SOUTH AFRICAN HUMAN RIGHTS COMMISSION

SUBMISSION ON THE CYBER-CRIMES AND CYBERSECURITY BILL [B6-2017]

For submission to the Portfolio Committee on Justice and Correctional Services

August 2017

SOUTH AFRICAN HUMAN RIGHTS COMMISSION

SUBMISSION ON THE CYBERCRIMES AND CYBERSECURITY BILL [B6-2017]

For submission to the Portfolio Committee on Justice and Correctional Services

August 2017

---

1. Introduction

The South African Human Rights Commission (SAHRC / Commission) welcomes the opportunity to engage with the Portfolio Committee on Justice and Correctional Services on the Cybercrimes and Cybersecurity Bill [B6-2017].

The SAHRC is aware of the expanding digital evironment and that communication and technological developments are evolving at a rapid pace. These are integral aspects of a modern world and as society shits to a digital environment the need for a legislative framework and the balancing of rights are becoming more critical. Through the Commission's complaint-handling process, it has seen an increase in the number of complaints relating to alleged rights violation which occur in the cyber environment. The Commission is also closely monitoring the international and national developments relating to the 'legislating the internet' and the various crimes which are perpetrated in the digital space. On this basis, the Commission shares its concerns on the Bill with the Portfolio Committee.

2. The mandate of the South African Human Rights Commission

2.1 Constitutional and Statutory Mandate

The SAHRC is a constitutionally created independent state institution. It is mandated by section 184 of the Constitution of the Republic of South Africa[1] which states,

> 184. (1) The South African Human Rights Commission must-
>
> (a) promote, respect for human rights and a culture of human rights;
>
> (b) promote the protection, development and attainment of human rights; and
>
> (c) monitor and assess the observance of human rights in the Republic.

In September 2014, the new South African Human Rights Commission Act 40 of 2013 came into effect, repealing its predecessor the Human Rights Commission Act 54 of 1994. Section 13 of the new Act expands on the powers and functions of the Commission.

Accordingly, section 13(1)(a)(i) provides,

> (a) The Commission is competent and is obliged to-
>
> (i) Make recommendations to organs of state at all levels of government where it considers such action advisable for the adoption of progressive measures for the promotion of human rights within the framework of the Constitution and the law, as well as appropriate measures for the further observance of human rights;

Section 13(1)(b)(v) further states,

> (b) The Commission-
>
> (v) Must review government policies relating to human rights and may make recommendations.

It is within the above mandate that the Commission shares its comments with the Portfolio Committee.

[1] Of 1996. Hereinafter the 'Constitution'.

3. SAHRC Concerns with the Cybercrimes and Cybersecurity Bill

3.1 Definitions Clauses

The SAHRC notes that there are several terms within the definitions clause which require further clarity. In this regard, the SAHRC points out the following in respect of the term 'access', which reads:

> **''access''**…includes, *without limitation,* to make use of data, a computer program, a computer data storage medium or a computer system or their accessories or components or any part thereof or any ancillary device or component to the extent necessary to search for and seize an *article*. (emphasis added)

Within this context, the Bill goes further to define 'article' as:

> **''article''** means any data, computer program, computer data storage medium or computer system which—
>
> *(a)* is concerned with, connected with or is, on reasonable grounds, believed to be concerned with or connected with the commission or suspected commission;
>
> *(b)* may afford evidence of the commission or suspected commission; or
>
> *(c)* is intended to be used or is, on reasonable grounds, believed to be intended to be used in the commission, of an offence in terms of Chapter 2 or sections 16, 17 or 18 or any other offence which may be committed by means of, or facilitated through, the use of such an article, whether within the Republic or elsewhere;

In reading these two clauses together, the SAHRC notes with concern the potential impact it may have on the right to privacy, (as protected under section 14 of the Constitution), particularly the 'without limitation' phrase. Effectively, under the Bill the State officials responsible for investigating cybercrimes, would be legally authorised to make use of data on the personal computer of a person, on the grounds that it is, 'concerned with'; 'connected with'; or has 'reasonable grounds' to believe that there is a connection with an offence. The SAHRC notes that there is no further clarity of these terms and that it may, from a practical perspective, lead to an inconsistent application of the provision. In addition, the Bill may impact the right to privacy on multiple grounds namely, i) 'person searched' if a mobile phone is on a person's body; ii) 'property searched' in terms of any device in a person's possession; and, iii) 'possessions seized' and 'communications infringed' in terms of 'data' being accessed

indiscriminately. The SAHRC therefore notes that the Bill vests a disproportionate amount of discretion and power to the official for the purposes of searching and accessing any person's device. Furthermore, if 'access' entails unfettered access to data, and 'data implies electronic representations of information in any form,' then authorities can access *any* electronic information of any person and possible do so without retribution. In addition, it may be implied that in order to invoke its sweeping orders under the Bill, officials would only need to suspect that a particular piece of data, a computer or any computer system may afford evidence of the commission or suspected commission of an offence. The SAHRC recommends that Parliament consider amending the definition of 'access' to rather adopt the term which relates to a 'reasonable limitation' to make use of data.

