



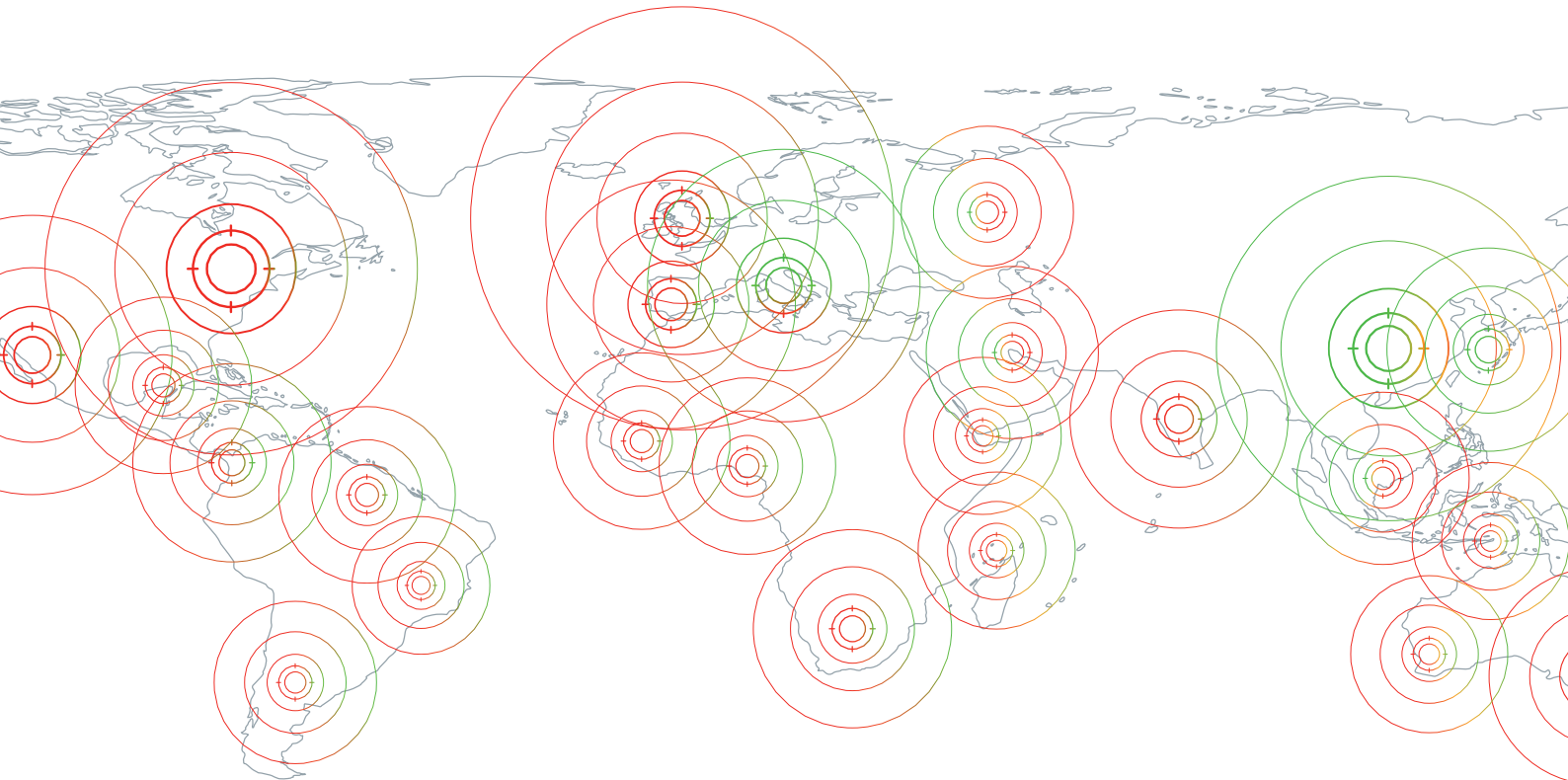
Automatisierte Entscheidungssysteme und der Kampf gegen COVID-19 – unsere Position

