Physical Address: 1st Floor, Richmond Forum Building, 18 Cedar Avenue, Richmond, 2092
Postal Address: P.O. Box 30668, Braamfontein, 2017, South Africa
T: +27 (0)11 482 1913
F: +27 (0)11 482 1906
E: fxi@fxi.org.za
W: www.fxi.org.za

Attention: Mr SJ Robbertse

The Department of Justice and Constitutional Development,
Private Bag X81,
PRETORIA,
0001
Email: cybercrimesbill@justice.gov.za.

Date: 11 December 2015

SUBMISSION ON THE DRAFT CYBERCRIMES AND CYBER SECURITY BILL

Introduction

1. The Freedom of Expression Institute (FXI) is a not for profit non-governmental organization which was established in 1994 primarily to promote and advance freedom of expression and associated rights. The FXI envisions a society where everyone enjoys freedom of expression and the right to access and disseminate information and knowledge. Our mission is to defend freedom of expression and eliminate inequalities in accessing and disseminating information in South Africa and the region.

2. FXI welcomes the opportunity availed by the Department of Justice and Constitutional Development (DOJ&CD) to make written submissions on the

Draft Cybercrimes and Cyber Security Bill (hereinafter referred to as "the Bill") published for public comment on 2 September 2015.

3. However the FXI's has concerns regarding the Bill's potential to infringe the rights to freedom of expression, access to information and the right to privacy.

3.1 We endorse the submission of the Association for Progressive Communications (APC) which summarized this Bill as framed in manner which disregards public interest.

3.2 We are in solidarity with the submission of the Right to Know (R2K) campaign, which calls for the withdrawal and redrafting of the Bill as it will criminalize access to information particularly for investigative journalists and whistleblowers.

3.3 Our key concerns are around the definitions, the broad powers bestowed on the state and the disproportionate penalties set out by the Bill.

3.3 If effected the Bill would affect groups such as Whistleblowers, investigative Journalists and other human rights activists, who are in constant interaction or possession of information. It is our belief that this Bill would have a chilling effect on access to information and freedom of expression.

Regional developments

4. The recent efforts of the current Special Rapporteur on Freedom of Expression and Access to information to enhance free expression and access to information across continent reveals renewed efforts to achieve these rights. The FXI believes that new legislation in South Africa should strive to align with continental human rights vision, particularly regarding Freedom of expression and Access to Information.

4.1 The 'Model Law on Access to Information in Africa' of 2013 developed under the Special Rapporteur emphasizes 'public interest' as a ground to override attempts to withhold information in Article 25. In adherence to this, public interest should be a prominent feature of the proposed Bill.

4.2 The 'Model law on Access to information in Africa' also recommends African states to exempt criminal and civil liability for people who disclose or authorize the disclosure in good faith of any information, in Article 87 (1). We propose that 'good faith' explicitly be considered as a distinguishing feature even where access is on face value construed 'unlawful'.

5. Cybercrimes and cybercrimes related legislation on the African content have already started to have a dire effect on freedom of expression and access to information. For example;

5.1 In Angola the Law to combat crime in the area of information technology and communication of 2011 disallows "intent of changing or subverting the functioning of state institutions, to force the authorities to undertake certain actions, to abstain from carrying out such acts (…)". Thus the effects of this law present themselves as draconian and counter the public's interest.

5.2 The Cybercrime and Computer Related Crimes Bill of Kenya has been criticized for providing incredibly broad offences that could impinge the right to freedom of expression.

5.3 The Cybercrimes Act of 2015 of Tanzania prohibits publishing 'false or misleading information.' This law has so far been used to scrutinise bloggers who discuss matters of governance.

5.4 The FXI is aware of and makes reference to these regional developments, in an effort to highlight the concern and the potential dire effects of the Bill on the Constitutional rights to freedom of expression and access to information.

Submissions

6. As outlined above the FXI is concerned with the broad definitions provided by the Bill.

6.1 'Critical data' (section 1) under the Bill, includes 'data that is important for 'the security, defence or international relations of the Republic', 'protection of public safety' as well as 'records of a financial institution'.

This definition would allow for the infringement of the right to access information as data may be declared 'critical' on the premise that it is supposedly national security, defence, international relations or public safety. It should be clarified that the determination of such data is subject to scrutiny based on the values of transparency and accountability.

6.2 The definition of 'national critical information infrastructure' (section 1) is also too broad as the classification of data that is in possession of or under the control of 'any department of State or administration in the national, provincial or local sphere of government.' The definition thus includes information that is of public interest.

6.3 In adhering to the principle of legal certainty, it is recommended that the Bill provides definitions of 'lawful authority' and 'unlawfulness'; as this will strengthen the premise of the Bill as a legislative tool that is consistent with the rule of law. Furthermore, explicit definitions will facilitate fair interpretative processes in the courts of law.