3.2 Clause 2: Cybercrimes

The Commission is concerned about the broadly defined nature of cybercrimes in the Bill. Clause (2)(1) and (2) reads that that

> **2.** (1) Any person who unlawfully and intentionally secures access to—
>
> *(a)* data;
>
> *(b)* a computer program;
>
> *(c)* a computer data storage medium; or
>
> *(d)* a computer system, is guilty of an offence.
>
> (2) For purposes of this section a person secures access to—
>
> *(a)* data when the person is in a position to—
>
> (i) alter, modify or delete the data;
>
> (ii) copy or move the data to a different location in the computer data storage medium in which it is held or to any other computer data storage medium;
>
> (iii) obtain its output data; or
>
> (iv) otherwise use the data;

The SAHRC notes with concern the use of the term 'intentionally' in the draft clause 2(1) and highlights instances where the draft provision may have unintended consequences. For example, the clause could potentially impact on investigative journalism and whistleblowing as data and information is often exchanged via electronic means listed under clause 2(1). This may have an impact on the rights of access to information and freedom of speech. Furthermore, the broad nature of the provision, particularly under clause 2(1)(a) may result in criminality of persons who may have access to information / data and subsequently deletes /

alters the data, but was unaware that it was obtained unlawfully and intentionally (in terms of the Bill). In order to circumvent these instances, it is recommended that the Portfolio Committee consider the definition of 'intent' within the Bill.

3.3 Clause 3: Unlawful acquiring of data

Clause 3(3) of the Bill reads that:

> 'Any person who is found in possession of data, in regard to which there is a *reasonable suspicion* that such data was acquired unlawfully as contemplated in subsection (1) and who is unable to give a *satisfactory exculpatory account* of such possession, is guilty of an offence'. (emphasis added).

The SAHRC notes that the Bill fails to provide guidance on what a 'reasonable suspicion' may be. This is concerning as it may result in an inconsistent understanding and application of the clause. The SAHRC recommends that the term is clearly defined.

In relation to the phrase, 'satisfactory exculpatory account', the SAHRC highlights several concerns, including, i) instances where a person may be unable to give a satisfactory exculpatory account, due to the fact that he / she does not speak the same language as the inquiring party; ii) that the term is subjective in nature; iii) that there is no clear guidelines on what would be considered as a 'satisfactory exculpatory account', and iv) that the clause, in its current form, may lead to inconsistent application by authorities. In order to address these issues, the SAHRC recommends that the Bill clearly define the term 'satisfactory exculpatory account'.

In addition, the SAHRC cross references to clause 5 of the Bill which relates to the aggravating factors which the court must consider when it imposes a sentence for cybercrimes. The factors are welcomed by the Commission, however it is suggested that a set of mitigating factors also be included when the court is imposing a sentence. Examples of potential mitigating factors may include for example, i) the nature and purpose of the clause 2 and clause 3 infringement; ii) the interests that are being protected or advanced by said infringement, and iii) the intention of the parties in infringing clauses 2 and 3.

3.4 Clause 16: Malicious Communications

Clause 16 of the Bill addresses malicious communications and further provides for instances to criminalise a data message. In particular, the clause reads that:

‘Any person who unlawfully makes available, broadcasts or distributes by means of a computer system, a data message to a specific person, group of persons or the general public with the intention to incite—

(a) the causing of any damage to any property belonging to; or

(b) violence against, a person or a group of persons is guilty of an offence.’

The SAHRC stresses that the public ought to be made aware that communications of this nature may incur criminal sanction and that a robust public education initiative is introduced to curtail communications of this nature. The SAHRC also recommends that the Bill is aligned to section 16(2) of the Constitution which guarantees freedom of expression but specifically recognises that it does not extend to the ‘incitement of imminent violence’ or the advocacy of hatred that is based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm.

3.5 Clause 17: Data message which is harmful

The SAHRC notes that clause 17 relates to data messages which are harmful.

17. (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 the 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 economic 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.

The SAHRC welcomes the intention of the clause. However, it requests clarity on what the implications may be for publication of 'fake news', which may not always necessarily be considered as 'harmful,' yet could have several implications in misleading the public.