1. Version (2. April 2020)

Angesichts der weltweiten Ausbreitung des COVID-19-Virus fragen sich viele, ob und wie man Systeme automatisierter Entscheidungsfindung (automated decision-making systems, ADMS) zur Eindämmung der Pandemie einsetzen kann. In den einzelnen Ländern werden unterschiedliche Lösungen entwickelt und umgesetzt: Diese reichen von autoritärer sozialer Kontrolle (China) bis hin zu datenschutzorientierten, dezentralisierten Lösungen („Safe Paths“ des MIT). Es folgt eine Reihe möglicher Prinzipien und Überlegungen. Sie sollen als Grundlage für eine informierte, demokratische und fruchtbare Diskussion über den Einsatz von ADMS zur Bewältigung der gegenwärtigen Pandemie dienen.

1. COVID-19 ist kein technologisches Problem. Analysen der bisherigen Reaktionen auf den Ausbruch zeigen, dass erfolgreiche Maßnahmen immer auf einem breit aufgestellten Gesundheitswesen beruhen. Singapur, Südkorea und Taiwan, die häufig als Vorbilder für die Eindämmung der Epidemie genannt werden, hatten alle bereits entsprechende Pläne, von denen die meisten nach dem SARS-Ausbruch von 2003 entwickelt wurden. Eine gute Vorbereitung auf eine Epidemie geht über technische Lösungen hinaus: Sie setzt voraus, dass man über Ressourcen, Kompetenzen, Pläne und die politische Legitimation verfügt. Und die Entschlossenheit, diese im Bedarfsfall rasch einzusetzen.

2. Es gibt keine Pauschallösung für den Ausbruch von COVID-19. Um das Virus erfolgreich bekämpfen zu können, sind Tests, Kontaktverfolgung und Einschränkungen erforderlich. Allerdings sind die jeweiligen Kontexte niemals identisch. Ein Land, in dem das Virus seit Monaten unentdeckt zirkuliert (z.B. Italien), unterscheidet sich von einem Land, das Träger des Virus frühzeitig identifiziert hat (z.B. Südkorea). Auch soziale, politische und kulturelle Unterschiede spielen bei der Durchsetzung der Gesundheitspolitik eine Rolle. Das bedeutet, dass die gleiche technologische Lösung in solch unterschiedlichen Kontexten sehr unterschiedliche Ergebnisse hervorbringen kann.



3. Demzufolge gibt es keinen Grund, bei der Bekämpfung der COVID-19-Pandemie überstürzt auf digitale Massenüberwachung zurückzugreifen.

Es ist nicht nur eine Frage des Datenschutzes – obwohl der Schutz der Privatsphäre ein Grundrecht bleibt und respektiert werden muss. Bevor wir uns beispielsweise mit datenschutzrechtlichen Bedenken zum Einsatz von Apps zur digitalen Kontaktverfolgung befassen, sollten wir fragen: **Funktionieren sie überhaupt?** Ergebnisse aus der Fachliteratur und von früheren Epidemien ergeben derzeit ein gemischtes Bild und hängen stark vom Kontext ab. Dabei müssen die Rechte mit dem zu erwartenden Nutzen (Leben retten) abgewogen werden. Aber es besteht keine Notwendigkeit, unsere fundamentalen Freiheiten zu opfern, wenn es keinem Zweck dient.

4. Ausgangssperren können nicht unbegrenzt bestehen. Wir müssen darüber nachdenken, wie wir schrittweise zur "Normalität" zurückkehren können.

Die meisten Szenarien beinhalten eine Form digitaler Überwachung, welche notwendig zu werden scheint, wenn man bestimmte Aspekte von COVID-19 berücksichtigt: die Existenz von Patient:innen ohne Symptome, die dennoch ansteckend sein können; die 14-tägige Inkubationszeit; die Tatsache, dass es noch keine Heilmittel oder Impfstoffe für die Krankheit gibt. Zivilgesellschaftliche Organisationen müssen bereit sein, sich an der Diskussion über die vorgesehenen Überwachungsmaßnahmen zu beteiligen, um bei der Erarbeitung angemessener Lösungsansätze mitzuwirken.

