Activists: Cambodia’s Draft Cybercrime Law Imperils Free Expression, Privacy

By Sun Narin
October 11, 2020 02:42 AM

FILE - Critics say Cambodia’s draft cybercrime law could help the government intensify its crackdown on freedom of expression, while also raising privacy and data collection concerns.

PHNOM PENH, CAMBODIA - A recent draft of the cybercrime law obtained by VOA Khmer has drawn concerns from NGOs and rights groups over clauses that could help the government intensify its crackdown on freedom of expression, while also raising privacy and data collection concerns.

The draft law, the formulation of which was first announced in 2010, was intended to regulate Cambodia’s cyberspace, giving judicial police and courts access to investigate criminal infractions. However, an August draft of the law reveals that it could be used to further curtail freedom of expression while relying on vaguely defined scenarios to justify its implementation.

VOA Khmer provided Interior Ministry Secretary of State Bun Honn a copy of the leaked draft. The official refused to confirm the authenticity of the text, although he did not reject its contents. Bun Honn is in charge of drafting the long-delayed legislation.
“The discussions are not yet completed, and we haven’t asked approval from the government about the draft law,” he said. “Who gave the draft (to VOA Khmer)?”

Bun Honn attempted to dissuade journalists from reporting its contents.

**180 days of data**

The draft law requires service providers to “preserve traffic data for at least 180 days” in order to facilitate requests from “competent authorities.” However, the draft does not clearly outline the kinds of service providers that come under the scope of this law.

The draft states that any natural or legal person storing data on behalf of others or providing users the possibility of communicating through telecommunications systems is considered to be a service provider. It is unclear if this would be limited to internet and mobile service providers or also include cybercafes and organizations that provide internet access to their staff.

Article 45 of the draft would allow authorities to fine or imprison people who, using information technology, “knowingly or intentionally” make false statements that could be detrimental to “public safety,” “national security” and “friendly relations of Cambodia and other countries.”

If convicted, a person could face a maximum of three years in prison and up to $2,500 in fines, according to the draft law.

Similarly, Article 40 can be used to punish people for causing “interruptions, fear, threats, abuses, intimidation” through the use of computers. Maximum imprisonment under this article is six months in prison, the draft says.

Soeung Saroeun, executive director at the Cooperation Committee for Cambodia, which represents a coalition of local and international NGOs, said stakeholder consultations should be conducted before passing the draft law because it involves private sector service providers and the general public, who mainly use Facebook.

“At first glance, our concern is about the consumer’s privacy because service providers have the legal right to record and store for at least 180 days,” Soeung Saroeun said. “It is not right. How can privacy be protected?”

He also expressed concern about the draft article related to sharing of alleged fake news, which carries potential prison sentences.
“How do you define and protect from fake news?” Soeung Saroeun said, adding that people could share information that only later is shown to be untrue.

Soeung Saroeun said his organization had requested a copy of the draft law from the Interior Ministry on two occasions but received no response.

**Fake news arrests**

The government has detained individuals, mostly linked to the dissolved opposition Cambodia National Recuse Party, (CNRP) for posting social media messages in support of the party over the last three years, most recently when leader Sam Rainsy unsuccessfully attempted to return to Cambodia in November.

The government arrested more than 30 Cambodians from January to April, according to Human Rights Watch, for allegedly posting fake news. Human rights groups have classified this as an attempt to curb dissent over the administration’s handling of the viral outbreak and its economic impact.

The draft law contains provisions on other cybercrimes, such as identity theft, computer-related forgery and theft, intellectual property infractions and crimes related to pornography.

In June, a U.S. Justice Department expert conducted a workshop with Interior Ministry officials to discuss the draft legislation, according to the U.S. Embassy in Phnom Penh. Leading U.S. technology companies were present to provide feedback and best practices related to protection of fundamental rights and Cambodia’s information technology systems.

Chad Roedemeier, a U.S. Embassy spokesperson, said the diplomatic mission was aware of the draft law and had engaged with the government to emphasize the importance of the draft legislation protecting freedoms enjoyed by Cambodians and of taking into account the needs of users, citizens and businesses.

“A law that fails to balance Cambodia’s security needs with the needs of businesses and end users could negatively impact foreign investment and reduce opportunities for Cambodia’s small-to-medium-sized technology companies – both within and outside Cambodia,” Roedemeier said in an email.

“The human rights and fundamental freedoms that individuals have offline must also be protected online,” he said.
National Internet Gateway

Chak Sopheap, executive director at the Cambodian Center for Human Rights, said other clauses in the leaked draft law were problematic. She said her concerns relate to the use of terms such as “public order” and “security,” which, she noted, were vague and open to interpretation by authorities.

“There is no clear definition when stating about public order and security and the [national] interest,” she said.

Rights advocates have said that the lack of legislation to regulate the online space has not stopped the government from arresting and charging individuals for online expression. The government has also attempted to put into place infrastructure and frameworks to monitor online activity.

In July, the Cambodian government had proposed the establishment of a national internet gateway to control and monitor online traffic, drawing concern from rights groups and businesses.

The proposal was detailed in a prime ministerial order titled the “Establishment of the National Internet Gateway (NIG),” obtained by VOA Khmer, and states that once the NIG is established it will control all internet operations in the country.

In a May 2018 government notice, the Ministries of Telecommunications, Information and Interior formed a working group to monitor the accuracy of news on online media platforms and social media, with each ministry tasked with different roles in the online monitoring mechanism.

The government also instructed internet service providers to block 17 websites days prior to the 2018 national election because they were likely to “obstruct the election.” Ministries and provincial officials have also been asked to monitor content posted by citizens, including in private messaging groups.