

1 June 2017

Trinidad and Tobago: Major Problems Remain with Cybercrime Bill

The Centre for Law and Democracy (CLD) is deeply troubled by the government of Trinidad and Tobago's decision to reintroduce its Cybercrime Bill with only minor amendments to the previous draft. When it was first introduced in May 2015, the Cybercrime Bill was heavily criticised by media and human rights organisations, including CLD, for vague and overbroad content offences which would have prohibited a range of innocuous, normal or even beneficial online activity. Despite some minor revisions, the current version of the Cybercrime Bill still suffers from these problems.

"Overbroad content offences are always illegitimate, but are particularly dangerous online, where many people are still in the process of discovering their voice," said Michael Karanicolas, Senior Legal Officer at CLD. "The Bill, if passed in its current form, could have a substantial chilling effect on online speech in Trinidad and Tobago."

Some minor improvements have been made in the latest draft, notably the deletion of section 7, which prohibited the illegal interception of information and which duplicated an offence in the existing Interception of Communications Act. However, several other overbroad prohibitions remain, including sections 5, 6, 7, 8, 9, 12, 13 and 15. In each case, the prohibitions are so broad that they include perfectly legitimate online activity. Furthermore, the Cybercrime Bill creates a presumption of criminality for expressive activities which are undertaken "without lawful excuse or justification", shifting the onus onto users to demonstrate that their actions are legitimate. This type of reverse onus runs contrary to international freedom of expression standards, which only allow States to prohibit limited and clearly defined conduct. This problem is compounded by the fact that the term "justification" is unduly vague.

Sections 8 and 12 are particularly problematical insofar as they essentially make it illegal for journalists to receive leaked information, including from whistleblowers. Leaks often serve as an information safety valve, performing vital public functions, for example by drawing consumer attention to a defect in a product. Even when it is reasonable to sanction those who breach a computer system to obtain information or share information beyond its authorised recipients, journalists should be allowed to receive and report on the information they receive without fear of retaliation.

A problematical cyberbullying provision in the earlier draft has been removed, but this has been replaced by another problematical provision, section 18, which makes it illegal to use a computer system to communicate with intent to cause harm, including serious

emotional distress, to another person. A well-written news article about a war or famine may cause emotional distress. Similarly, an article about corruption would likely inflict harm, emotional and otherwise, on guilty officials. More broadly, international experience suggests that laws which aim to protect people against vaguely defined forms of emotional distress are often abused, for example by politicians to suppress legitimate criticism. Section 16, which prohibits the recording of non-consensual pornography, section 19, which prohibits online extortion and harassment, and existing offences in the Offences Against the Person Act, should give the police adequate tools to combat harmful online speech.

In 2015, when the Cybercrime Bill was first tabled, CLD urged the government of Trinidad and Tobago to revise it substantially before attempting to adopt it. The limited revisions which have been made do not go nearly far enough to resolve the Bill's major problems. We urge the government to consider major amendments to the Bill, in particular to narrow the scope of prohibited speech so that it only captures inherently harmful conduct, to protect third party recipients of information against any risk of sanction and to remove any offences based on the idea of inflicting emotional distress.

CLD's Analysis of the 2015 Cybercrime Bill is available via: <u>https://www.law-democracy.org/live/trinidad-and-tobago-problems-with-cybercrime-bill/</u>.

For further information, please contact:

Michael Karanicolas Senior Legal Officer Centre for Law and Democracy email: <u>michael@law-democracy.org</u> tel: +1 902 448-5290 www.law-democracy.org Twitter: @law_democracy