5. Datenschutz und der Schutz vor COVID-19 schließen sich nicht gegenseitig aus.

Lösungen wie die am MIT entwickelte Plattform Safe Paths und die Initiative Pan-European Privacy Preserving Proximity Tracing verbinden die digitale Kontaktverfolgung mit einem offenen, dezentralisierten und stärker auf die Wahrung von Rechten gerichteten Ansatz. Auf diese Weise begegnen auch Länder wie Singapur dem Problem (z.B. durch die App Trace-Together), dessen Ansatz sich von dem Südkoreas und Israels unterscheidet.

6. Jede Lösung muss in einer Weise umgesetzt werden, die mit der Demokratie in Einklang steht.

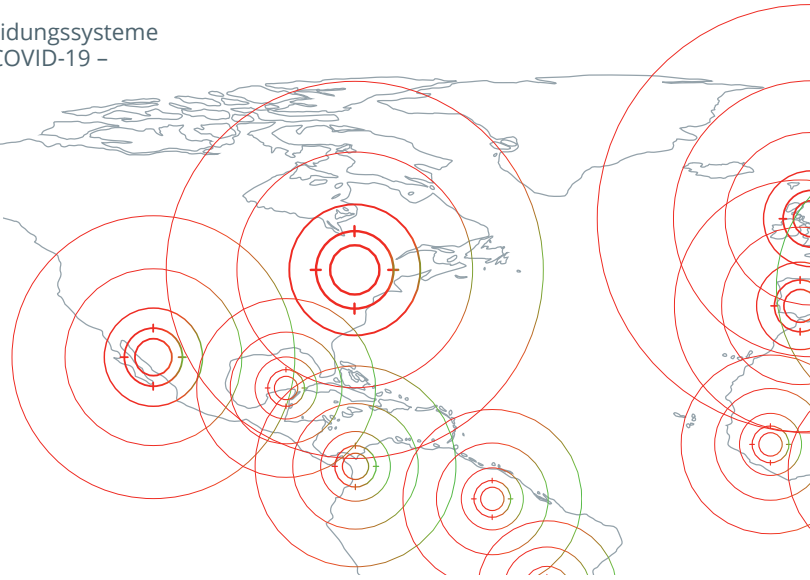
Die Demokratie steht der Eindämmung der Pandemie nicht im Wege: Sie ist die einzige Hoffnung, die wir haben, um dem Ausbruch mit Vernunft zu begegnen und die Rechte aller zu respektieren. Transparenz sollte an erster Stelle stehen bei 1) den technologischen Lösungen, an denen gearbeitet wird, 2) den Expertenteams oder Ad-hoc-Institutionen, die zu ihrer Erarbeitung geschaffen wurden, 3) den Belegen dafür, warum sie tatsächlich umgesetzt werden sollten, 4) denjenigen, die sie letztlich entwickeln und einsetzen werden, insbesondere wenn private Akteure beteiligt sind. Nur Transparenz gewährleistet, dass Zivilgesellschaft und Parlamentarier:innen in der Lage sind, Entscheidungsträger:innen zur Rechenschaft zur verpflichten.

7. Die Umwandlung soziodemografischer Informationen in computerlesbare Daten (datafication), die mit der Entwicklung von ADMS zur Bekämpfung des Virus einhergeht, wird neue soziale Kategorien schaffen, die immer auch die Gefahr für eine Diskriminierung in sich bergen. **Regierungen müssen die Stigmatisierung von Menschen verhindern**, die in den falschen Kategorien landen, und sie müssen die Rechte von Personen wahren, die auf den verwendeten Bewertungsskalen nicht hoch genug abschneiden, insbesondere bei der Triage in der Gesundheitsversorgung.