6.4 The definition of 'computer terrorist activity' includes acts that 'threatens the unity and territorial integrity of the Republic (section 15 (5) (b) (i)(ii)) and intimidates, induces or causes feelings of insecurity among members of the public, or a segment of the public, with regard to its security, including its economic security, or to induce, cause or spread feelings of terror, fear or panic in a civilian population.' The Bill's definition of cyber terrorism is too broad and does not take explicit account of the Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004, which exempts lawful advocacy, protest, dissent or industrial action.

7. As it stands, the Bill provides for broad powers to the state that would have a negative effect on access to information and freedom of expression.

7.1 Section 58 (2) empowers the Cabinet member responsible for State Security to 'declare any information infrastructure or category or class of information structures as 'National Critical Information Infrastructure.' This includes information that is regarded as being 'such a strategic nature that any interference with them or their loss, damage, disruption or immobilization may 'cause any major economic loss, cause the destabilization of the economy', 'prejudice the security, defence, law enforcement or international relations, cause interference with or a disruption of an essential service' or 'create a public emergency situation'. This criteria is too wide and could be detrimental to the flow of information, particularly where to civil and political rights. It is recommended that declaration of national critical information infrastructure is shared with the relevant Chapter 9 institutions in endeavor to make conclusions which enhance public interest.

7.3 Section 65, grants the President the authority to enter into any agreement with foreign states on conditions deemed fit. These powers are provided without the requirement that the President adheres to the Constitution and International Human rights law when entering into these Agreements. It is recommended that the President is subject to the requirement of public disclosure of such information.

8. The Bill places limitations on the right to access information in a number of clauses.

8.1 Section 4 criminalizes the unlawful access to data, a computer device, a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure.

Restricting unlawful access to data such as personal and financial information is necessary; however the definitions of “access”, “critical data” and “national information infrastructure” are broad and overreaching, therefore likely to be problematic in realizing the right to access information.

8.2 Sections 28 to 34 of the Bill deals with the search for, access to and seizure of certain articles. These provisions allow for any member of a law enforcement agency or an investigator accompanied by a member of a law enforcement agency to access or seize any article, whether within the Republic or elsewhere. This can be done with or without a search warrant. Section 29 (c) and (d) permits a member of the law enforcement agency or an investigator to search any person who is believed on reasonable grounds to be able to furnish information of importance on a matter connected to the investigation and who is found near a container, on or at such premises, vehicle or aircraft as well as to search any person believed to furnish information related to the matter under investigation and who is nearby, uses or is in possession or direct control of any data, computer data and database amongst others. Anyone could be subjected to a search or seizure of articles as well as be subjected to targeted surveillance without proof of their actual involvement or knowledge of an offence. This would be an infringement to the right to privacy and requires further consideration in view of this right.

8.3 Section 16 (5) (b) criminalizes the possession, communication of, delivering, availing or receiving data which is in the possession of the State and which is classified as confidential. This section could be used to limit

access to information for investigative journalist and whistleblowers whose interests are in good faith to expose any irregularities including corruption or mismanagement of institutions which is important to ensure state accountability.

9. The Bill also infringes on the right to disseminate information through section 20 which deals with copyright infringements. The copyright offence in the Bill will criminalize virtually all activities related to copyright online. In its current wording, one would be penalized if it was believed that certain work is subject to copyright laws and would be prejudicial to the owner. The section does not take into account any legitimate reasons to use the work or consent given by the copy right owner as per the Copyright Act of 1978. FXI believes that copyright should not be used as a means to block access to and dissemination of information. The internet presents the finest and diverse source of information for people and this source should not be unjustly limited by copyright.

10. The fines and prison sentences imposed in the Bill for cybercrimes are excessive and may be seen as a means to censor online communities. Section 4 (2) (a) for example, sanctions accessing data, computer devices, computer networks and databases with a fine not exceeding R5 million or a period not exceeding 5 years.

Welcomed Provisions

11. The drafting of the Cybercrimes and Cyber security Bill, is important to ensure safeguards against criminal activities in the cyber world. The criminalization of acts such as the unlawful access to personal and financial information as well as the

unlawful possession, provision, receipt or use of passwords, access codes or similar data or devices, amongst others, are important in ensuring the privacy of individuals and the confidentiality of communications.

Conclusion

12. It is an undisputed fact that cybercrimes are increasing and states must have legislation to deal with offences. In drafting and implementing legislation, the spirit and purport of the Constitution as the supreme law of the land must be considered. Legislators must carefully balance all interests in society and meet the requirements of the limitation clause if rights are infringed. The Cybercrimes and Cybersecurity bill is a 'necessary evil' addition to South Africa's legislations; however, there are aspects of the Bill that unreasonably infringe on the rights of access to information and freedom of speech. These infringements must be expeditiously remedied in the revised versions of the proposed legislation.

13. The FXI appreciates the opportunity to make these representations and stresses that the comments above are made in the spirit of contributing to strengthening the responsible exercise of the right to freedom of expression on online platforms and promotion of the right to freedom of expression in South Africa.

14. We look forward to participating in the public hearings regarding the Bill.