

DIPLOMAT
19-11-22

The Quiet Evolution of Vietnam's Digital Authoritarianism

Digital rights in Vietnam are declining as a new system of surveillance and control has emerged in the country, with the support of Western tech giants.

By Gerard McDermott and Alice Larsson

On November 4, the Vietnamese Ministry of Information and Communications announced that authorities would enforce stricter regulations around the removal of “toxic” content from social media platforms. This new regulation requires that fake news is removed from social media within 24 hours, narrowing the previous window of 48 hours. Information deemed particularly sensitive may be taken down within three hours. Speaking at the National Assembly, Minister Nguyen Manh Hung warned that “false news, if it is handled slowly, will spread very widely.”

An annual report by Freedom House recently ranked Vietnam as the fifth worst country in the world for internet freedom. Scoring 22 out of 100, higher only than Cuba, Iran, Myanmar, and China, Vietnam's positioning remains unchanged from the year before, as the Vietnamese Communist Party (VCP) continues in its efforts to dominate the country's digital realm. Over the last decade, the VCP has been slowly tightening its control over the internet by ramping up online censorship, issuing harsh fines and prison sentences for the supposed misuse of social media, collecting citizens' online data, and compelling international tech giants to comply with the government's mounting requirements.

The VCP has ruled Vietnam as a one-party state since 1976. Since the mid-1980s, the country has experienced an exceptionally high level of economic growth and the country enjoys one of the highest levels of internet connectivity in the Asia-Pacific. Since the late 2000s, the Vietnamese state has undergone a quiet evolution in terms of its capabilities for monitoring its population online and censoring dissidents.

Similar to their counterparts elsewhere in Southeast Asia, netizens in Vietnam have experienced a significant and incremental decline in digital rights in recent years. The VCP government has passed repressive legislation, developed institutions for the purposes of surveillance and information control, developed a system for policing social media, and used bandwidth throttling to muffle dissenting voices. What is exceptional in the Vietnamese context has been the regime's ability to rein in Big Tech firms such as Meta (the parent company of Facebook) and use them to help enforce its emerging system of digital authoritarianism.

It has been argued that Vietnam is following in China's footsteps in terms of building its own “national internet,” yet what makes the VCP's brand of digital authoritarianism different to that of China, Russia, or Iran is the VCP's tolerance of foreign social media platforms, which have been incorporated into its system of surveillance and information control. As one of the world's fastest growing economies, many small and medium-sized enterprises in Vietnam heavily depend on Facebook for their business transactions. Banning foreign social media platforms outright risks upending social and economic behavior in a country that now has one of the highest numbers of Facebook users per population in the world.

On the premise of bringing law and order to the digital realm, the regime's latest Cybersecurity Law came into effect in 2019. This law differs from legislation that came before it by deftly shifting the burden of responsibility to service providers such as Google and Facebook, requiring that they open offices in Vietnam, store user data locally, and remove content at the request of government authorities.

It has dealt yet another blow to the few independent voices in the country, criminalizing anti-state rhetoric such as "denying revolutionary achievements," "causing confusion," or disseminating "anti-state" propaganda. Traditional media outlets are already under the control of the government (This, however, does not exempt them from heavy fines for publishing supposedly false information.) Access to international websites such as Human Rights Watch or the BBC is often difficult, and websites that are critical of the VCP, such as The Vietnamese, Luat Khoa, or Project 88, are inaccessible in the country.

Control over social media platforms is a demanding yet politically vital matter for the VCP. As Vietnam's internet penetration climbs to over 70 percent, due in large part to its growing youth population, the use of social media platforms such as Facebook and YouTube is also on the rise. The struggle between the VCP and Facebook peaked in 2020, when Facebook's servers in Vietnam were taken offline for several weeks in a bid to force compliance with the country's new censorship legislation. Faced with the prospect of being shut down entirely in a market reportedly worth \$1 billion in annual revenue, Facebook eventually bowed to the government's pressure, setting a dangerous precedent for the severe curbing of online expression.

Following a lengthy redrafting process, Decree 53 of the aforementioned Cybersecurity Law came into effect on October 1 this year, clarifying the rules that mandate all domestic companies and many foreign companies, including social media platforms, telecommunications services, payment providers, and gaming platforms, to store user data information locally and provide it to authorities upon request. Many bloggers, YouTubers, and online commentators have been severely punished for expressing their opinions and beliefs online, and the number of prison sentences handed down has persisted beyond the most recent crackdown on anti-regime rhetoric in the lead-up to the country's tightly controlled elections in 2021.

The U.S.-funded broadcaster Radio Free Asia, whose website is routinely blocked in Vietnam, claims that since the beginning of the year, more than 40 activists and Facebook users have been arrested or convicted, often on charges such as "anti-state propaganda." In October, a Facebook user with an online following of over 300,000 people was sentenced to two years imprisonment for online posts, which included "unverified information" that "negatively affected the stock market."

