

Cybersicherheit

Demokratie ist das Schutzschild gegen Missbrauch

Dr. Jasmin Lorch

German Institute of Development and Sustainability (IDOS)

Ani Tovmasyan

Unabhängige Forscherin und Beraterin



Bonn, 27. Oktober 2025. Zum Ende des European Cybersecurity Awareness Month (ECSM) im Oktober 2025 stellt sich eine entscheidende Frage: Wie wirken sich Cybersicherheitsmaßnahmen – wie Anti-Fake-News-Gesetze oder Initiativen zur Datenlokalisierung – in unterschiedlichen politischen Kontexten aus? Der ECSM wird unter anderem von der Europäischen Union, verschiedenen nationalen Regierungen – auch autokratischen – und globalen wirtschaftlichen Akteuren weltweit begangen, um Cybersicherheitsrisiken entgegenzuwirken. Doch ein Blick nach Asien zeigt, dass Cybersicherheitsmaßnahmen auch als Mittel der Repression eingesetzt werden können, wenn sie nicht in demokratische Institutionen und politische Praktiken eingebettet sind.

Cybersicherheitsgesetze als Mittel der Zensur

Unter Berufung auf Onlinesicherheit wenden mehrere asiatische Regierungen Gesetze zur digitalen Regulierung so an, dass sie staatliche Kontrolle über öffentliche Meinungsäußerung verstärken. Im zunehmend autokratisch regierten Indien schreiben das Gesetz zum Schutz digitaler personenbezogener Daten (2023) und damit verbundene Rechtsvorschriften zwar bestimmte Nutzer*innenrechte fest, erlauben es dem Staat aber zugleich, Unternehmen zur Herausgabe von Informationen aufzufordern und die Löschung von Onlineinhalten anzuordnen. Forschungsarbeiten zeigen, dass Autokraten Gesetze gegen Fake News und Verleumdung, die häufig in Rechtrahmen zur Onlineregulierung enthalten sind, zunehmend dazu nutzen, Kritiker*innen zum Schweigen zu bringen.

„Cybersicherheitsmaßnahmen können auch als Mittel der Repression eingesetzt werden, wenn sie nicht in demokratische Institutionen und politische Praktiken eingebettet sind.“

Dabei sind die Straftatbestände oft vage formuliert und lassen Regierungen viel Ermessensspielraum. So bezieht sich Kasachstans Gesetz von 2023 zu Internetplattformen und Internetwerbung sowohl auf Online-Ressourcen als auch auf Messaging-Apps wie WhatsApp und sieht Haftungspflichten für die vorsätzliche wie auch die unbeabsichtigte Verbreitung von „Falschinformationen“ vor. In Kirgistan kann die Regierung unter Berufung auf das Gesetz zum Schutz vor Falschinformationen von 2021 Inhalte verbieten, die sie als falsch erachtet. Das Online-Sicherheitsgesetz von 2024 in Sri Lanka kriminalisiert „falsche Aussagen“, „beleidigende Nachrichten“ und Inhalte, die „die öffentliche Ordnung stören“ – und ermöglicht so die politische Verfolgung von Regierungskritiker*innen. In Myanmar verleiht das Cybersicherheitsgesetz von 2025 der Militärdiktatur weitreichende Zensurbefugnisse. Zudem stellt es die Erbringung digitaler Sicherheitsdienstleistungen ohne staatliche Lizenz unter Strafe – vermutlich ein gezielter Angriff auf zivilgesellschaftliche Organisationen und Unternehmen, die digitale Sicherheitsschulungen anbieten.

Digitale Überwachung und Schikanen

Mehrere autokratische Regierungen kombinieren solche repressive Gesetze mit Cyber-Überwachung. Recherchen der thailändischen NROs iLaw und DigitalReach, des Citizen Lab und des Security Lab von Amnesty International deckten 2021 den Einsatz der Spionagesoft-

ware Pegasus gegen thailändische Pro-Demokratie-Aktivist*innen auf. Später stellte sich heraus, dass auch Oppositionelle, Journalist*innen und Regierungsvertreter*innen in Europa mit Pegasus überwacht wurden. Da Pegasus teuer ist, greifen Autokraten in Asien oft auch auf andere Überwachungssoftware zurück. Zudem setzen sie Sicherheitskräfte und Informant*innen ein, die soziale Medien gezielt nach regierungskritischen Äußerungen durchsuchen. In Kambodscha betonen Aktivist*innen, dass kritische Beiträge in den sozialen Medien rasch gelöscht werden und Online-Aktivist*innen oft ins Visier regierungstreuer Influencer*innen geraten. Einige berichten von physischen Repressionen durch die sogenannte „Cyberpolizei“ – womit digitale in physische Repression übergeht. „Sie werden dich finden. [...] Sie werden dich auf die Polizeistation vorladen“ oder „dich verhaften“ (Autorinneninterview 2025). Auch der Einparteiensstaat Vietnam kontrolliert soziale Medien und nutzt regierungsnahen Influencer*innen zur Verbreitung seiner eigenen Narrative.

Ambivalente Auswirkungen von Datenlokalisierung

Mehrere Regierungen in Asien fordern von Online-Plattformen, Datenverwaltern und Unternehmen, Daten auf lokalen Servern zu speichern. Datenlokalisierung kann legitimen Regierungszielen wie Datensouveränität und der Abwehr von Cyberangriffen dienen, in repressiven Kontexten aber auch zur Beschneidung digitaler Freiräume beitragen. Das vietnamesische Cybersicherheitsgesetz von 2019 verpflichtet Online-Dienstleister, die Daten von vietnamesischen Nutzer*innen auf Servern in Vietnam zu speichern. Dadurch können Behörden darauf zugreifen und Inhalte löschen lassen. Auch Usbekistan verlangt mit dem ergänzten Gesetz „über personenbezogene Daten“ von 2021, dass Internetanbieter und Social-Media-Plattformen Daten auf lokalen Servern speichern.

Dies macht deutlich, dass demokratische Rahmenbedingungen maßgeblich darüber entscheiden, ob Cybersicherheitsmaßnahmen tatsächlich Sicherheit schaffen. Ohne demokratische Schutzmechanismen können sie leicht als Instrument für Repression missbraucht werden. Diese Erkenntnis ist auch für Europa relevant, wo demokratische Staaten versuchen, Desinformation entgegenzuwirken und europäische Datensouveränität zu stärken, etwa durch den Auf- und Ausbau einer europäischen digitalen Infrastruktur. Aktuell scheinen solche Maßnahmen zweifellos notwendig, um demokratische Institutionen zu schützen, doch könnten sie von rechtsextremen Parteien missbraucht werden, wenn es diesen gelingt, an die Macht zu kommen. Umso wichtiger ist es, breite gesellschaftliche Unterstützung für demokratische Werte und Institutionen aufrechtzuerhalten und zu stärken.

Die aktuelle Kolumne ISSN 2512-9074

Zitationsvorschlag: Lorch, J. / Tovmasyan, A. (2025). Demokratie ist das Schutzschild gegen Missbrauch (Die aktuelle Kolumne 27.10.2025). Bonn: IDOS

© German Institute of Development and Sustainability (IDOS)