8. Selbst wenn sich tatsächlich als nützlich erweisen, sollten **digitale Überwachungsverfahren konsequent auf bestehenden Datenschutzprinzipien basieren**: Wie kürzlich vom European Data Protection Board in einer Erklärung klargestellt wurde, müssen Notwendigkeit, Verhältnismäßigkeit, Zweckbindung und die Rechtsstaatlichkeit im Allgemeinen auch bei einem Notfall im Bereich des Gesundheitswesens respektiert werden. Bürger:innen müssen in der Lage sein, gegen jede Entscheidung, die von einem automatisierten System bezüglich COVID-19 getroffen wird, Einspruch zu erheben (insbesondere gegen Apps, die feststellen, ob jemand mit einer infizierten Person in Kontakt gekommen ist und sich in Quarantäne begeben muss). Regierungen und Auftragnehmer:innen müssen sich an die Bestimmungen der DSGVO halten.

9. **Bereits bestehende ADM-Lösungen sollten nicht für COVID-19-Maßnahmen übernommen und weiterverwendet werden.** Denn automatisierte Systeme, die sich auf Trainingsdaten aus der Vergangenheit stützen, können aufgrund ihrer Konzeption nicht mit einer kurzfristigen Änderung der Bedingungen umgehen, unter denen sie eingesetzt werden. Vorhersagende Polizeiarbeit, automatisierte Unterstützung von Richter:innen, Bonitätsprüfungen und Bewertungen anderer ADMS können Ergebnisse liefern, die außerhalb ihres normalen Bereichs liegen (z.B. hinsichtlich der Fehlerraten). Solche Systeme sollten dringend überprüft (Audit) oder gar nicht eingesetzt werden.

10. **Eine Pandemie ist per Definition global. Es muss eine Reihe globaler, vielfältiger und koordinierter Reaktionen auf sie geben.** Ein weltweites Netzwerk von kooperierenden Organisationen der



Zivilgesellschaft, sollten den Umgang mit der Pandemie beobachten. Frühere Ausnahmesituationen haben uns gelehrt, dass Notlagen skrupellosen politischen Entscheidungsträger:innen den perfekten Vorwand bieten, um Infrastrukturen zur Massenüberwachung zu legitimieren, die unnötigerweise – und auf unbestimmte Zeit – die Rechte aller verletzen. Widerstand dagegen war nur dann (teilweise) erfolgreich, wenn er global, koordiniert und nachdrücklich formuliert war – mit Klarheit und Beweisen auf unserer Seite.

11. **Wir sollten dafür sorgen, dass diese Debatte über die COVID-19-Überwachung nicht in einem Vakuum stattfindet.** Einige ADMS, vor allem die Gesichtserkennung, haben sich bereits als problematisch erwiesen. Der derzeitige Ausnahmezustand kann nicht als Rechtfertigung für ihren Einsatz herangezogen werden: Im Gegenteil, alle Fragen, die in "normalen" Zeiten hervorgehoben werden – mangelnde Genauigkeit, systematische Voreingenommenheit (bias), allgemeine Bedenken hinsichtlich eines möglichen Missbrauchs biometrischer Daten – gewinnen in aussergewöhnlichen Zeiten, in denen die Gesundheit und Sicherheit aller auf dem Spiel steht, noch mehr an Bedeutung. Wir sollten nicht nur sicherstellen, dass diese entscheidende Debatte nicht von Technologen oder Technologien geführt wird, sondern auch dafür sorgen, dass die betreffenden Technologien nachweislich der Gesellschaft zugute kommen. Die Aussetzung der direkten persönlichen Kommunikation bietet die Möglichkeit, noch mehr soziale und andere grundlegende Dienstleistungen online zu verlagern, wo ADMS immer öfter Sachbearbeiter:innen ersetzen. Dies könnte katastrophale Folgen für die Bürger:innen haben, denen es an Zugang oder Mitteln mangelt, digitale Werkzeuge kritisch zu verstehen. Wir müssen sicherstellen, dass dies nicht geschehen wird.