Telkom

Submission to the Select Committee on Security and Justice

Cybercrimes Bill, 2019

CONTENTS

1 INTRODUCTION

1.1 Telkom welcomes the opportunity to provide comments to Cybercrimes Bill, published on 23 October 2018.

1.2 Telkom commends the decision to constrain this Bill to cybercrimes and exclude cybersecurity from the ambit of this Bill.

1.3 Save where such comments have been addressed by the Bill, Telkom persists with arguments made in its joint submission with Cell C and Vodacom to the Cybercrimes and Cybersecurity Bill, 2017, submitted on 10 August 2017, as appropriate (the "Previous Submission").

1.4 In particular, Telkom reiterates and adds certain concerns with regard to powers to investigate, search, access and seize electronic communications (chapter 5), as well as obligations on electronic communications operators to preserve certain data.

1.5 We set out our further comments below.

2 COMMENTS

2.1 Definitions

a) Telkom notes the amendment of the definition of "computer" in the Bill. We are of the view however that the word *"computer"* cannot be defined to include "any data, computer program or computer data storage medium that are related to, connected with or used with such a device" and any such wording should be contained under a separate definition as appropriate.

2.2 Chapter 5 (Powers to investigate, search, access and seize)

2.2.1 Standard operating procedures

a) Telkom would like to emphasise the importance of clear Standard Operating Procedures to clarify the obligations set out in Chapter 5. We support a process of consultation with industry when drafting the Standard Operating Procedures and reiterate our comments in the Previous Submission that these operating procedures should also apply to the operations of private sector computer security incident response teams to ensure uniformity of process and ease of presentation of evidence in court. We further confirm that special procedures will be necessary as the investigative procedures provided for in Chapter 2 of the Criminal Procedure Act are not sufficient when it comes to procedures to investigate cybercrimes and dealing with electronic evidence.

b) It is further our understanding that the law on the conduct of search and seizure operations will be respected, and that search warrants will be served with due regard to the rights of individuals and the businesses to avoid interference with infrastructure and networks that can disrupt communications.

2.2.2 Interception of data and retention of data

a) Telkom notes the inclusion of a definition for the ‘’interception of data”.[1] Telkom proposes that the content of s40 be aligned with the heading of this section[2] in as far as references to archived communication-related information are proposed to be deleted from s40.

b) Telkom further suggests that the definition of interception should be aligned with the definition of same in RICA. In addition to this, any preservation or disclosure directions that fall outside the ambit of RICA should be handled in terms of a separate process to be put in place. We further caution that that there is no safeguard against duplicate costs due to obligations under RICA and the Bill that may serve the same purpose and deliver similar results.

c) The Bill seems to impose a new obligation on electronic communications service providers to retain the results of lawful interception (s48(7)(b) read together with s48(6)). There is no obligation in the RICA Act for service providers to store the results of any interception of any indirect communications for later disclosure and the results of interception are currently only delivered in real-time to the authorised destination. Furthermore, under RICA, there is clarity as regards the type of real-time or archived information that may be requested under direction from a Designated Judge as defined in RICA, as well as the manner in which such interception orders must be executed for fixed line and mobile services, voice and data services, real-time and messaging services. These targeted interception measures are applied with caution due to the nature of the information involved.

d) We note that the Bill defines “traffic data” to mean “data relating to a communication indicating the communication’s origin, destination, route, format, time, date, size, duration or type, of the underlying service.” We propose that this definition be aligned with the definition of communication-related information under RICA, as necessary. Should there be a new obligation on electronic communications service providers to retain the results of lawful interception, RICA would need to be amended to make provision for this. Any such amendment should further be in consultation with electronic communications service providers due to the substantial operational and financial impact on such service providers.

e) Telkom also takes note of the various directives which can be provided to electronic communications service providers, namely to provide real-time communication-related information in respect of a customer on an ongoing basis as it becomes available; expedited preservation of data and preservation of evidence directions to preserve such real-time communication-related information; a disclosure of data direction to provide real-time communication-related information in respect of a customer that was stored by the electronic communications service provider, and a direction to provide traffic data. In this regard, Telkom reiterates the need for a study to assess operational and financial implications on operators regarding requests for the preservation and expedited preservation of data.

f) Furthermore, when receiving preservation orders as envisaged in the Bill, electronic communications service providers might be placed in the situation that they cannot comply

[1] **“interception of data**"means the acquisition, viewing, capturing or copying of data of a non-public nature through the use of a hardware or software tool contemplated in section 4(2) or any other means, so as to make some or all of the data available to a person, other than the lawful owner or holder of the data, the sender or the recipient or the intended recipient of that data and includes the examination or inspection of the contents of the data; and diversion of the data or any part thereof from its intended destination to any other destination.

