



t +27 21 556 5502
a P.O. Box 50110
West Beach
Cape Town 7441
e info@forsa.org.za
www.forsa.org.za

To: Mr V. Ramaano

**PARLIAMENTARY PORTFOLIO COMMITTEE ON JUSTICE AND
CORRECTIONAL SERVICES**

Per e-mail: vramaano@parliament.gov.za

Re: Invitation for Comments on the **CYBERCRIME AND CYBERSECURITY BILL B6-**
2017 (Deadline: 10 August 2017)

Date: 10 August 2017

-
1. We refer to the invitation by the Parliamentary Portfolio Committee on Justice and Correctional Services ("the Committee") for written submissions on Bill B6-2017: The Cybersecurity and Cybercrime Bill ("the Bill").
 2. Freedom of Religion South Africa (FOR SA) is a non-profit organisation working to protect and promote religious freedom in South Africa, representing over 6 million people.
 3. FOR SA's interest in the Bill, lies in the potential implications of the Bill for freedom of religion and particularly freedom of (religious) expression in South Africa.
 4. We make the following written submissions to the Committee, **but would also appreciate the opportunity to appear and make verbal submissions at any hearings to be held with regard to the Bill.**
 5. While we appreciate the legitimate objectives of the Bill (to prevent and combat cybercrime), we are concerned that a number of provisions in the Bill are over-broad and may have certain unintended consequences.

6. Section 17: "Data message which is harmful"

6.1 Chapter 3 of the Bill relates to "*malicious communications*", and includes within its scope **data messages which are considered "*harmful*"**. In terms of s 17 of the Bill,

"(1) Any person who unlawfully and intentionally makes available, broadcasts or distributes, by means of a computer system, a data message which is harmful, is guilty of an offence.

(2) For purposes of subsection (1), a data message is harmful when –

(a) it threatens a person with –

(i) damage to any property belonging to, or violence against, that person; or

(ii) damage to any property belonging to, or violence against, any member of the family or household of the person or any other person in a close relationship with that person;

(b) it threatens a group of persons with damage to any property belonging to, or violence against, the group of persons or any identified person forming part of the group of persons or who is associated with the group of persons;

(c) it intimidates, encourages or harasses a person to harm himself or herself or any other person; or

(d) it is inherently false in nature and it is aimed at causing mental, psychological, physical or economical harm to a specific person or a group of persons,

and a reasonable person in possession of the same information and with regard to all the circumstances would regard the data message as harmful."

6.2 The practical implication of the above section is that if a person sends a (whatsapp, skype, tweet, e-mail, etc.) message that could be regarded as "*harmful*" (because it could incite others to cause damage to property, or hurt people); or if a person shares "fake news" on social media (that could have the same effect) - that person could, in terms of the Bill, be found guilty of a criminal offence and fined or imprisoned for three (3) years.

6.3 We are concerned that the above section, in its current form, violates the constitutional protection for Freedom of Expression for being over-broad. In terms of s 16(2) of the Constitution, the only permissible restrictions on Freedom of Expression are:

- 6.3.1 Propaganda for war;
- 6.3.2 Incitement of imminent violence; and
- 6.3.3 Advocacy of hatred that is based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm. (In this context, our courts have already interpreted “harm” as having an expansive meaning and extending beyond physical harm).

6.4 With regard to section 17(2)(c) in particular (i.e. the prohibition on “cyber-bullying”), the following:

- 6.4.1 While we appreciate the intention to protect vulnerable people from online harassment, we fear that this provision could have a chilling effect on Freedom of Expression which includes robust political expression that is often crude and unpleasant (but which, in terms of the Bill, would qualify as criminal offences). For example, in terms of this section, a statement such as “go jump off a bridge” (which is generally understood as “leave me alone”), or “break a leg” (which is generally understood as a “good luck” message), on a tweet or whatsapp message, could potentially qualify as a “harmful” (and therefore, criminal) message;
- 6.4.2 In any case, genuine cyberbullying should be dealt with in terms of the Protection from Harassment Act, 17 of 2011 which allows a person to get a protection order against their harasser (after which, continued harassment is a criminal offence).

