisweilen sogar gefährlicher Ort ist. Und sie sollen eine epidemiologische Eindämmung des Virus bewerkstelligen, während sie der Unterhöhlung demokratischer Öffentlichkeit und der ökonomischen Korrumpierbarkeit verdächtigt werden.

Fußnoten

[1] Claudia Aradau, Security That Matters. Critical Infrastructure and Objects of Protection, in: Security Dialogue 41 (2010), 5, S. 491–514; Andreas Folkers, Kritische Infrastruktur, in: Nadine Marquardt / Verena Schreiber (Hg.), Ortsregister. Ein Glossar zu Räumen der Gegenwart, Bielefeld 2012, S. 154–159.

[2] Amina Nolte / Carola Westermeier, Den Staat wieder spüren – Heimat und Infrastruktur [21.4.2020], in: theorieblog, 23.10.2018.

[3] Antina Schnitzler, Democracy's Infrastructures. Techno-Politics and Protest after Apartheid, Princeton, NJ / Oxford 2016.

[4] Mike Laufenberg, Sexualität und Biomacht. Vom Sicherheitsdispositiv zur Politik der Sorge, Bielefeld 2014; Katrin Meyer, Kritik der Sicherheit. Vom gouvernementalen Sicherheitsdenken zur Politik der geteilten Sorge, in: traverse. Zeitschrift für Geschichte 16 (2009), 1, S. 25–39.

[5] Siehe auch den Beitrag von Thorsten Bonacker in diesem Schwerpunkt zu „Sicherheit in der Krise".

[6] Ulrike Nimz / Edeltraud Rattenhuber, Gefangen auf engstem Raum [21.4.2020], in:

Süddeutsche Zeitung, 31.3.2020.

[7] Meike Laaf, Wann kommt die App, die hilft? [21.4.2020], in: Die Zeit, 11.4.2020.

[8] Katrin Büchenbacher / Martin Kölling, Tiefe Infektionszahlen, weniger Todesfälle. Weshalb Chinas Nachbarstaaten die Corona-Epidemie besser beherrschen als viele europäische Länder [21.4.2020], in: Neue Zürcher Zeitung, 21.3.2020.

[9] Ulf Buermeyer / Johannes Abeler / Matthias Bäcker, Corona-Tracking & Datenschutz: kein notwendiger Widerspruch [21.4.2020], in: Netzpolitik, 29.3.2020.

[10] Leopoldina Nationale Akademie der Wissenschaften (Hg.), Dritte Ad-hoc Stellungnahme. Corona-Virus-Pandemie – die Krise nachhaltig überwinden [21.4.2020], 13.4.2020, S. 5 ff.

[11] Paul Mozur / Raymond Zhong / Aaron Krolik, In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags [21.4.2020], in: New York Times, 1.3.2020.

[12] European Commission (Hg.), Coronavirus. Commission Adopts Recommendation to Support Exit Strategies through Mobile Data and Apps [21.4.2020], Pressemitteilung, 8.4.2020.