In October 2021, five independent journalists of Bao Sach (Clean Newspaper) received prison sentences of two to four years under Article 331 of the Penal Code for "abusing democratic freedoms" based on their Facebook and YouTube content. The following December, the activist Trinh Ba Phuong received a 10-year prison sentence under Article 117 of the Penal Code for "conducting anti-state propaganda." The trial was partially premised on Phuong's Facebook activity, including posts and livestreams.

Within the government, the Ministry of Public Security (MPS), Ministry of Information and Communications (MIC), and Ministry of Defense (MOD) are among those tasked with ensuring that toxic or "offensive" content is removed from online platforms. The MPS also has the

authority to revoke domain names and suspend information systems for national security purposes.

Following the introduction of Vietnam's new cyber laws, international tech giants have proved complicit in the censorship of online content. In 2021, the MIC reported that 3,377 posts were blocked or removed by Facebook, 13,141 videos were removed from YouTube, and 1,180 videos were removed from TikTok. (Twitter is not widely used in Vietnam.) Force 47, the cyber army overseen by the MPS, is also highly active on Facebook. Under the guise of protecting the public against the threat of "fake news," 10,000 "troops" report anti-government content and accounts, and endeavor to spread pro-government messages online.

Valentin Weber has argued that Vietnam is attempting to imitate China's system of surveillance and information control. China has trained diplomats from Vietnam in surveillance methods at its Baise executive leadership academy in Guangxi. Well-known Chinese cybersecurity firm Melya Pico has provided training to employees of the state in Vietnam. A recent meeting between the two heads of state led to the signing of number of agreements indicating that Sino-Vietnamese cooperation will greatly strengthen in the coming years. In addition to China, Russia has also been exporting defense technology to Vietnam for decades and the two authoritarian regimes are believed to cooperate with each other in a many different areas.

However, tools and techniques for enhancing the regime's digital authoritarian capabilities have mostly been home-grown or have come from a number of infamous private surveillance firms known to have operated in Vietnam in recent years. Israeli firm Cellebrite have been hired by the Vietnamese government. Cytrox spyware has been used in the country and cyberespionage firm Circles has also been recently employed by the government of Vietnam. Overall, Vietnam has received a significant amount of surveillance tech from Israeli firms. The employment of private surveillance firms by Hanoi is not a recent development. Infamous and now banned spyware firm FinFisher was assisting the regime to monitor dissidents as far back as 2013.

Vietnam has also shown itself to be highly competent in terms of its cyber-warfare capabilities. In 2020, the Vietnamese government was accused of sponsoring a cyberattack against China with the aim of attaining information about the outbreak of COVID-19. An elite team of hackers known as "Ocean Lotus" or "APT32" have become well-known in recent years for carrying out cyberattacks abroad, monitoring dissidents at home, and being involved in misinformation campaigns. State-sponsored attackers have also carried out technical attacks against websites run by the Vietnamese diaspora that are critical of the regime.

Notably, Vietnam has collaborated with its Southeast Asian neighbors in regional cybersecurity drills in the past. It also maintains a strong relationship with Singapore, signing an agreement related to cybersecurity with the republic last month. Singapore's own standards for digital rights and freedom of expression online have also declined in recent years.

Recently, COVID-19 has provided the state with the opportunity for the mass collection of data. Vietnam introduced contact tracing during the SARS epidemic of 2002-2004. During the COVID-19 pandemic, the government introduced Bluezone, a tracing app that collected a large amount of data from users. It later emerged that the type and amount of data collected by the app was significantly more than the government had publicly stated. Regulations for the handling of

this data have not been published and it is unclear whether the data will be deleted or anonymized after the pandemic.

The evolution of Vietnam's digital authoritarianism has been incremental, cautious, and shaped by the country's reliance on foreign investment. Taking into account the developments outlined above, it appears that the VCP is drifting in the same direction as other states in the region, such as Myanmar, Thailand, Cambodia, and Singapore. What is exceptional in the case of Vietnam is the regime's effective management and use of Big Tech in the suppression of dissent within its borders. Considering the "tech recession" that has recently begun, it is clear that the cooperative role of these firms will continue for the foreseeable future.

AUTHORS

GUEST AUTHOR

Gerard McDermott

Gerard McDermott is a PhD candidate at City University Hong Kong. He has previously published in *Kyoto Review of Southeast Asia*, *Prachatai*, *Politico*, and *Peace Review*. He is originally from the Republic of Ireland

GUEST AUTHOR

Alice Larsson

Alice Larsson is a MSc student in London. Formerly based in Vietnam, her research interests are human rights, interstate conflict, and civil unrest in Southeast Asia.