6.5 With regard to section 17(2)(d) in particular (i.e. the prohibition on “fake news”), we are concerned that:

- 6.5.1 The term “*inherently false*” has not been defined anywhere, and is open to multiple interpretations and is itself subject to shifting social norms and opinions, rather than objective standards. For example, the issue of whether dagga use is beneficial or harmful to an individual, is contentious with both sides stating their opinions as scientific “fact”. If a person were to distribute one side of the story (because that is what he/she believes), the other side could potentially accuse the person of distributing something that is “*inherently false*” – and vice versa.
- 6.5.2 Also, because of the vagueness of the term, people who in fact are guilty of knowingly and intentionally sharing “fake news”, may escape liability; but on the

other hand, people who intentionally but ignorantly (not knowing that it is in fact “fake news”) share “fake news”, are potentially rendered criminals;

6.5.3 It is further not clear whose “*aim*” it should be to “*cause harm*”, in order for the message to qualify as criminal in terms of the Bill – the original author of the “fake news”, or the person who (on-)shares the “fake news” (intentionally, but again potentially ignorant of the original author’s intent or the potential effect of the message on another person or group). For example, one of the unintended consequences of the section in its current form, is that if a journalist (or indeed, any person) were to repeat the “fake news” in a news report (or post) for purposes of drawing attention to, commenting on, or critically evaluating the “fake news”, he/she may potentially be found guilty under this clause – even if his/her personal intent was not to cause harm to any person or group.

6.5.4 By including specific types of “*harm*” (e.g. mental, psychological, etc.) in the provision, it may be assumed that other types of harm are excluded. In the circumstances, it is best to limit the statement to “harm” rather than elaborating on the various types of harm that may (or may not) be included.

6.6 In view of the foregoing, **we recommend that section 17 of the Bill be amended to bring it in line with (and confine it to the limitations on free speech in s 16(2) of) the Constitution.**

6.7 Additionally, we propose that the common law defences that are available against a claim of defamation (e.g. jest, public media privilege, fair comment, etc.), be incorporated in section 17 of the Bill to avoid the unintended consequences explained above.

7. The broad powers and responsibilities of the State:

8. While we appreciate that the State has, of necessity, an important oversight role to play in the prevention and combating of cybercrime, we are concerned that the powers given to the State in terms of the Bill are far too broad, and therefore open to abuse. In particular, we mention the following:

8.1 In terms of sections 53 – 57, the Cyber Response Committee is tasked with implementing government policy relating to cybersecurity, and reports to the Joint Standing Committee on Intelligence. The Committee only allows participation by public entities after the Chairperson / entity / Director-General: State Security requests the Committee that they assist in writing. No provision is made for public involvement in a Committee that will have broad powers. No allowance is made for strong civilian oversight over, or engagement in, what can only be described as an internet 'policing agency'. (Sections 53 – 57)

8.2 In terms of section 56, "*the Cabinet member responsible for administration of justice must make regulations to regulate information sharing regarding cybersecurity incidents and the ... investigation ... of cybercrime.*" This section could potentially be used to withhold information from the public or civil society, as regulations do not need Parliamentary vetting and therefore effectively can be used to keep public interest organisations and the public in the dark about alleged cybercrimes etc. Public participation in the democratic government of the country is therefore handicapped and all fundamental rights are threatened.

8.3 In terms of sections 58, a private person / entity in control of a "*critical information infrastructure*" must, at its own cost, appoint an independent auditor to audit its compliance with the State's directives; and the State, through *inter alia* the Security Agency, will evaluate the adequacy and effectiveness of the audit. Failure to appoint an auditor is a criminal offence. This provision paves the way for invasive State interference in private entities, allowing it to invade privately owned data, devices, networks or physical infrastructures or buildings and issue directives accordingly. This is a major concern for the right to privacy (section 14 of the Constitution).

9. General Comments:

9.1 We have a general concern that, apart from s 17 of the Bill, a number of other provisions in the Bill are so broad, that the average person / internet-user would not be aware of the (potentially criminal) implications of using the internet, sending messages via e-mail or social media, or on other messaging platforms – and could easily (unknowingly, and without any intention to commit a cybercrime) find themselves on the wrong side of the law.

9.2 In particular, the broad provisions of the Bill (particularly in section 2 thereof) could potentially make “criminals” of innocent or well-meaning people who (through ignorance or indiligence, rather than deliberate hacking) mishandle other people’s personal data.

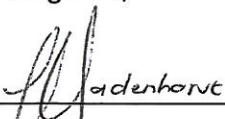
9.3 The Protection of Personal Information Act, 4 of 2013 (POPI) has already been passed to protect data and ensure that companies and individuals who handle other people’s personal data, do not misuse that information or violate their privacy.

9.4 Our concern is that this Bill, to a large degree, is an unnecessary duplication of POPI (which is not yet fully in operation. Ideally however, government should be putting its efforts and resources towards rolling out this Act, rather than creating a new law which to a large extent duplicates what is already there).

9.5 The requirements in terms of the Bill are particularly burdensome (from a finance, and capacity point of view) on religious and non-charitable organisations who are already heavily regulated and entirely reliant on the free-will offerings of their members, donors, etc. to cover their operation costs (including compliance with a host of statutory laws, including for example POPI).

5. We trust that these submissions will be of assistance to you, and look forward to receiving the dates of any public hearings to be held with regard to the Bill.

Kind regards,



Adv Nadene Badenhorst

Legal Counsel

Freedom of Religion South Africa (FOR SA)

E-mail: legal@forsa.org.za