

Resilienz im digitalen Zeitalter



Die zunehmende Digitalisierung aller Bereiche des Lebens ermöglicht vernetzte, schnelle und effiziente Interaktion und Kommunikation, hinterlässt zugleich aber auch überall ihre digitalen Spuren. Man muss davon ausgehen, dass alle Datenspuren, die Nutzende absichtlich oder unabsichtlich generieren, ein „geheimes Leben“ entwickeln – dass sie gesammelt, gespeichert, analysiert und miteinander kombiniert werden.¹ Diese Daten stellen eine reichhaltige Informationsquelle dar, die für kommerzielle oder propagandistische Zwecke genutzt werden kann. Datenschutz und Schutz der Privatsphäre sind dabei nur die Spitze eines Eisbergs. Andere Probleme betreffen etwa die potentielle Homogenisierung von Informationsumgebungen oder die verdeckte Einflussnahme auf den gesellschaftlichen Diskurs durch KI-getriebene Accounts, die automatisiert und massenhaft Falschinformationen und polarisierende Inhalte streuen.

All dies wirft die Frage auf, wie wir als Individuen und als Gesellschaft auf Probleme der digitalen Transformation vorbereitet sind. Resilienz ist ein nützlicher theoretischer Rahmen, um über solche Probleme nachzudenken. Im Kern bezeichnet Resilienz die Eigenschaft von Individuen und Systemen, existenzbedrohenden Gefahren zu widerstehen und ihre Funktion sowie ihren Bestand zu sichern. Überlegungen zu einer informationsbezogenen Resilienz können dabei nur interdisziplinär gedacht werden und betreffen alle Ebenen der Gesellschaft, Individuen, Institutionen und die Gesellschaft insgesamt – und auch die öffentlichen Diskurse sowie ihre Strukturen und Normen. Diskursive Resilienz etwa, wie sie im Beitrag von Bilandzic, Kalch, Kinnebrock, Buchner, Kollar und Schuller als Begriff entwickelt wird, ist die Fähigkeit des Diskurses auf digitalen Plattformen oder (sozialen) Medien und seiner Teilnehmer, mit negativen Phänomenen wie Polarisierung, Fragmentierung und Radikalisierung des Diskurses umzugehen. Psychische Resilienz wiederum bezieht sich auf die Widerstandsfähigkeit eines Individuums gegen äußere Widrigkeiten und kann, wie die Ausführungen von Göritz, Bührle und Wimmer zeigen, auch gezielt durch Resilienztrainings aufgebaut werden. Wie ein erfolgreiches Resilienztraining im Bereich Cybersicherheit aussehen kann, stellen Brehmer, Steinherr und Stöckl in ihrem Beitrag vor. Die Resilienz in der Beziehung zwischen Mensch und Maschine steht im Mittelpunkt der Ausführungen von Ziethmann, Friedrich und Schlögl-Flierl, wenn diese den Einsatz von synthetischen Daten in KI-Modellen im Bereich der Medizin untersuchen.

Relevant für das Thema Resilienz sind auch die sonstigen Beiträge aus diesem Heft, soweit sie sich mit dem Thema der Anonymisierung befassen. Wie wichtig es für einen resilienten Umgang mit Krisen ist, dass Staat, Gesellschaft und Wissenschaft für Problemlösungen auf eine entsprechende Datenbasis zurückgreifen können, hat die Corona-Krise eindrücklich vor Augen geführt. Datenschutz ist hier immer wieder dafür verantwortlich gemacht worden, dass es an einer solchen Datenbasis fehlt. Umso größer sind die Erwartungen, dass dank des Instruments der Datenanonymisierung der datenschutzkonforme Aufbau einer breiten Wissensbasis möglich ist. Welche Herausforderungen damit einhergehen, ist ebenfalls Thema der Beiträge im vorliegenden Heft.

Helena Bilandzic und Benedikt Buchner

¹ Sinnreich, A., & Gilbert, J. (2024). The secret life of data. Navigating hype and uncertainty in the age of algorithmic surveillance. The MIT Press.