The SAHRC further notes the inclusion of the 'reasonable person' standard in assessing the degree of harmfulness i.e. a *reasonable person* in possession of the same information and with regard to all the circumstances would regard the data message as *harmful*" (emphasis added). The Commission however recommends that in order to fully establish a reasonable person standard in the Bill, reference ought to be made to the context in which a data message may have been sent.

3.6 Clause 18: Distribution of a data message without consent

Clause 18 relates to the criminalisation in distribution of a data message without consent. The clause states that:

> **18.** (1) Any person who unlawfully and intentionally makes available, broadcasts or distributes, by means of a computer system, a data message of an intimate image of an identifiable person knowing that the person depicted in the image did not give his or her consent to the making available, broadcasting or distribution of the data message, is guilty of an offence.
>
> (2) For purposes of subsection (1), ''intimate image'' means a visual depiction of a person made by any means—
>
> *(a)* under circumstances that give rise to a reasonable expectation of privacy; and
>
> *(b)* in which the person is nude, is exposing his or her genital organs or anal region or, in the case of a female, her breasts.

The SAHRC welcomes the clause, noting the high levels of cyberbullying and the phenomenon of 'revenge porn'[2] where intimate images are shared by partners on a non-consensual basis. The SAHRC however notes the use of the term 'female' in clause 18(2)(ii)

[2] 'Revenge porn' is the term which has been coined for the sexually explicit portrayal of one or more people that is distributed without their consent via any medium and often distributed by a partner of the intimate relationship. See, https://en.wikipedia.org/wiki/Revenge_porn

and points out that the term is limited to biological status. It is recommended that the term is replaced with the word 'woman' which is broader, taking into account intersex, transgendered and persons with body variations, who identify themselves as woman.

3.7 Clause 27: Investigation, search and seizure

The SAHRC notes that clause 27 addresses instances where an article may be searched, accessed and seized by virtue of a search warrant and permits searches of a container, premises, vehicle, facility, ship or aircraft. The Commission specifically points out that clause 27(b)(2)(c) states that a search warrant must authorize the police official to,

> 'search any person who is believed, on reasonable grounds, to be able to furnish any information of material importance concerning the matter under investigation and who is found *near* such container, on or at such premises, vehicle, facility, ship or aircraft.' (emphasis added)

The SAHRC notes that the term 'near' within this context is unclear. It further highlights that the lack of guidance in this regard could potentially be used as justification to search persons outside the immediate scope of the item that was granted a warrant to be searched. Whilst the Commission notes that clause 31(1)(b) states that, 'a police official may without a warrant, as contemplated in section 40 of the Criminal Procedure Act, 1977, arrest any person—'whom he or she *reasonably suspects* of having committed any offence in terms of Chapter 2 or section 16, 17 or 18…', it expresses concern that the broad nature of the provision may lead to abuse. The Commission recommends that the standard for 'reasonable suspicion' within the context of the Bill is expanded upon to ensure a proper balance between the need to combat cybercrimes and the protection of personal dignity.

3.8 Clause 53: Cyber Response Committee

The SAHRC notes the establishment of a Cyber Response Committee (CRC), to implement the cyber initiative of the country. The Commission further notes that the CRC is comprised of state actors and recommends that chapter 9 organisations, experts in the field and civil society organisations are included on the Committee, so as to ensure that a diverse set of interests are represented.

It is critical that the CRC operates within a human rights framework to ensure the balancing of interests of law enforcement and fundamental human rights. Noting the sensitivity of

information that may be collected, especially in relation to personal information and safeguarding the right to privacy, the Bill should encourage a collaborative approach between the CRC, the Information Protection Regulator, the SAHRC, the Ministry of Home Affairs or the South African Revenue Services (SARS) and other relevant government agencies.

In addition, it is recommended that the CRC should prioritise the safety of children and women, to intercept/prevent crimes against this vulnerable groups in accordance with the United Nations Convention on the Rights of the Child and the Budapest Convention on Cybercrime.

4. Conclusion

The SAHRC recognises the need for a legislative framework to address cybercrimes and cybersecurity in South Africa and the need for delicate balance between freedom of expression and the right to privacy within the context of the Bill. As noted above, the broad aspects of some of Bill's provisions may impact on investigative journalism, informants and whistle-blowers. Furthermore, crimes under the Bill ought to be more narrowly defined and the intention of the parties should be a factor when prosecuting cybercrimes. The SAHRC also reiterates that the Bill would require extensive public education initiatives as well as regular training for officials who will be tasked with its implementation.

The SAHRC avails itself for engagement with the Portfolio Committee, to share its further insights on the Bill.

***