ICNL INTERNATIONAL CENTER FOR NOT-FOR-PROFIT LAW

Five Things to Know

Zambia's Cyber Crimes Act 2025

In April 2025, Zambia's Parliament enacted the Cyber Crimes Act, 2025 ("the Act"). The Act imposes rules that could undermine online freedom of expression in Zambia.

1. The Act could undermine the right to use encryption and VPNs.

The Act criminalizes certain types of online communication that "deceive or mislead" as to the origin of the communication. Authorities could use this vague provision to disproportionately restrict legitimate tools such as encryption or Virtual Private Networks (VPNs) that enable users to communicate anonymously and securely, which are important aspects of the ability to exercise the rights to freedom of expression and privacy online. This undermines the safe and free use of online spaces for civil society and others to connect and gather.

2. The Act creates a criminal defamation offense that could chill online expression.

The Act criminalizes using a computer to disseminate false information, a statement, or an image that damages a person's reputation. Governments sometimes use this type of vague provision to target legitimate speech, such as criticism of prominent figures. For instance, a social media post voicing criticism based on the author's subjective opinions could be deemed a "false statement" that damages a person's reputation, violating the law. In 2023, Zambia decriminalized defamation in the Penal Code, in accordance with human rights norms, but the Act appears to re-criminalize it for online speech.

3. Prohibition of harassment is too broad and could restrict speech.

The Act prohibits the transmission of extremely broad categories of data and information. For example, a person may not transmit "obscene," "vulgar," or "lewd" data with the intent to humiliate or cause emotional distress to another person. Although such speech may be objectionable, the Act's provisions are so broad that they could target legitimate speech. For instance, an activist who transmits a satirical cartoon of a public figure could be deemed to have transmitted "vulgar" information intending to "humiliate" a person, which would violate the law.

4. Prohibition on "inauthentic data" is too broad and could restrict legitimate expression.

The Act prohibits taking actions that present "inauthentic data" in ways that could mislead another person about whether the data is authentic. The authorities have wide discretion to decide that data is inauthentic. For example, a research report containing economic data different from the government's official data could be deemed "inauthentic." This could unjustifiably restrict research and other forms of legitimate expression.

5. The Act creates offenses with significant criminal penalties.

Offenses under the Act are subject to criminal penalties. For instance, violating the Act's provision on "deceptive electronic communications" can result in a prison term of up to seven years. Civil society actors should familiarize themselves with the Cyber Crimes Act and take actions to avoid these significant penalties.

ICNL will continue to monitor legal developments around the Cyber Crimes Act 2025. For more information or to request our analysis of the Cyber Security Act 2025, please contact africa@icnl.org.

This brief is produced for informational purposes only and does not constitute legal advice or substitute for legal counsel. Laws may change, and interpretations of local law may vary.