[2] The heading of s40 is “Interception of indirect communication, obtaining of real-time communication-related information and archived communication-related information.”

in full or partially with such orders because of *inter alia* inadequate storage capacity, hardware and software requirements. Telkom reiterates its concerns re the legal workload and costs to contest regular preservation orders on grounds of unreasonable expectations or substantive technical limitations. Telkom is concerned that orders to preserve data or evidence for the purposes of criminal proceedings in cases relating to cybercrime(s) may be served on an *ad hoc* basis, impose a heavy burden on operators depending on the nature of the information required and that the preservation of such information may in some instances be infeasible. It is further unclear whether a disclosure of data direction will contain further instructions to refine the data to be disclosed, such as the analysis and filtering of data, the format in which such data must be provided, or the preparation and pre-processing of data prior to submission for further forensic analysis, where such data processing/formatting facilities may not be readily available.

g) Finally, Telkom notes that the designated judge still refers to a judge designated in terms of RICA. The judge's duties are now, in addition to those under RICA, to further the objectives of preservation of data, evidence or other article, seizure of data, the expedited disclosure of traffic data and data obtained from interception and preservation. A judge can under s48 also order that in addition to real-time communication-related information, archived communication-related information be obtained and preserved. Clarification is required as to what extent the contents of directions contemplated under RICA may deviate from directions contemplated under the Cybercrimes Bill, in particular as all the directions are issues by a judge designated in terms of RICA.

2.3 Chapter 9 - Obligations of Electronic Communications Service Providers and Financial Institutions

2.3.1 Reporting of Cybercrimes

a) With regard to the Obligations of Electronic Communications Service Providers and Financial Institutions as set out in s54[3], Telkom confirms that there is no obligation an electronic communications service provider to monitor the data it transmits or stores or actively seek information indicating criminal activity.

[3] S54(1) provides that "An electronic communications service provider or financial institution that is aware or becomes aware that its computer system is involved in the commission of any category or class of offences provided for in Chapter 2 and which is determined in terms of subsection (2), must (a) without undue delay and, where feasible, not later than 72 hours after having become aware of the offence, report the offence in the prescribed form and manner to the South African Police Service; and (b) preserve any information which may be of assistance to the law enforcement agencies in investigating the offence. S54(2) provides that "The Cabinet member responsible for policing, in consultation with the Cabinet member responsible for the administration of justice, must by notice in the Gazette, prescribe the category or class of offences which must be reported to the South African Police Service in terms of subsection (1); and the form and manner in which an electronic communications service provider or financial institution must report offences to the South African Police Service." S54(3) states that "An electronic communications service provider or financial institution that fails to comply with subsection (1), is guilty of an offence and is liable on conviction to a fine not exceeding R50 000." S54(4) states that "Subject to any other law, or obligation, the provisions of subsection (1) must not be interpreted as to impose obligations on an electronic communications service provider or financial institution to monitor the data which the electronic communications service provider or financial institution transmits or stores; or actively seek facts or circumstances indicating any unlawful activity."

3 GENERAL

3.1 Telkom is of the view that where information stands to be preserved by an electronic communications provider, the ambit of same as well as the time period for which the information stands to be preserved, should be reasonable.

3.2 Further, in light of the fact that electronic communications service providers are mere conduits of information or data, Telkom reiterates the request for the inclusion of a "mere conduit clause", specifying that "electronic communications service providers shall not be criminally liable for criminal actions committed on its network unless they (electronic communications service providers) have intentionally and unlawfully committed an offence under the Cybercrimes Act."

4 CONCLUSION

Telkom supports the Cybercrimes Bill as an important step to fight cybercrime. However, we are concerned with regards to the effect of various directives and obligations on operators to retain real-time electronic communications and caution that there is a need for reasonable expectations as regards the fulfilment of these directives. We emphasise that clear Standard Operating Procedures regarding the search and seizure of data, drafted in consultation with industry, is imperative to clarify the ambit of such directives as well as avoid any unintended effect on electronic communications networks as well as the interruption of electronic communications services to customers.

We trust that the above is in order and would like the opportunity to make oral representations in due course.

---THE END --