

Cyber Security

# Democracy is the firewall against abuse

Dr. Jasmin Lorch

German Institute of Development and Sustainability (IDOS)

Ani Tovmasyan

Independent researcher and consultant



Bonn, 27 October 2025. As the Cybersecurity Awareness Month of October 2025 ends, it is worth asking how cyber security measures, such as anti-fake news laws and data localisation, play out in different political contexts. This annual campaign is an initiative observed by the European Union, diverse national governments, including autocratic ones, as well as economic players worldwide to counter cyber security risks. However, examples from Asia show that cyber security measures can also become tools of repression unless grounded in democratic institutions and politics.

### Cyber security laws as means of censorship

Under the pretext of guaranteeing online safety, many governments in Asia employ digital regulation

laws in ways that can enhance state control over public expression. In autocratising India, the Digital Personal Data Protection Act (2023) and related delegated legislation enshrine certain user rights but, at the same time, empower the government to request information from companies and order the blocking of online contents. Research shows that autocrats increasingly use anti-fake news and anti-defamation laws, often included in digital regulation frameworks, to silence critics.

*“Examples from Asia show that cyber security measures can become tools of repression unless grounded in democratic institutions and politics.”*

Oftentimes, offenses are formulated vaguely, enabling ample government discretion. In Kazakhstan, the Law on Online Platforms and Online Advertising (2023), which pertains to online resources as well as messaging apps, such as WhatsApp, generates administrative liabilities for both willful and unintended dissemination of “false information”. Similarly, the Kyrgyz Law on Protection from False Information (2021) allows the government to ban content it deems false. In Sri Lanka, the Online Safety Act (2024) criminalises “false statements”, “offensive messages” and contents “disturbing public order”, enabling the political persecution of government critics. In Myanmar, the Cyber Security Law (2025) provides the military junta with broad-based censorship powers. Moreover, it criminalises the delivery of digital security services without a government license, a provision likely targeting civil society organisations (CSOs) and media organisations that provide digital security training.

#### **Online surveillance and harassment**

Several autocratic governments combine such restrictions with cyber surveillance. In 2021, investigations by the Thai NGOs iLaw and DigitalReach as well as the Citizen Lab and the Security Lab of Amnesty International revealed the deployment of the spy software Pegasus against Thai pro-democracy activists. The software was later found to have been used against opposition figures, journalists and state officials in Europe as well. While Pegasus remains expensive, autocratic governments across Asia also rely on other digital surveillance tools – as well as security officers and informers who monitor statements made by government critics on social

media. Cambodian CSO activists, for instance, emphasise that critical social media posts are quickly removed by the authorities and that online activists are often targeted by pro-government influencers. Some activists point to physical repression by “cyber police”, illustrating how online and offline repression intersect. “They will find you. [...] they will ask you to the police office”, or “arrest you” (author’s interview, 2025). Similarly, the one-party government of Vietnam tightly regulates social media, while also working with influencers to promote its own discourse.

#### **Ambiguous impacts of data localisation**

Several governments in Asia have begun to obligate online platforms, data fiduciaries and companies to store data on local servers. While data localisation responds to legitimate government concerns about data sovereignty and protection from cyber-attacks, it can curtail digital space, if the overall regulatory environment is repressive. The Vietnamese Cybersecurity Law (2019) requires that online service providers that collect or process data from Vietnamese users store such data on servers in Vietnam, enabling government authorities to access it and request the removal of content. Similarly, the amended Law of the Republic of Uzbekistan “On Personal Data” (2021) obligates internet providers and social media platforms to store user data inside the country.

These examples show that democratic institutions and a democratic regulatory environment are key for cyber security measures to act as a source of security rather than repression. This overall finding is also relevant for Europe, where democratic states seek to counter fake news and strive to enhance European data sovereignty, including by enhancing European digital infrastructures. Evidently, such measures are necessary to protect democratic institutions at this point in time. However, they could backfire if far-right parties managed to capture state power, highlighting the need to sustain robust social support for democracy.